Mathematik Entdecken I* und II*

Alexandru Constantinescu

15. November 2024

Freie Universität Berlin
2022-2023

* Das ist kein Skript. Es sind nur meine Notizen zur Vorlesung. Fehler können und werden vorkommen.

Inhaltsverzeichnis

Literaturverzeichnis

Die Reihenfolge ist "Vorlesung-chronologisch".

[Webseite] http://userpage.fu-berlin.de/aconstant/ME1.html

[Hou2012] Kevin Houston, *Wie man mathematisch denkt. Eine mathematische Einführung in die mathematische Arbeitstechnik für Studienanfänger*, Heidelberg: Springer Spektrum, **2012**.

[Rau08] Wolfgang Rautenberg, *Grundkurs Mengenlehre*, Skript FU Berlin, http://page.mi.fu-berlin.de/raut/Mengenlehre/m.pdf **2008**.

[AZ99] Martin Aigner und Günter M. Ziegler, *Proofs from the Book*, Berlin, Germany (1999).

Voraussetzungen

Das Hauptziel dieser Vorlesung ist, Ihnen die Instrumente zu geben, damit Sie sich selbstständig in der Welt der Mathematik bewegen können, damit Sie die Mathematik selbst entdecken können. Insbesondere bedeutet dies: Mathematik lesen und Mathematik schreiben. Das klingt viel einfacher, als es ist, und das wird auch die größte Herausforderung sein: zu akzeptieren, dass wir (alle von uns) uns noch verbessern können. Eine zweite Herausforderung ergibt sich aus der Natur der Mathematik. Im Vergleich zu vielen anderen Disziplinen, in denen die zentralen Objekte des Studiums klar sind (wie z.B. *Felinologie*) oder nur wenige wissen, worum es geht (wie z.B. *Paleophytologie*), haben die meisten Menschen eine Vorstellung davon, was Mathematik ist. Sehr oft haben die Leute auch Gefühle darüber. "Ich liebe/hasse Mathematik" ist eine der häufigsten Reaktionen, die ich bekomme, wenn ich jemandem sage, dass ich Mathematiker bin. Das führt zur zweiten Herausforderung: Wissen wir wirklich, was es ist? Und sind unsere Gefühle darüber wirklich ehrlich? Das werden wir herausfinden. Was man von Anfang an akzeptieren muss, ist, dass die Mathematik nicht der Realität unterworfen ist. Sicher, die Anfänge, vor Tausenden von Jahren, waren fast immer das, was wir heute angewandte Mathematik nennen würden. Aber seit Euklid hat sich die Mathematik von der Realität abgekoppelt. Die Rechtecke sind nicht mehr Stücke Agrarland, sondern ideale Rechtecke. Genau wie die Zahl 5 nicht mehr 5 Äpfel oder 5 Säcke Korn oder 5 Finger ist. Fünf ist jetzt eine Idee, die der Mathematik gehört.

Also, was sind die Voraussetzungen? Die mathematischen Voraussetzungen sind minimal: den Umgang mit Zahlen beherrschen und die grundlegenden Symbole der Mathematik kennen, wie z. B. $+, -, \cdot, =, \frac{1}{2}$. Noch wichtiger sind jedoch folgende Voraussetzungen:

I **Interesse.** Sie haben Interesse an der Mathematik selbst. Nicht daran wie diese angewandt werden kann, oder daran welche Vorteile sie auf dem Arbeitsmarkt bringen kann. Diese Aspekte sind auch sehr wichtig. Sie sind aber nicht worum es in dieser Vorlesung geht.

II **Leistung.** Sie akzeptieren, dass die eigentliche Leistung von Ihnen kommen muss. Wir sind da, um alle Ihre mathematischen Fragen zu beantworten und um Erklärungen zu geben[1]. Aber die Ideen und Techniken die wir hier Darstellen, müssen Sie sich selber, durch Übung und Arbeit, aneignen.

III **Kommunikation.** Es hilft Fragen zu stellen. Nicht nur weil man Antworten bekommt, sondern weil man eigene Ideen und Lücken erst verstehen muss. Also fragen Sie so oft wie es Sinn hat. Und versuchen Sie auch Fragen der anderen zu beantworten.

IV **Falsch liegen.** Falsche Antworten sind genau so gut wie die richtigen. Sicher, nicht bei Klausuren/Hausaufgaben. Aber in den Tutorien/Zentralübung/Vorlesung versuchen Sie Fragen zu beantworten, auch wenn Sie nicht sicher sind, dass Ihre Antwort richtig ist. Das hilft dem Lernprozess viel mehr als Sie denken.

V **Ehrlichkeit.** Seien Sie ehrlich mit sich selbst. Macht Ihnen Mathematik Spaß? Fliegt die Zeit vorbei wenn Sie an einer Matheaufgabe arbeiten? Oder verlieren Sie die Geduld wenn Sie den Lösungsweg nicht gleich sehen? Mathematik kann unglaublich viel Spaß machen! Wenn es aber kein bisschen Spaß bringt, dann kann das Mathestudium oder eine Karriere die auf Mathematik zentriert ist eine Belästigung sein. Das gilt natürlich für alles im Leben, aber durch die Einsamkeit des Mathematikers und die abstrakte Natur der Disziplin ist das in diesem Fall ein bisschen wichtiger.

[1] So oft wie menschlich möglich.

Wichtige Zeichen

$\neg$ **oder** nicht()	Negation
$\Rightarrow$	impliziert
$\Longleftrightarrow$	äquivalent
$\forall$	für alle
$\exists$	es existiert
$\exists!$	es existiert und ist eindeutig
$\in$	ist ein Element von / ist in
$\emptyset$	die leere Menge
$\subseteq$	ist eine Teilmenge von (darf gleich sein)
$\subsetneq$	ist eine Teilmenge von, aber nicht gleich
$\cap$	Schnitt
$\cup$	Vereinigung
$\setminus$	Mengendifferenz
: **oder** $\mid$	mit der Eigenschaft, dass (wenn man eine Menge definiert, z.B. $\mathbb{N}_{>0} := \{n \in \mathbb{N} \ : \ n > 0\}$)
(a, b)	geordnetes Paar **oder** das offene Interval
$\sharp A$ oder $\lvert A \rvert$	die Kardinalität der Menge A
$A \to B$	eine Abbildung von A nach B
$A \hookrightarrow B$	eine injektive Abbildung von A nach B
$A \twoheadrightarrow B$	eine surjektive Abbildung von A nach B
$\mapsto$	bildet ab auf
f^{-1}	die inverse Abbildung **oder** das Urbild (wobei f eine Abbildung ist)
$\mathbb{N}$	die Menge der natürlichen Zahlen (samt 0)
$\mathbb{N}_{>0}$	die Menge der positiven natürlichen Zahlen
$\mathbb{Z}$	die Menge der ganzen Zahlen
$\mathbb{Q}$	die Menge der rationalen Zahlen
$\mathbb{R}$	die Menge der reellen Zahlen
$\mathbb{C}$	die Menge der komplexen Zahlen
i	die imaginäre Einheit. Es gilt $i^2 = 1$
$\overline{z}$	die konjugiert komplexe Zahl zu z
$\lvert z \rvert$	der Betrag von z
$\sum$	Summe
$\prod$	Produkt
$a \mid b$	a teilt b
$b \vdots a$	b ist teilbar durch a

Tabelle 1: Häufig beuntzte Symbole

α	A	Aplha	β	B	Beta	γ	Γ	Gamma
δ	Δ	Delta	ε	E	Epsilon	ζ	Z	Zeta
η	H	Eta	θ	Θ	Theta	ι	I	Iota
κ	K	Kappa	λ	Λ	Lambda	μ	M	My
ν	N	Ny	ξ	Ξ	Xi	o	O	Omikron
π	Π	Pi	ρ	R	Rho	σ	Σ	Sigma
τ	T	Tau	υ	Υ	Ypsilon	φ	Φ	Phi
χ	X	Chi	ψ	Ψ	Psi	ω	Ω	Omega

Tabelle 2: Griechisches Alphabet

Teil I

Mathematik Entdecken 1

Kapitel 1

Die Bausteine

Notation

Wir werden folgende Zahlen-Mengen als bekannt annehmen[1]

Die natürlichen Zahlen	$\mathbb{N}$	$=$	$\{0, 1, 2, \dots\}$
Die ganzen Zahlen	$\mathbb{Z}$	$=$	$\{\dots, -2, -1, 0, 1, 2, \dots\}$
Die rationalen Zahlen	$\mathbb{Q}$	$=$	$\{\frac{a}{b} \ : \ a, b \in \mathbb{Z} \text{ und } b \neq 0\}$
Die reellen Zahlen	$\mathbb{R}$	$=$	$\{\mathbf{x}.\mathbf{y} \ : \ \mathbf{x} = \text{endlich viele Ziffern}, \mathbf{y} = \text{unendlich viele Ziffern}\}$
Die komplexen Zahlen	$\mathbb{C}$	$=$	$\{a + i \cdot b \ : \ a, b \in \mathbb{R} \text{ und } i^2 = -1\}$.

Wenn a eine natürliche Zahl ist, dann schreiben wir $a \in \mathbb{N}$. Wenn a eine ganze Zahl ist, $a \in \mathbb{Z}$, usw. Mehr über dieser Notation finden Sie in Teil 1.2.1.

Die reellen Zahlen können besser beschrieben werden[2].

Man sollte noch bemerken, dass die natürlichen Zahlen bei Null beginnen. Das war historisch nicht immer so, und auch heute fangen für viele Autoren[3] die natürlichen Zahlen mit 1 an. Für uns wird aber Null eine natürliche Zahl sein.

1.1 Mathematische Aussagen

1.1.1 Definition und Beispiele

Definition 1.1. Eine **Aussage** ist ein Satz, der entweder *wahr* oder *falsch* ist - **aber nicht beides**.

Also nicht alle Sätze sind Aussagen. In vielen Fällen kann das vom Kontext abhängig sein.

Beispiele:

[1] Auch wenn die genauen und gründlichen Definitionen gar nicht einfach sind, für unsere Zwecke hier werden die "naiven" Definitionen reichen.

[2] Zum Beispiel die berühmte Kreiszahl π kann als Verhältnis zwischen dem Umfang und den Durchmesser eines beliebiges Kreises beschrieben werden. Diese elegante und wichtige Beschreibung wäre nicht sichtbar auch wenn man die vollständige Dezimalbruchentwicklung kennen würde.

[3] Insbesondere in [Hou2012], die Hauptquelle für den ersten Teil dieses Kurses, ist die Konvention anders: dort ist $\mathbb{N} = \{1, 2, \dots\}$.

(i) “Heute ist Montag.”

(ii) “2+2=4.”

(iii) “Alle Katzen sind grau.”

(iv) “Alle Katzen sind nicht grau.”

(v) “Es gibt Katzen die nicht grau sind.”

(vi) “0=1.”

(vii) “x ist eine ungerade Zahl.”

(viii) “Die Wurzel einer natürlichen Zahl ist rational.”

(ix) “$x > 0$”.

(x) “Dieser Satz ist falsch.”

Bemerkung 1.2. Ich will die abstrakte Schreibweise der Prädikatenlogik vermeiden. Ich finde Mathematik schöner wenn diese in einer natürlichen Sprache geschrieben ist. Dafür muss aber die Genauigkeit nicht geopfert werden. Deswegen ist es für Mathe-Anfänger immer eine gute Übung mathematische Sätze in präzise Prädikate umzuformulieren.

Wir werden Aussagen mit großen Buchstaben bezeichnen: A, B, usw.

1.1.2 Wahrheitstabellen und Negation

Wie in der Definition 1.1 festgelegt, ist eine Aussage entweder *wahr* oder *falsch*. Wir tragen das in einer so genannten Wahrheitstabelle als **Input** ein:

A
wahr
falsch

Definition 1.3. Die **Negation** der Aussage A ist die Aussage, die falsch ist, wenn A wahr ist, und umgekehrt. Wir bezeichnen das mit nicht(A) oder $\neg A$.

Das heißt, dass wir für nicht(A) folgende Wahrheitstabelle (in Abhängigkeit von den Wahrheitswert von A) haben. Die erste Spalte ist der Input, und die zweite der Output[4].

A	nicht(A)
wahr	falsch
falsch	wahr

Negationen von einfachen Aussagen sind auch einfach. Interessanter wird es später wenn wir Implikationen und Quantoren betrachten.

Beispiel 1.4. Die Negation von A : *Die natürliche Zahl n ist eine gerade Zahl.* ist

nicht(A): *Die natürliche Zahl n ist* **nicht** *eine gerade Zahl.*

Das kann auch als *Die natürliche Zahl n ist eine ungerade Zahl.* formuliert werden.

[4] Allgemein sind die Spalten der kleinsten Bausteine die Input-Spalten, und der Output sind die Spalten der Wahrheitstabelle für zusammengesetzte Aussagen.

Bemerkung 1.5. Die Negation der Negation einer Aussage ist zu der ursprünglichen Aussage **logisch äquivalent**. Das heißt, dass die entsprechenden Spalten in der Wahrheitstabelle gleich sind:

A	nicht(A)	nicht(nicht(A))
wahr	falsch	wahr
falsch	wahr	falsch

1.1.3 Und & Oder

Zwei Aussagen können mit Hilfe der logischen Verknüpfungen **und** und **oder** zu einer neuen Aussage verbunden werden. "Und" verhält sich sehr ähnlich mit dem umgangssprachlichen *und*. Das heißt, die Aussage "A und B" ist nur dann wahr, wenn sowohl A als auch B wahr sind. Sonst ist "A und B" falsch. Bei "Oder" muss man ein bisschen mehr aufpassen, weil es ein **einschließliches** oder **inklusives Oder** ist. Das heißt, damit die Aussage "A oder B" wahr ist muss mindestens eine der zwei Aussagen wahr sein; es dürfen aber auch beide wahr sein. Somit ist "A oder B" falsch genau dann, wenn sowohl A als auch B falsch sind. Hier ist das ganze in Wahrheitstabellen zusammengefasst:

A	B	A und B	A oder B
w	w	w	w
w	f	f	w
f	w	f	w
f	f	f	f

Bemerkung 1.6. Es seien A, B und C beliebige Aussagen.

1. Die Aussage "nicht(A und B)" ist zu der Aussage "nicht(A) oder nicht(B)" logisch äquivalent.
2. Die Aussage "nicht(A oder B)" ist zu der Aussage "nicht(A) und nicht(B)" logisch äquivalent.
3. Die Aussage "A und (B und C)" ist zu der Aussage "(A und B) und C" logisch äquivalent.
4. Die Aussage "A oder (B oder C)" ist zu der Aussage "(A oder B) oder C" logisch äquivalent.
5. Die Aussage "A und (B oder C)" ist zu der Aussage "(A und B) oder (A und C)" logisch äquivalent.
6. Die Aussage "A oder (B und C)" ist zu der Aussage "(A oder B) und (A oder C)" logisch äquivalent.

Beweis-Skizze: Übung. Q.E.D.

Eine **Tautologie** ist eine Aussage, deren Wahrheitstabelle für jeden Input immer *wahr* als Output gibt. Zum Beispiel:

$$A \text{ oder nicht}(A).$$

Eine **Kontradiktion** (oder ein Widerspruch) ist eine Aussage deren Wahrheitstabelle für jeden Input immer *falsch* als Output gibt. Zum Beispiel:

$$A \text{ und nicht}(A).$$

[1] 16.10.'24

1.1.4 Quantoren

Der Ausdruck "für alle" wird als der **Allquantor** bezeichnet, und wird als $\forall$ geschrieben. Zum Beispiel:

$$\forall a \in \mathbb{N} \textit{ ist } 2a+1 \textit{ eine ungerade Zahl}. \tag{1.1}$$
$$\forall a \in \mathbb{N} \textit{ gilt } 2a+3=5. \tag{1.2}$$

Um die Wahrheit einer Aussage, die mit $\forall x \ldots$ anfängt, zu überprüfen, muss man sich vorstellen dass man ein beliebiges Element x gegeben hat (und es nicht selber wählt!) und damit umgehen muss. Dieses x sollte mit jedem anderen Element mit der gegebenen Eigenschaft ersetzbar sein ohne unserer Argumentation zu schaden.

Der Ausdruck "es gibt" wird als der **Existenzquantor** bezeichnet, und wird als $\exists$ geschrieben. Zum Beispiel:

$$\exists\, a \in \mathbb{N} \textit{ mit } 2a+1 \textit{ gerade}. \tag{1.3}$$
$$\exists\, a \in \mathbb{N},\ \textit{sodass } 2a+3=5. \tag{1.4}$$

Um die Wahrheit einer Aussage, die mit $\exists\, x \ldots$ anfängt, zu überprüfen, muss man ein Element selbst finden das eine gegebene Eigenschaft erfüllt.

Die Quantoren $\forall$ und $\exists$ kommutieren nicht! Zum Beispiel:

$$\forall a \in \mathbb{N}, \exists\, b \in \mathbb{N},\ \textit{sodass } \ b > a \textit{ gilt},$$

sagt uns, dass es keine größte natürliche Zahl gibt. Aber:

$$\exists\, b \in \mathbb{N},\ \textit{sodass } , \forall a \in \mathbb{N} \ \ b > a \textit{ gilt},$$

sagt uns, dass es eine größte natürliche Zahl gibt: b. Das ist falsch.

Die Negation einer Aussage die Quantoren enthält erfolgt nach dem Prinzip:

$$\begin{aligned} \text{nicht}\,(\forall x \textit{ gilt } A(x)) \quad &\Leftrightarrow \quad \exists\, x \textit{ sodass } \text{nicht}(A(x)) \\ \text{nicht}\,(\exists\, x \textit{ sodass } A(x)) \quad &\Leftrightarrow \quad \forall x \textit{ gilt } \text{nicht}(A(x)) \end{aligned}$$

Die **Negation von $\exists$ ist $\forall$** und somit ist die **Negation von $\forall$ ist $\exists$**. Also die Negation von *Alle Katzen sind grau.* ist nicht "Alle Katzen sind nicht grau", sondern

Es gibt eine Katze die nicht grau ist.

1.1.5 Implikationen

Eine **Implikation** (oder Subjunktion) ist eine Aussage der Form:

$$\textbf{Wenn } \textit{Aussage } A \textit{ wahr ist, } \textbf{dann } \textit{ist Aussage } B \textit{ wahr}. \tag{1.5}$$

Man sagt dazu auch "A **impliziert** B" oder "Aus A folgt B" und wir schreiben dafür

$$A \Rightarrow B.$$

Die Aussage A heißt **Voraussetzung** (oder Annahme, oder Bedingung) und die Aussage B heißt **Schlussfolgerung**. Implikationen sind oft nicht in der Form (1.5) gegeben. Zum Beispiel:

$$\textit{Die Summe zweier gerader Zahlen ist gerade.} \tag{1.6}$$

ist eine Implikation. Wenn wir folgende drei Aussagen betrachten:

A : *Die natürliche Zahl a ist gerade.*

B : *Die natürliche Zahl b ist gerade.*

C : *Die natürliche Zahl $a+b$ ist gerade.*

dann kann man die Aussage (1.6) so formulieren:

$$(A \text{ und } B) \Rightarrow C.$$

Eine äquivalente Formulierung der Implikation $A \Rightarrow B$ ist:

$$A \textit{ ist } \textbf{nur dann } \textit{wahr, } \textbf{wenn } B \textit{ wahr ist.}$$

Die Wahrheitstabelle für eine Implikation ist die folgende:

A	B	A⇒B
w	w	w
w	f	f
f	w	w
f	f	w

Hier ist wichtig zu bemerken, dass falsche Aussagen als Voraussetzung immer eine wahre Implikation geben. Also die Wahrheit der Implikation $A \Rightarrow B$ sagt nichts über die Wahrheit der Aussage B und genau so wenig über die Wahrheit von A. Nur wenn sowohl A als auch die Implikation $A \Rightarrow B$ wahr sind, dann folgt es, dass B wahr sein muss. Und wenn B falsch ist und $A \Rightarrow B$ wahr, dann muss auch A falsch sein.

Die Idee, dass eine falsche Voraussetzung die Implikation wahr macht scheint nicht eingängig zu sein. Hier ist mein Versuch diese falsche Intuition wieder gut zu machen.

Beispiel 1.7. Die meisten Sätze in der Mathematik sagen, dass eine Implikation wahr ist:

$$\textit{Für alle } x \in \mathbb{R} \textit{ ist folgende Aussage wahr: } x > 3 \Rightarrow x^2 > 3.$$

Das ist nicht der klügste Satz, aber es ist wahr. Das heißt die obige Implikation ist wahr für alle $x \in \mathbb{R}$, auch wenn diese kleiner als 3 sind. Man kann hier auch bemerken, dass wenn $x > 3$ falsch ist, dann kann $x^2 > 3$ sowohl wahr als auch falsch sein.

Die **Negation von** $A \Rightarrow B$ ist nicht wieder eine Implikation, sondern:

$$A \text{ und nicht}(B).$$

Es ist eine gute Übung das mit Hilfe einer Wahrheitstabelle zu überprüfen. Zum Beispiel, die Implikation:

$$\textit{Wenn 704 durch 11 teilbar ist, dann gilt } 7 - 0 + 4 = 0.$$

ist falsch, weil deren Negation wahr ist:

$$704 = 11 \cdot 64 \text{ } \textit{und} \text{ } 7 - 0 + 4 = 11 \neq 0.$$

Die Umkehrung (oder Konversion) der Aussage $A \Rightarrow B$ ist die Aussage $B \Rightarrow A$. Wir sagen, dass zwei Aussagen **logisch äquivalent** sind wenn sowohl $A \Rightarrow B$ als auch deren Umkehrung, $B \Rightarrow A$, beide wahr sind. Wir schreiben dafür:

$$A \Leftrightarrow B.$$

Das A und B logisch äquivalent sind heißt auch, dass die Wahrheitswerte von A und B übereinstimmen:

A	B	$A \Rightarrow B$	$B \Rightarrow A$	$A \Leftrightarrow B$
w	w	w	w	w
w	f	f	w	f
f	w	w	f	f
f	f	w	w	w

Bemerkung 1.8. Die Operationen *und* und *oder* sind **kommutativ**. Das heißt, dass für alle Aussagen A und B gilt:

$$(A \text{ und } B) \Leftrightarrow (B \text{ und } A); \qquad (A \text{ oder } B) \Leftrightarrow (B \text{ oder } A).$$

Die Inversion der Implikation $A \Rightarrow B$ ist die Aussage:

$$\text{nicht}(A) \Rightarrow \text{nicht}(B).$$

Die Implikation und deren Inversion werden in der Umgangssprache manchmal als äquivalent gesehen:

Wenn Du nicht aufräumst, dann bekommst Du kein Eis.

wird mit Sicherheit von einem Kind als "Wenn ich aufräume, dann bekomme ich Eis!" interpretiert. Die kalte Logik sagt aber nichts über was nach dem Aufräumen passiert. Das heißt, als mathematische Aussagen sind diese **nicht logisch äquivalent**. Allgemein gibt es keinen Zusammenhang zwischen der Wahrheit der beiden. Zum Beispiel, die wahre Aussage:

I1: *Wenn die Zahl a größer als 20 ist, dann ist a größer als 10.*

hat die Inversion:

I2: *Wenn die Zahl a kleiner als oder gleich mit 20 ist, dann ist a kleiner als oder gleich mit 10.*

die falsch ist. Die Inversion folgender Aussage ist aber wahr:

Wenn die Zahl a gerade ist, dann ist auch a^2 gerade.

Die Kontraposition der Implikation $A \Rightarrow B$ ist die Implikation "nicht(B)⇒nicht(A)".

Bemerkung 1.9. Eine Implikation ist zu ihrer Kontraposition logisch äquivalent.

Beweis-Skizze:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
w	w	f	f	w	w
w	f	f	w	f	f
f	w	w	f	w	w
f	f	w	w	w	w

Q.E.D.

Diese Bemerkung ist sehr wichtig und wird uns eine Methode für mathematische Beweise liefern. Zum Beispiel, die Kontraposition der obigen Implikation I1 ist:

Wenn a nicht größer als 10 ist, dann ist a nicht größer als 20.

1.1.6 Notwendig und hinreichend

Eine **notwendige Bedingung** für B ist eine Aussage A, die **gelten muss**, damit die Aussage B wahr sein kann. Eine Garantie für die Wahrheit von B ist sie aber nicht. Anders gesagt:

$$\big(A \text{ ist notwendig für } B\big) \quad \Longleftrightarrow \quad \big(B \Rightarrow A\big)$$

Zum Beispiel, für $a, b \in \mathbb{N}_{>0}$ haben wir

$$a \leqslant b \;\text{ ist notwendig für }\; a \,|\, b.$$

Eine **hinreichende Bedingung** für B ist eine Aussage A, die **garantiert**, dass die Aussage B wahr ist. Allerdings kann B wahr sein auch wenn A nicht wahr ist. Anders gesagt:

$$\big(A \text{ ist hinreichend für } B\big) \quad \Longleftrightarrow \quad \big(A \Rightarrow B\big)$$

Zum Beispiel, für $a, b, c \in \mathbb{R}$ haben wir

"a, b, c sind die Seitenlängen eines Dreiecks" ist hinreichend für "$a + b \geqslant c$".

1.2 Mengen und Abbildungen

Mengen sind die Bausteine der Mathematik. Mit deren Hilfe können fast alle grundlegenden Strukturen der modernen Mathematik rigoros definiert werden.

1.2.1 Mengen wohl definieren

Wir geben hier Georg Cantors[5] Definition für Menge. Die moderne (und korrekte) Definition ist wesentlich komplizierter. Cantors Definition ist eher ungenau und basiert auf Intuition, anderseits ist diese suggestiv und für unsere Zwecke ausreichend.

[5](1845-1918) Deutscher Mathematiker, Gründer der Mengenlehre: https://de.wikipedia.org/wiki/Georg_Cantor.

Definition 1.10 (Cantor 1895)**.** *Unter einer* ***Menge*** *verstehen wir jede* **wohldefinierte** *Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die ‚Elemente' von M genannt werden) zu einem Ganzen. In Zeichen drücken wir dies so aus:*

$$M = \{m\}.$$

Die Objekte in der Zusammenfassung werden **Elemente** der Menge genannt. Wenn x ein Element der Menge M ist, dann schreiben wir $x \in M$, und lesen das x *ist ein Element von* M oder x *ist in* M. Wenn x nicht ein Element der Menge M ist, dann schreiben wir $x \notin M$. Die Menge ohne Elemente heißt die **leere Menge** und wird mit $\emptyset$ bezeichnet.

Wir haben alle Probleme die vorkommen könnten unter "wohldefiniert" versteckt. Ein wichtiger Punkt wäre, dass eine wohldefinierte Menge sich nicht selbst als Element enthalten kann. Das führt zu Russels Paradox (siehe weiter unten). Um die Grundlagen der Theorie der Mengen ganz sauber aufzubauen, braucht man überraschend viel Zeit. Damit beschäftigt sich die Mengenlehre ([Rau08]). Ich werde hier nur bemerken, dass *die Mengenlehre verschafft sich ihre Mengen nicht aus der physikalischen Realität, sondern mittels eigens postulierter Existenzprinzipien.*[6] Hier ist ein Beispiel eines solchen Axioms:

$$\exists \emptyset \forall y y \notin \emptyset$$

Das sagt uns, dass die leere Menge existiert. In menschlicher Sprache sagt das Axiom, dass es eine Menge $\emptyset$ existiert, für welche die aussage $y \notin \emptyset$ wahr für alle möglichen y ist. Anders gesagt, für kein y ist die Aussage $y \in \emptyset$ wahr. Das heißt, dass $\emptyset$ kein einziges Element enthält.

Bemerkung 1.11. Die genauste Formulierung die uns die obige Definition erlaubt ist:

$$\text{Wenn } M \text{ eine Mengen ist, dann ist } x \in M \text{ eine Aussage für alle } x.$$

Eine Menge kann man beschreiben/definieren indem man:

1. die Elemente zwischen Kommas auflistet.
   (a) $\{1, 2, 3, 4, 5\}$.
   (b) $\{Haus, Hund, Katze, \clubsuit, 100, 0\%* :)\}$.
   (c) $\mathbb{N} = \{0, 1, 2, 3, \dots\}$. In dieser Vorlesung werden wir immer annehmen, dass $0 \in \mathbb{N}$.
   (d) $\mathbb{Z} = \{\dots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \dots\}$.
   (e) $\{1, 2, \dots, 100\}$ die Menge der natürlichen Zahlen von 1 bis 100.
   (f) $\{2, \dots, 10\}$ ist nicht unbedingt eindeutig: es könnte $\{2, 3, \dots, 10\}$ oder $\{2, 4, \dots, 10\}$ sein.
   (g) $X = \{1, 2, 4, 6, 10, 12, 16, 18, 22, 28, \dots\}$ - **Übung:** wie geht es hier weiter?
2. eine Eigenschaft angibt:

   $$\{x \mid x \text{ hat die Eigenschaft } E\} \text{ oder } \{x \in M \ : \ x \text{ hat die Eigenschaft } E\}.$$

   In diesem Fall liest man " $\mid$ " oder " : " als *sodass* oder *für die gilt* oder *mit der Eigenschaft, dass.*
   (a) $\emptyset = \{x \mid x \neq x\}$.

[6] [Rau08]

(b) $\mathbb{R} = \{x \ : \ x \text{ ist eine reelle Zahl}\}$.
(c) $2\mathbb{Z} = \{x \in \mathbb{Z} \ : \ x \text{ ist durch 2 teilbar}\}$.
(d) **Achtung:** $\{x \mid 0 \leqslant x \leqslant 1\}$ ist unklar. Mögliche Aufklärungen sind:

(i) $\{x \in \mathbb{Z} \mid 0 \leqslant x \leqslant 1\}$.
(ii) $\{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\}$.
(iii) $\{x \in \mathbb{Q} \mid 0 \leqslant x \leqslant 1\}$.

3. eine Formel (oder einen Ausdruck) auf alle/einige Elemente einer Menge anwendet.

$$\{\text{Formel/Ausdruck } F(x) \mid x, y, \ldots \in M \text{ und } x, y, \ldots \text{ haben die Eigenschaft } E\}.$$

(a) $2\mathbb{Z} = \{2 \cdot x \mid x \in \mathbb{Z}\}$.
(b) $\mathbb{Q} = \{\frac{p}{q} \mid p, q \in \mathbb{Z} \text{ und } q \neq 0\}$.
(c) $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R} \text{ mit } i^2 = -1\}$.

Beispiele:

1. $3 \in \{1, 2, 3, 4, 5\}$ aber $6 \notin \{1, 2, 3, 4, 5\}$.
2. $2^{2^2} \in 2\mathbb{Z}$, $123456^{101} \in 2\mathbb{Z}$, $32749^2 \notin 71\mathbb{Z}$, $\sqrt{101} \notin \mathbb{Q}$.
3. Mengen dürfen andere Mengen als Elementen enthalten, aber nicht sich selbst. Das führt zu mancher Verwirrung am Anfang. Man sollte sich aber an dieser Idee gewöhnen, weil das in vielen wichtigen Umständen vorkommen wird:
$$2 \in \{2\} \text{ aber } 2 \notin \{\{2\}\}.$$

Die nächste Definition und die folgende Bemerkung sind "offensichtlich". Beide werden aber sehr oft angewendet, und deswegen ist es gut wenn man diese ausdrücklich formuliert.

Definition 1.12. Zwei Mengen sind **gleich** (oder **identisch**) wenn sie dieselben Elemente haben.

Wenn die Menge M gleich der Menge N ist, schreiben wir $M = N$. Wenn nicht, schreiben wir $M \neq N$. Man sagt auch, dass zwei identische Mengen sind *umfangsgleich*.

Bemerkung 1.13. Die Gleichheit der Mengen M und N ist äquivalent zu der Aussage

$$m \in M \Rightarrow m \in N \quad \textbf{und} \quad n \in N \Rightarrow n \in M.$$

Also wenn man $M = N$ zeigen muss, soll man für jedes $m \in M$ zeigen, dass $m \in N$, und für jedes $n \in N$ zeigen, dass $n \in M$.

Beispiele:

1. Aus der Definition folgt es auch, dass die Elemente einer Menge in keiner bestimmten Reihenfolge sind: $\{2, 6, 13\} = \{6, 13, 2\}$.
2. Der Definition nach können Mengen ein Element nicht mehrmals enthalten:
$$\{2\} = \{2, 2\} = \{2, 2, 2, 2, 2, 2, 2, 2\}.$$

3. $\{z \in \mathbb{Z} \mid z \text{ ist durch 2 teilbar}\} = \{2z \mid z \in \mathbb{Z}\}$.
4. $\{\frac{3k}{5k} \ : \ k \in \mathbb{Z},\ k \neq 0\} = \{\frac{6}{10}\}$.
5. $\{\frac{a}{b} \ : \ a, b \in \mathbb{Z} \text{ und } b \neq 0\} = \{\frac{a}{b} \ : \ a, b \in \mathbb{Z} \text{ und } b \neq 0 \text{ und } \mathrm{ggT}(a, b) = 1\}$.
6. $\{1, 2\} \neq \{1, 2, 3\}$.
7. $\{2, 3\} \neq \{\{2\}, 3\}$.
8. $\{x \in \mathbb{R} \mid 0 \leqslant x \leqslant 1\} \neq \{x \in \mathbb{Q} \mid 0 \leqslant x \leqslant 1\}$.

Jede Sammlung von Elementen aus einer Menge ist immer eine Menge:

Definition 1.14. Eine Menge N heißt **Teilmenge** der Menge M, wenn jedes Element von N auch in M enthalten ist. Wir schreiben dafür $N \subseteq M$. Wenn $N \subseteq M$ und $N \neq M$, dann heißt N eine **echte Teilmenge** von M. Wir schreiben in diesen Fall $N \subsetneq M$ oder $N \subset M$.

Die Bezeichnung $N \subset M$ wird in der Literatur inkonsistent verwendet, und kann also verwirrend sein. Ich bevorzuge deswegen $N \subseteq M$ und $N \subsetneq M$.

Beispiele:

1. $\{Haus, Hund, \{3, 4\}\} \subseteq \{Hund, \{3, 4\}, Katze, Haus\}$.
2. $\{3, 4\} \not\subseteq \{Hund, \{3, 4\}, Katze, Haus\}$.
3. $\{2z \mid z \in \mathbb{Z}\} \subseteq \mathbb{Z}$.
4. $\{2z \mid z \in \mathbb{Z}\} \not\subseteq \mathbb{N}$.
5. $\{1, 2, 3\} \not\subseteq \{2, 3, 4\}$.
6. $M \subseteq M$ gilt für alle Mengen M.
7. $\emptyset \subseteq M$ gilt für alle Mengen M.
8. $\emptyset \subsetneq M$ gilt für alle Mengen $M \neq \emptyset$.
9. $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$.
10. Sei M eine Menge, dann ist 2^M oder $\mathcal{P}(M) = \{N \mid N \subseteq M\}$. Insbesondere: $\emptyset \in 2^M\ \forall M$.

[2] 18.10.'24

Eine essentielle Eigenschaft des axiomatischen Aufbaus der Mathematik ist die Widerspruchsfreiheit: eine Aussage und dessen Negation dürfen nicht gleichzeitig wahr oder gleichzeitig falsch sein. Anders gesagt, es soll keine Aussage A geben, sodass die Aussage "$A \Leftrightarrow \neg A$" wahr ist. Cantors Definition einer Menge kann zu folgender Antinomie führen.

Russels Paradox (1903) (nach dem Britischen Mathematiker Bertrand Russel[7] 1872-1970).
Sei $S = \{M \mid M \text{ ist eine Menge}\}$ die Zusammenfassung aller Mengen. Wäre S selbst eine Menge, dann hätte diese die Eigenschaft

$$\text{(E)} \qquad S \in S.$$

Es gibt aber auch Mengen die (E) nicht erfüllen, z.B. $\emptyset$, oder $\{1, 2, 3\}$. Man baut dann die Teilmenge von S:

$$T = \{M \in S \mid M \notin M\}.$$

[7] https://de.wikipedia.org/wiki/Bertrand_Russell

Dann haben wir aber, dass $T \in T \Rightarrow T \notin T$ und $T \notin T \Rightarrow T \in T$. Also $T \in T \Leftrightarrow T \notin T$ - und das bricht die Widerspruchsfreiheit.

Hier ist ein weiteres Paradox der naiven Mengenlehre. Wenn Russels Antinomie ein *logisches* Paradox ist, unser nächstes Beispiel ist ein *semantisches* Paradox. Dies ist ein Hinweis darauf, dass die Umgangssprache kein präzises Instrument für den Aufbau einer Theorie ist.

Berrys Paradox Sagen wir, dass alle Wörter der Deutschen Sprache in einem Wörterbuch aufgelistet sind. Betrachten wir folgende Menge

$$T := \textit{Die Menge der natürlichen Zahlen, die mit weniger als fünfzehn Wörter beschreiben kann.}$$

Da es nur endlich viele Wörter gibt, dann gibt es auch nur endlich viele Kombinationen von höchstens 15 davon. Das heißt, dass die Menge T endlich ist, und somit gibt es auch die kleinste natürliche Zahl mit $k \notin T$. Diese Zahl ist also *die kleinste natürliche Zahl die nicht mit weniger als fünfzehn Wörter beschrieben werden kann.* Wir haben diese aber gerade mit 14 Wörter beschrieben, und somit soll auch $k \in T$.

Es hat lange gedauert bis die Mengenlehre axiomatisch "gefestigt" wurde. Für unsere Zwecke hier reicht es nur zu wissen, dass es so etwas gibt. Wir werden aber weiter mit Cantors Definition arbeiten, und als "wohldefinierte" Mengen die Mengen verstehen, die sich selber nicht enthalten. Die Zusammenfassung aller Mengen ist also keine Menge, sondern eine **Klasse**.

Ein **Venn-Diagramm** ist eine Methode Mengen als Scheiben (oder Flecken) in der Ebene darzustellen.

1.2.2 Operationen mit Mengen

Definition 1.15. Seien M_1, M_2 zwei Mengen.

Die **Vereinigung** (oder die Vereinigungsmenge) von M_1 und M_2 ist die Menge, die aus allen Elementen besteht, die in M_1 oder in M_2 (oder in beiden) enthalten sind:

$$M_1 \cup M_2 := \{x \ : \in M_1 \text{ oder } x \in M_2\}.$$

Der **Durchschnitt** (oder die Schnittmenge) von M_1 und M_2 ist die Menge, die aus allen Elementen besteht die sowohl in M_1 als auch in M_2 enthalten sind:

$$M_1 \cap M_2 := \{x \ : \ x \in M_1 \text{ und } x \in M_2\}.$$

Die **Differenz** (oder Differenzmenge) von M_1 und M_2 ist die Menge, die aus allen Elementen von M_1 besteht die nicht in M_2 sind:

$$M_1 \setminus M_2 := \{x \ : \ x \in M_1 \text{ und } x \notin M_2\}.$$

Wenn wir zusätzlich $M_2 \subseteq M_1$ voraussetzen, dann heißt die Differenz $M_1 \setminus M_2$ das **Komplement** von M_2 in M_1, und wird mit $\complement_{M_1} M_2$ bezeichnet. Wenn M_1 klar aus dem Kontext ist, dann schreiben wir nur $M_2^{\complement}$.

Die Mengen M_1 und M_2 heißen **disjunkt** wenn $M_1 \cap M_2 = \emptyset$.

Für jede Menge M definieren wir die **Potenzmenge von M** als die Menge aller Teilmengen von M. Wir bezeichnen das als $\mathcal{P}(M)$ oder 2^M. (Können Sie raten warum man 2^M verwendet?) Also

$$2^M := \{N \ : \ N \subseteq M\}.$$

Insbesondere haben wir immer $\emptyset, M \in 2^M$.

Beispiele:

1. Wenn $M = \{1, 2, 3, 4\}$ und $N = \{2, 4, 6, 8\}$, dann gilt

$$M \cup N = \{1, 2, 3, 4, 6, 8\}, \qquad M \cap N = \{2, 4\}, \qquad M \setminus N = \{1, 3\}.$$

2. Für alle Mengen M gilt

$$M \cup M = M, \qquad M \cap M = M, \qquad M \setminus M = \emptyset.$$

3. Wenn $A = \{x \in \mathbb{R} \ : \ x > \frac{7}{11}\}$ und $B = \{z \in \mathbb{Z} \ : \ z < 6\}$, dann gilt

$$A \cap B = \{1, 2, 3, 4, 5\}$$

Bemerkung 1.16. Für alle Mengen A, B, C gilt

$$\begin{array}{rcl} (A \cup B) \cup C & = & A \cup (B \cup C) \quad \text{und} \\ (A \cap B) \cap C & = & A \cap (B \cap C) \end{array}$$

Allgemein gilt aber **nicht**, dass $(A \setminus B) \setminus C = A \setminus (B \setminus C)$. (Übung: Geben Sie ein Gegenbeispiel.) Die obige Eigenschaft von $\cup$ und $\cap$ heißt **Assoziativität**[8]. Wir hätten also die Bemerkung als: *Der Durchschnitt und die Vereinigung von Mengen sind assoziativ, die Mengendifferenz aber nicht.* formulieren können.

Bemerkung 1.17. Dank der Assoziativität kann man durch Iteration Operationen für endlich viele Mengen definieren. Es seien also $n \in \mathbb{N}_{>0}$ und $M_1, \ldots, M_n$ Mengen. Dann gilt:

$$\begin{array}{rcl} M_1 \cup \cdots \cup M_n & := & (M_1 \cup \cdots \cup M_{n-1}) \cup M_n \\ M_1 \cap \cdots \cap M_n & := & (M_1 \cap \cdots \cap M_{n-1}) \cap M_n \end{array}$$

Das ist keine Konvention. Für jede mögliche Klammersetzung bekommt man immer das Gleiche. [9]

Für unendlich viele Mengen kann man die Vereinigung und den Schnitt auch definieren. Um das aber mit Genauigkeit zu machen muss man zuerst Familien definieren. Wir verschieben also unendliche Schnitte und Vereinigungen bis Teil 1.2.9.

1.2.3 Die Kardinalität einer Menge

Wir werden hier erstmals eine naive Definition für endliche Mengen und deren Kardinalität verwenden. Diese ist intuitiv und freundlich, aber es basiert sehr stark auf der Bedeutung von *endlich* und *Anzahl* in der Umgangssprache. Deswegen werden wir später, in Teil 1.2.10, auch eine mathematisch genaue Definition sehen.

[8] Die Addition und die Multiplikation der reellen Zahlen ist assoziativ.

[9] Das ist nicht der Fall für die Mengendifferenz. Wir werden dafür auch keine Konvention einführen, Also

$$M_1 \setminus M_2 \setminus \cdots \setminus M_n$$

ist nicht definiert. Was definiert ist ist $\Big(\ldots \big((M_1 \setminus M_2) \setminus M_3 \big) \cdots \setminus M_{n-1} \Big) \setminus M_n$.

Definition 1.18. Wenn M eine Menge die leer ist oder aus endlich vielen Elementen besteht, dann sagen wir, dass M eine **endliche Menge** ist. Wenn M endlich ist, dann nennt man die Anzahl ihrer Elemente **Kardinalität** von M. Man schreibt dafür $|M|$ oder $\sharp M$.
Wenn eine Menge M nicht endlich ist, dann sagen wir, dass diese eine **unendliche Menge** ist.

Wir werden von der *Kardinalität von unendlichen Mengen* noch nicht sprechen[10], weil sie nicht so einfach zu definieren ist. Für jetzt reicht es zu sagen, dass es unendliche Mengen gibt, die nicht gleichviele Elementen haben (cf. Definition 1.43).

Beispiele:

1. $|\{1,2,3,4\}| = 4$.
2. $|\{1,2,\{3,4\}\}| = 3$.
3. $|\mathbb{N}| = \infty$

1.2.4 Das Kartesische Produkt

Nach Definition 1.12 spielt die Reihenfolge der Elementen einer Menge keine Rolle. Wir werden aber geordnete Auflistungen von Elementen brauchen. Es gibt mehrere Möglichkeiten diese mit Hilfe von bereits eingeführten Begriffe zu definieren. Wir werden hier zwei solche Varianten zeigen. Die erste Version braucht nur den Begriff von Menge, die zweite, die einfacher zu geordnetes n-Tupel verallgemeinerbar ist, braucht auch natürliche Zahlen.

Definition 1.19. (a) **[Kuratowski 1921]** Seien M und N zwei Mengen, und seien $m \in M$ und $n \in N$. Das **geordnete Paar** mit erstes Element m und zweites Element n ist definiert als

$$(m,n) := \big\{\{m\},\{m,n\}\big\}.$$

(b) **[Hausdorff 1914]** Seien 1 und 2 zwei verschiedene Objekte (zum Beispiel $\emptyset$ und $\{\emptyset\}$). Seien M_1 und M_2 zwei Mengen, und seien $m_i \in M_i$ für $i \in \{1,2\}$. Das **geordnete Paar** mit erstem Element m_1 und zweitem Element m_2 ist die Menge

$$(m_1,m_2) := \big\{\{1,m_1\},\{2,m_2\}\big\}.$$

Bemerkung 1.20. Ein geordnetes Paar ist also eine Zusammenfassung zweier (nicht unbedingt verschiedener) Objekte, wobei die Reihenfolge eine essentielle Rolle spielt. Insbesondere

$$(m_1,m_2) = (n_1,n_2) \Leftrightarrow m_1 = n_1 \text{ und } m_2 = n_2.$$

Also, wenn $m_1 \neq m_2$, dann haben wir $(m_1,m_2) \neq (m_2,m_1)$.

Wir werden diese Bemerkung ganz ausführlich beweisen. Das Ziel ist einen ersten ganz sauberen Beispiel von Beweis zu geben. In der Regel werden Bemerkungen oft ohne Beweis angegeben. Das heißt nicht, dass kein Beweis nötig ist. Es heißt meistens, dass der Beweis direkt aus schon bekannten Definitionen und Theoreme folgt. Bevor wir aber Bemerkung beweisen, werden wir ein *Lemma*[11] beweisen.

[10] Wir werden aber trotzdem manchmal $|M| = \infty$ schreiben. Das liest man aber *die Mengen M ist unendlich* und nicht *die Kardinalität von M ist Unendlichkeit.*

[11] In der Mathematik nennt man Lemma ein Hilfssatz. Das heißt eine Aussage, die als wahr bewiesen wird, und die dann (meistens mehrmals) in weitere Beweise verwendet wird. Siehe auch Abschnitt 2.1.3.

Lemma 1.21. *Die Mengen* $\{a\}$ *und* $\{b, c\}$ *sind genau dann gleich, wenn* $a = b = c$.

Beweis-Skizze: Wir werden direkt folgende Äquivalenz beweisen:

$$\{a\} = \{b, c\} \iff a = b \,\text{und}\, b = c.$$

Die Gleichheit der Mengen $\{a\} = \{b, c\}$ ist per Definition (oder Bemerkung 1.13) äquivalent zu

$$a \in \{b, c\} \,\text{und}\, b \in \{a\} \,\text{und}\, c \in \{a\}.$$

Die Interpretation des Zeichens $\in$ ist: $m \in M \Leftrightarrow \exists y \in M$ mit $m = y$. Also die obige Aussage ist äquivalent zu:

$$\big(a = b \;\text{ oder }\; a = c\big) \,\text{und}\, b = a \,\text{und}\, c = a.$$

Das ist äquivalent zu $a = b = c$. Q.E.D.

Wir führen den Beweis der Bemerkung 1.2.4 für die Definition von Kuratowski durch. Das heißt nicht, dass wir die Definition beweisen! Es heißt, dass wir die von Kuratowski gegebene Definition von geordnetes Paar benutzen. Wir wollen eine Äquivalenz "$A \Leftrightarrow B$" beweisen. Das heißt "$A \Rightarrow B$ und $B \Rightarrow A$". Wir werden die zwei Implikationen separat behandeln, und jeweils mit $\boxed{\Rightarrow}$, beziehungsweise $\boxed{\Leftarrow}$, bezeichnen.

Beweis-Skizze: der Bemerkung 1.2.4.

$\boxed{\Rightarrow}$ Die Voraussetzung ist also $\big\{\{m_1\}, \{m_1, m_2\}\big\} = \big\{\{n_1\}, \{n_1, n_2\}\big\}$. Wir trennen den Beweis dieser Implikation in zwei Fällen[a].

Fall 1: $m_1 = m_2$. Dann haben wir $\big\{\{m_1\}, \{m_1, m_2\}\big\} = \big\{\{m_1\}\big\} = \big\{\{n_1\}, \{n_1, n_2\}\big\}$, also aus Lemma 1.21 folgt

$$\{m_1\} = \{n_1\} = \{n_1, n_2\}.$$

Aus demselben Lemma 1.21 folgt $m_1 = n_1 = n_2$. Zusammen mir der Voraussetzung von Fall 1 gilt also: $m_1 = m_2 = n_1 = n_2$.

Fall 2: $m_1 \neq m_2$. Aus der Gleichheit der zwei großen Mengen und aus dem Lemma 1.21[b] folgt

$$\{m_1\} = \{n_1\} \,\text{und}\, \{m_1, m_2\} = \{n_1, n_2\}.$$

Daraus folgt (ist aber nicht äquivalent zu!):

$$m_1 = n_1 \,\text{und}\, \big(m_2 = n_1 \;\text{ oder }\; m_2 = n_2\big).$$

Aus der Distributivität von " und " bezüglich " oder " bekommen wir

$$\big(m_1 = n_1 \,\text{und}\, m_2 = n_1\big) \;\text{ oder }\; \big(m_1 = n_1 \,\text{und}\, m_2 = n_2\big).$$

Die linke Seite von " oder " ist aber falsch, weil wir mit der Voraussetzung $m_1 \neq m_2$ arbeiten. Das heißt, dass die rechte Seite wahr sein muss, und das ist genau was wir beweisen wollten.

Wir haben also in beiden Fällen gezeigt, dass die Schlussfolgerung "$m_1 = n_1$ und $m_2 = n_2$ gilt.

$\boxed{\Leftarrow}$ Die Voraussetzung ist jetzt $m_1 = n_1$ und $m_2 = n_2$. Es folgt also $\{m_1\} = \{n_1\}$ und $\{m_1, m_2\} = \{n_1, n_2\}$. Also die zwei großen Mengen sind auch gleich.

Wir haben also bewiesen, dass beide Implikationen wahr sind, und somit die Äquivalenz:

$$\Big(\big\{\{m_1\}, \{m_1, m_2\}\big\} = \big\{\{n_1\}, \{n_1, n_2\}\big\}\Big) \iff \Big(m_1 = n_1 \text{ und } m_2 = n_2\Big).$$

Q.E.D.

[a] Wenn man eine Fallunterscheidung durchführt, muss man sicher sein, dass die Aussage "Fall 1 oder Fall 2" eine Tautologie ist. In diesem Beweis ist es "$m_1 = m_2$ oder $m_1 \neq m_2$".

[b] Das Lemma 1.21 schließt $\{m_1, m_2\} = \{n_1\}$ aus, weil sonst wären $m_1 = m_2 = n_1$.

Bemerkung 1.22. Eine gute Frage in der Vorlesung war: *Warum definieren wir nicht* (m, n) *als* $\big\{\{m\}, \{m, n\}, \{n\}\big\}$*?*. Die Antwort ist einfach: weil dann $(1, 2) = (2, 1)$ gelten würde, und genau das wollten wir vermeiden. Also *Less is more.*

Definition 1.23. Seien M und N zwei Mengen. Das **kartesische Produkt** (oder die Produktmenge) von M und N ist die Menge aller Paare (m, n), die mit Elementen $m \in M$ und $n \in N$ möglich sind. Wir bezeichnen[12] diese Menge mit $M \times N$:

$$M \times N := \{(m, n) \mid m \in M \text{ und } n \in N\}.$$

Wenn $M = N$ schreiben wir für $M \times M =: M^2$.

Kartesisch heißt es nach dem Philosoph und Mathematiker René Descartes[13] (1596-1650).

Beispiele:

1. $M = \{0, 1\}$ $N = \{1, 2, 3\}$

$$M \times N = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3)\}.$$

2. $\mathbb{R}^2$ kann man sich als die Euklidische Ebene vorstellen. $\mathbb{Z}^2$ ist eine *diskrete*[14] Teilmenge davon.

Wir werden später das Kartesische Produkt einer beliebigen Familie einführen (siehe Definition 1.40). Da wir aber um Abbildungen formal zu definieren auch Tripel brauchen werden, definieren wir hier n-Tupel erstmals induktiv. Sei $n \in \mathbb{N}$, mit $n \geq 1$. Wenn $n = 1$, dann ist ein 1-Tupel einfach eine Menge die ein einziges Element enthält. Wenn $n = 2$, dann ist ein 2-Tupel ein geordnetes Paar. Für $n \geq 3$ ist ein n-Tupel ein geordnetes Paar, welches an der ersten Stelle ein $n-1$-Tupel hat:

$$(a_1, \ldots, a_n) := ((a_1, \ldots, a_{n-1}), a_n). \tag{1.7}$$

Wichtig ist hier wieder, dass n-Tupel durch folgende Bemerkung vollständig charakterisiert sind:

$$(a_1, \ldots, a_n) = (b_1, \ldots, b_n) \iff a_i = b_i \quad \forall\, i = 1, \ldots, n.$$

[3] 23.10.'24

[12] Hier, in dieser Definition, bezeichnet (m, n) ein geordnetes Paar, und nicht ein offenes Intervall.

[13] https://de.wikipedia.org/wiki/René_Descartes

[14] Es heißt so, weil die Paare $(a, b) \in \mathbb{Z}^2$ einen Mindestabstand halten. Die Teilmenge $\mathbb{Q}^2$ ist im Gegenteil dicht in $\mathbb{R}^2$.

1.2.5 Abbildungen

Wir fangen mit der intuitiven Definition von Abbildung an. Diese sollte man sich merken. Das einzige Problem ist, dass sich diese Definition zu stark auf der Umgangssprache verlässt.

Eine Abbildung f von der Menge A nach der Menge B ist eine Vorschrift, die jedem Element $x \in A$ auf eindeutige Weise ein Element $y \in B$ zuordnet. Wir schreiben dafür $f : A \longrightarrow B$ und bezeichnen für alle $x \in A$ das entsprechende eindeutig bestimmte Element aus B mit $f(x)$:

$$\forall\, x \in A, \exists!\ f(x) \in B.$$

Da "Vorschrift" nicht mathematisch definiert ist, sollten wir versuchen uns auf schon eingeführte Begriffen verlassen. Das heißt wir sollten Abbildungen allein durch Mengen definieren. Man kann das machen, indem man eine Abbildung als eine Teilmenge der Produktmenge $A \times B$, die eine zusätzliche Eigenschaft erfüllen muss, definiert.

Definition 1.24. Eine **Abbildung** f von einer Menge A in eine Menge B ist ein Tripel $f = (A, B, \Gamma_f)$, wobei Γ_f eine Teilmenge der Produktmenge $A \times B$ ist und folgende Eigenschaft hat:

$$\forall x \in A, \quad \exists!\ y \in B \text{ sodass } (x, y) \in \Gamma_f.$$

Die Bezeichnung Γ steht für Graph und so heißt auch die Menge Γ_f: der **Graph von** f. Wir die Schreibweise $f = (A, B, \Gamma_f)$ nie wieder verwenden. Wir werden stattdessen die natürlichere und suggestive Schreibweise

$$f : A \longrightarrow B$$

für Abbildung von A nach B benutzen. Wir schreiben dafür auch

$$A \xrightarrow{f} B.$$

Wir bezeichnen mit $f(x)$ das durch f eindeutig bestimmte y aus B, sodass $(x, y) \in \Gamma_f$. Wir bezeichnen diese Zuordnung auch mit

$$x \longmapsto f(x) \qquad \text{oder} \qquad x \xmapsto{f} f(x)$$

Die Menge A heißt der **Definitionsbereich** von f. Die Menge B heißt der **Wertebereich** von f. Wenn $A' \subseteq A$, ist das **Bild von A' unter f** die Menge

$$f(A') := \{f(x) \mid x \in A'\}.$$

Die Menge $f(A)$ heißt das **Bild** von f. Wenn $B' \subseteq B$ ist das **Urbild** von B' unter f die Menge

$$f^{-1}(B') := \{x \in A \mid f(x) \in B'\}.$$

Wenn $B' = \{y\}$, dann schreiben wir $f^{-1}(y) := f^{-1}(\{y\})$ und nennen diese Menge die **Faser** von f über y.

Wir haben formal eine Abbildung von A nach B als Tripel definiert, damit klar ist was es heißt wenn zwei Abbildungen gleich sind. Also $f : A \longrightarrow B$ ist gleich mit $g : C \longrightarrow D$ genau dann, wenn $A = C$, $B = D$, und $f(a) = g(a)\ \ \forall\, a \in A$. Zum Beispiel, $\lfloor \cdot \rfloor : \mathbb{R} \longrightarrow \mathbb{R}$, definiert durch

$$\lfloor x \rfloor := \max\{z \in \mathbb{Z}\ :\ z \leqslant x\},$$

und $\lfloor\cdot\rfloor : \mathbb{R} \longrightarrow \mathbb{Z}$ (genauso definiert) sind nicht gleich, obwohl beide denselben Effekt auf die reellen Zahlen haben.
Sei $f : A \longrightarrow B$ eine Abbildung, und sei $A' \subseteq A$. Eine **Einschränkung** (des Definitionsbereichs) von f (auf A'), ist eine Abbildung $f|_{A'} : A' \longrightarrow B$ definiert durch $f_{A'}(a) := f(a)$ für alle $a \in A'$. Also wenn A' eine echte Teilmenge von A ist, dann ist die Einschränkung nicht gleich mit der ursprünglichen Abbildung. Mann kann auch den Wertebereich einer Abbildung einschränken oder sogar erweitern, aber das geht nur für Mengen B' mit $\text{Bild}(f) \subseteq B'$.

Abbildungen zwischen Mengen gibt es fast immer. Die einzige Ausnahme ist wenn der Definitionsbereich nicht die leere Menge ist, aber der Wertebereich leer ist. Insbesondere, gibt es genau eine Abbildung von der leeren Menge, in jede andere Menge: $\varphi : \emptyset \longrightarrow A$, die als Tripel besser beschreibbar ist: $(\emptyset, A, \emptyset)$. Es ist die einzige Möglichkeit, weil $\emptyset \times A = \emptyset$.

Beispiele:

1. Seien $A = B = \{1, 2, 3\}$. Eine der folgenden Teilmengen von A^2 ist nicht eine Abbildung:

$$\begin{aligned} \Gamma_{f_1} &= \{(1,3),(2,3),(3,3)\} \\ \Gamma_{f_2} &= \{(1,1),(1,2),(1,3)\} \\ \Gamma_{f_3} &= \{(1,1),(2,2),(3,3)\} \end{aligned}$$

2. Für jede Menge M kann man die **identische Abbildung** der Menge M (oder Identität von M) definieren:
$$\text{id}_M : M \longrightarrow M, \quad x \longmapsto x.$$

3. Ist folgende Teilmenge von $\mathbb{R}^2$ eine Abbildung?
$$\Gamma_f = \{(x, y) \in \mathbb{R}^2 \mid y^2 = x\}.$$

4. $f : \mathbb{N} \longrightarrow \mathbb{N}$ mit $f(n) = n - 1$ ist keine Abbildung.
5. $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ mit $f(n) = n - 1$ ist eine Abbildung.
6. $f : \mathbb{R} \longrightarrow \mathbb{R}$ mit $f(x) = \frac{1}{x}$ ist keine Abbildung
7. $f : \mathbb{R} \setminus \{0\} \longrightarrow \mathbb{R} \setminus \{0\}$ mit $f(x) = \frac{1}{x}$ ist eine Abbildung.
8. Für jedes $i \in \{1, 2\}$ können wir die **kanonische Projektion**
$$p_i : A_1 \times A_2 \longrightarrow A_i, \quad (a_1, a_2) \mapsto a_i.$$

9. Wenn $A' \subseteq A$ haben wir eine **kanonische Inklusion/Injektion**
$$i : A' \longrightarrow A, \quad a' \mapsto a'.$$

1.2.6 Die Verknüpfung von Abbildungen

Definition 1.25. Seien $A \xrightarrow{f} B \xrightarrow{g} C$ zwei Abbildungen. Die **Komposition**[15] **von g mit f** ist die Abbildung mit Definitionsbereich A, Wertebereich C und die jedem Element $a \in A$ das Element $g\big(f(a)\big)$ aus C zuordnet. Wir bezeichnen diese Abbildung mit $g \circ f$, also:

$$\begin{aligned} g \circ f : A &\longrightarrow C \\ a &\longmapsto g\big(f(a)\big) \end{aligned} .$$

Achtung! Abbildungen kann man nicht immer verknüpfen!

Man kann zwei Abbildungen nur dann verknüpfen wenn der Wertebereich der zweiten Abbildung gleich dem Definitionsbereich der ersten Abbildung ist. Es kann also sein, dass $g \circ f$ existiert, aber $f \circ g$ nicht. Wenn $f : A \longrightarrow B$ und $g : B' \longrightarrow C$, aber Bild $f \subseteq B'$, dann würde $g(f(x))$ trotzdem Sinn machen, und somit eine Abbildung von A nach C definieren. Wir bestehen aber darauf, dass die Komposition nur dann definiert ist wenn $B = B'$, was man in diesem Fall machen könnte, ist g auf Bild f einzuschränken, und dann die beiden Abbildungen verknüpfen.

