Vorkurs Mathematik

Christoph Bock und Yvonne Deuster

Vorlesung

an der

Universität zu Köln

Propädeutik zum WS 2007/2008

Version vom 7. Oktober 2007

Vorwort

Am Mathematischen Institut wird vor Beginn des Wintersemesters ein Vorkurs angeboten. Er richtet sich an Studienanfänger, die ein Studium in einem der folgenden Studiengänge aufnehmen wollen: Mathematik, Wirtschaftsmathematik, Wirtschaftsinformatik, Lehramt an Gymnasien, Gesamtschulen und Berufskollegs (mit Mathematik als Unterrichtsfach) sowie Physik, Geophysik und Meteorologie.

Mittels des Vorkurses soll der Einstieg in das Studium erleichtert werden. Sein Stil ist an den Charakter der Mathematikvorlesungen angelehnt. Während an der Schule mathematische Begriffe und Methoden vielfach lediglich an Beispielen erfahren werden, werden in Universitätsvorlesungen zunächst mathematische Theorien (wie z.B. Analysis, Algebra und Stochastik) auf der Basis klar formulierter Definitionen entwickelt. Im Vorkurs soll man ein erstes Verständnis für diese Zielsetzung, für den Charakter exakter Definitionen und für die Herleitung mathematischer Resultate gewinnen.

In dieser Vorlesung wird die Existenz der aus der Schule bekannten Zahlenbereiche $\mathbb{N}_+, \mathbb{N}, \mathbb{Z}, \mathbb{Q}$ und $\mathbb{R}$ bzw. $\mathbb{R}_+$ mit $\mathbb{N}_+ \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ bzw. $\mathbb{R}_+ \subset \mathbb{R}$ sowie die Kenntnis der Rechenoperationen der Addition, Subtraktion, Multiplikation und Division (zunächst) vorausgesetzt. $\mathbb{N}$ – und damit auch $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$ –, der Ring $\mathbb{Z}$ der ganzen Zahlen und die Körper $\mathbb{Q}$ der rationalen Zahlen sowie $\mathbb{C}$ der komplexen Zahlen werden im Verlaufe der Vorlesung eingeführt.

Die Literatur, die wir bei bei der Ausarbeitung der Vorlesung verwendet haben, findet sich unten. [6] eignet sich für den Schulabgänger am besten, um sich mit der Art und Weise, wie an der Universität Mathematik betrieben wird, vertraut zu machen. [4] enthält Material, das jeder mathematisch gebildete Mensch kennen sollte; und das trifft auch auf [2] zu. Letzteres ist allerdings erheblich umfangreicher. [1] macht den Leser mit der mathematischen Sprache und Notation vertraut.

Fragen, Verbesserungsvorschläge oder Anmerkungen können Sie gerne an `bock(at)mi.uni-koeln.de` senden.

Köln, im Herbst 2007 Christoph Bock und Yvonne Deuster

Inhaltsverzeichnis

1 Aussagen und Regeln des logischen Schließens

Mathematik ist die Betrachtung abstrakter Strukturen, die durch Definitionen (oder Axiome) gegeben sind, und die Herleitung von Eigenschaften, die man über diese Strukturen aussagen kann. Diese Herleitung soll so geschehen, daß alle Menschen zu denselben Ergebnissen kommen (können) und nicht etwa zu sich widersprechenden. Daher beschäftigt man sich mit *logischem Schließen*. Außerdem muß man sich darüber klar sein, wie man die obigen Eigenschaften formuliert. Dies führt zur Betrachtung von *Aussagen*.

Definition 1.1 (Aussagen, Axiome)**.** Eine *Aussage* ist ein sprachlich und grammatisch richtiger Ausdruck, dem eindeutig ein Wahrheitswert – entweder wahr (w) oder falsch (f) – zugeordnet ist.

Ein *Axiom* ist eine Aussage, die wir ohne Begründung als wahr betrachten.

Beispiel. Wir setzen im folgenden (zunächst) die Kenntnis der Objekte $\mathbb{N}_+$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ voraus.

1.) 13 ist eine Primzahl. Aussage, w

2.) 13 ist eine Glückszahl. keine Aussage

3.) $\sqrt{2}$ ist rational. Aussage, f

4.) In unserem Milchstraßensystem gibt es weiteres Leben. Aussage, w oder f

5.) Es macht Spaß, eine Vorlesung vor 400 Hörern zu halten. keine Aussage

6.) Der FC wird im Jahre 2010 deutscher Meister sein.[1] Aussage, w oder f

Definition 1.2 (Logische Verknüpfung von Aussagen zu neuen Aussagen)**.** Es seien A und B Aussagen. Wir definieren dann neue Aussagen *non* A (i.Z. $\boxed{\neg A}$), A *und* B (i.Z. $\boxed{A \wedge B}$), A *oder* B (i.Z. $\boxed{A \vee B}$), *entweder* A *oder* B (i.Z. $\boxed{A \veebar B}$), *aus* A *folgt* B (i.Z. $\boxed{A \Rightarrow B}$) und A *ist äquivalent zu* B (i.Z. $\boxed{A \Leftrightarrow B}$) durch die folgenden *Wahrheitswertetafeln*:

(i)

A	$\neg A$
w	f
f	w

(ii)

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

Bemerkung.

1.) Im Unterschied zur Umgangssprache ist für uns also *aus* A *folgt* B insbesondere immer dann wahr, wenn A falsch ist, (egal ob B wahr oder falsch ist).

[1] Der erstgenannte Autor möchte gerne erwähnen, daß bei der Nennung dieses Beispieles in seiner Vorlesung ein Hörer aufgestanden ist und gesagt hat: „Das ist eine Aussage, und die ist wahr.“ Jener hofft, daß es sich hierbei tatsächlich um eine wahre Aussage handelt.

Beispiel.

a) *Wenn morgen die Sonne scheint, gehen wir schwimmen.*
Sollte es morgen regnen, so habe ich mein Versprechen gehalten, gleichgültig, ob wir schwimmen gehen oder nicht.

b)
$$5 - 2 = 1 \Longrightarrow 4 \text{ ist eine Primzahl}$$
und
$$5 - 2 = 1 \Longrightarrow 5 \text{ ist eine Primzahl}$$
sind gemäß unserer Definition wahre Aussagen, obwohl sie umgangssprachlich wohl eher als unsinnig bezeichnet würden.

2.) Die Schreibweisen

Satz. *Vor.: A* *Beh.: B*	oder	**Satz.** *Gelte A. Dann folgt B.*

sind per definitionem gleichbedeutend mit $A \Rightarrow B$.

Insbesondere ist jeder Satz wahr, dessen Voraussetzung falsch ist.

Als *Beweis* eines solchen Satzes bezeichnen wir den unter Benutzung von wahren Aussagen erfolgenden Wahrheitsnachweis für die Aussage $A \Rightarrow B$, d.h. die Verifizierung einer „wenn, dann"-Aussage und a priori nicht etwa die Verifizierung der in der Behauptung genannten Aussage B.

Da $A \Rightarrow B$ bei falscher Voraussetzung A stets wahr ist, reduziert sich die Verifizierung von $A \Rightarrow B$ auf den Nachweis von: Falls gilt „A ist wahr", so folgt auch „B wahr."

Definition 1.3 (Aussageformen, Tautotologien, Regeln des logischen Schließens)**.**

(i) Sei $k \in \mathbb{N}_+$. Eine *(k-stellige) Aussageform* ist ein Ausdruck α mit k Leerstellen derart, daß für beliebeige Aussagen $A_1, \dots A_k$ gilt
$$\alpha(A_1, \dots, A_k) \text{ ist eine Aussage.}$$

(ii) Sei $k \in \mathbb{N}_+$. Eine (k-stellige) Aussageform α heißt *Tautologie* oder *tautologisch* genau dann, wenn $\alpha(A_1, \dots, A_k)$ für alle Aussagen $A_1, \dots A_k$ eine wahre Aussage ist.

(iii) Eine *Regel des logischen Schließens* ist eine Aussageform
$$\alpha \Longrightarrow \beta \quad \text{oder} \quad \alpha \Longleftrightarrow \beta,$$
wobei α, β Aussageformen sind.

Beispiel.

1.) Indem man für alle Aussagen A, B

$$\alpha(A) :\Longleftrightarrow \neg A,$$
$$\beta(A,B) :\Longleftrightarrow A \wedge B$$

setzt, wird eine einstellige Aussageform α und eine zweistellige Aussageform β definiert.

2.) Indem man für alle Aussagen A

$$\gamma(A) :\Longleftrightarrow A \vee (\neg A)$$

setzt, wird eine Tautologie γ definiert.

Satz 1.4. *Sind A, B, C beliebige Aussagen, so sind die folgenden Aussagen sämtlich wahr:*

$$\begin{aligned}
\neg(\neg A) &\iff A, && (1)\\
\neg(A \wedge B) &\iff ((\neg A) \vee (\neg B)), && (2)\\
\neg(A \vee B) &\iff ((\neg A) \wedge (\neg B)), && (3)\\
(A \wedge (B \vee C)) &\iff ((A \wedge B) \vee (A \wedge C)), && (4)\\
(A \vee (B \wedge C)) &\iff ((A \vee B) \wedge (A \vee C)), && (5)\\
(A \Rightarrow B) &\iff ((\neg B) \Rightarrow (\neg A)), && (6)\\
(A \Rightarrow B) &\iff ((\neg A) \vee B), && (7)\\
(\neg(A \Rightarrow B)) &\iff (A \wedge (\neg B)), && (8)\\
(A \Rightarrow B) &\iff ((A \Rightarrow B) \wedge (B \Rightarrow A)), && (9)\\
(A \wedge (A \Rightarrow B)) &\Longrightarrow B. && (10)
\end{aligned}$$

Beweis als Übung. □

Bemerkung.

1.) Eine Aussage der Form $A \Leftrightarrow B$ können wir also nach (8) stets durch die Aussage $(A \Rightarrow B) \wedge (B \Rightarrow A)$ ersetzen. Dies liefert eine Strategie zum Beweis von Äquivalenzen.

2.) Aus (6) ergibt sich ein wichtiges Beweisprinzip, nämlich das *Prinzip des indirekten Beweises (Widerspruchsbeweises)*:

Eine Aussage A ist zu zeigen. Dann wird unter der Annahme $\neg A$ eine Beweiskette konstruiert, welche auf die Negation $\neg S$ eines bereits bekannten Satzes S führt.

Damit wird also $\neg A \Rightarrow \neg S$ gezeigt. Nach der Schlußregel (6) ist dies äquivalent zu $S \Rightarrow A$. Da S bereits als wahr bekannt ist, folgt aus (10) die Aussage A.

Ein Beispiel hierfür ist der Beweis des folgenden Satzes.

Satz 1.5. $\sqrt{2}$ *ist nicht rational.*

Beweis. Angenommen $\sqrt{2}$ ist rational. Da sich jede rationale Zahl vollständig kürzen läßt, existieren $r, s \in \mathbb{N}_+$ mit $\sqrt{2} = \frac{r}{s}$ und $\frac{r}{s}$ vollständig gekürzt. Es folgt $2 = \frac{r^2}{s^2}$, also

$$r^2 = 2s^2, \tag{11}$$

und somit ist r^2 gerade. Da das Quadrat einer ungeraden Zahl ungerade ist[2], muß nun gelten

$$r \text{ ist gerade.} \tag{12}$$

Daher existiert eine Zahl $\tilde{r} \in \mathbb{N}_+$ mit $r = 2\tilde{r}$ und (11) impliziert $4\tilde{r}^2 = 2s^2$. Division durch 2 ergibt $2\tilde{r}^2 = s^2$, d.h., daß s^2 gerade ist. Analog zu oben muß nun auch s gerade sein, also sind nach (12) sowohl r als auch s gerade und besitzen daher beide 2 als Teiler, im Widerspruch dazu, daß $\frac{r}{s}$ vollständig gekürzt ist. □

Wir haben einige Möglichkeiten gefunden, zwei (oder auch endlich viele) Aussagen zu einer neuen Aussage zu verbinden. Die wichtigsten sind „und“ und „oder“. Wie steht es aber, wenn man unendlich viele Aussagen mit „und“ oder „oder“ verknüpfen will?

Definition 1.6. Es seien $k \in \mathbb{N}_+$. Eine *k-stellige Aussageform mit Einsetzungsklassen* $\Omega_1, \dots \Omega_k$ ist ein sprachlich und grammatisch richtiger Ausdruck H mit k Leerstellen derart, daß für alle x_1 aus Ω_1, ..., x_k aus Ω_k gilt

$$H(x_1, \dots, x_k) \text{ ist eine Aussage.}$$

Beispiel.

1.) Seien $\Omega_1 := \mathbb{R}$ und

$$H(x) :\Longleftrightarrow x \in \mathbb{Q}.$$

Dann sind $H(1)$ und $H(\frac{1}{2})$ wahr, aber $H(\sqrt{2})$ ist falsch.

2.) Seien $\Omega_1 := \mathbb{N}$ und

$H(x) :\Longleftrightarrow x$ ist Summe des Quadrates zweier positiver natürlicher Zahlen.

Dann sind $H(2)$ und $H(25)$ wahr, aber $H(3)$ ist falsch.

3.) Sind $\Omega_1 := \Omega_2 := \mathbb{R}$ und

$$H(x_1, x_2) :\Longleftrightarrow x_1 \le x_2,$$

so ist $H(2,3)$ wahr und $H(3,2)$ falsch.

[2] $(2n+1)^2 = 4n^2 + 4n + 1$ und $4n^2 + 4n$ ist gerade.

Definition 1.7 (Quantoren)**.**

(i) Sei H eine einstellige Aussageform mit einsetzungsklasse Ω. Wir definieren dann zwei neue Aussageformen $\boxed{\forall_x H(x)}$, i.W. „*für alle x gilt $H(x)$*“, und $\boxed{\exists_x H(x)}$, i.W. „*es existiert (mindestens) ein x, für das $H(x)$ gilt*“, wie folgt:

$\forall_x H(x)$ ist per definitionem genau dann wahr, wenn für alle x aus Ω die Aussage $H(x)$ wahr ist;

$\exists_x H(x)$ ist per definitionem genau dann wahr, wenn für mindestens ein x aus Ω die Aussage $H(x)$ wahr ist.

$\boxed{\forall}$ und $\boxed{\exists}$ heißen *Quantoren*, die aus berechtigten Gründen auch mit $\boxed{\bigwedge}$ und $\boxed{\bigvee}$ bezeichnet werden.

Bemerkung.

1.) Es gilt

$$(\neg(\forall_x H(x))) \iff (\exists_x (\neg H(x)))$$

und

$$(\neg(\exists_x H(x))) \iff (\forall_x (\neg H(x)))\,.$$

2.) Es ist einfach, Beispiele zu finden, in denen $\forall_x H(x)$ falsch, aber $\exists_x H(x)$ wahr ist.

(ii) Seien H eine zweistellige Aussageform mit Einzetzungsklassen Ω_1, Ω_2. Dann können wir neue Aussageformen

$$\boxed{\forall_{x_1}\forall_{x_2} H(x_1,x_2)}, \quad \boxed{\forall_{x_2}\forall_{x_1} H(x_1,x_2)},$$
$$\boxed{\forall_{x_1}\exists_{x_2} H(x_1,x_2)}, \quad \boxed{\exists_{x_2}\forall_{x_1} H(x_1,x_2)},$$
$$\boxed{\exists_{x_1}\forall_{x_2} H(x_1,x_2)}, \quad \boxed{\forall_{x_2}\exists_{x_1} H(x_1,x_2)},$$
$$\boxed{\exists_{x_1}\exists_{x_2} H(x_1,x_2)}, \quad \boxed{\exists_{x_2}\exists_{x_1} H(x_1,x_2)}$$

definieren.

Bemerkung. I.a. kommt ea auf die Reihenfolge der Quantoren an, wie das Beispiel $\Omega_1 := \Omega_2 := \mathbb{R}$ mit

$$H(x_1,x_2) :\iff x_1 \le x_2$$

zeigt.

Satz 1.8. *Sei H eine zweisteellige Aussageform mit Einsetzungsklassen Ω_1, Ω_2. Dann gilt*

$$(\forall_{x_1}\forall_{x_2} H(x_1,x_2)) \iff (\forall_{x_2}\forall_{x_1} H(x_1,x_2))$$

und

$$(\exists_{x_1}\exists_{x_2} H(x_1,x_2)) \iff (\exists_{x_2}\exists_{x_1} H(x_1,x_2))\,.$$

Beweis. Wir beweisen nur „$\Rightarrow$“ der ersten Aussage, den restlichen Teil des Beweises überlassen wir als Übung.

Wir müssen zeigen

$$\forall_{x_1} \forall_{x_2} H(x_1, x_2) \text{ ist wahr } \Longrightarrow \forall_{\tilde{x_2}} \forall_{\tilde{x_1}} H(\tilde{x_1}, \tilde{x_2}) \text{ ist wahr.}$$

Sei also $\forall_{x_1} \forall_{x_2} H(x_1, x_2)$ wahr. Ist $\tilde{x_2}$ aus Ω_2 beliebig, so ist zu zeigen, daß $\forall_{\tilde{x_1}} H(\tilde{x_1}, \tilde{x_2})$ wahr ist, und dies ist mit $x_1 := \tilde{x_1}$ und $x_2 := \tilde{x_2}$ für jedes $\tilde{x_1}$ aus Ω_1 klar. □

2 Mengen (insbesondere natürliche Zahlen) und Abbildungen

Naive Mengenlehre

Wir wollen nun Objekte bereitstellen, über die wir etwas aussagen können, sog. *Mengen*. Die meisten Menschen haben heute vermutlich ein intuitives Verständnis von dem, was sie unter einer Menge verstehen.

Definition 2.1 (Mengen à la CANTOR (1877))**.** Eine *Menge* ist eine Zusammenfassung von bestimmten, wohlunterschiedenen Objekten unserer Anschauung oder unseres Denkens, welche wir dann die *Elemente* der Menge nennen, zu einem Ganzen.

Ist a ein Element einer Menge M, so schreiben wir $\boxed{a \in M}$ und andernfalls $\boxed{a \notin M}$.

Wir werden bald sehen, daß dieser „naive" Mengenbegriff nicht ganz unproblematisch ist. Zunächst wollen wir aber mit ihm arbeiten.

Definiton (Quantoren)**.** Seien M eine Menge und H eine einstellige Aussageform, deren Einsetzungsklasse Ω die Menge M umfaßt.

Wir definieren drei neue Aussagen wie folgt:

(i) $\boxed{\forall_{x \in M} H(x)} :\Longleftrightarrow \forall_x \left(x \in M \Rightarrow H(x)\right)$.

(ii) $\boxed{\exists_{x \in M} H(x)} :\Longleftrightarrow \exists_x \left(x \in M \wedge H(x)\right)$.

(iii) $\boxed{\exists!_{x \in M} H(x)} :\Longleftrightarrow \exists_{x \in M} \left(H(x) \wedge \forall_{y \in M} \left(H(y) \Rightarrow x = y\right)\right)$.

Man schreibt übrigens auch $\boxed{\forall\!\!\!\cdot}$ anstelle von $\exists!$.