Bemerkung 1.26. (a) Die Verknüpfung von Abbildungen ist **assoziativ**. Das heißt, wenn man drei komponierbare Abbildungen $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$ hat, dann gilt

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

(b) Für jede Abbildung $f : A \longrightarrow B$ gilt $f \circ \mathrm{id}_A = \mathrm{id}_B \circ f = f$.

Beispiele: Seien $f, g, h : \mathbb{R} \longrightarrow \mathbb{R}$ die drei Abbildungen gegeben durch

$$x \xmapsto{f} x^2 \qquad x \xmapsto{g} 2x \qquad x \xmapsto{h} x - 1.$$

Dann gilt

$$x \xmapsto{f \circ g} 4x^2 \qquad x \xmapsto{f \circ g \circ h} 4x^2 - 8x + 4$$
$$x \xmapsto{g \circ f} 2x^2 \qquad x \xmapsto{h \circ g \circ f} 2x^2 - 1.$$

[4]25.10.'24

1.2.7 Eigenschaften von Abbildungen

Definition 1.27. Eine Abbildung $f : A \longrightarrow B$ heißt

$$\begin{aligned} \textbf{injektiv} &\iff \forall\, x, y \in A \text{ gilt } x \neq y \Rightarrow f(x) \neq f(y). \\ \textbf{surjektiv} &\iff \forall\, b \in B, \quad \exists\, x \in A \text{ sodass } f(x) = b. \\ \textbf{bijektiv} &\iff \forall\, b \in B, \quad \exists!\, x \in A \text{ sodass } f(x) = b. \end{aligned}$$

[15] oder die Verknüpfung/Zusammensetzung/ Hintereinanderausführung/ Verkettung/ Hintereinanderschaltung.

Bemerkung 1.28. Sei $f : A \longrightarrow B$ eine Abbildung. Es gilt

$$\begin{aligned} f \text{ ist injektiv} &\iff \forall\, b \in B \text{ die Faser } f^{-1}(b) \text{ höchstens ein Element enthält.} \\ &\iff \forall\, x, y \in A \text{ mit } f(x) = f(y) \text{ folgt } x = y. \\ f \text{ ist surjektiv} &\iff \forall\, b \in B \text{ die Faser } f^{-1}(b) \text{ mindestens ein Element enthält.} \\ f \text{ ist bijektiv} &\iff \forall\, b \in B \text{ die Faser } f^{-1}(b) \text{ genau ein Element enthält.} \\ &\iff f \text{ ist injektiv und surjektiv.} \end{aligned}$$

Beispiele:

1. $f : \mathbb{R} \longrightarrow \mathbb{R}^2, f(x) = (x, 0)$ (oder $(x - 1, 2x + 1)$ oder (x, x^2)) sind alle 3 injektiv. Man kann sich diese als Einbettungen der reellen Gerade in der reellen Ebene vorstellen.
2. Die Projektionen $p_1, p_2 : \mathbb{R}^2 \longrightarrow \mathbb{R}$ sind surjektiv.
3. Auch in konkreten Fällen, soll man Abbildungen mit dem Ausdruck der diese definiert **nicht** gleichstellen. Man betrachte $\cdot 3 : \mathbb{R} \longrightarrow \mathbb{R}, x \mapsto 3x$, die invertierbar (und bijektiv) mit Inverse gegeben durch $x \mapsto (1/3)x$ ist. Die Abbildung $\cdot 3 : \mathbb{Z} \longrightarrow \mathbb{Z}$ hingegen, die auch durch $x \mapsto 3x$ definiert ist, ist nicht invertierbar und nicht surjektiv.
4. Genauso wie im obigen Beispiel: $f : \mathbb{R} \longrightarrow \mathbb{R}$ definiert durch $f(x) = x^2$ ist nicht injektiv, aber $f|_{\mathbb{N}} : \mathbb{N} \longrightarrow \mathbb{R}$ ist injektiv.
5. Siehe alle Beispiele in [Hou2012, Kapitel 30].

1.2.8 Invertierbare Abbildungen

Definition 1.29. Ein Abbildung $f : A \longrightarrow B$ heißt **invertierbar** genau dann, wenn

$$\exists\, f^{-1} : B \longrightarrow A \;\text{ sodass } f \circ f^{-1} = \mathrm{id}_B \text{ und } f^{-1} \circ f = \mathrm{id}_A\,.$$

A priori schließt die obige Definition die Möglichkeit, dass es verschiedene Abbildungen f^{-1} gibt, nicht aus. Das muss erst beweisen werden. Danach dürfen wir diese **die** Inverse von f nennen.

Proposition 1.30. *Wenn eine Abbildung $f : A \longrightarrow B$ invertierbar ist, dann ist die Abbildung f^{-1} aus der Definition 1.29 eindeutig bestimmt.*

Beweis-Skizze: Wir können eigentlich eine stärkere Aussage beweisen:

Seien $f', f'' : B \longrightarrow A$ zwei Abbildungen, sodass $f' \circ f = \mathrm{id}_A$ und $f \circ f'' = \mathrm{id}_B$ gelten. Dann gilt

$$f' = f''.$$

Aus $f' \circ f = \mathrm{id}_A$ folgt durch Verknüpfen mit f'' auf der rechten Seite, dass $(f' \circ f) \circ f'' = \mathrm{id}_A \circ f''$. Aus Bemerkung 1.26 folgt also

$$f' = f' \circ \mathrm{id}_B = f' \circ (f \circ f'') = f''.$$

Q.E.D.

Definition 1.31. Wenn $f : A \longrightarrow B$ eine invertierbare Abbildung ist, dann heißt die (nach Proposition 1.30) eindeutige Abbildung $f^{-1} : B \longrightarrow A$ aus der Definition 1.29 die **Inverse** (oder die **Umkehrabbildung**) von f.

Es kann sein, dass es nur eine der Abbildungen f' oder f'' existieren. In diesem Fall haben wir folgende Bezeichnungen.

Definition 1.32. Sei $f : A \longrightarrow B$ eine Abbildung.

Eine Abbildung $f' : B \longrightarrow A$ heißt **Linksinverse** oder **Retraktion** von f genau dann, wenn

$$f' \circ f = \mathrm{id}_A \,.$$

Eine Abbildung $f'' : B \longrightarrow A$ heißt **Rechtsinverse** oder **Sektion** von f genau dann, wenn

$$f \circ f'' = \mathrm{id}_B \,.$$

Satz 1.33. *Sei $f : A \longrightarrow B$ eine Abbildung zwischen zwei nicht-leeren Mengen. Dann gilt*

(i) *f ist injektiv $\iff$ f hat eine Retraktion.*

(ii) *f ist surjektiv $\iff$ f hat eine Sektion.*

(iii) *f ist bijektiv $\iff$ f ist invertierbar.*

[5] 30.10.'24

Beweis-Skizze:

(i) $\boxed{\Rightarrow}$ Weil f injektiv ist, existiert für jedes $y \in f(A)$ ein einziges $x \in A$ mit $f(x) = y$. Wir bezeichnen das zu y zugeordnete x mit x_y. Wir wählen auch ein beliebiges Element $a \in A$ und definieren $f' : B \longrightarrow A$ durch

$$f'(y) = \begin{cases} x_y & \text{wenn } y \in f(A) \\ a & \text{wenn } y \notin f(A). \end{cases}$$

Diese ist eine Abbildung und erfüllt $f' \circ f = \mathrm{id}_A$.

$\boxed{\Leftarrow}$ Sei $f' : B \longrightarrow A$ so dass $f' \circ f = \mathrm{id}_A$. Seien $x, y \in A$ mit $f(x) = f(y)$. Dann haben wir

$$x = \mathrm{id}_A(x) = f'(f(x)) = f'(f(y)) = \mathrm{id}_A(y) = y.$$

Also f ist injektiv.

(ii) $\boxed{\Rightarrow}$ Wir wollen eine Abbildung $f'' : B \longrightarrow A$ definieren. Sei $y \in B$. Da f surjektiv ist, existiert mindestens ein $x \in A$ sodass $f(x) = y$. Wir wählen so ein x_y für jedes y und definieren $f''(y) := x_y$. Jedem $y \in B$ wurde genau ein Element aus A zugeordnet: x_y. Wir haben also eine Abbildung von B in A definiert. Da $f''(y)$ aus der Menge $f^{-1}(x)$ gewählt wurde, haben wir $f \circ f'' = \mathrm{id}_B$.

$\boxed{\Leftarrow}$ Sei $f'' : B \longrightarrow A$ sodass $f \circ f'' = \mathrm{id}_B$. Für jedes $y \in B$ haben wir $f''(y) \in f^{-1}(y)$, weil $f(f''(y)) = \mathrm{id}_B(y) = y$. Also f ist surjektiv.

(iii) $\boxed{\Rightarrow}$ Da f bijektiv ist, folgt aus Teil (i) und (ii) die Existenz von f' und f''. Aus dem Beweis der Proposition 1.30 folgt das $f' = f'' = f^{-1}$.

$\boxed{\Leftarrow}$ Wenn f invertierbar ist, dann existiert $f^{-1} : B \longrightarrow A$ mit $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$. Aus (i) und (ii) folgt das f injektiv und surjektiv ist.

Q.E.D.

Bemerkung 1.34 (Student aus der ersten Reihe (2021))**.** Wenn f die Retraktion einer Abbildung ist, dann ist f surjektiv, und wenn f die Sektion einer Abbildung ist, dann ist f injektiv.

Beispiel 1.35. Wenn eine Abbildung injektiv ist, dann kann es mehrere Retraktionen haben. Sei zum Beispiel $f : \mathbb{N} \longrightarrow \mathbb{N}$ gegeben durch $f(n) = n + 1$. Dann gilt für jedes $a \in \mathbb{N}$, dass die Abbildung $r_a : \mathbb{N} \longrightarrow \mathbb{N}$ gegeben durch

$$r_a(n) = \begin{cases} a & \text{wenn } n = 0 \\ n - 1 & \text{wenn } n \neq 0 \end{cases}$$

eine Retraktion von f ist. Ähnlich kann man sehen, dass auch Sektionen nicht eindeutig sind. Können Sie eine ähnliche Familie von Beispielen finden?

Bemerkung 1.36. Seien $A \xrightarrow{f} B \xrightarrow{g} C$ zwei Abbildungen.

(a) Wenn f und g invertierbar sind, dann ist $g \circ f$ invertierbar mit Inverse $f^{-1} \circ g^{-1}$.

(b) Wenn f und g injektiv (bzw. surjektiv) sind, dann ist $g \circ f$ injektiv (bzw. surjektiv).

Die Umkehrung gilt allgemein nicht (d.h. $g \circ f$ - inj./surj./inv. $\not\Rightarrow$ f und g - inj./surj./inv.).

Hier ist eine weitere Charakterisierung[16] der Injektivität.

Satz 1.37. *Eine Abbildung $f : A \longrightarrow B$ ist injektiv wenn und nur wenn für jede Menge A' und für alle Abbildungen $g, g' : A' \longrightarrow A$ gilt*

$$\text{aus } f \circ g = f \circ g' \text{ folgt } g = g'.$$

Beweis-Skizze: $\boxed{\Rightarrow}$ `Variante 1:` Sei f injektiv, und seien $A', g,$ und g' beliebig mit der Eigenschaft, dass $f \circ g = f \circ g'$. Für jedes $x \in A'$ haben wir also $f(g(x)) = f(g'(x))$. Da f injektiv ist, folgt daraus, dass $g(x) = g(x')$. Wir haben also bewiesen, dass

$$g(x) = g'(x) \ \forall x \in A'.$$

Das heißt, dass $g = g'$.
`Variante 2:` Aus Satz 1.33 existiert eine Linksinverse f' von f, also

$$f \circ g = f \circ g' \Rightarrow f' \circ (f \circ g) = f' \circ (f \circ g') \Rightarrow (f' \circ f) \circ g = (f' \circ f) \circ g' \Rightarrow \mathrm{id}_A \circ g = \mathrm{id}_A \circ g' \Rightarrow g = g'.$$

$\boxed{\Leftarrow}$ Wir wissen also, dass für jede Menge A' und für alle Abbildungen $g, g' : A' \longrightarrow A$ gilt "aus $f \circ g = f \circ g'$ folgt $g = g'$". Wir wollen zeigen, dass f injektiv ist. Nehmen wir an, dass das Gegenteil wahr ist, und zwar $\exists\, x \neq x' \in A$ mit $f(x) = f(x')$. Wir werden jetzt zeigen, dass die Negation der Voraussetzung gilt. Dafür wählen wir die Menge $A' = \{1, 2\}$ und definieren die Abbildung g, g' mit

$$\Gamma_g = \{(1, x), (2, x')\} \quad \text{und} \quad \Gamma_{g'} = \{(1, x), (2, x)\}.$$

[16] Abbildungen mit dieser Eigenschaft heißen *Monomorphismen*.

Weil $x \neq x'$ haben wir auch $g \neq g'$. Aber

$$\Gamma_{f\circ g} = \{(1, f(x)), (2, f(x')\} = \{(1, f(x), (2, f(x))\} = \Gamma_{f\circ g'}.$$

Wir haben also gezeigt, dass es A', g, g' gibt mit $f \circ g = f \circ g'$ und $g \neq g'$ - ein Widerspruch ↯.
Q.E.D.

Surjektivität hat eine duale Beschreibung[17].

Satz 1.38. *Eine Abbildung $f : A \longrightarrow B$ ist surjektiv wenn und nur wenn für jede Menge B' und für alle Abbildungen $g, g' : B \longrightarrow B'$ gilt*

$$\text{aus } g \circ f = g' \circ f \text{ folgt } g = g'.$$

Beweis-Skizze: $\boxed{\Rightarrow}$ Aus Satz 1.33 folgt, dass f eine Sektion $s : B \longrightarrow A$ hat. Das heißt, $f \circ s = \mathrm{id}_B$. Wenn wir also beide Seiten von $g \circ f = g' \circ f$ mit s verknüpfen, und die Assoziativität anwenden, bekommen wir $g = g'$.
$\boxed{\Leftarrow}$ Nehmen wir an, dass f nicht surjektiv ist. Dann existiert ein Element $b' \in B$, das nicht im Bild von f liegt. Wir definieren dann $g, g' : B \longrightarrow \{0, 1\}$ durch

$$g(b) = 0, \ \forall \ b \in B. \qquad g'(b) = \begin{cases} 0, & \text{wenn } b \neq b' \\ 1, & \text{sonst .} \end{cases}$$

Dann haben wir $g \circ f = g' \circ f$, aber $g \neq g'$, ein Widerspruch ↯. Q.E.D.

1.2.9 Familien von Mengen

Oft haben wir mehr als zwei Mengen im Spiel. Wir könnten sogar unendlich viele Mengen auf einmal betrachten und behandeln. Und manchmal könnten einige dieser Mengen mehrmals ins Spiel kommen. Wir brauchen also einen wohl definierten Begriff, der uns eine solche Situation beschreibt. Dafür führen wir den Begriff von *Familie von Mengen* ein. Eine Familie besteht aus einer *Indexmenge* I, dessen Elemente **Indizes** heißen, aus einer Menge $\mathcal{M}$, dessen Elementen Mengen sind (dazwischen auch die Mengen die wir in unserer Familie haben wollen), und aus einer Abbildung $f : I \longrightarrow \mathcal{M}$. Das heißt, dass wir jedem Index $i \in I$ eine Menge $M_i \in \mathcal{M}$ zuordnen. Wir sprechen dann von einer von I indizierten **Familie** von Mengen und schreiben dafür

$$(M_i)_{i\in I}.$$

Wir können die Definition von Vereinigung und Durchschnitt auf Familien verallgemeinern.

Definition 1.39. Wenn I eine Indexmenge ist und $(M_i)_{i\in I}$ eine Familie von Teilmengen einer Menge M ist, dann definieren wir die Vereinigung, beziehungsweise den Durchschnitt, der Familie als

$$\bigcup_{i\in I} M_i := \{x \in M \mid \exists\, i \in I \text{ sodass } x \in M_i\},$$

$$\bigcap_{i\in I} M_i := \{x \in M \mid \forall\, i \in I \text{ gilt } \ x \in M_i\}.$$

[17] Abbildungen mit der folgenden Eigenschaft heißen *Epimorphismen*.

Wenn $I = \{1, \dots, n\}$, dann schreiben wir

$$\bigcup_{i=1}^{n} M_i := M_1 \cup \dots \cup M_n := \bigcup_{i \in \{1,\dots,n\}} M_i.$$

Wenn $I = \mathbb{N}$, dann schreiben wir

$$\bigcup_{i \geqslant 0} M_i := \bigcup_{i=0}^{\infty} M_i \quad := \quad M_0 \cup \dots \cup M_n \cup \dots := M_0 \cup M_1 \dots := \bigcup_{i \in \mathbb{N}} M_i.$$

Analoges gilt für den Durchschnitt.

Beispiele:

1. Das Komplement der Menge aller ganzen Zahlen in der Menge der reellen Zahlen ist

$$\begin{aligned} \mathbb{R} \setminus \mathbb{Z} &= \dots \cup (-2,-1) \cup (-1,0) \cup (0,1) \cup (1,2) \dots \\ &= \bigcup_{a \in \mathbb{Z}} (a, a+1), \end{aligned}$$

   wobei $(a,b) = \{x \in \mathbb{R} \mid a < x < b\}$ das offene Intervall bezeichnet[18]

2. $$\bigcap_{i=1}^{\infty} (-\frac{1}{i}, \frac{1}{i}) = \{0\} \qquad \bigcup_{i=1}^{\infty} (-i, i) = \mathbb{R}$$

Wir werden jetzt das Kartesische Produkt auf Familien verallgemeinern.

Definition 1.40. Sei I eine Indexmenge und $(M_i)_{i \in I}$ eine Familie von Mengen M_i. Das **Kartesische Produkt der Familie** $(M_i)_{i \in I}$ ist die Menge

$$\prod_{i \in I} M_i := \left\{ I \xrightarrow{f} \textstyle\bigcup_{i \in I} M_i \mid \forall\, i \in I \text{ gilt } f(i) \in M_i \right\}.$$

Wenn $I = \{1, 2, \dots, n\}$, dann heißt ein Element der Menge $\prod_{i=1}^{n} M_i$ ein **n-Tupel**. Die kompakte Schreibweise für eine n-Tupel $f : I \longrightarrow M$ ist

$$(x_1, \dots, x_n), \qquad \text{wobei } x_i := f(i) \in M_i.$$

Das scheint ein Zirkelschluss zu sein, weil wir in der Definition von Abbildung den Begriff *Tripel* (also 3-Tupel) verwendet haben. Das ist es aber nicht, weil wir vorher endliche Tupel ohne Hilfe der Abbildungen definiert haben. Die erste Bemerkung sollte also sein, dass n-Tupel wie in (1.7) definiert (siehe Seite 23) und die endlichen n-Tupel aus Definition 1.40 sind äquivalente Begriffe. Das heißt beide sind vollständig durch die folgende Eigenschaft charakterisiert:

Bemerkung 1.41. Aus der Definition von n-Tupel und der Definition von Menge folgt, dass

$$(x_1, \dots, x_n) = (y_1, \dots, y_n) \quad \Longleftrightarrow \quad x_i = y_i \;\; \forall\, i = 1, \dots, n$$[19]

[18] Meistens in dieser Vorlesung wird (a,b) ein geordnetes Paar bezeichnen, cf. Definition 1.19.

[19] $\forall\, i = 1, \dots, n$ ist eine Schreibweise für $\forall\, i \in \{1, \dots, n\}$

Für den sorgfältigen Aufbau der Mengenlehre braucht man folgendes Axiom. Obwohl wir hier Mengen nicht axiomatisch eingeführt haben, erwähnen wir dieses Axiom weil wir es später explizit (oder implizit durch andere äquivalente Aussagen) anwenden werden. Mehr zu diesem Axiom findet man in [Rau08, 2.7].

Das Auswahlaxiom. *Zu jeder Menge $\mathcal{P}$ von nicht-leeren Mengen gibt es eine Abbildung f die jedem $X \in \mathcal{P}$ ein Element $f(X) \in X$ zuordnet.*

Bemerkung 1.42. Das Auswahlaxiom ist äquivalent zu der Aussage:

Für jede Familie $(M_i)_{i\in I}$ von nicht-leeren Mengen ist das kartesische Produkt $\prod_{i\in I} M_i$ nicht leer.

Beispiele:

1. Wenn $A = \{0, 1\}$, dann haben wir
$$A^3 = \{(0,0,0), (1,0,0), (0,1,0), (0,0,1), (1,1,0), (1,0,1), (0,1,1), (1,1,1)\}.$$
2. $\mathbb{R}^3 = \{(x, y, z) \mid x, y, z \in \mathbb{R}\}$.
3. Wenn M die Menge aller Zeichen die man mit einer Laptop-Tastatur schreiben kann, dann ist jedes Buch ein unendliches Tupel aus $M^{\mathbb{N}}$ mit der Eigenschaft, dass ab einer gewissen Stelle nur das Leerzeichen vorkommt, und wir das nicht mehr aufschreiben.

1.2.10 Mächtigkeit

Wir haben bis jetzt die Anzahl von Elementen einer Menge nicht genau definiert. Der Grund dafür ist, dass wir intuitive Begriffe von Kardinalität, von Endlichkeit und Unendlichkeit zur Verfügung hatten. Die Definition *Eine Endliche Menge ist eine Menge die endlich viele Elementen hat*, obwohl sehr intuitiv, klingt "unmathematisch"[20]. Der Intuition von was "endlich" und "Anzahl" heißt kann man (und soll man) weiterhin gut vertrauen. Man sollte aber diese auch gründlich definieren. Der letzte Teil dieses Kapitels ist ein Beispiel für die genaue Formulierung eines intuitiven Begriffes betrachten. "Genau" heißt in diesem Kontext, dass es nur mit Hilfe von Begriffen die bereits mathematisch definiert wurden formuliert ist.

Definition 1.43. Zwei Mengen A und B heißen **gleichmächtig** genau dann, wenn es eine Bijektion von A in B gibt.

Das poetische an diesem Teil ist, dass die Definition von Endlichkeit ist "nicht Undendlichkeit". Das ist so, weil die Definition von unendliche Menge natürlicher[21] ist.

Definition 1.44 (Dedekind Unendlichkeit)**.** Eine Menge M ist **unendlich** genau dann, wenn es eine echte Teilmenge $M' \subsetneq M$ gibt die gleichmächtig mit M ist. Eine Menge ist **endlich** wenn diese nicht unendlich ist.

[20] Was ich hier meine ist, dass ein Begriff "endlich" scheint durch sich selbst "endlich viele" definiert zu sein.

[21] das heißt wir durch die Existenz einer gewisser Art von Abbildung gegeben, und Existenz ist schöner als Nichtexistenz.

Man kann unendliche Mengen auch mit Hilfe von der Menge der natürlichen Zahlen definieren: Eine Menge M ist endlich, wenn es eine natürliche Zahl n und eine Bijektion $f : M \longrightarrow \mathbb{N}_{<n}$ gibt, wobei $\mathbb{N}_{<n} := \{a \in \mathbb{N} \ : \ a < n\} = \{0, 1, \ldots, n-1\}$. Da wir die natürlichen Zahlen hier nicht genau definiert haben, habe ich das nicht als Definition gegeben. Diese Aussage ist äquivalent zu Dedekinds Definition, und wir werden das als Satz beweisen (cf. Satz 1.53).

Bemerkung 1.45. Eine Menge M ist unendlich wenn und nur wenn es eine injektive Abbildung $f : M \longrightarrow M$ gibt die nicht surjektiv ist. Diese findet man indem man den Wertebereich der Bijektion zwischen M und $M' \subsetneq M$ auf M erweitert.

Die Abbildung $f : \mathbb{N} \longrightarrow \mathbb{N}$, $f(n) = n + 1$, zeigt dass die Menge der natürlichen Zahlen unendlich ist.

Definition 1.46. Eine Menge ist **abzählbar** wenn sie gleichmächtig zu der Menge der natürlichen Zahlen ist.

Satz 1.47. *Wenn eine Menge M eine unendliche Menge N als echte Teilmenge hat ($N \subsetneq M$) dann ist die Menge M auch unendlich.*

Beweis-Skizze: Weil N unendlich ist, gibt es $f : N \longrightarrow N$ die injektiv aber nicht surjektiv ist. Wir definieren dann $\bar{f} : M \longrightarrow M$ durch

$$\bar{f}(x) = \begin{cases} x, & \text{wenn } x \in M \setminus N \\ f(x), & \text{wenn } x \in N. \end{cases}$$

Dann ist auch $\bar{f}$ injektiv aber nicht surjektiv, also ist M unendlich. Q.E.D.

Korollar 1.48. Jede Teilmenge einer endlichen Menge ist endlich.

Satz 1.49. *Es sei M eine Menge und $2^M = \{N \subseteq M\}$ die Potenzmenge davon. Es gibt keine bijektive Abbildung $f : M \longrightarrow 2^M$.*

Beweis-Skizze: (Siehe VL.10 Video ab Minute 0:43:00)
Wir nehmen an, es existiert eine bijektive Abbildung $f : M \longrightarrow 2^M$. Wir definieren dann

$$B := \{m \in M \ : \ m \notin f(m)\} \in 2^M.$$

Weil f bijektiv, also insbesondere surjektiv, ist, existiert $b \in M$ mit $f(b) = B$. Wir haben dann folgende Äquivalenzen:

$$b \notin B \iff b \notin f(b) \iff b \in B.$$

Wir haben somit einen Widerspruch, es kann also keine Bijektion f geben. Q.E.D.

Bemerkung 1.50. Abzählbare Mengen sind die kleinsten unendlichen Mengen.

Satz 1.51. *Die Menge der reellen Zahlen ist nicht abzählbar.*

Beweis-Skizze: (Siehe VL.10 Video ab Minute 0:01:00) Q.E.D.

Satz 1.52. *Die Menge* $\mathbb{N}_{<n} := \{a \in \mathbb{N} \mid a < n\}$ *ist endlich.*

Beweis-Skizze: Wir beweisen das durch vollständige Induktion.
Der Induktionsanfang: $\boxed{k = 0}$ - dann ist $\mathbb{N}_{<0} = \emptyset$ und diese hat keine echte Teilmengen, und ist also nach Definition 1.44 endlich.
Extra:
Wir schauen uns auch den Fall $k = 1$ an: $\mathbb{N}_{<1} = \{0\}$. Dann ist $\mathbb{N}_{<1} \times \mathbb{N}_{<1} = \{(0,0)\}$, also die einzige Abbildung $f : \mathbb{N}_{<1} \longrightarrow \mathbb{N}_{<1}$ ist $\mathrm{id}_{N_{<1}}$.

$\boxed{k \Rightarrow k+1}$ Sei $k \geq 1$, sodass $N_{<k}$ endlich ist. Sei $f : \mathbb{N}_{<k+1} \longrightarrow \mathbb{N}_{<k+1}$ eine injektive Abbildung. Wir haben $\mathbb{N}_{<k} \subset \mathbb{N}_{<k+1}$, also können wir über $f(\mathbb{N}_{<k})$ sprechen.
Fall 1: $f(\mathbb{N}_{<k}) \subseteq \mathbb{N}_{<k}$. Dann ist aus der induktiven Voraussetzung $f(\mathbb{N}_{<k}) = \mathbb{N}_{<k}$, also muss auch $f(k) = k$ und f ist surjektiv.
Fall 2: $f(N_{<k}) \not\subseteq N_{<k}$. Dann existiert $a \in \mathbb{N}_{<k}$ mit $f(a) = k$. Da f injektiv ist, muss $f(k) \neq k$ sein, also $f(k) = b \in \mathbb{N}_{<k}$. Wir definieren dann

$$f'(x) = \begin{cases} f(x) & \text{wenn } x \notin a, k \\ b & \text{wenn } x = a \\ k & \text{wenn } x = k \end{cases}$$

Wir haben, dass f' injektiv ist, $f'(\mathbb{N}_{<k+1}) = \mathbb{N}_{<k+1}$ und $f'(\mathbb{N}_{<k}) \subseteq \mathbb{N}_{<k}$. Aus Fall 1 ist also f' surjektiv, und also auch f. Q.E.D.

Satz 1.53. *Für jede endliche Menge* M *gibt es ein eindeutiges* $n \in \mathbb{N}$*, sodass* M *gleichmächtig mit* $\mathbb{N}_{<n}$ *ist.*

Beweis-Skizze: Sei M eine beliebige endliche Menge. Nehmen wir an, dass für alle $n \in \mathbb{N}$, M nicht gleichmächtig zu $\mathbb{N}_{<n}$ ist. Wenn $M = \emptyset$, dann ist $M = \mathbb{N}_{<0}$. Also $M \neq \emptyset$. Wir suchen einen Widerspruch. Zu diesem Ziel werden wir induktiv eine Familie von injektive Abbildungen $(f_n : \mathbb{N}_{<n} \longrightarrow M)_{n \geq 1}$ mit der Eigenschaft das $\mathrm{Bild}(f_n) \subsetneq \mathrm{Bild}(f_{n+1})$ konstruieren[a].

$\boxed{n = 1}$ Da $M \neq \emptyset$ folgt, dass $\exists\, y_0 \in M$. Wir definieren dann $f_1 : \mathbb{N}_{<1} \longrightarrow M$ durch

$$f_1(0) = y_0.$$

$\boxed{n \Rightarrow n+1}$ Sei $f_n : \mathbb{N}_{<n} \longrightarrow M$ die injektive Abbildung die wir für den induktiven Schritt voraussetzen. Unsere Annahme ist, dass M mit keiner der Mengen $M_{<k}$ gleichmächtig ist. Insbesondere, darf f_n nicht surjektiv sein. Es gibt also $y_{n+1} \in M \setminus \mathrm{Bild}(f_n)$. Wir definieren dann $f_{n+1} : \mathbb{N}_{<n+1} \longrightarrow M$ durch

$$f_{n+1}(a) := \begin{cases} f(a) & \text{wenn } a < n \\ y_{n+1} & \text{wenn } a = n. \end{cases}$$

Die Abbildung f_{n+1} ist wohl definiert, injektiv, und $\mathrm{Bild}(f_n) \subsetneq \mathrm{Bild}(f_{n+1})$ weil $y_{n+1} \notin \mathrm{Bild}(f_n)$. Wir haben also eine Teilmenge $Y = \{y_i \mid i \in \mathbb{N}\} \subseteq M$, die gleichmächtig zu $\mathbb{N}$ und somit unendlich ist, definiert. Aus Satz 1.47 folgt, dass M unendlich ist – ein Widerspruch ↯. Es existiert also ein

$n \in \mathbb{N}$ sodass M gleichmächtig mit $\mathbb{N}_{<n}$ ist.

Wenn es zwei verschiedene natürliche Zahlen m und n, und zwei bijektive Abbildungen $f : M \longrightarrow \mathbb{N}_{<n}$ und $g : M \longrightarrow \mathbb{N}_{<m}$ gibt, dann können wir ohne die Allgemeinheit zu verlieren annehmen, dass $m < n$. Dann ist $\mathbb{N}_{<m} \subsetneq \mathbb{N}_{<n}$ und $g \circ f^{-1} : \mathbb{N}_{<n} \longrightarrow \mathbb{N}_{<m}$ eine bijektive Abbildung von $\mathbb{N}_{<n}$ in der echten Teilmenge $\mathbb{N}_{<m}$ - ein Widerspruch zur Endlichkeit von $\mathbb{N}_{<n}$ (Satz 1.52). Q.E.D.

[a] "Induktiv konstruieren" heißt zuerst f_1 definieren, dann annehmen, dass f_n definiert wurde und mit Hilfe von f_n eine Abbildung f_{n+1} definieren.

Definition 1.54. Sei M eine endliche Menge. Die **Mächtigkeit** (oder **Kardinalität**) von M ist die eindeutige natürliche Zahl für die M gleichmächtig mit $\mathbb{N}_{<n}$ ist. Für unendliche Mengen definieren wir die Mächtigkeit einfach als ∞. Die Mächtigkeit von M wird mit $|M|$ oder $\sharp M$ bezeichnet.

[6] 1.11.'24

Kapitel 2

Mathematik Lesen und Schreiben

Lesen Sie Kevin Houston *Wie man mathematisch Denkt*, Teil III und IV (Kapitel 14 – 26)!

2.1 Mathematischer Text

Mathematik wird selten wie Prosa präsentiert. Das Material wird in kleinen Stücke zerlegt die *Definition, Satz, Proposition, Lemma, Korollar, Bemerkung, Beweis, Beispiel, Vermutung* genannt werden. Oft werden diese auch durchnummeriert. Deswegen ist ein mathematischer Text üblicherweise auch von weitem einfach zu erkennen.

Mathematik ließt man auch anders als Literatur. Die Information ist sehr dicht, und man braucht viel Zeit um es auszupacken. Es ist auch empfohlen Mathematik mit einem Stift in der Hand zu lesen. Dann kann man Notizen machen, Beispiele hinzufügen, Beweisschritte ergänzen. Es ist nicht selten, eine ganze Stunde beim Lesen einer einzigen Seite eines Mathebuchs zu verbringen. Fühlen Sie Sich also nicht unter Zeitdruck. Stellen Sie lieber sicher, dass Sie den Text gut verstanden haben. Weiter lesen und dann später zurückkommen ist auch eine gute Methode. Sie finden viel mehr zu diesem Thema (und viel besser geschrieben) in [Hou2012, Kapitel 1]. Hier werde ich nur kurz die Bausteine eines mathematischen Textes erklären.

2.1.1 Axiome

Axiome sind Aussagen die als Ausgangspunkt einer mathematischen Theorie gewählt werden. Das heißt, es sind Aussagen die von Anfang an als wahr genommen werden, ohne einen Beweis zu brauchen. In Euklids *Elementen* war diese "Aussagen die offensichtlich wahr sind". In der modernen Mathematik werden diese aber einfach als Wahl betrachtet. Nicht jede Wahl ist genau so gut wie jede andere. Insbesondere will man keine Widersprüche in der Theorie aufbauen. Wir haben ein solches Problem mit Cantors Definition von Menge gesehen.

Wir haben bis jetzt wenig davon gesehen, weil wir die Axiomatik der Mengenlehre übersehen haben. Wir werden viel mehr darüber in dem Teil über elementare Geometrie sprechen. Wir haben aber ein Beispiel gehabt:

Axiom: *Es existiert eine Menge $\emptyset$, sodass "$x \notin \emptyset$" wahr für alle möglichen x ist.*

Die Existenz der Lehren Menge kann man nicht beweisen. Man könnte sich auch eine Theorie vorstel-

len ohne einer leeren Menge. Es ist aber praktisch dieses Axiom als Grundlage der Mengenlehre zu nehmen.

Die Eigenschaften die in grundlegende Definition vorkommen werden auch Axiome genannt. Das werden wir später durch Ordnungsrelationen, Äquivalenzrelationen, affine/projektive Geometrie, Gruppen illustrieren.

2.1.2 Definitionen

Genaue Definitionen sind zentral für die höhere Mathematik. Das ist einer der großen Unterschiede zu der Schul-Mathematik. Man muss sich einigen was "Wörter" (Begriffe) heißen. Das muss man sehr genau formulieren und man sollte sich nur auf Begriffe die durch Axiome oder Definitionen schon festgelegt wurden verlassen.

Wir haben bis jetzt mehrere Beispiele von Definitionen gesehen. Wir haben auch gesehen, was für Probleme entstehen können wenn man sich zu viel auf der Alltagssprache verlässt. (Siehe Definitionen 1.2.1 und 1.18).

In einer Definition werden meistens die Natur und die Eigenschaften des Begriffes gegeben. Zum Beispiel:

Definition 2.1. Eine **Primzahl** ist eine natürliche Zahl p mit den Eigenschaften $p > 1$ und p ist nur durch 1 und sich selbst teilbar.

Manchmal definiert man eine Eigenschaft. Das heißt, man führt ein Adjektiv ein, das eine längere Eigenschaft ersetzt. Zum Beispiel:

Definition 2.2. Eine Menge M ist **unendlich** genau dann, wenn es eine echte Teilmenge $M' \subsetneq M$ gibt die gleichmächtig mit M ist.

Hier haben wir dem Adjektiv "unendlich" eine klare mathematische Bedeutung gegeben wenn es sich auf einer Menge bezieht. Die "klare mathematische Bedeutung" ist die Aussage

$$\exists\, M' \subsetneq M \text{ und } \exists\, f : M' \longrightarrow M \text{ bijektiv.}$$

Wir haben also eigentlich **unendliche Menge** definiert, und nicht nur *unendlich*. Man soll auch bemerken, dass wir für diese Definition die Begriffe *Menge*, *echte Teilmenge*, und *gleichmächtig* voraussetzen.

Achtung! Wenn in einer Definition nur "wenn" vorkommt, dann wird es als "genau dann wenn" interpretiert. Das ist eine weit verbreitete Konvention. Zum Beispiel:

Definition: *Eine ganze Zahl ist **gerade** wenn diese durch Zwei teilbar ist.*

Sagt uns eigentlich:

Definition: $z \in \mathbb{Z}$ *ist **gerade*** $\iff 2 \mid z$.

[7] 6.11.'24

2.1.3 Sätze, Propositionen, Lemmata, Korollare, Vermutungen

Diese sind die Bausteine der Mathematik. Es gibt ein wichtiger Unterschied zwischen den ersten vier und Vermutungen: die ersten vier haben auch einen Beweis, Vermutungen (noch) nicht. Das heißt, die ersten vier sind *wahre Aussagen*. Vermutungen sind *hoffentlich wahre Aussagen*. Die Vermutungen kann man als den lebendigen Teil der Mathematik sehen; oder als die Baustellen. Forschung in der Mathematik ist oft die Suche nach dem Wahrheitswert einer Vermutung. Also die Suche nach einem Beweis oder nach einer Widerlegung einer Aussage.

Strukturell sind sie als Aussagen nicht zu unterscheiden. Alle fünf sind Aussagen, und diese können (fast) immer als eine Implikation formuliert werden:

Satz: *Wenn V, dann S.*

Oft ist aber V eine komplexe (d.h. zusammengesetzte) Aussage, die meistens mit Hilfe der Konjunktion *und* zusammen gesetzt wird. Wenn also $V = V_1$ und V_2 und $\dots$ und V_m, dann werden die V_i die **Voraussetzungen** genannt. Die Aussage S wird **Schlussfolgerung** genannt. Man muss aber aufpassen, da Sätze nicht immer in so einer klaren Standardform gegeben werden.

Der Unterschied zwischen *Satz, Proposition, Lemma*, und *Korollar* hat nichts mit der Formulierung zu tun, sondern mit der Wichtigkeit der Aussage. Das heißt mit den Zusammenhängen mit dem Rest der Theorie, mit der Universalität der Aussage, und oft auch mit der Eleganz oder mit der Schönheit der Aussage. Ich übernehme hier die Beschreibung von Kevin Houston [Hou2012, Kapitel 14]:

- **Satz** oder **Theorem**: Eine sehr wichtige wahre und bewiesene Aussage.
- **Proposition**: Eine weniger wichtige, aber immer noch interessante wahre und bewiesene Aussage.
- **Lemma**: Eine wahre und bewiesene Aussage die zum Beweis andere Aussagen benötigt wird.
- **Korollar**: Eine wahre Aussage die auf einfache Weise[1]aus einem Satz, aus einer Proposition, oder aus einem Lemma folgt.

Wir geben hier die drei Beispiele aus [Hou2012, Kapitel 16][2] und noch zwei weitere.

Satz 1: *Wenn $m, n \in \mathbb{Z}$ ungerade sind, dann ist $m \cdot n$ ungerade.*

Satz 2: *Es gibt unendlich viele Primzahlen.*

Satz 3: *Die reelle Zahl $\sqrt{2}$ ist irrational.*

Satz 4: *In einem rechtwinkligen Dreieck ist das Quadrat der Hypotenuse gleich der Summe der Quadrate der anderen beiden Seiten.*

Satz 5: *Es seien A, B, C Mengen mit $A \cap C \subseteq B$ und $a \in C$. Es gilt $a \notin A \setminus B$.*

Wir geben hier Umformulierungen dieser Sätze als Implikationen. Das ist ein wichtiger Schritt im Identifizieren der Voraussetzungen und der Schlussfolgerung. Satz 1 ist schon als Implikation formuliert.

[1] *Einfach* heißt meistens einen Sonderfall der Schlussfolgerung oder eine Verstärkung der Voraussetzung. Zum Beispiel **Satz:** *Das Produkt zweier ungeraden Zahlen ist ungerade.* hat das **Korollar:** *Das Quadrat einer ungeraden Zahl ist ungerade.*

[2] Diesen Kapitel (eigentlich das ganze Buch) sollten Sie lesen!

Satz 2: *Wenn P die Menge der Primzahlen ist, dann ist P unendlich.*

Satz 3: *Wenn $x = 2$, dann ist $\sqrt{x}$ irrational.*

Satz 4: *Wenn Δ ein rechtwinkliges Dreieck mit Seitenlängen a und b, und mit Länge der Hypotenuse c, dann gilt $a^2 + b^2 = c^2$.*

Satz 5: *Wenn $A \cap C \subseteq B$ und $a \in C$, dann $a \notin A \setminus B$.*

Weil die Schlussfolgerung in Satz 5 die Negation einer Aussage ist, lohnt es sich daran umzubasteln:

$$\begin{aligned}
a \notin A \setminus B &\Leftrightarrow \text{nicht}(a \in A \setminus B). \\
&\Leftrightarrow \text{nicht}(a \in A \,\text{und}\, a \notin B). \\
&\Leftrightarrow a \notin A \ \text{ oder } a \in B. \\
&\Leftrightarrow \text{nicht}(\text{nicht}(a \notin A \ \text{ oder } a \in B.)) \\
&\Leftrightarrow \text{nicht}(a \in A \,\text{und}\, a \notin B.)) \\
&\Leftrightarrow a \in A \Rightarrow a \in B.
\end{aligned}$$

Die Wir könne also Satz 5 nochmal umformulieren:

Satz 5: *Wenn $A \cap C \subseteq B$ und $a \in C$, dann $a \in A \Rightarrow a \in B$.*

Weil die Schlussfolgerung eine Implikation ist, können wir die Voraussetzung dieser Implikation ($a \in A$) zu den Voraussetzungen des Satzes dazu packen:

Satz 5: *Wenn $A \cap C \subseteq B$ und $a \in C$ und $a \in A$, dann $a \in B$.*

Nach dieser Umformulierung ist der Satz fast offensichtlich.

2.2 Beweistechniken

Ein Beweis besteht aus einer Kette von Aussagen. Diese sind durch die Regeln der Logik miteinander verbunden, sodass eine Aussage an einer gewissen Stelle aus eine oder mehrere der vorigen Aussagen folgt. Das werden wir einen Schritt im Beweis nennen. Was eine angemessene Schreibweise für ein Beweis ist, ist leider schwierig im ganz allgemeinem Fall zu definieren. Wenn man wirklich alle Schritte aufschreiben würde, dann wären die meisten Beweise viel zu lang. Alle *schwierige* Schritte sollten aber im Beweis vorkommen. Diese zu erkennen ist eine Fähigkeit die man trainieren muss. Wir zeigen hier einige der wichtigsten Strategien die man in einem Beweis anwenden kann.

2.2.1 Direkter Beweis

Satz 2.3. *Es seien A und B Mengen. Dann gilt $A \cap B \subseteq A \cup B$.*

Beweis-Skizze:

$$\begin{aligned}
x \in A \cap B &\Rightarrow x \in A \,\text{und}\, x \in B, && \text{(aus der Definition von } \cap) \\
&\Rightarrow x \in A, && \text{(aus der Definition von } \textit{und}) \\
&\Rightarrow x \in A \ \text{ oder } x \in B, && \text{(aus der Definition von } \textit{oder}) \\
&\Rightarrow x \in A \cup B. && \text{(aus der Definition von } \cup)
\end{aligned}$$

Q.E.D.

Lemma 2.4. *Wenn m eine ungerade ganze Zahl ist, dann ist auch m^2 ungerade.*

Beweis-Skizze: Wenn m ungerade ist, dann existiert $k \in \mathbb{Z}$ sodass $m = 2k + 1$. Daraus folgt

$$m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

also auch ungerade. Q.E.D.

Korollar 2.5. Es sei $m \in \mathbb{Z}$. Wenn m^2 gerade ist, dann ist auch m gerade.

Beweis-Skizze: Das ist die Kontraposition der Aussage aus Lemma 2.4. Q.E.D.

2.2.2 Widerspruchsbeweis

Sei die Aussage deren Wahrheit wir beweisen wollen

$$A: \qquad V \Rightarrow S.$$

In einem Widerspruchsbeweis zeigen wir eigentlich, dass die Negation dieser Implikation falsch ist. Das heißt wir zeigen

$$\text{nicht}(A): \qquad V \text{ und nicht}(S) \quad \text{ist falsch.}$$

Das beweist man, indem man einen Widerspruch daraus folgt. Ein Widerspruch ist eine Aussage W die immer falsch ist. Also

$$\text{wenn } [A \Rightarrow W] \text{ wahr ist, dann muss } A \text{ falsch sein.}$$

Der häufigste Widerspruch ist "E und nicht(E)" für irgendwelche Aussage E. Oft ist E ein Teil der Voraussetzung oder S; es muss aber nicht das sein. Hier sind zwei Beispiele dieser Beweisstrategie.

Satz 2.6. *Die reelle Zahl $\sqrt{2}$ ist irrational.*

Das heißt, $\sqrt{2}$ ist nicht rational. Genauer gesagt, es gibt keine $m, n \in \mathbb{Z}$ mit $n \neq 0$ sodass $\sqrt{2} = \frac{m}{n}$.

Beweis-Skizze: Nehmen wir an, dass $\sqrt{2} = \frac{m}{n}$ mit $m, n \in \mathbb{Z}$. Wir dürfen auch annehmen, dass m und n teilerfremd[a] sind, weil jeder Bruch so dargestellt werden kann. Dann haben wir

$$\begin{aligned} \sqrt{2} &= \tfrac{m}{n} \\ 2 &= \left(\tfrac{m}{n}\right)^2 \\ 2 &= \tfrac{m^2}{n^2} \\ 2n^2 &= m^2. \end{aligned}$$

Aus Korollar 2.5 folgt m ist gerade. Also existiert ein $k \in \mathbb{Z}$ mit $m = 2k$, und somit

$$2n^2 = (2k)^2 = 4k^2 \iff n^2 = 2k^2.$$

Wieder aus Korollar 2.5 folgt, dass n gerade ist. Also m und n sind beide gerade, also beide durch

2 teilbar, und das widerspricht "m und n sind teilerfremd". Das heißt, dass die Aussage als wahr folgen würde, die aber ein Widerspruch ist, ist:

$$(m \text{ und } n \text{ sind teilerfremd}) \text{ und } (2 \text{ teilt } m \text{ und } 2 \text{ teilt } n).$$

Q.E.D.

[a] Das heißt, dass m und n keinen andere gemeinsame (positive) Teiler außer 1 haben. Das ist äquivalent zu der Aussage:

$$\text{Wenn } d \text{ teilt } m \text{ und } d \text{ teilt } n, \text{ dann } d = 1.$$

Wir können das für jeden Bruch annehmen, weil wenn $m = d \cdot m'$ und $n = d \cdot n'$ dann gilt

$$\frac{m}{n} = \frac{\cancel{d} \cdot m'}{\cancel{d} \cdot n'} = \frac{m'}{n'}.$$

Proposition 2.7. *Es gibt keine positive ganze Zahlen x und y, sodass $x^2 - y^2 = 1$.*

Beweis-Skizze: Nehmen wir an $\exists\, x, y \in \mathbb{Z}$ mit $x, y > 0$ und $x^2 - y^2 = 1$. Wir haben dann

$$x^2 - y^2 = (x + y)(x - y) = 1.$$

Weil $x, y \in \mathbb{Z}$, dann haben wir auch $x + y, x - y \in \mathbb{Z}$. Das heißt aber, dass $x + y = x - y = 1$, oder $x + y = x - y = -1$. In beiden Fällen folgt $y = 0$. Der Widerspruch ist also "$y > 0$ und $y = 0$". Wir zeigen genauer warum $y = 0$ aus $x + y = x - y = 1$ folgt:

$$\begin{array}{rcl} x + y & = & 1 \\ x - y & = & 1 \quad - \\ \hline 2y & = & 0 \end{array}$$

Also $y = 0$. Für -1 ist der Beweis analog[a]. Q.E.D.

[a] Das heißt, es reicht -1 an der stelle von 1 einzusetzen um den Beweis zu bekommen.

[8] 8.11.'24

2.2.3 Beweis durch Fallunterscheidungen

Die Idee hinter dieser Technik ist eine Voraussetzung hinzuzufügen, die uns den Beweis erleichtert. Der Nachteil ist, dass wir dann mindestens zwei verschiedene Implikationen zeigen müssen. Im einfachsten Fall handelt sich um eine so genannte *Dichotomie*, das heißt eine Aufteilung in zwei: F oder nicht(F). Im allgemeinem Fall:

$$F1 \text{ oder } F2 \text{ oder } \ldots \text{ oder } Fn$$

ist es wichtig, dass die Aussage "$F1$ oder $F2$ oder $\ldots$ oder Fn" eine Tautologie ist. Das heißt, dass wir alle Situationen abgedeckt haben.

Für unser erstes Beispiel fangen wir mit einer Definition an.

Definition 2.8. Es seien n und k natürliche Zahlen. Der **Binomialkoeffizient** "n **über** k" wird mit $\binom{n}{k}$ bezeichnet und ist definiert als

$$\binom{n}{k} = \text{ Die Anzahl von Teilmengen der Menge } \{1,\dots,n\}, \text{ die } k \text{ Elemente haben.}$$

Beispiel 2.9. Wenn $n = 4$ und $k = 2$ dann ist $\binom{4}{2} = 6$, weil

$$\big\{A \subseteq \{1,2,3,4\} \;:\; \sharp A = 2\big\} = \big\{\{1,2\},\{1,3\},\{1,4\},\{2,3\},\{2,4\},\{3,4\}\big\}.$$

Satz 2.10. *Für alle $n, k \in \mathbb{N}_{>0}$ gilt*

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Beweis-Skizze: Es sei $A \subseteq \{1,\dots,n\}$ mit $\sharp A = k$. Dann gilt entweder $n \notin A$ oder $n \in A$. Diese sind die zwei Fälle die wir separat betrachten.

Fall 1: $n \notin A$. Dann ist eigentlich A eine Teilmenge von $\{1,\dots,n-1\}$. Per Definition von Binomialkoeffizient, gibt es also $\binom{n-1}{k}$ davon.

Fall 2: $n \in A$. Dann ist $A \setminus \{n\}$ eine Teilmenge von $\{1,\dots,n-1\}$ mit $k-1$ Elementen. Wieder per Definition gibt es $\binom{n-1}{k-1}$ davon.

Wir haben also bewiesen, dass es $\binom{n-1}{k}$ Teilmengen von $\{1,\dots,n\}$ mit Kardinalität k, die n nicht enthalten, gibt und $\binom{n-1}{k-1}$ Teilmengen von $\{1,\dots,n\}$ mit Kardinalität k, die n enthalten, gibt. Also, dass

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Q.E.D.

Definition 2.11. Die **Betragsfunktion** ist die Abbildung $|\cdot| : \mathbb{R} \longrightarrow \mathbb{R}_{\geqslant 0}$ gegeben durch

$$|x| := \begin{cases} x, & \text{wenn } x \geqslant 0, \\ -x, & \text{wenn } x < 0. \end{cases}$$

Satz 2.12 (Dreiecksungleichung)**.** *Es seien $x, y \in \mathbb{R}$. Es gilt $|x+y| \leqslant |x| + |y|$.*

Beweis-Skizze: **Fall 1:** $x, y \geqslant 0$ Dann gilt auch $x + y \geqslant 0$, also

$$|x+y| = x + y = |x| + |y|.$$

Fall 2: $x, y < 0$ Dann gilt auch $x + y < 0$, also

$$|x+y| = -(x+y) = -x + (-y) = |x| + |y|.$$

Fall 3: $x \geqslant 0$ und $y < 0$

Teilfall 3.1: $x + y \geqslant 0$. Wir haben $y < 0 < -y$, also:

$$|x+y| = x + y \leqslant x + (-y) = |x| + |y|.$$

Teilfall 3.2: $x + y < 0$. Wir haben $-x \leqslant 0 \leqslant x$, weil $x \geqslant 0$. Also:

$$|x + y| = -(x + y) = -x + (-y) \leqslant x + (-y) = |x| + |y|.$$

Fall 4: $x < 0$ und $y \geqslant 0$ Diese Bedingung wir aus der Bedingung in Fall 3 durch vertauschen von x und y erhalten. Weil die Aussage die wir zeigen wollen symmetrisch in x und y ist, ist Fall 4 äquivalent zu Fall 3. Q.E.D.

Eine **symmetrische Aussage** in x und y ist eine Aussage die unverändert bleibt wenn x und y vertauscht werden. In dem obigen Satz war das so, weil

$$|x + y| \leqslant |x| + |y| \quad \Longleftrightarrow \quad |y + x| \leqslant |y| + |x|.$$

Die Symmetrie der Aussage folgt also aus der Kommutativität der Addition.

2.2.4 Beweis durch Kontraposition

Wir wiederholen kurz die Definition von Kontraposition einer Implikation und dessen wichtigste Eigenschaft.

Definition 2.13. Die **Kontraposition** der Implikation "$A \Rightarrow B$" ist die Implikation "$\neg B \Rightarrow \neg A$".

Bemerkung 2.14. Eine Implikation ist zu ihrer Kontraposition logisch äquivalent.

Beweis-Skizze:

A	B	$\neg A$	$\neg B$	$A \Rightarrow B$	$\neg B \Rightarrow \neg A$
w	w	f	f	w	w
w	f	f	w	f	f
f	w	w	f	w	w
f	f	w	w	w	w

Q.E.D.

Beispiel 2.15. Die Implikation $x^2 - 9 = 0 \Rightarrow x = 3$ hat die Kontraposition $x \neq 3 \Rightarrow x^2 - 9 \neq 0$.

Lemma 2.16. *Es sei $x \in \mathbb{Z}$. Wenn x^2 gerade ist, dann ist auch x gerade.*

Beweis-Skizze: Es ist deutlich einfacher das durch Kontraposition zu beweisen. Weil die Negation von "ist gerade" "ist ungerade" ist, ist die Kontraposition unserer Implikation

Wenn $x \in \mathbb{Z}$ ungerade ist, dann ist auch x^2 ungerade.

Der Beweis ist dann identisch zu dem Beweis von Lemma 2.4: Wenn $x \in \mathbb{Z}$ ungerade ist, dann existiert $k \in \mathbb{Z}$ sodass $x = 2k + 1$. Daraus folgt

$$x^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

also auch x^2 ist ungerade. Q.E.D.

Beispiel 2.17. Es seien A, B, C, D Mengen, sodass $C \setminus D \subseteq A \cap B$, und sei $x \in C$. Man zeige, dass

$$x \notin A \Rightarrow x \in D.$$

Beweis-Skizze: Wir zeigen, dass $x \notin D \Rightarrow x \in A$:
Aus $x \in C$ und $x \notin D$ haben wir per Definition $x \in C \setminus D$.
Aus $C \setminus D \subseteq A \cap B$ folgt $x \in A \cap B$. Daraus folgt aus der Definition von $A \cap B$, dass $x \in A$.
Q.E.D.

[9] 13.11.'24

2.2.5 Vollständige Induktion

Die Folge $1, 2, 3, 4, \ldots$ ist das einfachste Beispiel von Unendlichkeit in der Mathematik. Im Vergleich zu anderen natürlichen unendlichen Mengen (die Menge $\mathbb{Q}$ der rationalen Zahlen, die Menge aller Punkte einer Gerade in der euklidischen Ebene $\mathbb{R}^2$, die Menge aller Dreiecken in der Ebene) diese Menge hat zwei Vorteile: wir wissen genau wo es anfängt (bei 1) und, wenn wir bis n angekommen sind, wissen wir genau welche die "nächste" Zahl ist: $n+1$. Dieser Schritt von n nach $n+1$ ist die Basis einer der fundamentalen Formen von mathematischem Denken: Das Prinzip der Vollständigen Induktion.

Wir fangen mit einem Satz an, der die Methode der vollständigen Induktion als richtig bestätigt.

Satz 2.18. *Es sei $(A(n))_{n\in\mathbb{N}}$ eine Familie von Aussagen die nach der Menge der natürlichen Zahlen indiziert ist. Wenn*

(IA) *$A(0)$ wahr ist, und*

(IS) *$A(k) \Rightarrow A(k+1)$ wahr für alle $k \in \mathbb{N}$ ist,*

dann ist $A(n)$ wahr für alle $n \in \mathbb{N}$.

Beweis-Skizze: Wir führen einen Widerspruchsbeweis. Nehmen wir an, dass nicht alle $A(n)$ wahr sind. Das heißt, es existiert eine kleinste natürliche Zahl n_0, für welche $A(n_0)$ falsch ist. Aus (IA) haben wir, dass $n_0 > 0$. Das heißt, dass $n_0 - 1 \in \mathbb{N}$. Aus der Minimalität von n_0 folgt dann, dass $A(n_0 - 1)$ wahr ist. Aus (IS) folgt aber, dass auch $A(n_0)$ wahr ist. Wir haben somit ein Widerspruch bekommen: $A(n_0)$ ist falsch und $A(n_0)$ ist wahr. Unsere Annahme, dass $A(n)$ nicht für alle $n \in \mathbb{N}$ wahr ist, muss also falsch gewesen sein. Q.E.D.

Die Bedingung (IA) heißt **Induktionsanfang**. Die Bedingung (IS) heißt **Induktionsschritt** oder Induktionsschluss. Die Annahme, dass $A(k)$ wahr ist heißt Induktionsannahme oder **induktive Voraussetzung** (IV).

Der Satz 2.18 gilt auch wenn der Induktionsanfang bei $A(1)$ ist. Man muss in dem Beweis nur $\mathbb{N}$ mit $\mathbb{N}_{>0}$, also *natürliche Zahl* mit *positive natürliche Zahl*, ersetzen.

Satz 2.19 (Kleiner Gauß)**.** *Für alle $n \in \mathbb{N}$ gilt*

$$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Beweis-Skizze:
1. Vollständige Induktion:

(IA): $k = 0$ $\sum_{i=0}^{0} 0 = 0 = \frac{0 \cdot 1}{2}$.

(IS): $k \Rightarrow k+1$ Wir nehmen also an

$$\text{(IV):} \qquad \sum_{i=0}^{k} i = \frac{k(k+1)}{2}.$$

Wir berechnen

$$\begin{aligned}
\sum_{i=0}^{k+1} i &= \left(\sum_{i=0}^{k} i\right) + k + 1 && \text{aus der Assoziativität der Addition} \\
&= \frac{k(k+1)}{2} + k + 1 && \text{aus der (IV)} \\
&= (k+1) \cdot \left(\frac{k}{2} + 1\right) && \text{aus der Distributivität der Multiplikation bezüglich der Addition} \\
&= (k+1) \cdot \frac{k+2}{2} \\
&= \frac{(k+1)(k+2)}{2} \\
&= \frac{(k+1)\big((k+1)+1\big)}{2}.
\end{aligned}$$

2. Direkter Beweis:
Sei $n \in \mathbb{N}$. Wir bezeichnen mit $N = \sum_{i=0}^{n} i$. Also N ist eine natürliche Zahl. Aus der Kommutativität der Addition gilt

$$\begin{array}{rcccccccccc}
N &=& 0 &+& 1 &+& 2 &+& \dots &+& n \\
N &=& n &+& n-1 &+& n-2 &+& \dots &+& 0 \qquad + \\
\hline
2N &=& n &+& n &+& n &+& \dots &+& n
\end{array}$$

Wir haben insgesamt $n+1$ Summanden, also $2N = (n+1)n$ und somit $N = \frac{n(n+1)}{2}$. Q.E.D.

Komische Sachen können passieren wenn wir ein ähnliches Verfahren für unendliche Summen anwenden. Zum Beispiel, wenn

$$A = 1 - 1 + 1 - 1 + 1 - 1 + \dots$$

Dann haben wir

$$1 - A = 1 - (1 - 1 + 1 - 1 + \dots) = 1 - 1 + 1 - 1 + \cdots = A$$

Also $1 - A = A$ und somit $1 = 2A$, also $A = \frac{1}{2}$. Das heißt

$$1 + 1 - 1 + 1 - 1 + 1 - 1 + \cdots = \frac{1}{2}.$$

Es wird besser aber! Wenn $B = 1 - 2 + 3 - 4 + 5 - 6 + \dots$ dann berechnen wir

$$\begin{aligned} A - B &= (1 - 1 + 1 - 1 + \dots) - (1 - 2 + 3 - 4 + \dots) \\ &= (1 - 1) + (-1 + 2) + (1 - 3) + (-1 + 4) + \dots \\ &= 0 + 1 + (-2) + 3 + (-4) + \dots \\ &= B. \end{aligned}$$

Also $A - B = B$, und somit $2B = A$. Aber wir wissen schon, dass $A = \frac{1}{2}$, also ist $B = \frac{1}{4}$. Das heißt

$$1 - 2 + 3 - 4 + 5 - 6 + \dots = \frac{1}{4}.$$

Jetzt kommt das beste: Wir setzten $C = 1 + 2 + 3 + 4 + 5 + \dots$ und berechnen

$$\begin{aligned} B - C &= (1 - 2 + 3 - 4 + \dots) - (1 + 2 + 3 + 4 + \dots) \\ &= (1 - 1) + (-2 + -2) + (3 + -3) + (-4 + -4) + \dots \\ &= 0 + (-4) + 0 + (-8) + 0 + (-12) + \dots \\ &= -4 \cdot C. \end{aligned}$$

Wir haben also $B = -3C$, oder $C = -\frac{1}{3}B = -\frac{1}{3} \cdot \frac{1}{4} = -\frac{1}{12}$. Das heißt,

$$1 + 2 + 3 + 4 + 5 + \dots = -\frac{1}{12}.$$

Diese Berechnung ist als Ramanujansumme[3] bekannt. Obwohl es in dieser naiver Form absurd scheint, hat diese Anordnung von Werten für divergente Summen viele Anwendungen in der Zahlentheorie und in der Physik.

Beispiel 2.20. Für jede positive natürliche Zahl n kann ein $2^n \times 2^n$ Quadratnetz (oder Quadratgitter) in dem ein beliebiges Quadrat entfernt wurde mit L-förmige Kacheln, bestehend aus 3 Quadrate, gekachelt werden.

Beispiel 2.21. In der Kombinatorik gibt es ein "offensichtliches" Prinzip: das Schubfachprinzip[4]:

Werden n Objekte in r Fächer gegeben, wobei $r < n$ ist, dann enthält mindestens einder der Fächer mehr als eines der Objekte.

Das kann man in der Sprache der Abbildungen umformulieren:

Es seien N und R endliche Mengen. Wenn $f : N \longrightarrow R$ eine Abbildung ist, wobei $|R| < |N|$, dann ist f nicht injektiv.

Wir haben also eine Implikation, und diese ist zu ihrer Kontraposition äquivalent:

Es seien N und R endliche Mengen. Wenn $f : N \longrightarrow R$ eine injektive Abbildung ist, dann gilt $|R| \geqslant |N|$.

Diese letzte Aussage, die äquivalent zum Schubfachprinzip ist, beweisen wir durch Induktion über $n := |N|$.

Beweis: Wenn $n = 0$, dann ist die Aussage $|R| \geqslant 0$ wahr.

[3] Nach Srinivasa Ramanujan benannt.

[4] Auf Englisch hat es einen etwas lustigeren Namen: *Pigeon hole principle.*

Wir nehmen an, die Aussage sei wahr für $|N| = n-1$ für ein $n \geqslant 1$. Sei jetzt N eine endliche Menge mit $|N| = n$. Also $N \neq \emptyset$ und somit existiert $a \in N$. Weil f injektiv ist, folgt es, dass $f(a') \neq f(a)$ für alle $a' \in N \setminus \{a\}$. Wir können also die Abbildung $f' : N \setminus \{a\} \longrightarrow R \setminus \{f(a)\}$ definieren. Diese ist selber injektiv und, weil $|N \setminus \{a\}| = n-1$, folgt aus der Induktiven Voraussetzung, dass

$$|R \setminus \{f(a)\}| \geqslant |N \setminus \{a\}|.$$

Also $r - 1 \geqslant n - 1$, und somit auch $r \geqslant n$. □

Bemerkung 2.22. Es gibt "raffiniertere" Induktionsvarianten[5]:

(a) **Verspätete Induktion:** Man verwendet einen anderen Induktionsanfang als $A(0)$, nämlich $A(n_0)$ für ein $n_0 \in \mathbb{N}$. Zum Beispiel $A(1), A(5)$ oder $A(37)$. Dann gilt $A(n)$ ist wahr für alle $n \geqslant n_0$.

(b) **Verstärkte Induktion:** Wir ändern den Induktionsschritt von $A(k) \Rightarrow A(k+1)$ auf

$$A(k-1) \text{ und } A(k) \Rightarrow A(k+1).$$

In diesem Fall muss man auch den Induktionsanfang auf "$A(0)$ und $A(1)$ sind wahr" anpassen.

(c) **Starke Induktion:** Wir ändern den Induktionsschritt von $A(k) \Rightarrow A(k+1)$ auf

Wenn $A(j)$ für alle $j = 0, \ldots, k$ wahr ist, dann folgt $A(k+1)$.

In diesem Fall muss man den Induktionsanfang nicht anpassen.

Verspätete Induktion

Hier ist eine Beispiel für die erste Variation der Induktion.

Beispiel 2.23. Man finde $n_0 \in \mathbb{N}$, sodass

$$\frac{n^2}{2} - 4 > \frac{n^2}{4}$$

für alle $n \geqslant n_0$.

Beweis-Skizze: Man kann anfangen, indem man sich die Aussage für kleine Werte anschaut:

$n = 0:$	$-4 > 0$	falsch
$n = 1:$	$-7/2 > 1/4$	falsch
$n = 2:$	$-2 > 1$	falsch
$n = 3:$	$2/4 > 9/4$	falsch
$n = 4:$	$4 > 4$	falsch
$n = 5:$	$34/4 > 25/4$	wahr

Wir vermuten dann, dass $n_0 = 5$ und beweisen es durch verspätete Induktion.

(IA) Der Induktionsanfang $5^2/2 - 4 > 5^2/4$ wurde schon gezeigt.

[5] Nur die letzte Bezeichnung ist verbreitet. Die anderen zwei kommen selten in der Literatur vor.

(IS) Sei $k \in \mathbb{N}$ mit $k \geqslant 5$. Wir nehmen an

$$\text{(IV)} \quad \frac{k^2}{2} - 4 > \frac{k^2}{4}.$$

Wir schauen uns jetzt $\frac{(k+1)^2}{2} - 4$ an:

$$\begin{aligned}
\frac{(k+1)^2}{2} - 4 &= \frac{k^2+2k+1}{2} - 4 \\
&= \frac{k^2}{2} - 4 + \frac{2k+1}{2} \qquad \text{(aus der (IV))} \\
&> \frac{k^2}{4} + \frac{4k+2}{4} \\
&= \frac{k^2+2k+1}{4} + \frac{2k+1}{4} \qquad \text{weil } k \geqslant 4 > 0 \\
&> \frac{(k+1)^2}{4}.
\end{aligned}$$

Somit ist die Aussage

$$\frac{n^2}{2} - 4 > \frac{n^2}{4} \quad \forall\, n \geqslant 5$$

bewiesen.

2. Direkter Beweis: Wir hätten in dieser Situation auch anders anfangen können, nämlich indem wir die Ungleichung bearbeiten.

$$\frac{n^2}{2} - 4 > \frac{n^2}{4} \iff \frac{n^2}{4} - 4 > 0 \iff \frac{n^2-16}{4} > 0 \iff n^2 - 16 > 0.$$

Wir müssen also das Vorzeichen von $n^2 - 16$ betrachten, und das ist einfach:

$$n^2 - 16 = (n-4)(n+4)$$

Also

$$n^2 - 16 \begin{cases} > 0 & \text{wenn } n < -4 \text{ oder } n > 4 \\ = 0 & \text{wenn } n = -4 \text{ oder } n = 4 \\ < 0 & \text{wenn } -4 < n < 4 \end{cases}.$$

Q.E.D.

Eine interessantere Anwendung dieser Variante der Induktion ist folgende: Man finde $n_0 \in \mathbb{N}$, sodass

$$2^n > n^2 \quad \forall\, n \in \mathbb{N} \text{ mit } n \geqslant n_0.$$

Verstärkte Induktion

Beispiel 2.24. Es seien $x_0 = 2$ und $x_1 = 3$ und für $n \geqslant 2$ sei

$$x_n = 3x_{n-1} - 2x_{n-2}$$

Man zeige, dass $x_n = 2^n + 1$ für alle $n \in \mathbb{N}$.

Beweis-Skizze: Wir beweisen die Aussage durch verstärkte Induktion. Wir werden also den Induktsionsschritt $[A(k-1)\,\text{und}\,A(k) \Rightarrow A(k+1)]$ verwenden, deswegen haben wir zwei Fälle als Induktionsanfang.

(IA)

$$\begin{aligned} n = 0: &\qquad 2^n + 1 = 2^0 + 1 = 1 + 1 = 2 = x_0, \\ n = 1: &\qquad 2^n + 1 = 2^1 + 1 = 2 + 1 = 3 = x_1. \end{aligned}$$

(IS) Wir nehmen an, dass

$$x_{k-1} = 2^{k-1} + 1 \qquad \text{und} \qquad x_k = 2^k + 1.$$

Wir haben dann

$$\begin{aligned} x_{k+1} &= 3x_k - 2x_{k-1} \qquad \text{(aus der (IV))} \\ &= 3(2^k + 1) - 2(2^{k-1} + 1) \\ &= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2 \\ &= 3 \cdot 2^k - 2^k + 3 - 2 \\ &= (3-1) \cdot 2^k + 1 \\ &= 2^{k+1} + 1. \end{aligned}$$

Q.E.D.

Man betrachte die **Fibonacci Zahlen**[6]

$$\begin{aligned} F_0 &= 0, \\ F_1 &= 1, \\ F_n &= F_{n-2} + F_{n-1} \quad \forall\, n \geqslant 2. \end{aligned}$$

Satz 2.25. *Für jedes $n \in \mathbb{N}$ gilt*

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

Beweis-Skizze: Übung Q.E.D.

[10] 15.11.'24

Starke Induktion

Satz 2.26 (Wohlordnungsprinzip)**.** *Jede nicht leere Teilmenge von $\mathbb{N}$ enthält ein kleinstes Element.*

Das heißt

$$\forall\, \emptyset \neq S \subseteq \mathbb{N}, \quad \exists\, n_0 \in S, \quad \text{sodass } n_0 \leqslant n \quad \forall\, n \in S.$$

[6] Nach Leonardo Fibonacci (1170-1240) benannt.

Beweis-Skizze: Wir werden den Satz durch eine Mischung von Kontraposition und starke Induktion beweisen. Unser Ziel ist folgende Implikation für alle $S \subseteq \mathbb{N}$ zu zeigen:

$$S \neq \emptyset \Rightarrow S \text{ hat ein kleinstes Element.}$$

Nach Definition **??** und Bemerkung 1.9 ist diese Implikation zur folgenden Implikation logisch äquivalent:

$$S \text{ hat kein kleinstes Element } \Rightarrow S = \emptyset.$$

Um diese Implikation zu beweisen, verwenden wir folgende Charakterisierung der leeren Teilmenge von $\mathbb{N}$:

$$\text{für } S \subseteq \mathbb{N} \text{ gilt } S = \emptyset \iff n \notin S \ \ \forall n \in \mathbb{N}.$$

Sei also $S \subseteq \mathbb{N}$ das kein kleinstes Element enthält. Wir werden durch starke Induktion beweisen, dass $n \notin S$, für alle $n \in \mathbb{N}$.

(IA) $n = 0$. Wenn $0 \in S$, dann ist 0 das kleinste Element in S, weil $0 \leqslant n$ für alle $n \in \mathbb{N}$.

(IS) Sei $k \in \mathbb{N}$. Wir nehmen an

$$\text{(IV)} \quad i \notin S \ \ \forall i = 0, \ldots, k.$$

Wir wollen zeigen, dass $k + 1 \notin S$. Das machen wir durch ein Widerspruchbeweis:
Nehmen wir an, dass $k + 1 \in S$. Aus (IV) haben wir, dass

$$\text{Wenn } i \in S, \text{ dann } i \geqslant k + 1.$$

Also $k + 1$ das kleinste Element aus S. Ein Widerspruch, weil S kein kleinstes Element enthält. Q.E.D.

Folgende Sätze können auch durch starke Induktion bewiesen werden:

Satz 2.27 (Divison mit Rest)**.** *Für alle natürlichen Zahlen n und m, mit $m > 0$, existieren $q, r \in \mathbb{N}$ mit $r < m$, sodass*

$$n = qm + r.$$

Beweis-Skizze: Übung Q.E.D.

Satz 2.28. *Jede natürliche Zahl ist ein Produkt von Primzahlen*[7]*.*

Beweis-Skizze: Übung Q.E.D.

2.2.6 Falsche Beweise und häufige Fehler

Hier sind einige Tipps um Fehler in Beweise zu finden. Diese Liste ist aber weit von vollständig.

- Die Aussagen im Beweis erkennen. Oft sind diese Implikationen.

[7] Wir betrachten eine Primzahl als ein Produkt von Primzahlen mit einem einzigen Faktor.

- Die Wahrheit der Implikationen überprüfen. Wenn es Implikationen sind, dann muss man nicht den Wahrheitswert der Komponenten überprüfen, sondern der Implikation. Das ist besonders wichtig bei Beweisen durch Widerspruch. Zum Beispiel

  $$\text{Wenn } 1 = 2, \text{ dann } 2 = 3$$

  ist eine wahre Implikation.

- Die Richtigkeit einer Aussage oder einer Formel kann man an extremen oder an einfachen Beispielen testen[8]. Für die folgende Summe kann man schnell sehen, dass

  $$\sum_{i=1}^{n} i^2 = \frac{n(n-1)(2n-1)}{6}$$

  nicht für alle n stimmen kann: Für $n = 1$ bekommt man $1 = 0$. Was bekommt man für $n = 2$? $n = 3$?

- Man soll die Aussagen mit bewiesenen Sätze vergleichen.

Unter den häufigen Fehler die man in einem Beweis machen kann sind:

- Das was zu beweisen ist als Voraussetzung anzunehmen. Wenn man also zeigen muss, dass $V \Rightarrow S$, reicht es nicht S ist wahr anzunehmen, und dann eine Wahre Aussage herzuleiten. Hier ist ein Beispiel eines solches Fehlers:

  Man zeige, dass $a^2 + b^2 \geqslant 2ab$ *für alle* $a, b \in R$.
  Falscher Beweis: Wir haben

  $$a^2 + b^2 \geqslant 2ab \Rightarrow a^2 + b^2 - 2ab \geqslant 0 \Rightarrow (a-b)^2 \geqslant 0. \tag{2.1}$$

  Weil das Quadrat einer reellen Zahl immer nicht-negativ ist, muss auch $a^2 + b^2 \geqslant 2ab$ gelten. Q.E.D.

  Der logische Fehler: Wenn $A \Rightarrow B$ wahr ist, und B wahr ist, dann muss A nicht unbedingt wahr sein.

  Hier ist noch ein Beispiel:

  $$0 < -1 < -2 \Rightarrow (-1)^2 < (-2)^2 \Rightarrow 1 < 4$$

  also auch $-1 < -2$. Die Implikation und die Schlussfolgerung sind richtig, aber $-1 < -2$ falsch.

- Obwohl die Implikationskette (2.2) ein falscher Beweis ist, zeigt uns diese Kette wie man den richtigen Beweis finden kann. In diesem Fall sind eigentlich alle Implikationen sogar Äquivalenzen, also kann man folgenden Beweis finden:

  Man zeige, dass $a^2 + b^2 \geqslant 2ab$ *für alle* $a, b \in R$.

[8] Testen ist aber nicht dasselbe wie beweisen! Man kann aber dadurch Fehler entdecken und Formeln anpassen.

Richtiger Beweis: Für alle reelle Zahlen $x \in \mathbb{R}$ gilt $x^2 \geqslant 0$. Insbesondere, für alle $a, b \in \mathbb{R}$ gilt dann $(a-b)^2 \geqslant 0$. Wir haben dann:

$$(a-b)^2 \geqslant 0 \Rightarrow a^2 - 2ab + b^2 \geqslant 0 \Rightarrow a^2 + b^2 \geqslant 2ab. \tag{2.2}$$

Q.E.D.

- Die Wurzel ist eine Abbildung $\sqrt{\cdot} : \mathbb{R} \longrightarrow \mathbb{R}$, also nimmt diese einen einzigen Wert:

  Falsch: $\sqrt{4} = \pm 2$.
  Richtig: $\sqrt{4} = 2$.

  Was gilt ist, dass die Lösungen der Gleichung $x^2 - 4 = 0$ zwei sind:

  $$x_{1,2} = \pm\sqrt{4} = \pm 2.$$

- Nicht alles was durch Wurzeln ausgedrückt ist, ist irrational:

  $$\sqrt{7+\sqrt{24}} - \sqrt{7-\sqrt{24}} = 2$$

Beweis-Skizze: Sei wir bezeichnen $\alpha = \sqrt{7+\sqrt{24}} - \sqrt{7-\sqrt{24}}$. Weil $7+\sqrt{24} > 7-\sqrt{24}$, gilt das auch für die Wurzeln, und somit ist $\alpha > 0$. Das bedeutet $\alpha = \sqrt{\alpha^2}$. Wir berechnen dann α^2:

$$\begin{aligned}
\alpha^2 &= \left(\sqrt{7+\sqrt{24}} - \sqrt{7-\sqrt{24}}\right)^2 \\
&= 7 + \sqrt{24} - 2 \cdot \sqrt{(7+\sqrt{24})(7-\sqrt{24})} + 7 - \sqrt{24} \\
&= 14 - 2 \cdot \sqrt{49-24} \\
&= 14 - 2 \cdot 5 \\
&= 4.
\end{aligned}$$

Also $\alpha = \sqrt{4} = 2$. Q.E.D.

- $a + b = c \not\Rightarrow a^2 + b^2 = c^2$.

- Man muss vorsichtig mit Implikationen und Äquivalenzen umgehen. Insbesondere, wenn diese nicht so offensichtlich dabei sind, wie beim Lösen von Gleichungen. Zum Beispiel:

  Man finde alle $x \in \mathbb{R}$ *mit* $\sqrt{x+3} = x + 1$.
  Falsche Lösung: Wir quadrieren beide Seiten:

$$\begin{aligned}
\sqrt{x+3} &= x+1 \\
x+3 &= (x+1)^2 \\
x+3 &= x^2 + 2x + 1 \\
0 &= x^2 + x - 2 \\
0 &= (x-1)(x+2)
\end{aligned}$$

Also $x = 1$ und $x = -2$ sind die Lösungen. Q.E.D.

Wenn wir aber die Probe machen:

$$\sqrt{1+3} = 1 + 1 \qquad \text{aber} \qquad \sqrt{-2+3} \neq -2 + 1.$$

Das Problem ist, dass nicht alle Gleichungen in der obigen Kette äquivalent sind:

$$\sqrt{x+3} = x + 1 \quad \not\Longleftrightarrow \quad x + 3 = (x+1)^2.$$

Alle anderen sind äquivalent. Der Fehler hier ist, dass wenn wir $f^2 = g^2$ lösen, dann finden wir nicht nur die Lösung $f = g$, sonder auch $f = -g$.

- Wenn man durch Null teilt dann bricht die Welt zusammen. Alles wird Null. Hier ist ein Beispiel wie das passieren kann:

  Es seien $a, b \in \mathbb{R}$ mit $a = b$. Dann, wenn wir beide Seiten der Gleichheit mit a multiplizieren, bekommen wir

  $$a^2 = ab.$$

  Wir können dann von beiden Seiten b^2 abziehen:

  $$a^2 - b^2 = ab - b^2.$$

  Dann haben wir also $(a-b)(a+b) = (a-b)b$. Wir können also kürzen, und bekommen $a+b = b$. Aber $b = a$, also

  $$2b = b$$

  und somit $2 = 1$. Wir ziehen dann 1 von beiden Seiten ab, und somit haben wir bewiesen, dass

  $$1 = 0.$$

- Minus kann zu etwas positives führen. Das heißt, $-x$ ist nicht immer negativ! Zum Beispiel wenn $x = -3$, dann ist $-x = 3 > 0$.

- Aber nicht alle Zahlen sind positiv. Insbesondere wenn man Ungleichungen umstellt, muss man darauf achten:

  $$\frac{1}{x} < 2 \quad \not\Longleftrightarrow \quad \frac{1}{2} < x$$

  Zum Beispiel -1 erfüllt $\frac{1}{-1} < 2$ aber $\frac{1}{2} < -1$ nicht. Der Fehler lag, dass von der ersten Ungleichung zu der zweiten haben wir mit beide Seiten mit x multipliziert, und durch 2 geteilt. Wenn aber $x < 0$ ist, dann ändert sich auch die Richtung der Ungleichung. Richtig wäre also

  $$\frac{1}{x} < 2 \quad \Leftrightarrow \begin{cases} \frac{1}{2} < x & \text{wenn } x > 0 \\ \frac{1}{2} > x & \text{wenn } x < 0 \end{cases}.$$

2.2.7 Wie beweise ich das?

Es gilt für alle

Es gibt kein allgemeines Rezept für Aussagen der Form:

$P(x)$ *ist wahr* $\forall\, x \in A$.

Hier sind einige Möglichkeiten:

- Man fängt mit "Es sei $x \in A$ beliebig." an, und führt einen direkten Beweis durch.
- Man nimmt an, dass $\exists\ x \in A$, sodass $\neg P(x)$, und sucht einen Widerspruch.
- Wenn $A = \mathbb{N}$, dann kann man vollständige Induktion anwenden.
- Wenn $A = \mathbb{Z}$, dann kann man zwei Mal vollständige Induktion anwenden: für $P(x)$ mit $x \in \mathbb{N}$ und für $P(-x)$ mit $x \in \mathbb{N}$.

Existenz

Wie zeigt man, dass etwas (mit einer gegebenen Eigenschaft) existiert?

- Man konstruiert es direkt.
- Man nimmt an, es existiert nicht und findet einen Widerspruch.

Nicht-Existenz

Wie zeigt man, dass etwas (mit einer gegebenen Eigenschaft) **nicht** existiert?

- Man nimmt an, es existiert und findet einen Widerspruch.

Implikation: $A \Rightarrow B$

- Direkter Beweis: $A \Rightarrow A_1 \Rightarrow \ldots \Rightarrow B$.
- Kontraposition: Man zeigt $\neg B \Rightarrow \neg A$.
- Widerspruchsbeweis: Man zeigt, dass

  $$\neg(A \Rightarrow B) \text{ das äquivalent zu } [A \text{ und } \neg B] \text{ ist,}$$

  falsch ist, indem man daraus ein Widerspruch herleitet.

Äquivalenz: $A \Leftrightarrow B$

- Man zeigt $A \Rightarrow B$ und $B \Rightarrow A$. Oft separat.

Gleichheit von Zahlen: $a = b$

- Man zeigt $a \leqslant b$ und $b \leqslant a$.
- Man zeigt $a - b = 0$.

Gleichheit von Abbildungen: $f = g$

Man muss erstmals sicher sein, dass beide Abbildungen dieselben Definitions- und Wertebereiche haben:

$$f = g \text{ kann nur gelten, wenn } f, g : M \longrightarrow N.$$

Dann zeigt man

$$f(x) = g(x) \quad \forall\, x \in M.$$

Gleichheit von Mengen: $M = N$

Es gilt

$$M = N \qquad \Longleftrightarrow \qquad M \subseteq N \text{ und } N \subseteq M.$$

Oft müssen die Inklusionen separat bewiesen werden.

Für Mengeninklusionen $M \subseteq N$ muss man zeigen, dass

$$\forall\, x \in M \quad \Rightarrow x \in N.$$

Eindeutigkeit

Wenn man eine Aussage der Form:

Es gibt ein eindeutiges x mit der Eigenschaft E.

zeigen muss, dann muss man so anfangen:

Beweis: Es seien x und y mit der Eigenschaft E.
Dann (*sauber aufgeschriebenes logisches Argument*), also $x = y$. Q.E.D

Unendlichkeit einer Menge

- Man konstruiert eine Bijektion/Surjektion zu einer unendlichen Menge.
  (z.B. zu $\mathbb{N}$ oder $\mathbb{Q}$ oder $\mathbb{R}$.)
- Man nimmt an, es sei endlich und findet einen Widerspruch.
  (z.B. wenn es Zahlen sind, dann gibt es eine größte/eine kleinste Zahl in der Menge).
- Man findet eine injektive aber nicht surjektive Abbildung der Menge in sich selbst.

Injektivität

Um zu zeigen, dass $f : X \longrightarrow Y$ injektiv ist, hat man folgende Möglichkeiten:

- Seien $a, b \in X$ mit $f(a) = f(b)$. Dann ... $a = b$.
- Seien $a, b \in X$ mit $a \neq b$. Dann ... $f(a) \neq f(b)$.
- Es existiert $g : Y \longrightarrow X$, sodass $g \circ f = \mathrm{id}_X$.
- Sei $y \in Y$ beliebig. Dann gilt $|f^{-1}(y)| \leqslant 1$.

Surjektivität

Um zu zeigen, dass $f : X \longrightarrow Y$ surjektiv ist, hat man folgende Möglichkeiten:

- Sei $y \in Y$ beliebig. Dann ... existiert $x \in X$ mit $f(x) = y$.
  Dieses x muss man oft explizit (in Abhängigkeit von y) konstruieren.
- Es existiert $g : Y \longrightarrow X$, sodass $f \circ g = \mathrm{id}_Y$.
- Sei $y \in Y$ beliebig. Dann gilt $|f^{-1}(y)| \geqslant 1$.
  (Das ist aber eigentlich sehr oft nichts anderes als der erste Punkt).

Bijektivität

Um zu zeigen, dass $f : X \longrightarrow Y$ bijektiv ist, hat man folgende Möglichkeiten:

- Man zeigt f ist injektiv und f ist surjektiv separat.
- Falls $|Y| = |X| < \infty$, dann reicht eine der beiden (Inj/Surj.)
- Es existiert eine Inverse $f^{-1} : Y \longrightarrow X$, d.h.

$$f \circ f^{-1} = \mathrm{id}_Y \text{ und } f^{-1} \circ f = \mathrm{id}_X .$$

- Sei $y \in Y$ beliebig. Dann gilt $|f^{-1}(y)| = 1$ (wobei hier $f^{-1}(y)$ die Faser bezeichnet).
- Falls man **nicht-Bijektivität** zeigen muss, es könnte der Fall sein, dass $|X| \neq |Y|$. Das würde reichen.

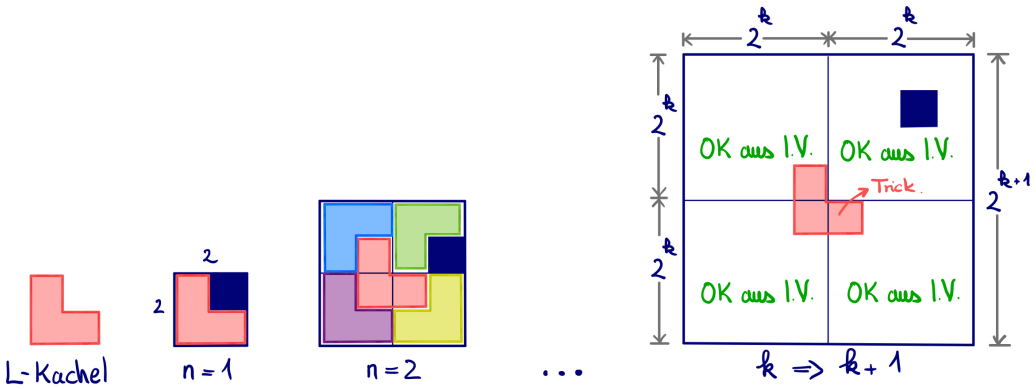


Abbildung 2.1: Kachel-Induktion

Kapitel 3

Elementare Zahlentheorie

In diesem Kapitel wird *Zahl* immer eine ganze Zahl heißen. Die Menge der ganzen Zahlen bezeichnen wir mit $\mathbb{Z}$ und nehmen als bekannt an:

$$\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots.$$

Auf dieser Menge sind zwei[1] Verknüpfungen/algebraische Operationen definiert: Addition ($+$) und Multiplikation ($\cdot$). Wir nehmen diese als bekannt an. Wir erinnern aber die wichtige Eigenschaft:

$$\text{Wenn } a, b \in \mathbb{Z} \text{ und } a \cdot b = 0, \text{ dann } a = 0 \text{ oder } b = 0.$$

Die Betragsfunktion $|\cdot| : \mathbb{Z} \longrightarrow \mathbb{N}$ ist definiert durch

$$z \longmapsto |z| := \begin{cases} z & \text{wenn } z \geqslant 0 \\ -z & \text{wenn } z < 0 \end{cases}.$$

Die Betragsfunktion erfüllt für alle $a, b \in \mathbb{Z}$:

$$|ab| = |a||b| \quad \text{und} \quad |a + b| \leqslant |a| + |b|.$$

3.1 Teilbarkeit in $\mathbb{Z}$

Definition 3.1. Für $a, b \in \mathbb{Z}$ sagen wir, dass a **teilt** b (oder b ist durch a teilbar), und schreiben $a \mid b$ (oder $b \vdots a$) genau dann wenn $\exists c \in \mathbb{Z}$, sodass $b = ac$. Wenn $a \mid b$, dann ist a ein **Teiler** von b, und, b ist ein **Vielfaches**[2] von a.

Bemerkung 3.2. Für alle $a, b, c \in \mathbb{Z}$ gilt:

(i) $a \mid 0$.

(ii) $0 \mid a \Leftrightarrow a = 0$.

[1] Die Division bringt uns meistens außerhalb von $\mathbb{Z}$ (in $\mathbb{Q}$) es ist also nicht eine Operation **auf** $\mathbb{Z}$. Und die Subtraktion ist eine versteckte Addition: $a - b = a + (-b)$.

[2] Hier muss man ein bisschen aufpassen, wenn man über kleinste gemeinsame Vielfachen spricht. Dort werden eigentlich nur nicht-triviale (also $\neq 0$) Vielfachen betrachtet.

(iii) $\pm 1 \,|\, a$ und $\pm a \,|\, a$.

(iv) Wenn $a \,|\, b$, dann gilt $|a| \leqslant |b|$.

(v) $a \,|\, b \Rightarrow a \,|\, b \cdot c$.

(vi) $(a \,|\, b$ und $b \,|\, c) \Rightarrow a \,|\, c$.

(vii) Wenn $a \,|\, b_1$ und $a \,|\, b_2$, dann $a \,|\, (b_1 c_1 + b_2 c_2)$ für alle $c_1, c_2 \in \mathbb{Z}$.

(viii) Wenn $c \neq 0$, dann gilt $a \,|\, b \Leftrightarrow (ac) \,|\, (bc)$.

(ix) $(a \,|\, b \,\text{und}\, b \,|\, a) \Leftrightarrow a = \pm b$.

Wir erinnern, an dem Wohlordnungsprinzip der Natürlichen Zahlen (Satz 2.26). Dieses sagt, dass jede nicht-leere Teilmenge ein minimales Element besitzt. Genauer formuliert:

$$\forall\, M \subseteq \mathbb{N}, \text{ mit } M \neq \emptyset, \exists\, m_0 \in M \text{ sodass } m_0 \leqslant m, \forall\, m \in M.$$

Satz 3.3 (Division mit Rest)**.** *Wenn $a, b \in \mathbb{Z}$ mit $b \neq 0$, dann existieren eindeutige ganze Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = qb + r \qquad \text{und} \qquad 0 \leqslant r < |b|.$$

Beweis-Skizze: Wir betrachten den Fall $b > 0$ zu erst.

Sei $S := \{a - sb \;:\; s \in \mathbb{Z} \,\text{und}\, a - sb \geq 0\} \subseteq \mathbb{N}$. Wir werden die Wohlordnung von $\mathbb{N}$ anwenden um den Rest als das Minimum von S zu definieren. Dafür müssen wir zu erst zeigen, dass diese Menge nicht leer ist.

$\boxed{S \neq \emptyset}$ Wenn $a > 0$, dann $a = a - 0 \cdot b \in S$.

Wenn $a < 0$, dann, weil $b > 0 \Rightarrow 1 - b \leqslant 0$, haben wir $0 \leqslant a(1-b) = (a - ab) \in S$.

Weil $\mathbb{N}$ wohl geordnet ist $\Rightarrow$ hat S ein Minimum. Wir setzen

$$r := a - s_0 b := \min S \quad \text{und} \quad q := s_0.$$

$\boxed{r < b}$ Wenn $r \geq b$, dann ist $r - b \geq 0$. Also $r > r - b = a - s_0 b - b \geq 0$ - ↯ zu $r = \min S$.

$\boxed{\text{Eindeutigkeit}}$ Wenn es andere q' und r' mit $a = q'b + r'$ existieren, dann haben wir

$$(q' - q)b = r - r' \tag{3.1}$$

Wenn $q = q'$, dann haben wir offensichtlich $r = r'$.

Wenn $q \neq q'$, dann können wir ohne die Allgemeinheit zu Beschränken $q' > q$, also $q' - q \geq 1$, annehmen. Also, wenn wir beide Seiten mit b multiplizieren bekommen wir

$$(q' - q)b \geq b > |r - r'| \;\text{↯zu (3.1)}.$$

Die rechte Ungleichung gilt, weil, wenn $0 \leqslant r, r' < b$, dann $|r - r'| < b$.

Sei jetzt $b < 0$. Dann ist $-b > 0$ und aus dem obigen Fall existieren eindeutige $q \in \mathbb{Z}$ und $0 \leqslant r < -b = |b|$, sodass

$$a = q(-b) + r = (-q)b + r,$$

und somit ist auch dieser Fall bewiesen. Q.E.D.

Bemerkung 3.4. Für $a, b \in \mathbb{Z}$ gilt

$$b \,|\, a \iff \text{Der Rest bei der Division von } a \text{ durch } b \text{ ist } 0.$$

3.2 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Wir geben hier etwas allgemeinere Definitionen als die üblichen. Ich finde diese Definitionen haben mehr Vorteile als Nachteile.

- **Vorteil:** Die wichtige Eigenschaft (ggT 2) muss nicht bewiesen werden, diese wird als Axiom angenommen.
- **Nachteil:** Man muss die Existenz beweisen.
- **Vorteil:** Der Beweis der Existenz ist auch ein Beweis für das Lemma von Bézout.
- **Nachteil:** Es ist abstrakt: es bringt weniger Intuition ins Spiel.
- **Vorteil:** Es ist abstrakt: es kann für andere Strukturen übernommen werden; zum Beispiel für Polynome in $\mathbb{R}[x]$.

dass man diese dann einfacher für beliebige Ringe übernehmen kann. Auf $\mathbb{Z}$ folgt allein aus der nächsten Definition die Eindeutigkeit nicht; aber fast.

Definition 3.5. Seien $a, b \in \mathbb{Z}$.

1. Ein **größter gemeinsamer Teiler** von a und b ist eine Zahl $d \in \mathbb{N}$ mit den Eigenschaften:

   (ggT 1) $d \mid a$ und $d \mid b$,
   (ggT 2) Wenn $d' \mid a$ und $d' \mid b$, dann $d' \mid d$.

2. Ein **kleinstes gemeinsames Vielfaches** von a und b ist eine Zahl $m \in \mathbb{N}$ mit den Eigenschaften:

   (kgV 1) $a \mid m$ und $b \mid m$,
   (kgV 2) Wenn $a \mid m'$ und $b \mid m'$, dann $m \mid m'$.

Bemerkung 3.6. Aus Bemerkung 3.2 Punkt (ix) ist gibt es höchstens zwei ggT und zwei kgV. Anders gesagt, Zahlen die (ggT 1) und (ggT 2) erfüllen sind eindeutig bis auf Vorzeichen bestimmt, und das gleiche gilt auch für Zahlen die (kgV 1) und (kgV 2) erfüllen. Wir müssen aber erst zeigen, dass es diese immer gibt.

Satz 3.7. *Für alle $a, b \in \mathbb{Z}$ existiert ein eindeutiger* nicht-negatives *größter gemeinsamer Teiler und ein eindeutiges* nicht-negatives *kleinstes gemeinsames Vielfaches. Diese werden mit* $\mathrm{ggT}(a, b)$*, beziehungsweise* $\mathrm{kgV}(a, b)$ *bezeichnet.*

Beweis-Skizze: Wenn $a = b = 0$, dann gilt $\mathrm{ggT}(a, b) = 0$. Wir nehmen also jetzt an, dass a und b nicht beide Null sind.

ggT. Wir definieren die Menge der positiven $\mathbb{Z}$-linearen Kombinationen von a und b.

$$L_+(a, b) := \{\ell \in \mathbb{N}_{>0} \ : \ \exists\, \lambda, \mu \in \mathbb{Z} \text{ mit } \lambda \cdot a + \mu \cdot b = \ell\}$$

Wenn wir $\lambda = a$ und $\mu = b$ setzen, dann bekommen wir $\ell = a^2 + b^2 > 0$. Also ist $L_+(a, b) \neq \emptyset$.

Weil $L_+(a,b) \subseteq \mathbb{N}$ existiert nach dem Wohlordnungsprinzip ein Minimum in $L_+(a,b)$. Sei dieses:

$$d = \lambda_0 a + \mu_0 b := \min L_+(a,b) \in \mathbb{N}_{>0}, \tag{3.2}$$

mit $\lambda_0, \mu_0 \in \mathbb{Z}$.

(ggT 1) Wir zeigen zu erst, dass $d \mid a$. Aus der Division mit Rest existieren $q, r \in \mathbb{Z}$ mit $0 \leqslant r < d$, sodass $a = dq + r$. Wenn wir also (3.2) einsetzen, dann bekommen wir

$$a = (\lambda_0 a + \mu_0 b)q + r.$$

Wenn $0 < r < d$, dann haben wir

$$0 < r = (1 - \lambda_0)q \cdot a + (-\mu_0 q) \cdot b \in \ S \text{ und } r < d = \min S.$$

Das ist ein Widerspruch zur Minimalität, also $r = 0$. Das heißt aber, dass $d \mid a$.
Dass $d \mid b$, folgt völlig analog.

(ggT 2) Sei d' ein gemeinsamer Teiler. Dann existieren $a', b' \in \mathbb{Z}$ mit $a = d'a', b = d'b'$. Also

$$d = \lambda_0 d'a' + \mu_0 d'b' = d'(\lambda_0 a' + \mu_0 b') \Rightarrow d' \mid d_0.$$

Das zeigt die Existenz eines positives ggT.

Die Eindeutigkeit folgt jetzt aus der Bemerkung 3.6.

kgV. Wenn $a = 0$ oder $b = 0$, dann ist Null das einzige gemeinsame Vielfache, und somit ist 0 ein kgV.
Wir nehmen jetzt an, dass $a \neq 0 \neq b$ und definieren

$$m_0 = \min\{m \in \mathbb{N}_{>0} \ : \ a \mid m \text{ und } b \mid m\},$$

und zeigen, dass es ein kgV ist.

(kgV 1) Das gilt per Definition.

(kgV 2) Sei m ein anderes gemeinsames Vielfaches. Aus der Division mit Rest existieren $q, r \in \mathbb{Z}$ mit $0 \leqslant r < m_0$, sodass

$$m = qm_0 + r.$$

Wenn $r \neq 0$, dann ist $r = m - qm_0 \in \mathbb{N}_{>0}$ ein gemeinsames Vielfaches von a und b (weil m und m_0 es sind), das kleiner als m_0 ist – ein Widerspruch zu der Definition von m_0. Also $r = 0$, und somit $m_0 \mid m$ für alle gemeinsame Vielfachen von a und b.

Die Eindeutigkeit folgt, wie beim ggT, aus der Bemerkung 3.6. Q.E.D.

Für zwei ganze Zahlen a, b, wenn wir **den** ggT oder **das** kgV erwähnen, dann meinen wir immer die nicht-negativen Zahlen aus Satz 3.7.

Bemerkung 3.8. Für alle $a, b \in \mathbb{Z}$ gilt

1. $\text{ggT}(0,0) = 0$

2. $\mathrm{kgV}(0,a) = 0$,
3. $\mathrm{ggT}(0,a) = a$
4. Wenn $a \mid b$, dann $\mathrm{ggT}(a,b) = |a|$ und $\mathrm{kgV}(a,b) = |b|$.

Wir bezeichnen die Menge aller gemeinsamer Teiler von $a, b \in \mathbb{Z}$ mit

$$T_{a,b} := \{k \in \mathbb{Z} \ : \ k \mid a \text{ und } k \mid b\}.$$

Wir haben immer $1 \in T_{a,b}$, also $T_{a,b} \neq \emptyset$. Wenn $a = b = 0$, dann ist $T_{0,0} = \mathbb{Z}$. Aber sonst ist es immer eine endliche Menge (weil $d \mid a \Rightarrow |d| \leqslant |a|$) und es gilt

$$\mathrm{ggT}(a,b) = \max T_{a,b}.$$

Wir hätten den ggT auch so definieren können. Zu zeigen aber, dass alle andere gemeinsame Teiler dadurch selbst teilbar sind, wäre nicht einfach gewesen. Eigentlich hätte man auch die lineare Kombination Darstellung anwenden müssen. Diese Darstellung ist sehr wichtig, und hat einen Eigenen Namen:

Lemma 3.9 (Lemma von Bézout)**.** *Seien $a, b \in \mathbb{Z}$. Es existieren $\lambda, \mu \in \mathbb{Z}$, sodass*

$$\mathrm{ggT}(a,b) = \lambda \cdot a + \mu \cdot b.$$

Definition 3.10. Zwei ganze Zahlen $a, b \in \mathbb{Z}$ heißen **teilerfremd**, wenn $\mathrm{ggT}(a,b) = 1$.

Allgemein[3] **folgt** aus $d = \lambda a + \mu b$ **nicht**, dass $d = \mathrm{ggT}(a,b)$. Es gibt eine sehr wichtige Ausnahme:

Korollar 3.11. Für $a, b \in \mathbb{Z}$ sind folgende aussagen äquivalent.

(i) $\mathrm{ggT}(a,b) = 1$.

(ii) Es existieren $\lambda, \mu \in \mathbb{Z}$, sodass $\lambda a + \mu b = 1$.

Beweis-Skizze: (i)⇒(ii) ist ein Sonderfall von Lemma 3.9.

(ii)⇒(i) Sei d ein gemeinsamer Teiler. Das heißt $d \mid a$ und $d \mid b$, also $d \mid \lambda a + \mu b = 1$, und somit $d = \pm 1$. Also unserer Konvention nach, ist $\mathrm{ggT}(a,b) = 1$. Q.E.D.

Lemma 3.12. *Für alle $a, b \in \mathbb{Z}$ gilt $|ab| = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b)$.*

Beweis-Skizze: Wenn $a = 0$ oder $b = 0$, dann folgt der Satz aus Bemerkung 3.8.
Es reicht den Satz für $a, b > 0$ zu zeigen. Sei $d = \mathrm{ggT}(a,b) > 0$. Weil $d \mid ab$, existiert ein $l \in \mathbb{N}$ mit $ab = dl$. Wir werden zeigen, dass $l = \mathrm{kgV}(a,b)$.

(kgV 1) Es existieren $k_a, k_b \in \mathbb{N}$ mit $dk_a = a$ und $dk_b = b$. Also

$$\begin{aligned} ld &= ab = dk_b a \overset{d \neq 0}{\Longrightarrow} l = k_b a \Rightarrow a \mid l \\ ld &= ab = dk_a b \overset{d \neq 0}{\Longrightarrow} l = k_a b \Rightarrow b \mid l. \end{aligned}$$

also (kgV1) ist für l erfüllt.

[3] Übung: Finden Sie ein Beispiel.

(kgV 2) Sei jetzt $m \in \mathbb{N}$ mit $a \mid m$ und $b \mid m$. Also $\exists\, n_a, n_b \in \mathbb{N}$ mit $m = an_a = bn_b$. Aus Bézouts Lemma 3.9 folgt, dass es $\lambda, \mu \in \mathbb{Z}$ existieren mit $d = \lambda a + \mu b$. Also

$$md = m\lambda a + m\mu b = (bn_b)\lambda a + (an_a)\mu b = ab(\lambda n_b + \mu n_a) = dl(n_b\lambda + n_a\mu) \overset{d\neq 0}{\Longrightarrow} l \mid m.$$

Somit ist auch (kgV2) für l erfüllt. Q.E.D.

Lemma 3.13 (von Euklid)**.** *Wenn $d \mid ab$ und $\mathrm{ggT}(a, d) = 1$, dann $d \mid b$.*

Beweis-Skizze: Weil $\mathrm{ggT}(a, d) = 1 \overset{\text{Lemma } 3.9}{\Longrightarrow} \exists\, \lambda, \mu \in \mathbb{Z}$ mit $\lambda a + \mu d = 1$. Also wenn wir beide Seiten mit b multiplizieren, dann bekommen wir

$$\lambda ab + \mu db = b.$$

Weil d beide Summanden teilt, folgt $d \mid b$. Q.E.D.

3.3 Der Euklidische Algorithmus

Lemma 3.14. *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$, und seien q, r die eindeutig-bestimmten ganze Zahlen aus dem Satz 3.3 der Division mit Rest. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.*

Beweis-Skizze: Seien also $q, r \in \mathbb{Z}$ mit $0 \leqslant r < |b|$, sodass

$$a = qb + r.$$

Wir zeigen, dass $T_{a,b} = T_{b,r}$, das heißt, dass die Mengen aller gemeinsamer Teiler gleich sind.

$\boxed{\subseteq}$ Sei $d \in T_{a,b}$. Weil $r = a - qb$, $d \mid a$ und $d \mid b$ folgt, dass $d \mid r$.

$\boxed{\supseteq}$ Sei $e \in T_{b,r}$. Weil $a = qb + r$, $e \mid b$ und $e \mid r$ folgt, dass $e \mid a$. Q.E.D.

Der Euklidische Algorithmus.
`Eingabe:` $a, b \in \mathbb{Z}$.
`Schritt 0:` Wenn $a = 0$, dann `Ausgabe` $= |b|$.
Wenn $b = 0$, dann `Ausgabe` $= |a|$.
`Schritt 1:` Definiere $i := 0$, $r_{-1} := a$, $r_0 := b$.
`Schritt 2:` Durch Anwenden des Divisionssatz 3.3 für r_{i-1} und r_i finde die eindeutigen q und r mit

$$r_{i-1} = qr_i + r, \qquad \text{und} \qquad 0 \leqslant r < r_i.$$

`Schritt 3:` $\boxed{\text{Wenn } r \neq 0}$ definiere $i := i + 1$, $r_i := r$, und wiederhole `Schritt 2` (für das neue i).
$\boxed{\text{Sonst}}$ `Ausgabe`$= r_i$.

Beispiel 3.15. Seien $a = 161$ und $b = 28$. Wir haben

$$\begin{aligned} 161 &= 5 \cdot 28 + 21 \\ 28 &= 1 \cdot 21 + \boxed{7} \leftarrow \text{letzter Rest } \neq 0 \\ 21 &= 3 \cdot 7 + 0 \end{aligned}$$

Also $\mathrm{ggT}(161, 28) = 7$. Es gibt auch einen erweiterten euklidischen Algorithmus, der uns auch die zwei ganze Zahlen λ, μ aus dem Lemma von Bézout (Lemma 3.9) gibt.

Satz 3.16. *Der euklidische Algorithmus endet und gibt als Antwort* $\mathrm{ggT}(a, b)$.

Beweis-Skizze: Es endet, weil $b = r_0 > r_1 > \cdots \geq 0$. Dass die Antwort der ggT ist, folgt aus Lemma 3.14 und Bemerkung 3.8 4.. Q.E.D.

Bemerkung 3.17. Lemma 3.12 und den euklidischen Algorithmus geben ein Verfahren für die Bestimmung des kleinstes gemeinsames Vielfaches zweier Zahlen $a, b \in \mathbb{Z}$:

$$\mathrm{kgV}(a, b) = \frac{|ab|}{\mathrm{ggT}(a, b)} = \frac{|a|}{\mathrm{ggT}(a, b)} \cdot |b|.$$

3.4 Primzahlen

Definition 3.18. Eine **Primzahl** ist eine natürliche Zahl $p > 1$ dessen einzige positive Teiler 1 und p sind.

Beispiel 3.19. Primzahlen: 2,3,5,7,101,32 003, 65 537.

nicht Primzahlen: 4,6,15,60, 4 294 967 297.

Ist 2021 eine Primzahl?

Satz 3.20. *Die Zahl $p \in \mathbb{N}$ ist eine Primzahl genau dann, wenn "für alle $a, b \in \mathbb{Z}$ aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$".*

Beweis-Skizze: $\boxed{\Rightarrow}$ Aus Lemma 3.13.
$\boxed{\Leftarrow}$ Wenn $d \mid p \Rightarrow p = dk$. Also $p \mid dk$. Dann $(p \mid d \text{ oder } p \mid k) \Rightarrow (d = p \text{ oder } d = 1)$. Q.E.D.

Korollar 3.21. Es seien p eine Primzahl, $n \geqslant 2$ und $a_1, \ldots, a_n \in \mathbb{Z}$. Dann gilt

$$p \mid (a_1 \cdots a_n) \quad \Longleftrightarrow \quad \exists\, i \in \{1 \ldots n\}, \text{ sodass } p \mid a_i.$$

Satz 3.22 (Hauptsatz der elementaren Zahlentheorie)**.** *Es seien $a \in \mathbb{Z} \setminus \{0, \pm 1\}$ und $\epsilon \in \{\pm 1\}$, sodass $\epsilon \cdot a > 0$. Dann gibt es eindeutig bestimmte $s \in \mathbb{N}_{>0}$, Primzahlen $p_1 < \cdots < p_s$, und $k_1, \ldots, k_s \in \mathbb{N}_{>0}$, sodass*

$$a = \epsilon \cdot p_1^{k_1} \cdots p_s^{k_s}.$$

Beweis-Skizze: Es reicht den Fall $a > 1$ zu betrachten.

Existenz. Sei $S = \{a \in \mathbb{N}_{>1} \ : \ a \text{ ist } \textbf{kein} \text{ Produkt von Primzahlen}\} \subseteq \mathbb{N}$. Nehmen wir an, dass $S \neq \emptyset$. Dann, weil $\mathbb{N}$ wohl geordnet ist, existiert ein kleinstes Element in S:

$$a_0 := \min S.$$

Wäre a_0 eine Primzahl, dann wäre es auch ein Produkt (der Länge 1) von Primzahlen. Also a_0 hat einen anderen Teiler als 1 und a_0 selbst: sei es $b \in \mathbb{N}_{>1}$. Somit existiert $c \in \mathbb{N}$ mit

$$a_0 = b \cdot c.$$

Weil $1 < b < a_0$, muss auch $1 < c < a_0$. Also, weil $a_0 = \min S$, gilt $b, c \notin S$. Das heißt b und c lassen sich als Produkt von Primzahlen schreiben, und somit auch $b \cdot c = a_0$. Das heißt, dass $a_0 \notin S$ – ein Widerspruch. Also $S = \emptyset$.

Eindeutigkeit. Seien $s, r \in \mathbb{N}_{>0}$, Primzahlen $p_1 < \cdots < p_s$ und $q_1 < \cdots < q_r$, und $k_1, \ldots, k_s \in \mathbb{N}_{>0}$ und $l_1, \ldots, l_r \in \mathbb{N}_{>0}$, sodass

$$p_1^{k_1} \cdots p_s^{k_s} = q_1^{l_1} \cdots q_r^{l_r}.$$

Aus Korollar 3.21 folgt, dass für jedes $i = 1, \ldots, s$ existiert ein $j \in \{1, \ldots, r\}$, sodass $p_i \mid q_j$. Weil beide Primzahlen sind, folgt daraus

$$p_i = q_j.$$

Also $\{p_1, \ldots, p_s\} \subseteq \{q_1, \ldots, q_r\}$. Völlig Analog folgt die umgekehrte Inklusion, also $s = r$ und $p_i = q_i$ für $i = 1, \ldots, s$.
Wir nehmen an, dass $k_1 \neq l_1$. Ohne Beschränkung der Allgemeinheit können wir $k_1 < l_1$ annehmen. Dann können wir in

$$p_1^{k_1} \cdots p_s^{k_s} = p_1^{l_1} \cdots p_s^{l_s},$$

beide Seiten durch $p_1^{k_1}$ teilen und bekommen

$$p_2^{k_2} \cdots p_s^{k_s} = p_1^{l_1 - k_1} \cdot p_2^{k_2} \cdots p_s^{l_s}.$$

Das ist aber ein Widerspruch zum ersten Teil. Also $k_1 = l_1$, und wir können den Beweis durch Induktion beenden. Q.E.D.

Die eindeutig bestimmte Primzahlen aus dem obigen Satz heißen die **Primfaktoren** von a.

Satz 3.23. *Es gibt unendlich viele Primzahlen.*

Beweis-Skizze: Nehmen wir an, dass es nur endlich viele Primzahlen gibt. Seien diese $1 < p_1 < \cdots < p_s$. Dann ist aber $n = p_1 \cdots p_s + 1$ eine positive ganze Zahl, die nach Satz 3.22 eindeutig bestimmte Primfaktoren hat. Keiner davon kann aber unter den $p_1, \ldots, p_s$ sein, weil diese den Rest 1 bei der Division von n geben. Das ist ein Widerspruch. Q.E.D.

In [AZ99, Kapitel 1] finden Sie fünf weitere Beweise für diesen Satz.

3.4.1 Der Sieb des Eratosthenes

Das ist ein klassischer (im wahren Sinne des Wortes) Algorithmus, der für eine gegebene natürliche Zahl $n \in \mathbb{N}$ alle Primzahlen zwischen 2 und n bestimmt. Das läuft so:

Das Sieb des Eratosthenes.

`Eingabe:` $n \in \mathbb{Z}$ mit $n \geqslant 2$.

`Setze:` $p_0 := 2$, $N_0 := \{3, \ldots, n\}$, $\mathcal{P}_0 := \{p_0\}$.

`Schritt` i`:` Seien $i \geqslant 0$, p_i, N_i, $\mathcal{P}_i$ schon bestimmt.

Dann setze: $N_{i+1} := N_i \setminus \{a \cdot p_i \ : \ a \in \mathbb{N}_{>0}\}$,

und dann:

Wenn $N_{i+1} = \emptyset$, dann breche den Algorithmus ab.

Wenn $N_{i+1} \neq \emptyset$, dann setze $p_{i+1} := \min N_{i+1}$,

$\mathcal{P}_{i+1} := \mathcal{P}_i \cup \{p_{i+1}\}$,

$i := i + 1$,

und wiederhole.

`Ausgabe:` $\mathcal{P}_i$ = die Menge aller Primzahlen zwischen 2 und n.

3.4.2 Primzahlen der Form $b^m + 1$

Satz 3.24. *Es seien $b \geqslant 2$ und $m \geqslant 1$ ganze Zahlen. Wenn $b^m + 1$ eine Primzahl ist, dann ist b gerade und es existiert ein $k \in \mathbb{N}$, sodass $m = 2^k$.*

Beweis-Skizze: Wenn b ungerade ist, dann ist $b^m + 1$ gerade und größer als 2. Es kann also keine Primzahl sein.
Wenn $p \geqslant 3$ ein Primfaktor von m ist, dann haben wir $m = p \cdot q$ mit $q \in \mathbb{N}$. Das heißt

$$b^m + 1 = b^{pq} + 1 = (b^q)^p + 1 = (b^q + 1)\left((b^q)^{p-1} - (b^q)^{p-2} + \cdots - b^q + 1\right).$$

Ein Widerspruch. Also 2 ist der einzige Primfaktor von m. Q.E.D.

Eine **Fermat-Zahl** ist eine natürliche Zahl der Form:

$$F_k = 2^{(2^k)} + 1, \quad \text{für } k \geqslant 0.$$

Wenn F_k eine Primzahl ist, dann heißt diese eine Fermat-Primzahl. Für $k = 0, 1, 2, 3, 4$ haben wir

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537.$$

Alle fünf sind Primzahlen. Für $k = 5$ aber ist

$$F_5 = 4\,294\,967\,297$$

ist keine Primzahl. Der kleinste Primfaktor davon ist 641. Es ist eine offene Frage, ob es unendlich viele Fermat-Primzahlen gibt. Wahrscheinlich nicht. Die größte bekannte Fermat Primzahl ist F_4.

3.4.3 Primzahlen der Form $2^m - 1$.

Satz 3.25. *Es sei $m \geqslant 2$ eine ganze Zahl. Wenn $2^m - 1$ eine Primzahl ist, dann ist m eine Primzahl.*

Beweis-Skizze: Nehmen wir an, dass $2^m - 1$ eine Primzahl ist. Wenn m keine Primzahl ist, existieren ganze Zahlen $p, q \geqslant 2$ mit $m = pq$. Dann gilt

$$2^m - 1 = 2^{(pq)} - 1 = (2^p)^q - 1 = (2^p - 1)\left(2^{p(q-1)} + 2^{p(q-2)} + \cdots + 2^p + 1\right).$$

Weil $p, q > 1$, sind beide Faktoren oben größer als 2 und somit haben wir einen Widerspruch bekommen. Q.E.D.

Eine **Mersenne-Zahl** ist eine ganze Zahl der Form

$$M_k = 2^k - 1, \text{für } k \geqslant 0.$$

Wenn M_k eine Primzahl ist, dann heißt es eine Mersenne-Primzahl. Der Satz 3.25 sagt also, dass alle Mersenne-Primzahlen sich in der Menge $\{M_p \ : \ p \text{ ist eine Primzahl}\}$ befinden. Die ersten vier Kandidaten: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ sind Mersenne-Primzahlen. Aber $M_{11} = 2047 = 23 \cdot 89$ ist keine Primzahl. Es ist unbekannt ob es unendlich viele Mersenne-Primzahlen gibt, oder ob es unendlich viele Mersenne-Zahlen, die nicht prim sind, gibt.

3.5 Modulare Arithmetik

3.5.1 Kongruenz modulo einer natürlichen Zahl

Definition 3.26. Sei $n \in \mathbb{N}$. Wir definieren die Relation **Kongruenz modulo** n auf $\mathbb{Z}$, die man mit $\equiv \bmod n$ bezeichnet, durch

$$a \equiv b \bmod n \quad \Longleftrightarrow \quad n \,|\, (a - b).$$

Falls a nicht kongruent zu b modulo n ist, schreiben wir $a \not\equiv b \bmod n$.

Beispiele:

1. $-2 \equiv 7 \bmod 9$.
2. $100 \equiv -8 \equiv 1 \bmod 9$.
3. $1 \equiv -1 \bmod n \Leftrightarrow n \in \{1, 2\}$.
4. $a \equiv b \bmod 0 \Leftrightarrow a = b$.
5. $a \equiv b \bmod 1 \ \ \forall\, a, b \in \mathbb{Z}$.
6. $a \equiv 0 \bmod n \Leftrightarrow n \,|\, a$.

Bemerkung 3.27. 1. Zwei ganze Zahlen sind genau dann kongruent modulo n, wenn sie denselben Rest bei der Division durch n haben.

2. Für die Kongruenz modulo n gelten folgende Eigenschaften:

Reflexivität:	$a \equiv a \bmod n$ für alle $a \in \mathbb{Z}$.
Symmetrie:	Wenn $a \equiv b \bmod n$, dann $b \equiv a \bmod n$.
Transitivität:	Wenn $a \equiv b \bmod n$ und $b \equiv c \bmod n$, dann $a \equiv c \bmod n$.

Beweis-Skizze:

1. Es seien $a, b \in \mathbb{Z}$ und es seien q_a, q_b, r_a, r_b die eindeutig bestimmten Zahlen aus dem Satz der Division mit Rest durch n. Das heißt

$$a = q_a \cdot n + r_a, \qquad b = q_b \cdot n + r_b \text{ und } 0 \leqslant r_a, r_b < n.$$

   Wir wollen also zeigen, dass

$$a \equiv b \bmod n \iff r_a = r_b.$$

   $\boxed{\Rightarrow}$ Wenn $a \equiv b \bmod n$, dann gilt per Definition $n \mid a - b$. Also

$$n \mid (q_a - q_b)n + (r_a - r_b).$$

   Weil $n \mid (q_a - q_b)n$, folgt aus der obigen Teilbarkeit, dass $n \mid r_a - r_b$. Weil sowohl r_a als auch r_b zwischen 0 und $n - 1$ liegen, gilt auch

$$|r_a - r_b| < n.$$

   Die einzige Zahl mit Betrag kleiner als n die durch n teilbar ist, ist die Null. Also $r_a - r_b = 0$.

   $\boxed{\Leftarrow}$ Wenn $r_a = r_b$, dann folgt $a - b = (q_a - q_b)n$. Also $n \mid a - b$ und somit $a \equiv b \bmod n$.

2. **Reflexivität:** $a - a = 0$ ist durch n teilbar, also $a \equiv a \bmod n$.

   Symmetrie: Wenn $n \mid a - b$, dann gilt auch $n \mid b - a$, also $a \equiv b \bmod n \Rightarrow b \equiv a \bmod n$.

   Transitivität: Wenn $n \mid a - b$ und $n \mid b - c$, dann teilt n auch deren Summe, also

$$n \mid (a - b) + (b - c) = a - c.$$

Q.E.D.

Wir sammeln alle ganze Zahlen, die denselben Rest bei der Division durch n haben, in einer Menge die wir Restklasse nennen. Das ist die Idee. Technisch[4] aber ist es einfacher Restklassen wie folgt zu definieren.