Beispiel (für Mengen)**.**

1.) $\mathbb{N} = \{0, 1, 2, \ldots\}$ und $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.

2.) $\{2n + 1 \mid n \in \mathbb{N}\} = \{1, 3, 5, 7, \ldots\}$ ist die Menge der *ungeraden Zahlen*.

$\{x \in \mathbb{N} \mid \exists_{y \in \mathbb{N}}\, y^2 = x\} = \{0, 1, 4, 9, 16, \ldots\}$ ist die Menge der *Quadratzahlen*.

Für alle $a, b \in \mathbb{R}$ mit $a \leq b$ setzen wir $\boxed{[a, b]} := \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

Man kann eine Menge auf zwei Arten beschreiben: Entweder durch eine Aufzählung ihrer Elemente oder durch eine charakteristische Eigenschaft. Man beachte, daß es bei der Aufzählung der Elemente einer Menge nicht auf die Reihenfolge der Elemente ankommt, z.B. gilt $\{0, 1\} = \{1, 0\}$. Außerdem können Elemente mehrfach aufgezählt werden, z.B. $\{0\} = \{0, 0, 0\}$.

Definition 2.2. Es seien M, N Mengen.

(i) N heißt *Teilmenge von* M (i.Z. $\boxed{N \subset M}$) genau dann, wenn $\forall_{a \in N}\, a \in M$ gilt.

Ist N keine Teilmenge von M, so schreiben wir $\boxed{N \not\subset M}$.

(ii) Wir sagen N *ist gleich* M (i.Z. $\boxed{N = M}$) genau dann, wenn $N \subset M$ und $M \subset N$ gilt

Wenn $N = M$ nicht gilt, d.h. per definitionem N *ist ungleich* M, so schreiben wir $\boxed{N \neq M}$.

Satz 2.3. *Es gibt genau eine Menge* $\boxed{\varnothing}$*, die kein Element enthält.*

Beweis. Da $M := \{\,\}$ kein Element besitzt, genügt es die Eindeutigkeit zu zeigen:

Sei N eine weitere Menge die kein Element besitzt. Nach 2.2 (ii) haben wir nachzuweisen, daß für alle a aus der Klasse aller Objekte gilt

$$a \in M \iff a \in N. \tag{13}$$

Nach Definition von M ist die linke Seite von (13) falsch, und nach Voraussetzung ist die rechte Seite von (13) ebenfalls falsch, d.h. (13) ist wahr. □

Definiton (Leere Menge)**.** $\varnothing$ heißt die *leere Menge*.

Definition 2.4. Es seien M und N Mengen. Wir definieren dann

(i) die *Vereinigung von* M *und* N als die Menge

$$\boxed{M \cup N} := \{a \,|\, a \in M \vee a \in N\},$$

(ii) den *Schnitt von* M *und* N als die Menge

$$\boxed{M \cap N} := \{a \,|\, a \in M \wedge a \in N\},$$

(iii) die *Differenz von* M *und* N als die Menge

$$\boxed{M \setminus N} := \{a \,|\, a \in M \wedge a \notin N\} \text{ und}$$

(iv) die *Potenzmenge von* M als die Menge

$$\boxed{\mathfrak{P}(M)} := \{\widetilde{N} \,|\, \widetilde{N} \subset M\}.$$

Satz 2.5. *Sind* L, M, N *Mengen, so gelten*

(i) die Kommutativität

$$M \cup N = N \cup M \quad \wedge \quad M \cap N = N \cap N,$$

(ii) die Assoziativität

$$(M \cup N) \cup L = M \cup (N \cup L) \quad \wedge \quad (M \cap N) \cap L = M \cap (N \cap L),$$

(iii) die Distributivität

$$M \cap (N \cup L) = (M \cap N) \cup (M \cap L),$$
$$M \cup (N \cap L) = (M \cup N) \cap (M \cup L),$$
$$(M \cup N) \setminus L = (M \setminus L) \cup (N \setminus L),$$
$$(M \cap N) \setminus L = (M \setminus L) \cap (N \setminus L) \text{ und}$$

(iv) die de Morganschen-Regeln

$$M \setminus (N \cup L) = (M \setminus N) \cap (M \setminus L),$$
$$M \setminus (N \cap L) = (M \setminus N) \cup (M \setminus L).$$

Beweis als Übung. □

Axiomatische Mengenlehre

Wir kommen zurück auf die eingangs erwähnte Problematik des Cantorschen Mengenbegriffes.

Wir können Mengen als Elemente anderer Mengen auffassen, beispielsweise gilt $\{0\} \in \{\{0\}\}$. (Achtung: $\{0\} \subset \{\{0\}\}$ gilt nicht!) Gemäß der Cantorschen Definition einer Menge können wir dann auch die Menge der Mengen, die sich nicht selbst enthalten, bilden:

$$M_R := \{N \mid N \text{ ist Menge und } N \notin N\}.$$

Es gibt jetzt zwei Möglichkeiten: Entweder gilt $M_R \in M_R$; dann folgt aus der Definition von M_R: $M_R \notin M_R$. Oder es gilt $M_R \notin M_R$; dann folgt aus der Definition von M_R aber $M_R \in M_R$. Damit haben wir gezeigt:

$$M_R \in M_R \iff M_R \notin M_R.$$

Gemäß der Cantorschen Definition einer Menge steht jedoch für ein Objekt a und eine Menge M eindeutig fest, ob $a \in M$ oder $a \notin M$ gilt. Die einzig mögliche Konsequenz ist:

$$M_R \text{ ist keine Menge.}$$

Dieses Beispiel von Bertrand Russel (1901) nennt man die *Russelsche Antinomie*. Sie zeigt, daß der von Cantor vorgeschlagene Mengenbegriff zu allgemein ist. Solche Antinomien wurden schon in der Antike betrachtet. Der Kreter Epimenides sagte im 6. Jh. v. Chr.: „Alle Kreter lügen."

Um den obigen Widerspruch (und weitere) zu vermeiden, verzichten wir völlig auf die Definition einer Menge und gehen statt dessen axiomatisch vor. Die heute üblicherweise der Mathematik zugrundeliegende *Axiomatische Mengenlehre nach* Zermelo *und* Fraenkel *mit Auswahlaxiom*, die man kurz mit (ZFC) bezeichnet, werden wir im folgenden angeben. Soweit man weiß, ist (ZFC) widerspruchsfrei.

Wir betrachten eine Klasse von Objekten, die wir *Mengen* nennen. Für je zwei Mengen X, Y stehe eindeutig fest, ob $X \in Y$ oder $Y \notin X$ gilt.

Axiom 1 (Existenz-Axion)**.** Es gibt (mindestens) eine Menge, die kein Element besitzt.

Axiom 2 (Extensions-Axion)**.** Zwei Mengen sind genau dann gleich, wenn sie dieselben Elemente besitzen.

Axiom 2 besagt genau, daß für alle Mengen M, N gilt

$$M = N \iff M \subset N \wedge N \subset M.$$

Wie beim Beweis von Satz 2.3 folgt aus den Axiomen 1 und 2, daß genau eine Menge $\boxed{\varnothing}$, die kein Element besitzt, existiert.

Axiom 3 (Komprehensions-Axiom)**.** Sei P eine für Mengen definierte einstellige Aussageform.

Dann ist für jede Menge M auch

$$\{X \in M \mid P(X) \text{ ist wahr}\}$$

eine Menge.

Beispiel.

1.) Wenn wir bereits wüßten, daß $\mathbb{N}$ eine Menge ist, so folgte aus Axiom 3, daß auch die Menge der geraden Zahlen

$$\{n \in \mathbb{N} \mid 2 \mid n\}$$

eine Menge ist.

2.) Sind M, N Mengen, so sind auch

$$M \cap N = \{X \in M \mid X \in N\},$$
$$M \setminus N = \{X \in M \mid X \notin N\}$$

Mengen.

Axiom 4 (Paarmengen-Axiom)**.** Sind M, N Mengen, so ist auch $\{M, N\}$ eine Menge. (Beachte, daß im Falle $M = N$ gilt, daß $\{M\}$ eine Menge ist.)

Beispiel. $\{\varnothing\}, \{\{\varnothing\}\}$ und $\{\varnothing, \{\varnothing\}\}$ sind Mengen.

Axiom 5 (Vereinigungsmengen-Axiom)**.** Ist $\mathfrak{M}$ eine Menge, so ist auch $\bigcup_{M \in \mathfrak{M}} M$ eine Menge.

Axiom 5 nennen wir der Vollständigkeit halber, wichtig für uns ist das folgende Beispiel:

Beispiel. Für Mengen A, B ist nach Axiom 4 auch $\{A, B\}$ eine Menge, und es gilt nach Axiom 5, daß auch

$$A \cup B = \{X \mid \exists_{M \in \{A,B\}}\, X \in M\}$$

eine Menge ist.

Axiom 6 (Potenzmengen-Axiom)**.** Mit M ist auch $\mathfrak{P}(M)$ eine Menge.

Aus den bisherigen Axiomen folgt nur die Existenz endlicher Mengen. Wir möchten aber selbstverständlich eine Menge

$$\{0, 1, 2, \dots\}$$

haben – und diese dann die *Menge der natürlichen Zahlen* nennen. Wir beginnen damit, die ersten natürlichen Zahlen zu definieren:

Definition 2.6.

$$\boxed{0} := \varnothing,$$
$$\boxed{1} := 0 \cup \{0\} = \{\varnothing\},$$
$$\boxed{2} := 1 \cup \{1\} = \{\varnothing, \{\varnothing\}\},$$
$$\boxed{3} := 2 \cup \{2\} = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\}$$
usw.

Allgemein setzen für eine Menge X den *Nachfolger von* X als

$$\boxed{S(X)} := X \cup \{X\}$$

und schreiben auch $\boxed{X+1}$ für $S(X)$. Also gilt $1 = 0+1$, $2 = 1+1$, $3 = 2+1$ usw.

Eine Menge I heißt *induktiv* genau dann, wenn gilt

$$0 \in I \quad \wedge \quad (X \in I \Longrightarrow X+1 \in I).$$

Da man aus den ersten sechs Axiomen nicht die Existenz einer induktiven Menge herleiten kann, ist es naheliegend, das folgende hinzuzunehmen.

Axiom 7 (Unedlichkeitsaxiom)**.** Es existiert (mindestens) eine induktive Menge, die wir mit $\boxed{I_0}$ bezeichnen.

Definition 2.7. Nach Axiom 3 ist

$$\boxed{\mathbb{N}} := \{X \in I_0 \,|\, X \in I \text{ für jede induktive Menge } I\}$$

eine Menge, die wir die *Menge der natürlichen Zahlen* nennen.

Satz 2.8. *$\mathbb{N}$ ist eine induktive Menge, und für jede induktive Menge I gilt $\mathbb{N} \subset I$.*

Beweis. Aus der Definition von $\mathbb{N}$ folgt offenbar

$$X \in \mathbb{N} \Longleftrightarrow X \in I \text{ für jede indultive Menge } I. \tag{14}$$

Hieraus ergibt sich sofort, da0 $\mathbb{N}$ Teilmenge einer jeden induktiven Menge ist. Zu zeigen bleibt, daß $\mathbb{N}$ induktiv ist:

1.) Für jede induktive Menge I gilt per definitionem $0 \in I$, also nach (14) auch $0 \in \mathbb{N}$.

2.) Sei $n \in \mathbb{N}$. Dann gilt nach (14) für jede induktive Menge I auch $n \in I$, also $n+1 \in I$. Wiederum nach (14) gilt dann auch $n+1 \in \mathbb{N}$. □

Satz 2.9 (Prinzip der vollständigen Induktion, 1. Version)**.** *Sei P eine für natürliche Zahlen definierte einstellige Aussageform mit*

$$P(0) \qquad \text{(„Induktionsanfang“),}$$
$$\forall_{n \in \mathbb{N}} \, (P(n) \Longrightarrow P(n+1)) \qquad \text{(„Induktionsschritt“).}$$

Dann gilt: $\forall_{n \in \mathbb{N}} P(n)$.

Beweis. $I := \{n \in \mathbb{N} \,|\, P(n)\}$ ist nach Voraussetzung eine induktive Menge, d.h. nach Satz 2.8: $\mathbb{N} \subset I$, also $\forall_{n \in \mathbb{N}} P(n)$. □

Anwendungen des Prinzipes der vollständigen Induktion sowie Primzahlen

Der auf dem zuletzt herausgegebenen 10 DM-Schein abgebildete CARL FRIEDRICH GAUSS (1777 - 1855) hat den folgenden Satz angeblich als Schüler (mit anderer Begründung) bewiesen.

Satz 2.10. $\forall_{n\in\mathbb{N}} \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$.

Beweis. Wir definieren auf den natürlichen Zahlen eine einstellige Aussageform P durch

$$\forall_{n\in\mathbb{N}}\, P(n) :\Longleftrightarrow \sum_{i=0}^{n} i = \frac{n(n+1)}{2}.$$

Induktionsanfang: Wir müssen zeigen, daß $P(0)$ gilt, und das ist klar.

Induktionsschritt: Wir müssen unter der Annahme, daß $P(n)$ für $n \in \mathbb{N}$ gilt, welche man *Induktionsvoraussetzung* nennt, zeigen, daß $P(n+1)$ gilt. Aus der Induktionsvoraussetzung folgt

$$\begin{aligned}\sum_{i=1}^{n+1} i &= \left(\sum_{i=1}^{n} i\right) + (n+1) = \frac{n(n+1)}{2} + (n+1)\\ &= \frac{(n+1)\cdot(n+2)}{2},\end{aligned}$$

womit $P(n+1)$ gezeigt ist.

Der Satz folgt nun aus Satz 2.9. □

Der Beweis des folgenden Satzes demonstriert die übliche Kurznotation eines Beweises durch vollständige Induktion.

Satz 2.11. $\forall_{n\in\mathbb{N}} \sum_{i=0}^{n}(2i+1) = (n+1)^2$.

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

$$\begin{aligned}\sum_{i=0}^{n+1}(2i+1) &= \left(\sum_{i=0}^{n}(2i+1)\right) + 2(n+1) + 1 \overset{\text{IV}}{=} (n+1)^2 + 2(n+1) + 1\\ &= ((n+1)+1)^2\end{aligned}$$

□

Bemerkung.

1.) (Unerläßlichkeit der Verankerung)

Für die offenbar falsche Formel

$$\forall_{n\in\mathbb{N}} \sum_{i=0}^{n} i = \frac{n(n+1)}{2} + 5$$

gelingt o.w. der Induktionsschritt, aber natürlich nicht die Verankerung.

2.) (Unerläßlichkeit des Induktionsschrittes)

Betrache den Ausdruck $n^2 + n + 17$. Setzt man $n \in \{0, 1, \ldots, 15\}$ ein, so erhält man $17, 19, 23, 29, 37, 47, \ldots, 257$, also stets Primzahlen, s.u. 2.14. Man könnte vermuten, daß $n^2 + n + 17$ für jedes $n \in \mathbb{N}$ eine Primzahl ist. Aber

$$16^2 + 16 + 1 = 16 \cdot (16 + 1) + 17 = (16 + 1) \cdot 17 = 17^2$$

ist keine Primzahl.

Man kann übrigens zeigen, daß

$$a_k\, n^k + a_{k-1}\, n^{k-1} + \ldots + a_1\, n + a_0 \text{ mit } k \in \mathbb{N}_+ \text{ und } a_0, \ldots, a_k \in \mathbb{Z}$$

niemals für alle $n \in \mathbb{N}$ eine Primzahl ergeben kann. Aber z.B. $n^2 - 79\, n + 1601$ liefert erstmals für $n = 80$, wobei $n \in \mathbb{N}$ sei, keine Primzahl.

Satz ? Für jedes $n \in \mathbb{N}$ besitzen je n paarweise verschiedene Menschen dieselbe Augenfarbe.

„Beweis.“ Für $n = 0$ (oder $n = 1$) ist die Aussage trivial.

Sei also $n \in \mathbb{N}$ und gelte die Behauptung für n. Sind dann $(n + 1)$ paarweise verschiedene Menschen $M_1, \ldots, M_{n+1}$ gegeben, so besitzen nach Induktionsvoraussetzung sowohl $M_1, \ldots, M_n$ als auch $M_2, \ldots, M_{n+1}$ dieselbe Augenfarbe, also auch $M_1, \ldots, M_{n+1}$.

Wo liegt der Fehler?

Satz 2.12 (Prinzip der vollständigen Induktion, 2. Version)**.** *Sei P eine für natürliche Zahlen definierte einstellige Aussageform mit*

$$\begin{aligned} &P(0) && \text{(„Induktionsanfang“),}\\ &\forall_{n \in \mathbb{N}}\, ((P(0) \wedge \ldots \wedge P(n)) \Longrightarrow P(n+1)) && \text{(„Induktionsschritt“).} \end{aligned}$$

Dann gilt: $\forall_{n \in \mathbb{N}}\, P(n)$.

Beweis. Wir definieren eine auf den natürlichen Zahlen definierte Aussageform $\widetilde{P}$ durch

$$\forall_{n \in \mathbb{N}}\, \left(\widetilde{P}(n) :\Longleftrightarrow P(0) \wedge \ldots \wedge P(n)\right).$$

Da aus der Voraussetzung sofort $\widetilde{P}(0)$ folgt, haben wir wegen Satz 2.9 zu zeigen, daß auch gilt

$$\forall_{n \in \mathbb{N}}\, \left(\widetilde{P}(n) \Longrightarrow \widetilde{P}(n+1)\right).$$

Dies ist aber klar. □

Wir werden die zweite Version des Prinzipes der vollständigen Induktion nutzen, um zu zeigen, daß sich jede natürliche Zahl, die größer als eins ist, als Produkt von Primzahlen schreiben läßt.

Definition 2.13. Seien $k \in \mathbb{Z}$ und $t \in \mathbb{Z} \setminus \{0\}$.

Wir sagen „t *teilt* k“ (i.Z. $\boxed{t \mid k}$) genau dann, wenn eine Zahl $l \in \mathbb{Z}$ mit $k = l \cdot t$ existiert.

Definition 2.14 (Primzahlen)**.** Eine natürliche Zahl $p \in \mathbb{N}$ mit $p > 1$ heißt *Primzahl* genau dann, wenn p als einzige positiven Teiler die Zahlen 1 und p besitzt.

Bemerkung. Wir haben den Begriff der *Primzahl* eingeführt, nicht etwa die sog. *Primeigenschaft*, vgl. Übungen.

Satz 2.15. *Ist $p \in \mathbb{N}$ mit $p > 1$, so sind die folgenden Aussagen äquivalent:*

(i) *p ist Primzahl.*

(ii) *p ist* unzerlegbar*, d.h. per definitionem, daß für $m, n \in \mathbb{N}$ mit $p = m \cdot n$ gilt $m = 1$ oder $n = 1$.*

Beweis. „(i) $\Rightarrow$ (ii)“ Seien p eine Primzahl und $m, n \in \mathbb{N}$ mit $p = m \cdot n$. Dann folgt $m \mid p$, also – da p Primzahl – $m = 1$ oder $m = p$. Im Falle $m = 1$ sind wir fertig. Im Falle $m = p$ folgt aus $p = m \cdot n$, daß gilt $n = 1$.