Definition 3.28. Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$. Die **Restklasse von a modulo n** ist die Menge:

$$[a]_n := \{b \in \mathbb{Z} \ : \ a \equiv b \bmod n\}.$$

Jedes Element der Restklasse heißt **Repräsentant** der Restklasse. Zum Beispiel, jede gerade Zahl ist ein Repräsentant der Restklasse $[0]_2$ und jede ungerade Zahl ist ein Repräsentant der Restklasse $[1]_2$. Aus Bemerkung 3.27 folgt, dass

$$[a]_n = [b_n] \Leftrightarrow a \equiv b \bmod n.$$

Weiterhin, aus der Transitivität der Konkruenz wenn $a \not\equiv b \bmod n$, dann sind die Restklassen von a und b disjunkt.
Wenn $r \in \{0, \ldots, n-1\}$ der Rest bei der Division von a durch n ist, dann gilt

$$[a]_n = [r]_n.$$

[4] Das heißt genauer und einfacher damit umzugehen.

Weil für $i, j \in \{0, \ldots, n-1\}$ mit $i \neq j$ gilt $i \not\equiv j \bmod n$, gibt es genau n Restklassen modulo n. Wir bezeichnen die Menge aller Restklassen modulo n mit $\mathbb{Z}/n\mathbb{Z}$. Diese kann also beschrieben werden als:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\}.$$

3.5.2 Rechnen modulo einer natürlichen Zahl

Wir definieren die **Addition** $(+)$ und die **Multiplikation** $(\cdot)$ **modulo** n als:

$$\begin{aligned} + &: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \qquad [a]_n + [b]_n := [a+b]_n \\ \cdot &: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \qquad [a]_n \cdot [b]_n := [a \cdot b]_n \end{aligned}$$

Satz 3.29 (Modulare Operationen)**.** *Sei $n \in \mathbb{N}_{>0}$. Die Addition und die Multiplikation modulo n sind wohl-definierte Operationen auf $\mathbb{Z}/n\mathbb{Z}$ (d.h. unabhängig vom Repräsentanten).*

Beweis-Skizze: Um zu zeigen, dass diese Operationen wohldefiniert sind, muss man zeigen, dass $\forall\, a, b, c, d \in \mathbb{Z}$ mit der Eigenschaft, dass $a \equiv b \bmod n$ und $c \equiv d \bmod n$ gilt

$$a + c \equiv b + d \bmod n \qquad \text{und} \qquad ac \equiv bd \bmod n.$$

Es reicht aber zu zeigen, dass für alle $a, b, c \in \mathbb{Z}$, wenn $a \equiv b \bmod n$, dann gilt auch $a + c \equiv b + c \bmod n$ und $ac \equiv bc \bmod n$. Das folgt aus der folgenden einfachen Rechnung:

$$\begin{aligned} (a+c) - (b+c) &= a - b, \\ (ac) - (bc) &= c(a-b). \end{aligned}$$

Q.E.D.

Bemerkung 3.30. Wenn $a \equiv b \bmod n$, dann gilt auch $a^m \equiv b^m \bmod n$, für alle $m \in \mathbb{N}$.

Beweis-Skizze: **Variante 1:** $a^m - b^m = (a-b)(a^{m-1} + \cdots + b^{m-1})$
Variante 2: Induktion nach m:

$$\left.\begin{array}{r} a \equiv b \mod n \\ a^m \equiv b^m \mod n \end{array}\right\} \overset{\text{Satz 3.29}}{\Longrightarrow} a \cdot a^m \equiv b \cdot b^m \bmod n.$$

Q.E.D.

Wir sagen, dass eine ganze Zahl $a \in \mathbb{Z}$ eine **Quadratzahl** (oder einfach ein Quadrat) ist, wenn es ein $k \in \mathbb{N}$ existiert, sodass

$$a = k^2.$$

Eine Restklasse $[a] \in \mathbb{Z}/n\mathbb{Z}$ ist ein Quadrat in $\mathbb{Z}/n\mathbb{Z}$, wenn es eine Restklasse $[k] \in \mathbb{Z}/n\mathbb{Z}$ gibt, sodass $[a] = [k]^2$ in $\mathbb{Z}/n\mathbb{Z}$ gilt.

Beispiel 3.31. Die ersten 17 Quadratzahlen in $\mathbb{Z}$ sind:

$$0, 1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256$$

In $\mathbb{Z}/3\mathbb{Z}$ ist $[-1]_3$ kein Quadrat. In $\mathbb{Z}/5\mathbb{Z}$ haben wir aber:

$$[-1]_5 = [4]_5 = [2]_5^2.$$

Folgender Satz gibt uns eine Methode um zu testen, ob eine Zahl ein Quadrat sein könnte. Das heißt, dass falls es schief läuft, dann ist die Zahl kein Quadrat.

Satz 3.32. *Wenn $a \in \mathbb{Z}$ ein Quadrat ist, dann ist auch $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ ein Quadrat für alle $n \in \mathbb{N}$.*

Beweis-Skizze: Wenn a ein Quadrat ist, dann existiert $k \in \mathbb{N}$ mit $a = k^2$. Also für alle $n \in \mathbb{N}$ gilt auch $[a]_n = [k^2]_n = [k]_n^2$. Q.E.D.

Beispiel 3.33. In $\mathbb{Z}/5\mathbb{Z}$ die Quadrate sind

$$[0]_5^2 = [0]_5, \quad [1]_5^2 = [1]_5, \quad [2]_5^2 = [4]_5, \quad [3]_5^2 = [4]_5, \quad [4]_5^2 = [1]_5.$$

Insbesondere $[2]_5$ und $[3]_5$ sind keine Quadrate. Ist $222^{1000} + 777^{1000}$ ein Quadrat? Das auszurechnen wäre mühsam. Wenn wir aber modulo 5 rechnen, dann haben wir:

$$\begin{aligned}
[222^{1000} + 777^{1000}]_5 &= [222]_5^{1000} + [777]_5^{1000} \\
&= [2]_5^{1000} + [2]_5^{1000} \\
&= [2^2]_5^{500} + [2^2]_5^{500} \\
&= [-1]_5^{500} + [-1]_5^{500} \\
&= [1]_5 + [1]_5 \\
&= [2]_5.
\end{aligned}$$

Also $222^{1000} + 777^{1000}$ ist kein Quadrat.

Wir können also in $\mathbb{Z}/n\mathbb{Z}$ oft einfacher als in $\mathbb{Z}$ rechnen. Alle Eigenschaften der Addition und der Multiplikation der ganzen Zahlen bleiben erhalten. In den folgenden Gleichungen kann $*$ sowohl durch $+$ als auch durch $\cdot$ ersetzt werden:

$$\begin{aligned}
\big([a] * [b]\big) * [c] &= [a] * \big([b] * [c]\big) \\
[a] * [b] &= [b] * [a] \\
[0] + [a] &= [a] \\
[1] \cdot [a] &= [a] \\
[a] + [-a] &= [0] \\
[a] \cdot \big([b] + [c]\big) &= [a] \cdot [b] + [a] \cdot [c]
\end{aligned}$$

Es gibt aber noch ein Vorteil außer der Möglichkeit verschiedene Repräsentanten für Restklassen zu wählen. Manchmal können wir sogar teilen. Der nächste Satz zeigt genau was das heißt und wann das möglich ist.

Satz 3.34. *Sei $n \in \mathbb{N}_{>0}$ und $[a] \in \mathbb{Z}/n\mathbb{Z}$ mit $[a] \neq [0]$. Es existiert ein Element $[a]^{-1} \in \mathbb{Z}/n\mathbb{Z}$ mit $[a] \cdot [a]^{-1} = [1]$ genau dann, wenn $\mathrm{ggT}(a, n) = 1$.*

Beweis-Skizze:

$$\begin{aligned} \mathrm{ggT}(a,n) = 1 &\overset{\text{Kor 3.11}}{\iff} \exists\, s,t \in \mathbb{Z} \text{ mit } as + nt = 1 \\ &\iff [as] + [nt] = [1] \\ &\iff [a][s] + [0] = [1] \\ &\iff [a]^{-1} = [s]. \end{aligned}$$

Q.E.D.

Wir werden hier den **erweiterten euklidischen Algorithmus** anwenden, ohne diesen explizit zu erklären.

Beispiel 3.35. Finde das Inverse von 28 in $\mathbb{Z}/39\mathbb{Z}$. Wir wenden den erweiterten euklidischen Algorithmus an:

$$\begin{aligned} 39 &= 28 \cdot 1 + 11 \\ 28 &= 11 \cdot 2 + 6 \\ 11 &= 6 \cdot 1 + 5 \\ 6 &= 5 \cdot 1 + \boxed{1} \\ 5 &= 1 \cdot 5 + 0. \end{aligned}$$

Also

$$\begin{aligned} 1 &= 6 - 1 \cdot 5 \\ &= 6 - 1 \cdot (11 - 1 \cdot 6) \\ &= (-1) \cdot 11 + 2 \cdot 6 \\ &= (-1) \cdot 11 + 2 \cdot (28 - 2 \cdot 11) \\ &= 2 \cdot 28 + (-5) \cdot 11 \\ &= 2 \cdot 28 + (-5) \cdot (39 - 28) \\ &= 7 \cdot \mathbf{28} + (-5) \cdot \mathbf{39}. \end{aligned}$$

Das heißt, dass

$$[1]_{39} = [7]_{39} \cdot [28]_{39} + [-5]_{39} \cdot [39]_{39} = [7]_{39} \cdot [28]_{39}.$$

Also das Inverse von $[28]_{39}$ ist $[7]_{39}$.

3.5.3 Rechnen modulo einer Primzahl

Hier ist ein besonderer Vorteil des Rechnen modulo einer Primzahl.

Satz 3.36. *Sei p eine Primzahl, und $a, b \in \mathbb{Z}$. Dann gilt*

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Beweis-Skizze: Nach der binomischen Formel gilt

$$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i.$$

Es reicht zu bemerken, dass für $0 < i < p$ die Binomialkoeffizienten $\binom{p}{i}$ durch p teilbar sind. Das gilt, weil

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

und weil p eine Primzahl ist, dann lässt sich die p im Nenner durch $i!$ nicht kürzen. Q.E.D.

Übung. Gilt auch die Umkehrung des Satzes 3.36? Kann man auch sagen, welche Binomialkoeffizienten $\binom{k}{n}$ durch n teilbar sind, wenn man die Primfaktorzerlegung kennt?

Satz 3.37 (Kleiner Satz von Fermat)**.** *Sei p eine Primzahl. Für alle $a \in \mathbb{Z}$ gilt*

$$a^p \equiv a \bmod p.$$

Beweis-Skizze: Für $a \geqslant 0$ zeigen wir die Aussage durch Induktion nach a. Der Fall $a = 0$ ist offensichtlich. Wir nehmen jetzt an, die Aussage sei wahr für a. Für $a+1$ haben wir aus Satz 3.36 und der induktiven Voraussetzung, dass

$$(a+1)^p \equiv a^p + 1^p \equiv a + 1 \bmod p.$$

Für $a < 0$ haben wir aus dem ersten Fall, dass $(-a)^p \equiv -a \bmod p$. Wenn $p = 2$, dann gilt $(-a) \equiv a \bmod 2$, und die Aussage folgt. Für $p > 2$ haben wir

$$-a \equiv (-a)^p \equiv (-1)^p (a)^p \equiv -a^p \bmod p,$$

und die Aussage folgt durch Multiplikation mit -1. Q.E.D.

Die Umkehrung des kleinen Satzes von Fermat gilt nicht. Das heißt es existieren Zahlen n, die nicht prim sind, für die $x^n \equiv x \bmod n$ für alle $x \in \mathbb{Z}$ gilt. Solche Zahlen heißen *Carmichael-Zahlen*[5]. Die kleinsten zwei solche Zahlen sind

$$561 = 3 \cdot 11 \cdot 17 \text{ und } 1105 = 5 \cdot 13 \cdot 17.$$

Bemerkung 3.38. Der Kleine Satz von Fermat ist zu folgender Aussage äquivalent:

$$a^{p-1} \equiv 1 \bmod p, \qquad \text{für } a \not\equiv 0 \bmod p.$$

Beispiel 3.39. Was ist $3^{100} \bmod 7$? Man kann hier sowohl den Satz 3.37 als auch die Bemerkung 3.38 anwenden. Erstmals die Bemerkung:

$$3^{100} \equiv 3^{6 \cdot 16 + 4} \equiv (3^6)^{16} \cdot 3^4 \equiv 1^{16} \cdot 81 \equiv 4 \bmod 7.$$

Um den Satz 3.37 anzuwenden, bemerken wir erstmals, dass $100 = 7 \cdot 14 + 2$. Also

$$3^{100} \equiv (3^7)^{14} \cdot 3^2 \equiv 3^{14} \cdot 3^2 \equiv (3^7)^2 \cdot 3^2 \equiv 3^2 \cdot 3^2 \equiv 3^4 \equiv 4 \bmod 7.$$

[5] https://de.wikipedia.org/wiki/Carmichael-Zahl

3.5.4 Teilbarkeit Kriterien

Sei $a \in \mathbb{N}$ dargestellt im dekadischen System:

$$a = \overline{a_m a_{m-1} \dots a_1 a_0}.$$

Das heißt, für alle i gilt $a_i \in \{0, \dots, 9\}$ und

$$a = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \dots + a_1 \cdot 10 + a_0.$$

Die **Quersumme** von a ist die Summe der Ziffern von a:

$$Q(a) := \sum_{i=1}^{m} a_i.$$

Für $n = 3$ oder $n = 9$ haben wir aus Satz 3.29, dass

$$a \equiv \sum_{i=0}^{m} a_i 10^i \equiv \sum_{i=0}^{m} a_i \bmod n.$$

Das heißt $3 \mid a$, bzw. $9 \mid a$, genau dann, wenn $3 \mid Q(a)$, bzw. $9 \mid Q(a)$. Analog, für $n = 11$ kann man die **alternierende Quersumme** betrachten: $AQ(a) = \sum_{i=0}^{m} (-1)^i a_i$ und bekommt:

$$11 \mid a \iff 11 \mid AQ(a).$$

Zum Beispiel, $11 \mid 957$ weil $11 \mid 9 - 5 + 7 = 11$.
Übung: Was passiert für andere $n = 2, \dots, 15$? Und was passiert für andere Zahlensysteme?

3.6 Relationen

Definition 3.40. Eine **Relation** auf einer Menge M ist eine Teilmenge $R \subset M \times M$.

Eine Relation ist also eine Menge geordneter Paare. Wenn $(x, y) \in R$ schreiben wir

$$x \sim_R y \qquad \text{oder} \qquad x \sim y$$

und man sagt, dass x in Relation zu y steht.

Definition 3.41. Eine Relation heißt

$$\begin{aligned} \textbf{reflexiv} &\iff x \sim x \quad \forall\, x \in M. \\ \textbf{symmetrisch} &\iff x \sim y \Rightarrow y \sim x. \\ \textbf{antisymmetrisch} &\iff x \sim y \,\text{und}\, y \sim x \Rightarrow x = y. \\ \textbf{transitiv} &\iff x \sim y \,\text{und}\, y \sim z \Rightarrow x \sim z. \end{aligned}$$

Die einzige Relation die alle vier (eigentlich, die die ersten drei) Eigenschaften erfüllt ist die Gleichheit. Uns werden aber zwei bestimmte Arten von Relationen interessieren, die jeweils 3 davon erfül len: Äquivalenzrelationen – die Objekte identifizieren/gleichsetzen, und Ordnungsrelationen – die Objekte vergleichen und (manchmal) sagen welches größer/besser/schöner ist.

3.6.1 Äquivalenzrelationen

Definition 3.42. Eine **Äquivalenzrelation** auf einer Menge M ist eine Relation $\sim_R$ die *reflexiv*, *symmetrisch*, und *transitiv* ist.

Wenn $\sim_R$ eine Äquivalenzrelationist und $x \sim_R y$, dann sagen wir, dass x äquivalent zu y (unter R) ist.

Definition 3.43. Sei $\sim$ eine Äquivalenzrelation auf der Menge M. Eine **Äquivalenzklasse** für $\sim$ ist eine Teilmenge von M der Form:

$$[x]_\sim = \{m \in M \;:\; m \sim x\},$$

wobei $x \in M$. In diesem Fall heißt $[x]$ **die Äquivalenzklasse von** x.

Wir bezeichnen Äquivalenzklassen auch mit $\widehat{x}$ oder $\widetilde{x}$ oder ähnliches.

Beispiel 3.44. Für die Kongruenz modulo 3 als Äquivalenzrelation auf $\mathbb{Z}$ haben wir die Äquivalenzklassen:

$$\begin{aligned} [0] &= \{3k \;:\; k \in \mathbb{Z}\} = \{\cdots -6, -3, 0, 3, 6, 9, \dots\} \\ [1] &= \{3k+1 \;:\; k \in \mathbb{Z}\} = \{\cdots -5, -2, 1, 4, 7, 10, \dots\} \\ [2] &= \{3k+2 \;:\; k \in \mathbb{Z}\} = \{\cdots -4, -1, 2, 5, 8, 11, \dots\} \end{aligned}$$

Es gibt keine weitere Äquivalenzklassen. Für alle $k \in \mathbb{Z}$ gilt:

$$[0] = [3k] \qquad [1] = [3k+1] \qquad [2] = [3k+2].$$

Insbesondere: $[0] = [3] = [99] = [123\,456\,789]$.

Beispiele:

1. Das "schärfste" Beispiel von Äquivalenzrelation ist die Gleichheit. Also
$$R_= := \{(x, x) \mid x \in M\}.$$
Da wir Reflexivität brauchen, ist diese Relation in allen Äquivalenzrelationen enthalten. Die Menge $R_=$ heißt auch mit *Diagonale* von $M \times M$ und wird mit $\Delta_{M\times M}$ oder einfach Δ bezeichnet.
2. **Kongruenz Modulo** $m \in \mathbb{N}$ auf $\mathbb{Z}$. Diese wird mit $\equiv_m$ oder $\equiv \mod m$ bezeichnet:
$$x \equiv_m y \quad \text{oder} \quad x \equiv y \bmod m \quad \overset{\text{Def}}{\iff} \quad x - y \text{ ist durch } m \text{ teilbar.}$$
Diese ist eine der wichtigsten Äquivalenzrelation der Algebra und Zahlentheorie.
3. Auf der Mengen der Karten in einem Stapel von 52 Spielkarten können wir folgende Äquivalenzrelation definieren: zwei Karten sind äquivalent, wenn diese dasselbe Zeichen haben. Dann gibt es vier Äquivalenzklassen: ♣, ♠, ♢, ♡.
4. Kongruenz und Ähnlichkeit für Dreiecke in der Euklidischen Ebene sind beide Äquivalenzrelationen.
5. Sei $Z = \mathbb{N}^2 = \{(a, b) \ : \ a, b \in \mathbb{N}\}$. Wir definieren die Äquivalenzrelation auf Z durch
$$(a, b) \sim (c, d) \quad \iff \quad a + d = b + c.$$
Die Äquivalenzklassen dieser Relation sind in Bijektion mit den ganzen Zahlen.
6. Sei $Q = \{(a, b) \mid a \in \mathbb{Z} \text{ und } b \in \mathbb{Z} \setminus \{0\}\}$. Eine Äquivalenzrelation auf Q ist
$$(a, b) \sim (c, d) \quad \iff \quad a \cdot d = b \cdot c.$$
Die Äquivalenzklassen dieser Relation sind in Bijektion mit den rationalen Zahlen.
7. Sei $R = \{(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \ : \ (x_n)_{n\in\mathbb{N}} \text{ ist eine Cauchy Folge}\}$. Sie finden die Definition von Cauchy Folge hier unten[6]. Auf dieser Menge definieren wir die Äquivalenzrelation
$$(x_n) \sim (y_n) \quad \iff \quad \lim_{n\to\infty} (x_n - y_n) = 0.$$
Die Äquivalenzklassen dieser Relation sind in Bijektion mit den reellen Zahlen.
8. Auf der Menge $\mathbb{R}[x]$, der Polynome mit reellen Koeffizienten in einer Variable x, definieren wir die Äquivalenzrelation
$$f \sim g \quad \iff \quad (x^2 + 1) \,|\, (f - g).$$
Die Äquivalenzklassen dieser Relation sind in Bijektion mit den komplexen Zahlen.
9. Jede Abbildung $f : A \longrightarrow B$ definiert eine Äquivalenzrelation auf A:
$$a \sim_f b \quad \iff \quad f(a) = f(b).$$
10. Auf der Potenzmenge 2^M kann ist Gleichmächtigkeit eine Äquivalenzrelation:
$$A \sim_{gm} B \iff \exists f : A \longrightarrow B \text{ bijektiv.}$$
Ist Gleichmächtigkeit allgemein eine Äquivalenzrelation?

[6] (x_n) ist eine Cauchy Folge wenn $\forall\, \varepsilon \in \mathbb{Q}_+, \ \exists N \in \mathbb{N}, \ \text{sodass } |x_n - x_m| < \varepsilon \ \forall\, m, n > N.$

11. Die Relation $\subseteq$ auf 2^M ist nicht eine Äquivalenzrelation, weil diese nicht symmetrisch ist.
12. Die Relation $A \sim B \Leftrightarrow A \cap B = \emptyset$ auf 2^M ist nicht eine Äquivalenzrelation, weil sie nicht reflexiv und nicht transitiv ist.
13. Sei M die Menge aller lebendigen Menschen.
    (a) "$m_1 \sim_{AG} m_2 \Leftrightarrow m_1$ und m_2 denselben Arbeitgeber haben" ist symmetrisch, könnte transitiv sein (z.B. wenn niemand zwei Arbeitgeber hat), ist aber nicht reflexiv (Kinder, Arbeitslose, Rentner).
    (b) "$m_1 \sim_{SA} m_2 \Leftrightarrow m_1$ und m_2 dieselbe Staatsangehörigkeit haben" ist nicht transitiv (Doppelte Staatsangehörigkeit).

3.6.2 Ordnungsrelationen

Definition 3.45. Eine **Ordnungsrelation** auf der Menge M ist eine Relation $\preceq$ auf M die *reflexiv*, *antisymmetrisch*, und *transitiv* ist.

Bemerkung 3.46. In der Definition von Ordnungsrelation wird nicht verlangt, dass man alle Elemente miteinander vergleichbar sind. Die Teilbarkeit auf der Menge der natürlichen Zahlen ist ein gutes Beispiel dafür: Primzahlen sind unvergleichbar.

Folgende Bezeichnungen werden auftreten. Eine partiell **geordnete Menge** ist ein geordnetes Paar $(M, \preceq)$, wobei $\preceq$ eine Ordnungsrelation auf M ist. Manchmal wird "partiell" ausgelassen. Zwei Elemente $x, y \in M$ sind **vergleichbar** wenn $x \preceq y$ oder $y \preceq x$. Zwei Elemente sind **unvergleichbar** wenn diese nicht vergleichbar sind. Eine Ordnungsrelation heißt **total** wenn jede zwei Elemente vergleichbar sind. Eine **Wohlordnung** ist eine Ordnungsrelation für welche in jeder nicht leeren Teilmenge $M' \subseteq M$ ein minimales Element existiert, nämlich ein $x \in M'$, sodass $x \preceq y \quad \forall\, y \in M'$. Wir sagen in diesem Fall, dass $(M, \preceq)$ **wohl geordnet** ist.

Beispiele:

1. Die "natürliche" Ordnung auf $\mathbb{N} = \{0, 1, 2, \dots\}$, definiert durch
$$a \leqslant b \iff \exists k \in \mathbb{N} \text{ sodass } b = a + k,$$
ist eine Ordnungsrelation. Eine ganz wichtige Eigenschaft dieser Relation ist, dass es eine Wohlordnung ist. Wir werden das hier beweisen.

Beweis-Skizze: Erstmals zeigen wir, dass es tatsächlich eine Ordnungsrelation ist.
Reflexivität $a = a + 0, \quad \forall\, a \in \mathbb{N}$ also $a \leqslant a$.
Antisymmetrie $a \leqslant b \Leftrightarrow b = a + k$ und $b \leqslant a \Leftrightarrow a = b + k'$. Also, wenn wir einsetzen, dann bekommen wir $a = a + k + k' \;\Rightarrow\; k = k' = 0 \;\Rightarrow\; a = b$.
Transitivität $a \leqslant b \leqslant c \Rightarrow b = a + k$ und $c = b + h \Rightarrow c = a + (k + h) \Rightarrow a \leqslant c$.

Bemerkung: Wir haben $0 \leqslant n \;\forall\, n \in \mathbb{N}$, weil $n = 0 + n$.

Wir zeigen jetzt, dass es eine Wohlordnung ist. Sei also $\emptyset \neq A \subseteq \mathbb{N}$ beliebig. Wir wollen zeigen, dass $\min A$ existiert (i.e. $\exists m \in A$ mit $m \leqslant a, \forall\, a \in A$)

Fall 1: $0 \in A$**.** Dann ist $\min A = 0$.
Fall 2: $0 \notin A$**.** Wir nehmen an, dass es $\min A$ nicht gibt, und suchen einen Widerspruch. Dieser wird $A = \emptyset$ sein.
Sei $B := \mathbb{N} \setminus A$. Wir beweisen durch vollständige Induktion, dass $\forall\, n \in \mathbb{N}$ gilt $\{1, \ldots, n\} \subseteq B$. Daraus folgt dass $B = \mathbb{N}$, und somit unser Widerspruch: $A = \emptyset$.
Induktionsanfang $0 \in B$, weil wir im Fall $0 \notin A$ sind.
Induktionsschritt Wir haben als Voraussetzung $\{0, \ldots, n\} \subseteq B$, und wollen zeigen, dass $n+1 \in B$. Aus der Voraussetzung folgt $n < a \quad \forall\, a \in A$. Also $n + 1 \leqslant a \quad \forall\, a \in A$. Da wir angenommen haben, dass $\min A$ nicht existiert, haben wir $n + 1 \notin A$, also $n + 1 \in B$.

Q.E.D.

2. $(\mathbb{N}, <)$ ist keine Ordnungsrelation, weil diese nicht reflexiv ist.
3. $(\mathbb{Z}, \leqslant)$ ist geordnet durch $a \leqslant b \Leftrightarrow b - a \in \mathbb{N}$. Das ist aber keine Wohlordnung, weil $\mathbb{Z}$ selbst kein minimales Element hat.
4. Eine andere Ordnungsrelation auf $\mathbb{Z}$ ist $a \preceq b \Leftrightarrow |a| < |b|$ oder $(|a| = |b| \text{ und } a \leqslant b)$.
5. Die Mengeninklusion sollte eine Ordnungsrelation sein. Wir können aber nicht sagen, dass es eine Ordnungsrelation ist, ohne eine Menge von Teilmengen zu erwähnen. Eine Relation braucht eine Menge, und die "Menge aller Mengen" existiert nicht. Also, für jede Menge M ist $(2^M, \subseteq)$ eine partiell geordnete Menge.
6. $(\mathbb{N}, |)$ wobei $|$ die Teilbarkeit der ganzen Zahlen ist auch eine partiell geordnete Menge (cf. Definition 3.1).
7. Die Teilbarkeit auf der Menge $\mathbb{Z}$ ist nicht antisymmetrisch: $a| - a$ und $-a|a$, aber $a \neq -a$ wenn $a \neq 0$.

3.6.3 Äquivalenzklassen und die Faktormenge

Die Äquivalenzklasse von x ist also die Menge *genau* die Elementen aus M enthält die äquivalent zu x sind. Ich finde folgende Charakterisierung auch sehr suggestiv. Diese könnte die obige Definition ersetzen.

Satz 3.47. *Sei $\sim$ eine Äquivalenzrelation auf der Menge M. Eine Teilmenge $C \subseteq M$ ist genau dann eine Äquivalenzklasse für $\sim$, wenn folgende Axiome erfüllt sind:*

(ÄK 1) $C \neq \emptyset$.

(ÄK 2) *Wenn $a, b \in C$, dann $a \sim b$.*

(ÄK 3) *Für alle $m \in M$ gilt, wenn $\exists\, y \in C$ mit $y \sim m$, dann $m \in C$.*

Beweis-Skizze: $\boxed{\Rightarrow}$ Wenn C eine Äquivalenzklasse ist, dann existiert $x \in M$, sodass $C = [x]_\sim = \{m \in M \;:\; m \sim x\}$. Dann haben wir:

(ÄK 1): $x \in C$, also $C \neq \emptyset$.

(ÄK 2): Seien $a, b \in C = [x]$. Das heißt, dass $a \sim x$ und $b \sim x$, also wegen der Symmetrie haben wir $a \sim x$ und $x \sim b$. Aus der Transitivität folgt dann $a \sim b$.

(ÄK 3): Sei $m \in M$ und $y \in C = [x]$ mit $y \sim m$. Aus $y \in [x]$ folgt per Definition $x \sim y$. Aus der

Transitivität folgt dann $x \sim m$, und somit $m \in [x] = C$.

$\boxed{\Leftarrow}$ Sei $C \subseteq M$ eine Menge die (ÄK 1), (ÄK 2) und (ÄK 3) erfüllt.

Aus (ÄK 1) folgt, dass es $x \in C$ existiert. Wir werden beweisen, dass $C = [x]$. Wir zeigen dafür die zwei Inklusionen.

Sei $c \in C$ beliebig. Weil $x, c \in C$, folgt aus (ÄK 2), dass $c \sim x$, also, dass $c \in [x]$. Somit haben wir $C \subseteq [x]$ gezeigt.

Sei $y \in [x]$ beliebig. Es gilt also für y, dass es $x \in C$ existiert mit $y \sim x$. Aus (ÄK 3) folgt $y \in C$. Somit haben wir auch $[x] \subseteq C$ bewiesen. Q.E.D.

Definition 3.48. Ein **Repräsentant** der Äquivalenzklasse C ist ein Element $x \in C$.
Ein **Repräsentantensytem** für die Äquivalenzrelation $\sim$ ist eine Teilmenge $M' \subseteq M$ mit der Eigenschaft, dass $|M' \cap C| = 1$ für jede Äquivalenzklasse C.

Beispiele:

1. Für die Kongruenz modulo 3 auf $\mathbb{Z}$ ist für $i = 0, 1, 2$ jede Zahl der Form $3k + i$ ein Repräsentant der Äquivalenzklasse $[i]$. Es gibt also unendlich viele Repräsentantensysteme. Hier sind drei solche Beispiele:
$$\{0, 1, 2\}, \quad \{-1, 0, 1\}, \quad \{102, -17, 23\}.$$

2. Für die Äquivalenzrelation durch das Zeichen auf dem Stapel Spielkarten haben hat jede Äquivalenzklasse 13 mögliche Repräsentanten:
$$\text{Äquivalenzklasse aller } \clubsuit \text{ Karten} = [\mathbf{A}\clubsuit] = [\mathbf{2}\clubsuit] = \cdots = [\mathbf{10}\clubsuit] = [\mathbf{B}\clubsuit] = [\mathbf{D}\clubsuit] = [\mathbf{K}\clubsuit].$$
Jedes Repräsentantensystem enthält vier Karten, eine von jedem Zeichen.

Satz 3.49. *Sei $\sim$ eine Äquivalenzrelation auf der Menge M.*

(i) *Wenn C_1 und C_2 zwei Äquivalenzklassen sind, dann gilt entweder $C_1 \cap C_2 = \emptyset$ oder $C_1 = C_2$.*

(ii) *Die Menge M ist die Vereinigung aller Äquivalenzklassen bezüglich $\sim$:*
$$M = \bigcup_{C = \text{Äq.Kl}} C.$$

Beweis-Skizze:

(i) Es reicht zu zeigen, dass $C_1 \cap C_2 \neq \emptyset \Rightarrow C_1 = C_2$. Aus der Symmetrie der Aussage (C_1 und C_2 kann man vertauschen) reicht es $C_1 \subseteq C_2$ zu zeigen.
$C_1 \cap C_2 \neq \emptyset \Leftrightarrow \exists x \in C_1 \cap C_2 \Leftrightarrow \exists x$ mit $x \in C_1$ und $x \in C_2$. Sei $y \in C_1 \overset{(\text{ÄK 2})}{\Longrightarrow} x \sim y$. Da $x \in C_2 \overset{(\text{ÄK 3})}{\Longrightarrow} y \in C_2$.

(ii) Äquivalenzklassen sind Teilmengen von M, also auch die Vereinigung aller Äquivalenzklassen ist in M enthalten. Für die andere Inklusion bemerken wir, dass für jedes $m \in M$ gilt wegen der Reflexivität der Äquivalenzrelation, dass $m \in [m]$.
Q.E.D.

Eine **Partition** (oder Unterteilung) einer Menge M ist eine Teilmenge $\mathcal{P} \subset 2^M$ mit der Eigenschaft, dass

$$A \cap B = \emptyset \ \ \forall\, A, B \in \mathcal{P} \qquad \text{und} \qquad \bigcup_{A \in \mathcal{P}} A = M.$$

Bemerkung 3.50. Satz 3.49 sagt, dass jede Äquivalenzrelation auf einer Menge eine Partition (in Äquivalenzklassen) definiert. Das heißt, dass jedes Element gehört genau einer Äquivalenzklasse.

Bemerkung 3.51. Die Umkehrung des Satzes 3.49 gilt auch:

Wenn $\mathcal{P}$ eine Partition von M ist, dann ist die Relation $\sim_{\mathcal{P}}$ definiert durch

$$x \sim_{\mathcal{P}} y \iff \exists\, A \in \mathcal{P} \ \text{ mit } x, y \in A$$

eine Äquivalenzrelation.

Beweis-Skizze: Reflexivität: Weil $M = \bigcup_{A \in \mathcal{P}} A$, existiert für jedes $m \in M$ ein $A \in \mathcal{P}$, sodass $m \in A$. Also $m \sim m$ für alle $m \in M$.

Symmetrie: Wenn $m \sim n$, dann existiert $A \in \mathcal{P}$ mit $m, n \in A$, also auch $n, m \in A$, also auch $n \sim m$.

Transitivität: Seien $m, n, p \in M$ mit $m \sim n$ und $n \sim p$. Es existieren also $A, B \in \mathcal{P}$, sodass

$$m, n \in A \quad \text{und} \quad n, p \in B.$$

Also $n \in A \cap B$ und somit $A \cap B \neq \emptyset$. Weil $\mathcal{P}$ eine Partition ist, folgt dann, dass $A = B$. Somit haben wir $m, p \in A = B$ und per Definition $m \sim p$. Q.E.D.

Definition 3.52. Sei $\sim$ eine Äquivalenzrelation auf der Menge M. Die **Faktormenge** (oder Quotientenmenge, oder Menge der Äquivalenzklassen) von M durch $\sim$ ist die Menge

$$M/_\sim := \{C \ : \ C \ \text{ ist eine Äquivalenzklasse für } \sim \text{ in } M\}.$$

Die Quotientenabbildung (oder kanonische Projektion, oder kanonische Surjektion) ist die Abbildung die jedes Element in dessen Äquivalenzklasse abbildet:

$$p : M \longrightarrow M/_\sim \qquad x \mapsto [x].$$

Man kann diese Menge als auch $M/_\sim = \{[x] \ : \ x \in M\}$ beschreiben. Die Schreibweise in der Definition 3.52 soll betonen, dass die Elementen von $M/_\sim$ Mengen sind.

Bemerkung 3.53. Für zwei Äquivalenzklassen $[x], [y] \in M/_\sim$ haben wir

$$[x] = [y] \iff x \sim y.$$

Extra:
Eine universelle Eigenschaft ist eine Methode mathematische Objekte ohne Angabe einer konkreten Konstruktion zu definieren. Die Faktormenge kann man auch durch eine universelle Eigenschaft definieren, wir formulieren aber diese als Satz hier. Dieser Satz wird oft angewendet um Abbildungen mit eine Quotientenmenge als Definitionsbereich zu definieren.

Satz 3.54. *Sei $\sim$ eine Äquivalenzrelation auf die Menge M. Sei $f : M \longrightarrow A$ eine beliebige Abbildung.*

(i) *Die Zuordnung $[m] \longmapsto f(m)$ definiert genau dann eine Abbildung $\widehat{f} : M/_\sim \longrightarrow A$, wenn*

$$a \sim b \Rightarrow f(a) = f(b).$$

(ii) *Wenn $\widehat{f}$ eine Abbildung ist, dann haben wir*

(a) $\text{Bild}\, f = \text{Bild}\, \widehat{f}$. *Insbesondere, $\widehat{f}$ ist genau dann surjektiv, wenn f ist surjektiv.*

(b) *$\widehat{f}$ ist genau dann injektiv, wenn $a \sim b \Leftrightarrow f(a) = f(b)$.*

Vor dem eigentlichen Beweis will ich versuchen die Idee des Argumentes darzustellen. Wir haben durch $[m] \mapsto f(m)$ genau dann eine Abbildung von $M/_\sim$ nach A definiert, wenn jedem Element (also Äquivalenzklasse) $[m] \in M/_\sim$ ein einziges Element aus A zugeordnet wird. Wir haben für jede $[m]$ mindestens eine Element: $f(m) \in A$. Wenn es eindeutig ist, dann heißt es, dass wenn wir einen andere Repräsentanten von $[m]$ wählen, zum Beispiel $m' \in M$ mit $[m] = [m']$, dann sollen wir kein neues Element zuordnen. Also $f(m')$ sollte gleich mit $f(m)$ sein, wenn $[m] = [m']$.

Beweis-Skizze:

(i) $\boxed{\Rightarrow}$ Wir nehmen an, dass $\widehat{f}([m]) = f(m)$ eine Abbildung definiert. Seien $a, b \in M$ mit $a \sim b$. Dann haben wir $[a] = [b]$. Also $f(a) = \widehat{f}([a]) = \widehat{f}([b]) = f(b)$.

$\boxed{\Leftarrow}$ Um das obige Argument präzise zu machen, schauen wir uns das Graphen der Zuordnung an:

$$\Gamma = \{([a], f(a)) \;\; : \;\; a \in M\} \subseteq (M/_\sim) \times A$$

Wir wollen überprüfen, dass es das Graphen einer Abbildung im Sinne der Definition 1.24 ist. Das heißt, dass es genau ein geordnetes Paar mit $[a]$ als erstes Element enthält. Für jedes $[a] \in M/_\sim$ haben wir ein Element in Γ, nämlich $([a], f(a))$. Es fehlt also nur zu zeige, dass

$$[a] = [b] \Rightarrow ([a], f(a)) = ([b], f(b)).$$

Nach Bemerkung 3.53 ist äquivalent zu der Voraussetzung: $a \sim b \Rightarrow f(a) = f(b)$.

(ii) (a)

$$b \in \text{Bild}\, f \iff \exists\, a \in M \text{ mit } f(a) = b \iff \exists\, [a] \in M/_\sim \text{ mit } \widehat{f}([a]) = b \iff b \in \text{Bild}\, \widehat{f}.$$

(b) $\boxed{\Rightarrow}$ Sei $\widehat{f}$ injektiv und seien $a, b \in M$. Wir haben

$$f(a) = f(b) \quad \iff \quad \widehat{f}([a]) = \widehat{f}([b]) \quad \overset{\widehat{f}=\text{inj}}{\iff} \quad [a] = [b] \iff a \sim b.$$

$\boxed{\Leftarrow}$ Seien $[a], [b] \in M/_\sim$ mit $\widehat{f}([a]) = \widehat{f}([b])$. Dann haben wir

$$\widehat{f}([a]) = \widehat{f}([b]) \quad \overset{\text{Def}}{\iff} \quad f(a) = f(b) \quad \overset{\text{Voraus.}}{\iff} \quad a \sim b \quad \overset{3.53}{\iff} [a] = [b].$$

Also $\widehat{f}$ ist injektiv.

Q.E.D.

Kapitel 4

Ein bisschen Geometrie

"In abstract mathematics [...] a geometry is anything that satisfies a certain set of axioms."
Robin Hartshorne

4.1 Euklids Elemente

Die Elemente von Euklid (im Original *Stoicheia*) sind das mit Abstand einflussreichste Buch der Geschichte der Mathematik. Wenn wir Euklids Elemente öffnen, finden wir im ersten Teil bekannte Aussagen über Punkte, Geraden, Dreiecke, Kreise in der Ebene. Wir finden Sätze wie *Die Summe der Winkel eines Dreiecks ist 180°*. (Buch I Satz 32[1]) oder den Satz des Pythagoras (Buch I Satz 47). Diese kommen so bekannt vor, weil so wurde Geometrie für mehr als 2000 Jahre beigebracht. Viele dieser Sätze sind immer noch die Basis der geometrischen (Schul-)Lehre.

Eine naive Weise die Geometrie zu beschreiben wäre: eine Zusammenfassung von Fakten, oder Wahrheiten, über die reale Welt. Und das war es auch in der Frühzeit: praktische Regeln für das Messen von Grundstücken, für Stadtplanung, für Bauen. Die Babylonier kannten schon vor Pythagoras den berühmten Satz über der Summe der Quadraten (1900-1600 v.Chr.). Es ist aber unklar ob sie einen Beweis dafür hatten. Es gibt Hinweise, dass die Ägypter Seilschlaufen, die durch zwölf Knoten in zwölf gleiche Strecken geteilt waren, für das Messen von Grundstücken verwendet haben. Weil $12 = 3+4+5$ konnte man damit ein pythagoreisches Dreieck bilden und somit einen rechten Winkel.

Mit den antiken Griechen ändern sich zwei wichtige Punkte in der Anschauung der Geometrie:

1. *Die Natur der geometrischen Wahrheit*, die nicht mehr die Realität betrifft, sondern "ideale Formen". Man braucht absolute Genauigkeit, nicht nur gute Approximationen.
2. *Der Akzent auf Beweis*. Es reicht nicht zu sagen, "das und das ist wahr", und auch nicht Beispiele zu geben wo das wahr ist. In Euklid's Buch muss alles begründet sein.

Euklids hervorragende Leistung war das ganze Material in einer logischen kohärenten Form zu strukturieren, wobei jedes Ergebnis aus den vorherigen folgern kann, und indem man mit wenige Postulaten und Axiomen, die als "offensichtlich" erklärt werden, anfängt. Zum Beispiel, im Beweis des Satzes von Pythagoras werden die Sätze I.41, ... , verwendet. Wenn man dann weiter die Beweise dieser Sätze

[1] Euklid verwendet keine Grade sondern sagt, dass es gleich mit 2 rechten Winkeln ist.

betrachtet, dann werden weitere XXXX gebraucht. Wichtig dabei ist, dass wenn der Satz I.m in dem Beweis Satz I.n verwendet wird, dann gilt auch $m < n$. Nach endlich vielen Schritten führen wir den Beweis des Satzes des Pythagoras auf den Axiomen zurück. Der Weg ist aber lang: es werden insgesamt XXXX Aussagen gebraucht. Die "Hyperlinks" in diesem Text bilden ein komplexes Netzwerk. Alle aussagen sind auf den Axiomen zurückzuführen.

Diese Methode ist immer noch der Standard der Mathematik, und sogar der ganzen Wissenschaft. Aus moderner Sicht aber, enthält der Text von Euklid Lücken: es werden "offensichtlich wahre" Aussagen verwendet, die man aber nicht aus den Axiomen folgern kann. Zum Beispiel: wenn man auf einer Strecke $[AB]$ jeweils einen Kreis mir Radius $|AB|$ und Zentrum A, beziehungsweise B konstruieren, dann schneiden sich diese Kreise. Das entspricht unserer Intuition, ist aber nicht aus Euklids Axiomen herzuleiten (siehe 4.1.3).

Das Problem ist, dass Euklids Geometrie "abstrakt genug" ist. Das heißt, die Axiome sind immer noch an der Realität gebunden. Wie Platons ideale Welt, die zwar nicht die Realität ist, die aber nur ein Ideal für das Wahrgenommene ist. Das moderne Vorgehen ist geometrische Sätze allein auf der Grundlage der Logik aus den Axiomen herzuleiten.

4.1.1 Chronologie

Wir wissen sehr wenig über den Autor der *Elementen*. Euklid von Alexandria[2] ist wahrscheinlich um ∼300 v.Chr. in Athen geboren, hat vermutlich Zeit an der platonischen Akademie in Athen verbracht, und ist dann nach Alexandria gezogen, wo er zur Zeit Ptolemaios I. (ca. 367–283 v. Chr.) wirkte. Hier ist eine weit von vollständiger Chronologie der Mathematiker im antiken Griechenland:

624 - 544 v.Chr.	Thales von Milet
570 - 510 v.Chr.	Pythagoras von Samos
410 - 347 v.Chr.	Eudoxos von Knidos
428 - 348 v.Chr.	Platon
384 - 322 v.Chr.	Aristoteles
∼ 340∼ 270 v.Chr.	**Euklid von Alexandria**
287 - 212 v.Chr.	Archimedes von Syrakus
262 - 190 v.Chr.	Apollonios von Perge
45 - 120 n.Chr.	Menelaos von Alexandria
100 - 160 n.Chr.	Claudius Ptolemäus
100 v.Chr ∼ 350 n.Chr.	Diophant von Alexandria
335 - 405 n.Chr.	Theon von Alexandria
290 - 350 n.Chr.	Pappos von Alexandria

Überlieferung der Elemente

In 4 Jhd.n.Chr. produzierte Theon von Alexandria eine Version von Euklids Elemente, die bis 1808 die einzige verbreitete Variante war. In 1808, Johan Ludvig Heiberg, fand in der Vatikan Bibliothek eine Kopie die nicht von Theon stammt. Dieses Manuskript stammt aus dem 10 Jhd. aus Byzanz.

[2] Nicht zu verwechseln mit Euklid von Megara!

∼100	zwei antike Papyrus Fragmente (Satz II.5, Definition I.15)
888	ältestes erhaltenes Manuskript 888 in Byzanz
∼500	erste lateinische Version: Boethius
∼760	erste arabische Version (via Byzanz) Ishaq ibn Hunayn / Thabit ibn Qurra
1120	eine Arabisch-Lateinische Übersetzung von Adelard von Bath, ein Englischer Mönch, und so kommt es nach Westeuropa
1482	erste Druckversion nach einer Griechisch-Lateinischer Übersetzung von Campanus von Novara ∼1260
1543	erste nicht-lateinische Übersetzung (Italienisch, von Niccolò Tartaglia)
1555	erste deutsche Übersetzung (Johann Scheubel)

4.1.2 Struktur der Elementen

Es gibt 13 Bücher. Jedes Buch fängt mit Definitionen an. Das erste Buch hat zusätzlich 5 Postulate und 5-10 Axiome (oder Grundsätze, oder Allgemeine Regeln, oder „evidente Wahrheiten“) am Anfang. Danach kommt in jedes Buch eine Folge von „Satz + Beweis, Satz + Beweis, . . .“. Jeder Satz ist nur wörtlich ausgedruckt. Dann, am Anfang des Beweises, wird alles wiederholt indem man die Bezeichnung einführt.

Definitionen

Die ersten Definitionen bringen nichts wirklich Neues, als was man schon über Punkte und Geraden weiß. Diese Definitionen sind auf unserer Intuition basiert. Aus moderner Sicht, wo mehrere „Geometrien“ möglich sind, ist das eher ungenau. Der moderne Ansatz ist grundlegende Objekte wie Punkte und Geraden nicht zu definieren. Man betrachtet diese als gegeben und verlangt stattdessen die Erfüllung gewisser Axiome. Zum Beispiel, in einem Körper weiß man nicht *was* die Elemente *sind*. Man verlangt aber die Existenz zweier Operationen und ein gewisses Verhalten aller Elementen bezüglich dieser (Assoziativität, Distributivität, Kommutativität, Neutralelement, inverses Element). Klassisch wurde das aber anders gemacht:

Definitionen aus Buch I:

1. Ein Punkt ist, was keine Teile hat.
2. Eine Linie ist breitenlose Länge.
3. Die Enden einer Linie sind Punkte.
4. Eine Fläche ist, was nur Länge und Breite hat.
5. Die Enden einer Fläche sind Linien.

   . . .

8. Ein ebener Winkel wird von zwei sich berührenden und nicht aufeinander liegenden Linien[3] einer Ebene gebildet und benennt die Neigung der einen zur anderen.
9. Wenn es Geraden sind, die einen Winkel bilden, werden sie die Schenkel des Winkels genannt.
10. Ist eine Gerade so auf einer anderen errichtet, dass die nebeneinander liegenden Winkel gleich sind, dann ist jeder der Winkel ein rechter Winkel und die errichtete Gerade eine Senkrechte zur andern.

[3] Ein ebener Winkel ist also dort wo sich zwei Linien (Kurven) schneiden. Es gibt aber keinen 0° oder 180° Winkel.

...

15. Ein Kreis ist eine ebene, von einer einzigen Linie [die Umfang oder Bogen heißt] umfasste Figur mit der Eigenschaft, dass alle von einem innerhalb der Figur gelegenen Punkt bis zur Linie [zum Umfang des Kreises] laufende Strecken einander gleich sind.

...

19. Geradlinige Figuren sind solche, die von Strecken umfasst werden, dreiseitige die von drei, vierseitige die von vier, vielseitige die von mehr als vier Strecken umfassten.

...

23. Parallel sind gerade Linien, die in derselben Ebene liegen und dabei, wenn man sie nach beiden Seiten ins unendliche verlängert, auf keiner einander treffen."

Was bei Euklid hier "gleich" heißt, würde in der Modernen Sprache "kongruent" heißen. Wir betrachten das also als eine Äquivalenzrelation.

Postulate und Allgemeine Regeln

Diese sind der Startpunkt der ganzen logischen Struktur. Wenn man klassisch denkt, dass es eine einzige "wahre" Geometrie die die Welt in ihrer idealen Form beschreibt, dann kann man diese als selbstverständlich/offensichtlich betrachten. Wenn man den modernen Standpunkt nimmt, wo man euklidische Geometrie als eine abstrakte mathematische Theorie betrachtet, diese sind einfach zufällig ausgewählte Startpunkte der Theorie. Man fragt sich über ihre "absolute Wahrheit" nicht. Man behauptet nur, dass *wenn* die Axiome gelten, dann sind die Theoreme auch wahr. Später kann man nach dessen Relevanz fragen, aber das ist schon Philosophie.
Man kann den Unterschied zwischen Postulate und Allgemeine Regeln so sehen: die Postulate behandeln geometrische Aussagen, während die Allgemeine Regeln universell sind - diese letzten sind wahr für die ganze Wissenschaft. Eine andere Teilung ist: Die Postulate erlauben eine geometrische Errichtung; die Regeln sagen, dass etwas war ist.

Postulate

1. Von einem beliebigen Punkt zu einem anderen ist eine gerade Strecke zu ziehen,
2. und eine gerade Strecke ist beliebig verlängerbar,
3. und um einen beliebigen Punkt ist mit beliebigem Radius ein Kreis beschreibbar,
4. und alle rechten Winkel sind unter sich gleich,
5. und zwei Geraden, die von einer Geraden geschnitten werden, wobei die innen liegenden beiden Winkel zusammen kleiner als zwei rechte sind, treffen sich dort, wonach die Winkel liegen.

Postulat 5. ist verwickelter als die anderen vier. Es klingt mehr als Satz und nicht als Axiom. Für mehr als 2000 Jahre haben Mathematiker (und nicht nur) ohne Erfolg versucht dieses als Folgerung der anderen vier zu beweisen. Das Zeigt Euklids Genie, diese Aussage als Postulat mitzunehmen. „Die Jahrhunderte währende Diskussion mündete letztlich in die sensationelle Entdeckung der nicht-euklidischen Geometrien (Gauss, Lobatschewski, Bolyai). Und genau aus diesen nicht-euklidischen Geometrien erwuchs dann später das mathematische Gerüst der Allgemeinen Relativitätstheorie Einsteins."

Allgemeine Regeln

1. Das was demselben gleich ist, ist unter sich gleich,
2. und Gleichem das Gleiche hinzugefügt ergibt Gleiches,
3. und Gleichem das Gleiche weggenommen ergibt Gleiches,
4. *und Ungleichem das Gleiche hinzugefügt ergibt Ungleiches,*
5. *und Ungleichem das Gleiche weggenommen ergibt Ungleiches,*
6. *und Gleiches verdoppelt ergibt Gleiches,*
7. *und Gleiches halbiert ergibt Gleiches.*
8. Das was übereinstimmt ist gleich.
9. Das Ganze ist größer als ein Teil davon.
10. *Zwei Gerade schließen keine Fläche ein.*

Die Regeln 4.-7. und 10. kommen in früheren Ausgaben der *Elementen* nicht vor. Spätere Editoren haben diese hinzugefügt, weil sie explizit in Beweise vorkommen.

4.1.3 Schnitte von Kreise und Geraden

Manchmal bezieht sich Euklid auf Intuition, oder Aussagen die offensichtlich vom Anschauen der Bilder sind, aber die keine Axiome sind. Das kommt schon im Satz I.1 vor.

Satz 4.1 (Buch I. Satz 1)**.** *Auf einer gegebenen geraden Strecke ein gleichseitiges Dreieck errichten.*

Beweis-Skizze: Sei $[AB]$ die gegebene Strecke. Man zeichne die Kreise K_1, bzw. K_2, mit Zentrum A, bzw. B, und beide mit Radius $|AB|$. Sei einer der Schnittpunkte von K_1 mit K_2 der Punkt C. Dann ist $\triangle ABC$ ein gleichseitiges Dreieck. Q.E.D.

Was fehlt hier? Wir wissen nicht ob sich die zwei Kreise schneiden. Es ist klar wenn man sich das Bild anschaut, aber man kann nichts explizites anwenden. Es gibt zwei Probleme hier:

1. Die relative Position der Kreise.
2. Warum gibt es ein Schnittpunkt (wenn die Position „richtig“ ist).

„Richtig“ heißt ein Teil von K_2 liegt im Inneren von K_1, und ein Teil außerhalb.

Wir könnten den Zwischenwertsatz anwenden: $f : [0,1] \longrightarrow \mathbb{R}$, stetig, mit $f(0) < 0$ und $f(1) > 0$, dann gibt es eine $x \in [0,1]$ mit $f(x) = 0$. Aber Euklid kannte das nicht (stetige Funktionen und die reelle Zahlen wurden erst im 19 Jhd. genau definiert.) Die Sache wird schwieriger wenn man das Problem in der Ebene $\mathbb{Q}^2$ betrachtet: wenn $A = (0,0)$ und $B = (1,0)$, dann muss der Punkt C Koordinaten $(\frac{1}{2}, \frac{\sqrt{3}}{2})$ haben. Anders gesagt, die zweite Koordinate ist gezwungen die Gleichung $4x^2 - 3 = 0$ zu erfüllen, und das ist über den $\mathbb{Q}$ nicht lösbar. Das heißt, dass die euklidische Geometrie entweder die reelle Zahlen in den Axiome einbauen muss, oder Dedekinds Axiom nehmen soll.

4.1.4 Superposition

Es gibt auch Ungenauigkeiten in dem Beweis folgendes Satzes. Dieser Satz wird von David Hilbert als Axiom (Seite-Winkel-Seite) gewählt.

Satz 4.2 (I.4)**.** *Sind bei zwei Dreiecken zwei Seiten des einen gleich zwei Seiten des andern und ist auch der von ihnen eingeschlossene Winkel gleich, dann stimmen die Seiten überein, auf denen die Dreiecke errichtet sind, und die errichteten Dreiecke, somit die übrigen Winkel, die diesen Seiten gegenüber liegen.*

Im Beweis bringt man einen Punkt auf dem anderen und man liegt die Strecken auf Strecken. Das zeigt erst, dass die 8. Allgemeine Regel auch umgekehrt wirken soll. Eine Kritik an diesem Satz kam schon in 1557 von Jacques Peletier: „Satz I.4. gehört zu den Grundsätzen, weil der Beweis durch Superposition zur Mechanik, und nicht zur Mathematik gehört". Euklid erklärt nicht was *Bewegungen* (Translationen, Drehungen, Spiegelungen) sind und warum es *genug* davon gibt. Genug heißt in diesem Fall:

1. Man kann jeden Punkt zu jedem anderen bringen.
2. Man kann um jeden Punkt drehen, sodass jeder Radius an dem Punkt zu jedem anderen Radius an dem Punkt gebracht werden kann.
3. Man kann an jeder Gerade spiegeln.

Bewegungen werden ab dem 19. Jahrhundert durch Wirkungen von *Gruppen* beschrieben. Diese spielen jetzt eine zentrale Rolle in der Geometrie und in der Physik. Das *Erlanger Programm* von Felix Klein will Geometrie durch die erlaubten Gruppenwirkungen studieren.

4.1.5 Flächeninhalt

Satz 4.3 (I.35)**.** *Parallelogramme, auf derselben Grundseite errichtet, zwischen denselben Parallelen sind gleich.*

Satz 4.4 (I.37)**.** *Dreiecke, auf derselben Grundseite errichtet, zwischen denselben Parallelen sind gleich.*

Hier meint Euklid mit "gleich", dass diese Figuren denselben[4] Flächeninhalt haben. Was ist aber der Flächeninhalt? Es ist eine Funktion, die jeder Figur eine reelle Zahl zuordnet. Intuitiv, ist es das Produkt zweier Längen. Wir sollten das aber als undefiniert betrachten. Es ist eine Äquivalenzrelation (also eine reflexive, symmetrische und transitive binäre Relation), die noch folgende Axiome erfüllt:

1. Kongruente Figuren haben denselben Flächeninhalt.
2. Wenn man Paare von Figuren mit gleichem Flächeninhalt *addiert* (das heißt, nebeneinanderstellt, ohne das sich diese schneiden) dann haben diese neue Figuren gleichen Flächeninhalt.
3. Dasselbe gilt wenn man Figuren mit gleichem Flächeninhalt weg nimmt.
4. Hälften von Figuren (zwei kongruente Teile) haben den halben Flächeninhalt.
5. Das Ganze ist größer als ein Teil davon.

Interessant ist noch, dass Euklid folgende Konstruktion gleich vor Pythagoras Satz stellt:

Satz 4.5 (I.46)**.** *Über einer geraden Strecke das Quadrat beschreiben.*

[4] "Gleich" heißt nicht immer dasselbe in Euklids Elemente.

Pythagoras Satz spricht über Quadrate, und Euklid spricht über keine Figuren die man nicht mit Zirkel und Lineal errichten kann. Zum Beispiel, gibt es kein Erwähnen vom gleichmäßigen Siebeneck in den *Elementen*; diese Figur "existiert" nicht.

Satz 4.6 (I.47 - Satz von Pythagoras)**.** *Im rechtwinkligen Dreieck ist das Quadrat über der dem rechten Winkel gegenüber liegenden Seite gleich den Quadraten über den Seiten zusammen, die ihn einschließen.*

4.2 Axiomatische Geometrie

Man hat zwei Möglichkeiten sich der klassischen ebenen Geometrie, der so genannten *euklidischen Geometrie*, mit moderner[5] mathematischer Genauigkeit anzunähern. Man kann den axiomatischen (oder synthetischen) Weg wählen und einfach von Punkten und Geraden sprechen, die nach gewissen Regeln (Axiomen) interagieren. Der andere Ansatz ist als Punkte die Elemente von $\mathbb{R}^2$ zu wählen, und als Geraden die Lösungsmengen linearer Gleichungen der Form $ax + by + c = 0$ mit $(a, b) \neq (0, 0)$ zu setzten. Der zweite Ansatz ist ein Teil der linearen Algebra und wir werden es hier nur als Modell betrachten. Für den Rest dieses Kapitels werden wir einige Ideen der synthetischen Annäherung betrachten.

Im Jahr 1899 hat David Hilbert Axiome, mit denen man die euklidische Geometrie mit moderner Genauigkeit aufbauen kann, vorgeschlagen. Diese kommen in drei Gruppen zusammen mit zwei weiteren Axiomen: Inzidenzaxiome, Anordnungsaxiome, Kongruenzaxiome, das Parallelenaxiom und das Kreisaxiom. In dem axiomatischen Ansatz der klassischen Geometrie sind auch das archimedische Axiom und das Axiom von Dedekind zu betrachten.

Leider kann man nicht immer zeigen, dass Axiomen-Systeme (formale Systeme) wiederspruchsfrei sind, das heißt, dass man nicht sowohl einen Satz als auch seine Negation beweisen kann. Kurt Gödels Erste Unvollständigkeitssatz besagt, dass es in hinreichend starken widerspruchsfreien Systemen immer unbeweisbare Aussagen gibt. Der Zweite Unvollständigkeitssatz besagt, dass hinreichend starke widerspruchsfreie Systeme ihre eigene Widerspruchsfreiheit nicht beweisen können. Relative Wiederspruchsfreiheit eines Axiomen-Systems $\mathcal{S}$ gilt, wenn es eine mathematische Theorie $\mathcal{T}$ gibt, in der man ein Modell für $\mathcal{S}$ bauen kann. Dann, wenn $\mathcal{T}$ wiederspruchsfrei ist, ist auch $\mathcal{S}$ wiederspruchsfrei. Zum Beispiel, wenn wir an die reelle Zahlen „glauben", dann müssen wir auch an Hilberts Axiome „glauben".

Die elementaren Objekte der synthetischen Geometrie sind Punkte und Geraden. Diese sind nicht definiert, sondern *gegeben*. Das heißt, es wird eine Menge $\mathcal{X}$ gegeben, dessen Elemente wir **Punkte** nennen, und eine Untermenge der Menge aller Teilmengen von $\mathcal{X}$: $\mathcal{G} \subseteq 2^{\mathcal{X}}$, dessen Elemente wir **Geraden** nennen. Wir sagen also nicht **was** diese sind, nur **dass** es diese gibt. Ein solches geordnetes Paar $(\mathcal{X}, \mathcal{G})$ heißt **Inzidenzstruktur** (oder **Punkten-Geraden Konfiguration**). Inzidenzstrukturen, die gewisse Axiome erfüllen sind die unterliegenden Objekte der axiomatischen ebenen Geometrie.

4.2.1 Inzidenzaxiome

Sei $(\mathcal{X}, \mathcal{G})$ eine Inzidenzstruktur. Wenn ein Punkt P zu einer Geraden g gehört, dann sagen wir auch, dass P auf g **liegt**, oder, dass die Gerade g durch P **läuft**. Weil jede Gerade eine *Menge* von Punkten

[5] Der Standard für Präzision in der Mathematik hat sich mit der Zeit verändert. Die "moderne" Mathematik beginnt in dem 19. Jahrhundert.

https://en.wikipedia.org/wiki/History_of_mathematics#19th_century

https://de.wikipedia.org/wiki/Geschichte_der_Mathematik#Mathematik_im_19._Jahrhundert

ist, schreiben wir wie bis jetzt gewohnt $P \in g$ oder $P \notin g$. Die Punkte $P_1, \dots, P_n \in \mathcal{X}$ mit $n \geqslant 2$ heißen **kollinear**, wenn eine Gerade $g \in \mathcal{G}$ existiert, sodass

$$P_i \in g \quad \forall\, i = 1, \dots, n.$$

Die Punkte $P_1, \dots, P_n$ heißen **nicht kollinear**, wenn diese nicht kollinear sind. Also wenn es keine Gerade gibt, die *alle* enthält. Anders formuliert:

$$P_1, \dots, P_n \text{ sind nicht kollinear} \iff \forall\, g \in \mathcal{G} \quad \exists\, i \in \{1, \dots, n\}, \text{ sodass } P_i \notin g.$$

Definition 4.7. Eine Inzidenzstruktur $(\mathcal{X}, \mathcal{G})$ wird **Inzidenzgeometrie** genannt, wenn die folgenden drei Axiome erfüllt sind:

I1. Für zwei verschiedene Punkte $A, B \in \mathcal{X}$, gibt es genau eine Gerade $g \in \mathcal{G}$ mit $A, B \in g$.

I2. Jede Gerade enthält mindestens zwei Punkte.

I3. Es gibt mindestens drei nicht kollineare Punkte.

Die eindeutige Gerade aus **I1.**, die A und B enthält wird mit AB bezeichnet.

Aus diesem bescheidenen Anfang, kann man nicht viel erwarten. Man kann aber schon einige Sätze beweisen.

Satz 4.8. *Zwei verschiedene Geraden g, h einer Inzidenzgeometrie $(\mathcal{X}, \mathcal{G})$ schneiden sich höchstens in einem Punkt.*

Beweis-Skizze: Wenn $A, B \in g \cap h$ mit $A \neq B \overset{\text{I1.}}{\Longrightarrow} g = h = AB$. Q.E.D.

Ein **Modell** für ein axiomatisches System ist eine Realisierung der undefinierten Begriffe in einem Sonderfall, sodass die Axiome erfüllt sind. Man kann daran als Beispiel denken.

Beispiele: Wir haben folgende Beispiele und nicht-Beispiele.

1. Existiert eine Inzidenzgeometrie $(\mathcal{X}, \mathcal{G})$ mit $\mathcal{G} = \emptyset$ oder mit $\mathcal{X} = \emptyset$?[6]

2. Drei Punkte und drei Geraden: $\mathcal{X} = \{A, B, C\}, \quad \mathcal{G} = \big\{\{A, B\}, \{A, C\}, \{B, C\}\big\}$.

3. Fünf Punkte und zehn Geraden: $\mathcal{X} = \{A, B, C, D, E\}$, $\mathcal{G} = \big\{g \subseteq \mathcal{X} \;:\; |g| = 2\big\}$.

4. Das Musterbeispiel ist $\mathcal{X} = \mathbb{R}^2 = \{(x, y) \;:\; x, y \in \mathbb{R}^2\}$ mit

$$\mathcal{G}_{\mathbb{R}^2} = \big\{\{(x, y) \in \mathbb{R}^2 \;:\; ax + by + c = 0\} \;:\; a, b, c \in \mathbb{R} \text{ und } (a, b) \neq (0, 0)\big\}.$$

Wir bezeichnen diese Inzidenzstruktur mit

$$\mathbb{A}^2_{\mathbb{R}} := (\mathbb{R}^2, \mathcal{G}_{\mathbb{R}^2}).$$

Um die Inzidenzaxiome zu überprüfen werden wir (minimale) Kenntnisse über lineare Gleichungssysteme annehmen. (Siehe 4.6.) Wichtig ist zu bemerken (siehe Bemerkung 4.79), dass verschiedene

[6] Wenn $\mathcal{X} = \emptyset$, dann ist **I3.** verletzt. Wenn **I3.** erfüllt ist, dann existieren auch zwei verschiedene Punkte, und somit nach **I1.** auch mindestens eine Gerade. Also $\mathcal{G} \neq \emptyset$.

Tripel (a, b, c) und (a', b', c') genau dann dieselbe Gleichung definieren, wenn ein $\lambda \in \mathbb{R} \setminus \{0\}$ existiert mit

$$(a, b, c) = (\lambda a', \lambda b', \lambda c').$$

I1. Seien $P = (p_1, p_2) \neq Q = (q_1, q_2)$ zwei verschiedene Punkte in $\mathbb{R}^2$. Wir wollen eine lineare Gleichung $ax + by + c = 0$ finden, die sowohl von P als auch von Q erfüllt ist. Dann müssen wir noch zeigen, dass wenn zwei verschiedene Gleichungen diese Eigenschaft haben, dann sind deren Lösungsmengen gleich. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass

$$p_1 \neq q_1.$$

Wir suchen also $a, b, c \in \mathbb{R}$, mit $(a, b) \neq (0, 0)$, sodass:

$$\begin{cases} \mathbf{G}_P: & ap_1 + bp_2 + c &= 0, \\ \mathbf{G}_Q: & aq_1 + bq_2 + c &= 0. \end{cases}$$

Wir können die Differenz der zwei Gleichungen betrachten und bekommen

$$\mathbf{G}_P - \mathbf{G}_Q: \quad (p_1 - q_1)a + (p_2 - q_2)b = 0$$

Weil $p_1 \neq q_1$ dürfen wir durch $p_1 - q_1$ teilen und bekommen dann:

$$\mathbf{G}': \quad a = -\frac{p_2 - q_2}{p_1 - q_1} b.$$

Wir bezeichnen mit $\alpha = -\frac{p_2 - q_2}{p_1 - q_1}$ und setzen[7] $a = \alpha \cdot b$ in $\mathbf{G}_P$ ein.

$$\mathbf{G}_P - p_1\mathbf{G}': \quad p_1(\alpha \cdot b) + p_2 b + c = 0$$

Wir bekommen daraus $c = -(p_2 + p_1\alpha) \cdot b$. Wir bezeichnen mit $\gamma = -(p_2 + p_1\alpha)$ und bekommen somit für jedes $\beta \in \mathbb{R}$ eine Lösung des Gleichungssystems:

$$(a, b, c) = (\alpha\beta, \beta, \gamma\beta),$$

wobei $\alpha, \gamma \in \mathbb{R}$ fixiert und von P und Q abhängig sind. Also hat jede Gleichung die sowohl von P als auch von Q erfüllt wird die Form:

$$(\alpha\beta)x + \beta y + (\gamma\beta) = 0 \qquad \text{mit } \beta \in \mathbb{R}.$$

Wenn $\beta \neq 0$, dann ist das die Gleichung einer Gerade. Und nach nach Bemerkung 4.79, handelt es sich um eine eindeutige Gerade.

I2. Jede Gerade ist die Lösungsmenge einer Gleichung der Form $ax + by + c = 0$ mit $(a, b) \neq (0, 0)$. Wir können annehmen, dass $a \neq 0$. Dann, wenn $y = 0$ folgt $x = -\frac{c}{a}$ und wenn $y = 1$, $x = -\frac{b+c}{a}$. Wir haben also mindestens zwei Lösungen, also mindestens zwei Punkte auf jeder Gerade. **I3.** Die Punkte $(0, 0), (1, 0), (0, 1)$ sind nicht kollinear. Wenn alle drei die Gleichung $ax + by + c = 0$ erfüllen, dann folgt

$$\begin{aligned} 0 + 0 + c &= 0, \\ a + 0 + c &= 0, \\ 0 + b + c &= 0. \end{aligned}$$

[7] Formal gesehen, betrachten wir also $\mathbf{G}_P - p_1\mathbf{G}'$, deren Lösungsmenge die gesuchte Lösungsmenge enthält.

Also $a = b = c = 0$, und das ergibt per Definition nicht die Gleichung einer Gerade. □

Es lohnt sich Geraden in $\mathbb{R}^2$ auch anders zu beschreiben. Für zwei unterschiedliche Punkte $A = (a_1, a_2)$ und $B = (b_1, b_2)$ ist die eindeutig bestimmte Gerade durch A und B:

$$AB = \{tA + (1-t)B \ : \ t \in \mathbb{R}\}.$$

Man kann einfach überprüfen, dass diese ist die Lösungsmenge einer linearen Gleichung, also eine Gerade im Sinne der vorherigen Definition, ist.

5. Wir haben in dem vorherigen Beispiel nur die elementaren algebraischen Eigenschaften von $\mathbb{R}$ verwendet. Das heißt, die Assoziativität und Kommutativität der Addition und der Multiplikation, die Distributivität, die Existenz von 0,1, die Existenz von $-a \in \mathbb{R}$ mit $a + (-a) = 0$ für alle $a \in \mathbb{R}$ und die Existenz von $\frac{1}{a}$ für alle $a \neq 0$ in $\mathbb{R}$. Das heißt wir könnten $\mathbb{R}$ mit jeder "Zahlenstruktur", die diese Eigenschaften hat, ersetzen: $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ mit p eine Primzahl. Es würde aber nicht mit $\mathbb{Z}$ funktionieren. Was würde schief laufen?

6. Wenn $\mathcal{X}$ die Menge der Punkte auf der Kugel und die Geraden die große Kreise (Schnitt von Ebenen durch den Mittelpunkt mit der Kugel) sind, dann haben wir ein nicht-Beispiel. Warum?

Definition 4.9. Seien $(\mathcal{X}, \mathcal{G})$ und $(\mathcal{X}', \mathcal{G}')$ zwei Inzidenzstrukturen. Ein **Isomorphismus von Inzidenzstrukturen** ist eine bijektive Abbildung $\varphi : \mathcal{X} \longrightarrow \mathcal{X}'$ mit der Eigenschaft, dass Geraden auf Geraden abgebildet werden. Das heißt $g \in \mathcal{G} \iff \varphi(g) \in \mathcal{G}'$. Wir sagen, dass die Inzidenzstrukturen $(\mathcal{X}, \mathcal{G})$ und $(\mathcal{X}', \mathcal{G}')$ **isomorph** sind, wenn es einen Isomorphismus von Inzidenzstrukturen zwischen den beiden gibt. Wir schreiben dann

$$(\mathcal{X}, \mathcal{G}) \simeq (\mathcal{X}', \mathcal{G}').$$

Bemerkung 4.10. Wenn $\varphi : \mathcal{X} \longrightarrow \mathcal{X}'$ ein Isomorphismus von Inzidenzstrukturen ist, dann erfüllt $\mathcal{X}$ eines der obigen Axiome wenn und nur wenn $\mathcal{X}'$ dasselbe Axiom erfüllt. Insbesondere, wenn $(\mathcal{X}, \mathcal{Q})$ eine Inzidenzgeometrie oder eine affine Ebene ist, die isomorph zu $(\mathcal{X}', \mathcal{G}')$ ist, dann ist $(\mathcal{X}', \mathcal{G}')$ auch eine Inzidenzgeometrie beziehungsweise eine affine Ebene.

Beispiel 4.11. 1. Bis auf Isomorphismus gibt es nur eine Inzidenzgeometrie mit 3 Punkten. Aus **I3.** folgt, dass es keine Gerade mit 3 Punkten gibt. Aus **I1.** sind alle Mengen mit 2 Punkten Geraden, und aus **I2.** sind diese die einzigen.

2. Es gibt bis auf Isomorphismus zwei Modelle für eine Inzidenzgeometrie mit 4 Punkten: $\mathbb{A}^2_{\mathbb{Z}_2}$ und der *Kegel* über einer Geraden mit 3 Punkten:

$$\mathcal{X} = \{A, B, C, D\} \text{ und } \mathcal{G} = \Big\{\{A, B, C\}, \{A, D\}, \{B, D\}, \{C, D\}\Big\}.$$

Definition 4.12. Zwei Geraden $g, h \in \mathcal{G}$ heißen **parallel**, wenn $g = h$ oder $g \cap h = \emptyset$. Wir schreiben

$$g \parallel h.$$

Das Parallelenaxiom von Euklid war etwas indirekt formuliert:

Parallelenaxiom von Euklid: *Zwei Geraden, die von einer Geraden geschnitten werden, wobei die innen liegenden beiden Winkel zusammen kleiner als zwei rechte sind, treffen sich dort, wonach die Winkel liegen.*

Wir dürfen das in einer Inzidenzgeometrie nicht so formulieren, weil "Winkel" (also auch "rechte Winkel"), "innen liegend", "kleiner als" für Winkel, nicht definiert wurden. Dieses Axiom wurde von Playfair[8] umformuliert. Er hat gezeigt, dass, sobald die obigen Begriffe "richtig" (das heißt im Sinne der *Elementen* von Euklid) eingeführt sind, jedes der folgenden Axiome zu dem Parallelenaxiom von Euklid äquivalent sind.

P. $\forall\, A \in \mathcal{X}$ und $\forall\, g \in \mathcal{G}$ gibt es **höchstens** eine Gerade g' mit $A \in g'$ und $g \parallel g'$.

P$^+$. $\forall\, A \in \mathcal{X}$ und $\forall\, g \in \mathcal{G}$ gibt es **genau** eine Gerade g' mit $A \in g'$ und $g \parallel g'$.

Offensichtlich folgt aus **P$^+$.** auch **P.**. Obwohl diese zwei Axiome unter der Vorgabe aller Inzidenz-, Anordnungs-, und Kongruenzaxiome äquivalent sind, sind diese in einer Inzidenzgeometrie nicht äquivalent.

Beispiele:

1. $\mathcal{X} = \{A, B, C\}$ mit $\mathcal{G} = \big\{\{A, B\}, \{A, C\}, \{B, C\}\big\}$ erfüllt **P.**, aber nicht **P$^+$.**.
2. $\mathcal{X} = \{A, B, C, D, E\}$ mit $\mathcal{G} = \{g \in 2^{\mathcal{X}} \;:\; \sharp g = 2\}$ erfüllt keine der beiden.

Eine wichtige Frage für ein Axiomen-System ist ob diese unabhängig voneinander sind. Das direkt zu beweisen ist aussichtslos. Wir suchen also ein Modell wo alle Axiome außer eines gelten.

Satz 4.13. *Die Axiome **I1.**, **I2.**, **I3.** und **P.** sind unabhängig.*

Beweis-Skizze: $\boxed{\textbf{I1.}+\textbf{I2.}+\textbf{I3.} \not\Rightarrow \textbf{P.}}$ Fünfeck mit Diagonalen
$\boxed{\textbf{I1.}+\textbf{I2.}+\textbf{P.} \not\Rightarrow \textbf{I3.}}$ $\mathcal{X} = \{A, B\}$ und $\mathcal{G} = \{\mathcal{X}\}$.
$\boxed{\textbf{I1.}+\textbf{I3.}+\textbf{P.} \not\Rightarrow \textbf{I2.}}$ $\mathcal{X} = \{A, B, C\}$ und $\mathcal{G} = \{\{A, B\}, \{A, C\}, \{B, C\}, \{A\}\}$. ($\{A\}$ ist die einzige Parallele zu BC durch A)
$\boxed{\textbf{I2.}+\textbf{I3.}+\textbf{P.} \not\Rightarrow \textbf{I1.}}$ $\mathcal{X} = \{A, B, C\}$ und $\mathcal{G} = \emptyset$. $\boxed{\textbf{I1.}+\textbf{I3.}+\textbf{P.} \Rightarrow \textbf{I2.}}$ Q.E.D.

Das ist nicht mehr der Fall wenn wir **P$^+$.** statt **P.** nehmen. Tatsächlich kann man zeigen, dass **I1.**, **I3.** und **P$^+$.** implizieren auch **I2.**

4.2.2 Die affine Ebene

Definition 4.14. Eine **affine Ebene** ist eine Inzidenzstruktur, die die Axiome **I1.**, **I2.**, **I3.**, **P$^+$.** erfüllt.

Satz 4.15. *Wenn $(\mathcal{X}, \mathcal{G})$ eine Inzidenzgeometrie ist, dann*

$$\textbf{P.} \iff \parallel \text{ ist eine Äquivalenzrelation auf } \mathcal{G}.$$

Beweis-Skizze: Es ist klar, dass $g \parallel g$ und $g \parallel h \Leftrightarrow h \parallel g$ für alle $g, h \in \mathcal{G}$ gelten. Nur die Transitivität fehlt also.
$\boxed{\Rightarrow}$ Seien $g \parallel h$ und $h \parallel l$. Wenn $g \nparallel l$, dann $\exists P \in g \cap l$. Da es aber nur eine einzige Parallele zu h durch P gibt, folgt $g = l$.

[8] Rev. Prof. John Playfiar - 1748-1819, Church of Scotland minister.

$\boxed{\Leftarrow}$ Sei $P \notin g$ und h, l zwei Geraden durch P, die parallel zu g sind. Aus der Symmetrie und der Transitivität folgt also, dass auch $h \parallel l$. Da $P \in h \cap l$, folgt $h = l$. Q.E.D.

Korollar 4.16. In einer affinen Ebene ist Parallelität transitiv. Das heißt, wenn $(\mathcal{X}, \mathcal{G})$ ist eine affine Ebene, dann gilt für alle $g, h, \ell \in \mathcal{G}$:

$$g \parallel h \,\text{und}\, h \parallel \ell \Rightarrow g \parallel \ell.$$

User Musterbeispiel $\mathbb{A}^2_{\mathbb{R}}$, sowie $\mathbb{A}^2_{\mathbb{Q}}$, $A^2_{\mathbb{C}}$, $A^2_{\mathbb{Z}/p\mathbb{Z}}$, sind alle affine Ebenen. Zum Glück haben wir diese mit schon $\mathbb{A}$, wie **a**ffine Ebene, bezeichnet. Wir zeigen das jetzt für $\mathbb{R}$. Man sollte jetzt beobachten welche Eigenschaften von $\mathbb{R}$ in dem Beweis benutzt werden. Als erstes interpretieren wir die Parallelität bezüglich der Koeffizienten der Gleichungen die die Geraden definieren.

Lemma 4.17. *Seien $g, g' \in \mathcal{G}_{\mathbb{R}^2}$ zwei Geraden gegeben durch die Gleichungen $ax + by + c = 0$ und $a'x + b'y + c' = 0$. Es gilt:*

$$g \parallel g' \iff \exists\ \lambda \in \mathbb{R} \setminus \{0\} \text{ mit } (a, b) = (\lambda a', \lambda b').$$

Beweis-Skizze: $\boxed{\Rightarrow}$ Wenn $g = g'$, dann folgt das Ergebnis aus Satz 4.83.

Wenn $g \cap g' = \emptyset$, dann muss ich es noch sauber schreiben. Die Schritte sind aber:
$a = 0 \Rightarrow a' = 0$ und also $b \neq 0 \neq b'$. Dann ist es einfach: $\lambda = \frac{b}{b'}$.
$a \neq 0 \Rightarrow a' \neq 0$ und $\lambda = \frac{a}{a'}$.

$\boxed{\Leftarrow}$ Wenn $0 \neq \lambda \in \mathbb{R}$ existiert mit $(a, b) = (\lambda a', \lambda b')$, dann bekommen wir

$$\left\{\begin{array}{rcl} ax + by + c & = & 0 \\ a'x + b'y + c' & = & 0 \end{array}\right. \Leftrightarrow \left\{\begin{array}{rcl} \lambda a'x + \lambda b'y + c & = & 0 \\ \lambda a'x + \lambda b'y + \lambda c' & = & 0 \end{array}\right.$$

Also ist die Lösungsmenge in der Lösungsmenge der Differenz der Gleichungen enthalten. Das heißt in

$$\{(\alpha, \beta) \in \mathbb{R}^2 \ : \ c - \lambda c' = 0\}$$

Wenn $c \neq \lambda c'$, dann ist die Lösungsmenge, und somit der Schnitt $g \cap g'$, die leere Menge.
Wenn $c = \lambda c'$, dann sind die zwei Gleichungen nach Satz 4.83 äquivalent, also $g = g'$.
In beiden Fällen bekommen wir also, dass $g \parallel g'$. Q.E.D.

Satz 4.18. *Die Inzidenzstruktur $\mathbb{A}^2_{\mathbb{R}}$ ist eine affine Ebene.*

Beweis-Skizze: Wir haben schon in Beispiel 4.2.1 **4.** bewiesen, dass es eine Inzidenzgeometrie ist. Wir müssen also nur noch $\mathbf{P}^+$**.** beweisen.

Sei g eine beliebige Gerade gegeben durch $ax + by + c = 0$ und sei $P = (p_1, p_2) \in \mathbb{R}^2$ ein beliebiger Punkt. Wir behaupten, dass die Gerade g' gegeben durch

$$ax + by - (p_1 a + p_2 b) = 0 \tag{4.1}$$

P enthält parallel zu g ist. Offensichtlich erfüllt (p_1, p_2) die Gleichung (4.1). Wenn ein $Q \in g \cap g'$ existiert, dann haben wir

$$\left\{\begin{array}{rcl} q_1 a + q_2 b + c & = & 0, \\ q_1 a + q_2 b - (p_1 a + p_2 b) & = & 0. \end{array}\right.$$

Aus der Differenz der Gleichungen bekommen wir

$$p_1 a + p_2 b + c = 0.$$

Also $P \in g$ und $g' = g$. Das heißt, dass $g \parallel g'$.
Wir müssen noch die Eindeutigkeit zeigen. Seien h und h' parallele Geraden zu g mit $P \in h$ und $P \in h'$. Nach Lemma 4.17 haben die Gleichungen dieser Geraden die Form

$$h: \quad \lambda a \cdot x + \lambda b \cdot y + d = 0 \qquad \text{und} \qquad h': \quad \lambda' a \cdot x + \lambda' b \cdot y + d' = 0,$$

mit $\lambda, \lambda' \in \mathbb{R} \setminus \{0\}$. Wieder nach Lemma 4.17 folgt $h \parallel h'$. Da aber $P \in h \cap h'$ ist der Schnitt nicht leer. Es muss also $h = h'$ gelten. Q.E.D.

Ich betone hier, dass es nicht eine einzige affine Ebene gibt. Zum Beispiel $\mathbb{A}^2_{\mathbb{R}}$ und $\mathbb{A}^2_{\mathbb{Q}}$ sind zwei nicht isomorphe[9] affine Ebenen. Es gibt auch affine Ebenen mit endlich viele Punkten. Zum Beispiel $\mathbb{A}^2_{\mathbb{Z}/p\mathbb{Z}}$ für jede Primzahl $p \in \mathbb{Z}$. Es gibt auch weitere, aber die Anzahl der Punkte kann nicht beliebig sein.

Satz 4.19. *Wenn $(\mathcal{X}, \mathcal{G})$ eine affine Ebene ist mit $\sharp\mathcal{X} < \infty$, dann existiert $n \in \mathbb{N}_{>1}$ mit $\sharp\mathcal{X} = n^2$.*

Beweis-Skizze: Wir lassen den Beweis dafür als Übung erstmals. Die schritte sind:

1. Wenn g und g' Geraden in einer affinen Ebene sind, dann existiert eine Bijektion $\varphi : g \longrightarrow g'$.
2. Für jede Gerade g in der affinen Ebene $(\mathcal{X}, \mathcal{G})$ gilt $\mathcal{X} = \bigcup_{h \in \mathcal{G}, h \parallel g} h$.
3. Wenn eine affine Ebene eine Gerade g mit $\sharp g = n$ enthält, dann gilt $\sharp\mathcal{X} = n^2$.

Q.E.D.

4.2.3 Anordnungs-Axiome

Sei $(\mathcal{X}, \mathcal{G})$ eine Inzidenzgeometrie. Das heißt, dass die Axiome **I1.-I3.** für $(\mathcal{X}, \mathcal{G})$ gelten, aber das Axiom **P** nicht unbedingt. Für Tripeln von Punkten A, B, C führen wir die Relation

$$B \textbf{ liegt zwischen } A \textbf{ und } C$$

ein. Wir schreiben dafür A_B_C, und verlangen, dass folgende Axiome gelten:

A1. Wenn A_B_C, dann gilt auch C_B_A und A, B, C sind unterschiedliche **kollineare** Punkte.

A2. Wenn $A, B \in \mathcal{X}$ mit $A \neq B \Rightarrow \exists\, C \in \mathcal{X}$ mit A_B_C.

A3. Wenn A, B, C verschieden und kollinear sind, dann genau einer liegt zwischen den anderen zwei.

A4. (Pasch) Seien A, B, C drei nichtkollineare Punkte, und g eine Gerade durch keinen von denen. Wenn $\exists D \in g$ mit A_D_B, dann $\exists\, E \in g$ mit entweder A_E_C oder B_E_C (aber nicht beide).

Eine Inzidenzstruktur die die Axiome **I1.-I3.** und **A1.-A4.** erfüllt heißt **Geordente Geometrie**.

[9] Die Punktmenge $\mathbb{Q}^2$ ist abzählbar, aber $\mathbb{R}^2$ ist überabzählbar. Es gibt also keine Bijektionen zwischen den beiden.

Definition 4.20. Wenn $A \neq B$ zwei Punkte sind, definieren wir die **offene Strecke**

$$(AB) := \{C \in \mathcal{X} \mid A\_\_C\_\_B\}.$$

Die **abgeschlossene Strecke** ist definiert als

$$[AB] := (AB) \cup \{A, B\}.$$

Lemma 4.21. *Sei $(\mathcal{X}, \mathcal{G})$ eine geordnete Geometrie. Für jede Gerade $g \in \mathcal{G}$ ist die Relation*

$$A \sim_g B \iff A = B \text{ oder } (AB) \cap g = \emptyset$$

eine Äquivalenzrelation auf $\mathcal{X} \setminus g$.

Beweis-Skizze: $A \sim_g A$ und $A \sim_g B \Rightarrow B \sim_g A$ sind klar.
Seien A, B, C drei verschiedene Punkte mit $A \sim_g B$ und $B \sim_g C$. Wir wollen $A \sim_g C$ beweisen.

Fall 1: A, B, C sind nicht kollinear. Dann folgt alles aus Pasch's Axiom **A4.**.

Fall 2: A, B, C sind kollinear. Sei h die Gerade durch A, B, C. Da $A, B, C \notin g$, folgt $\sharp(g \cap h) \leq 1$. Aus **I2.** gibt es ein Punkt $D \in g \setminus h$. Aus **A2.** gibt es ein Punkt E mit $D\_\_A\_\_E$ (insbesondere $A \neq E$). Also A, D, E sind kollinear nach **A1.**. Es folgt auch $(AE) \cap g = \emptyset$ (sonst $A\_\_D\_\_E$). Also $A \sim_g E$. Da $D \notin h$ folgt auch $E \notin h$ (sonst wäre $E = h \cap DE = h \cap AE = A$). Insbesondere sind (B, C, E), (A, C, E) und (A, B, E) Trippeln nicht-kollinearer Punkte. Wir können also Fall 1 anwenden:
Aus Fall 1 für B, C, E folgt $C \sim_g E$. Aus Fall 1 für A, B, E folgt $B \sim_g E$. Also, aus Fall 1 für A, C, E folgt $A \sim_g C$. Q.E.D.

Satz 4.22. *Sei $(\mathcal{X}, \mathcal{G})$ eine geordnete Geometrie und $g \in \mathcal{G}$. Dann teilt g die Menge $\mathcal{X} \setminus g$ in zwei nicht-leere Teilmengen H_1, H_2 mit den Eigenschaften*

(i) *Wenn $A, B \in \mathcal{X} \setminus g$ zur selben H_i gehören, dann $(AB) \cap g = \emptyset$.*

(ii) *Wenn $A, B \in \mathcal{X} \setminus g$ nicht zur selben H_i gehören, dann $(AB) \cap g = P \in \mathcal{X}$.*

Beweis-Skizze: Nach Lemma 4.21 reicht es zu zeigen, dass es genau zwei Äquivalenzklassen für $\sim_g$ gibt. Diese werden H_1 und H_2 mit den erwünschten Eigenschaften sein.

Aus **I3.** folgt $\exists A \notin g$, also auch die Äquivalenzklasse davon: $H_1 = [A]_{\sim_g}$. Sei $D \in g$ beliebig. Aus **A2.** existiert ein Punkt C, sodass $A\_\_D\_\_C$. Dann ist $A \not\sim_g C$, existiert auch $H_2 := [C]_{\sim_g}$.
Um zu zeigen, dass es keine weitere Klassen gibt, reicht folgende Implikation zu zeigen:

$$A \not\sim_g C, \quad B \not\sim_g C \qquad \Rightarrow \qquad A \sim_g B.$$

Fall 1: A, B, C sind nicht kollinear. Das folgt wieder aus Paschs Axiom **A4.**.
Fall 2: A, B, C sind kollinear. Wie im Beweis der Lemma 4.21 finden wir $E \sim_g A$. Da $A \not\sim_g C$ und $A \sim_g E$ folgt es, dass $C \not\sim_g E$ (da Äquivalenzrelation). Dann, aus Fall 1 für B, C, E folgt $B \sim_g E$, und aus Transitivität auch $A \sim_g B$. Q.E.D.

Definition 4.23. Wir nennen H_1 und H_2 die zwei von g bestimmten **offene Halbebenen**, und, wenn $A, B \in H_i$, sagen wir, dass A, B auf **derselben Seite von g** sind. Für $A \notin g$ bezeichnen wir mit

$H_g(A)$:= die von g bestimmte offene Halbebene die A enthält.

$H_g[A]$:= $g \cup H_g(A)$ = die von g bestimmte abgeschlossene Halbebene die A enthält.

Satz 4.24. *Sei $P \in g$ ein Punkt auf einer Gerade. Die Menge $g \setminus P$ ist in zwei nicht-leere Teilmengen S_1 und S_2 geteilt, sodass*

(i) *$A, B \in S_i$ für irgendwelcher i $\iff$ $P \notin (AB)$.*

(ii) *$A \in S_1$ und $B \in S_2$ $\iff$ $P \in (AB)$.*

Beweis-Skizze: Aus **I3.** gibt es ein Punkt $E \notin g$. Sei $h = PE$. Dann, aus Satz 4.22 gibt es zwei Teilmengen H_1' und H_2 von $\mathcal{X} \setminus h$, und wir definieren $S_i = g \cap H_i$. Um zu sehen, dass $S_i \neq \emptyset$ wählt man $A \in g$, mit $A \neq P$ und wendet dann **A2.** an, um B mit A–P–B zu finden. Alles folgt jetzt direkt aus dem Satz 4.22. Q.E.D.

Definition 4.25. Wir nennen die obigen S_1 und S_2 die von P auf g bestimmten *offenen Halbgeraden*. Wenn $A, B \in S_i$, sagen wir, dass A, B auf *derselben Seite von P* sind.

Definition 4.26. Der *offene Strahl* aus A durch B ist

$$(AB := \{C \in AB \mid C \text{ und } B \text{ liegen auf der selben Seite von } A \text{ auf } AB\}$$

Der *abgeschlossene Strahl* aus A durch B ist

$$[AB := \{A\} \cup (AB.$$

In beiden Fällen heißt A der *Ursprung* des Strahls.

Definition 4.27. Für drei nicht-kollineare Punkte A, B, C definieren wir das *Dreieck*

$$\triangle ABC := [AB] \cup [BC] \cup [AC].$$

Ein *Winkel* ist die Vereinigung zweier Strahlen $[AB$ und $[AC$, die den selben Ursprung A haben, und die nicht auf derselben Gerade liegen. (Es gibt also keine $0°$ oder $180°$ Winkel.) Wir bezeichnen es mit $\angle BAC$.

Definition 4.28. Das **Innere eines Winkels** $\angle BAC$ ist

$$\operatorname{inn} \angle BAC = H_{AB}(C) \cap H_{AC}(B).$$

Das **Innere eines Dreiecks** $\triangle ABC$ ist

$$\operatorname{inn} \triangle ABC = (\operatorname{inn} \angle BAC) \cap (\operatorname{inn} \angle CBA) \cap (\operatorname{inn} \angle ACB).$$

Satz 4.29 (Querstangensatz)**.** *Sei $\angle BAC$ ein Winkel, und $D \in \operatorname{inn} \angle BAC$ ein Punkt im Inneren. Dann gilt*

$$[AD \cap (BC) \neq \emptyset.$$

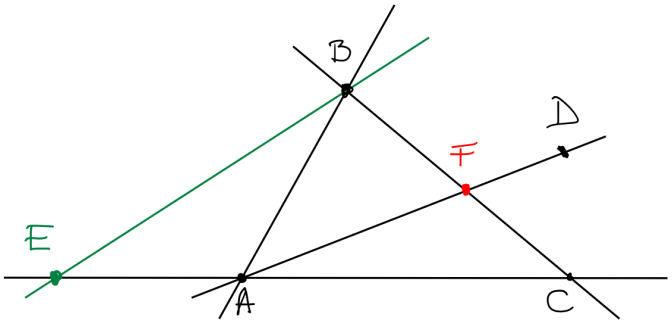


Abbildung 4.1: Bild zum Beweis von Satz 4.29.

Beweis-Skizze:

Aus **A2.** finden wir $E \in AC$ mit E_A_C, und wenden das Axiom **A4.** von Pasch in $\triangle BEC$ mit der Gerade AD. ($B \notin AD$ weil dann wäre D nicht in inn$\angle BAC$.) Wir müssen zeigen, dass $(BE) \cap AD = \emptyset$. Da $[BE] \cap AB = B$, haben wir $H_{AB}(P) = H_{AB}(E)$, $\forall\ P \in (BE)$. Der Punkt E wurde aber gewählt, so dass $H_{AB}(E) \neq H_{AB}(C)$. Also,

$$\forall\ P \in (BE), \quad H_{AB}(P) \cap H_{AB}(C) = \emptyset.$$

Da $[AD \cap AB = A$, haben wir $H_{AB}(Q) = H_{AB}(D)$, $\forall\ Q \in [AD$. Der Punkt liegt aber per Definition in $H_{AB}(C)$, d.h. $H_{AB}(D) = H_{AB}(C)$, also

$$\forall\ Q \in [AD, \quad H_{AB}(Q) = H_{AB}(C) \iff Q \in H_{AB}(C).$$

Also $[AD \cap (BE) = \emptyset$.

Genauso, für die andere Halbgerade S_2 auf AD:

$$\forall\ P \in (BE), \forall\ Q \in S_2, \quad H_{AC}(P) \cap H_{AC}(Q) = \emptyset$$

Also $AD \cap (BE) = \emptyset$ und aus Pasch's Axiom folgt $AD \cap (BC) = F$. Es fehlt nur noch $F \in [AD$: das folgt weil $F \in H_{AB}(C) = H_{AB}(D)$. Q.E.D.

Beispiel 4.30. $\mathbb{R}^2$ mit der "gewöhnlichen" Anordnung ist eine geordnete Geometrie:

- Auf der reellen Gerade $\mathbb{R}$: $a\_b\_c \iff a < b < c$ oder $a > b > c$. Das erfüllt **A1-A3.**.
- In der reellen Ebene $\mathbb{R}^2$ definiert man die Anordnung für drei kollineare Punkte $A = (a_1, a_2)$ $B = (b_1, b_2)$, $C = (c_1, c_2) \in \mathbb{R}^2$ durch

$$A\_B\_C \iff a_1\_b_1\_c_1 \text{ oder } a_2\_b_2\_c_2 \text{ (oder beide).}$$

- Lineare Operationen (Addition, Multiplication) erhalten oder invertieren die Ordnung ($a < b < c \Rightarrow an < bn < cn$ oder $an > bn > cn$). Also diese erhalten die Anordnung, und $\mathbb{R}^2$ erfüllt **A1-A3.**.

- Sei $\varphi : \mathbb{R}^2 \longrightarrow \mathbb{R}$ mit $\varphi(x, y) = ax + by + c$ eine lineare (affine) Abbildung, und $g = V(\varphi = 0)$. Seien A, B, C drei Punkte so dass $g \cap (AB) \neq \emptyset$. Dann, haben wir $\varphi(A)\_0\_\varphi(B)$. Insbesondere $\varphi(A) > 0$ und $\varphi(B) < 0$, oder umgekehrt. Dann, ist $\varphi(C)$ entweder positiv, oder negativ, und dann trifft die gerade g die entsprechende Strecke.
- In diesem Fall haben wir

$$\begin{aligned} [AB] &= \{tA + (1-t)B \mid 0 \leqslant t \leqslant 1\} \\ (AB) &= \{tA + (1-t)B \mid 0 < t < 1\} \end{aligned}$$

4.2.4 Kongruenz-Axiome für Strecken und Winkel

Strecken

In einer geordneten Geometrie, postulieren wir einen undefinierten Begriff von **Kongruenz von abgeschlossenen Strecken** und schreiben das als $[AB] \equiv [CD]$, der folgende Axiome erfüllen soll:

KS1. Gegeben $[AB]$ und ein Strahl s mit Ursprung C, dann $\exists! D \in s$ mit $[AB] \equiv [CD]$.

KS2. Jede Strecke ist zu sich selber kongruent und

$$[AB] \equiv [CD] \quad \text{und} \quad [AB] \equiv [EF] \Rightarrow [CD] \equiv [EF].$$

KS3. (Addition) Seien A_B_C und D_E_F. Dann gilt

$$[AB] \equiv [DE] \,\text{und}\, [BC] \equiv [EF] \Rightarrow [AC] \equiv [DF].$$

Satz 4.31. *Die Kongruenz $\equiv$ ist eine Äquivalenzrelation auf* $\{[AB] \;:\; A, B \in \mathcal{X} \text{ mit } A \neq B\}$.

Beweis-Skizze: Reflexivität kommt explizit in (KS2) vor.
Symmetrie folgt aus (KS2) mit $[EF] = [AB]$
Transitivität: $[AB] \equiv [CD]$ und $[CD] \equiv [EF]$, dann aus der Symmetrie auch $[CD] \equiv [AB]$, und aus (KS2) folgt $[AB] \equiv [EF]$. Q.E.D.

Lemma 4.32. *Wenn A_B_C drei Punkte sind, r ein Strahl mit Ursprung D, und $E, F \in r$, dann*

$$\text{wenn } [AB] \equiv [DE] \;\text{ und }\; [AC] \equiv [DF] \quad \Rightarrow \quad D\_E\_F \;\text{ und }\; [BC] \equiv [EF].$$

Beweis-Skizze: Sei nun s der Strahl auf DE mit Ursprung E, und mit $D \notin s$. Sei F' der einzige Punkt auf s (also D_E_F') mit $[BC] \equiv [EF']$. Dann, aus (KS3) folgt $[AC] \equiv [DF']$. Wir haben $F, F' \in (DE$, weil $F \in r = (DE$ wurde vorausgesetzt, und $D\_E\_F' \Leftrightarrow F' \in (DE$. Es folgt also aus (KS1) $F = F'$, also D_E_F und $[BC] \equiv [EF]$. Q.E.D.

Die Kongruenzaxiome erlauben uns eine Ordnungsrelation für Äquivalenzklassen von Strecken zu definieren.

Definition 4.33. Seien $[AB], [CD]$ zwei Strecken. Wir sagen, $[AB]$ **kleiner als** $[CD]$ ist, und schreiben

$$[AB]<[CD] \iff \exists\ E \in (AB) \text{ mit } [AB] \equiv [CE].$$

Satz 4.34. (a) *Die Ordnung ist unabhängig vom Repräsentant der Kongruenzklasse:*

$$\text{Wenn } [AB] \equiv [A'B'] \text{ und } [CD] \equiv [C'D'], \text{ dann } [AB] < [CD] \iff [A'B'] < [C'D'].$$

(b) *Die Relation aus Definition 4.33 ist eine Ordnungsrelation auf* (Strecken/ $\equiv$) *im folgenden Sinne:*

(i) *Es ist transitiv:* $[AB] < [CD], \quad [CD] < [EF] \quad \Rightarrow \quad [AB] < [EF]$

(ii) *Für zwei gegebene Strecken* $[AB]$ *und* $[CD]$ *kommt genau eine der folgenden Situationen vor:*

$$[AB] < [CD] \quad \text{oder} \quad [AB] \equiv [CD] \quad \text{oder} \quad [CD] < [AB].$$

Beweis-Skizze: (a) Sei $E \in (CD)$, also $C\_\_E\_\_D$. Sei $E' \in (C'D'$ der einzige Punkt aus (KS1) mit $[C'E'] \equiv [CE]$. Aus Lemma 4.32 folgt, dass $C'\_\_E'\_\_D'$. Aus $[A'B'] \equiv [AB] \equiv [CE] \equiv [C'E']$ folgt dann $[A'B'] < [C'D']$.

(b) (i) Sei $P \in [CD]$ mit $[AB] \equiv [CP]$. Sei $Q \in [EF]$ mit $[CD] \equiv [EQ]$ und $R \in [EQ]$ mit $[CP] \equiv [ER]$. Dann ist aus Lemma 4.32 $E\_\_R\_\_Q$ und, da auch $E\_\_Q\_\_F$ folgt auch, dass $E\_\_R\_\_F$ (Übung).

(ii) Wähle $E \in (CD$ aus (KS1) mit $[AB] \equiv [CE]$. Die drei Situationen entsprechen genau zwei der erlaubten Möglichkeiten aus (A3) und die einzige aus (KS1)

$$C\_\_E\_\_D \quad \text{oder} \quad D = E \quad \text{oder} \quad C\_\_D\_\_E.$$

($D\_\_C\_\_E$ kommt nicht vor weil $E \in (CD$.)

Q.E.D.

In $\mathbb{R}^2$ definieren wir der Euklidischen Distanz zwischen zwei Punkte $A = (a_1, a_2)$ und $B = (b_1, b_2)$ als

$$\mathrm{d}(A, B) = \sqrt{(a_1 - b_1)^2 + (a_2 - b_2)^2}.$$

Die Kongruenz von Strecken ist dann definiert als

$$[AB] \equiv [CD] \iff \mathrm{d}(A, B) = \mathrm{d}(C, D).$$

Winkel

In einer geordneten Geometrie, mit Streckenkongruenz, postulieren wir einen undefinierten Begriff von **Kongruenz von Winkel** und schreiben das als $\angle BAC \equiv \angle EDF$, der folgende Axiome erfüllen soll:

KW1. Gegeben $\angle BAC$, ein Strahl $[DE$ und eine der von DE definierten Halbebenen H_1, $\exists!$ $[DF$ ein abgeschlossener Strahl mit $(DF \subset H_1$ und $\angle BAC \equiv \angle EDF$.

KW2. Jeder Winkel ist zu sich selber kongruent und für alle Winkel α, β, γ gilt

$$\angle\alpha \equiv \angle\beta \quad \text{und} \quad \angle\beta \equiv \angle\gamma \Rightarrow \angle\alpha \equiv \angle\gamma.$$

KW3. (SWS) Wenn $\triangle ABC$ und $\triangle DEF$ mit $[AB] \equiv [DE]$, $[AC] \equiv [DF]$, und $\angle BAC \equiv \angle EDF$, dann gilt auch $[BC] \equiv [EF]$, $\angle ABC \equiv \angle DEF$ und $\angle ACB \equiv \angle DFE$.

Wir sagen, dass zwei Dreiecke $\triangle ABC$ und $\triangle DEF$ kongruent sind wenn, wie im Axiom **KW3.** sind die drei Seiten und die Winkel paarweise kongruent sind.

Axiom (KW3) oder (SWS) kommt vor, weil Euklid's Beweis für diesen Satz ungenau war. Man kann sehen, dass dieses Axiom äquivalent zu "es gibt genug Automorphismen die Anonrdung und Kongruenz erhalten"

BEW1 Für zwei Punkte A, A' gibt es φ mit $\varphi(A) = A'$

BEW2 Für drei Punkte O, A, A' gibt es φ mit $\varphi(O) = O$ und $\varphi([OA) = \varphi([OA')$

BEW3 Für jede Gerade g, die die Halbebenen H_1, H_2 gibt, existiert φ mit $\varphi(P) = P$, $\forall\ P \in g$ und $\varphi(H_1) = H_2$, $\varphi(H_2) = H_1$.

Wir werden diese Äquivalenz nicht beweisen. Es ist aber gut sich zu merken, dass (KW3) unabhängig von den anderen Axiomen ist (Übung), und dass dieses Axiom die "Homogenität" der Ebene gibt (sie sieht aus und verhāhlt sich überall gelich).

Satz 4.35. *Die Kongruenzrelation die Axiome (KW1-3) erfüllt ist eine Äquivalenzrealtion auf der Menge aller Winkel.*

Beweis-Skizze: Übung. - geht genau sau wie Satz 4.31, mit (KW2) statt (KS2) Q.E.D.

Die Summe zweier Strecken kann man einfach definieren: wir nehmen auf $[AB$ den einzigen Punkt E mit $[BE] \equiv [CD]$ und definieren $[AB] + [CD] := [AE]$. Man kann einfach sehen dass diese eine Addition auf Äquivalenzkalssen von Strecken ist. Für Winkel ist das aber nicht so einfach. Erstens, ist das dritte Axiom verschieden, zweitens, Winkel könnten sich zu Winkel die $\geqslant 180°$ sind - und diese sind nicht definiert. Man muss also aufpassen.

Definition 4.36. Sei $\angle BAC$ ein Winkel, und D ein Punkt auf AC auf der anderen Seite von A als C. Die Winkel $\angle BAC$ und $\angle DAB$ heißen **Nebenwinkel**. Wir schreiben dafür $\angle BAC + \angle DAB = \_\angle$.

Satz 4.37. *Wenn $\angle BAC + \angle DAB = \_\angle$, $\angle B'A'C' + \angle D'A'B' = \_\angle$, und $\angle BAC \equiv \angle B'A'C'$, dann auch $\angle DAB \equiv \angle D'A'B'$.*

Beweis-Skizze: Wir können die Punkte so wählen, dass $[AB] \equiv [A'B']$, $[AC] \equiv [A'C']$ und $[AD] \equiv [A'D']$. Dann, aus (KS3) haben wir auch $[CD] \equiv [C'D']$. Wir wenden jetzt (SWS) für die Dreiecke:

$$\triangle BAC \equiv \triangle B'A'C' \quad \Rightarrow \quad \triangle DCB \equiv \triangle D'C'B' \quad \Rightarrow \quad \triangle ADB \equiv \triangle A'D'B'$$

und aus der letzten Kongruenz folgt $\angle DAB \equiv \angle D'A'B'$ Q.E.D.

Definition 4.38. Wenn $B\_\_A\_\_D$ und $C\_\_A\_\_E$ mit $BD \neq CE$, dann heißen die Winkel $\angle BAC$ und $\angle DAE$ **Gegenwinkel**.

Korollar 4.39. Gegenwinkel sind kongruent.

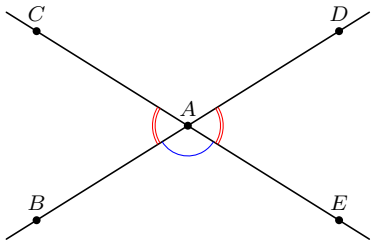


Abbildung 4.2: Gegenwinkel sind kongruent.

Satz 4.40. *Sei $\angle BAC$ und $[AD$ ein Strahl in $\operatorname{inn}\angle BAC$. Wenn $\angle DAC \equiv \angle D'A'C'$, $\angle BAD \equiv \angle B'A'D'$, und wenn $(A'B'$ und $(A'C'$ nicht auf derselben Seite von $A'D'$ liegen, dann*

(a) definieren die Strahlen $[A'B'$ und $[A'C'$ einen Winkel

(b) $\angle BAC \equiv \angle B'A'C'$

(c) $(A'D' \subseteq \operatorname{inn}\angle B'A'C'$

Beweis-Skizze: Aus Satz 4.29 wissen wir, dass $[BC] \cap (AD \neq \emptyset$, und dürfen also $D \in (BC)$ wählen, also $B\_\_D\_\_C$. Wir dürfen auch B', C', D' mit anderen Punkten auf den ensprechenden Geraden ersätzen, so dass $[AB] \equiv [A'B']$, $[AC] \equiv [A'C']$ und $[AD] \equiv [A'D']$. Aus $\angle DAC \equiv \angle D'A'C'$, $\angle BAD \equiv \angle D'A'D'$ und (SWS) bekommen wir

$$\triangle BAD \equiv \triangle B'A'D' \qquad \text{und} \qquad \triangle DAC \equiv \triangle D'A'C'.$$

Also $[DC] \equiv [D'C']$ und $\angle ADC \equiv \angle A'D'C'$.
Sei E' ein Punkt mit $B'\_\_D'\_\_E'$. Dann $NWA'D'E'A'D'B'$. Wir haben $\angle A'D'B' \equiv \angle ADB$, $\angle ADB + \angle ADC = \_\angle$ und $\angle ADC \equiv \angle A'D'C'$. Also, aus der Transitivität der Kongruenz, und aus Satz 4.37 folgt

$$\angle A'D'E' \equiv \angle A'D'C'.$$

Da C' und E' auf derselben Seite von $A'D'$ sind (die andere als B'), haben wir aus $(KW1)$, dass es derselbe Winkel ist, also $[D'E'] = [D'C']$, und also $B'\_\_D'\_\_C'$ (also auch (c), wenn (a) gilt). Aus (KW3) + Voraussetzung, haben wir $[BC] \equiv [B'C']$, und aus (SWS)

$$\triangle ABC \equiv \triangle A'B'C'.$$

Da $\angle D'A'C'$ ein Winkel ist, sind also D', A', C' nicht kollinear, und dann sind auch B', A', C' nicht

kollinear (sonst $A' \in B'C' = D'C'$). Also ist $\angle B'A'C'$ ein Winkel (also (a)). Aus der kongruenz, folgt auch $\angle BAC \equiv \angle B'A'C'$. Q.E.D.

Wir können jetzt auch für (Kongruenzklassen von) Winkel eine Ordnungsrelation definieren.

Definition 4.41. Seien $\angle BAC$ und $\angle EDF$ zwei Winkel. Wir sagen, dass $\angle BAC$ **kleiner als** $\angle EDF$, und schreiben $\angle BAC < \angle EDF$, wenn

$$\exists \text{ ein Strahl } [DG \subset \operatorname{inn} \angle EDF \text{ mit } \angle BAC \equiv \angle GDF.$$

Satz 4.42. *Die oben definierte Relation ist eine Ordungnsrelation auf die Menge der Kongruenzkalssen von Winkel.*

Beweis-Skizze: Geht genauso wie der Beweis für Strecken (Satz 4.34). Q.E.D.

Definition 4.43. Eine **Hilbertebene** (oder **neutrale Geometrie**) ist eine geordnete Geometrie, zusammen mit Kongruenzbegriffe für Strecken und Winkel die die Axiome (KS1-3) und (KW1-3) erfüllt.

Es heißt neutral, weil es keinen Stadnpunkt bezüglich dem Parallelenaxiom hat. Man kann damit, fast das ganze erste Buch von Euklid beweisen. Eine Ausnahme ist immer die existenz gliechseitiger Dreiecke (Satz I.1 aus den Elementen). Es gibt aber gleichschenklige Dreiecke.

Definition 4.44. Ein **rechter Winkel** ist ein Winkel der kongruent zu einem seiner Nebenwinkel ist.

Definition 4.45. Zwei Geraden sind **orthogonal** wenn sich diese in einem Punkt treffen, und einer (also alle 4) der Winkel die so entstehen ein rechter Winkel ist.

Satz 4.46. *Zwei rechte Winkel sind immer kongruent.*

Beweis-Skizze: Seien $\alpha = \angle BAC$ und $\alpha' = \angle B'A'C'$ zwei rechte Winkel, nämlich kongruent zu ihren Nebenwinkeln $\beta = \angle DAB$ bzw. $\beta' = \angle D'A'B'$. Nehmen wir an, dass $\alpha \not\equiv \alpha'$. Dann, aus Satz 4.42 folgt $\alpha < \alpha'$ oder $\alpha' < \alpha$.
O.B.d.A. $\alpha < \alpha'$. Per Definition existiert ein Strahl $[A'E' \subset \operatorname{inn} \alpha'$ mit $\angle E'A'B' \equiv \alpha$. Da $C' \not\sim_{A'E'} B'$ und $D' \not\sim_{A'E'} B'$, folgt aus Satz 4.22, dass $C' \sim_{A'E'} D'$. D.h. $(A'C') \subset \operatorname{inn} \angle D'A'E'$, und also auch $\beta' < \angle D'A'E'$. Aber

$$\angle D'A'E' + \angle E'A'B' = \measuredangle \quad \text{und} \quad \alpha \equiv \angle E'A'B'$$

also nach Satz 4.37, da α und β Nebenwinkel sind, folgt $\angle E'A'D' \equiv \beta$. Also $\beta' < \beta$. Da aber $\alpha \equiv \beta$ und $\alpha' \equiv \beta'$, bekommen wir aus Satz 4.42, dass $\alpha' < \alpha$ - Wiederspruch. Q.E.D.

Also, im gegensatz zu Euklid, muss man das nicht als Axiom nehmen.

Definition 4.47. Ein Dreieck $\triangle ABC$ ist **gleichschenklig** wenn zwei Seiten kongruent sind.

Satz 4.48. $\triangle ABC$ *ist gleichschenklig mit* $[AB] \equiv [AC] \iff \angle ABC \equiv \angle ACB$.

Beweis-Skizze: $\boxed{\Rightarrow}$ SWS für $\triangle BAC$ und $\triangle CAB$.
$\boxed{\Leftarrow}$ Wenn $[AB] < [AC]$, sei $A' \in (AC)$ mit $[A'C] \equiv [AB]$. Dann, aus SWS für $\triangle ABC$ und $\triangle A'CB$ folgt $\angle A'BC \equiv \angle ACB$. Aus $\angle ABC \equiv \angle ACB$ und (KW1) folgt $A' = A$. Mit (KS1) folgt OK. Q.E.D.

Satz 4.49. *Rechte Winkel existieren. Genauer gesagt, gegeben g und $A, B \in g$, $\exists\ C \notin g$ mit $\angle BAC$ ein rechter Winkel.*

Beweis-Skizze: Sei $D \in g$ mit $(AD) \cap (AB) = \emptyset$ und $[AB] \equiv [AD]$. Sei $E \notin g$.
$\boxed{\text{Wenn } \angle EBA \equiv \angle EDA}$, dann $C = E$ und, aus Satz 4.48 folgt $\triangle BAE \equiv \triangle DAE$, also auch $\angle BAE \equiv \angle DAE$.
$\boxed{\text{Sonst, o.B.d.A. } \angle EBA < \angle EDA.}$ Dann, existiert $(DC' \subset \operatorname{inn} \angle EDA$ mit $\angle EBA \equiv \angle C'DA$. Aus Satz 4.29 folgt $(DC' \cap (BE) \neq \emptyset$. Wir bezeichnen $C := (DC' \cap (BE)$, und, wie im ersten Fall, haben wir $\triangle BAC \equiv \triangle DAC$. Q.E.D.

Satz 4.50 (SSS)**.** *Seien $\triangle ABC$ und $\triangle A'B'C'$, mit $[AB] \equiv [A'B']$, $[AC] \equiv [A'C']$, und $[BC] \equiv [B'C']$, dann gilt $\triangle ABC \equiv \triangle A'B'C'$.*

Beweis-Skizze: Man wählt B'' mit $(B'B'') \cap A'C' \neq \emptyset$, und $\angle BAC \equiv \angle B''A'C'$. Dann folgt $\triangle BAC \equiv \triangle B''A'C'$. Da die $\triangle A'B'B''$ und $C'B'B''$ gleichschenklig sind + Satz für Winkeladdition, folgt $\angle A'B'C' \equiv \angle A'B''C'$, und dann aus SWS und Transitivität sind wir fertig. Q.E.D.

Satz 4.51. *Gegeben $[AB]$, es gibt ein gleichschenkliges Dreieck mit Basis $[AB]$.*

Beweis-Skizze: Es existiert $C \notin AB$. Wenn $\angle CAB \equiv \angle CBA$, dann sind wir fertig. Sonst, wenn einer kleiner ist, gibt es ein Strahl im Inneren, und das Dreieck ist gleichschenklig weil die Winkel gleich sind. Q.E.D.

Definition 4.52. **Die Winkelhalbierende** eines Winkels $\angle BAC$ ist ein Strahl $[AD] \subset \operatorname{inn} \angle BAC$ mit der Eigenschaft, dass $\angle BAD \equiv \angle CAD$.

Definition 4.53. **Der Mittelpunkt** einer Strecke $[AB]$ ist ein Punkt $M \in (AB)$ mit der Eigenschaft, dass $[AM] \equiv [BM]$.

Satz 4.54. *Für jeder Winkel existiert die Winkelhalbierende. Für jede Strecke existiert die Mitte.*

Beweis-Skizze: Es funktioniert genau wie im Buch von Euklid, nur statt gleichseitige Dreiecke, muss man gleichschenklige Dreiecke nehmen. Übung. Q.E.D.

Satz 4.55. *In einem Dreieck $\triangle ABC$ ist der Aussenwinkel von $\angle C$ größer als $\angle A$ und auch größer als $\angle B$.*

Beweis-Skizze: Sei D mit $B\_\_C\_\_D$. Wir zeigen, dass $\angle A < \angle ACD$. Sei E die Mitte von $[AC]$ und sei F mit $B\_\_E\_\_F$ und $[BE] \equiv [EF]$. Dann, da Gegenwinkel kongruent sind (Korollar 4.39), haben wir $\triangle AEB \equiv \triangle CEF$. Also $\angle A \equiv \angle ACF$. Es reicht also z.z., dass $(CF) \subset \operatorname{inn} \angle ACD$. Wir haben

$$\left.\begin{array}{l} B \not\sim_{AC} D \\ B \not\sim_{AC} F \end{array}\right\} \Rightarrow D \sim_{AC} F \qquad \left.\begin{array}{l} E \sim_{BC} F \\ E \sim_{BC} A \end{array}\right\} \Rightarrow A \sim_{BC} F$$

Also $F \in \operatorname{inn} \angle ACD$, und also auch $(CF \subset \operatorname{inn} \angle ACD$. Q.E.D.

Satz 4.56. *Euklids Sätze I.1-28 aus Buch I. gelten in einer Hilbertebene, mit der Ausnahme von Satz I.1, und Satz I.22.*

Z.B.

Satz 4.57. *Im Dreieck liegt dem größeren Winkel die größere Seite gegenüber.*

4.2.5 Kreise in der Neutralen Geometrie

Sei $(\mathcal{X}, \mathcal{G})$ eine Hilbert Ebene. Wir werden Kreise definieren, und ein weiteres Axiom verlangen, so dass Kreise und Geraden sich schneiden wann sie sich schneiden müssen.

Definition 4.58. Seien $O \neq A$ zwei verschieden Punkte. Der **Kreis** $\Gamma_{O,A}$ mit Mittelpunkt O und Radius $[OA]$ ist

$$\Gamma_{O,A} := \{B \in \mathcal{X} \ : \ [OA] \equiv [OB]\}.$$

Wenn eine Gerade $g \ni O$, dann, aus (KS1), folgt $\sharp(g \cap \Gamma_{O,A}) = 2$. Die Eindeutighkeit des Mittelpunktes ist aber aus der Definition nicht offensichtlich.

Satz 4.59. *Seien $\Gamma = \Gamma_{O,A}$ und $\Gamma' = \Gamma_{O',A'}$ zwei Kreise. Wenn $\Gamma = \Gamma'$ als Punktmengen, dann $O = O'$.*

Beweis-Skizze: Wenn $O \neq O'$, sei $g = OO'$. Dann, sei $\{C, D\} = g \cap \Gamma$. Also $C \_ O \_ D$. Da $\Gamma = \Gamma'$, haben wir auch $[O'C] \equiv [O'D]$, also, da $C \neq D$, auch $C \_ O' \_ D$. O.B.d.A. $C \_ O \_ O'$. Dann, aus den Eigenschaften der Anordnung, folgt $O \_ O' \_ D$, also

$$[OC] < [O'C] \equiv [O'D] < [OD] - \text{ Wiederspruch!}$$

Also $O = O'$. Q.E.D.

Definition 4.60. Das **Innere** eines Kreises $\Gamma_{O,A}$ ist

$$\operatorname{inn} \Gamma_{O,A} := \{B \ : \ [OB] < [OA]\} \cup \{O\}.$$

Das **Äußere** eines Kreises $\Gamma_{O,A}$ ist

$$\operatorname{ext} \Gamma_{O,A} := \{B \ : \ [OA] < [OB]\}.$$

Definition 4.61. Wir sagen, dass eine Gerade g zum Kreis Γ **tangent** ist, wenn $\sharp(g \cap \Gamma) = 1$.
Wir sagen, dass ein Kreis Δ zum Kreis Γ *tangent* ist, wenn $\sharp(\Delta \cap \Gamma) = 1$.