„(ii) $\Rightarrow$ (i)“ Seien p unzerlegbar und $t \in \mathbb{N}$ ein positiver Teiler von p, d.h.

$$\exists_{n \in \mathbb{N}}\, p = n \cdot t.$$

Da p unzerlegbar ist, folgt entweder $n = 1$ oder $t = 1$. Ist $t = 1$, so ist die Behauptung wegen der Beliebigkeit von t gezeigt. Ist $n = 1$, so gilt $t = p$, und die Behauptung ist ebenfalls wegen der Beliebigkeit von t gezeigt. □

Satz 2.16. *Jede natürliche Zahl $n > 1$ ist (endliches) Produkt von Primzahlen.*

Beispiel. $15 = 3 \cdot 5$ und $70 = 2 \cdot 5 \cdot 7$.

Bemerkung.

1.) Das Produkt kann auch nur aus einem Faktor bestehen, nämlich dann, wenn n eine Primzahl ist.

2.) Primfaktoren können mehrfach auftreten, z.B. gilt $12 = 2 \cdot 2 \cdot 3$.

3.) Wir werden unten einsehen, daß die Zerlegung in Primfaktoren bis auf die Reihenfolge der Faktoren eindeutig ist.

Beweis des Satzes. Wir definieren auf den natürlichen Zahlen eine einstellige Aussageform P wie folgt

$$\forall_{n \in \mathbb{N}}\ \big(P(n) :\Longleftrightarrow (n+2) \text{ ist endliches Produkt von Primzahlen}\big).$$

$P(0)$ ist trivial. Sei also $n \in \mathbb{N}$ mit $P(0) \wedge \ldots, \wedge P(n)$. Wir haben zu zeigen, daß $P(n+1)$ gilt. Ist $n+3$ eine Primzahl, so sind wir fertig. Ist $n+3$ keine Primzahl, so existieren nach Satz 2.15 Zahlen $k, l \in \mathbb{N}$ mit $k > 1$ und $l > 1$ derart, daß $n+3 = k \cdot l$, also $2 \leq k, l \leq n+2$, gilt. Nun lassen sich wegen $P(0) \wedge \ldots, \wedge P(n)$ sowohl k als auch l als endliches Produkt von Primzahlen schreiben, woraus sich $P(n+1)$ ergibt. □

Satz 2.17 (Prinzip der Wohlordnung der Menge der natürlichen Zahlen)**.** *Jede nicht-leere Teimenge von $\mathbb{N}$ besitzt ein kleinstes Element.*

Bemerkung. Die zu $\mathbb{N}$ gleichmächtige Menge $\{\frac{1}{n+1} \mid n \in \mathbb{N}\} \subset \mathbb{Q}$ besitzt kein kleinstes Element.

Beweis des Satzes. Wir führen den Beweis indirekt und nehmen an, daß X eine nicht-leere Teilmenge von $\mathbb{N}$ ist, die kein kleinstes Element besitzt. Wir definieren auf den natürlichen Zahlen eine einstellige Aussageform P durch

$$\forall_{n\in\mathbb{N}}\ (P(n) :\Longleftrightarrow n \notin X)$$

und zeigen $\forall_{n\in\mathbb{N}} P(n)$, womit $X = \varnothing$, also ein Widerspruch nachgewiesen ist.

$P(0)$ ist evident, denn 0 ist das kleinste Element von $\mathbb{N} \supset X$.

Sei nun $n \in \mathbb{N}$ und gelte $P(0) \wedge \ldots \wedge P(n)$, d.h.

$$0, \ldots, n \notin X.$$

Wäre $n+1 \in X$, so wäre $n+1$ das kleinste Element von X, Widerspruch! Damit gilt auch $P(n+1)$. □

Satz 2.18 (Fundamentalsatz der Arithmetik)**.** *Jede natüliche Zahl, die größer als eins ist, läßt sich bis auf die Reihenfolge der Faktoren eindeutig als (endliches) Produkt von Primzahlen schreiben.*

Beweis. Die Existenz haben wir bereits in Satz 2.16 bewiesen. Zu zeigen bleibt die Eindeutigkeit. Hierbei schließen wir indirekt und nehmen an, es gäbe eine natürliche Zahl, die größer als eins ist, die sich auf zwei Arten in Primfaktoren zerlegen läßt. Nach Satz 2.17 gibt es dann ein kleinstes $n \in \mathbb{N}$ mit $n \geq 2$ verschiedenen Primfaktorzerlegungen

$$n = p_1 \cdots p_r, \tag{15}$$

$$n = q_1 \cdots q_s. \tag{16}$$

Ohne Beschränkung der Allgemeinheit gelte $p_1 \leq \ldots \leq p_r$ und $q_1 \leq \ldots \leq q_r$. Da n die kleinste natürliche Zahl größer eins mit zwei verschiedenen Primfaktorzerlegungen ist, gilt $p_1 \neq q_1$, denn sonst hätte $\frac{n}{p_1} = \frac{n}{q_1}$ dieselbe Eigenschaft.

Ohne Beschränkung der Allgemeinheit gelte weiter $p_1 < q_1$. Dann folgt

$$q_1 > p_1 > 2, \tag{17}$$

da n im Falle $p_1 = 2$ wegen (15), (16) sonst eine gerade sowie ungerade natürliche Zahl wäre, und wir setzen

$$m := \underbrace{n - p_1 \cdot q_2 \cdots q_s}_{\overset{(15)}{=} p_1\cdot(p_2\cdots p_r - q_2\cdots q_s)} \overset{(16)}{=} (q_1 - p_1)\cdot q_2 \cdots q_s \in \{2, \ldots n-1\}, \tag{18}$$

beachte, daß p_1, q_1 Primzahlen mit (17) sind.

Da n die kleinste natürliche Zahl größer eins mit verschiedenen Primfaktorzerlegungen ist, folgt aus (18) und $p_1 < q_1 \leq q_2 \leq \ldots \leq q_s$

$$p_1 \,|\, (q_1 - p_1) \quad \vee \quad p_1 \in \{q_2, \ldots, q_s\},$$

also wegen $p_1 < q_1 \leq q_2 \leq \ldots \leq q_s$: $p_1 | (q_1 - p_1)$. Somit existiert $k \in \mathbb{N}_+$ mit $p_1 \cdot k = q_1 - p_1$, d.h.

$$q_1 = p_1 \cdot \underbrace{(k+1)}_{\geq 2},$$

im Widerspruch dazu, daß q_1 eine Primzahl ist. □

Abbildungen

Seien M, N Mengen. Intuitiv würden wir eine Abbildung $f\colon M \to N$ als eine Zuordnung definieren, die jedem Elemten $x \in M$ genau ein Element $f(x) \in N$ zuordnet. Vom axiomatischen Standpunkt aus gesehen, kennen wir jedoch nur Mengen und wollen sämtliche Objekte als Mengen definieren. Wie können wir eine Abbildung als Menge interpretieren?

Zunächst benötigen wir die Definition des *kartesischen Produktes zweier Mengen*: Gehen wir vorerst wieder von der Intuition aus, so würden wir das Produkt von M und N als

$$M \times N := \{(a,b) \,|\, a \in M \wedge b \in N\}$$

definieren und zwei Elemente $(a,b), (\tilde{a},\tilde{b}) \in M \times N$ genau dann gleich nennen, wenn gilt $a = \tilde{a}$ sowie $b = \tilde{b}$. Was aber genau soll (a,b) sein? Und warum ist $M \times N$ eine Menge?

Das folgende Lemma, dessen Beweis wir dem Leser als Übung überlassen, liefert eine Möglichkeit eine Menge $M \times N$ mit den gewünschten Eigenschaften zu definieren.

Lemma 2.19. *Seien M, N Mengen, und $a, \tilde{a} \in M$ sowie $b, \tilde{b} \in N$.*
Dann gilt:

(i) $\big\{\{a\},\{a,b\}\big\} \in \mathfrak{P}(\mathfrak{P}(M \cup N))$.

(ii) $\big\{\{a\},\{a,b\}\big\} = \big\{\{\tilde{a}\},\{\tilde{a},\tilde{b}\}\big\} \iff \big(a = \tilde{a} \wedge b = \tilde{b}\big)$. □

Definition 2.20. Es seien M, N Mengen.

(i) Für $a \in M$ und $b \in N$ definieren wir

$$\boxed{(a,b)} := \big\{\{a\},\{a,b\}\big\} \in \mathfrak{P}(\mathfrak{P}(M \cup N)).$$

(ii) Nach Axiom 3 ist

$$\boxed{M \times N} := \{X \in \mathfrak{P}(\mathfrak{P}(M \cup N)) \,|\, X = (a,b) \wedge a \in M \wedge b \in N\}$$

eine Menge, die wir das *kartesische Produkt von M und N* nennen.

Eine Abbildung $f\colon M \to N$ soll, wie oben besprochen, jedem Element $x \in M$ genau ein Element $f(x) \in N$ zuordnen. Wir können diese Zuordnung $x \mapsto f(x)$ für jedes $x \in M$ als ein Element $(x, f(x)) \in M \times N$ auffassen. Daher definieren wir:

Definition 2.21. Es seien M, N Mengen.

Eine *Abbildung* $f\colon M \to N$ ist per definitionem eine Teilmenge Γ_f von $M \times N$ derart, daß gilt

$$\forall_{x \in M} \exists!_{y \in N} (x,y) \in \Gamma_f. \tag{19}$$

Für jedes $x \in N$ heißt das eindeutig bestimmte Element y wie (19) der *Wert von f an der Stelle x*, und man schreibt hierfür auch $\boxed{f(x)}$.

Ist A eine Teilmenge von M, so heißt die Menge, vgl. Axiom 3,

$$\boxed{f(A)} := \{b \in N \mid \exists_{a \in A}\, f(a) = b\}$$

das *Bild von A unter f*.

Für jede Teilmenge B von M setzen wir das *Urbild von B unter f* als

$$\boxed{\overline{f}^1(B)} := \{a \in M \mid \exists_{b \in B}\, f(b) = a\}.$$

Die Menge aller Abbildungen $M \to N$ sei mit $\boxed{\mathrm{Abb}(M,N)}$ bezeicnet. Daß dies eine Menge ist, folgt aus Axiom 3 und (19).

Definition 2.22 (Injektion, Surjektion und Bijektion)**.** Es seien M, N Mengen und $f\colon M \to N$ eine Abbildung. Wir definieren

(i) f *injektiv* $:\Longleftrightarrow \forall_{x,\tilde{x} \in M}\, (f(x) = f(\tilde{x}) \Rightarrow x = \tilde{x})$,

(ii) f *surjektiv* $:\Longleftrightarrow \forall_{y \in N} \exists_{x \in M}\, f(x) = y$,

(iii) f *bijektiv* $:\Longleftrightarrow f$ injektiv und surjektiv $\Longleftrightarrow \forall_{y \in N} \exists!_{x \in M}\, f(x) = y$.

Eine injektive bzw. surjektive bzw. bijektive Abbildung nennt man auch *Injektion* bzw. *Surjektion* bzw. *Bijektion*.

Definition 2.23 (Identität, Einschränkung, Kompsition, katesisches Produkt einer Mengenfamilie)**.** Seien M, N Mengen.

(i) Die Abbildung

$$\boxed{\mathrm{id}_M\colon M \longrightarrow M, \quad x \longmapsto x,}$$

heißt die *Identität von M*.

Ist darüber hinaus A eine Teilmenge von M, so heißt die Abbildung

$$\boxed{A \hookrightarrow M, \quad a \longmapsto a,}$$

die *Inklusion von A in M*, und für eine Abbildung $f\colon M \to N$ nennen wir

$$\boxed{f|_A\colon A \longrightarrow N, \quad a \longmapsto f(a),}$$

die *Einschränkung von f auf A*.

(ii) Ist $f\colon M \to N$ eine bijektive Abbildung, so heißt

$$\boxed{f^{-1}\colon N \longrightarrow M, \quad y \longmapsto x, \text{ wobei } x \text{ wie in 2.22 (iii) sei,}}$$

die *Umkehrabbildung von f*.

Zeige als Übungsaufgabe, daß dies tatsächlich eine Abbildung ist.

(iii) Sind L eine weitere Menge und $f\colon M \to N$ sowie $g\colon N \to L$ Abbildungen, so nennen wir

$$\boxed{g \circ f\colon M \longrightarrow L, \quad x \longmapsto g(f(x)),}$$

die *Komposition von f und g*.

Zeige als Übungsaufgabe, daß dies tatsächlich eine Abbildung ist.

(iv) Seien M eine Menge und $(M_i)_{i\in I}$ eine *Familie von Teilmengen von* M, d.h. per definitionem, daß I eine Menge und

$$I \longrightarrow M, \quad i \longmapsto M_i,$$

eine Abbildung mit $\forall_{i\in I}\, M_i \subset M$ ist. Dann heißt die Menge

$$\boxed{\bigtimes_{i\in I} M_i} := \{f \in \mathrm{Abb}(I, M) \,|\, \forall_{i\in I}\, f(i) \in M_i\}$$

das *kartesische Produkt der Mengenfamilie* $(M_i)_{i\in I}$.

Satz 2.24. *Es seien* M_1, M_2, M_3 *Mengen und* $f_1\colon M_1 \to M_2$, $f_2\colon M_2 \to M_3$ *Abbildungen.*

Dann gilt:

(i) f_1 *und* f_2 *injektiv* $\Longrightarrow$ $f_2 \circ f_1$ *injektiv.*

Die Umkehrung ist i.a falsch.

(ii) f_1 *und* f_2 *sujektiv* $\Longrightarrow$ $f_2 \circ f_1$ *surjektiv.*

Die Umkehrung ist i.a falsch.

(ii) f_1 *und* f_2 *bijektiv* $\Longrightarrow$ $f_2 \circ f_1$ *bijektiv.*

Die Umkehrung ist i.a falsch.

(iv) $f_2 \circ f_1$ *injektiv* $\Longrightarrow$ f_1 *injektiv.*

(v) $f_2 \circ f_1$ *surjektiv* $\Longrightarrow$ f_2 *surjektiv.*

Beweis als Übung. □

Wir nennen nun die letzten beiden Axiome von (ZFC), Axiom 8 allerdings nur der Vollständigkeit halber – wir werden es nicht ausnutzen.

Axiom 8 (Ersetzungs-Axion)**.** Es sei P eine für Mengen definierte zweistellige Aussageform derart, daß zu jeder Menge X genau eine Menge Y mit $P(X, Y)$ existiert.

Dann existiert zu jeder Menge A (genau) eine Menge B mit

$$y \in B \Longleftrightarrow \exists_{x\in A}\, P(x, y).$$

Bemerkung.

1.) Wir können mittels der Axiome 1 - 7 folgende Mengen definieren:

$$\boxed{\omega} := \mathbb{N},$$
$$\boxed{\omega + 1} := S(\omega) = \omega \cup \{\omega\} = \{0, 1, 2, \ldots, \omega\},$$
$$\boxed{\omega + 2} := S(\omega + 1) = \{0, 1, 2, \ldots, \omega, \omega + 1\}$$
usw.

Aber mittels der Axiome 1 - 7 können wir keine Menge $\{\omega + n \,|\, n \in \mathbb{N}\}$ nachweisen.

2.) Ebenfalls läßt sich mittels der Axiome 1 - 7 nicht zeigen, daß eine Menge existiert, deren Elemente gerade

$$\varnothing, \{\varnothing\}, \{\{\varnothing\}\}, \{\{\{\varnothing\}\}\}, \ldots$$

sind.

Um solches zu garantieren, benötigt man Axiom 8.

Axiom 9 (Auswahlaxiom)**.** Es seien M eine Menge, I eine nicht-leere Menge und $(M_i)_{i \in I}$ eine Familie nicht-leerer Teilmengen von M.

Dann gilt $\times_{i \in I} M_i \neq \varnothing$, also existiert eine Abbildung

$$f \colon I \longrightarrow M \quad \text{mit} \quad \forall_{i \in I}\, f(i) \in M_i.$$

Bemerkung. Seien $M := \{1,2,3\}$, $I := \{1,2,3,4\}$, $M_1 := \{1,3\}$, $M_2 := \{1,2\}$, $M_3 := \{2\}$ und $M_4 := \{2,3\}$. Dann ist

$$\begin{array}{rcl} f \colon \{1,2,3,4\} & \longrightarrow & \{1,2,3\} \\ 1 & \longmapsto & 3 \\ 2 & \longmapsto & 1 \\ 3 & \longmapsto & 2 \\ 4 & \longmapsto & 3 \end{array}$$

offenbar eine Abbildung $f \colon I \to M$ mit $\forall_{i \in I}\, f(i) \in M_i$. Wir können die Existenz eines f wie im Auswahlaxiom also durch explizite Angabe garantieren, und dies ist immer der Fall, wenn I eine *endliche* Menge ist.

Das Auswahlaxiom spielt erst dann eine Rolle, wenn I keine endliche Menge mehr ist.

Seien z.B. $M := \mathbb{R}$, $I := \mathfrak{P}(\mathbb{R}) \setminus \{\varnothing\}$ und $\forall_{i \in \mathfrak{P}(\mathbb{R}) \setminus \{\varnothing\}}\, M_i := i$. Das Auswahlaxiom besagt, daß es eine Abbildung $f \colon \mathfrak{P}(\mathbb{R}) \setminus \{\varnothing\} \to \mathbb{R}$ gibt, die jeder nicht-leeren Teilmenge von $\mathbb{R}$ ein Element aus dieser Menge zuordnet. Eine solche Abbildung könnten wir niemals explizit angeben und ihre Existenz daher auch ohne das Auswahlaxiom nicht beweisen.

Definition 2.25 (Mächtigkeit von Mengen)**.** Es seien M, N Mengen.

(i) Wir sagen, *die Mächtikeit von M ist kleiner oder gleich als der von N* (i.Z. $\boxed{\#M \leq \#N}$) genau dann, wenn eine injektive Abbildung $M \to N$ existiert.

(ii) M und N heißen *gleichmächtig* (i.Z. $\boxed{\#M = \#N}$) genau dann, wenn eine bijektive Abbildung $M \to N$ existiert.

(iii) *Die Mächtigkeit von M heißt kleiner als die von N* (i.Z. $\boxed{\#M < \#N}$) genau dann, wenn gilt $\#M \leq \#N$ und $\#M \neq \#N$.

(iv) M heißt *endlich* $:\Longleftrightarrow \exists_{n \in \mathbb{N}}\, \#n = \#M$.[3]

[3] Für $n \in \mathbb{N}$ gilt $n = \{0, \ldots, n-1\}$, also $\#n = \#\{1, \ldots, n\} = n$.

(v) M heißt *unendlich* $:\Longleftrightarrow \neg(M \text{ endlich})$.

(vi) M heißt *höchstens abzählbar* $:\Longleftrightarrow \#M \leq \#\mathbb{N}$.

(vi) M heißt *abzählbar* $:\Longleftrightarrow \#M = \#\mathbb{N}$.

(vii) M heißt *überabzählbar* $:\Longleftrightarrow \#M > \#\mathbb{N}$.