Satz 4.62. *Sei $\Gamma_{O,A}$ ein Kreis, und $g \ni A$, die Senkrechte and OA durch A. Dann ist g tangent zu $\Gamma_{O,A}$ und*

$$g \setminus \{A\} \subset \operatorname{ext} \Gamma_{O,A}.$$

Umgekehrt, wenn g tangent and $\Gamma_{O,A}$ ist, mit $A \in g$, dann $g \perp OA$. Also die Tangente zu einem Kreis in einem Punkt ist eindeutig.

Beweis-Skizze: Sei $B \in g$, mit $A \neq B$. Im $\triangle OAB$ ist $\angle A$ gleich mit seinem Aussenwinkel, also, nach Satz 4.55, ist $\angle B < \angle A$. Nach Satz I.19 (4.57 im Skript), ist also $[OA] < [OB]$, also $B \in \operatorname{ext}\Gamma_{O,A}$.

Sei g tangent an $\Gamma_{O,A}$. Wir wollen $OA \perp g$. Wir haben $OA \neq g$ - weil OA den Kreis in 2 Punkte schneidet. Sei B der Fußpunkt der Senkrechten aus O auf g. Wenn $B \neq A$, dann wähle C auf g mit $A\_\_B\_\_C$ und $[AC] \equiv [BC]$. Dann, aus SWS für $\triangle OBC$ und $\triangle OBA$, folgt $[OA] \equiv [OC]$, also $A \neq C \in \Gamma_{O,A} \cap g$ - Wiederspruch. Q.E.D.

Korollar 4.63. Wenn eine Gerade einen Kreis trifft, aber nicht dazu tangent ist, dann trifft diese den Kreis genau in zwei Punkte.

Beweis-Skizze: Gäbe es 3 verschiedene Schnittpunkte A, B, C (o.B.d.A. $A\_\_B\_\_C$) dann haben wir 3 gleichschenklige Dreiecke, und dann ist der Winkel $\angle OAB$ ein rechter Winkel. Q.E.D.

Satz 4.64. *Seien O, O', A drei verschiedene Punkte. Die Kreise $\Gamma_{O,A}$ und $\Gamma_{O',A}$ sind tangent wenn und nur wenn O, O', A kollinear sind.*

Beweis-Skizze: $\boxed{\Rightarrow}$ Wenn O, O', A nicht kollinear sind, dann sei $AC \perp OO'$, mit $C \in OO'$ und sei B mit $A\_\_C\_\_B$ und $[AC] \equiv [CB]$. Dann, aus (SWS) für $\triangle OAC$ und $\triangle OBC$ folgt $[OA] \equiv [OB]$, und aus (SWS) für $\triangle O'AC$ und $\triangle O'BC$ folgt $[O'A] \equiv [O'B]$. Also $B \in \Gamma_{O,A} \cap \Gamma_{O',A}$ – Wiederspruch.
$\boxed{\Leftarrow}$ Sei $B \in \Gamma_{O,A} \cap \Gamma_{O',A}$. Wenn $B \in OO'$, dann $B\_\_O\_\_A$ und $B\_\_O'\_\_A$, und $O = O' =$ der Mittelpunkt von $[AB]$. Also $B \notin OO'$.
Fall 1: $O\_\_O'\_\_A$**:** $[OA] \equiv [OB] \Rightarrow \angle OBA \equiv \angle OAB$ und $[O'A] \equiv [O'B] \Rightarrow \angle O'BA \equiv \angle O'AB$. Also $\angle OBA \equiv \angle O'BA$ - Wiederspruch zu (WK1).
Fall 2: $O\_\_A\_\_O'$**:** $[OA] \equiv [OB] \Rightarrow \angle OBA \equiv \angle OAB$ und $[O'A] \equiv [O'B] \Rightarrow \angle O'BA \equiv \angle O'AB$. Da $\angle OAB + \angle O'AB = \measuredangle$, folgt auch $\angle OBA + \angle O'BA = \measuredangle$, also O, O', B sind kollinear – Wiederspruch.

Q.E.D.

Korollar 4.65. Wenn sich zwei nicht-tangente Kreise in einem Punkt treffen, dann besteht der Schnitt genau aus 2 Punkte.

Beweis-Skizze: Nich tangent $\Rightarrow O, O', A$ nicht kollinear, und aus $\boxed{\Rightarrow}$ gibt es ein zweiter Schnittpunkt. Sei dieser B, und sei D ein dritter Schnittpunkt. O.B.d.A. $D \sim_{OO'} A$. Aus (SSS) haben wir $\triangle OAO' \equiv \triangle ODO'$. Und aus (KS1) und (KW1) folgt $A = D$. Q.E.D.

Also wenn sich Kreise und Geraden schneiden, dann ist das "wie erwartet". Aber wir haben keine Garantie, dass es Schnittpunkte gibt. Wir brauchen fogendes **Kreis-Gerade-Schnitt-Axiom**:

E. Wenn Γ und Δ zwei Kreise sind, so dass $\operatorname{inn}\Gamma \cap \Delta \neq \emptyset$ und $\operatorname{ext}\Gamma \cap \Delta \neq \emptyset$, dann $\Gamma \cap \Delta \neq \emptyset$.

Satz 4.66. *Wenn **E.** in einer Hilbert Ebene gilt, und $g \cap \operatorname{inn}\Gamma = A$, dann trifft die Gerade g den Kreis Γ in zwei Punkte.*

Beweis-Skizze: Sei $\Gamma = \Gamma_{O,R}$. Wenn $O \in g$, dann aus (KS1) gibt es zwei Punkte. Wenn $O \notin g$, dann sei $B \in g$ mit $OB \perp g$. Sei O' mit O_B_O' und $[OB] \equiv [OB']$. Sei $\Delta = \Gamma_{O',R'}$, mit $[OR] \equiv [O'R']$. Dann (KS1) $OO' \cap \Delta = \{C, D\}$. Sei C der Punkt mit $O \sim_{O'} C$.
Weil $A \in \operatorname{inn}\Gamma$, haben wir $[OA] < [OR]$. Da $\triangle OBA$ rechtwinklig ist, folgt $[OB] < [OA]$. Also auch $[O'B] < [O'R'] = [O'C]$ Also O'_B_C, und dann $O \sim_g C$.
Fall 1: O_C_B dann $[OC] < [OB] < [OR]$, also $C \in \operatorname{inn}\Gamma$.
Fall 1: C_O_B dann auch C_O_O' also $[OC] < [O'C] \equiv [OR]$, also $C \in \operatorname{inn}\Gamma$.
Anderseits, da $O\_O'\_D$ haben wir $[OR] \equiv [O'D] < [OD]$, also $D \in \operatorname{ext}\Gamma$.
Dann, aus **E.** folgt, dass $\Gamma \cap \Delta \ni E$. Wir wollen noch $E \in g$. Aus (SSS) haben wir $\triangle OEB \equiv \triangle O'EB$, also $EB \perp OO'$, also $BE = g$. Q.E.D.

Wenn **E.** gilt, dann haben wir auch Satz I.1. aus Euklids *Stoichea*.

Definition 4.67. Eine **Euklidische Ebene** ist eine Hilbert Ebene in der die Axiome $\mathbf{P}^+$**.** und **E.** gelten.

Wir erhalten in der Euklidischen Ebene (fast) alle Sätze der ersten vier Bücher der Elementen von Euklid. Hier ist ein kleines Beispiel:

Satz 4.68 (I.27)**.** *In einer Hilbert Ebene, seien A_E_B und C_F_D mit $AB \neq CD$ und $A \not\sim_{EF} D$. Wenn $\angle AEF \equiv \angle EFD$, dann $AB \parallel CD$.*

Beweis-Skizze: Wenn $G = AB \cap CD$, o.B.d.A $G \sim_{EF} B$, also auch $G \sim_{EF} D$. Dann in $\triangle GEF$ ist der Innenwinkel $\angle EFG$ kongruent zum Aussenwinkel $\angle AEF$ - Wiederspruch zu Satz 4.55. Q.E.D.

Für die umgekehrte Aussage brauchen wir Axiom $\mathbf{P}^+$**.**.

Satz 4.69 (I.29)**.** *In einer Euklidischen Ebene, wenn A_E_B und C_D_F mit $AB \neq CD$ und $AB \parallel CD$, dann $\angle FEA \equiv \angle EFD$.*

Beweis-Skizze: Seien G_E_H mit $\angle GEF \equiv \angle EFD$ (es existiert aus (KW1)). Dann, aus Satz 4.68 ist auch $GH \parallel CD$. Da $E \in GH$ und $E \in AB$, folgt aus (P), dass $GH = AB$, und also auch $\angle FEA \equiv \angle EFD$.

Q.E.D.

4.2.6 Weitere Axiome

[Hartshorne:] *The Archimedian principle, that given two line segments, some multiple of the first will exceed the second, is so embedded in our experience of the world that it is hard to imagine a geometry in which this would not hold. Even the farthest star has a distance from the earth that can be measured in light years, and even if we take the inch as our standard unit of length, some number of inches, albeit a very large number, will exceed the distance to that farthest star. As long as we retain the notion that geometry somehow represents the real world, we are bound to accept Archimedes' principle as a truth. In abstract mathematics, on the other hand, a geometry is anything that satisfies a certain set of axioms.*

Es gibt noch zwei Axiome, die aber weniger geometrisch sind, im Sinne, dass diese irgendwie auf die reelle Zahlen zurückzuführen sind. Das erste ist das Axiom von Archimedes (287-212 v.Chr - *Noli turbare circulos meos*)

(Arch.) Gegeben zwei Strecken $[AB]$,$[CD]$, $\exists\, n \in \mathbb{N}$, so dass $n \cdot [AB] > [CD]$.

Archimedes Axiom kommt aber in Euklids *Elemente* stillschweigend (Buch V), oder explizit (X.1) vor. Archimedes Axiom ist von allen Axiomen einer Euklidischen Ebene unabhängig, und man kann also von *Archimedische* und *nicht-Archimedische* Geometrie sprechen.
Das zweite ist das Axiom von Dedekind (1831-1916):

(Ded.) Wenn eine Gerade g als disjunkte Vereinigung $g = S \sqcup T$ geschrieben werden kann, wobei kein Punkt in S zwischen zwei Punkte in T liegt, und kein Punkt in T zwischen zwei Punkte in S liegt, dann $\exists! P \in g$ mit

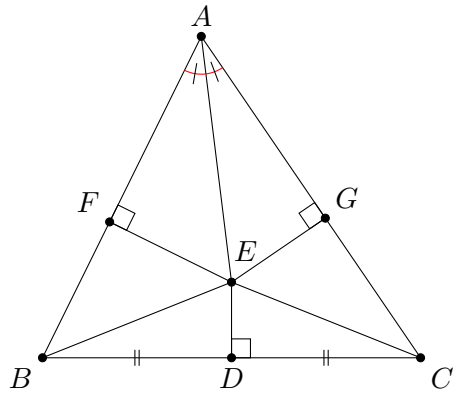
$$\forall\ A \in S, \forall\ B \in T \quad \Rightarrow \quad A = P \text{ oder } B = P \text{ oder } A\_\_P\_\_B.$$

Dieses Axiom ist sehr stark. Daraus folgen (Arch) und **E.**, und eine euklidische Ebene mit (D) kann nur $\mathbb{E}^2_{\mathbb{R}}$ sein. Das ist aber zu modern, zu startk, und Feinheiten über Konstruktionen mit Zirkel und Lineal.

4.3 Bilder können täuschen

In diesem Teil werden wir sehen, dass uns Bilder zu falschen Beweisen führen werden. Wir zeigen jetzt, dass jedes Dreieck gleichschenklig ist.

Falscher Beweis: Sei $\triangle ABC$ ein beliebiges Dreieck. Sei D der Mittelpunkt von $[BC]$ und sei E der Schnittpunkt der Mittelsenkrechten auf $[BC]$ mit der Winkelhalbierenden des Winkels $\angle BAC$. Seien dann F und G die Fußpunkte der Senkrechten aus E auf AB, beziehungsweise auf AC. Es gilt dann nach WWS, dass $\triangle AFE \equiv \triangle AGE$. Insbesondere haben wir



$$[AF] \equiv [AG].$$

Aus SWS haben wir $\triangle BDE \equiv \triangle CDE$. Wir haben dann in den rechtwinkligen Dreieken, dass $EF \equiv EG$ und $BE \equiv EC$. In rechtwinklingen Dreiecken gilt auch der Kongruenzsatz SSW, also $\triangle BFE \equiv \triangle CHE$, und somit

$$[BF] \equiv [CG].$$

Wir haben dann, aus dem Kongruenzaxiom **KS.3.**, dass $[AB] \equiv [AC]$. Also das beliebige Dreieck $\triangle ABC$ ist gleichschenklig.

Q.E.D?

4.4 Der Satz des Pythagoras

Satz 4.70 (Euklids Elemente, I.47)**.** *Im rechtwinkligen Dreieck ist das Quadrat über der dem rechten Winkel gegenüber liegenden Seite gleich den Quadraten über den Seiten, die ihn einschließen, zusammen.*

Dieser Satz ist einer der ältesten Theoreme der Geometrie. Wahrscheinlich auch das bekannteste. Pythagoras von Samos lebte um 500 v.Chr, aber der Satz war schon im antiken Babylon bekannt[10]. Man kann also vermuten, dass die Aussage seit mehr als 3000 Jahre bekannt ist. *Let that sink in for a moment.* Es gibt viele Beweise dieses Satzes. Wir schauen uns gleich einige davon an.

In diesem Kapitel wird das rechtwinklige Dreieck aus Pythagoras Satz $\triangle ABC$ heißen und der rechte Winkel wird $\angle A$ sein. Die klassischen Beweisen handeln nicht mit Längen als Zahlen und algebraische Gleichungen. Wir werden das aber in manche Beweise verwenden. Deswegen bezeichnen wir:

$$|AB| = a, \quad |AC| = b \,\text{und}\, |BC| = c.$$

Die Umkehrung des klassischen Satzes gilt auch, und somit wäre die vollständige Aussage:

$$a^2 + b^2 = c^2 \iff \measuredangle A = 90°.$$

Wir werden aber hier nur die klassische Richtung beweisen.

4.4.1 Euklids Beweis

Die Abbildung 4.4 auf Seite 109 unterstützt den folgenden Beweis. Wir fangen mit einer Konstruktion an.

Beweis: Wir errichten die Quadrate auf den Kanten des Dreiecks: $\square ABDE$, $\square ACGF$, und $\square BCHI$. Die Aussage des Satzes ist also, dass

$$\text{Fläche}(\square ABDE) + \text{Fläche}(\square ACGF) = \text{Fläche}(\square BCHI). \tag{4.2}$$

Wir errichten dafür die Höhe $[AJ]$ im Dreieck $\triangle ABC$ und verlängern diese bis sie die Kante HI des Quadrates $\square BCHI$ in dem Punkt K trifft. Die Strecke $[JK]$ trennt das Quadrat $\square BCHI$ in zwei Rechtecken: $BIKJ$ und $CHKJ$. Wir werden zweigen, dass jedes dieser Rechtecken dieselbe Fläche wie eines der Quadraten auf den Katheten hat. Weil das große Quadrat aus den beiden Rechtecken zusammengesetzt ist, wird daraus (4.2) folgen. Wir behandeln beide Katheten gleich, es reicht also zu zeigen, dass $\square ABDE$ und das Rechteck $BIKJ$ dieselbe Fläche haben. Dafür reicht es zu zeigen, dass

$$\text{Fläche}(\triangle ABD) = \text{Fläche}(\triangle BIJ), \tag{4.3}$$

weil die Flächen der Vierecken das doppelte der Flächen dieser Dreiecke sind. Dafür bemerken wir dass

$$\text{Fläche}(\triangle ABD) = \text{Fläche}(\triangle CBD),$$

[10] Es ist eigentlich nicht klar ob Pythagoras oder seine Folger (er war eher eine religiöse Persönlichkeit, als ein Mathematiker.) den Satz kannten

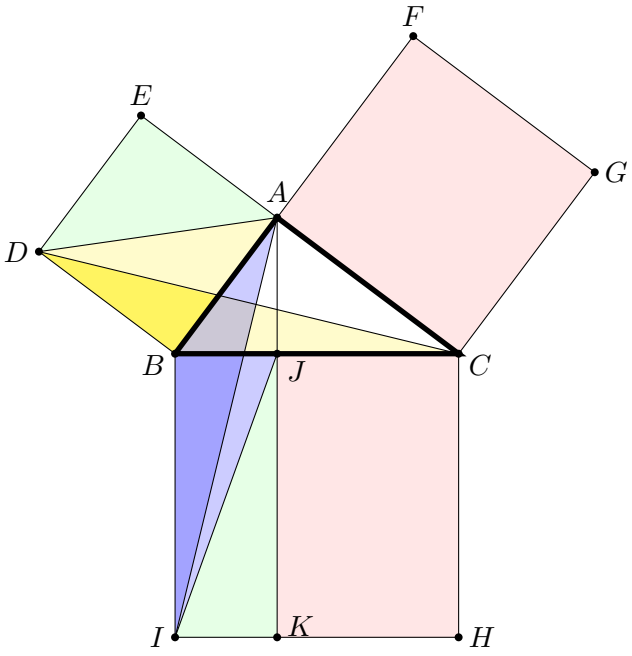


Abbildung 4.3: Fläche($\triangle ABD$)=Fläche($\triangle CBD$); $\triangle CBD \equiv \triangle IBA$; Fläche($\triangle IBA$)=Fläche($\triangle IBJ$);

weil $AC \parallel BD$. Es gilt auch $AJ \parallel BI$, also

$$\text{Fläche}(\triangle BIA) = \text{Fläche}(\triangle BIJ).$$

Der letzte Schritt ist zu Bemerken, dass $\triangle CBD \equiv \triangle BIA$. Das gilt aus SWS weil

$$[BC] \equiv [BI], \quad \angle CBD \equiv \angle ABI \text{ und } [BD] \equiv [BA].$$

Q.E.D.

4.4.2 Pyhtagoras Beweis

Dieser Beweis verwendet zwei unterschiedliche Aufschnitte eines Quadrates mit Seitenlänge $a + b$, wobei a und b die Längen der Katheten sind. Dabei entstehen jedes Mal vier gleiche Dreiecke, alle vier gleich zu dem gegebenen rechtwinkligen Dreieck. Das eine Mal entsteht noch ein Quadrat mit Seitenlänge c, die Länge der Hypotenuse. Das andere Mal entstehen zwei Quadrate mit Seitenlängen a, beziehungsweise b.

4.4.3 Algebraischer Beweis

Dieser Beweis ist auch sehr alt. Er kommt in dem Werk des Indischen Mathematiker Bhaskara ($\sim$1100 n.Chr.) vor. Man vermutet aber, dass er auch im Antiken Indien bekannt war.

Beweis: Wir nehmen an, ohne die Allgemeinheit zu beschränken, dass $a \geqslant b$. Dann kann man ein Quadrat mit Seitenlänge c in vier rechtwinkligen Dreiecken mit Seitenlängen a, b, c und einem kleinen

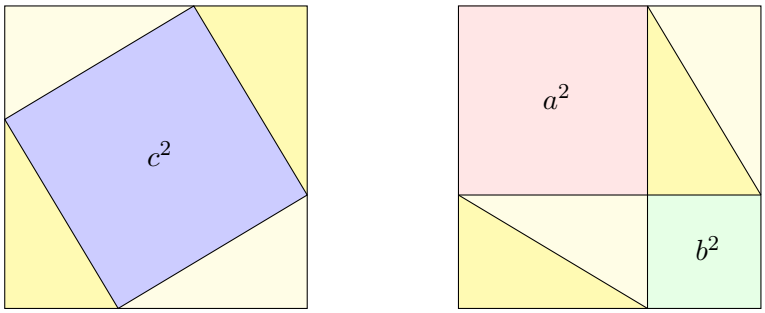


Abbildung 4.4: Pythagoras Beweis

Quadrat mit Seitenlänge $a - b$ aufschneiden (siehe Abbildung 4.5). Wir wissen, dass die Fläche des rechtwinkligen Dreiecks gleich mit $\frac{ab}{2}$ ist. Es gilt also:

$$c^2 = 4 \cdot \frac{ab}{2} + (a-b)^2 = 2ab + a^2 - 2ab + b^2 = a^2 + b^2.$$

Q.E.D.

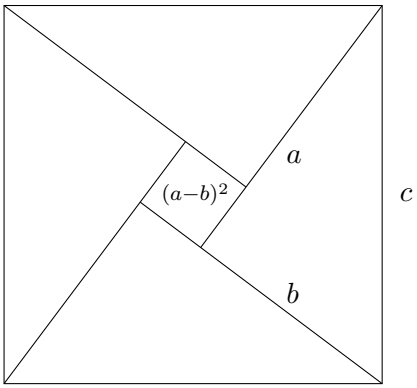


Abbildung 4.5: Algebraischer Beweis

4.4.4 Einsteins (?) Beweis

Es ist unsicher ob dieser Beweis tatsächlich von Albert Einstein[11] ist. Es ist aber sicher sehr einfach und elegant. Wir erinner, dass zwei Dreiecke **ähnliche Dreiecke** sind, genau dann wenn die Winkeln paarweise kongruent sind. Dafür schreiben wir $\triangle ABC \simeq \triangle MNP$. Es gilt also

$$\triangle ABC \simeq \triangle MNP \quad \Longleftrightarrow \quad \angle A \equiv \angle M, \quad \angle B \equiv \angle N \text{ und } \angle C \equiv \angle P.$$

In diesem Fall sind die entsprechenden Seiten der zwei Dreiecke proportional. Das heißt:

$$\frac{|AB|}{|MN|} = \frac{|BC|}{|NP|} = \frac{|CA|}{|PM|}.$$

[11] Siehe https://www.newyorker.com/tech/annals-of-technology/einsteins-first-proof-pythagorean-theorem.

Es folgt dann, dass auch die anderen wichtigen Strecken eines Dreiecks (d.h. die Höhen, die Winkelhalbierenden, die Seitenhalbierenden, das Radius des eingeschriebenen Kreises, usw.) auch Proportional sind. Weil die Fläche eines Dreiecks das Produkt zweier Längen ist, folgt daraus, dass die Flächen ähnlicher Figuren proportional zu den Quadraten der Seitenlängen sind. Genauer gesagt, wenn $[AD]$ die Höhe aus der Ecke A im Dreieck $\triangle ABC$ ist, und wenn $[MQ]$ die Höhe aus der Ecke M im ähnlichen Dreieck $\triangle MNP$ ist, dann gilt

$$\frac{|BC|}{|NP|} = \frac{|AD|}{|MQ|} \quad \text{also auch} \quad \frac{|AD|}{2|BC|} = \frac{|MQ|}{2|NP|} =: \alpha$$

Es folgt also, dass

$$\text{Fläche}(\triangle ABC) = \frac{|AD| \cdot |BC|}{2} = \frac{|AD|}{2|BC|} \cdot |BC|^2 = \alpha \cdot |BC|^2.$$

Analog, folgt auch $\text{Fläche}(\triangle MNP) = \alpha \cdot |NP|^2$.

Beweis: Wir haben im rechtwinkligen Dreieck $\triangle ABC$ ziehen wir die Höhe aus der Ecke des rechten Winkels: $[AD]$ (siehe Abbildung 4.6). Dann, gilt

$$\triangle ABC \simeq \triangle DBA \simeq \triangle DAC.$$

Es gilt dann

$$\text{Fläche}(\triangle ABC) = \text{Fläche}(\triangle DBA) + \text{Fläche}(\triangle DAC).$$

Aus der obigen Bemerkung und der Ähnlichkeit der Dreiecke existiert ein Proportionalitätsfaktor $\alpha \neq 0$ wir bekommen

$$\alpha \cdot |BC|^2 = \alpha \cdot |AB|^2 + \alpha \cdot |AC|^2.$$

Wir kürzen $\alpha \neq 0$ und bekommen die berühmte Gleichheit.

Q.E.D.

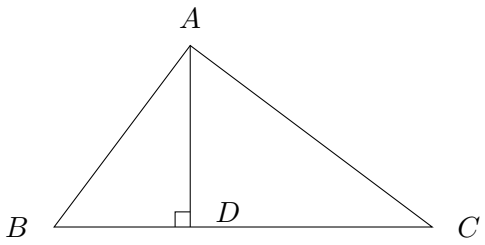


Abbildung 4.6: Eleganter Beweis

4.4.5 Epsteins Beweis

Ich glaube dieser Beweis wird Paul Sophus Epstein[12] (1883-1966) zugeordnet [Botema], aber ich muss weitere Quellen suchen. Die Beweisidee ist die drei Quadrate in Dreiecke zu zerschneiden und Kongruenzen zu finden. In der Abbildung 4.7 haben kongruente Dreiecke dieselbe Farbe.

Beweis: Wir fangen mit einer Konstruktion an (siehe Abbildung 4.7):

[12] also dem Physiker https://de.wikipedia.org/wiki/Paul_Sophus_Epstein, nicht dem Epstein der ...

- Man bildet die Quadrate auf den Seiten des gegebenen rechtwinkligen Dreiecks:

$$\square ABDE \qquad \square ACGF \qquad \square BCHI.$$

- Man zeichnet Winkelhalbierende $[AQ]$ des Winkels $\angle BAC$ und verlängert diese bis sie die Seite $[IH]$ in L schneidet.
- Die Diagonale $[DA]$ und die Diagonale $[GA]$ sind beide senkrecht auf $[AQ]$. Deswegen sind D, A, G kollinear.
- Man verlängert $[BI]$ bis diese $[DA]$ in J trifft.
- Man verlängert $[HC]$ bis diese $[GA]$ in K trifft.
- Man verlängert $[DB]$ bis diese $[AL]$ in M trifft.
- Man verlängert $[GC]$ bis diese $[AL]$ in N trifft.
- Man errichtet die Senkrechte in M auf $[AL]$ die $[BI]$ in O trifft.
- Man errichtet die Senkrechte in N auf $[AL]$ die $[CH]$ in P trifft.
- Man zeichnet noch die Kanten $[EJ]$, $[FK]$, $[MI]$ und $[NH]$.

Man verwendet dann die vielen 45° Winkel, die rechten Winkel, und die Kongruenten Seiten der Quadraten um alle Kongruenzen der bunten Dreiecken zu beweisen. [Ich muss das Bild noch mit kongruenten Winkel ergänzen].

Zum Beispiel:

- $\measuredangle QBA = \measuredangle JBD = 90° - \gamma$,
- $[AB] \equiv [DB]$ als Seiten des Quadrates $ABDE$.
- $\measuredangle BAQ = \measuredangle BDJ = 45°$.

Aus WSW folgt dann $\triangle ABQ \equiv \triangle DBJ$. Und so weiter...

Q.E.D.

4.4.6 Garfields Beweis

Das ist nicht der berühmte Kater, sondern der 20. Präsident der Vereinigten Staaten von Amerika, James Abram Garfield (1831-1881). Der Beweis stammt aus dem Jahr 1876.

Beweis: Man betrachte Abbildung 4.8 zur Unterstützung.

Auf der Halbgerade $[AC$ wählt man den Punkt D, sodass $A\_\_C\_\_D$ und $[CD] \equiv [AB]$. Man wählt ein Punkt E auf derselben Seite von AC wie B, sodass $[ED] \equiv [AC]$ und $\angle CDE$ ein rechter Winkel ist. Dann gilt

$$\triangle BAC \equiv \triangle DCE.$$

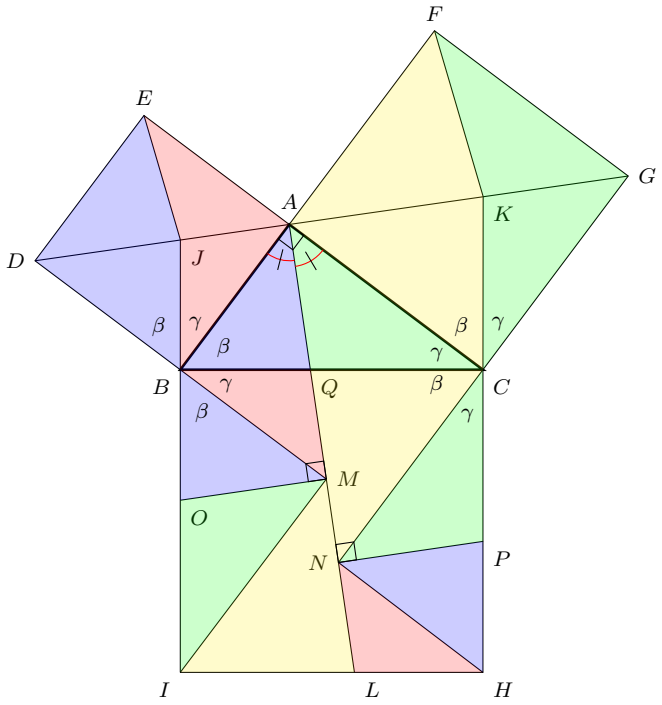


Abbildung 4.7: Epsteins Beweis: viele kongruente Dreiecke

Das Dreieck $\triangle BCE$ ist auch rechtwinklig in C. Weil $BA \parallel DE$ ist $ABED$ ein Trapez. Das heißt, der Flächeninhalt von $ABED$ ist

$$\text{Fläche}(ABED) = \frac{(|AB| + |DE|) \cdot |AD|}{2} = \frac{(a+b)(a+b)}{2}.$$

Anderseits gilt

$$\begin{aligned} \text{Fläche}(ABED) &= \text{Fläche}(\triangle ABC) + \text{Fläche}(\triangle CDE) + \text{Fläche}(\triangle BCE) \\ &= \frac{ab}{2} + \frac{ab}{2} + \frac{c^2}{2}. \end{aligned}$$

Es folgt somit $(a+b)^2 = 2ab + c^2$, also $a^2 + b^2 = c^2$. Q.E.D.

4.4.7 Da Vincis Beweis

Dafür brauchen wir erstmals die Kongruenz von n-Ecken zu definieren und zwei Sätze darüber zu beweisen.

Definition 4.71. Sei $n \geqslant 3$. Zwei (konvexe[13]) n-Ecke $A_1 \dots A_n$ und $B_1 \dots B_n$ sind kongruent, wenn für alle $i \in \{1, \dots, n\}$ gilt[14]

$$[A_i A_{i+1}] \equiv [B_i B_{i+1}] \text{ und } \angle A_{i-1} A_i A_{i+1} \equiv B_{i-1} B_i B_{i+1}.$$

[13] Eine Punktmenge $\mathcal{M}$ ist konvex, wenn für jede zwei beliebige Punkte P und Q aus $\mathcal{M}$ gilt $[PQ] \subseteq \mathcal{M}$. Ein n-Eck, das als Punktmenge aus der Vereinigung der Kanten $[A_i A_{i+1}]$ besteht, ist konvex, genau dann, wenn das n-Eck vereinigt mit seinem Inneren (der Schnitt der Inneren der Winkeln $\angle A_{i-1} A_i A_{i+1}$) eine konvexe Menge bildet.

[14] Man sollte an den Indizes als Elementen von $\mathbb{Z}/n\mathbb{Z}$ denken. Das heißt, $A_{n+1} = A_1$ und $A_0 = A_n$.

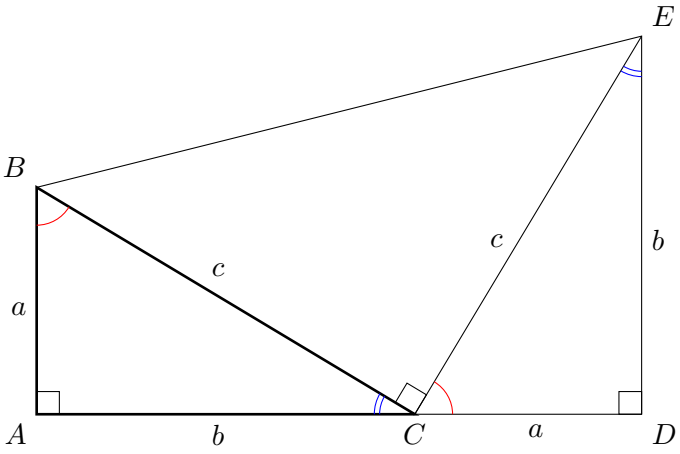


Abbildung 4.8: Garfields Beweis

Der folgende Satz gilt auch für nicht konvexe n-Ecke. Mir müssen aber dafür Winkel die größer als 180° sind einführen und mehrere Fälle unterscheiden. Wir beweisen also den Satz nur für konvexe n-Ecke.

Satz 4.72. *Kongruente n-Ecke haben dieselbe Fläche.*

Beweis-Skizze: Wir beweisen das durch Induktion nach n.

I.A. Die Aussage ist wahr für Dreiecke.

$n \Rightarrow n+1$ Seien $A_1 \dots A_{n+1}$ und $B_1 \dots B_{n+1}$ kongruente $(n+1)$-Ecke. Weil $n+1 \geqslant 4$, können wir $[A_1A_3]$ und $[B_1B_3]$ verwenden um die $(n+1)$-Ecke als die Vereinigung eines Dreiecks $(\triangle A_1A_2A_3)$mit einem n-Eck $(A_1A_3A_4 \dots A_{n+1})$ schreiben. Das gilt, weil die $(n+1)$-Ecken konvex sind, und somit auch die Strecke liegt im Innen.

Weil $[A_1A_2] \equiv [B_1B_2]$, $\angle A_1A_2A_3 \equiv \angle B_1B_2B_3$ und $[A_2A_3] \equiv [B_2B_3]$, folgt aus SWS, dass

$$\triangle A_1A_2A_3 \equiv \triangle B_1B_2B_3.$$

Es folgt also auch

$$[A_1A_2] \equiv [B_1B_2], \qquad \angle A_2A_1A_3 \equiv \angle B_2B_1B_3 \text{ und } \angle A_3A_1A_2 \equiv \angle B_3B_1B_2.$$

Aus den Winkelkongruenzen, weil (dank der Konvexität) $A_3 \in \operatorname{inn} \angle A_{n+1}A_1A_2$, folgt

$$\angle A_{n+1}A_1A_3 = \angle A_{n+1}A_1A_2 - \angle A_3A_1A_2 \equiv \angle B_{n+1}B_1B_2 - \angle B_3B_1B_2 = \angle B_{n+1}B_1B_3.$$

Analog bekommt man auch $\angle A_1A_3A_4 \equiv \angle B_1B_3B_4$ und somit die Kongruenz der n-Ecke:

$$A_1A_3A_4 \dots A_{n+1} \equiv B_1B_3B_4 \dots B_{n+1}.$$

Aus der induktiven Voraussetzung sind die Flächen der Dreiecke, beziehungsweise der n-Ecke gleich, also auch die Flächen Ihrer Vereinigungen. Q.E.D.

Für Dreiecke haben wir verschiedene Kongruenzsätze. In allen reicht es drei Kongruenzen zu finden

um alle sechs zu folgern. Der folgende Satz zeigt, dass wir bei n-Ecken $2n-3$ Kongruenzen, um die übrigen drei zu folgern, brauchen.

Satz 4.73. *Es seien $A_1 \dots A_n$ und $B_1 \dots B_n$ zwei n-Ecke. Wenn*

$$\begin{aligned} [A_iA_{i+1}] &\equiv [B_iB_{i+1}] \quad \forall i = 1, \dots, n-1 \text{ und} \\ \angle A_iA_{i+1}A_{i+2} &\equiv \angle B_iB_{i+1}B_{i+2} \quad \forall i = 1, \dots, n-2. \end{aligned}$$

dann $A_1 \dots A_n \equiv B_1 \dots B_n$.

Beweis-Skizze: Der Satz folgt durch dasselbe induktive Verfahren wie im Satz 4.72. Q.E.D.

Wir kommen endlich zum Beweis von Leonardo da Vinci.

Beweis: Wir fangen mit der Konstruktion an (siehe dafür die Abbildung 4.9).

- Wir errichten auf den Seiten von $\triangle ABC$ die Quadrate: $\square ABDE$, $\square ACGF$, und $\square BCHI$.
- Wir verbinden E mit F. Aus SWS folgt $\triangle BAC \equiv \triangle EAF$.
- $[DA]$ und $[AG]$ sind Diagonalen in den Quadraten $\square ABDE$, beziehungsweise $\square ACGF$. Das heißt, dass die Winkel $\angle DAB$ und $\angle GAC$ jeweils die Hälfte eines rechten Winkels sind. Weil der Winkel $\angle BAC$ ein rechter Winkel ist, folgt dass D, A und G kollinear sind.
- Wir konstruieren noch den Punkt J, sodass

  $$\angle JIH \equiv \angle ACB \text{ und } \angle IHJ \equiv \angle ABC.$$

  Dann, weil $[BC] \equiv [IH]$, folgt $\triangle ABC \equiv \triangle JHI$.

- Wir zeichnen noch die Strecke $[AJ]$.

Das Ziel ist zu zeigen, dass die Flächen der Sechsecken $ABIJHC$ und $DBCGFE$ gleich sind. Durch Abziehen der doppelten Fläche des Dreiecks $\triangle ABC$, bekommen wir dann die erwünschte Gleichheit.

Um die Gleichheit für die Sechsecken zu beweisen, zweigen wir, dass folgende Vierecken kongruent sind:

$$ABIJ \equiv DBCG \equiv DEFG \equiv JHCA.$$

Wir verwenden dafür den Satz 4.73. Wir haben

$$\begin{array}{ccccccccc} [\mathbf{AB}] & \equiv & [DB] & \equiv & [DE] & \equiv & [JH] & & \\ \angle ABI & \equiv & \angle DBC & \equiv & \angle DEF & \equiv & \angle JHC & = 90^\circ + \beta. \\ [BI] & \equiv & [\mathbf{BC}] & \equiv & [EF] & \equiv & [CH] & & \\ \angle BIJ & \equiv & \angle BCG & \equiv & \angle EFG & \equiv & \angle HCA & = 90^\circ + \gamma. \\ [IJ] & \equiv & [CG] & \equiv & [FG] & \equiv & [\mathbf{CA}] & & \end{array}$$

und somit die erwünschten Kongruenzen.

Q.E.D.

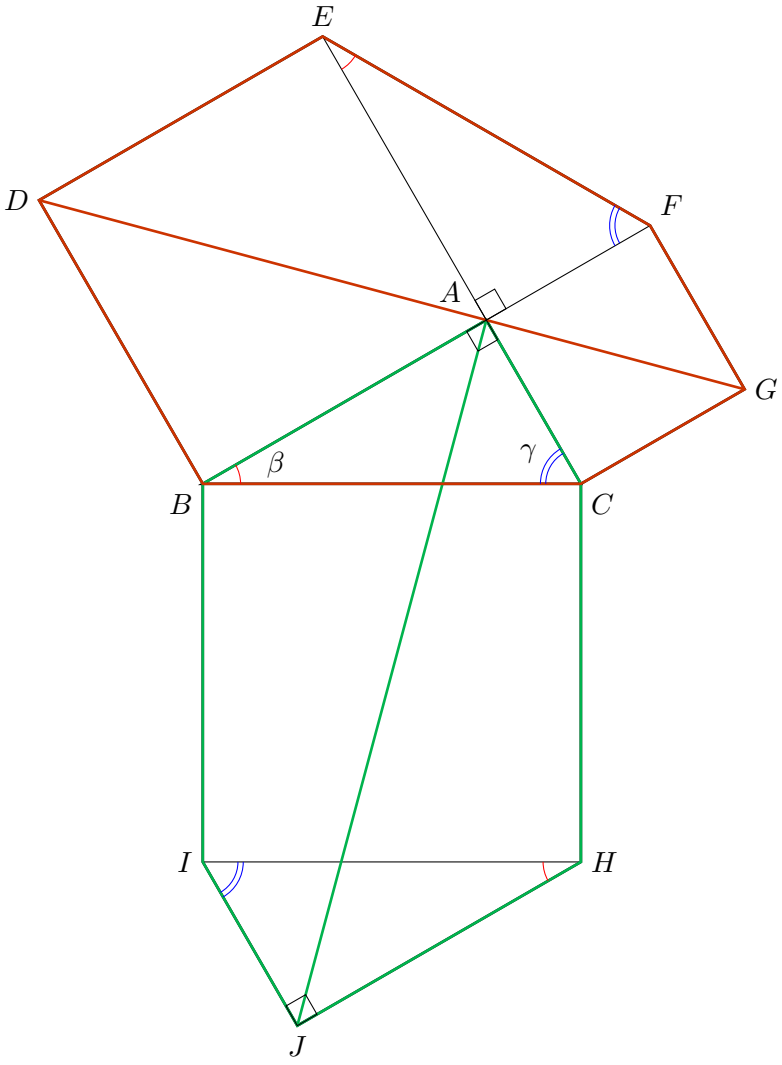


Abbildung 4.9: Leonardo Da Vinci's Beweis

4.4.8 Vektorieller Beweis

Der Nachteil dieses Beweises ist, dass wir unser Dreieck in $\mathbb{R}^2$ sehen müssen. Auf $\mathbb{R}^2$ haben wir das Skalarprodukt:

$$\langle \bullet , \bullet \rangle : \mathbb{R}^2 \times \mathbb{R}^2 \longrightarrow \mathbb{R}.$$

Das ist eine bilineare Abbildung. Das heißt insbesondere, dass für alle Vektoren v, v', w, w' gilt

$$\begin{aligned} \langle v, w - w' \rangle &= \langle v, w \rangle - \langle v, w' \rangle \text{ und} \\ \langle v - v', w \rangle &= \langle v, w \rangle - \langle v', w \rangle . \end{aligned}$$

Es gilt auch $\langle v, v \rangle > 0$ für alle $v \neq 0$. Die Länge (oder Norm) eines Vektors ist dann

$$\|v\| = \sqrt{\langle v, v \rangle}.$$

Zwei Vektoren v, w sind orthogonal[15] genau dann, wenn $\langle v, w \rangle = 0$.

Wenn $\triangle ABC$ ein Dreieck mit rechtem Winkel $\angle A$ ist, dann können wir die Koordinaten so wählen, dass $A = (0, 0)$, $B = (0, a)$ und $C = (0, b)$, mit $a, b \in \mathbb{R}_{>0}$. Wir definieren dann die Vektoren $v = (0, a)$ und $w = (0, b)$. Es gilt

$$\begin{aligned} \|v - w\|^2 = \langle v - w, v - w \rangle &= \langle v, v - w \rangle - \langle w, v - w \rangle \\ &= \langle v, v \rangle - \langle v, w \rangle - \langle w, v \rangle + \langle w, w \rangle \\ &= \langle v, v \rangle + \langle w, w \rangle \\ &= \|v\|^2 + \|w\|^2. \end{aligned}$$

wobei die dritte Gleichheit aus der Orthogonalität von v und w folgt. Weiterhin gilt $|AB| = \|v\|$, $|AC| = \|w\|$ und $|BC| = \|v - w\|$ und der Satz folgt.

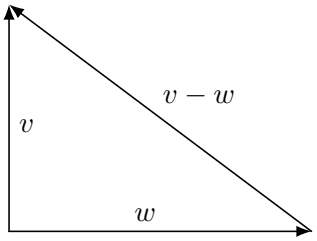


Abbildung 4.10: Vektorieller Beweis

[15] Das heißt, dass der Winkel zwischen ihnen ein rechter Winkel ist.

4.5 Körper

Wir haben gesehen, dass die Addition und die Multiplikation modulo n mehrere gemeinsame Eigenschaften mit der Addition und der Multiplikation der reellen Zahlen haben. Wenn n eine Primzahl ist, dann sind auch alle Restklassen außer der Nullklasse invertierbar. Wir sammeln diese Eigenschaften als Axiome zusammen um algebraische Körper zu definieren.

Definition 4.74. Ein **Körper** ist ein Tripel $(\mathbb{K}, +, \cdot)$, wobei $\mathbb{K}$ eine Menge ist, $+$ und $\cdot$ sind Abbildungen die **Addition**, beziehungsweise **Multiplikation** heißen:

$$\begin{aligned} + : \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} & \qquad \cdot : \mathbb{K} \times \mathbb{K} &\longrightarrow \mathbb{K} \\ (a, b) &\longmapsto a + b & (a, b) &\longmapsto a \cdot b \end{aligned}$$

und die die folgenden Axiome erfüllen:

(**K1**) Die Addition und die Multiplikation sind **assoziativ**. Das heißt, dass für alle $a, b, c \in \mathbb{K}$ gilt

$$a + (b + c) = (a + b) + c \qquad \text{und} \qquad a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

(**K2**) Die Addition und die Multiplikation sind **kommutativ**. Das heißt, dass für alle $a, b \in \mathbb{K}$ gilt

$$a + b = b + a \qquad \text{und} \qquad a \cdot b = b \cdot a.$$

(**K3**) Die Multiplikation ist über der Addition **distributiv**. Das heißt, dass für alle $a, b, c \in \mathbb{K}$ gilt

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

(**K4**) Für beide Operationen existieren **neutrale Elementen**: $0 \in \mathbb{K}$ und $1 \in \mathbb{K}$ mit $0 \neq 1$. Das heißt, für alle $a \in \mathbb{K}$ gilt

$$0 + a = a + 0 = a \qquad \text{und} \qquad 1 \cdot a = a \cdot 1 = a.$$

(**K5**) Es gibt **inverse Elementen** (außer der multiplikativen Inversen der Null). Das heißt:

- (**K5.1**) Für alle $a \in \mathbb{K}$ existiert $-a \in \mathbb{K}$, sodass $a + (-a) = (-a) + a = 0$.
- (**K5.2**) Für alle $a \in \mathbb{K} \setminus \{0\}$ existiert $a^{-1} \in \mathbb{K}$, sodass $a \cdot a^{-1} = a^{-1} \cdot a = 1$.

Ein Tripel wie in der obigen Definition, dass alle Axiome bis auf (**K5.2**) erfüllt heißt **kommutativer Ring mit 1**. Es gibt noch einen Unterschied: in einem Ring ist $0 = 1$ erlaubt. Dann gibt es nur aber ein einziges Element, weil $0 \cdot a = 0$ für alle a. Also $a = 1 \cdot a = 0 \cdot a = 0$ für alle a.

Beispiel 4.75. 1. $(\mathbb{R}, +, \cdot)$ den Körper der reellen Zahlen nehmen wir als bekannt an.

2. $(\mathbb{Q}, +, \cdot)$ der Körper der rationalen Zahlen. Wenn man den Körper der reellen Zahlen kennt, muss man zuerst bemerken, dass die Summe und das Produkt zweier rationaler Zahlen wieder eine rationale Zahlen ist. In anderen Worten, dass die Einschränkungen von $+$ und $\cdot$ von $\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$ auf $\mathbb{Q} \times \mathbb{Q} \longrightarrow \mathbb{Q}$ tatsächlich Abbildungen sind. Die Assoziativität, Kommutativität, Distributivität werden vererbt. Da 0 und 1 rationale Zahlen sind, werden diese auch vererbt. Es bleibt noch zu bemerken, dass wenn $q \in \mathbb{Q}$, dann ist auch $-q \in \mathbb{Q}$ und $q^{-1} = \frac{1}{q} \in \mathbb{Q}$ (wenn $q \neq 0$).

3. $(\mathbb{Z}, +, \cdot)$ ist kein Körper. Es ist aber ein kommutativer Ring mit 1. Der Beweis läuft wie im Fall von $\mathbb{Q}$. Fast alles funktioniert immer noch, wenn man $\mathbb{Q}$ mit $\mathbb{Z}$ ersetzt. Das einzige was nicht mehr gilt ist die Existenz von $\frac{1}{z} \in \mathbb{Z}$ für alle $z \in \mathbb{Z} \setminus \{0\}$.
4. $(\mathbb{N}, +, \cdot)$ ist kein Ring. Die Axiome (**K1-K4**) sind erfüllt, aber sowohl (**K5.1**) als auch (**K5.2**) gelten nicht.
5. $(\mathbb{C}, +, \cdot)$ der Körper der komplexen Zahlen. Die zugrunde liegende Menge ist

$$\mathbb{C} = \{a + bi \quad : \quad a, b \in \mathbb{R}\},$$

wobei die Addition und Multiplikation „die üblichen"sind wenn man i als Variable betrachtet, die $i^2 = -1$ erfüllt. Das heißt, für alle $a + bi, c + di \in \mathbb{C}$ haben wir

$$\begin{aligned} (a + bi) + (c + di) &= (a + c) + (b + d)i \\ (a + bi) \cdot (c + di) &= ac + adi + bci + bdi^2 \\ &= (ac - bd) + (ad + bc)i \end{aligned}$$

Es ist dann einfach zu überprüfen, dass die 0 und die 1 auch dabei sind:

$$0 = 0 + 0i, \qquad 1 = 1 + 0i.$$

Für $a + bi \in \mathbb{C}$ haben wir $-(a + bi) = (-a) + (-b)i$, und wenn $a + bi \neq 0$, dann haben wir

$$\begin{aligned} (a + bi)^{-1} &= \frac{1}{a + bi} \\ &= \frac{a - bi}{(a + bi)(a - bi)} \\ &= \frac{a - bi}{a^2 - (bi)^2} \\ &= \frac{a - bi}{a^2 + b^2} \\ &= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i. \end{aligned}$$

6. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit 1 für alle $n \in \mathbb{N}$. Wir haben in Satz 3.29 gezeigt, dass man eine Addition und eine Multiplikation auf der Menge der Restklassen definieren kann. Beide sind durch die entsprechende Operation auf Repräsentanten (also auf ganze Zahlen) definiert. Somit werden manche Eigenschaften vererbt: Assoziativität, Kommutativität, Distributivität.

$$\begin{aligned} [a] + ([b] + [c]) &= [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c], \\ [a] + [b] &= [a + b] = [b + a] = [b] + [a], \\ [a] \cdot ([b] + [c]) &= [a] \cdot [b + c] = [a(b + c)] = [ab + ac] = [a][b] + [a][c]. \end{aligned}$$

Die Assoziativität und die Kommutativität der Multiplikation funktioniert analog. Und auch direkt aus der Definitionen folgt für alle $[a] \in \mathbb{Z}/n\mathbb{Z}$:

$$[0] + [a] = [a], \quad [1] \cdot [a] = [a], \quad [a] + [-a] = [0].$$

7. In Satz 3.34 haben wir gesehen, dass $[a]$ genau dann ein multiplikatives Inverses in $\mathbb{Z}/n\mathbb{Z}$ hat, wenn $\mathrm{ggT}(a,n)=1$. Das heißt, aber nichts anderes als

$$(\mathbb{Z}/n\mathbb{Z},+,\cdot) \text{ ist ein Körper} \iff n \text{ eine Primzahl ist.}$$

   Es existieren also endliche Körper mit $2,3,5,7,11,13,\ldots$ Elementen. Gibt es Körper mit n Elementen für jedes $n\in\mathbb{N}_{>1}$?

8. Auf folgender Teilmenge von $\mathbb{R}$ haben wir auch eine Körperstruktur mit den Einschränkungen der reellen Operationen:

$$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \;:\; a,b\in\mathbb{Q}\}.$$

   Man überprüft einfach, dass die Summe und das Produkt zweier solcher Zahlen wieder in $\mathbb{Q}(\sqrt{2})$ liegen:

$$\begin{aligned}(a+b\sqrt{2})+(c+d\sqrt{2}) &= (a+c)+(b+d)\sqrt{2},\\ (a+b\sqrt{2})\cdot(c+d\sqrt{2}) &= (ac+2bd)+(ad+bc)\sqrt{2}.\end{aligned}$$

   Wir haben auch

$$0=0+0\sqrt{2},\quad 1=1+0\sqrt{2},\quad -(a+b\sqrt{2})=(-a)+(-b)\sqrt{2}.$$

   Das einzige wo man sich ein bisschen bemühen muss sind die multiplikativen Inversen: Wenn $a+b\sqrt{2}\neq 0$, dann gilt

$$(a+b\sqrt{2})^{-1}=\frac{1}{a+b\sqrt{2}}=\frac{a-b\sqrt{2}}{(a+b\sqrt{2})(a-b\sqrt{2})}=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}.$$

Eine wichtige Eigenschaft, die für alle Körper gilt ist:

$$\textit{Wenn } ab=0, \textit{ dann } a=0 \textit{ oder } b=0.$$

Die Begründung dafür ist: wenn $ab=0$ und $a\neq 0$, dann existiert $a^{-1}\in\mathbb{K}$, also

$$b=1\cdot b=(a^{-1}a)\cdot b=a^{-1}(ab)=a^{-1}0=0.$$

Bemerkung 4.76. In jedem Körper gilt:

$$0\cdot a=a\cdot 0=0 \quad \forall\, a\in\mathbb{K}.$$

Beweis-Skizze: Sei $a\in\mathbb{K}$ beliebig. Wegen der Kommutativität der Multiplikation reicht es $0\cdot a=0$ zu zeigen. Wir haben $0+0=0$ und aus der Distributivität bekommen wir

$$0\cdot a=(0+0)\cdot a=0\cdot a+0\cdot a.$$

Wenn wir auf beiden Seiten $-(0\cdot a)$ addieren dann haben wir:

$$\begin{aligned}-(0\cdot a)+(0\cdot a) &= -(0\cdot a)+\big(0\cdot a+0\cdot a\big)\\ 0 &= \big(-(0\cdot a)+0\cdot a\big)+0\cdot a\\ 0 &= 0\cdot a,\end{aligned}$$

wobei wir die Assoziativität der Addition und die Eigenschaft des additiven Inverses verwendet haben. Q.E.D.

4.6 Gleichungen

Es sollte intuitiv klar sein, was eine Gleichung ist. Wir wollen hier diese Intuition nicht abschaffen. Die kurze Einführung unten ist nur ein flüchtiger Blick in die Richtung einer mathematisch gründlichen Definition einer Gleichung.

Eine Gleichung mit Unbekannten $x_1, \ldots, x_n$ ist ein Prädikat[16] in dem das "="-Symbol genau ein Mal vorkommt, und für das man die Unbekannten x_i mit Elementen einer Menge ersetzten kann, sodass man eine Aussage bekommt (ein Satz von dem entschieden werden kann ob er wahr oder falsch ist). Eine Gleichung ist also keine Aussage. Die Unbekannten sind auch keine Elemente aus der Menge, in der man die Lösungen sucht. Zum Beispiel wenn man $2x-1=0$ in $\mathbb{R}$ lösen will, ist "x" keine reelle Zahl, sondern ein Symbol das man algebraisch behandeln kann. Das heißt, man kann es mit Koeffizienten multiplizieren und das Ergebnis zu anderen Unbekannten oder Koeffizienten addieren. Eine Gleichung ist eine Frage; die Antwort darauf ist eine Menge.

Das Wesentliche an einer Gleichung ist also, dass sie eine Lösungsmenge besitzt. Dazu muss man sich am Anfang klar machen, aus welcher Menge M die Lösungen kommen sollen. Dann besteht die Lösungsmenge einer Gleichung $\mathbf{G}(x_1, \ldots, x_n)$ mit Unbekannten $x_1, \ldots, x_n$ aus allen n-Tupeln in M^n, die bei dem Einsetzen in $\mathbf{G}$ eine wahre Aussage liefern:

$$\mathcal{L}_{\mathbf{G}} = \{(\alpha_1, \ldots, \alpha_n) \in M^n \ : \ \mathbf{G}(\alpha_1, \ldots, \alpha_n) \text{ ist eine wahre Aussage}\}.$$

4.6.1 Allgemeine Lineare Gleichungen

Eine **lineare Gleichung** mit Unbekannten $x_1, \ldots, x_n$ und mit Koeffizienten in einem Körper $\mathbb{K}$ ist eine Gleichung in der auf beiden Seiten des "="-Zeichens Polynome[17] von Grad $\leqslant 1$ in $\mathbb{K}[x_1, \ldots, x_n]$ vorkommen, und deren Lösungsmenge eine Teilmenge von $\mathbb{K}^n$ sein muss:

$$\mathbf{G}' : \qquad c_1x_1 + \cdots + c_nx_n + d = c'_1x_1 + \cdots + c'_nx_n + d'. \tag{4.4}$$

Zwei lineare Gleichungen $\mathbf{G}$ und $\mathbf{G}'$ mit n Unbekannten und Koeffizienten in $\mathbb{K}$ sind **äquivalent**, wenn diese dieselben Lösungsmengen haben. Eine schnelle Überprüfung der Axiome zeigt, dass diese Relation eine Äquivalenzrelation auf der Menge aller linearen Gleichungen (über $\mathbb{K}$ in $x_1, \ldots, x_n$) ist. Durch addieren in $\mathbf{G}'$ auf beiden Seiten mit dem Polynom $(-c'_1)x_1 + \cdots + (-c'_n)x_n + (-d')$ bleibt wegen der Kürzungsregel die Lösungsmenge unverändert. Wir sagen, dass eine solche Operation die **Form der Gleichung**[18] ändert. Jede lineare Gleichung kann also in die folgende Form gebracht werden:

$$\mathbf{G} \qquad a_1x_1 + \cdots + a_nx_n + b = 0 \qquad \text{mit } a_i, b \in \mathbb{K} \ \ \forall\, i = 1, \ldots, n. \tag{4.5}$$

[16] Das heißt eine Reihe von mathematischen Symbolen.

[17] Wir werden $\mathbb{K}[x_1, \ldots, x_n]$ nicht genau definieren; das bezeichnet den Ring der Polynome in den Variablen $x_1, \ldots, x_n$ mit Koeffizienten aus $\mathbb{K}$. Diese sind endliche Summen von *Monomen* mit Koeffizienten $c_i \in \mathbb{K}$:

$$\textstyle\sum_{i=1}^{n} c_i x_1^{d_{i,1}} \cdots x_n^{d_{i,n}}, \qquad d_{i,j} \in \mathbb{N}.$$

Der Grad eines Monoms ist die Summe der Exponenten: also $d_{i,1} + \cdots + d_{i,n}$. Grad $\leqslant 1$ heißt also, dass alle bis auf einen Exponent Null sind, und der eine ist kleiner als oder gleich mit 1. Deswegen haben wir die Form aus (4.4).

[18] Genauer gesagt, ändert sie den Repräsentanten der Äquivalenzklasse der Gleichung. Da wir aber an der Lösungsmenge interessiert sind, finde ich den Ausdruck „Form der Gleichung"suggestiver.

Eine **Lösung** der Gleichung $\mathbf{G}$ ist ein n-Tupel $(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n$, sodass $a_1\alpha_1 + \cdots + a_n\alpha_n + b = 0$ gilt. Wir nennen eine lineare Gleichung mit Koeffizienten in $\mathbb{K}$ auch $\mathbb{K}$-lineare Gleichung. Die Lösungsmenge der Gleichung (4.5) ist dann

$$\mathcal{L}_{\mathbf{G}} = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{K}^n \ : \ a_1\alpha_1 + \cdots + a_n\alpha_n + b = 0\}.$$

Definition 4.77. Ein **$\mathbb{K}$-lineares Gleichungssystem** (LGS) mit m Gleichungen in n Unbekannten $x_1, \ldots, x_n$ und Koeffizienten im Körper $\mathbb{K}$ ist eine Sammlung von m $\mathbb{K}$-linearen Gleichungen in $x_1, \ldots, x_n$. Eine **Lösung** des Gleichungssystems ist ein Element von $\mathbb{K}^n$ das (gleichzeitig) eine Lösung für alle m Gleichungen ist.

Jedes LGS kann auf folgender Form gebracht werden

$$(\mathbf{LGS}): \quad \begin{cases} \mathbf{G}_1: & a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n + b_1 &=& 0 \\ \mathbf{G}_2: & a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n + b_2 &=& 0 \\ \quad\vdots & \qquad\qquad\vdots & & \\ \mathbf{G}_m: & a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n + b_m &=& 0 \end{cases} \tag{4.6}$$

Die Lösungsmenge des linearen Gleichungssystems ist also

$$\mathcal{L}_{\mathbf{LGS}} = \mathcal{L}_{\mathbf{G}_1} \cap \cdots \cap \mathcal{L}_{\mathbf{G}_m}.$$

4.6.2 Lineare Gleichungen in zwei Unbekannten

Wir werden uns jetzt nur mit linearen Gleichungen in zwei Unbekannten x und y beschäftigen. Wir bezeichnen die Koeffizienten mit $a, b, c \in \mathbb{K}$. Wir betrachten also Gleichungen der Form

$$\mathbf{G}: \qquad ax + by + c = 0 \qquad \text{mit } a, b, c \in \mathbb{K}. \tag{4.7}$$

Fast alles was wir hier zeigen, kann auf den Fall mit $n \geqslant 1$ Unbekannten verallgemeinert werden.

Bemerkung 4.78. Wenn wir lineare Polynome addieren oder mit Elementen aus $\mathbb{K}$ multiplizieren, dann bekommen wir immer noch ein lineares Polynom. Das heißt, für alle $a, b, c, d, e, f, \lambda \in \mathbb{K}$ haben wir:

$$\begin{aligned} (ax + by + c) + (dx + ey + f) &= (a + d)x + (b + e)y + (c + f), \\ \lambda \cdot (ax + by + c) &= (\lambda \cdot a)x + (\lambda \cdot b)y + (\lambda \cdot c). \end{aligned}$$

Bemerkung 4.79. Sei $\ell = ax + by + c \in \mathbb{K}[x, y]$ ein lineares Polynom und sei $\lambda \in \mathbb{K} \setminus \{0\}$. Die folgende Gleichungen sind äquivalent:

$$\mathbf{G}: \quad \ell = 0 \qquad \text{und} \qquad \lambda\mathbf{G}: \quad \lambda \cdot \ell = 0.$$

Beweis-Skizze: Wir müssen die Gleichheit der folgenden Mengen zeigen:

$$\mathcal{L}_1 := \{(\alpha, \beta) \in \mathbb{K}^2 \ : \ a\alpha + b\beta + c = 0\} = \{(\alpha, \beta) \in \mathbb{K}^2 \ : \ (\lambda a)\alpha + (\lambda b)\beta + \lambda c = 0\} =: \mathcal{L}_2$$

Wir zeigen also die gegenseitige Inklusion.
$\boxed{\subseteq}$ Sei $(\alpha, \beta) \in \mathcal{L}_1$ beliebig. Also $a\alpha + b\beta + c = 0$. Wenn wir beide Seiten mit λ multiplizieren bekommen wir $\lambda\ell(\alpha, \beta) = \lambda \cdot 0 = 0$. Also $(\alpha, \beta) \in \mathcal{L}_2$.

$\boxed{\supseteq}$ Sei $(\alpha, \beta) \in \mathcal{L}_2$ beliebig. Also $(\lambda a)\alpha + (\lambda b)\beta + \lambda c = 0$. Weil $\lambda \neq 0$, existiert $\lambda^{-1} \in \mathbb{K}$ mit $\lambda^{-1} \cdot \lambda = 1$. Wir multiplizieren dann beide Seiten mit λ^{-1} und bekommen $\ell(\alpha, \beta) = 0$. Q.E.D.

Unser nächstes Ziel ist die Lösungsmenge einer allgemeinen Gleichung der Form (4.7) zu beschreiben. Dafür fangen wir mit linearen Gleichungen in einer einzigen Unbekannten an.

Lemma 4.80. *Die Lösungsmenge der $\mathbb{K}$-linearen Gleichung* $\mathbf{G}$ *in* ***einer Unbekannten***[19]

$$\mathbf{G}: \quad ax + b = 0 \quad (a, b \in \mathbb{K}) \qquad \textit{ist} \qquad \mathcal{L}_{\mathbf{G}} = \begin{cases} \emptyset & \textit{wenn } a = 0 \textit{ und } b \neq 0, \\ \mathbb{K} & \textit{wenn } a = 0 \textit{ und } b = 0, \\ \{-a^{-1}b\} & \textit{sonst.} \end{cases}$$

Beweis-Skizze: Wir haben zwei Fälle:

Fall 1: $a \neq 0$. Dann, weil $\mathbb{K}$ ein Körper ist und $a \neq 0$, existiert ein $a^{-1} \in \mathbb{K}$. Man kann damit die Gleichung auf beiden Seiten multiplizieren und bekommt

$$x + a^{-1}b = 0.$$

Wir addieren dann auf beiden Seiten $-a^{-1}b$ und bekommen somit

$$\{\alpha \in \mathbb{K} \ : \ a\alpha + b = 0\} = \{-a^{-1}b\} \ \text{ oder } \left\{-\frac{b}{a}\right\}.$$

Fall 2: $a = 0$**.** Dann ist die Lösungsmenge

$$\mathcal{L} = \{\alpha \in \mathbb{K} \ : \ 0 = b\}$$

und wir haben zwei Unterfälle:

$$\mathcal{L} = \begin{cases} \mathbb{K} & \text{wenn } b = 0, \\ \emptyset & \text{wenn } b \neq 0. \end{cases}$$

Wir haben also eine vollständige Beschreibung der Lösungsmenge in allen Fällen. Q.E.D.

Satz 4.81. *Die Lösungsmenge der $\mathbb{K}$-linearen Gleichung* $\mathbf{G}$ *in* ***zwei Unbekannten***

$$\mathbf{G}: \quad ax+by+c = 0 \quad (a, b, c \in \mathbb{K}) \qquad \textit{ist} \qquad \mathcal{L}_{\mathbf{G}} = \begin{cases} \emptyset & \textit{wenn } a = b = 0 \textit{ und } c \neq 0, \\ \mathbb{K}^2 & \textit{wenn } a = b = c = 0, \\ \textit{in Bijektion mit } \mathbb{K} & \textit{sonst.} \end{cases}$$

Beweis-Skizze: Wir betrachten wieder zwei Fälle.

Fall 1: $(a, b) = (0, 0)$. Dann haben wir

$$\mathcal{L}_{\mathbf{G}} = \{(\alpha, \beta) \in \mathbb{K}^2 \ : \ c = 0\} = \begin{cases} \mathbb{K}^2 & \text{wenn } c = 0, \\ \emptyset & \text{wenn } c \neq 0. \end{cases}$$

[19] **Vorsicht!** Die Gleichung $2x + 3 = 0$ könnte sowohl in einer als auch in zwei Unbekannten sein, mit dem Koeffizient von y gleich Null. Was sich dann ändert ist die Lösungsmenge. Man soll also immer die Anzahl der Unbekannten einer Gleichung verdeutlichen.

Fall 2: $(a, b) \neq (0, 0)$. Wir können oBdA[a] annehmen, dass $a \neq 0$. Wir können dann, nach Bemerkung 4.79 mit a^{-1} multiplizieren ohne die Lösungsmenge zu beeinflussen. Wir müssen also folgende Gleichung lösen:

$$x + a^{-1}by + a^{-1}c = 0 \tag{4.8}$$

Für jeden Wert $\beta \in \mathbb{K}$, den wir an Stelle von y einsetzen, bekommen wir eine lineare Gleichung in einer Unbekannten x. Der Koeffizient von x ist nicht Null, also folgt aus Lemma 4.80, dass wir für jedes β eine Lösung haben: $x = -a^{-1}b\beta - a^{-1}c$. Also

$$\mathcal{L} = \{(-a^{-1}b\beta - a^{-1}c, \beta) \quad : \quad \beta \in \mathbb{K}\}.$$

Das heißt, dass wir eine Abbildung $\mathbb{K} \longrightarrow \mathcal{L}$ mit

$$\beta \longmapsto (-a^{-1}b\beta - a^{-1}c, \beta)$$

haben. Diese hat eine Umkehrung $\mathcal{L} \longrightarrow \mathbb{K}$ gegeben durch $(\alpha, \beta) \longmapsto \beta$, es ist also eine bijektive Abbildung. Q.E.D.

[a] Sonst können wir die Koeffizienten und die Unbekannten umbenennen, sodass das der Fall ist.

Beispiel 4.82. Wie viele nicht-äquivalente lineare Gleichungen in einer und wie viele nicht-äquivalente lineare Gleichungen in zwei Variablen gibt ist für $\mathbb{K} = \mathbb{Z}/2\mathbb{Z}$? Und für $\mathbb{K} = \mathbb{Z}/3\mathbb{Z}$?

Satz 4.83. *Zwei $\mathbb{K}$-lineare Gleichungen $\mathbf{G}$ und $\mathbf{G}'$ sind genau dann äquivalent, wenn ein $\lambda \in \mathbb{K} \setminus \{0\}$ existiert, sodass $\lambda \cdot \mathbf{G} = \mathbf{G}'$.*

Beweis-Skizze: Eine Implikation wurde schon in Bemerkung 4.79 gezeigt. Es bleibt also zu zeigen, dass wenn zwei lineare Gleichungen äquivalent sind, dann existiert ein $\lambda \neq 0$ mit $\lambda \cdot \mathbf{G} = \mathbf{G}'$. Seien also $a, a', b, b', c, c' \in \mathbb{K}$ und zwei Gleichungnen

$$\mathbf{G}: \quad ax + by + c = 0 \qquad \text{und} \qquad \mathbf{G}': \quad a'x + b'y + c' = 0$$

mit $\mathcal{L} = \mathcal{L}'$, wobei diese $\mathcal{L}_{\mathbf{G}}$, beziehungsweise $\mathcal{L}_{\mathbf{G}'}$ bezeichnen.

Fall 1: $\mathcal{L} = \mathcal{L}' = \emptyset$. Dann folgt nach Satz 4.81 $a = b = a' = b' = 0$ und $c \neq 0 \neq c'$. Es existiert also $c^{-1} \in \mathbb{K}$. Dann haben wir $\lambda = c' \cdot c^{-1} \neq 0$.

$$\frac{c'}{c} \cdot \mathbf{G} = \mathbf{G}'.$$

Fall 2: $\mathcal{L} = \mathcal{L}' = \mathbb{K}^2$. Aus Satz 4.81 folgt, dass alle Koeffizienten Null sind. Also $1 \cdot \mathbf{G} = \mathbf{G}'$.

Fall 3: $\mathcal{L} = \mathcal{L}'$ sind beide in Bijektion mit $\mathbb{K}$. Dann folgt nach Satz 4.81 $(a, b) \neq (0, 0) \neq (a', b')$. Wir können oBdA annehmen, dass $a \neq 0$. Dann können wir $\mathbf{G}$ mit $\frac{1}{a} \cdot \mathbf{G}$ ersetzen und bekommen somit

$$\mathcal{L} = \{(\alpha, \beta) \in \mathbb{K} \quad : \quad \alpha + b\beta + c = 0\} = \Big\{\big(-(b\beta + c)\,,\ \beta\big) \quad : \quad \beta \in \mathbb{K}\Big\}.$$

Weil $\mathcal{L} = \mathcal{L}'$ haben wir für alle $\beta \in \mathbb{K}$:

$$-a'(b\beta + c) + b'\beta + c' = 0.$$

Wir bekommen also für $\beta = 0$, dass

$$-a'c + c' = 0 \quad \Longleftrightarrow \quad c' = a'c.$$

Also hat $\mathbf{G}'$ die Form $a'x + b'y + a'c = 0$. Wenn wir dann die Lösung für $\beta = 1$ einsetzen, haben wir

$$-a'(b + c) + b' + a'c = 0 \quad \Longleftrightarrow \quad -a'b + b' = 0 \quad \Longleftrightarrow \quad b' = a'b.$$

Also hat $\mathbf{G}'$ die Form $a' \cdot x + a'b \cdot y + a'c = a'(x + b \cdot y + c) = 0$. Das heißt

$$\mathbf{G}' = a' \cdot \Big(\frac{1}{a} \cdot \mathbf{G}\Big).$$

Wenn $a' = 0$ wäre, dann wäre auch $\mathcal{L}' = \mathbb{K}^2$. Da es aber nicht der Fall ist, muss $a' \neq 0$ sein. Wir setzen dann

$$\lambda = \frac{a'}{a}$$

und bekommen $\lambda\mathbf{G} = \mathbf{G}'$. Q.E.D.

Man sollte bemerken, dass wir im zweiten Teil des obigen Beweises konkrete Werte für $\beta \in \mathbb{K}$ eingesetzt haben. Diese waren 0 und 1, und diese gibt es immer in jedem Körper $\mathbb{K}$. Man könnte also sagen, dass dieser allgemeine Fall uns die Wahl einfacher gemacht hat: ohne weitere Voraussetzungen an $\mathbb{K}$ kennen wir keinen andere Elemente außer 0 und 1.

Wir werden lineare Gleichungssysteme mit zwei Gleichungen erst in dem nächsten Teil betrachten. Uns wird aber nur eine qualitative Eigenschaft der Lösungsmenge interessieren: nämlich wie viele Elemente diese enthalten kann6. Viel mehr über lineare Gleichungssysteme werden Sie in der Linearen Algebra lernen. Wir machen hier nur eine einfache allgemeine Bemerkung.

Bemerkung 4.84. Wenn $\mathbf{a} = (\alpha_1, \ldots, \alpha_n)$ eine Lösung des LGS mit zwei Gleichungen $\mathbf{G}_1$ und $\mathbf{G}_2$ ist, dann ist $\mathbf{a}$ auch eine Lösung der Gleichung§

$$\lambda\mathbf{G}_1 + \mu\mathbf{G}_2 \quad \forall\, \lambda, \mu \in \mathbb{K}.$$

Um das zu sehen braucht man nur $\mathbf{a}$ einzusetzen.

Teil II

Mathematik Entdecken 2

Kapitel 5

Gruppen und Symmetrie

Einführung

Was ist "symmetrischer" ein Quadrat oder ein gleichseitiges Dreieck? Ein Kreis oder ein Punkt? Das Polynom $x_1x_2x_3 - 1$ oder das Polynom $x_1x_2 - x_2x_3$? Wir werden in diesem Kapitel symmetrisch als das was unverändert unter gewisse bijektive Transformationen unverändert bleibt.

In der euklidischen ebenen Geometrie, dass heißt in der reellen $\mathbb{R}^2 = \{ (x, y) \ : \ x, y \in \mathbb{R} \}$ Ebene die mit dem euklidischen Abstand

$$\mathrm{d}\left((x_1, y_1), (x_2, y_2)\right) = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$$

ausgestattet ist, werden diese Transformationen *Isometrien* sein. Diese sind Abbildungen $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ mit der Eigenschaft, dass

$$\mathrm{d}(P, Q) = \mathrm{d}(f(P), f(Q) \quad \forall \ P, Q \in \mathbb{R}^2.$$

Allein aus dieser Eigenschaft folgen Bijektivität und Linearität. Das braucht aber einen relativ langen Beweis. Wichtiger noch wird sein, dass die Menge aller Isometrien zusammen mit der Verknüpfung von Abbildungen eine *Gruppe* bildet. Was das genau heißt werden wir bald sehen. Aber vorher will ich noch ein Beispiel erwähnen, das eine wichtige Rolle in der Symmetrie spielt: *die symmetrische Gruppe.* Es gibt eine solche Gruppe für jede natürliche Zahl n. Die Elementen der n-ten symmetrischen Gruppe sind die Permutationen von n Elementen. Eine Permutation von n Elementen ist nichts anderes als eine bijektive Abbildung von $\{1, \ldots, n\}$ in sich selbst.

Mit der Hilfe von Gruppen können wir genauer formulieren was wir unter "symmetrisch" meinen. Für Figuren in der euklidischen Ebene werden *die Symmetrien* die Isometrien sein, die Figur wieder auf sich selbst abbilden. Zum Beispiel, für ein gleichseitiges Dreieck sind diese die Drehungen um den Mittelpunkt[1] um 120 und um 240, und die Spiegelungen an den Geraden die jeweils eine Ecke mit dem Mittelpunkt der gegenüber liegenden Seite verbinden. Wenn man dazu die identische Transformation nimmt, also die Drehung um 0, dann haben wir alle sechs "Symmetrien" des Dreiecks. Wir werden sehen, dass diese eine Untergruppe der Isometrien bilden. Für das Quadrat gibt es insgesamt acht Symmetrien. Es gilt allgemein, dass jedes regelmäßiges n-Eck, mit $n \geqslant 3$, genau $2n$ Symmetrien hat. Was sind die Symmetrien des Kreises oder des Punktes?

[1] Damit ist der Mittelpunkt des Umkreises des Dreiecks gemeint; also der Schnittpunkt der Mittelsenkrechten der Seiten.

Für polynomielle Funktionen ist Symmetrie verbunden mit dem Vertauschen (also dem Permutieren) der Variablen sein. Funktionen, die unverändert bleiben wenn die Variablen auf allen möglichen Wege permutiert werden, heißen *symmetrisch*. Zum Beispiel

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 - 4x_1x_2 - 4x_1x_3 - 4x_2x_3 + 100$$

ist symmetrisch. Wenn man aber ein einziges Koeffizient ändert, zum Beispiel wenn man $-4x_1x_2$ mit $-5x_1x_2$ ersetzt und alles andere gleich lässt, dann ist die neue Funktion nicht mehr symmetrisch. Viele Phänomene die in der Wissenschaft besitzen eine natürliche Symmetrie, also die Gleichungen, die diese beschreiben sollen, müssen selber symmetrisch sein. Zum Beispiel wenn x_1, x_2, x_3 die Raumkoordinaten sind, dann entsprechen diese einer Wahl des Beobachters. Das Naturereignis bleibt unverändert, wenn wir die Koordinaten umbenennen. Die Gleichung die wir also suchen sollte auch diese Eigenschaft haben.

Die Gruppentheorie ist ungefähr 200 Jahre alt und ist eng verbunden mit der Entwicklung der modernen Mathematik und Wissenschaft. Die Ereignisse rund herum den Anfängen der Gruppentheorie sind fast genau so spannend und romantisch. Die Geschichte von Évariste Galois[2] werde ich aber hier nicht erzählen.

[2] 25. Oktober 1811 - 31. Mai 1832, war ein französischer Mathematiker und Revolutionär.

"*The date is 13 May 1832. In the dawn mist, two young Frenchmen face each other, pistols drawn, in a duel over a young woman. A shot is fired; one of the men falls to the ground fatally wounded. He dies two weeks later, from peritonitis, aged 21, and is buried in the common ditch – an unmarked grave. One of the most important ideas in the history of mathematics and science very nearly dies with him.*"

Ian Stewart, *Why Beauty is Truth*

5.1 Gruppen

In diesem Teil wird ein Grundbegriff der abstrakten Algebra einführen: Gruppen. Diese bilden die mathematische Struktur hinter dem allgemeinen Konzept der Symmetrie.

5.1.1 Innere Verknüpfungen

Definition 5.1. Eine **innere Verknüpfung** (oder **innere algebraische Operation**) auf einer Menge M ist eine Abbildung $* : M \times M \longrightarrow M$. Wir bezeichnen mit $a * b := *(a, b)$.

1. Die Verknüpfung $*$ heißt **assoziativ** wenn $a * (b * c) = (a * b) * c, \quad \forall\, a, b, c \in M$.
2. Die Verknüpfung $*$ heißt **kommutativ** wenn $a * b = b * a, \quad \forall\, a, b, \in M$.
3. Ein **neutrales Element** für $*$ ist ein Element $e \in M$ mit der Eigenschaft

$$e * m = m * e = m \quad \forall\, m \in M.$$

Bemerkung 5.2. Wenn es ein neutrales Element für $*$ gibt, dann ist dieses eindeutig.

Beweis-Skizze: Seien e, e' neutrale Elemente. Dann gilt $e' = e * e' = e$. Q.E.D.

Definition 5.3. Sei e ein neutrales Element der inneren Verknüpfung $*$ auf M.
Ein **linksinverses Element** für $m \in M$ bezüglich $*$ und e ist ein Element $m' \in M$ mit der Eigenschaft

$$m' * m = e.$$

Ein **rechtsinverses Element** für $m \in M$ bezüglich $*$ und e ist ein Element $m'' \in M$ mit der Eigenschaft

$$m * m'' = e.$$

Ein Element das sowohl linksinvers, als auch rechtsinvers von m ist heißt einfach **inverses Element** von m.

Wir haben schon links- und rechstinverse Elemente in Satz 1.33 gesehen. Wir sehen gleich in der nächsten Bemerkung, dass die Assoziativität zu guten Sachen führt.

Bemerkung 5.4. Sei $*$ assoziativ, mit neutralem Element $e \in M$. Wenn $m \in M$ sowohl ein linksinverses Element $m' \in M$ als auch ein rechtsinverses $m'' \in M$ bezüglich $*$ und e besitzt, dann sind diese gleich. Insbesondere, ist das inverse Element, wenn es existiert, eindeutig.

Beweis-Skizze: Seien m', m'' inverse Elementen von m bezüglich $*$ und e. Dann gilt

$$m' = m' * e = m' * (m * m'') = (m' * m) * m'' = e * m'' = m''.$$

Q.E.D.

Man kann auch nur links oder rechst neutrale Elemente definieren. Wir brauchen das nicht und machen das auch nicht.

Bezeichnung. Wir können also über *das* Inverse von m sprechen und wir werden es meistens durch m^{-1} bezeichnen. Wenn aber die Operation mit $+$ bezeichnet ist, dann bezeichnen wir auch das inverse Element von m mit $-m$.

Bemerkung 5.5. Sei M eine Menge und $*$ eine innere Verknüpfung auf M, die assoziativ ist und die ein neutrales Element e hat.

(i) Wenn $m \in M$ invertierbar ist, dann ist auch m^{-1} invertierbar und es gilt

$$(m^{-1})^{-1} = m.$$

(ii) Wenn $m, n \in M$ invertierbar sind, dann ist auch $m * n$ invertierbar und es gilt

$$(m * n)^{-1} = n^{-1} * m^{-1}.$$

Beispiele:

1. Addition und Multiplikation auf der $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Diese sind assoziativ, kommutativ, haben neutrales Element 0 bzw. 1. Inverse gibt es immer für die Addition. Für die Multiplikation gibt es Inverse in $\mathbb{Q}, \mathbb{R}$ beziehungsweise $\mathbb{C}$ genau dann, wenn $m \neq 0$. Multiplikative Inverse gibt es in $\mathbb{Z}$ nur für ± 1, und in $\mathbb{N}$ nur für die 1.
2. Für $X = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, bezeichnen wir mit $X^\times := X \setminus \{ 0 \}$. Die Multiplikation ist eine Operation auch für $X^\times$, aber die Addition ist keine Operation für $\mathbb{Z}^\times, \mathbb{Q}^\times, R^\times, X^\times$, weil $1 + (-1) \notin \mathbb{Z}^\times$ usw. Für $\mathbb{N}_{>0}$ ist aber die Addition eine innere Verknüpfung.
3. Für $X = [-2, 2] \subset \mathbb{R}$ sind $+$ und $\cdot$ keine Operationen.
4. Die modulare Operationen auf $\mathbb{Z}/n\mathbb{Z}$ sind auch innere Verknüpfungen (cf. Teil 3.5).
5. Die Abbildung $\frown : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$, definiert durch $a \frown b := a^b$ ist eine innere Verknüpfung auf $\mathbb{N}$. Diese ist aber nicht assoziativ:

$$2^{(3^4)} = 2^{81} = 2,417851\ldots \cdot 10^{24} \neq 4096 = (2^3)^4.$$

   Diese hat ein rechst-neutrales Element: 1; es gibt aber kein links-neutrales Element.
6. Ein kleines und abstraktes Beispiel zeigt, dass ohne Assoziativität, das inverse Element nicht eindeutig sein könnte. Operationen auf kleinen endlichen Mengen kann man gut durch Tafeln darstellen. Zum Beispiel, wenn $M = \{ e, a, b \}$ mit $e \neq a \neq b \neq e$, dann können wir folgende Verknüpfungstafel definieren:

$*$	e	a	b
e	e	a	b
a	a	e	e
b	b	e	e

   Wir können daraus lesen, dass $e * x = x * e = x, \quad \forall\, x \in M$, und dass $x * y = e, \ \forall x, y \in \{ a, b \}$. Also e ist ein neutrales Element und a hat zwei verschiedene Inversen: a und b. Das heißt, dass die Verknüpfung $*$ nicht assoziativ sein kann.

   Übung: *Man finde ein Tripel* $(\alpha, \beta, \gamma) \in M^3$, *sodass* $(\alpha * \beta) * \gamma \neq a * (\beta * \gamma)$.

7. Wenn M eine Menge ist, dann ist $\circ$ eine innere Verknüpfung auf

$$\mathrm{Iso}(M) = \{\, f : M \longrightarrow M \;\; : \;\; f \text{ ist bijektiv} \,\}.$$

Diese ist assoziativ, hat das neutrale Element id_M und jedes Element hat das inverse Element f^{-1}.

8. Knuths "uparrow" Bezeichnung $\uparrow$: $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ mit $a \uparrow b := a^b = a \cdot (a \cdot \ldots (a \cdot a)))$ wobei a kommt b-Mal vor.

Man kann das iterieren durch $\uparrow\uparrow$: $\mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$ indem man $a \uparrow\uparrow b := a \uparrow (a \uparrow \ldots (a \uparrow a))$, wobei a genau b-Mal vorkommt, definiert. Und so weiter: $a \uparrow^3 b := a \uparrow\uparrow\uparrow b := a \uparrow\uparrow (a \ldots (a \uparrow\uparrow a))$.

Die größte Zahl die in einem mathematischen Beweis vorkam ist *Graham's number* g_{64}. Man fängt mit $g_1 := 3 \uparrow\uparrow\uparrow\uparrow 3 = 3 \uparrow^4 3$ an, und definiert $g_n := 3 \uparrow^{g_{n-1}} 3$. Schon g_1 ist unvorstellbar groß.

$$\underbrace{3^{3^{\cdot^{\cdot^{\cdot^{3}}}}} \Big\} 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}} \Big\} \ldots \Big\} 3^{3^3} \Big\} 3}_{3\uparrow\uparrow\uparrow 3 = 3^{3^{\cdot^{\cdot^{\cdot^{3}}}}} \Big\} 3^{3^3} \} 3}$$

Die Zahl $3 \uparrow\uparrow\uparrow 3$ ist also ein Potenzturm der Höhe $3^{3^3} = 7625597484987 \approx 7{\cdot}10^{12}$, und das ist $\ggg$ das Volumen des beobachtbares Universums in Planck-Volumen gemäßen! (1 PVE $\approx 4,222 \cdot 10^{-105} m^3$.)

Dies sind Operationen, die weder assoziativ noch kommutativ sind und die kein neutrales Element besitzen (obwohl es ein rechts-neutrales Element gibt: $a \uparrow 1 = a \neq 1 \uparrow a$, wenn $a \neq 1$). Es existiert jedoch ein rechts-inverses Element: $a^0 = 1$. Wenn die Verknüpfung assoziativ wäre, würden sowohl ein rechts-neutrales als auch ein rechts-inverses Element existieren.

5.1.2 Grundlegende Definitionen der Gruppentheorie

Eine Gruppe wird oft als eine Menge zusammen mit einer Verknüpfung definiert. Das bringt die richtige Intuition ins Spiel, aber das "zusammen mit" kann genauer formuliert werden:

Definition 5.6. Eine **Gruppe** ist ein geordnetes Paar $(G, *)$, wobei G eine Menge ist und $*$ eine innere Verknüpfung auf G die folgende drei Axiome erfüllt ist.

Gr 1. $*$ ist **assoziativ**.

Gr 2. Es existiert ein **neutrales Element** $e \in G$.

Gr 3. Zu jedem $g \in G$ gibt es ein **inverses Element** g^{-1} bezüglich $*$ und e.

Eine Gruppe heißt **abelsch**[3] (oder kommutativ) wenn $*$ kommutativ ist. Wann immer die Verknüpfung klar aus dem Kontext ist, schreiben wir einfach G für die Gruppe $(G, *)$.

Aus den Bemerkungen 5.2 und 5.4 folgt, dass in jeder Gruppe das neutrale Element und das inverse Element immer eindeutig bestimmt sind. Aus **Gr 2.** folgt, dass $G \neq \emptyset$.

[3] nach dem norwegischen Mathematiker Niels Henrik Abel, 1802-1829.

Definition 5.7. Seien $(G_1, *)$ und $(G_2, \star)$ zwei Gruppen. Ein **Gruppenhomomorphismus** von G_1 nach G_2 ist eine Abbildung $\varphi : G_1 \longrightarrow G_2$ mit der Eigenschaft

$$\varphi(g * g') = \varphi(g) \star \varphi(g') \quad \forall\, g, g' \in G_1.$$

Ein Gruppenisomorphismus ist ein Gruppenhomomorphismus, das invertierbar als Gruppenhomomorphismus ist. Die genaue Formulierung ist die folgende.

Definition 5.8. Ein Gruppenhomomorphismus $\varphi : G_1 \longrightarrow G_2$ ist ein **Gruppenisomorphismus**, wenn es einen *Gruppenhomomorphismus* $\varphi^{-1} : G_2 \longrightarrow G_1$ gibt, sodass

$$\varphi \circ \varphi^{-1} = \mathrm{id}_{G_2} \quad \text{und} \quad \varphi^{-1} \circ \varphi = \mathrm{id}_{G_1}.$$

Wir sagen, dass zwei Gruppen G_1 und G_2 **isomorph** sind, wenn es ein Gruppenisomorphismus $\varphi : G_1 \longrightarrow G_2$ gibt. Wir schreiben in diesem Fall $G_1 \simeq G_2$.

In Lemma 5.17 werden wir sehen, dass ein bijektiver Gruppenhomomorphismus automatisch eine Isomorphismus ist. Die Formulierung aus Definition 5.8 hat den großen Vorteil, dass durch Ersetzen des Wortes "Gruppe", diese für viele andere mathematische Strukturen zu übernehmen ist. In manchen Fällen sind bijektive Morphismen wieder äquivalent zu Isomorphismen, aber nicht immer. Zum Beispiel, für topologische Räume gibt es bijektive Homomorphismen die nicht Isomorphismen sind.

Definition 5.9. Eine **Untergruppe** einer Gruppe $(G, *)$ ist eine Teilmenge $H \subseteq G$ die folgende Axiome erfüllt.

UG 1. Für alle $h_1, h_2 \in H$ gilt $h_1 * h_2 \in H$. (**Abgeschlossenheit**)

UG 2. Das neutrale Element e von G liegt auch in H. (**Neutrales Element**)

UG 3. Für jedes $h \in H$ gilt $h^{-1} \in H$. (**Inverses Element**)

Wir schreiben dafür $(H, *) \leq (G, *)$, öfter sogar $H \leq G$. Wenn $H \leq G$ aber $H \neq G$, dann schreiben wir $H \lneqq G$, $H \lneq G$, oder $H < G$.

Wenn **UG 1.** erfüllt ist, dann ist $*|_{H\times H} : H \times H \longrightarrow H$ eine wohl definierte, assoziative Verknüpfung auf H, und heißt die **induzierte** Verknüpfung auf H. In diesem Fall ist [**UG 2.** und **UG 3.**] äquivalent zu $[(H, *|_{H\times H})$ ist eine Gruppe].

5.1.3 Wichtige Beispiele

In der folgenden Liste stehen $+$ und $\cdot$ für die üblichen Addition, beziehungsweise Multiplikation.

1. Wir fangen mit einem nicht-Beispiel an. Die erste algebraische Struktur die man schon in der Schule lernt ist die Menge $\mathbb{N} = \{0, 1, 2, \dots\}$ der natürlichen Zahlen, zusammen mit der Addition. Diese ist assoziativ und hat ein neutrales Element: 0. Die positiven[4] natürlichen Zahlen sind aber nicht in $\mathbb{N}$ invertierbar:

   $$\text{Wenn } n > 0, \text{ dann } \nexists a \in \mathbb{N}, \text{ sodass } n + a = 0.$$

   Das heißt, dass $(\mathbb{N}, +)$ **keine Gruppe** ist.

[4] das hießt größer als Null.

In der Schule lernt man gleich nach der Addition die Subtraktion. Auf der Menge der natürlichen Zahlen ist das keine innere Verknüpfung, weil $a-b$ nicht immer in $\mathbb{N}$ liegt. Auf der Menge der ganzen Zahlen ist es eine innere Verknüpfung, es ist aber nicht assoziativ, und hat nur ein rechts-neutrales Element: die Null. Deswegen werden wir nicht über Subtraktion als algebraische Operation sprechen, sonder diese als Addition von inversen betrachten. Das heißt, für $a, b \in \mathbb{Z}$ ist

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

2. Die schon bekannten Zahlenmengen sind *additive*[5] abelsche Gruppen:

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +).$$

Das neutrale Element ist die Null, und das inverse Element von a bezüglich der Addition ist $-a$.

3. Dieselben Mengen sind **nicht Gruppen** zusammen mit der Multiplikation:

$$(\mathbb{Z}, \cdot), \quad (\mathbb{Q}, \cdot), \quad (\mathbb{R}, \cdot), \quad (\mathbb{C}, \cdot) - \textbf{nicht Gruppen!}.$$

Die Multiplikation ist in allen vier Fällen eine innere Verknüpfung, die assoziativ ist, und die auch ein neutrales Element hat: die Eins. Dieses sind aber nicht Gruppen, weil 0 nicht invertierbar bezüglich der Multiplikation ist. Das heißt, $\nexists a \in \mathbb{C}$, sodass $0 \cdot a = 1$.

4. In manchen Fällen reicht es die Null zu entfernen um eine multiplikative Gruppe zu finden. Wir bezeichnen hier $\mathbb{Q}^\times := \mathbb{Q}\setminus\{0\}$, $\mathbb{R}^\times = \mathbb{R}\setminus\{0\}$ und $\mathbb{C}^\times = \mathbb{C}\setminus\{0\}$. Die Multiplikation bleibt eine innere Verknüpfung auch auf diesen Mengen, und wir nehmen als bekannt an, dass die Gruppenaxiome für die folgenden drei Paare erfüllt sind.

$$(\mathbb{Q}^\times, \cdot), \quad (\mathbb{R}^\times, \cdot), \quad (\mathbb{C}^\times, \cdot).$$

5. Für $\mathbb{Z}$ reicht es nicht nur die Null zu entfernen. Die einzigen ganzen Zahlen, die invertierbar bezüglich der Multiplikation sind, sind -1 und 1. Also

$$(\mathbb{Z} \setminus \{0\}, \cdot) \qquad \textbf{ist keine Gruppe.}$$

Es ist wichtig zu betonen, dass wir immer über Invertierbarkeit *in der gegebenen Menge* sprechen. Das heißt, 22 ist nicht invertierbar in $\mathbb{Z}$, weil es keine ganze Zahl a gibt, sodass $22 \cdot a = 1$.

6. Die Modulare Operationen sind auch innere Verknüpfungen auf $\mathbb{Z}/n\mathbb{Z}$, wobei $n \in \mathbb{N}$. Es gilt:

$$(\mathbb{Z}/n\mathbb{Z}, +) \quad \text{ist eine Gruppe für alle } n \in \mathbb{N}.$$

Genau wie im Fall der komplexen Zahlen, damit wir eine Gruppe mit der Multiplikation finden, müssen wir nur die multiplikativ invertierbaren auswählen. Die modulare Multiplikation ist assoziativ und hat $[1]_n]$ als neutrales Element. Aus Bemerkung 5.5 folgt, dass die Einschränkung der Multiplikation eine innere Verknüpfung auf die Menge der multiplikativ-invertierbaren Elementen in $\mathbb{Z}/n\mathbb{Z}$ ist:

$$U(\mathbb{Z}/n\mathbb{Z}) = \left\{ [a]_n \in \mathbb{Z}/n\mathbb{Z} \;:\; \exists [a']_n \in \mathbb{Z}/n\mathbb{Z} [a]_n \cdot [a']_n = [1]_n \right\}.$$

In Satz 3.34 haben wir gesehen, dass

$$U(\mathbb{Z}/n\mathbb{Z}) = \left\{ [a]_n \in \mathbb{Z}/n\mathbb{Z} \;:\; \mathrm{ggT}(a, n) = 1 \right\}.$$

[5] das heißt nur, dass die Verknüpfung die gewöhliche Addition ist.

Insbesondere haben wir für jede Primzahl p, dass

$$(\mathbb{Z}/p\mathbb{Z} \setminus [0]_p, \cdot)$$

eine Gruppe ist.

7. Für jede Menge M ist die Menge aller bijektiven Selbstabbildungen

$$\mathrm{Sym}(M) = \{\, f : M \longrightarrow M \;\; : \;\; f \text{ ist bijektiv} \,\}$$

zusammen mit der Verknüpfung von Abbildungen eine Gruppe. Wir haben schon in Bemerkung 1.26 gesehen, dass ganz allgemein die Verknüpfung von Abbildungen assoziativ ist. Wenn $f, g : M \longrightarrow M$, dann sind diese immer verknüpfbar zu $f \circ g : M \longrightarrow M$ und $g \circ f : M \longrightarrow M$. Wenn beide bijektiv sind, dann sind auch beide Verknüpfungen bijektiv (Satz 1.33 (iii) und Bemerkung 1.36). Das heißt, dass die Verknüpfung von Abbildungen eine assoziative innere Verknüpfung auf $\mathrm{Sym}(M)$ ist. Das neutrale Element ist id_M und aus Satz 1.33 ist auch jedes Element in $\mathrm{Sym}(M)$ invertierbar.

Diese Gruppe ist besonders wichtig wenn die Menge M endlich ist. In diesem Fall, kann man annehmen, dass $M = \{\, 1, \ldots, n \,\}$ für ein $n \in \mathbb{N}_{>0}$ ist.

Definition 5.10. Die **symmetrische Gruppe** S_n ist die Gruppe $\mathrm{Sym}(\{\, 1, \ldots, n \,\}$ aller Bijektionen von $\sigma : \{\, 1, \ldots, n \,\} \longrightarrow \{\, 1, \ldots, n \,\}$ zusammen mit der Verknüpfung von Abbildungen. Ein Element $\sigma \in S_n$ heißt **Permutation** und wird aufgeschrieben als

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

8. Für jede Menge M können wir auch die Menge aller reellen Funktionen auf M definieren:

$$\mathcal{F}_{\mathbb{R}}(M) := \{\, f : M \longrightarrow \mathbb{R} \;\; : \;\; f \text{ ist eine Abbildung} \,\}.$$

Wenn M nicht $\mathbb{R}$ ist, dann kann man zwei Funktionen nicht mehr verknüpfen. Man kann aber eine Addition auf dieser Menge definieren. Für alle $f, g \in \mathcal{F}_{\mathbb{R}}(M)$ sei

$$f + g : M \longrightarrow \mathbb{R}, \qquad (f+g)(m) := f(m) + g(m) \;\; \forall\, m \in M.$$

Man sieht gleich, dass die Assoziativität der Addition auf $\mathbb{R}$ die Assoziativität der Addition auf $\mathcal{F}_{\mathbb{R}}(M)$ impliziert. Die konstante Funktion $0 : M \longrightarrow \mathbb{R}$, mit $0(m) = 0$ für alle $m \in M$ ist das neutrale Element, und das inverse einer Funktion $f : M \longrightarrow \mathbb{R}$ bezüglich der Addition von Funktionen ist die Funktion

$$-f : M \longrightarrow \mathbb{R} \qquad (-f)(m) = -(f(m)) \;\; \forall\, m \in M.$$

Das ist also auch eine Gruppe.

9. Matrizen mit $+$. Invertierbare $n \times n$ Matrizen mit Matrixmultiplikation.

5.1.4 Erste Eigenschaften

Bemerkung 5.11. Sei $(G, *)$ eine Menge mit inneren Verknüpfung $*$. Wenn folgende Axiome gelten, dann ist $(G, *)$ eine Gruppe.

Gr 1. $*$ ist assoziativ.

Gr 2'. Es existiert ein Element $e \in G$, sodass $e * g = g$, $\forall\ g \in G$. (links-neutrales Element)

Gr 3'. Zu jedem $g \in G$ gibt es ein links-inverses Element g' bezüglich $*$ und bezüglich jedem links-neutrales Element e.

Beweis-Skizze: Wir zeigen zu erst, dass wenn **Gr 1.**, **Gr 2.**, und **Gr 3'.** gelten, dann ist ein links-inverses Element auch rechts-invers, also dass **Gr 3.** gilt.
Sei $g \in G$, und sei g' sodass $g' * g = e$. Sei g'' ein links-inverses Element von g', also $g'' * g' = e$. Wir wollen zeigen, dass $g * g' = e$, also das g' auch ein rechst-inverses Element für g ist. Wir haben

$$\begin{aligned} g * g' &= (e * g) * g' && (\textbf{Gr 2'.}) \\ &= ((g'' * g') * g) * g' && (\textbf{Gr 3'.}) \\ &= (g'' * (g' * g)) * g' && (\textbf{Gr 1.}) \\ &= (g'' * e) * g' && (\textbf{Gr 3'.}) \\ &= g'' * (e * g') && (\textbf{Gr 1.}) \\ &= g'' * g' && (\textbf{Gr 2'.}) \\ &= e && (\textbf{Gr 3'.}) \end{aligned}$$

Wir zeigen jetzt, dass **Gr 2.** gilt, indem wir zeigen, dass wenn **Gr 1.**, **Gr 2'.**, und **Gr 3.** gelten, dann ist ein links-neutrales Element auch rechts-neutral. Sei $g \in G$ und e ein links-neutrales Element. Wir wollen also zeigen, dass $g * e = g$. Wir haben

$$g * e \overset{\textbf{Gr 3}}{=} g * (g' * g) \overset{\textbf{Gr 1}}{=} (g * g') * g \overset{\textbf{Gr 3}}{=} e * g \overset{\textbf{Gr 2'}}{=} g.$$

Q.E.D.

Da offensichtlich **Gr 2.** $\Rightarrow$**Gr 2'.** und **Gr 3.**$\Rightarrow$**Gr 3'.**, haben wir gezeigt, dass

$$[\textbf{Gr 1.} \text{ und } \textbf{Gr 2.} \text{ und } \textbf{Gr 3.}] \iff [\textbf{Gr 1.} \text{ und } \textbf{Gr 2'.} \text{ und } \textbf{Gr 3'.}].$$

Das heißt aber nicht, dass **Gr 3'.**$\Leftrightarrow$**Gr 3.** oder **Gr 2'.**$\Leftrightarrow$**Gr 2.** (Siehe das Beispiel 5. hier oben, und Satz 1.33 + ein Beispiel von injektive, aber nicht surjektive Abbildung). Wir hätten also eine Gruppe auch durch die Axiome **Gr 1.**,**Gr 2'.**, und **Gr 3'.** definieren können. Manche Autoren machen das auch. Ich finde, dass Definition 5.6 klarer ausdrückt was eine Gruppe ist. Der Nachteil ist, dass man mehr überprüfen muss um zu zeigen, dass etwas eine Gruppe ist. Aber, um schneller zu beweisen, dass eine Menge mit einer Verknüpfung eine Gruppe bildet, kann man immer Bemerkung 5.11 anwenden.

Die **Verknüpfungstafel** einer endlichen Gruppe mit n Elementen ist eine $n \times n$ Tabelle deren Spalten und Zeilen von den Elementen der Gruppe indiziert sind, sodass in der g-Zeile an der h-Stelle das Gruppenelement $g * h$ vorkommt. Die Reihenfolge der Elemente von G, sowohl in der Indexierung der Zeilen, als auch in der Indexierung der Spalten, ist dieselbe. Üblicherweise kommt das neutrale Element als erstes vor. Zum Beispiel, wenn $G = \mathbb{Z}/4\mathbb{Z}$ (also die Verknüpfung ist die Addition modulo 4) dann haben wir

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Folgendes Lemma hat als Folgerung, dass in jeder Zeile und in jeder Spalte jedes Gruppenelement genau ein Mal vorkommt. Es gilt also eine Art "Sudoku-Regel". Das Inverse von g kann man als den Spalten-Index des neutrales Elementes in der g-Zeile ablesen. Die Kommutativität entspricht der Symmetrie der Verknüpfungstafel bezüglich der Hauptdiagonale. Die Assoziativität kann man aus der Tafel nicht mehr gut lesen.

Lemma 5.12 (Kürzungsregeln)**.** *Sei $(G, *)$ eine Gruppe. Für alle $g_1, g_2, g_3 \in G$ gilt*

$$(g_1 * g_2 = g_1 * g_3 \implies g_2 = g_3) \qquad \text{und} \qquad (g_1 * g_3 = g_2 * g_3 \implies g_1 = g_2).$$

Beweis-Skizze: Wir verknüpfen linkst mit $g_1^{-1}*$ (bzw. rechts mit $* g_3^{-1}$) und wenden Assoziativität an. Q.E.D.

Bezeichnung. Wir haben die innere Verknüpfung mit $*$ bezeichnet, um zu betonen, dass es eine abstrakte Operation ist. Wir werden aber bald die bekannteren Symbole $+$ und $\cdot$ anwenden, mit der wichtigen Bemerkung, dass diese nicht unbedingt die Addition und die Multiplikation aus der Schule sind. Mit dieser Konvention, werden wir das neutrale Element der Verknüpfung $\cdot$ mit 1_G, oder einfach mit 1, bezeichnen. Das inverse Element bleibt g^{-1}. Für die Verknüpfung selbst werden wir

$$gh := g \cdot h$$

schreiben. Diese Verknüpfung muss nicht unbedingt kommutativ sein. Es kann also passieren, dass $gh \neq hg$.
Wenn wir die Verknüpfung auf G mit $+$ bezeichnen, ist die Konvention, dass diese Operation auch kommutativ ist. Wir haben unter dieser Notation für die Verknüpfung auch Soderbezeichnungen für neutrale und inverse Elemente: 0_G oder 0, und $-g$.

Die Assoziativität der Verknüpfung erlaubt uns die Verknüpfung endlich-vieler Elementen eindeutig zu definieren. Wenn die Operation $+$ oder $\cdot$ ist, dann schreiben wir

$$\begin{aligned} \textstyle\sum_{i=1}^n g_i &:= g_1 + g_2 + \cdots + g_n := ((g_1 + g_2) + \cdots + g_{n-1}) + g_n, \\ \textstyle\prod_{i=1}^n g_i &:= g_1 g_2 \dots g_n := ((g_1 \cdot g_2) \cdot \cdots \cdot g_{n-1}) \cdot g_n. \end{aligned}$$

Es ist wichtig, dass es *endlich* viele Elementen sind. Unendliche Summen und Produkte von Elementen sind in der abstrakten Algebra nicht definiert. Wenn $g_1 = \cdots = g_n = g$, dann schreiben wir

$$\begin{aligned} ng &:= \textstyle\sum_{i=1}^n g = g + \cdots + g, \\ g^n &:= \textstyle\prod_{i=1}^n g = g \cdot \cdots \cdot g. \end{aligned}$$

Wenn $n = 0$ dann ist die leere Summe per Definition gleich mit 0_G und das leere Produkt gleich mit 1_G. Für $n \in \mathbb{N}$ schreiben wir auch

$$\begin{aligned} (-n)g &:= \textstyle\sum_{i=1}^n -g = (-g) + \cdots + (-g), \\ g^{-n} &:= \textstyle\prod_{i=1}^n g^{-1} = g^{-1} \cdot \cdots \cdot g^{-1}. \end{aligned}$$

Bemerkung 5.13. Wenn $(G, \cdot)$ eine Gruppe ist, dann gilt für alle $a, b \in \mathbb{Z}$:

$$g^a \cdot g^b = g^{a+b}.$$

Insbesondere gilt $g^n \cdot g^{-n} = g^0 = e$, also $(g^n)^{-1} = g^{-n}$.

Beispiel 5.14. S_3 ist die kleinste nicht-kommutative Gruppe. Es hat als Elemente

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Wir haben $\sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \sigma_4\sigma_5 = e$. Diese Gruppe ist nicht kommutativ, weil $\sigma_1\sigma_2 = \sigma_5 \neq \sigma_4 = \sigma_2\sigma_1$. Die Operationstafel von S_3 ist

$\circ$	e	σ_1	σ_2	σ_3	σ_4	σ_5
e	e	σ_1	σ_2	σ_3	σ_4	σ_5
σ_1	σ_1	e	σ_5	σ_4	σ_3	σ_2
σ_2	σ_2	σ_4	e	σ_5	σ_1	σ_3
σ_3	σ_3	σ_5	σ_4	e	σ_2	σ_1
σ_4	σ_4	σ_2	σ_3	σ_1	σ_5	e
σ_5	σ_5	σ_3	σ_1	σ_2	e	σ_4

Weiterhin, jede endliche Gruppe ist einer symmetrischen Gruppe S_n als Untergruppe "enthalten"[6] Die Korrespondenz basiert sich auf der Beobachtung, dass jedes Element g einer Gruppe G eine bijektive Abbildung definiert: $\cdot g : G \longrightarrow G$ durch $x \mapsto x \cdot g$. Diese Abbildung ist bijektiv, weil das Inverse die Inverse definiert: $\cdot g^{-1} = (\cdot g)^{-1}$. Für endliche Gruppen können wir dann einen injektiven Gruppenhomomorphismus (cf. Definition 5.7) $G \longrightarrow S_{|G|}$ durch

$$G \ni g \mapsto \cdot g \in S_{|G|}$$

definieren.

Satz 5.15. *Eine Teilmenge $H \subseteq G$ ist genau dann eine Untergruppe von G, wenn $H \neq \emptyset$ und*

$$\forall\ a, b \in H \ \Rightarrow\ ab^{-1} \in H. \tag{5.1}$$

Beweis-Skizze: $\boxed{\Rightarrow}$ Wir nehmen an, dass für H die Axiome aus Definition 5.9 gelten. Aus **UG 2.** gilt $e \in H$, also $H \neq \emptyset$. Seien jetzt $a, b \in H$ beliebig. Aus **UG 3.** folgt $b^{-1} \in H$ und aus **UG 1.**, dass $ab^{-1} \in H$.

$\boxed{\Leftarrow}$ Weil $H \neq \emptyset$ existiert $h \in H$. Wir können dann in (5.1) $a = b = h$ einsetzen und bekommen:

$$ab^{-1} = hh^{-1} = e \in H.$$

Also **UG 2.** gilt. Wir wählen jetzt ein beliebiges $h \in H$ und setzen $a = e \in H$ (weil wir **UG 2.** bewiesen haben, dürfen wir das machen) und $b = h$ in (5.1) ein. Es folgt

$$ab^{-1} = eh^{-1} = h^{-1} \in H.$$

[6] wir brauchen Gruppenhomomorphismen, um das genau auszudrücken.

Also Axiom **UG 3.** gilt auch. Wir wählen jetzt $h_1, h_2 \in H$ beliebig. Wir setzten $a = h_1$. Aus **UG 3.** gilt $h_2^{-1} \in H$, und wir setzen dann $b = h_2^{-1}$. Es folgt dann aus (5.1):

$$ab^{-1} = h_1(h_2^{-1})^{-1} = h_1 h_2 \in H,$$

und somit gilt auch das Axiom **UG 1.**. Q.E.D.

Definition 5.16. Es sei $\varphi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus. Der **Kern** von φ ist die Faser über e_2, wobei e_2 das neutrale Element von G_2 ist. Wir bezeichnen den Kern mit $\operatorname{Ker}\varphi$, und haben also

$$\operatorname{Ker}\varphi := \{\, g \in G_1 \;:\; \varphi(g) = e_2 \,\}.$$

Der Kern ist also per Definition eine Teilmenge von G_1. Für jede Abbildung hatten wir in Teil 1.2.5 das **Bild** definiert. Wir können insbesondere also für einen Gruppenhomomorphismus $\varphi : G_1 \longrightarrow G_2$ über

$$\operatorname{Bild}\varphi := \{\, g_2 \in G_2 \;:\; \exists\, g_1 \in G_1 \varphi(g_1) = g_2 \,\}$$

sprechen. Das ist a priori eine Teilmenge von G_2. Wir werden in Lemma 5.18 zeigen, dass beide diese Mengen sogar Untergruppen sind. Zu erst zeigen wir aber einige elementare Eigenschaften von Gruppenhomomorphismen.

Lemma 5.17. *Es seien $(G_1, *)$ und $(G_2, star)$ zwei Gruppen und $\varphi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus. Bezeichne e_i das neutrale Element von G_i für $i = 1, 2$.*

(i) $\varphi(e_1) = e_2$.

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$.

(iii) *φ ist injektiv* $\Longleftrightarrow \operatorname{Ker}\varphi = \{\, e_1 \,\}$.

(iv) *φ ist surjektiv* $\Longleftrightarrow \operatorname{Bild}\varphi = G_2$.

(v) *Wenn φ bijektiv, dann ist $\varphi^{-1} : G_2 \longrightarrow G_1$ auch ein Gruppenhomomorphismus.*

Beweis-Skizze:

(i) Sei $g \in G_1$. Es gilt

$$\varphi(g) \star \varphi(e_1) = \varphi(g * e_1) = \varphi(g) = \varphi(g) \star e_2.$$

Nach der Kürzungsregel (Lemma 5.12 folgt $\varphi(e_1) = e_2$.

(ii) Sei $g \in G_1$ beliebig. Wir haben

$$\varphi(g) \star \varphi(g^{-1}) = \varphi(g * g^{-1}) = \varphi(e_1) = e_2.$$

Also, weil G_2 eine Gruppe ist, folgt aus der Eindeutigkeit des inverses Elementes, dass $\varphi(g)^{-1} = \varphi(g^{-1})$.

(iii) $\boxed{\Rightarrow}$ Wir haben aus Punkt (i), dass $e_1 \in \operatorname{Ker}\varphi$. Nehmen wir an, dass $g \in \operatorname{Ker}\varphi$ beliebig. Das bedeutet

$$\varphi(g) = e_2 = \varphi(e_1).$$

Aus der Injektivität von φ folgt dann $g = e_1$. Also $\operatorname{Ker}\varphi = \{\, e_1 \,\}$.

$\boxed{\Leftarrow}$ Es seien $g, h \in G_1$ mit $\varphi(g) = \varphi(h)$. Wenn wir beide Seiten der Gleichung rechts mit

$\varphi(h)^{-1}$ verknüpfen und Punkt (ii) anwenden, dann bekommen wir

$$\begin{aligned} \varphi(g) \star \varphi(h)^{-1} &= \varphi(h) \star \varphi(h)^{-1} \\ \varphi(g) \star \varphi\left(h^{-1}\right) &= e_2 \\ \varphi\left(g * h^{-1}\right) &= e_2. \end{aligned}$$

Also $g * h^{-1} \in \operatorname{Ker} \varphi$. Aus der Voraussetzung, ist $\operatorname{Ker} \varphi = \{e_1\}$, also

$$g * h^{-1} = e_1.$$

Wenn wir $*h$ auf beiden Seiten der Gleichheit anwenden, dann bekommen wir

$$g * h^{-1} * h = e_1 * h$$

also aus den Gruppenaxiomen, dass $g = h$. Somit ist φ injektiv.

(iv) Das ist einfach eine Umformulierung der Definition der Surjektivität (Definition 1.27).

(v) Wir müssen zeigen, dass

$$\varphi^{-1}(g' \star h') = \varphi^{-1}(g') * \varphi^{-1}(h') \quad \forall\ g', h' \in G_2.$$

Es seien $g', h' \in G_2$ beliebig. Weil φ bijektiv ist, existieren eindeutige $g, h \in G_1$, sodass

$$\varphi(g) = g' \quad \text{und} \quad \varphi(h) = h'.$$

Es gilt also auch $\varphi^{-1}(g') = g$ und $\varphi^{-1}(h') = h$. Wir haben dann

$$\begin{aligned} \varphi^{-1}(g' \star h') &= \varphi^{-1}(\varphi(g) \star \varphi(h)) && \text{(Definition von } g' \text{ und } h'.) \\ &= \varphi^{-1}(\varphi(g * h)) && \text{(weil } \varphi \text{ ein Homomorphismus ist)} \\ &= (\varphi^{-1} \circ \varphi)(g * h)) && \text{(Verknüpfung von Abbildungen)} \\ &= \mathrm{id}_{G_1}(g * h)) && \text{(weil } \varphi^{-1} \text{ die Inverse ist)} \\ &= g * h && \text{(Identische Abbildung)} \\ &= \varphi^{-1}(g') * \varphi^{-1}(h'). && \text{(Definition von } g' \text{ und } h'.) \end{aligned}$$

Q.E.D.

Lemma 5.18. *Es seien $(G_1, *)$ und $(G_2, \star)$ zwei Gruppen und $\varphi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus. Es gilt:*

(i) $\operatorname{Ker} \varphi$ *ist eine Untergruppe von* G_1.

(ii) $\operatorname{Bild} \varphi$ *ist eine Untergruppe von* G_2.

Beweis-Skizze:

(i) Seien $g, h \in \operatorname{Ker}\varphi$. Laut Satz 5.15 müssen wir zeigen, dass $g * h^{-1} \in \operatorname{Ker}\varphi$. Wir haben

$$\varphi(g * h^{-1}) = \varphi(g) \star \varphi(h^{-1}) = \varphi(g) \star (\varphi(h))^{-1} = e_2 \star (e_2)^{-1} = e_2.$$

Also $g * h^{-1} \in \operatorname{Ker}\varphi$.

(ii) Seien $g', h' \in \operatorname{Bild}\varphi$. Das heißt, es existieren $g, h \in G_1$, sodass

$$\varphi(g) = g' \quad \text{und} \quad \varphi(h) = h'.$$

Wir haben nach Bemerkung 5.17 (iii), dass $(h')^{-1} = (\varphi(h))^{-1} = \varphi(h^{-1})$. Es gilt also

$$g' \star (h')^{-1} = \varphi(g) \star \varphi(h^{-1}) = \varphi(g * h^{-1}) \in \operatorname{Bild}\varphi.$$

Q.E.D.

Satz 5.19. *Jede Untergruppe von $(\mathbb{Z}, +)$ hat die Form $n\mathbb{Z} := \{\, nz \;:\; z \in \mathbb{Z} \,\}$, für ein gewisses $n \in \mathbb{N}$.*

Beweis-Skizze: Sei $H < \mathbb{Z}$. Wenn $H = \{\, 0 \,\}$, dann $H = 0\mathbb{Z}$. Wenn $H \neq \{\, 0 \,\}$, dann $\exists\ h \in H$, mit $h \neq 0$. Da auch $-h \in H$, folgt, dass die Menge $H_+ := \{\, h \in H \;:\; h > 0 \,\}$ nicht leer ist. Weil $\mathbb{N}$ wohl geordnet ist, folgt dass es ein Minimum $n := \min H_+$ hat. Wir zeigen jetzt, dass $H = n\mathbb{Z}$.
$\boxed{\supseteq}$ Gilt offensichtlich aus (UG1) und (UG3).
$\boxed{\subseteq}$ Sei $h \in H$. Wir nehmen an, dass $h > 0$ (sonst ersetzten wir es mit $-h$). Aus Satz 3.3 folgt $\exists\ q, r \in \mathbb{Z}$ mit $0 \leqslant r < n$ so dass $h = qn + r$. Es gilt also

$$r = h - qn.$$

Aus (UG1), dass $qn \in H$, aus (UG3), dass $-qn \in H$ und wieder aus (UG1), dass $h - qn \in H$. Also wenn $r \neq 0$, haben wir $r \in H_+$ mit $r < n$ – ein Widerspruch ↯ zu $n = \min H_+$. Q.E.D.

Satz 5.20. *Wenn $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ ein Gruppenhomomorphismus[7] ist, dann existiert ein $a \in \mathbb{Z}$, sodass*

$$\varphi(z) = a \cdot z \quad \forall\ z \in \mathbb{Z}.$$

Beweis-Skizze: Wir zeigen, dass dieses $a = \varphi(1)$ ist. Wir haben für $n \in \mathbb{N}_{>0}$

$$\varphi(n) = \varphi(1 + \cdots + 1) = \varphi(1) + \cdots + \varphi(1) = n \cdot \varphi(1) = a \cdot n,$$

wobei $1 + \cdots + 1$ und $\varphi(1) + \cdots + \varphi(1)$ genau n Summanden haben. Für 0 gilt auch $\varphi(0) = 0 = a \cdot 0$. Wenn $z < 0$, dann gilt $z = -n$ mit $n \in \mathbb{N}$ und wir haben $\varphi(-1) = -\varphi(1) = -a$. Es gilt also

$$\varphi(z) = \varphi(-n) = \varphi\big((-1) + \cdots + (-1)\big) = \varphi(-1) + \cdots + \varphi(-1) = n \cdot \varphi(-1) = n \cdot (-a) = a \cdot (-n) = a \cdot z.$$

Q.E.D.

[7] Wenn man $\mathbb{Z}$ als Gruppe erwähnt, ohne eine Verknüpfung anzugeben, dann versteht man immer die Addition der ganzen Zahlen als Gruppenoperation.

5.1.5 Das Direkte Produkt von Gruppen

Wenn $(G_1, *)$ und $(G_2, \star)$ zwei Gruppen sind, dann kann man eine Gruppenstruktur auf dem kartesischen Produkt $G_1 \times G_2$ der zwei Mengen definieren:

$$(g_1, g_2) \diamond (h_1, h_2) := (g_1 * h_1, g_2 \star h_2).$$

Das ist eine innere Verknüpfung auf $G_1 \times G_2 = \{ (g_1, g_2) \ : \ g_i \in G_i, i = 1, 2 \}$. Die Assoziativität von $\diamond$ folgt direkt aus der Assoziativität von $*$ und $\star$. Das neutrale Element in $G_1 \times G_2$ ist (e_1, e_2), wobei für $i = 1, 2$ ist e_i das neutrale Element von G_i. Das inverse Element von (g_1, g_2) ist

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$

Die obig definierte Gruppe $(G_1 \times G_2, \diamond)$ heißt das **direkte Produkt** der Gruppen G_1 und G_2.

Beispiele:

1. $(\mathbb{R}^2, +)$ wobei $(x_1, x_2) + (x_1', x_2') := (x_1 + x_1', x_2 + x_2)'$. Genau so auch $(\mathbb{Q}^2, +)$, $(\mathbb{Z}^2, +)$, $(\mathbb{C}^2, +)$, $(\mathbb{Q}^{\times 2}, \cdot)$, $(\mathbb{R}^{\times 2}, \cdot)$, $(\mathbb{C}^{\times 2}, \cdot)$.
2. Man kann auch mehr machen: $(\mathbb{R}^3, +)$, $(\mathbb{R}^4, +), \ldots,$ $(\mathbb{R}^n, +)$ usw. Es spielt keine Rolle, dass es die reellen Zahlen sind, das geht auch für beliebige Gruppen.
3. Allgemeiner: wenn $(G, *)$ eine Gruppe ist und $n \in \mathbb{N}_{>0}$, dann kann man auf $G^n := \underbrace{G \times \cdots \times G}_{n-\text{Mal}}$ eine Gruppenstruktur definieren, indem man

   $$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) := (g_1 * h_1, \ldots, g_n * h_n)$$

   setzt. Assoziativität ist klar. Das neutrale Element ist $(e, \ldots, e)$ und das inverse ist $(g_1, \ldots, g_n)^{-1} = (g_1^{-1}, \ldots, g_n^{-1})$. Konkret:
4. Noch allgemeiner: Wenn $(G_1, *_1), \ldots, (G_n, *_n)$ Gruppen sind, dann kann man auf $\prod_{i=1}^n G_i$ eine Gruppenstruktur definieren, indem man

   $$(g_1, \ldots, g_n) * (h_1, \ldots, h_n) := (g_1 *_1 h_1, \ldots, g_n *_n h_n)$$

5. $(\mathbb{R}_{>0}, \cdot)$ und $(\mathbb{R}/\mathbb{Z}, +) \simeq S^1$ sind auch Gruppen, und $\mathbb{R}_{>0} \times S^1 \simeq \mathbb{C}^\times$. Dieser Isomorphismus entspricht der Polardarstellung der komplexen Zahlen.