Satz 2.26 (Dirichletscher Schubfächersatz)**.** *Für alle $n, k \in \mathbb{N}$ gilt*

$$\#\{1,\dots,n\} \leq \#\{1,\dots,k\} \Longleftrightarrow n \leq k.$$

„$\Leftarrow$“ Ist $n \leq k$, so ist die Inklusion

$$\{1,\dots,n\} \hookrightarrow \{1,\dots,k\}$$

eine injektive Abbildung.

„$\Rightarrow$“ Wir zeigen für jedes $n \in \mathbb{N}$

$$\underbrace{\forall_{k\in\mathbb{N}}\ (\#\{1,\dots,n\} \leq \#\{1,\dots,k\} \Longrightarrow n \leq k)}_{\Longleftrightarrow :P(n)}.$$

$n = 0$ ist trivial.

$n \mapsto n+1$: Sei also $n \in \mathbb{N}$ und gelte $P(n)$. Wir wollen zeigen, daß auch $P(n+1)$ gilt. Gegeben seien daher $k \in \mathbb{N}$ und eine injektive Abbildung

$$f\colon \{1,\dots,n+1\} \longrightarrow \{1,\dots,k\}.$$

Wegen $1 \in \{1,\dots,n+1\}$ gilt

$$\varnothing \neq f(\{1,\dots,n+1\}) \subset \{1,\dots,k\},$$

also $\{1,\dots,k\} \neq \varnothing$ bzw. $k \in \mathbb{N}_+$.

Wir definieren eine Abbildung $\sigma\colon \{1,\dots,k\} \to \{1,\dots,k\}$ durch

$$\sigma(i) := \begin{cases} i, & i \notin \{k, f(n+1)\}, \\ k, & i = f(n+1), \\ f(n+1), & i = k. \end{cases}$$

Dann gilt $\sigma \circ \sigma = \mathrm{id}_{\{1,\dots,k\}}$, womit σ nach Satz 2.24 (iv), (v) eine Bijektion ist. Aus Satz 2.24 (i) ergibt sich die Injektivität von

$$\tilde{f} := \sigma \circ f\colon \{1,\dots,n+1\} \longrightarrow \{1,\dots,k\},$$

welche nach dem Vorgenannten die Injektivität von

$$g := \tilde{f}|_{\{1,\dots,n\}}\colon \{1,\dots,n\} \longrightarrow \{1,\dots,k-1\}$$

impliziert, wobei wegen $k \in \mathbb{N}_+$ gilt: $k-1 \in \mathbb{N}$. Aus der Gültigkeit von $P(n)$ folgt $n \leq k-1$, d.h. $n+1 \leq k$, womit auch $P(n+1)$ gezeigt ist. □

Korollar 2.27. *Ist M eine endliche Menge, so existiert genau ein $n \in \mathbb{N}$ mit $\#\{1,\dots,n\} = \#M$.* □

Definition 2.28. Ist M eine endliche Menge mit $\#M = \#n$, wobei $n \in \mathbb{N}$ sei, so setzen wir

$$\boxed{\#M} := n$$

und nennen M eine *n-elementige Menge*.

Satz 2.29. *Seien M, N Mengen.*
Dann gilt:

(i) Ist M endlich und N eine Teilmenge von M, so sind auch N und $M \setminus N$ endlich mit

$$\#M = \#N + \#(M \setminus N).$$

(ii) Sind M und N endlich, so sind auch $M \cup N$ und $M \cap N$ endlich mit

$$\#(M \cup N) = \#M + \#N - \#(M \cap N).$$

Beweis. Zu (i): Wir zeigen die Aussage zunächst in den Fällen

$$N = \varnothing, \tag{20}$$
$$N = \{x\}. \tag{21}$$

[Im Falle (20) ist nichts zu zeigen, da dann $M \setminus N = M$ und $\#N = 0$ gilt.
Zu (21): Sei $\{x\} = N \subset M$. Dann gilt $M \neq \varnothing$, also existiert $m \in \mathbb{N}_+$ derart, daß $\#M = m$ gilt. Seien dann $f\{1,\dots,m\} \to M$ eine bijektive Abbildung und $k \in \{1,\dots,m\}$ das eindeutig bestimmte Element mit $f(k) = x$. Definiere

$$\sigma\colon \{1,\dots,m\} \longrightarrow \{1,\dots,m\}$$

via

$$\forall_{i \in \{1,\dots,m\}}\, \sigma(i) := \begin{cases} i, & i \notin \{k,n\}, \\ m, & i = k, \\ k, & i = m. \end{cases}$$

Aus $\sigma \circ \sigma = \mathrm{id}$ sowie Satz 2.24 (iv), (v) folgt die Bijektivität von σ und daher mittels Satz 2.24 (iii) auch die von

$$\tilde{f} := f \circ \sigma\colon \{1,\dots,m\} \longrightarrow M.$$

Wegen $\tilde{f}(m) = f(\sigma(m)) = f(k) = x$ wird durch

$$\forall_{i \in \{1,\dots,m-1\}}\, g(i) := \tilde{f}(i)$$

offenbar eine bijektive Abbildung $g\colon \{1,\dots,m-1\} \to M \setminus \{x\} = M \setminus N$ definiert, d.h. $M \setminus N$ ist endlich und $\#(M \setminus N) = m - 1 = \#M - \#N$.]

Nun beweisen wir (i) durch vollständige Induktion nach $m := \#M \in \mathbb{N}$:

$m = 0$ ist klar, da dann $M = \varnothing$, $N = \varnothing$ und $M \setminus N = \varnothing$ gilt.

$m \mapsto m+1$: Seien $m \in \mathbb{N}$ und gelte die Behauptung für m. Seien ferner M eine $(m+1)$-elementige Menge und $N \subset M$. Ist $N = \varnothing$, so ist die Behauptung nach (20) bereits gezeigt. Daher können wir annehmen, daß $x \in N \subset M$ existiert.

Nach (21) ist $\widetilde{M} := M \setminus \{x\}$ eine m-elementige Menge, und offenbar ist durch $\widetilde{N} := N \setminus \{x\}$ eine Teilmenge von $\widetilde{M}$ gegeben. Daher folgt aus der Gültigkeit der Behauptung für m die Endlichkeit von $\widetilde{N}$ und $\widetilde{M} \setminus \widetilde{N}$.

Sind $\tilde{n} := \#N$ und $f\colon \{1,\dots,\tilde{n}\} \to \widetilde{N}$ eine bijektive Abbildung, so ist offenbar

$$g\colon \{1,\dots,\tilde{n}+1\} \longrightarrow N, \quad i \longmapsto \begin{cases} f(i), & i \neq \tilde{n}+1, \\ x, & i = \tilde{n}+1, \end{cases}$$

ebenfalls eine solche, d.h. N ist endlich mit $\#N = \#\widetilde{N} + 1$.

Nun gilt nach Induktionsvoraussetzung $\#\widetilde{M} = \#\widetilde{N} + \#(\widetilde{M} \setminus \widetilde{N})$ und aus $\#M = m+1 = \#\widetilde{M}+1$, $\#N = \#\widetilde{N}+1$ sowie $M \setminus N = \widetilde{M} \setminus \widetilde{N}$ folgt die Behauptung für $m+1$.

Zu (ii): Beweis als Übung. □

Satz 2.30. *Sei M eine endliche Menge.*
Dann ist $\mathfrak{P}(M)$ endlich und $\#\mathfrak{P}(M) = 2^{\#M}$.

Beweis. Vollständige Induktion nach $m := \#M \in \mathbb{N}$:

$m = 0$ ist wegen $\mathfrak{P}(\varnothing) = \{\varnothing\}$ klar.

$m \mapsto m+1$: Sei eine $(m+1)$-elementige Menge Menge M gegeben. Wegen $m+1 \in \mathbb{N}_+$ existiert $x \in M$ und nach Satz 2.29 ist $M \setminus \{x\}$ eine m-elementige Menge. Daher gilt nach Induktionsvoraussetzung

$$\#\mathfrak{P}(M \setminus \{x\}) = 2^m$$

und somit auch

$$\#\{A \cup \{x\} \mid A \in \mathfrak{P}(M \setminus \{x\})\} = 2^m.$$

Wir zeigen

$$\mathfrak{P}(M) = \mathfrak{P}(M \setminus \{x\}) \cup \{A \cup \{x\} \mid A \in \mathfrak{P}(M \setminus \{x\})\}, \tag{22}$$

also folgt aus Satz 2.29

$$\#\mathfrak{P}(M) = 2^m + 2^m = 2^{m+1}.$$

Zu (22): Für jede Menge X gilt

$$\begin{aligned} X \in \mathfrak{P}(M) &\iff X \subset M \setminus \{x\} \vee (X \subset M \wedge X \not\subset M \setminus \{x\}) \\ &\iff X \in \mathfrak{P}(M \setminus \{x\}) \vee (\exists_{A \subset M \setminus \{x\}}\, X = A \cup \{x\}) \\ &\iff X \in \text{r.S.} \end{aligned}$$

□

Satz 2.31. *Es seien M, N nicht-leere Mengen.*
Dann existiert genau dann eine injektive Abbildung $M \to N$, wenn eine surjektive Abbildung $N \to M$ existiert.

Beweis. „⇒“ Sei $f\colon M \to N$ eine Injektion. Gesucht ist eine surjektive Abbildung $g\colon N \to M$. Wir betrachten die durch f natürlich gegebene Abbildung $\tilde{f}\colon M \to f(M)$. Dann ist $\tilde{f}$ bijektiv und besitzt eine bijektive Umkehrabbildung $\tilde{g}\colon f(M) \to M$. Wähle nun $x_0 \in M$, beachte $M \neq \varnothing$, und setze $\tilde{g}$ außerhalb von $f(M)$ durch den Wert x_0 zu einer Abbildung $g\colon N \to M$ fort. Dann ist mit $\tilde{g}$ auch g surjektiv.

„⇐“ Gegeben sei nun eine Surjektion $g\colon N \to M$. Wir müssen eine Injektion $f\colon M \to N$ finden. Die Idee ist, daß f ein Element $x \in M$ auf ein Element von $\overline{g}^1(\{x\})$ abbilden soll, denn dann gilt $g(f(x)) = x$ für alle $x \in M$, d.h. nach Satz 2.24 (v), daß f injektiv ist.

Seien $I := M$ und $N_x := \overline{g}^1(\{x\}) \subset N$ für jedes $x \in I$. Da $g\colon N \to M \neq \varnothing$ surjektiv ist, gilt für alle $x \in I = M$: $N_x \neq \varnothing$. Nach dem Auswahlaxiom gibt es daher eine Abbildung $f\colon I \to N$ mit $\forall_{x \in I=M}\, f(x) \in N_x$. □

Satz 2.32 (Äquivalenzsatz von Bernstein)**.** *Seien M, N Mengen.*

Existierten Injektionen $f\colon M \to N$ sowie $g\colon N \to M$, so existiert auch eine Bijektion $h\colon M \to N$, d.h. genau

$$(\#M \leq \#N \wedge \#N \leq \#M) \Longrightarrow \#M = \#N.$$

Wir bereiten den Beweis des Satzes durch das folgende Lemma vor:

Lemma 2.33. *Seien M, N, M_1 Mengen mit $M_1 \subset N \subset M$ und $\#M_1 = \#M$.*
Dann gilt $\#M = \#N$.

Beweis. Nach Voraussetzung existiert eine bijektive Abbildung $f\colon M \to M_1$. Wir definieren

$$M_0 := M,\ \forall_{n \in \mathbb{N}}\, M_{n+1} := f(M_n),\ N_0 := N \text{ und } \forall_{n \in \mathbb{N}}\, N_{n+1} := f(N_n). \tag{23}$$

Dann gilt

$$\forall_{n \in \mathbb{N}}\, M_{n+1} \subset N_n \subset M_n. \tag{24}$$

[Beweis von (24) durch vollständige Induktion:
$n = 0$ gilt nach Voraussetzung.
$n \mapsto n+1$: Sei $n \in \mathbb{N}$ und gelte (24) für n, d.h. $M_{n+1} \subset N_n \subset M_n$. Dann folgt

$$\underbrace{f(M_{n+1})}_{=M_{n+2}} \subset \underbrace{f(N_n)}_{=N_{n+1}} \subset \underbrace{f(M_n)}_{=M_{n+1}},$$

also gilt (24) für $n+1$.]

Wir setzen

$$\forall_{n \in \mathbb{N}}\, L_n := M_n \setminus N_n, \tag{25}$$

$$L := \bigcup_{n \in \mathbb{N}}^{\cdot} L_n \tag{26}$$

[Beachte, daß die Vereinigung in (26) disjunkt ist, da für $k, n \in \mathbb{N}$ mit $n < k$ gilt $L_k \overset{(25)}{\subset} M_k$ und $L_n \overset{(25)}{\subset} M \setminus \underbrace{N_n}_{\overset{(24)}{\supset} M_{n+1} \overset{(24)}{\supset} M_k} \subset M \setminus M_k$.]

Da f injektiv ist, folgt aus (25)

$$\forall_{n\in\mathbb{N}}\, f(L_n) \overset{(25)}{=} f(M_n \setminus N_n) = f(M_n) \setminus f(N_n) = M_{n+1} \setminus N_{n+1} \overset{(25)}{=} L_{n+1} \tag{27}$$

und aus (26) somit

$$f(L) = f(\dot{\bigcup_{n\in\mathbb{N}}} L_n) = \dot{\bigcup_{n\in\mathbb{N}}} \underbrace{f(L_n)}_{=L_{n+1}} = L \setminus L_0. \tag{28}$$

Wegen (27) und (28) wird durch

$$\forall_{x\in M}\, g(x) := \begin{cases} f(x) \in L \setminus L_0, & x \in L, \\ x \in M \setminus L, & x \in M \setminus L, \end{cases}$$

offenbar eine injektive Abbildung $g\colon M \to M$ mit

$$g(M) = (L \setminus L_0) \cup (M \setminus L) = M \setminus \underbrace{L_0}_{\overset{(25)}{=}\overset{(23)}{=} M\setminus N} = N$$

definiert. Daher existiert eine bijektive Abbildung $M \to N$. □

Beweis des Satzes. Seien also M, N Mengen und existierten injektive Abbildungen $f\colon M \to N$ sowie $g\colon N \to M$. Dann ist offenbar auch $g \circ f\colon M \to M$ eine injektive Abbildung, und es gilt

$$(g \circ f)(M) = g(\underbrace{f(M)}_{\subset N}) \subset g(N) \subset M.$$

Da M durch $g \circ f$ bijektiv auf $(g \circ f)(M)$ abgebildet wird, also auch eine bijektive Abbildung $(g \circ f)(M) \to M$ existiert, folgt aus Lemma 2.33, daß eine bijektive Abbildung $M \to g(N)$ existiert. Nun bildet g aber N bijektiv auf $g(N)$ ab, also folgt die Existenz einer bijektiven Abbildung $M \to N$. □

Den folgenden Satz beweisen wir in dieser Vorlesung nicht. Der Beweis würde das zum Auswahlaxiom äquivalente (hier ungenannte) *Lemma von* Zorn verwenden. Allein der Beweis der letztgenannten Äquivalenz würde den Rahmen dieser Vorlesung sprengen.

Satz 2.34. *Für alle Mengen M, N gilt $\#M \leq \#N$ oder $\#N \leq \#M$.*

Satz 2.35. *Für jede Menge M gilt $\#M < \#\mathfrak{P}(M)$.*

Beweis. Die Abbildung

$$M \longrightarrow \mathfrak{P}(M), \quad x \longmapsto \{x\},$$

ist offenbar injektiv. Wir müssen daher zeigen, daß keine Bijektion $M \to \mathfrak{P}(M)$ existiert. Wir beweisen sogar, daß keine Surjektion $M \to \mathfrak{P}(M)$ existiert.

Sei $f\colon M \to \mathfrak{P}(M)$ eine beliebige Abbildung. Dann ist $N := \{x \in M \mid x \notin f(x)\}$ eine Teilmenge von M, d.h. $N \in \mathfrak{P}(M)$.

Angenommen, es existiert $x_0 \in M$ mit $f(x_0) = N$. Dann gilt entweder $x_0 \in N$, also $x_0 \notin f(x_0) = N$ nach der Definition von N, oder es gilt $x_0 \notin N$, also $x_0 \in N$ nach der Definition von N. Daher kann kein $x_0 \in M$ mit $f(x_0) = N$ existieren, d.h. f ist nicht surjektiv. □

Satz 2.36. $\mathbb{Q}$ *ist abzählbar.*

Beweis. Der Beweis stammt von CANTOR und wird *Cantors erstes Diagonalargument* genannt. $\mathbb{N} \hookrightarrow \mathbb{Q}$ ist injektiv. Wegen des Äquivalenzsatzes von BERNSTEIN genügt es daher, eine surjektive Abbildung $\mathbb{N} \to \mathbb{Q}$ zu finden. Wir ordnen die positiven rationalen Zahlen folgendermaßen an.

$$\begin{array}{ccccccccccc}
\frac{1}{1} & \to & \frac{1}{2} & & \frac{1}{3} & \to & \frac{1}{4} & & \frac{1}{5} & \cdots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow & & \\
\frac{2}{1} & & \frac{2}{2} & & \frac{2}{3} & & \frac{2}{4} & & \frac{2}{5} & \cdots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & & & \\
\frac{3}{1} & & \frac{3}{2} & & \frac{3}{3} & & \frac{3}{4} & & \frac{3}{5} & \cdots \\
 & \swarrow & & \nearrow & & & & & & \\
\frac{4}{1} & & \frac{4}{2} & & \frac{4}{3} & & \frac{4}{4} & & \frac{4}{5} & \cdots \\
\downarrow & \nearrow & & & & & & & & \\
\frac{5}{1} & & \frac{5}{2} & & \frac{5}{3} & & \frac{5}{4} & & \frac{5}{5} & \cdots \\
\vdots & & \vdots & & \vdots & & \vdots & & \vdots &
\end{array}$$

Der Leser überlege, wie man nun die gesuchte Abbildung erhält. □

Satz 2.37. $\mathbb{R}$ *ist überabzählbar.*

Beweisskizze. Wir zeigen:

$$\#\mathrm{Abb}(\mathbb{N}, \{0,1\}) = \#\mathfrak{P}(\mathbb{N}), \tag{29}$$

$$\#\mathbb{R} \geq \#\mathrm{Abb}(\mathbb{N}, \{0,1\}). \tag{30}$$

Zu (29): Die Abbildung

$$\mathfrak{P}(\mathbb{N}) \longrightarrow \mathrm{Abb}(\mathbb{N}, \{0,1\}), \quad \mathrm{M} \longmapsto \chi_{\mathrm{M}},$$

wobei

$$\forall_{M \subset \mathbb{N}} \forall_{n \in \mathbb{N}} \chi_M(n) := \begin{cases} 0, & n \notin M, \\ 1, & n \in M, \end{cases}$$

ist bijektiv.