5.1.6 Die Ordnung eines Elementes

Sei $(G, \cdot)$ eine Gruppe mit neutralem Element e und sei $g \in G$ ein beliebiges Element.

Bemerkung 5.21. Wenn die Menge $\{ g^i \ : \ i \in \mathbb{N}_{>0} \}$ endlich ist, dann existiert ein $d \in \mathbb{N}_{>0}$, sodass

$$g^d = e.$$

Weil die Menge $\{ g^i \ : \ i \in \mathbb{N}_{>0} \}$ endlich ist, können nicht alle Potenzen von g paarweise unterschiedlich sein. Es existieren also $n, m \in \mathbb{N}_{>0}$ mit $n \neq m$ und $g^n = g^m$. Wir dürfen annehmen, dass $n > m$. Wenn wir also beide Seiten von $g^n = g^m$ mit $g^{-m} = (g^m)^{-1}$ multiplizieren, dann bekommen wir

$$g^{n-m} = g^{n-n} = e.$$

Definition 5.22. Für jedes Element $g \in G$ ist die **Ordnung des Elementes** g

$$\operatorname{ord} g = \begin{cases} \min \{\, k \in \mathbb{N}_{>0} \;:\; g^k \,\} & , \text{ wenn } \{\, k \in \mathbb{N}_{>0} \;:\; g^k \,\} \neq \emptyset, \\ \infty & , \text{ sonst.} \end{cases}$$

Proposition 5.23. *Sei $(G, \cdot)$ eine Gruppe und $g \in G$ mit $\operatorname{ord} g < \infty$. Die Abbildung $f_g : \mathbb{Z} \longrightarrow G$ definiert durch*

$$f_g(n) = g^n$$

ist ein Gruppenhomomoprhismus mit $\operatorname{Ker} f_g = (\operatorname{ord} g)\mathbb{Z}$.

Beweis-Skizze: Aus Lemma 5.18 ist $\operatorname{Ker} f_g$ eine Untergruppe von $\mathbb{Z}$. Aus Satz 5.19 existiert also ein $d \in \mathbb{N}_{>0}$, sodass $\operatorname{Ker} f_g = d\mathbb{Z}$. In dem Beweis des Satzes haben auch gesehen, dass $d = \min \{\, n \in \mathbb{Z}_{>0} \;:\; f_g(d) = 0 \,\}$. Das ist per Definition die Ordnung von g. Q.E.D.

Korollar 5.24. Sei $(G, \cdot)$ eine Gruppe, $g \in G$ und $m \in \mathbb{Z}$. Wenn $g^m = e$, dann gilt $\operatorname{ord} g \,|\, m$.

5.1.7 Die Symmetrische Gruppe

Sei $n \geqslant 1$. Wir haben schon in Definition 5.10 auf Seite 133 die symmetrische Gruppe S_n als die Menge aller Bijektionen $\sigma : \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\}$ zusammen mit der Verknüpfung von Abbildungen als Gruppenoperation definiert. Ein Element $\sigma \in S_n$ heißt Permutation und wird aufgeschrieben als

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}.$$

Ein einfacher induktiver Beweis, oder direktes Zählen, geben uns die Kardinalität von S_n:

$$\#S_n = n! = 1 \cdot \cdots \cdot n.$$

Insbesondere, haben S_1 und S_2 jeweils 1, beziehungsweise 2 Elementen. Das heißt, dass beide abelsche Gruppen sind. Wir haben gesehen (oder werden gesehen haben), dass Gruppen mit p Elementen, wenn p eine Primzahl ist, zyklisch, und somit kommutativ, sind. Außerdem, gibt es bis auf Isomorphismus nur zwei Gruppen mit 4 Elementen: $\mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Das heißt, dass wenn $\#G < 5$, dann ist G eine abelsche Gruppe. Die Gruppe S_3 hat $3! = 1 \cdot 2 \cdot 3 = 6$ Elemente, und ist nicht kommutativ. Es hat die Elemente:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Die Gruppe S_3 ist nicht kommutativ, weil

$$\sigma_1\sigma_2 = \sigma_5 \neq \sigma_4 = \sigma_2\sigma_1.$$

Das heißt, dass S_3 die kleinste[8] nicht-kommutative Gruppe ist. Für jedes $n \geqslant 4$ können wir auch Elemente $\sigma_1, \ldots, \sigma_5 \in S_n$ finden, die dieselbe Wirkung auf $1, 2, 3$ wie die $\sigma_k \in S_3$ haben, und alle $i \geqslant 4$ auf sich selbst abgebildet werden. Das beweist die folgende Bemerkung.

[8] Eigentlich haben wir nur gezeigt, dass es keine nicht-kommutative Gruppe mit weniger Elementen gibt. Es könnte aber theoretisch auch andere, nicht zu S_3 isomorphe Gruppen mit 6 Elementen geben, die auch nicht kommutativ sind. Wir werden aber sehen, dass die einzige andere Gruppe mit 6 Elementen $\mathbb{Z}/6\mathbb{Z}$ ist.

Bemerkung 5.25. Die Gruppe S_n ist genau dann kommutativ, wenn $n \geqslant 2$.

Sei $k \in \mathbb{N}_{>1}$. Ein **k-Zyklus** (oder zyklische Permutation der Länge k) ist eine Permutation $\sigma \in S_n$ mit der Eigenschaft, dass es paarweise unterschiedliche $i_1, \ldots, i_k \in \{1, \ldots, n\}$ gibt, sodass

$$\sigma(i_j) = i_{j+1} \quad \forall\, j = 1, \ldots, k \text{ (wobei die Indizes modulo } k \text{ verstanden werden}^{9}).$$

und $\sigma(\ell) = \ell$ für alle $\ell \in \{1, \ldots, n\} \setminus \{i_1, \ldots, i_k\}$. Wir schreiben in diesem Fall

$$\sigma =: (i_1\ i_2\ \ldots\ i_k).$$

In S_3 haben wir also außer der Identität drei 2-Zyklen: (12), (13), und (23) und zwei 3-Zyklen: (123) und (132). Man muss aufpassen, dass die Notation der Zyklen nicht eindeutig ist:

$$(123) = (231) = (312).$$

Aus der Zyklus-Notation allein ist auch nicht klar ob der obige 3-Zyklus in S_3, S_4 oder S_{101} lebt. Das sollte man vorher klar machen.

Zwei Zyklen $\gamma_1 = (i_1 \ldots i_r)$ und $\gamma_2 = (j_1 \ldots j_s)$ sind **disjunkt** wenn

$$\{\, i_1, \ldots, i_r \,\} \cap \{\, j_1, \ldots, j_s \,\} = \emptyset.$$

Für jede Permutation $\sigma \in S_n$ und jedes $i \in \{\, 1, \ldots, n \,\}$ definieren wir die **Bahn von i unter σ** als die Menge

$$\mathrm{Bahn}_\sigma(i) = \left\{\, \sigma^k(i) \;\; : \;\; k \in \mathbb{N} \,\right\}.$$

Wir nennen eine Bahn *nichttrivial* wenn $\#\,\mathrm{Bahn} > 1$.

Bemerkung 5.26. Für $i, j \in \{\, 1, \ldots, n \,\}$ gilt $\mathrm{Bahn}_\sigma(i) = \mathrm{Bahn}_\sigma(j)$ oder $\mathrm{Bahn}_\sigma(i) \cap \mathrm{Bahn}_\sigma(j) = \emptyset$. Daraus folgt, dass jede Permutation eine Äquivalenzrelation auf $\{\, 1, \ldots, n \,\}$ definiert:

$$i \sim_\sigma j \iff \mathrm{Bahn}_\sigma(i) = \mathrm{Bahn}_\sigma(j).$$

Die Äquivalenzklassen sind dann genau die Bahnen.

Beweis-Skizze: Es reicht zu zeigen, dass

$$\mathrm{Bahn}_\sigma(i) \cap \mathrm{Bahn}_\sigma(j) \neq \emptyset \quad \Rightarrow \quad \mathrm{Bahn}_\sigma(i) = \mathrm{Bahn}_\sigma(j).$$

Sei $k \in \mathrm{Bahn}_\sigma(i) \cap \mathrm{Bahn}_\sigma(j)$. Das heißt, es existieren $r, s \in \mathbb{N}_{>0}$, sodass

$$\sigma^r(i) = k = \sigma^s(j).$$

Daraus folgt, dass $\sigma^{r+(\mathrm{ord}\,\sigma - s)}(i) = \sigma^{\mathrm{ord}\,\sigma}(j) = \mathrm{id}(j) = j$. Wir bezeichnen mit $m := r + \mathrm{ord}\,\sigma - s$ und zeigen, dass $\mathrm{Bahn}_\sigma(j) \subseteq \mathrm{Bahn}_\sigma(i)$.

Sei also $a \in \mathrm{Bahn}_\sigma(j)$ beliebig. Es existiert dann ein $\ell \in \mathbb{N}_{>0}$, sodass $\sigma^\ell(j) = a$. Es folgt

$$a = \sigma^\ell(j) = \sigma^\ell(\sigma^m(i)) = \sigma^{\ell+m}(i) \in \mathrm{Bahn}_\sigma(i).$$

[9] Das heißt, dass wir $k+1$ und 1 identifizieren. Das spart uns die Fallunterscheidung: $\sigma(i_j) = i_{j+1}$ für $j = 1, \ldots, k-1$ und $\sigma(i_k) = i_1$.

Also $\text{Bahn}_\sigma(j) \subseteq \text{Bahn}_\sigma(i)$. Analog beweist man die andere Inklusion, also $\text{Bahn}_\sigma(i) = \text{Bahn}_\sigma(j)$. Q.E.D.

Für ein k-Zyklus $\gamma = (i_1 \ \dots \ i_k)$, mit $k \geqslant 2$, dann hat γ genau eine nichttriviale Bahn. Es gilt

$$\text{Bahn}_\gamma(i) = \begin{cases} \{ i_1, \dots, i_k \} & , \text{ wenn } i \in \{ i_1, \dots, i_k \} \\ \{ i \} & , \text{ wenn } i \notin \{ i_1, \dots, i_k \}. \end{cases}$$

Wir bezeichnen die eindeutige Bahn eines Zyklus γ mit

$$B(\gamma) = \{ i \ : \ \gamma(i) \neq i \}.$$

Die eindeutige Bahn bestimmt aber nicht den Zyklus. Disjunkte Zyklen kommutieren. Das folgt aus der allgemeineren Bemerkung

Bemerkung 5.27. Wenn $\sigma = \gamma_1 \cdots \gamma_r$ mit $B(\gamma_k) \cap B(\gamma_\ell) = \emptyset$ für $k \neq \ell$, dann gilt

$$\forall\, i \ \ \exists!\, k \quad \gamma_k(i) = \sigma(i) \quad \text{und} \quad \gamma_\ell(i) = i \quad \text{if } \ell \neq k.$$

Insbesondere, wenn γ und α disjunkte Zyklen sind, dann gilt

$$\gamma \cdot \alpha = \alpha \cdot \gamma.$$

Beweis-Skizze: Wenn $\sigma(i) \neq i$, aber es existiert nicht ein eindeutiges k wie oben, dann gibt es zwei Möglichkeiten:

Fall 1: Entweder $\gamma_k(i) = i$ für alle k. Aber dann gilt $(\gamma_1 \cdots \gamma_r)(i) = i \neq \sigma(i)$ - ↯.

Fall 2: Es existieren $k \neq \ell$ mit $\gamma_k(i) \neq i \neq \gamma_\ell(i)$. Aber das ist ein Widerspruch weil die Zyklen disjunkt sind. Q.E.D.

Satz 5.28. *Es sei $n \in \mathbb{N}_{>0}$. Für jede Permutation $\sigma \in S_n$ existieren eindeutige disjunkte Zyklen $\gamma_1, \dots, \gamma_r$, sodass*

$$\sigma = \gamma_1 \cdots \gamma_r.$$

Beweis-Skizze: Existenz.

Variante 1: Für jede Bahn die mehr als 1 Element hat, definieren wir einen Zyklus. Genauer gesagt, seien $\text{Bahn}_\sigma(i_1), \dots, \text{Bahn}_\sigma(i_r)$ alle unterschiedliche Bahnen mit $b_k := \#\,\text{Bahn}_\sigma(i_k) > 1$. Wir definieren dann

$$\gamma_k := (i_k \ \sigma(i_k) \ \dots \ \sigma^{b_k - 1}(i_k)).$$

Nach Bemerkung 5.26 sind die Zyklen $\gamma_1, \dots, \gamma_r$ disjunkt. Für jedes $i \in \{ 1, \dots, n \}$ haben wir:

Fall 1: Wenn $\#\,\text{Bahn}_\sigma(i) = 1$, dann gilt $\sigma(i) = i$ und auch $\gamma_k(i) = i$ für alle $k = 1, \dots, r$. Also

$$\sigma(i) = (\gamma_1 \cdots \gamma_r)(i).$$

Fall 2: Wenn $\#Bahn_\sigma(i) > 1$, dann existiert nach Bemerkung 5.26 ein einziges $k \in \{ 1, \dots, r \}$, sodass $\text{Bahn}_\sigma(i) = \text{Bahn}_\sigma(i_k)$. Das heißt, es existiert auch ein $j \in \{ 0, \dots, b_k - 1 \}$, sodass $i = \sigma^j(i_k)$. Daraus folgt,

$$\sigma(i) = \sigma(\sigma^j(i_k) = \sigma^{j+1}(i_k) = \gamma_k(i),$$

und $\gamma_\ell(i) = i$ für alle $\ell \neq k$. Es gilt also

$$\sigma(i) = (\gamma_1 \cdots \gamma_r)(i).$$

Variante 2: Man kann die Existenz auch durch Induktion beweisen. Dafür werden wir erstens für jede Permutation σ die Menge der von σ bewegten Elementen definieren:

$$B(\sigma) = \bigcup_{\#\,\mathrm{Bahn}_\sigma(i)>1} \mathrm{Bahn}_\sigma(i).$$

Das heißt, für ein $i \in \{\, 1, \ldots, n \,\}$ gilt

$$\sigma(i) \notin i \iff i \notin B(\sigma).$$

Wir werden dann n fixieren und dann die Aussage für alle $\sigma \in S_n$ durch Induktion nach $\#B(\sigma)$ beweisen. Die Aussage ist:

$$\mathcal{A}(k): \quad \#B(\sigma) = k \Rightarrow \ \sigma \text{ ist Produkt von disjunkten Zyklen.}$$

$\boxed{k = 0}$ Wenn $k = 0$, dann gilt $\sigma(i) = i$ für alle i, also $\sigma = \mathrm{id}$. Die Identität ist das leere Produkt disjunkter Zyklen.

$\boxed{\mathcal{A}(j) \ \ \forall j \leqslant k \Rightarrow \mathcal{A}(k+1)}$ Wir verwenden also die starke Induktion (siehe Bemerkung 2.22). Wir suchen dann das kleinste $i \in \{\, 1, \ldots, n \,\}$ mit $\sigma(i) \neq i$. Es gilt dann $\mathrm{Bahn}_\sigma(i) = \left\{\, i, \sigma(i), \ldots, \sigma^{b-1}(i) \,\right\}$, mit $b > 1$ und $\#\,\mathrm{Bahn}_\sigma(i) = b$. Wir definieren dann den b-Zyklus $\gamma \in \S_n$ durch

$$\gamma = (i \ \sigma(i) \ \ldots \ \sigma^{b-1}(i)).$$

Wir definieren auch $\tau \in S_n$ durch

$$\tau(j) = \begin{cases} \sigma(j) & , \text{ wenn } j \notin \mathrm{Bahn}_\sigma(i) \\ j & , \text{ wenn } j \in \mathrm{Bahn}_\sigma(i). \end{cases}$$

Es gilt dann $\#B(\tau) = \#B(\sigma) - b \geqslant k$ und $\mathbb{B}(\tau) \cap B(\gamma) = \emptyset$. Es gilt auch

$$\sigma = \gamma \cdot \tau,$$

also aus der induktiven Voraussetzung existieren $\gamma_2, \ldots, \gamma_r$ disjunkte Zyklen mit $\tau = \gamma_2 \cdots \gamma_r$. Es gilt auch $B(\gamma_k) \subseteq B(\tau)$, also $\gamma \cap \gamma_k = \emptyset$ für alle $k = 2, \ldots, r$. Somit haben wir

$$\sigma = \gamma \cdot \gamma_2 \cdots \gamma_r$$

ist ein Produkt disjunkter Zyklen.

Eindeutigkeit.

Jeder Zyklus hat genau eine nichttriviale Bahn. Das Produkt von r disjunkten Zyklen hat genau die r entsprechenden nichttriviale Bahnen. Also wenn $\gamma_1 \cdots \gamma_r = \sigma = \alpha_1 \cdots \alpha_s$, dann muss $r = s$ und $\text{Bahn}_{\gamma_k} = \text{Bahn}_{\alpha_k}$ gelten. Für jedes $i \in \{1, \ldots, n\}$ mit $\sigma(i) \neq i$ ein einziges k existiert mit $\sigma(i) = \gamma_k(i) = \alpha_k(i)$ und für alle anderen $\ell \neq k$ gilt $\gamma_\ell(i) = \alpha_\ell(i) = i$. Es folgt daraus, dass $\gamma_k = \alpha_k$ für alle $k = 1, \ldots, r$ und somit die Eindeutigkeit. Q.E.D.

Lemma 5.29. *Für jeden k-Zyklus $\gamma = (i_1 \ \ldots \ i_k) \in S_n$ gilt*

$$\gamma = (i_1 \ i_2) \cdots (i_{k-1} \ i_k).$$

Beweis-Skizze: Übung Q.E.D.

Lemma 5.30. *Für jede Transposition $(i \ j) \in S_n$ können wir annehmen, dass $i < j$ und es gilt*

$$\begin{aligned} (i \ j) &= (i \ i+1) \cdots (j-1 j) \\ &= (1 \ j) \cdot (1 \ j-1) \cdots (1 \ i) \end{aligned}$$

Korollar 5.31. Jede Permutation $\sigma \in S_n$ kann sowohl als Produkt der Transpositionen $(1\ 2), \ldots, (n-1\ n)$, als auch als Produkt der Transpositionen $(1\ 2), \ldots, (1, n)$ geschrieben werden.

Die Darstellungen aus dem obigen Korollar sind nicht unbedingt eindeutig. Zum Beispiel

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

Die Signatur einer Permutation

Auch wenn die Anzahl von Transpositionen nicht eindeutig ist, wir werden gleich sehen, dass die Parität der Anzahl von Transpositionen konstant ist. Deswegen werden wir sagen, dass eine Permutation **gerade** ist, wenn die Anzahl der Faktoren in einer Zerlegung als Produkt von Permutationen gerade ist. Wenn diese Anzahl ungerade ist, dann sagen wir dass die Permutation **ungerade** ist. Man muss aber zu erst beweisen, dass diese Definitionen Sinn[11] haben. Dafür führen wir folgender Begriff ein.

Definition 5.32. Das **Vorzeichen** (oder das **Signum** oder die **Signatur** oder die **Parität**) einer Permutation $\sigma \in S_n$ ist

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Das ist intrinsisch definiert, also man muss sich keine Sorgen machen, dass es Sinn macht.
Man kann das Signum auch durch über folgender Begriff beschreiben,

Definition 5.33. Sei $\sigma \in S_n$. Ein **Fehlstand** (oder eine **Inversion**) ist ein geordnetes Paar $(i, j) \in \{1, \ldots, n\}^2$ mit $i < j$ und $\sigma(i) > \sigma(j)$. Wir bezeichnen die Menge aller Fehlstände von σ mit

$$\text{inv}(\sigma) = \{(i, j) \mid 1 \leq i < j \leq n \text{ und } \sigma(i) > \sigma(j)\}.$$

[11] Das heißt, dass diese Parität wirklich invariant für jede Permutation ist.

Übung. Zeigen[12] Sie, dass für $\sigma \in S_n$ gilt $\operatorname{sgn}(\sigma) = (-1)^{|\operatorname{inv}(\sigma)|}$.

Bemerkung 5.34. Für die Identität $\mathrm{id}_n \in S_n$ gilt $\operatorname{sgn}(\mathrm{id}_n) = 1$.

Satz 5.35. *Die Abbildung* $\operatorname{sgn} : S_n \longrightarrow \{-1, 1\}$ *ist ein Gruppenhomomorphismus, wobei die Gruppenoperation auf* $\{-1, 1\}$ *die Multiplikation ist.*

Beweis-Skizze: Wir müssen also zeigen, dass für alle $\sigma, \pi \in S_n$ gilt $\operatorname{sgn}(\sigma \cdot \pi) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\pi)$. Der Trick ist der folgende:

$$\begin{aligned} \operatorname{sgn}(\sigma \cdot \pi) &= \prod_{i<j} \frac{\sigma\big(\pi(j)\big) - \sigma\big(\pi(i)\big)}{j - i} \\ &= \prod_{i<j} \frac{\sigma\big(\pi(j)\big) - \sigma\big(\pi(i)\big)}{\pi(j) - \pi(i)} \cdot \prod_{i<j} \frac{\pi(j) - \pi(i)}{j - i} \end{aligned}$$

Das zweite Produkt ist per Definition $\operatorname{sgn}(\pi)$. Wir müssen nur noch bemerken, dass das erste Produkt $\operatorname{sgn}(\sigma)$ ist. Dafür behaupten wir, dass jeder Bruch ein Bruch aus der Definition von $\operatorname{sgn}(\sigma)$ ist. Wenn wir $k := \pi(j)$ und $\ell := \pi(i)$ definieren, dann ist das einzige das stören könnte, dass $k < \ell$ vorkommen könnte. Aber das kann gleich wieder gut gemacht werden, weil

$$\frac{\sigma(k) - \sigma(\ell)}{k - \ell} = \frac{\sigma(\ell) - \sigma(k)}{\ell - k}.$$

Q.E.D.

Korollar 5.36. Wenn $\sigma \in S_n$, dann gilt $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$.

Bemerkung 5.37. Für eine Transposition $\tau = (i, j) \in S_n$ gilt $\operatorname{sgn}(\tau) = -1$.

Beweis-Skizze: Wir verwenden die obige Beschreibung des Signums als $(-1)^{|\operatorname{inv}(\sigma)|}$. Das heißt, das $\operatorname{sgn}(1\ 2) = -1$, weil es eine einzige Inversion hat.

Das kann man auch direkt beweisen. Bezeichne $\tau = (1\ 2)$. Es gilt dann

$$\begin{aligned} \operatorname{sgn}(\tau) &= \textstyle\prod_{1 \leqslant i < j \leqslant n} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \left(\textstyle\prod_{\substack{i=1 \\ j=2}} \frac{\tau(j) - \tau(i)}{j - i}\right) \cdot \left(\textstyle\prod_{\substack{i=1 \\ 3 \leqslant j \leqslant n}} \frac{\tau(j) - \tau(i)}{j - i}\right) \cdot \left(\textstyle\prod_{\substack{i=2 \\ 3 \leqslant j \leqslant n}} \frac{\tau(j) - \tau(i)}{j - i}\right) \cdot \left(\textstyle\prod_{3 \leqslant i < j \leqslant n} \frac{\tau(j) - \tau(i)}{j - i}\right) \\ &= \left(\tfrac{1-2}{2-1}\right) \cdot \left(\textstyle\prod_{3 \leqslant j \leqslant n} \frac{j-2}{j-1}\right) \cdot \left(\textstyle\prod_{3 \leqslant j \leqslant n} \frac{j-1}{j-2}\right) \cdot \left(\textstyle\prod_{3 \leqslant i < j \leqslant n} \frac{\cancel{j-i}}{\cancel{j-i}}\right) \\ &= (-1) \cdot \left(\textstyle\prod_{3 \leqslant j \leqslant n} \frac{\cancel{j-2}}{\cancel{j-1}} \cdot \frac{\cancel{j-1}}{\cancel{j-2}}\right) \cdot \left(\textstyle\prod_{3 \leqslant i,j \leqslant n} 1\right) \end{aligned}$$

Eine Beliebige Transposition $(i\ j)$ ist gleich[a] mit

$$(i\ j) = (1\ i) \cdot (2\ j) \cdot\ (1\ 2) \cdot (2\ j) \cdot (1\ i).$$

[12] Sie finden einen Eleganten Beweis dafür in [**?**, S.288]

Aus Satz 5.35 und Korollar 5.36 folgt, weil $(k\ \ell)^{-1} = (k\ \ell)$

$$\begin{aligned}\operatorname{sgn}(i\ j) &= \operatorname{sgn}(1\ i)\cdot\operatorname{sgn}(2\ j)\cdot\ \operatorname{sgn}(1\ 2)\cdot\operatorname{sgn}(2\ j)^{-1}\cdot\operatorname{sgn}(1\ i)^{-1}\\ &= \operatorname{sgn}(1\ 2)\cdot\operatorname{sgn}(1\ i)\cdot\operatorname{sgn}(2\ j)\cdot\operatorname{sgn}(2\ j)^{-1}\cdot\operatorname{sgn}(1\ i)^{-1}\\ &= -1.\end{aligned}$$

Q.E.D.

[a] wenn $i = 1$ oder $j = 2$, dann verwenden wir die Konvention, dass $(a\ a) = \mathrm{id}$.

Wir kommen endlich zur Invarianz der Parität der Anzahl von Transpositionen in der Zerlegung einer Permutation.

Korollar 5.38. (a) Wenn $\sigma \in S_n$ das Produkt der Transpositionen $\tau_1, \ldots, \tau_r \in S_n$ ist, dann gilt $\operatorname{sgn}(\sigma) = (-1)^r$.

(b) Wenn für $\sigma \in S_n$ gilt $\sigma = \tau_1 \cdot \cdots \cdot \tau_r = \tau'_1 \cdot \cdots \cdot \tau'_s$, mit τ_i und τ'_j Transpositionen für alle $i = 1, \ldots, r$ und alle $j = 1, \ldots, s$, dann gilt

$$r \equiv s \bmod 2.$$

(c) Die Menge $A_n = \{\, \sigma \in S_n \mid \operatorname{sgn}(\sigma) = 1 \,\} = \ker \operatorname{sgn}$ ist eine Untergruppe von S_n.

Die Untergruppe A_n heißt die **alternierende Untergruppe** von S_n.

Bemerkung 5.39. Für jede Transposition $\tau = (i, j) \in S_n$ haben wir die disjunkte Vereinigung

$$S_n = A_n \sqcup \tau A_n.$$

Weil $\operatorname{sgn}\tau = -1$, gilt auch $\langle\tau\rangle \cap A_n = \{\, \mathrm{id} \,\}$. Wenn $\langle\tau\rangle = \{\, \mathrm{id}, \tau \,\}$ die Untergruppe die von τ erzeugt wird bezeichnet, dann gilt

$$S_n = A_n \cdot \langle\tau\rangle = \{\, \alpha \cdot \beta \ : \ \alpha \in A_n, \quad \beta \in \langle\tau\rangle \,\}.$$

Um das zu sehen, müssen wir wenn $\sigma \in A_n$, dann kann man $\alpha = \sigma$ und $\beta = \mathrm{id}$ wählen. Wenn $\sigma \notin A_n$, dann gilt $\sigma\tau \in \mathbb{A}_n$ und wir können dann $\alpha = \sigma\tau$ und $\beta = \tau$ wählen. Anders gesagt, ist S_n das semidirekte Produkt[13] der Untergruppen A_n und $\operatorname{Span}_{\mathbb{K}}\{\tau\}$. Das wird als $S_n = A_n \rtimes \operatorname{Span}_{\mathbb{K}}\{\tau\}$ geschrieben.

Wir haben die **Alternierende Untergruppe** $A_n = \{\, \sigma \in S_n \ : \ \operatorname{sign}(\sigma) = 1 \,\}$ hat Index $[S_n : A_n] = 2$. Sei $\{\, \pm 1 \,\}$ die Gruppe mit zwei Elementen unter multiplikativen Bezeichnung. Die Abbildung $\operatorname{sign} : S_n \longrightarrow \{\, \pm 1 \,\}$ ist ein Gruppenhomomorphismus[14]. Die Alternierende Gruppe ist dann der Kern des Homomorphismus sign.

Der Satz von Cayley

Satz 5.40 (von Cayley[15])**.** *Für jede endliche Gruppe G existiert ein $n \in \mathbb{N}$, sodass G isomorph zu einer Untergruppe von S_n ist.*

[13] Der Begriff von semiderektes Produkt wurde nicht eingeführt. Machen Sie sich keine weitere Gedanken darüber.
[14] Das braucht einen kleinen Beweis
[15] Englischer Mathematiker (1821-1895)

Beweis-Skizze: Jedes Element g einer Gruppe G definiert eine bijektive Abbildung definiert: $m_g : G \longrightarrow G$ durch

$$x \mapsto m_g(x) := g \cdot x.$$

Diese Abbildung ist bijektiv, weil das Inverse Element von g die Inverse Abbildung definiert: $m_{g^{-1}} = (m_g)^{-1}$. Wir haben also eine Abbildung $\Phi : G \longrightarrow S_{\#G}$ gegen durch

$$g \mapsto m_g.$$

Aus der Assoziativität der Gruppenoperation von G haben wir für alle $g, h \in \mathbb{G}$:

$$m_{g \cdot h}(x) = (g \cdot h) \cdot x = g \cdot (h \cdot x) = m_g(m_h(x)) = (m_g \circ m_h)(x) \quad \forall\, x \in G.$$

Also Φ ist ein Gruppenhomomorphismus. Weiterhin, es gilt

$$m_g(x) = \mathrm{id}(x) \quad \forall\, x \in G \Rightarrow m_g(e) = g \cdot e = e \Rightarrow g = e.$$

Also $\operatorname{Ker} \Phi = \{\, e \,\}$ und somit ist Φ injektiv. Also $G \simeq \operatorname{Bild} \Phi \leq S_{\#G}$. Q.E.D.

Beispiel 5.41.

Wenn $G = \mathbb{Z}/3\mathbb{Z}$ dann haben wir $\Phi : G \longrightarrow S_3$ definiert durch durch

$$1 \;\mapsto\; \{\, 1,2,3 \,\} \xrightarrow{+0} \{\, 1,2,3 \,\} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{id},$$

$$2 \;\mapsto\; \{\, 1,2,3 \,\} \xrightarrow{+1} \{\, 1,2,3 \,\} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\ 2\ 3),$$

$$3 \;\mapsto\; \{\, 1,2,3 \,\} \xrightarrow{+2} \{\, 1,2,3 \,\} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\ 3\ 2).$$

Also die Untergruppe von S_3 ist $\left\{\, \mathrm{id}, \gamma, \gamma^2 \,\right\}$, wobei γ der 3-Zyklus (1 2 3) ist.

5.1.8 Erzeuger von Gruppen

Wir beweisen erstmals ein Lemma, das uns garantiert, dass "die von einer Teilmenge erzeugte Untergruppe", tatsächlich eine Untergruppe sein wird.

Lemma 5.42. *Sei $(G, \cdot)$ eine Gruppe. Wenn $(H_i)_{i \in I}$ eine Familie von Untergruppen*[16] *ist, dann gilt*

$$\bigcap_{i \in I} H_i \leq G.$$

[16] Das heißt, dass $H_i \leq G$ für alle $i \in I$.

Beweis-Skizze: Wir werden Satz 5.15 zwei Mal anwenden.

Seien $a, b \in \bigcap_{i\in I} H_i$ beliebig. Das heißt,

$$a, b \in H_i \quad \forall\, i \in I.$$

Weil $H_i \leq G$ für alle $i \in I$, folgt aus Satz 5.15, dass $ab^{-1} \in H_i$ für alle $i \in I$. Also, aus der Definition des Durchschnittes einer Familie (siehe Definition 1.39) haben wir

$$ab^{-1} \in \bigcap_{i\in I} H_i.$$

Q.E.D.

Die folgende Definition ist nicht spezifisch für die Gruppentheorie. In vielen anderen algebraischen oder geometrischen Strukturen[17], kann man über die von einer Menge erzeugte Unterstruktur sprechen. In der linearen Algebra lernt man schon am Anfang des Studiums über den Untervektorraum, der von einer Menge von Vektoren erzeugt ist. Die Idee wird auch dort dieselbe sein: Wenn S eine beliebige Teilmenge ist, dann ist die davon erzeugte Unterstruktur, die **kleinste** Unterstruktur die diese Menge enthält. Für Gruppen wird also "die von S erzeugte Untergruppe" die kleinste Untergruppe die S enthält sein. "Kleinste" bezieht sich hier auf der Mengeninklusion. Das heißt, es wird die Untergruppe H_0 sein, mit $S \subseteq H_0$ und wenn $S \subseteq H$ für eine Untergruppe H gilt, dann gilt auch $H_0 \subseteq H$. Das kann man genauer in der folgenden Form ausdrücken.

Definition 5.43. Sei $(G, \cdot)$ eine Gruppe und sei $S \subseteq G$ eine beliebige Teilmenge der unterliegenden Menge G. Die **von S erzeugte Untergruppe** von G ist die Untergruppe

$$\langle S\rangle = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H.$$

Es gilt insbesondere, dass $\langle\emptyset\rangle = \bigcap_{H\leq G} = \{\, e \,\}$, die Gruppe mit einem Element.

Die Definition von $\langle S\rangle$ sagt nichts über die Form der Elemente der Untergruppe. Wir werden aber gleich beweisen, dass die von S erzeugte Untergruppe genau die Elementen, die durch endlich viele Verknüpfungen von Elementen aus S und deren Inversen erhalten werden können, enthält.

Satz 5.44. *Sei $(G, \cdot)$ und $S \subseteq G$ eine Teilmenge. Man bezeichne mit $S^{-1} = \left\{\, s^{-1} \;:\; s \in S \,\right\}$. Es gilt*

$$\langle S\rangle = \left\{\, \textstyle\prod_{i=1}^{r} s_i \;:\; r \in \mathbb{N} \text{ und } s_i \in S \cup S^{-1} \;\; \forall\, i \,\right\}.$$

Wir erinnern hier, dass wenn $r = 0$, dann ist $\prod_{i=1}^{0} s_i$ das leere Produkt, also gleich mit dem neutralen Element von G.

Beweis-Skizze: Wir bezeichnen mit $\mathcal{P} = \left\{\, \prod_{i=1}^{r} s_i \;:\; r \in \mathbb{N} \text{ und } s_i \in S \cup S^{-1} \;\; \forall\, i \,\right\}$. Wir wollen also zeigen, dass

$$\mathcal{P} = \bigcap_{\substack{H\leq G\\ S\subseteq H}} H.$$

[17] Zum Beispiel in Ringen,in Moduln, in Algebren, in Vektorräumen, in affinen Räumen, in projektive Räumen

Wenn wir $r = 1$ und $s_1 = s \in S$ setzen, dann bekommen wir $s \in \mathcal{P}$ für alle $s \in S$. Also $S \subseteq \mathcal{P}$. Wenn wir beweisen, dass $\mathcal{P} \leq G$, dann folgt $\langle S \rangle \subseteq \mathcal{P}$. Wenn wir auch beweisen, dass $\mathcal{P} \subseteq H$ für alle $H \leq G$ mit $S \subseteq H$, dann bekommen wir auch $\mathcal{P} \subseteq \bigcap_{\substack{H \leq G \\ S \subseteq H}} H = \langle S \rangle$. Es reicht also folgende Aussagen zu beweisen:

1. $\mathcal{P} \leq G$.
2. $\mathcal{P} \subseteq H$ für alle $H \leq G$ mit $S \subseteq H$.

1. Wir verwenden wieder den Satz 5.15. Es seien $a, b \in \mathcal{P}$. Das heißt es existieren $r, \ell \in \mathbb{N}$ und $s_1, \ldots, s_r, t_1, \ldots, t_\ell \in S \cup S^{-1}$ mit

$$a = s_1 \cdots s_r \quad \text{und} \quad b = t_1 \cdots t_\ell.$$

   Es gilt dann, $b^{-1} = t_\ell^{-1} \cdots t_1^{-1}$ und, weil $t_i \in S \cup S^{-1}$, auch $t_i^{-1} \in S \cup S^{-1}$. Also

$$ab^{-1} = s_1 \cdots s_r \cdot t_\ell^{-1} \cdots t_1^{-1} \in \mathcal{P}.$$

2. Sei $g = s_1 \cdots s_r \in \mathcal{P}$ beliebig und sei $H \leq G$ mit $S \subseteq H$. Weil $S \subseteq H \leq G$, gilt aus **UG 3.** $s^{-1} \in H$ für alle $s \in S$. Also $s_1, \ldots, s_r \in H$, und aus **UG 1.** folgt $g \in H$.

Q.E.D.

Die Elemente einer Menge S mit $\langle S \rangle = G$ heißen **Erzeuger** von G. Wir sagen auch, dass S ein **Erzeugendensystem** von G ist. Ein Erzeugendensystem S von G ist minimal, wenn alle echte Teilmengen von S keine Erzeugendensysteme von G sind. Also wenn

$$\langle S \rangle = G \quad \text{und} \quad \langle S' \rangle \neq G \ \ \forall\ S' \subsetneq S.$$

Wir sagen, dass die Gruppe G **endlich erzeugt** ist, wenn es eine endliche Menge $S \subseteq G$ gibt, die ein Erzeugendensystem von G ist. Eine Gruppe G heißt **zyklische Gruppe** wenn es von einem einzigen Element erzeugt werden kann.

Bemerkung 5.45. Jede Gruppe hat mindestens ein Erzeugendensystem: $\langle G \rangle = G$. Interessanter sind aber minimale Erzeugendensysteme. Es gibt meistens mehrere davon, und es kann auch passieren, dass minimale Erzeugendensysteme verschiedene Kardinalitäten haben. Zum Beispiel:

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle = \langle 2, 3 \rangle = \langle 11, 25 \rangle\,.$$

Alle vier sind minimale Erzeugendensysteme. In den ersten zwei Fällen ist das sehr einfach: jede ganze Zahl ist eine endliche Summe von 1 und -1. Es gilt allgemeiner, dass wenn wir schon $G = \langle S \rangle$ wissen, dann gilt

$$G = \langle T \rangle \iff S \subseteq \langle T \rangle\,.$$

Die direkte Implikation ist trivial, und die Umkehrung folgt aus Satz 5.44. In unserem Fall gilt also

$$\mathbb{Z} = \langle a, b \rangle \iff 1 \in \langle a, b \rangle = \{\, \lambda \cdot a + \mu \cdot b \ \ :\ \ \lambda, \mu \in \mathbb{Z} \,\}\,.$$

Also, aus Korollar 3.11 gilt $\mathbb{Z} = \langle a, b \rangle \Leftrightarrow \mathrm{ggT}(a, b) = 1$. Wie würde man das für $\mathbb{Z} = \langle a_1, \ldots, a_n \rangle$ verallgemeinern? Wann ist $\{\, a_1, \ldots, a_n \,\}$ ein minimales Erzeugendensystem von $\mathbb{Z}$?

Bemerkung 5.46. Für jedes Element $g \in G$ gilt $\operatorname{ord} g = \#\langle g \rangle$.

In Korollar 5.31 haben wir also bewiesen, dass

$$S_n = \langle (1\ 2), \ldots, (n-1\ n) \rangle = \langle (1\ 2), \ldots, (1\ n) \rangle .$$

Es ist eine gute Übung zu überprüfen, dass beide der obigen Erzeugendensysteme minimal sind. Dabei könnte folgende Bemerkung helfen.

Bemerkung 5.47. Ein Erzeugendensystem $S \subseteq G$ ist genau dann minimal, wenn

$$s \notin \langle S \setminus s \rangle \quad \forall\, s \in S.$$

Also wenn $S = \{ s_1, \ldots, s_n \}$, dann ist S genau ein minimales Erzeugendensystem, wenn[18]

$$G = \langle s_1, \ldots, s_n \rangle \quad \text{und} \quad G \neq \langle s_1, \ldots, \widehat{s_i}, \ldots, s_n \rangle \quad \forall\, i = 1, \ldots, n.$$

5.1.9 Normalteiler und die Faktorgruppe

Wir werden in diesem Teil die Kongruenz modulo einer ganzen Zahl verallgemeinern. Wir haben gesehen, dass jede Untergruppe von $\mathbb{Z}$ die Form $n\mathbb{Z}$ hat. Wir haben mit $\mathbb{Z}/n\mathbb{Z}$ die Menge der Restklassen modulo n bezeichnet, weil es ein Sonderfall folgender Relation ist.

Sei G eine Gruppe. Für jede Untergruppe $H \leq G$ definieren wir die **rechte Kongruenz Modulo** H als die Relation

$$a \sim_H b \iff ab^{-1} \in H.$$

Wenn $G = (\mathbb{Z}, +)$ und $H = n\mathbb{Z}$ dann ist "ab^{-1}" das Element $a - b$, und $a - b \in n\mathbb{Z}$ ist äquivalent zu $n \mid a - b$, also

$$a \sim_{n\mathbb{Z}} b \Leftrightarrow a \equiv b \bmod n.$$

Lemma 5.48. *Für alle $H \leq G$ ist die Relation $\sim_H$ ist eine Äquivalenzrelation. Die Äquivalenzklassen haben die Form $Hg := \{ hg \ : \ h \in H \}$, mit $g \in G$.*

Beweis-Skizze: Aus **UG 2.** folgt $gg^{-1} = e \in H$ für alle $g \in G$. Also $g \sim_H g$ für alle $g \in G$ und somit ist $\sim_H$ reflexiv.

Wenn $g_1 \sim_H g_2$, dann gilt per Definition $g_1 g_2^{-1} \in H$. Aus **UG 3.** folgt $(g_1 g_2^{-1})^{-1} = g_2 g_1^{-1} \in H$. Also $g_2 \sim_H g_1$ und somit ist $\sim_H$ symmetrisch.

Für die Transitivität, seien $g_1, g_2, g_3 \in G$ mit $g_1 \sim_H g_2$ und $g_2 \sim_H g_3$. Es gilt also

$$g_1 g_2^{-1} \in H \text{ und } g_2 g_3^{-1} \in H.$$

Wir haben dann $g_1 g_3^{-1} = (g_1 e) g_3^{-1} = (g_1 (g_2^{-1} g_2)) g_3^{-1} = (g_1 g_2^{-1})(g_2 g_3^{-1}) \in H$.

[18] Die Bezeichnung $\{ s_1, \ldots, \widehat{s_i}, \ldots, s_n \}$ bedeutet $S \setminus \{ s_i \}$.

Sei $[g]_H$ eine Äquivalenzklasse für $\sim_H$. Das heißt,

$$\begin{aligned}
[g]_H &= \{\, x \in G \;:\; x \sim_H g \,\} \\
&= \{\, x \in G \;:\; xg^{-1} \in H \,\} \\
&= \{\, x \in G \;:\; \exists h \in H \text{ mit } xg^{-1} = h \,\} \\
&= \{\, x \in G \;:\; \exists h \in H \text{ mit } x = hg \,\} \\
&= \{\, hg \;:\; h \in H \,\}.
\end{aligned}$$

Q.E.D.

Für jede Untergruppe $H \leq G$, eine **Rechtsnebenklasse** von H ist eine Teilmenge von G der Form

$$Hg = \{\, hg \;:\; h \in H \,\}.$$

Für eine Untergruppe $H \leq G$ kann man auch eine linke Kongruenz Modulo H definieren

$$a \;{}_H\!\sim b \Leftrightarrow a^{-1}b \in H.$$

Analog zu dem Beweis von Lemma 5.48, zeigt man, dass auch ${}_H\!\sim$ eine Äquivalenzrelation auf G ist. Die Äquivalenzklasse in diesem Fall heißen **Linksnebenklassen** und sind Mengen der Form

$$gH = \{\, gh \;:\; h \in H \,\}$$

wobei $g \in G$. Wenn die Gruppe G kommutativ, dann gilt $gH = Hg$ für alle $g \in G$ und $H \leq H$. Für nicht-kommutative Gruppen gilt diese Gleichheit nicht immer.

Beispiel 5.49. In der symmetrischen Gruppe S_3 seien $H_2 = \langle(1\ 2)\rangle$ und $H_3 = \langle(1\ 2\ 3)\rangle$. Für H_2 haben wir folgende Nebenklassen:

$$\begin{array}{llllll}
H_2\,\mathrm{id} &= \{\,\mathrm{id}, (1\ 2)\,\} & H_2(1\ 3) &= \{\,(1\ 3), (1\ 3\ 2)\,\} & H_2(2\ 3) &= \{\,(2\ 3), (1\ 2\ 3)\,\} \\
\mathrm{id}\,H_2 &= \{\,\mathrm{id}, (1\ 2)\,\} & (1\ 3)H_2 &= \{\,(1\ 3), (1\ 2\ 3)\,\} & (2\ 3)H_2 &= \{\,(2\ 3), (1\ 3\ 2)\,\}
\end{array}$$

Es gilt also $H_2(1\ 3) \neq (1\ 3)H_2$ und $H_2(2\ 3) \neq (2\ 3)H_2$. Für H_3 haben wir nur zwei Nebenklassen: H_3 und $G \setminus H_3$.

$$\begin{aligned}
\mathrm{id}\,H_3 &= (1\ 2\ 3)H_3 = (1\ 3\ 2)H_3 = \{\,\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\,\}, \\
H_3\,\mathrm{id} &= H_3(1\ 2\ 3) = H_3(1\ 3\ 2) = \{\,\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\,\},
\end{aligned}$$

$$\begin{aligned}
(1\ 2)H_3 &= (1\ 3)H_3 = (2\ 3)H_3 = \{\,(1\ 2), (1\ 3), (2\ 3)\,\}, \\
H_3(1\ 2) &= H_3(1\ 3) = H_3(2\ 3) = \{\,(1\ 2), (1\ 3), (2\ 3)\,\}.
\end{aligned}$$

Genau wie wir Restklassen modulo n addieren können, wollen wir auch modulo einer Untergruppe rechnen. Das heißt, wir würden gerne eine innere Verknüpfung auf der Menge der rechts Nebenklassen, mit Hilfe der algebraischen Operation auf G, definieren. Das heißt, wir wollen, dass

$$(Hg) \cdot (Hg') := H(gg')$$

eine Wohldefinierte innere Verknüpfung ist. Das heißt, dass es unabhängig von der Wahl der Repräsentanten der Äquivalenzklassen ist. Wir werden jetzt sehen, dass das genau dann möglich ist, wenn die $\sim_H$ und ${}_H\!\sim$ dieselbe Äquivalenzrelation ist.

Lemma 5.50. *Für eine Untergruppe $H \leq G$ sind folgende Aussagen äquivalent.*

(i) $gH = Hg$ *für alle* $g \in G$.

(ii) *Für alle* $a, b, c, d \in G$ *gilt: wenn* $a \sim_H b$ *und* $c \sim_H d$, *dann gilt* $ac \sim_H bd$.

Beweis-Skizze: (i)⇒ (ii) Wir haben $ab^{-1}, cd^{-1} \in H$ und wollen zeigen, dass $ac(bd)^{-1} \in H$.

Aus $ab^{-1}, cd^{-1} \in H$ folgt die Existenz von $h_1, h_2 \in H$, sodass

$$a = h_1 b \quad \text{und} \quad c = h_2 d.$$

Wir suchen ein $h \in H$, sodass $ac = hbd$. Weil $bh_2 \in bH$ und aus (i) gilt $bH = Hb$, folgt, dass ein $h_3 \in H$ existiert, sodass $bh_2 = h_3 b$. Es gilt also

$$ac = (h_1 b)(h_2 d) = h_1(bh_2)d = h_1 h_3(bd).$$

Weil $H \leq G$, gilt auch $h_1 h_3 \in H$, also $(ac)(bd)^{-1} \in H$. Also $ac \sim_H bd$.

(ii)⇒(i) Sei $g \in G$ beliebig. Wir zeigen $gH = Hg$ indem wir beide Inklusionen zeigen.

"$\subseteq$" Sei $x \in gH$ beliebig. Es gibt also ein $h \in H$ mit $x = gh$. Wir haben $g \sim_H g$ und $h \sim_H e$, also aus (ii) folgt $gh \sim_h g$. Das heißt, es existiert ein $h' \in H$, sodass

$$(gh)g^{-1} = h'$$

Also $x = gh = h'g \in Hg$.

"$\supseteq$" Sei $y \in Hg$ beliebig. Also $y = hg$ für ein bestimmtes $h \in H$. Weil $g^{-1} \sim_H g^{-1}$ und $h \sim_H e$, folgt aus (ii), dass $g^{-1}h \sim_H g^{-1}$. Das heißt, es existiert ein $h' \in H$, sodass $(g^{-1}h)(g^{-1})^{-1} = h'$. Wenn wir beide Seiten links mit g multiplizieren, bekommen wir

$$hg = gh' \in gH.$$

Also $y \in gH$, und auch die zweite Inklusion gilt. Q.E.D.

Das Lemma sagt uns also, dass die Gruppenoperation eine Operation auf der Faktormenge $G/\sim_H$ genau dann induziert, wenn $gH = Hg$ für alle $g \in G$. Wir führen deswegen folgenden Begriff ein.

Definition 5.51. Eine Untergruppe $H \leq G$ heißt **normale Untergruppe** (oder **Normalteiler**) von G genau dann, wenn $gH = Hg$ für alle $g \in G$. Wir schreiben dafür $H \triangleleft G$.

Vorsicht! Die Gleichheit $gH = Hg$ bedeutet **nicht**, dass $gh = hg \ \ \forall\, g \in G, h \in H.$ In Beispiel 5.49 haben wir gesehen, dass $H = \langle(1\ 2\ 3)\rangle$ ein Normalteiler ist. Es gilt also $(1\ 2)H = H(1\ 2)$, aber

$$(1\ 2)(1\ 2\ 3) = (2\ 3) \neq (1\ 3) = (1\ 2\ 3)(1\ 2).$$

Bemerkung 5.52. Für eine Untergruppe $H \leq G$ gilt

$$H \triangleleft G \iff gHg^{-1} = H, \ \forall\, g \in G.$$

Die Bedingung auf der rechten Seite heißt auch, dass H invariant unter **Konjugation** mit g für jedes $g \in G$ ist.

Satz 5.53. *Sei G eine Gruppe, $H \triangleleft G$ ein Normalteiler und bezeichne $G/H = \{ gH \ : \ g \in G \}$ die Menge der Äquivalenzklassen von $\sim_H$. Die Menge G/H zusammen mit der inneren Verknüpfung*

$$\begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (Ha, Hb) & \longmapsto & Hab \end{array}$$

ist eine Gruppe.

Beweis-Skizze: Aus Lemma 5.50 ist die Abbildung wohl definiert, also tatsächlich eine innere Verknüpfung. Die Assoziativität folgt direkt aus der Assoziativität der Verknüpfung auf G. Direkt aus der Definition der Verknüpfung folgt auch, dass das neutrale Element $H = He$ ist und, dass das Inverse von Hg, die Nebenklasse Hg^{-1} ist. Q.E.D.

Wenn $H \triangleleft G$, dann heißt die Gruppe G/H aus Satz 5.53 die **Faktorgruppe** von G modulo H.

Endliche Gruppen

Beispiele:

1. $|\mathbb{Z}/6\mathbb{Z}| = 6$, $|2\mathbb{Z}/6\mathbb{Z}| = 3$, $[\mathbb{Z}/6\mathbb{Z} : 2\mathbb{Z}/6\mathbb{Z}] = 2$.
2.

Satz 5.54 (Lagrange)**.** *Sei G eine endliche Gruppe und $H \leq G$. Wir haben*

$$|G| = |H|[G : H].$$

Insbesondere $|H|$ teilt $|G|$ für jede Untergruppe von G.

Beweis-Skizze: Die Rechtsnebenklassen sind Äquivalenzklassen, also ist G eine disjunkte Vereinigung der Ha. Insbesondere $|G| = \sum_{a \in R} |Ha|$, wobei R ist eine Repräsentantensystem für $\sim_H$. Es reicht zu zeigen, dass $|H| = |Ha|$, $\forall\ a \in G$. Das heißt (cf. Definition 1.43), dass es eine Bijektion zwischen den beiden Mengen gibt. Wir haben für jedes $a \in G$ die bijektive Abbildung $\cdot a : H \longrightarrow Ha$. Die Umkehrabbildung ist $\cdot a^{-1}$. Q.E.D.

UNDER CONSTRUCTION:

Wichtiges Beispiel: Die Gruppe $\mathcal{Q}$ der Quaternionen. Diese ist eine nicht-kommutative Gruppe mit 8 Elementen:

$$\mathcal{Q} = \{ \pm 1, \pm i, \pm j, \pm k \}.$$

Die Verknüpfung ist multiplikativ bezeichnet, sodass die Vorzeichen genau wie bei der Multiplikation der reellen Zahlen Funktioniert. Insbesondere, ist 1 das neutrale Element von $\mathcal{Q}$, es gilt $(-1)^2 = 1$, und das Element (-1) kommutiert mit allen Elementen der Gruppe. Weiterhin gilt noch

$$i^2 = j^2 = k^2 = -1 \quad \text{und} \quad ijk = -1.$$

Aus diesen Relationen kann man dann beweisen, dass $ij = -ji$, $ik = -ki$ und $jk = -kj$. Welches der acht Elemente von $\mathcal{Q}$ wird gleich mit ij sein?

5.1.10 Kleine Matrizen

Wir betrachten hier zur Einfachheit nur Matrizen mit Einträgen aus $\mathbb{R}$. Alles was wir aber hier über Matrizen formulieren werden funktioniert genau so gut wenn man an der Stelle von $\mathbb{R}$ einen anderen Körper[19] wählt: $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}/p\mathbb{Z}$ wobei p eine Primzahl ist.

Eine Matrix mit reellen Einträgen ist eine rechteckige Tabelle von reellen Zahlen. Diese Tabelle muss vollständig gefüllt werden, es dürfen also keine "leere Stellen" vorkommen. Wir werden uns erstmals (und meistens in diesem Kapitel) mit 2×2-Matrizen beschäftigen. Die Verallgemeinerung zu $m \times n$-Matrizen, mit $m, n \in \mathbb{N}_{>0}$ ist offensichtlich wenn man feststellt, dass m die Anzahl von Zeilen ist und n die Anzahl von Spalten. Eine 2×2 reelle Matrix ist also eine Tabelle der Form

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} \qquad \text{wobei } a_{i,j} \in \mathbb{R}$$

Wir haben das mit Indizes formuliert, damit die Verallgemeinerung noch offensichtlicher wird. Mit Indizes kann man eine Matrix auch kompakter darstellen:

$$\begin{pmatrix} a_{1,1} & a_{1,2} \\ a_{2,1} & a_{2,2} \end{pmatrix} = (a_{i,j}).$$

Zwei 2×2 Matrizen $(a_{i,j})$ und $(b_{i,j})$ sind gleich, genau dann wenn $a_{i,j} = b_{i,j}$ für alle $i, j \in \{1, 2\}$. Für 2×2 Matrizen werden wir oft die Einträge einfach mit Kleinbuchstaben bezeichnen. Wir bezeichnen die Menge der 2×2 reellen Matrizen mit

$$\mathrm{Mat}_{2\times 2}(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;:\; a, b, c, d \in \mathbb{R} \right\}.$$

Auf dieser Menge definieren wir zwei innere Verknüpfungen, die Matrix Addition $+$ und die Matrix Multiplikation $\cdot$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & f \\ g & h \end{pmatrix} := \begin{pmatrix} a+e & b+f \\ c+g & d+h \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} := \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Dass $(\mathrm{Mat}_{2\times 2}(\mathbb{R}), +)$ eine abelsche Gruppe, die isomorph zu $\mathbb{R}^4$ ist, ist, ist einfach zu überprüfen. Für die Matrix Multiplikation ist es etwas komplizierter. Man kann direkt überprüfen, dass die Matrixmultiplikation assoziativ ist. Es gibt auch ein neutrales Element: die **Einheitsmatrix** (oder die **Identitätsmatrix**). Wir bezeichnen diese mit

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

[19] Eine Körper ist eine Menge $\mathbb{K}$ mit zwei inneren Verknüpfungen: eine Addition $+ : \mathbb{K}\times\mathbb{K} \longrightarrow \mathbb{K}$ und eine Multiplikation $\cdot : \mathbb{K} \times \mathbb{K} \longrightarrow \mathbb{K}$, sodass $(\mathbb{K}, +)$ eine abelsche Gruppe mit neutralem Element 0 ist, $(\mathbb{K} \setminus \{ 0 \}, \cdot)$ ist eine Abelsche Gruppe, und die Multiplikation ist distributiv bezüglich der Addition; das heißt:

$$a \cdot (b + c) = a \cdot b + a \cdot c \qquad \forall\, a, b, c \in \mathbb{K}.$$

Es ist einfach durch direktes rechnen zu überprüfen, dass

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\cdot\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\quad\forall\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

Das Paar $(\mathrm{Mat}_{2\times 2}(\mathbb{R}),\cdot)$ ist aber nicht ein Gruppe, weil nicht alle Matrizen invertierbar sind. Zum Beispiel:

$$\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}a & b\\ c & d\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}\neq\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\qquad\forall\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{Mat}_{2\times 2}(\mathbb{R}).$$

Gruppenhomomorphismen

Beispiele:

1. Die identische Abbildung $\mathrm{id}_G : G \longrightarrow G$ ein Gruppenhomomorphismus.
2. Wenn $H \leqslant G$ eine Untergruppe (cf. Definition 5.9) ist, dann ist $i : H \hookrightarrow G$ mit $h \mapsto h$ ein Gruppenhomomorphismus.
3. $\pi_i : G_1 \times G_2 \longrightarrow G_i$ mit $(g_1, g_2) \mapsto g_i$.
4. $\mathbb{Z} \xrightarrow{\cdot m} \mathbb{Z}$ mit $n \mapsto n \cdot m$ aber nicht $\mathbb{Z} \xrightarrow{+m} \mathbb{Z}$ mit $n \mapsto n + m$ wenn $m \neq 0$.
5. $\varphi : \mathbb{Z} \longrightarrow \langle x\rangle$ $n \mapsto x^n$, wobei $x \in G$ und $\langle x\rangle$ die von x erzeugte Untergruppe (cf. Definition 5.9).

Untergruppen

Beispiele:

1. Für jede Gruppe G sind $\{ e \}$ und G Untergruppen. Eine **echte** Untergruppe ist eine Untergruppe $H \leq G$ mit $H \neq \{ e \}$ und $H \neq G$.
2. $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$. Aber $\mathbb{Z}^\times \not< \mathbb{Z}$.
3. Die Menge $\{ z \in \mathbb{Z} \ : \ z \text{ ist gerade} \}$ ist eine Untergruppe $\mathbb{Z}$, aber die Menge aller ungeraden ganzen Zahlen ist keine Untergruppe.
4. Vorsicht! $\mathbb{Z}/n\mathbb{Z}$ ist keine Untergruppe von $\mathbb{Z}$. Es ist nicht einmal eine Teilmenge! Und obwohl wir injektive Abbildungen von $\mathbb{Z}/n\mathbb{Z}$ nach $\mathbb{Z}$ definieren können, können diese nie Gruppen Homomorphismen sein, weil $\varphi(1) \in \mathbb{Z}$ die Eigenschaft $n \cdot \varphi(1) = 0$ haben muss (weil $n \cdot \varphi(1) = \varphi(n \cdot 1) = \varphi(0) = 0 \in \mathbb{Z}$), und solche Elemente gibt es in $\mathbb{Z}$ nicht.
5. $\{ z \in \mathbb{C} \ : \ |z| = 1 \} < \mathbb{C}^\times$.
6. $\{ e, \sigma_1 \} < S_3$, $\{ e, \sigma_4, \sigma_5 \} < S_3$, aber $\{ e, \sigma_1, \sigma_2, \sigma_3 \} \not< S_3$
7. Für $n \in \mathbb{Z}$ ist $n\mathbb{Z} \leq \mathbb{Z}$.
8. Für $n, m \in \mathbb{N}_{>0}$ mit $\mathrm{ggT}(n, n) \notin \{ n, m \}$ ist $n\mathbb{Z} \cup m\mathbb{Z} \not\leq \mathbb{Z}$.
9. Sei $x \in G$. Wir definieren $x^0 = e$ und bezeichnen für $n \in \mathbb{N}_{>0}$

$$x^n = \underbrace{x * \cdots * x}_{n-\text{Mal}} \qquad \text{und} \qquad x^{-n} = (x^{-1})^n.$$

   Die Menge $\langle x\rangle := \{ x^n \ : \ n \in \mathbb{Z} \}$ ist eine Untergruppe von G, und heißt die von x erzeugte **zyklische Untergruppe** von G. Es kann sein, dass mehrere Potenzen von x gleich sind, also, dass $\langle x\rangle$ eine endliche Untergruppe ist. Zum Beispiel: $\mathrm{Span}_{\mathbb{K}}\{\sigma_1\} = \{ e, \sigma_1 \} < S_3$.

Index