Zu (30): Wir fassen $\mathrm{Abb}(\mathbb{N}, \{0,1\})$ als die Menge der Folgen $(a_n)_{n \in \mathbb{N}}$ in $\{0,1\}$ auf und definieren eine Abbildung $f\colon \mathrm{Abb}(\mathbb{N}, \{0,1\}) \to \mathbb{R}$ durch

$$\forall_{(a_n)_{n \in \mathbb{N}}} f((a_n)_{n \in \mathbb{N}}) = 0, a_0\, a_1\, a_2 \ldots.$$

Diese Abbildung ist offenbar injektiv. □

Bemerkung (Spezielle Kontinuumshypothese)**.** Der Beweis des letzten Satzes zeigt $\#\mathbb{R} \geq \#\mathfrak{P}(\mathbb{N})$. Tatsächlich gilt

$$\#\mathbb{R} = \#\mathfrak{P}(\mathbb{N}) > \#\mathbb{N}.$$

Es ist nun interessant zu fragen, ob es eine Menge M mit

$$\#\mathbb{R} > \#M > \#\mathbb{N}$$

gibt. Die sog. *spezielle Kontinuumshypothese* besagt, daß es keine solche Menge M gibt. ($\mathbb{R}$ heißt das *Kontinuum*.)

GÖDEL bewies 1939: Aus den Axiomen 1 - 9 läßt sich kein Widerspruch zur speziellen Kontinuumshypothese ableiten.

COHEN bewies 1963: Aus den Axiomen 1 - 9 läßt sich die spezielle Kontinuumshypothese nicht ableiten.

D.h. weder Gültigkeit noch Ungültigkeit der (speziellen) Kontinuumshypothese sind beweisbar.

Man vergleiche dies mit folgender Situation: Ein Körper ist eine Menge $\mathbb{k}$ zusammen mit zwei Operationen $+\colon \mathbb{k}\times\mathbb{k}\to\mathbb{k}$ und $\cdot\colon \mathbb{k}\times\mathbb{k}\to\mathbb{k}$, die neun Axiomen genügen, u.a.

$$\exists!_{0\in\mathbb{k}}\forall_{a\in\mathbb{k}}\, a+0=a,$$
$$\exists!_{1\in\mathbb{k}\setminus\{0\}}\forall_{a\in\mathbb{k}}\, 1\cdot a=a.$$

Hypothese: $\forall_{a\in\mathbb{k}}\, a^2\neq -1$.

Mit den Körperaxiomen läßt sich diese Hypothese weder herleiten noch widerlegen. Die Körper $\mathbb{Q}$ und $\mathbb{R}$ genügen der Hypothese. Der hier noch zu nennende Körper $\mathbb{C}$ besitzt das Element i mit $\mathrm{i}^2=-1$.

Äquivalenzrelationen

Definition 2.38. Sei M eine Menge.

(i) Sei ferner N eine Menge. Eine *Relation von M nach N* ist per definitionem eine Teilmenge R von $M\times N$. Für $(a,b)\in R$ schreiben wir auch $\boxed{a\,R\,b}$ bzw. $\boxed{a\sim_R b}$ oder kurz $\boxed{a\sim b}$ und sagen „a steht in Relation zu b“.

(ii) Eine *Äquivalenzrelation auf M* ist per definitionem eine Relation R von M nach M mit

(Ä1) $\forall_{a\in M}\, a\,R\,a$ (*Reflexivität*),

(Ä2) $\forall_{a,b\in M}\ (a\,R\,b\Longrightarrow b\,R\,a)$ (*Symmetrie*),

(Ä3) $\forall_{a,b,c\in M}\ ((a\,R\,b\wedge b\,R\,c)\Longrightarrow a\,R\,c)$ (*Transitivität*).

Beispiel.

1.) Sei H die Menge aller Menschen. Dann wird durch

$$\forall_{x,y\in H}\, x\sim y :\Longleftrightarrow x,y \text{ haben dieselbe Augenfarbe}$$

eine Äquivalenzrelation auf H definiert.

2.) Sei G die Menge aller Geraden in $\mathbb{R}^2$. Dann wird durch

$$\forall_{g,h\in G}\, g\sim h :\Longleftrightarrow g\parallel h$$

eine Äquivalenzrelation auf G definiert.

3.) Durch

$$\forall_{A,B\in M}\, A \sim B :\Longleftrightarrow \#A = \#B$$

wird eine Äquivalenzrelation auf M definiert.

4.) Durch

$$\forall_{x,y\in\mathbb{R}}\, x \sim y :\Longleftrightarrow x \leq y$$

wird eine Relation von $\mathbb{R}$ nach $\mathbb{R}$ definiert, die keine Äquivalenzrelation auf $\mathbb{R}$ ist.

Definition 2.39. Es seien M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Dann heißt für jedes $x \in M$

$$\boxed{[x]_\sim} := \{a \in M \mid a \sim x\}$$

die *Äquivalenzklasse von x modulo $\sim$* und die Menge

$$\boxed{M/_\sim} := \{[x]_\sim \mid x \in M\} = \{N \in \mathfrak{P}(M) \mid \exists_{x\in M}\, N = [x]_\sim\}$$

der *Raum der Äquivalenzklassen bzgl. $\sim$.*

Satz 2.40. *Seien M eine Menge, $\sim$ eine Äquivalenzrelation auf M und $x, y \in M$. Dann gilt*

(i) $x \sim y \Longleftrightarrow [x]_\sim = [y]_\sim$,

(ii) $\neg(x \sim y) \Longleftrightarrow [x]_\sim \cap [y]_\sim = \varnothing$ *und*

(iii) $M = \bigcup_{a\in M} [a]_\sim$.

Beweis. (iii) ist wegen der Reflexivität von $\sim$ trivial.

Zu (i): „$\Rightarrow$“ Aus $x \sim y$ folgt mittels der Transitivität von $\sim$ für alle $a \in [x]_\sim$: $a \in [y]$. Daher gilt $[x]_\sim \subset [y]_\sim$. Analog sieht man $[y]_\sim \subset [x]_\sim$ ein.

„$\Rightarrow$“ Aus $[x]_\sim = [y]_\sim$ folgt wegen $x \in [x]_\sim = [y]_\sim$, daß gilt $x \sim y$.

Zu (ii): „$\Rightarrow$“ Gelte $\neg(x \sim y)$. Existierte $a \in [x]_\sim \cap [y]_\sim$, so folgte aus der Symmetrie von $\sim$, daß $x \sim a$ und $a \sim y$ gilt, also wegen der Transitivität von $\sim$: $x \sim y$, im Widerspruch zur Voraussetzung.

„$\Leftarrow$“ Sei $[x]_\sim \cap [y]_\sim = \varnothing$. Aus $x \sim y$ folgte $x \in [y]_\sim$, Widerspruch! □

Beispiel.

1.) Betrachtet man die Äquivalenzrelation aus Beispiel 1.) zu 2.38, so ist $H/\sim$ eineindeutig mit der Menge aller Augenfarben identifizierbar.

2.) Wir betrachten die Äquivalenzrelation aus Beispiel 2.) zu 2.38. Sind p, q zwei verschiedene Punkte in der Ebene $\mathbb{R}^2$, so existiert genau eine Gerade $g_{p,q} \in G$. Daher erhalten wir eine surjektive Abbildung

$$\mathbb{R}^2 \longrightarrow G/_\sim, \quad p \longmapsto g_{0,p},$$

die nicht injektiv ist, da Vielfache eines Punktes dieselbe Gerade ergeben. Die Einschränkung dieser Abbildung auf den oberen Halbkreis

$$S_{\geq 0} := \{(x,y) \in \mathbb{R}^2 \mid \sqrt{x^2+y^2} = 1 \wedge y \geq 0\}$$

liefert uns eine Surjektion $S_{\geq 0} \to G/_\sim$, deren Einschränkung auf

$$S_+ := \{(x,y) \in \mathbb{R}^2 \mid \sqrt{x^2+y^2} = 1 \wedge y > 0\}$$

injektiv ist. Lediglich $(-1,0),(1,0)$ werden auf dasselbe Element abgebildet.. Wir können uns $G/_\sim$ also als oberen Halbkreis vorstellen, wobei die beiden Randpunkte verklebt werden. Dies ist geometrisch ein Kreis.

3.) Wir betrachten auf $\mathbb{R}$ die Äquivalenzrelation $\sim$, die durch

$$\forall_{x,y\in\mathbb{R}}\, x \sim y :\Longleftrightarrow x - y \in \mathbb{Z}$$

gegeben ist. Es gibt eine kanonische Abbildung $\mathbb{R} \to \mathbb{R}/_\sim$, die man sich als Projektion einer Schraubenlinie im $\mathbb{R}^3$ auf einen Kreis im $\mathbb{R}^2$ vorstellen kann. Daher „ist“ $\mathbb{R}/_\sim$ ein Kreis.

Definition 2.41 (Die Menge $\mathbb{Z}$ der ganzen Zahlen)**.** Wir definieren

$$\boxed{\mathbb{N}_+} := \{n \in \mathbb{N} \mid n > 0\},$$
$$\forall_{n\in\mathbb{N}_+}\, \boxed{-n} := (0,n),$$
$$\boxed{\mathbb{N}_-} := \{-n \mid n \in \mathbb{N}_+\},$$
$$\boxed{\mathbb{Z}} := \mathbb{N} \cup \mathbb{N}_- = \{\ldots,-2,-1,0,1,2,\ldots\}.$$

(Beachte, daß die Vereinigung in der letzten Zeile disjunkt ist, da aus $k \in \mathbb{N} \cap \mathbb{N}_-$ die Existenz von $\underbrace{n \in \mathbb{N}_+}_{\Rightarrow \#k = k}$ mit $\underbrace{k = (0,n) = \{\{0\},\{0,n\}\}}_{\Rightarrow \#k = 2 \,(\text{wegen } n \neq \varnothing)}$, also $k = 2 = \{\varnothing,\{\varnothing\}\}$ und $\varnothing = \{0\} \vee \varnothing = \{0,n\}$ folgte.)

Wir haben oben und in den Übungen bereits natürliche Zahlen addiert und multipliziert, obwohl wir diese Operationen noch gar nicht eingeführt hatten. U.a. das holen wir nun nach.

Definition 2.42.

(i) Die *Addition in* $\mathbb{N}$ wird rekursiv definiert durch

$$\forall_{n\in\mathbb{N}}\, n + 0 := n,$$
$$\forall_{n,k\in\mathbb{N}}\, n + (k+1) := (n+k) + 1\,(= S(n+k)).$$

Die *Multiplikation in* $\mathbb{N}$ wird rekursiv definiert durch

$$\forall_{n\in\mathbb{N}}\, n \cdot 0 := 0,$$
$$\forall_{n,k\in\mathbb{N}}\, n \cdot (k+1) := (n \cdot k) + n.$$

(ii) Sind $m, n \in \mathbb{N}$ mit $m \leq n$ (d.h. per definitionem $m \subset n$), so existiert genau ein $k \in \mathbb{N}$ mit $m + k = n$. (Dies beweist man durch vollständige Induktion.) Die *Differenz von m und n* ist dann per definitionem gleich k, und man schreibt $m - n := k$ bzw. in Übereinstimmung mit Obigem $-k$, falls $m = 0$.

(iii) Für $k \in \mathbb{Z}$ definieren wir den *Betrag von k* durch

$$|k| := \begin{cases} k, & k \in \mathbb{N}, \\ n, & k = (0, n) \in \mathbb{N}_-. \end{cases}$$

(iv) Die *Addition in $\mathbb{Z}$* ist gegeben durch

$$\forall_{k,l \in \mathbb{Z}}\, k + l := \begin{cases} k + l, & k, l \geq 0, \\ -(|k| + |l|), & k, l < 0, \\ k - |l|, & k \geq 0 \wedge l < 0 \wedge k \geq |l|, \\ -(|k| - |l|), & k \geq 0 \wedge l < 0 \wedge l > k, \\ l + k, & k < 0 \wedge l \geq 0. \end{cases}$$

Die *Subtraktion in $\mathbb{Z}$* ist gegeben durch

$$\forall_{k,l \in \mathbb{Z}}\, k - l := k + (-l).$$

Die *Multiplikation in $\mathbb{Z}$* ist gegeben durch

$$\forall_{k,l \in \mathbb{Z}}\, k \cdot l := \begin{cases} |k| \cdot |l|, & k, l \geq 0 \vee k, l < 0, \\ -|k| \cdot |l|, & \text{sonst.} \end{cases}$$

Definition 2.43 (Der Menge $\mathbb{Q}$ der rationalen Zahlen)**.** Wir definieren eine Äquivalenzrelation $\sim$ auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ wie folgt

$$\forall_{(p,q),(r,s) \in Z \times (\mathbb{Z} \setminus \{0\})}\, (p, q) \sim (q, r) :\Longleftrightarrow p \cdot s = q \cdot r.$$

Die *Menge* $\boxed{\mathbb{Q}}$ *der rationalen Zahlen* ist als $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/_\sim$ definiert.

Wir schreiben $\boxed{\frac{p}{q}}$ für $[(p, q)]_\sim \in \mathbb{Q}$.

$\mathbb{Z} \to \mathbb{Q}$, $k \mapsto \frac{k}{1}$, ist eine injektive Abbildung. Daher können wir $\mathbb{Z}$ als Teilmenge von $\mathbb{Q}$ auffassen.

Schließlich definieren wir für $\frac{p}{q}, \frac{r}{s} \in \mathbb{Q}$

$$\frac{p}{q} + \frac{r}{s} := \frac{p\,s + r\,q}{q\,s} \in \mathbb{Q},$$
$$\frac{p}{q} - \frac{r}{s} := \frac{p}{q} + \frac{-r}{s} \in \mathbb{Q},$$
$$\frac{p}{q} \cdot \frac{r}{s} := \frac{p\,r}{q\,s} \in \mathbb{Q}$$

und, falls zusätzlich $r \neq 0$ gilt,

$$\frac{\frac{p}{q}}{\frac{r}{s}} := \frac{p}{q} \cdot \frac{s}{r}.$$

Die *reellen Zahlen* kann man nun als „Vervollständigung“ der rationalen Zahlen konstruieren. Dies können wir aus zeitlichen Gründen jedoch hier nicht vorführen. Es sei daher auf [4] verwiesen.

3 Geometrie

Grundlagen

In diesem Kapitel sei stets $n \in \mathbb{N}_+$. Wir betrachten $\boxed{\mathbb{R}^n}$ als die Menge aller *n-Tupel* $(x_1, \ldots, x_n)$, wobei $\forall_{i \in \{1,\ldots,n\}} x_i \in \mathbb{R}$ gelte, zusammen mit der natürlich gegebenen Addition und skalaren Multiplikation, d.h.

$$\forall_{(x_1,\ldots,x_n),(y_1,\ldots,y_n)\in\mathbb{R}^n} (x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n),$$
$$\forall_{\alpha\in\mathbb{R}} \forall_{(x_1,\ldots,x_n)\in\mathbb{R}^n} \alpha\,(x_1, \ldots, x_n) = (\alpha\, x_1, \ldots, \alpha\, x_n).$$

Die formale Definition des $\mathbb{R}^n$ als Menge erhält man in Verallgemeinerung von Definition 2.20. $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{R}^n$ heißen *gleich* (i. Z. $\boxed{x = y}$) genau dann, wenn für alle $i \in \{1, \ldots, n\}$ gilt $x_i = y_i$.

Definition 3.1 ((Euklidische) Norm und (euklidischer) Abstand, Bälle)**.**

(i) Für alle $x, y \in \mathbb{R}^n$ heißen $\boxed{\|x\|} := \sqrt{{x_1}^2 + \ldots + {x_n}^2}$ die *(euklidische) Norm von* x sowie $\boxed{d(x,y)} := \|x - y\|$ der *(euklidische) Abstand von* x *und* y.

Bemerkung. Für alle $x, y, z \in \mathbb{R}^n$ und $\alpha \in \mathbb{R}$ gilt

$$(x \neq 0 \Longleftrightarrow \|x\| > 0), \quad \|\alpha\, x\| = |\alpha|\, \|x\|, \quad \|x + y\| \leq \|x\| + \|y\|.$$

(ii) Seien $p \in \mathbb{R}^n$ und $r \in \mathbb{R}$ mit $r > 0$. Dann heißen

$$\boxed{B_r(p)} := \{x \in \mathbb{R}^n \mid \|x - p\| < r\}$$

bzw.

$$\boxed{\overline{B_r(x)}} := \{x \in \mathbb{R}^n \mid \|x - p\| \leq r\}$$

offener bzw. *abgeschlossener Ball vom Radius* r *mit Mittelpunkt* p *in* $\mathbb{R}^n$.

Definition 3.2 (Offene und abgeschlossene Teilmengen von $\mathbb{R}^n$ sowie innere Punkte und Randpunkte einer Teilmenge von $\mathbb{R}^n$)**.** Sei M eine Teilmenge von $\mathbb{R}^n$.

(i) $x \in M$ heißt genau dann *innerer Punkt von* M, wenn $\varepsilon \in \mathbb{R}_+$ mit $B_\varepsilon(x) \subset M$ existiert. Die Menge der inneren Punkte von M bezeichnen wir mit $\boxed{M^\circ}$.

(ii) M heißt genau dann *offen in* $\mathbb{R}^n$, wenn jedes Element von M innerer Punkt von M ist.

(iii) $x \in M$ heißt genau dann *Randpunkt von* M, wenn $B_r(x)$ für jedes $r \in \mathbb{R}_+$ sowohl Elemente von M als auch von $\mathbb{R}^n \setminus M$ enthält. Die Menge aller Randpunkte von M bezeichnen wir mit $\boxed{\partial M}$.

(iv) M heißt genau dann *abgeschlossen*, wenn $\partial M \subset M$ gilt.

(v) Der *Abschluß von* M ist definiert als $\boxed{\overline{M}} := M \cup \partial M$.

Beispiel.

1.) Seien $p \in \mathbb{R}^n$ und $r \in \mathbb{R}_+$. Dann ist $\overline{B_r(p)}$ abgeschlossen, und es gilt

$$\left(\overline{B_r(p)}\right)^\circ = B_r(p)$$

sowie

$$\partial\overline{B_r(p)} = \overline{B_r(p)} \setminus B_r(p) = \{x \in \mathbb{R}^n \mid \|x - p\| = r\}.$$

Des weiteren ist $B_r(p)$ offen, und es gilt

$$B_r(p)^\circ = B_r(p)$$

sowie

$$\partial B_r(p) = \overline{B_r(p)} \setminus B_r(p) = \{x \in \mathbb{R}^n \mid \|x - p\| = r\}.$$

2.) $[0,1[$ ist weder offen noch abgeschlossen, $\partial[0,1[= \{0,1\}$, $[0,1[^\circ =]0,1[$.

3.) $\{\frac{1}{k} \mid k \in \mathbb{N}\}$ ist weder offen noch abgeschlossen und besitzt die Elemente von $\{\frac{1}{k} \mid k \in \mathbb{N}\} \cup \{0\}$ als Randpunkte sowie keine inneren Punkte.

Definition 3.3 (Beschränkte Teilmengen von $\mathbb{R}^n$)**.** Eine Teilmenge M von $\mathbb{R}^n$ heißt genau daan *beschränkt*, wenn $p \in \mathbb{R}^n$ und $r \in \mathbb{R}_+$ mit $M \subset B_r(p)$ existieren.

Beispiel.

1.) $\{\frac{1}{n} \mid n \in \mathbb{N}\}$ ist eine beschränkte Teilmenge von $\mathbb{R}$.

2.) $B_r(p)$ ist für jedes $p \in \mathbb{R}^n$ und jedes $r \in \mathbb{R}_+$ eine beschränkte Teilmenge von $\mathbb{R}^n$.

3.) $\mathbb{N}$ ist eine unbeschränkte Teilmenge von $\mathbb{R}$.

Definition 3.4 (Konvexität, Verbindungsstrecke)**.** Eine Teilmeneg C von $\mathbb{R}^n$ heißt *konvex* genau dann, wenn für alle $x, y \in C$ die *Verbindungssterecke von x mit y*

$$\boxed{[x,y]} := \{\lambda x + \mu y \mid \lambda, \mu \in \mathbb{R}_+ \cup \{0\} \wedge \lambda + \mu = 1\}$$

in C enthalten ist.

Beispiel.

1.) Aus den Eigenschaften der Norm folgt sofort, daß $B_r(x)$ für jedes $x \in \mathbb{R}^n$ sowie $r \in \mathbb{R}_+$ konvex ist.

2.) Ein Volldreieck, ein Vollquadrat und die Oberfläche eines Stopschildes sind konvexe Teilmengen von $\mathbb{R}^2$.

3.) Eine Vollkugel und ein Vollquader sind konvexe Teilmengen von $\mathbb{R}^3$.

4.) Ein Volltorus ist keine konvexe Teilmenge von $\mathbb{R}^3$.

Konvexe Polyeder

Wir geben zunächst eine anschauliche Definition.

Definition 3.5 (Polygon, konvexes Polyeder)**.**

(i) Ein *Polygon* ist eine nicht-leere Teilmenge einer Ebene des $\mathbb{R}^3$, deren Rand aus endlich vielen Strecken[4] besteht, derart, daß sich je zwei verschiedene solcher Strecken höchstens in einem gemeinsamen Randpunkt schneiden.

(ii) $M \subset \mathbb{R}^3$ heißt *konvexes Polyeder* genau dann, wenn M eine nicht-leere abgeschlossene beschränkte konvexe Menge ist, die so von Randteilen von Polygonen berandet ist – den sog. *Flächen von M* –, daß je zwei verschiedene Flächen von M höchstens eine der berandenden Strecken – d.i. per definitionem eine *Kante von M* – oder einen Randpunkt der Kanten von M – d.i. per definitionem eine *Ecke von M* – als Schnittmenge besitzen.

Beispiel. Ein Volldreieck und ein Vollrechteck sind konvexe Polygone. Eine Vollpyramide und ein Vollquader sind konvexe Polyeder. $[0,3]^3 \setminus [1,2]^3$ ist kein konvexes Polyeder, denn $[0,3]^3 \setminus [1,2]^3$ ist nicht konvex.

Um die letzte Definition etwas handfester zu geben, benötigen wir den Begriff der *konvexen Hülle*.

Definition 3.6 (Konvexe Hülle)**.** Seien $k \in \mathbb{N}_+$ und $p_1, \ldots, p_k \in \mathbb{R}^n$. Die *konvexe Hülle von $p_1, \ldots, p_k$* ist definiert als

$$\boxed{\mathrm{Konv}(p_1, \ldots, p_k)} := \left\{ \sum_{i=1}^{k} \lambda_i p_i \mid \forall_{i \in \{1,\ldots,k\}} \lambda_i \in \mathbb{R}_+ \cup \{0\} \wedge \sum_{i=1}^{k} \lambda_i = 1 \right\}.$$

Bemerkung. Sind $\lambda_1, \ldots, \lambda_k, \mu_1, \ldots, \mu_k \in \mathbb{R}_+ \cup \{0\}$ mit $\sum_{i=1}^{k} \lambda_i = \sum_{i=1}^{k} \mu_i = 1$, so gilt für alle $\lambda, \mu \in \mathbb{R}_+ \cup \{0\}$ mit $\lambda + \mu = 1$

$$\sum_{i=1}^{k} (\lambda \lambda_i + \mu \mu_i) = \underbrace{\lambda \sum_{i=1}^{k} \lambda_i + \mu \sum_{i=1}^{k} \mu_i}_{\in \mathbb{R}_+ \cup \{0\}} = 1,$$

$$\lambda \sum_{i=1}^{k} \lambda_i p_i + \mu \sum_{i=1}^{k} \mu_i p_i = \sum_{i=1}^{k} (\lambda \lambda_i + \mu \mu_i) p_i,$$

also ist $\mathrm{Konv}(p_1, \ldots, p_k)$ konvex.

Beispiel.

1.) Für $p, q \in \mathbb{R}^n$ gilt $\mathrm{Konv}(p, q) = [p, q]$.

2.) Sind p_1, p_2, p_3 paarweise verschiedene Elemente von $\mathbb{R}^3$, die nicht auf einer Geraden des $\mathbb{R}^3$ liegen, so ist $\mathrm{Konv}(p_1, p_2, p_3)$ das eindeutig bestimmte Volldreieck mit Ecken p_1, p_2, p_3.

3.) Für alle $q \in \mathrm{Konv}(p_1, \ldots, p_k)$ gilt $\mathrm{Konv}(p_1, \ldots, p_k, q) = \mathrm{Konv}(p_1, \ldots, p_k)$.

[4] Eine *Strecke* ist per definitionem eine Menge $[p, q]$ mit $p, q \in \mathbb{R}^3$ und $p \neq q$.

Satz 3.7. *Seien $k \in \mathbb{N}_+$ und $p_1, \ldots, p_k \in \mathbb{R}^n$.*
Dann ist $\mathrm{Konv}(p_1, \ldots, p_k)$ *die kleinste konvexe Menge, die $p_1, \ldots, p_k$ enthält.*

Beweis. Die Konvexität von $\mathrm{Konv}(p_1, \ldots, p_k)$ und

$$\forall_{i \in \{1,\ldots,k\}} p_i \in \mathrm{Konv}(p_1, \ldots, p_k)$$

ist bereits klar. Wir beweisen durch vollständige Induktion nach $k \in \mathbb{N}_+$, daß $\mathrm{Konv}(p_1, \ldots, p_k)$ Teilmenge jeder konvexen Menge, die $p_1, \ldots, p_k$ enthält, ist.

$k = 1$ ist trivial.

$k \mapsto k+1$: Seien $k \in \mathbb{N}_+$, $p_1, \ldots, p_{k+1} \in \mathbb{R}^n$ und C eine konvexe Teilmenge von $\mathbb{R}^n$ mit $p_1, \ldots, p_{k+1} \in C$. Nach Induktionsvoraussetzung gilt

$$\mathrm{Konv}(p_1, \ldots, p_k) \subset C. \tag{31}$$

Ferner seien $\lambda_1, \ldots, \lambda_{k+1} \in \mathbb{R}_+ \cup \{0\}$ mit $\sum_{i=1}^{k+1} \lambda_i = 1$ und

$$p := \sum_{i=1}^{k+1} \lambda_i p_i.$$

Im Falle $\lambda_{k+1} = 1$ gilt $p = p_{k+1} \in C$. Wir können daher ohne Einschränkung $\lambda_{k+1} \in [0, 1[$ annehmen. Wegen

$$\sum_{i=1}^{k} \frac{\lambda_i}{1 - \lambda_{k+1}} = \frac{1 - \lambda_{k+1}}{1 - \lambda_{k+1}} = 1$$

folgt dann

$$q := \sum_{i=1}^{k} \frac{\lambda_i}{1 - \lambda_{k+1}} p_i \in \mathrm{Konv}(p_1, \ldots, p_k) \overset{(31)}{\subset} C,$$

also aus der Konvexität von C

$$[q, p_{k+1}] \subset C.$$

Hieraus ergibt sich

$$p = (1 - \lambda_{k+1})\, q + \lambda_{k+1} p_{k+1} \in C,$$

womit der Satz bewiesen ist. □

Der letzte Satz ermöglicht es uns, einen konvexen Polyeder im $\mathbb{R}^3$ konkret als konvexe Hülle seiner Ecken zu beschreiben.

Satz 3.8. *Es seien $M \subset \mathbb{R}^3$ ein konvexes Polyeder, $p_1, \ldots, p_k \in \mathbb{R}^3$ derart, daß $\{p_1, \ldots, p_k\} \subset M$ die Menge der Ecken von M darstellt.*
Dann gilt $M = \mathrm{Konv}(p_1, \ldots, p_k)$.

Beweisskizze. Wegen des letzten Satzes genügt es zu zeigen, daß gilt

$$M \subset \mathrm{Konv}(p_1, \ldots, p_k).$$

Wir zerlegen das Polyeder in Komponenten und zeigen, daß diese sämtlich in $\mathrm{Konv}(p_1, \ldots, p_k)$ enthalten sind.

Sei $p_\alpha \in \{p_1, \ldots, p_k\}$ eine beliebige Ecke von M. Wir zerlegen die Seiten, die p_α nicht enthalten, mittels Diagonalen in Dreiecke, so daß die Ecken eines jeden solchen Dreieckes $\Delta(p_\beta, p_\gamma, p_\delta)$ in $\{p_1, \ldots, p_k\}$ enthalten sind. Wir verbinden p_α mit den Ecken von $\Delta(p_\beta, p_\gamma, p_\delta)$ und erhalten somit einen Tetraeder. Aufgrund der Konvexität von M ist das Tetraeder in M enthalten, und die Vereinigung solcher Tetraeder ist gleich M.

Es genügt zu zeigen, daß jeder der genannten Tetraeder in $\mathrm{Konv}(p_1, \ldots, p_k)$ enthalten ist. Es gilt

$$p_\beta, p_\gamma \in \{p_1, \ldots, p_k\},$$
$$[p_\beta, p_\gamma] \subset \left\{ \sum_{i=1}^{k} \lambda_i p_i \mid \sum_{i=1}^{k} \lambda_i = 1 \ \wedge \ \forall_{i \in \{1,\ldots,k\}} \lambda_i \in \mathbb{R}_+ \cup \{0\} \ \wedge \ \forall_{i \notin \{\beta,\gamma\}} \lambda_i = 0 \right\},$$
$$\Delta(p_\beta, p_\gamma, p_\delta) \subset \mathrm{Konv}(p_1, \ldots, p_k).$$

Damit enthält $\mathrm{Konv}(p_1, \ldots, p_k)$ auch das Tetraeder, welches von $p_\alpha, \ldots, p_\delta$ aufgespannt wird, da es von Strecken ausgefüllt wird, die von p_α zu Punkten des Dreieckes $\Delta(p_\beta, p_\gamma, p_\delta)$ führen. □

Der Eulersche Polyedersatz

Das Ziel dieses Abschnittes ist es, den folgenden Satz zu beweisen:

Satz 3.9 (Eulerscher Polyedersatz)**.** *Es sei $M \subset \mathbb{R}^3$ ein konvexes Polyeder. Mit E bzw. K bzw. F sei die Anzahl der Ecken bzw. Kanten bzw. Flächen von M bezeichnet.*

Dann gilt: $E - K + F = 2$.

Definition 3.10 (Netze)**.** Es sei $\mathcal{N} = (\mathcal{E}, \mathcal{K})$, wobei $\mathcal{E}$ eine nicht-leere endliche Menge von Elementen des $\mathbb{R}^3$ und $\mathcal{K}$ eine endliche Menge von Strecken seien.

Dann heißt $\mathcal{N}$ ein *Netz*, wenn die folgenden Eigenschaften erfüllt sind:

(a) Für jedes $S \in \mathcal{K}$ existieren $p, q \in \mathcal{E}$ mit $S = [p, q]$.

(b) Je zwei Elemente $S, S' \in \mathcal{K}$ schneiden sich höchstens in einem Punkt, welcher dann „Randpunkt“ sowohl von S als auch S' ist.

(c) Zu $p, q \in \mathcal{E}$ existieren $p_1, \ldots p_k \in \mathbb{R}^n$ mit

$$p = p_1 \quad \wedge \quad p_k = q \quad \wedge \quad \forall_{i \in \{1,\ldots,k-1\}} [p_i, p_{i+1}] \in \mathcal{K},$$

insbesondere gilt $\mathcal{K} \neq \varnothing$.

Die Elemente von $\mathcal{E}$ heißen *Ecken des Netzes* $\mathcal{N}$, und die Elemente von $\mathcal{K}$ heißen *Kanten des Netzes* $\mathcal{N}$. Als *Fläche des Netztes* $\mathcal{N}$, bezeichnen wir eine durch Kanten begrenzte Menge, die beschränkt ist und deren Elemente durch endlich viele Strecken „verbindbar“ sind.

Mittels der folgenden (anschaulichen) Konstruktion können wir aus jedem konvexen Polyeder P ein Netz gewinnen:

Wir wählen $p \in P^\circ$ und einen abgeschlossenen Ball B, der P enthält. Dann schneidet jede „von p ausgehende Halbgerade“ sowohl P als auch ∂B jeweils in genau einem Punkt.[5] Daher können wir jeder Ecke von P ein Element von ∂B zuordnen und somit die Ecken, Kanten und Flächen von P auf die Kugeloberfläche ∂B abbilden. Dann entfernen wir auf der Kugeloberfläche eine auf sie abgebildete Fläche ohne den Rand der abgebildeten Fläche und projizieren z.B. mittels *steographischer Projektion*[6] die verbleibende Menge auf eine Ebene. Anschaulich verbiegen wir damit die verbleibende Menge in eine solche Ebene. Auf diese Weise erhalten wir ein Netz $\mathcal{N}$, wobei die Anzahl der Ecken bzw. Kanten von $\mathcal{N}$ mit der Anzahl der Ecken bzw. Kanten von P übereinstimmt. Die Anzahl der Flächen von $\mathcal{N}$ ist gegenüber der Anzahl der Flächen von P um eins verringert.

Der Beweis von Satz 3.9 ergibt sich daher aus dem folgenden allgemeineren Resultat – beachte, daß nicht jedes Netz durch einen konvexen Polyeder induziert wird.

Satz 3.11. *Sei $\mathcal{N}$ ein Netz und bezeichne E bzw. K bzw. F die Anzahl der Ecken bzw. Kanten bzw. Flächen von $\mathcal{N}$.*

Dann gilt $E - K + F = 1$.

Beweis. Wir führen den Beweis duch vollständige Induktion nach K.

$K = 0$: Das einzige Netz, das keine Kante besitzt, besteht aus einer Ecke. Dann gilt offenbar $E - K + F = 1 - 0 + 0 = 1$.

$K \mapsto K + 1$: Seien $K \in \mathbb{N}$ und $\mathcal{N}$ ein Netz mit K Kanten. Bei Hinzunahme einer Kante zu einem Netz $\widetilde{\mathcal{N}}$, wobei $\widetilde{E}$ bzw. $\widetilde{K} = K + 1$ bzw. $\widetilde{F}$ die Anzahl der Ecken bzw. Kanten bzw. Flächen von $\widetilde{\mathcal{N}}$ bezeichne, so können zwei Fälle auftreten:

1. Fall: Zwei bereits existierende Ecken werden durch die neue Kante verbunden. Dann entsteht eine neue Fläche, d.h. $\widetilde{F} = F + 1$ und nach Induktionsvoraussetzung gilt $\widetilde{E} - \widetilde{K} + \widetilde{F} = E - (K + 1) + (F + 1) = E - K + F = 1$.

2. Fall: Die neue Kante wird an eine bereits existierende Ecke angeklebt, so daß der andere Randpunkt der neuen Kante eine neue Ecke ergibt. Folglich entsteht keine neue Fläche, und es gilt somit wegen der Induktionsvoraussetzung $\widetilde{E} - \widetilde{K} + \widetilde{F} = (E + 1) - (K + 1) + F = E - K + F = 1$. □

Platonische Körper

Definition 3.12 (Platonische Körper)**.** Sei $M \subset \mathbb{R}^3$ ein konvexes Polyeder.

[5] Sei nämlich C eine beliebige konvexe und beschränkte Menge mit $p \in C^\circ$.

Gäbe es eine „von p ausgehende Halbgerade“, die keinen Schnittpunkt mit ∂C hat, so würde C eine „unendlich lange Strecke“ enthalten, im Widerspruch zur Beschränktheit von C.

Seien nun zwei verschiedene Schnittpunkte q_1, q_2 von ∂C mit einer „von p ausgehenden Halbgerade, die zunächst q_1 und sodann q_2 trifft“ gegeben. Wegen $p \in C^\circ$existiert $\varepsilon \in \mathbb{R}_+$ mit $B_\varepsilon(p) \subset C$, und die Konvexität von C liefert, daß die Verbindungsstrecke von q_2 mit allen Punkten aus $B_\varepsilon(p)$ in C enthalten ist. Da diese Strecken einen Kegel ausfüllen, folgt $q_1 \in C^\circ$, Widerspruch!

[6] Ohne Einschränkung kann man hier die *steographische Projektion* $S^2 \setminus \{(0,0,1)\} \to \mathbb{R}^2$ *vom Nordpole aus* betrachten, wobei $S^2 = \partial B_1(0)$ sei. Jedem Element $\zeta \in S^2 \setminus \{(0,0,1)\} \subset \mathbb{R}^3$ wird das eindeutige Element von $\mathbb{R}^2 \times \{0\} \equiv \mathbb{R}^2$, welches die Gerade, die $(0,0,1)$ und ζ enthält, schneidet, zugeordnet.

M heißt *Platonischer Körper* genau dann, wenn folgende Eigenschaften erfüllt sind:

(a) Es existiert $m \in \mathbb{N}_+$ derart, daß an jeder Ecke von M dieselbe Anzahl m von Kanten zusammentrifft.

Offenbar muß dann $m \geq 3$ gelten.

(b) Es existiert $n \in \mathbb{N}$ mit $n \geq 3$ derart, daß alle Flächen von M zueinander kongruente n-Ecke sind; d.h. alle Flächen enthalten jeweils n Kanten.

Mittels des Eulerschen Polyedersatzes wollen wir nun die Platonischen Körper klassifizieren. Seien daher $M \subset \mathbb{R}^3$ ein Platonischer Körper und m, n wie in der letzten Definition gewählt. E bzw. K bzw. F bezeichne wieder die Anzahl der Ecken bzw. Kanten bzw. Flächen von M. Da jede Kante zwei Ecken enthält, gilt wegen 3.12 (a)

$$E = \frac{2}{m}K;$$

und da jede Kante zwei Flächen berandet, gilt wegen 3.12 (b)

$$F = \frac{2}{n}K.$$

Somit impliziert der Eulersche Polyedersatz

$$K = \frac{2mn}{2n - mn + 2m}. \tag{32}$$

Wegen $K > 0$, $m, n \geq 3$ ergibt sich hieraus

$$\begin{gathered} 2n - mn + 2m > 0, \\ 2n > m(n-2) \geq 3(n-2), \\ n < 6 \end{gathered}$$

und analog $m < 6$. Damit ist gezeigt: $m, n \in \{3, 4, 5\}$.

1. Fall: $m = 3$.

1.1. Fall: $n = 3$. Dann gilt $K \overset{(32)}{=} 6$, $E = \frac{2}{m}K = 4$ und $F = \frac{2}{n}K = 4$. M ist somit ein Tetraeder.

1.2. Fall: $n = 4$. Dann gilt $K \overset{(32)}{=} 12$, $E = \frac{2}{m}K = 8$ und $F = \frac{2}{n}K = 6$. M ist somit ein Würfel.

1.2. Fall: $n = 5$. Dann gilt $K \overset{(32)}{=} 30$, $E = \frac{2}{m}K = 20$ und $F = \frac{2}{n}K = 12$. M ist somit ein Dodekaeder.

2. Fall: $m = 4$. Dann gilt $0 < K \overset{(32)}{=} \frac{8n}{8-2n} = \frac{4n}{4-n}$, also $n = 3$ und $K = 12$, $E = \frac{2}{m}K = 6$ und $F = \frac{2}{n}K = 8$. M ist somit ein Oktaeder.

3.Fall: $m = 5$. Dann gilt $0 < K \overset{(32)}{=} \frac{10n}{10-3n}$, also $n = 3$ und $K = 30$, $E = \frac{2}{m}K = 12$ und $F = \frac{2}{n}K = 20$. M ist somit ein Ikosaeder.

4 Algebraische Strukturen

Gruppen

Sei G eine Menge. Eine *Verknüpfung auf G* ist per definitionem eine Abbildung

$$\circ\colon G \times G \longrightarrow G, \quad (g,h) \longmapsto g \circ h.$$

Beispiel.

1.) Die Addition $+\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist eine Verknüfung auf $\mathbb{N}$.

2.) Die Multiplikation $\cdot\colon \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ ist eine Verknüfung auf $\mathbb{N}$.

3.) Durch $\forall_{n,m \in \mathbb{N}}\, (n,m) \mapsto n - m$ ist keine Verknüfung auf $\mathbb{N}$ gegeben.

Definition 4.1 (Gruppen)**.** Eine Gruppe $(G, \circ)$ ist eine Menge G zusammen mit einer Verknüfung $\circ\colon G \times G \to G$, die die folgenden Axiome erfüllt:

(a) (Assoziativität)
Für alle $g,h,k \in G$ gilt $(g \circ h) \circ k = g \circ (h \circ k)$.

(b) Es existiert ein *neutrales Element* $\boxed{e} \in G$, d.h.

$$\forall_{g \in G}\, g \circ e = e \circ g = g.$$

(c) Es existieren *inverse Elemente*, d.h.

$$\forall_{g \in G} \exists_{h \in G}\, g \circ h = h \circ g = e.$$

Eine Gruppe $(G, \circ)$ heißt *abelsch* genau dann, wenn gilt

$$\forall_{g,h \in G}\, g \circ h = h \circ g.$$

Bemerkung.

1.) Im Falle abelscher Gruppen wird die Verknüpfung häufig mit $\boxed{+}$ bezeichnet. Im Falle nicht-abelscher Gruppen wird meistens $\boxed{\cdot}$ anstelle von $\circ$ geschrieben.

2.) Wenn keine Verwechselungen auftreten können, schreiben wir häufig kurz G für $(G, \circ)$.

Satz 4.2. *Sei $(G, \circ)$ eine Gruppe mit neutralem Element $e \in G$.*
Dann gilt:

(i) Ein neutrales Element ist eindeutig bestimmt.

(ii) Inverse Elemente sind eindeutig bestimmt.

Beweis. Zu (i): Ist e' auch neutrales Element, so gilt $e = e' \circ e = e \circ e' = e'$.
Zu (ii): Seien $g \in G$ und h, h' inverse Elemente von g, d.h.

$$g \circ h = h \circ g = e = g \circ h' = h' \circ g,$$

also gilt $h = h \circ e = h \circ (g \circ h') = (h \circ g) \circ h' = e \circ h' = h'$. □

Definiton. Sei $(G, \circ)$ eine Gruppe. Wir schreiben im folgenden $\boxed{g^{-1}}$ für das eindeutig bestimmte inverse Element von $g \in G$. Ist die Gruppe $(G, \circ)$ abelsch und die Verknüpfung mit + anstelle von $\circ$ notiert, so schreiben wir $\boxed{-g}$ anstelle von g^{-1}.

Satz 4.3 (Kürzungsregel)**.** *Sei $(G, \circ)$ eine Gruppe.*
Für alle $g, h, k \in G$ gilt

(i) $g \circ h = g \circ k \Longrightarrow h = k$,

(ii) $h \circ g = k \circ g \Longrightarrow h = k$.

Beweis. Wir zeigen (i); (ii) ergibt sich analog. Aus $g \circ h = g \circ k$ folgt ducrh Multiplikation mit g^{-1} von links: $h = k$. □

Korollar 4.4. *Seien $(G, \circ)$ eine Gruppe und $g, h \in G$.*
Dann gilt $\left(g^{-1}\right)^{-1} = g$ und $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

Beweis als Übung. □

Beispiel.

1.) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit neutralem Element 0 und zu $k \in \mathbb{Z}$ inversem Element $-k$.

2.) $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind abelsche Gruppen. $(\mathbb{N}, +)$ ist keine Gruppe.

3.) Eine einelementige Menge bildet zusammen mit der einzig möglichen Verknüpfung eine abelsche Gruppe.

4.) $(\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}, \cdot)$ und $(\mathbb{R}^* := \mathbb{R} \setminus \{0\}, \cdot)$ sind abelsche Gruppen.

5.) Die (hoffentlich) aus der Schule bekannten reellen 2×2 Matrizen bilden zusammen mit der üblichen Multiplikation eine Gruppe, die nicht abelsch ist.

Es seien $(G, \circ)$ eine Gruppe und $a \in G$. Die *Linkstraslation mit a* ist per definitionem die Abbildung

$$\boxed{L_a \colon G \longrightarrow G, \quad g \longmapsto a \circ g.}$$

Die *Rechtstraslation mit a* ist per definitionem die Abbildung

$$\boxed{R_a \colon G \longrightarrow G, \quad g \longmapsto g \circ a.}$$

Lemma 4.5. *Sei $(G, \circ)$ eine Gruppe.*
Dann sind für jedes $a \in G$ die Translationen $L_a \colon G \to G$ und $R_a \colon G \to G$ bijektiv.

Beweis. Sei $a \in G$.
Die Bijektivität von L_a und R_a bedeutet genau, daß es zu jedem $g \in G$ genau ein $h \in G$ und genau ein $k \in G$ mit

$$a \circ h = g \quad \text{sowie} \quad k \circ a = g \tag{33}$$

gibt.

Zur Existenz: $a \circ h = g$ ist gleichbedeutend mit $h = a^{-1} \circ g$ und $k \circ a = g$ mit $k = g \circ a^{-1}$.

Zur Eindeutigkeit: Seien auch $\tilde{h}, \tilde{k} \in G$ mit

$$a \circ \tilde{h} = g \quad \text{und} \quad \tilde{k} \circ a = g.$$

(33) ergibt dann zusammen mit der Kürzungsregel $h = \tilde{h} \wedge k = \tilde{k}$. □

Beispiel.

6.) Seien $(G, \circ)$ eine endliche Gruppe und $G = \{g_1, \ldots, g_n\}$. Als *Gruppentafel von G* bezeichnet man folgende Tabelle:

$\circ$	g_1	$\cdots$	g_i	$\cdots$	g_n
g_1	$g_1 \circ g_1$	$\cdots$	$g_1 \circ g_i$	$\cdots$	$g_1 \circ g_n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_j	$g_j \circ g_1$	$\cdots$	$g_j \circ g_i$	$\cdots$	$g_j \circ g_n$
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\ddots$	$\vdots$
g_n	$g_n \circ g_1$	$\cdots$	$g_n \circ g_i$	$\cdots$	$g_n \circ g_n$

Das letzte Lemma zeigt, daß sowohl jede Zeile als auch jede Spalte der Tabelle eine Permutation der Menge $\{g_1, \ldots, g_n\}$ darstellt.

Im Falle $n = 2$ muß die Gruppentafel folgende Gestalt haben:

$\circ$	e	g
e	e	g
g	g	e

Beachte, daß $g \circ g = g$ der Eindeutigkeit des neutralen Elementes widerspräche.

Im Falle $n = 3$ muß die Gruppentafel wie folgt aussehen:

$\circ$	e	g	h
e	e	g	h
g	g	h	
h	h		

Denn sowohl $g \circ g = e$ als auch $g \circ g = g$ widersprächen der Eindeutigkeit des neutralen Elementes. Die einzig mögliche Verknüpfungstafel ist daher die folgende Tabelle:

$\circ$	e	g	h
e	e	g	h
g	g	h	e
h	h	e	g

Im Falle $n = 4$ existieren mehrere Möglichkeiten, vgl. Übungen.

7.) (Zykische Gruppe der Ordnung $p \in \mathbb{N}_+$). Sei $p \in \mathbb{N}_+$. Wir definieren auf $\mathbb{Z}$ eine Äquivalenzrelation durch

$$\forall_{k,l\in\mathbb{Z}}\, k \sim l :\Longleftrightarrow p \,|\, (k-l).$$

Anstelle von $k \sim l$ schreiben wir auch $\boxed{k \equiv l\,(p)}$ und sagen „k ist kongruent zu l modulo p“. Die Menge der Äquivalenzklassen bzgl. $\sim$ bezeichnen wir mit $\boxed{\mathbb{Z}_p}$; sie besitzt p Elemente, welche wir in offensichtlicher Weise mit $\overline{0}, \ldots, \overline{p-1}$ notieren. Durch

$$\forall_{k,l\in\mathbb{Z}}\, \overline{k} + \overline{l} := \overline{k+l}$$

wird eine Verknüfung auf $\mathbb{Z}_p$ definiert, die $\mathbb{Z}_p$ zu einer abelschen Gruppe macht.

[Zur sog. „Wohldefiniertheit“ der Verknüpfung seien $k, l, k', l' \in \mathbb{Z}$ mit $\overline{k} = \overline{k'}$ und $\overline{l} = \overline{l'}$. Dann existieren $\tilde{k}, \tilde{l} \in \mathbb{Z}$ mit $k - k' = p\tilde{k}$ und $l - l' = p\tilde{l}$. Es folgt

$$k + l = k' + p\tilde{k} + l' + p\tilde{l} = (k' + l') + p(\tilde{k} + \tilde{l}),$$

also $p \,|\, ((k+l) - (k'+l'))$.

Daß $(\mathbb{Z}_p, +)$ eine abelsche Gruppe ist, folgt aus den jeweils entsprechenden Eigenschaften von $(\mathbb{Z}, +)$.]

$\mathbb{Z}_p$ heißt „die“ *zyklische Gruppe der Ordnung p*.

Bemerkung. $\mathbb{Z}$ heißt „die“ *unendlich zyklische Gruppe*.

8.) (Symmetrische Gruppe zum Index $n \in \mathbb{N}_+$). Sei $n \in \mathbb{N}_+$. Eine *Permutation von* $\{1, \ldots, n\}$ ist per definitionem eine bijektive Abbildung

$$\sigma\colon \{1, \ldots, n\} \longrightarrow \{1, \ldots, n\},$$

die wir in offensichtlicher Weise als

$$\sigma = \begin{pmatrix} 1 & \ldots & n \\ \sigma(1) & \ldots & \sigma(n) \end{pmatrix}$$

notieren können. Die Menge der Permutationen von $\{1, \ldots, n\}$ bildet zusammen mit der Komposition von Abbildungen eine Gruppe $\boxed{S_n}$, die sog. *symmetrische Gruppe zum Index n*. Im Falle $n \in \{1, 2\}$ ist S_n abelsch.

Bemerkung. Ist M eine nicht-leere endliche Menge, so können wir gemäß 2.27 ohne Einschränkung annehmen, daß $n \in \mathbb{N}_+$ mit $M = \{1, \ldots, n\}$ existiert.

Definition 4.6 (Untergruppen)**.** Seien $(G, \circ)$ eine Gruppe mit neutralem Element e und H eine Teilmenge von G.

$(H, \circ)$ (oder kurz H) heißt *Untergruppe von* $(G, \circ)$ genau dann, wenn folgende Eigenschaften erfüllt sind:

(a) $\forall_{h,h'\in H}\, h \circ h' \in H$,

(b) $e \in H$,

(c) $\forall_{h\in H}\, h^{-1} \in H$.

Beispiel.

1.) $(\mathbb{Z},+)$ ist eine Untergruppe von $(\mathbb{Q},+)$, und $(\mathbb{Q},+)$ ist eine Untergruppe von $(\mathbb{R},+)$.

2.) Seien $n \in \mathbb{N}_+$ und $m \in \{1,\dots,n\}$. Dann bildet die Menge der Elemente von S_n, die m auf m abbilden, eine Untergruppe von S_n.

3.) Es sei $n \in \mathbb{N}$. Dann ist

$$\boxed{n\mathbb{Z}} := \{k \in \mathbb{Z} \mid \exists_{l \in \mathbb{Z}}\, k = n \cdot l\} = \{\dots, -2n, n, 0, n, 2n, \dots\}$$

eine Untergruppe von $(\mathbb{Z},+)$.

Satz 4.7. *Sei G eine Untergruppe von $(\mathbb{Z},+)$.*
Dann existiert $n \in \mathbb{N}$ mit $G = n\mathbb{Z}$.

Beweis. Ohne Beschränkung der Allgemeinheit gelte $G \neq \{0\}$. Wir setzen

$$M := G \cap \mathbb{N}_+ \subset \mathbb{N}_+ \subset \mathbb{N}.$$

Dann folgt

$$M \neq \emptyset,$$

denn für $g \in G \setminus \{0\} \subset \mathbb{Z}$ gilt im Falle $g \notin \mathbb{N}_+$: $-g \in \mathbb{N}_+$. Daß ein solches g existiert folgt aus $G \neq \{0\}$.

Wegen des Wohlordnungsprinzipes der Menge der natürlichen Zahlen 2.17 besitzt M ein kleinstes Element $n \in \mathbb{N}_+$. Wir behaupten

$$G = n\mathbb{Z}.$$

Beweis hiervon: „$\supset$“ Sei $k \in \mathbb{Z}$. Zu zeigen ist $n \cdot k \in G$. Im Falle $k > 0$ ergibt sich induktiv $n \cdot k = \underbrace{n + \dots + n}_{k \text{ Summanden}} \in G$, da G eine Untergruppe von $(\mathbb{Z},+)$ ist. Im Falle $k < 0$ folgt hieraus $-n \cdot k = n \cdot (-k) \in G$, also auch $n \cdot k \in G$. Im Falle $k = 0$ gilt $n \cdot k = 0 \in G$.

„$\subset$“ Sei $g \in G$. Ohne Einschränkung gelte $g \neq 0$. Dann liefert „Division mit Rest von g durch n“ die Existenz von $k, r \in \mathbb{Z}$ mit $g = k \cdot n + r$ und $r \in \{0,\dots,n-1\}$.[7] Wegen $g \in G$ und $n \cdot (-k) \in G$ – beachte, daß „$\supset$“ bereits bewiesen ist – ergibt sich aus der Untergruppeneigenschaft von G: $r = g - k \cdot n \in G$. Da n das kleinste Element aus M ist, folgt aus $r \in \{0,\dots,n-1\}$, daß $r = 0$ gelten muß, also $g = n \cdot k$. □

[7] Für das zu findende r muß $r = g - k \cdot n$ für ein $k \in \mathbb{Z}$, also $r \in R := \{g - k' \cdot n \mid k' \in \mathbb{Z}\} \cap \mathbb{N}$ gelten. Es folgt $R \neq \emptyset$, denn im Falle $g \geq 0$ gilt $g - 0 \cdot n \in R$, und im Falle $g < 0$ gilt $g - g \cdot n = g \cdot (1-n) \in R$, da das Produkt zweier negativer Zahlen negativ ist. Daher liefert 2.17, die Existenz eines minimalen Elementes $r \in R$, d.h. es existiert $k \in \mathbb{Z}$ mit $r = g - k \cdot n$, und aus $r \geq n$ folgte $0 \leq r - n = g - k \cdot n - n = g - (k+1) \cdot n \in R$, im Widerspruch zur Minimalität von $r \in R$.

Homomorphismen

Wir haben Mengen mit einer zusätzlichen Struktur, der Verknüfung, studiert und wollen nun Abbildungen betrachten, die jene respektieren.

Definition 4.8 ((Gruppen)-Homomorphismen)**.** Seien $(G, \circ)$ und $(H, *)$ Gruppen.

Eine Abbildung $\varphi\colon G \to H$ heißt *(Gruppen-)Homomorphismus* genau dann, wenn für alle $g, g' \in G$ gilt $\varphi(g \circ g') = \varphi(g) * \varphi(g')$.

Beispiel.

1.) Für jedes $k \in \mathbb{Z}$ ist die Abbildung

$$\varphi_k\colon (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +), \quad l \longmapsto k \cdot l,$$

ein Homomorphismus.

2.) Die (hoffentlich) aus der Schule bekannte Abbildung

$$\exp\colon \mathbb{R} \longrightarrow \mathbb{R}^* = \mathbb{R} \setminus \{0\}, \quad x \longmapsto \mathrm{e}^x,$$

definiert einen Homomorphismus $(\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$ – beachte, daß für alle $x, y \in \mathbb{R}$ gilt $\mathrm{e}^{x+y} = \mathrm{e}^x \cdot \mathrm{e}^y$.

3.) Sei $(G, \cdot)$ eine Gruppe. Zusammen mit der Komposition $\circ$ von Abbildungen ist dann auch $\mathrm{Bij}(G) := \{f\colon G \to G \mid f \text{ bijektiv }\}$ eine Gruppe und

$$L\colon (G, \cdot) \longrightarrow (\mathrm{Bij}(G), \circ), \quad g \longmapsto L_g,$$

ein Homomorphismus.

Satz 4.9. *Es seien $(G, \circ)$ und $(H, *)$ Gruppen mit neutralen Elementen e_G und e_H sowie $\varphi : G \to H$ ein Homomorphismus.*

Dann gilt $\varphi(e_G) = e_H$ und $\forall_{g \in G}\, \varphi(g^{-1}) = \varphi(g)^{-1}$.

Beweis. 1.) Es gilt

$$e_H * \varphi(e_G) = \varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G),$$

also ergibt die Kürzungsregel $e_H = \varphi(e_G)$.

2.) Sei $g \in G$. Dann ergibt 1.)

$$e_H = \varphi(e_G) = \varphi(g \circ g^{-1}) = \varphi(g) * \varphi(g^{-1}),$$

und aus der Eindeutigkeit des neutralen Elementes folgt $\varphi(g)^{-1} = \varphi(g^{-1})$. □

Satz 4.10. *Es seien $(G, \circ)$ und $(H, *)$ Gruppen sowie $\varphi : G \to H$ ein Homomorphismus. Ferner sei H' eine Untergruppe von $(H, *)$.*

Dann ist $\overline{\varphi}^1(H')$ eine Untergruppe von $(G, \circ)$.

Beweis. Wir beweisen die Eigenschaften (a) - (c) aus Definition 4.6.

Zu (a): Seien $g, g' \in \overline{\varphi}^1(H')$. Dann gilt $\varphi(g), \varphi(g') \in H'$, also – da H' Untergruppe von $(H, *)$ –

$$\varphi(g \circ g') = \varphi(g) * \varphi(g') \in H',$$

d.h. $g \circ g' \in \overline{\varphi}^1(H')$.

Zu (b): Seien e_G bzw. e_H die neutralen Elemente von G bzw. H. Dann gilt $e_H \in H'$, also nach dem letzten Satz

$$\varphi(e_G) = e_H \in H'$$

und somit $e_G \in \overline{\varphi}^1(H')$.

Zu (c): Sei $g \in \overline{\varphi}^1(H')$. Dann gilt $\varphi(g) \in H'$, also nach dem letzten Satz – da H' Untergruppe von $(H, *)$ –

$$\varphi(g^{-1}) = \varphi(g)^{-1} \in H',$$

d.h. $g^{-1} \in \overline{\varphi}^1(H')$. □

Definition 4.11. Sei G, H Gruppen und $\varphi\colon G \to H$ ein Homomorphismus. Ferner bezeichne e_H das neutrale Element von H.

Dann heißt $\overline{\varphi}^1(\{e_H\})$ der *Kern von* φ, den wir mit $\boxed{\operatorname{Kern}\varphi}$ notieren.

Satz 4.12. *Seien* $(G, \circ)$ *und* $(H, *)$ *Gruppen sowie* $\varphi\colon G \to H$ *ein Homomorphismus.*

Dann ist $\operatorname{Kern}\varphi$ *eine Untergruppe von* $(G, \circ)$ *und* $\varphi(G)$ *eine Untergruppe von* $(H, *)$.

Beweis. Seien e_G und e_H die jeweiligen neutralen Elemente.

Die erste Aussage folgt sofort aus dem letzten Satz, da $\{e_H\}$ offenbar eine Untergruppe von $(H, *)$ ist. Zum Nachweis der zweiten Aussage beweisen wir wieder die Eigenschaften (a) - (c) aus Definition 4.6.

Zu (a): Seien $h, h' \in \varphi(G)$. Dann existieren $g, g' \in G$ mit $\varphi(g) = h$ und $\varphi(g') = h'$. Es folgt $h * h' = \varphi(g) * \varphi(g') = \varphi(g \circ g') \in \varphi(G)$.

Zu (b): Nach 4.9 gilt $e_H = \varphi(e_G) \in \varphi(G)$.

Zu (c): Sei $h \in \varphi(G)$. Dann existiert $g \in G$ mit $\varphi(g) = h$ und 4.9 ergibt $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1}) \in \varphi(G)$. □

Satz 4.13. *Seien* $(G, \circ)$ *und* $(H, *)$ *Gruppen sowie* $\varphi\colon G \to H$ *ein Homomorphismus.*

Dann ist φ *genau dann injektiv, wenn* $\operatorname{Kern}\varphi = \{e_G\}$, *wobei* e_G *das neutrale Element von* G *bezeichne, gilt.*

Beweis. Bezeichne e_H das neutrale Element von H.

„⇒“ $e_G \in \operatorname{Kern}\varphi$ ist nach dem letzten Satz klar. Angenommen es existierte $g \in G$ mit $g \neq e_G$ und $\varphi(g) = e_H$. Dann folgte aus $\varphi(g) = e_H = \varphi(e_G)$ ein Widerspruch zur Injektivität von φ.

„⇐“ Seien $g, g' \in G$ mit $\varphi(g) = \varphi(g')$. Dann gilt

$$e_H = \varphi(g) * \varphi(g)^{-1} = \varphi(g') * \varphi(g^{-1}) = \varphi(g' \circ g^{-1}),$$

also nach Voraussetzung der rechten Seite $g' \circ g^{-1} = e_G$, d.h. $g = g'$. □

Beispiel.

1.) $\exp\colon (\mathbb{R},+) \to (\mathbb{R}^*,\cdot)$ ist wegen $\forall_{x\in\mathbb{R}}\,(e^x = 1 \Leftrightarrow x = 0)$ injektiv.

2.) Für jedes $k \in \mathbb{Z} \setminus \{0\}$ ist φ_k wie in Beispiel 2.) zu 4.8 injektiv.

Satz 4.14. *Seien G, H Gruppen und $\varphi\colon G \to H$ ein bijektiver Homomorphismus, ein sog.* (Gruppen)-Isomorphismus.
Dann ist auch $\varphi^{-1}\colon H \to G$ ein (bijektiver) Homomorphismus.

Beweis als Übung. □

Definiton. Zwei Gruppen heißen *isomorph* genau dann, wenn ein Isomorphismus zwischen ihnen existiert.

Ringe und Körper

Nachdem wir Gruppen (also Mengen zusammen mit einer Verknüpfung) studiert haben, führen wir nun Mengen ein, auf denen zwei Verknüfungen gegeben sind, die in gewissem Sinne miteinander verträglich sind.

Definition 4.15 (Ringe)**.**

(i) Eine Ring $(R,+,\cdot)$ ist eine Menge R zusammen mit zwei Verknüpfungen

$$+\colon R \times R \longrightarrow R,$$

einer sog. *Addition*, und

$$\cdot\colon R \times R \longrightarrow R,$$

einer sog. *Multiplikation*, derart, daß folgende Eigenschaften erfüllt sind:

(a) $(R,+)$ ist eine abelsche Gruppe, wobei wir das neutale Element mit $\boxed{0}$ bezeichnen.

(b) $(R,\cdot)$ ist assoziativ, d.h. $\forall_{a,b,c}\, a\cdot(b\cdot c) = (a\cdot b)\cdot c$.

(c) [Distributivität]
Für alle $a,b,c \in R$ gilt

$$(a+b)\cdot c = (a\cdot c) + (b\cdot c),$$
$$c\cdot(a+b) = (c\cdot a) + (c\cdot b).$$

Wenn keine Verwechselungen auftreten können, schreiben wir auch kurz R für $(R,+,\cdot)$.

(ii) Ein Ring $(R,+,\cdot)$ heißt *unitär* oder *Ring mit Eins(-element)* genau dann, wenn $(R,\cdot)$ ein neutrales Elemnt besitzt, welches wir mit $\boxed{1}$ bezeichnen, d.h. $\forall_{a\in R}\, 1\cdot a = a\cdot 1 = a$.

(iii) Ein Ring $(R,+,\cdot)$ heißt *kommutativ* genau dann, wenn $\forall_{a,b\in\mathbb{R}}\, a\cdot b = b\cdot a$ gilt.

Wir vereinbaren, daß die Multiplikation eines Ringes stärker als die Addition bindet, d.h. es gilt die „Punkt- vor Strichrechnung“. Des weiteren schreiben wir für $a,b \in R$ anstelle von $a\cdot b$ auch ab.

Bemerkung. Sei R ein Ring. Dann folgt i.a. für $a, b, c \in R$ aus

$$a \cdot c = b \cdot c \quad \text{oder} \quad c \cdot a = c \cdot b$$

i.a. nicht $a = b$.

Satz 4.16. *Sei R ein Ring.*
Dann gilt

(i) $\forall_{a \in R}\, 0 \cdot a = a \cdot 0 = 0$,

(ii) $\forall_{a,b \in R}\, (-a) \cdot b = -(a \cdot b) = a \cdot (-b)$.

Beweis. Zu (i): Sei $a \in R$. Dann gilt

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

$0 = a \cdot 0$ ergibt sich analog.
Zu (ii): Seien $a, b \in R$. Dann gilt

$$(-a) \cdot b + a \cdot b = ((-a) + a)) \cdot b = 0 \cdot b = 0,$$

also $(-a) \cdot b = -(a \cdot b)$ und analog $a \cdot (-b) = -(a \cdot b)$. □

Bemerkung. Sei R ein unitärer Ring. Im Falle $1 = 0$ folgt aus dem letzten Satz für jedes $a \in R$

$$a = a \cdot 1 = a \cdot 0 = 0,$$

also $R = \{0\}$. Die Umkehrung gilt natürlich auch.

Beispiel.

1.) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind kommutative unitäre Ringe.

2.) $(\mathbb{N}, +, \cdot)$ ist kein Ring.

3.) Seien $M \subset \mathbb{R}$ und $R := \mathrm{Abb}(M, \mathbb{R})$. Indem wir die Addition und die Multiplikation elementweise definieren, erhalten wir eine kommutative Ringstruktur für R.

4.) Sei $\mathbb{R}[x] := \{\sum_{i=0}^{k} a_i x^i \mid k \in \mathbb{N} \wedge a_i \in \mathbb{R}\}$ die Menge der sog. *reellen Polynome in einer Variablen x*. Wir versehen $\mathbb{R}[x]$ mit einer Addition, indem wir die Summanden nach den Potenzen von x sortieren und diese „Koeffizienten“ addieren, sowie mit einer Multiplikation, die durch formale Multiplikation der Polynome erhalten wird. Dadurch wird $\mathbb{R}[x]$ zu einem kommutativen unitären Ring, „dem“ *Polynomring über $\mathbb{R}$ in einer Variablen.*

Definition 4.17 (Unterringe)**.** Seien $(R, +, \cdot)$ ein Ring und R' eine Teilmenge von R.

$(R', +, \cdot)$ (oder kurz R) heißt *Unterring von* $(R, +, \cdot)$ genau dann, wenn $(R', +)$ eine Untergruppe von $(R, +)$ ist und $a \cdot b \in R'$ für alle $a, b \in R'$ gilt.

Definition 4.18 ((Ring)-Homomorphismen)**.** Es seien $(R,+,\cdot)$ und $(S,\oplus,\odot)$ Ringe sowie $\varphi\colon R\to S$ eine Abbildung.

φ heißt ein *(Ring)-Homomorphismus* genau dann, wenn für alle $a,b\in R$ gilt: $\varphi(a+b)=\varphi(a)\oplus\varphi(b)$ und $\varphi(a\cdot b)=\varphi(a)\odot\varphi(b)$.

Beispiel.

1.) Die Inklusionen $\mathbb{Z}\hookrightarrow\mathbb{Q}$ und $\mathbb{Q}\hookrightarrow\mathbb{R}$ sind Ringhomomorphismen.

2.) Seien R,S Ringe. Dann ist die Abbildung

$$\varphi\colon R\longrightarrow S,\quad a\longmapsto 0,$$

ein Ringhomomorphismus, der sog. *Nullhomomorphismus*.

Bemerkung. Im Falle unitärer Ringe wird in der Literatur bei der Definition eines Ringhomomorphismus häufig gefordert, daß dieser *unitär* ist, d.h. per definitionem, daß dieser das Einselement auf das Einselement abbildet. Nicht jeder Ringhomomorphismus ist dann unitär: Der Nullhomomorphismus wie im letzten Beispiel ist z.B. nur unitär, wenn $S=\{0\}$ gilt.

Sei $p\in\mathbb{N}_+$. Wir definieren auf $\mathbb{Z}_p$, „der“ zyklischen Gruppe der Ordnung p, vgl. Beispiel 7.) nach 4.5, eine Multiplikation durch

$$\forall_{k,l\in\mathbb{Z}}\ \overline{k}\cdot\overline{l}.$$

Dies ist wohldefiniert, da zu allen $k,k',l,l'\in\mathbb{Z}$ mit $\overline{k}=\overline{k'}$ und $\overline{l}=\overline{l'}$ Zahlen $\tilde{k},\tilde{l}\in\mathbb{Z}$ existieren derart, daß gilt

$$k=k'+p\cdot\tilde{k}\quad\text{sowie}\quad l=l'+p\cdot\tilde{l},$$

also

$$k\cdot l=k'\cdot l+p\cdot\left(k'\cdot\tilde{l}+\tilde{k}\cdot l'+p\cdot\tilde{k}\cdot\tilde{l}\right),$$

und $p\mid(k\cdot l-k'\cdot l)$.

Dann ist $(\mathbb{Z}_p,+,\cdot)$ ein kommutativer unitärer Ring – dies folgt sofort aus den jeweils entsprechenden Eigenschaften von $(\mathbb{Z},+,\cdot)$. Wir notieren die *Abbildungstafeln von* $(\mathbb{Z}_p,\cdot)$ für $p\in\{2,3,4,5\}$:

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Offenbar ist $\left(\mathbb{Z}_p \setminus \left\{\overline{0}\right\}, \cdot\right)$ für $p \in \{2,3,5\}$ eine abelsche Gruppe.[8] In $\mathbb{Z}_4$ gilt $\overline{2} \cdot \overline{2} = \overline{0} \notin \mathbb{Z}_4 \setminus \left\{\overline{0}\right\}$.

Definition 4.19. Ein Ring $(R, +, \cdot)$ heißt *nullteilerfrei* genau dann, wenn für alle $a, b \in R$ gilt

$$a \cdot b = 0 \Longrightarrow (a = 0 \vee b = 0).$$

Satz 4.20. *Sei $p \in \mathbb{N}$ mit $p \geq 2$.*
Dann ist $\mathbb{Z}_p$ genau dann nullteilerfrei, wenn p eine Primzahl ist.

Beweis. „⇒“ Sei p keine Primzahl, also existieren natürliche Zahlen $n, m \in \mathbb{N}_+$ mit $1 < n, m < p$ und $p = n \cdot m$. Dann folgt $\overline{n} \cdot \overline{m} = \overline{0}$, d.h. $\mathbb{Z}_p$ ist nicht nullteilerfrei.
„⇐“ Seien p eine Primzahl und $k, l \in \mathbb{Z}$ mit $\overline{k} \cdot \overline{l} = \overline{0}$. Dann existiert $\kappa \in \mathbb{Z}$ derart, daß $k \cdot l = p \cdot \kappa$ gilt. Wir können $k, l \in \mathbb{N}$ und damit $\kappa \in \mathbb{N}$ annehmen. Im Falle $k \cdot l \in \{0,1\}$ folgt trivialerweise $\overline{k} = 0 \vee \overline{l} = \overline{0}$. Im Falle $k \cdot l \geq 2$ ergibt der Fundamentalsatz der Arithmetik 2.18, daß $p \mid (k \cdot l)$ gilt, d.h. nach 2.15: $\overline{k} = 0 \vee \overline{l} = \overline{0}$. □

Ein nullteilerfreier kommutativer unitärer Ring besitzt nicht notwendig inverse Elemente bzgl. der Multiplikation. In der Natur treten solche Ringe, die letztgenannte Eigenschaft doch erfüllen, allerdings so häufig auf, daß sie eine eigene Bezeichnung verdienen.

Definition 4.21 (Körper)**.** Ein unitärer Ring $(\mathbb{k}, +, \cdot)$ (oder kurz $\mathbb{k}$) heißt *Körper* genau dann, wenn $(\mathbb{k} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist.

Beispiel.

1.) $(\mathbb{Z}, +, \cdot)$ ist kein Körper.

2.) $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper.

Satz 4.22. *Sei $(\mathbb{k}, +, \cdot)$ ein Körper.*
Dann gilt $0 \neq 1$, und $\mathbb{k}$ ist nullteilerfrei.

Beweis. Aus der Definition eines Körpers folgt sofort $1 \in \mathbb{k} \setminus \{0\}$ und aus $a, b \in \mathbb{k}$ mit $a, b \neq 0$ sowie $\underbrace{a \cdot b}_{\in \mathbb{k} \setminus \{0\}} = 0$ ein Widerspruch. □

Satz 4.23. *Ein endlicher nullteilerfreier kommutativer unitärer Ring ist ein Körper.*

[8] Es ist kein Zufall, daß p in diesen Fällen eine Primzahl ist, s.u. 2.24.

Beweis. Sei also $(R,+,\cdot)$ ein endlicher nullteilerfreier kommutativer unitärer Ring. Zu zeigen ist, daß jedes fixierte $a \in R \setminus \{0\}$ ein inverses Element bzgl. $\cdot$ in $R \setminus \{0\}$ besitzt.

Wir definieren $f\colon R \to R$ durch $\forall_{b\in R}\, f(b) = a\cdot b$. Diese Abbildung ist injektiv, denn für alle $b,c \in R$ folgt aus $a\cdot b = a\cdot c$

$$a\cdot(b-c) = a\cdot b - a\cdot c = 0,$$

also wegen $a \neq 0$ und der Nullteilerfreiheit: $b = c$.

Dies und die Endlichkeit von R impliziert die Surjektivität der Abbildung $f\colon R \to R$.[9] Daher existiert $a' \in R$ mit $a\cdot a' = f(a') = 1$. Offenbar gilt $a' \neq 0$. □

Korollar 4.24. *Sei $p \in \mathbb{N}_+$ mit $p \geq 2$.*
Dann ist $\mathbb{Z}_p$ genau dann ein Körper, wenn p eine Primzahl ist.

Beweis. „⇒“ Sei $t \in \mathbb{N}_+$ ein Teiler von p. Dann existiert (wegen $p > 0$) eine Zahl $k \in \mathbb{N}_+$ mit $p = k\cdot t$, insbesondere gilt

$$k,t \in \{1,\dots,p\} \quad \text{und} \quad p = k\cdot t, \tag{34}$$

sowie $\overline{k}\cdot\overline{t} = \overline{0}$. Da $\mathbb{Z}_p$ als Körper vorausgesetzt ist, existiert $s \in \mathbb{Z}\setminus\{0\}$ mit $\overline{t} = (\overline{s})^{-1}$, also folgt

$$\overline{0} = \overline{0}\cdot\overline{s} = \overline{k}\cdot\overline{t}\cdot\overline{s} = \overline{k}$$

und $k \in p\mathbb{Z} = \{\dots,-2p,-p,0,p,2p,\dots\}$. Daher ergibt (34): $k = p$ und $t = 1$. Folglich ist p eine Primzahl.

„⇐“ folgt aus 4.20 und 4.23. □

Seien $(R,+,\cdot)$ ein Ring, $k \in \mathbb{Z}$ und $a \in R$. Wir definieren

$$\boxed{k\cdot a} := \begin{cases} \overbrace{a+\dots+a}^{k \text{ Summanden}}, & k > 0,\\ 0, & k = 0,\\ -(k\cdot a), & k < 0. \end{cases}$$

Definition 4.25 (Charakteristik)**.** Sei R ein unitärer Ring. Falls ein kleinstes $\chi \in \mathbb{N}_+$ mit $\chi\cdot 1 = 0$ existiert, so heißt χ die *Charakteristik von R* (i.Z. $\boxed{\mathrm{Char}(R)}$). Existiert kein solches $\chi \in \mathbb{N}_+$, so setzen wir die *Charakteristik von R* gleich null.

Beispiel.

1.) $\mathrm{Char}(\mathbb{Q}) = \mathrm{Char}(\mathbb{R}) = 0$.

2.) $\mathrm{Char}(\mathbb{Z}) = 0$.

3.) Für alle $p \in \mathbb{N}_+$ gilt $\mathrm{Char}(\mathbb{Z}_p) = p$.

Satz 4.26. *Sei $\mathbb{k}$ ein Körper.*
Dann gilt: $\mathrm{Char}(\mathbb{k}) = 0$ *oder* $\mathrm{Char}(\mathbb{k})$ *ist eine Primzahl.*

[9] Wäre nämlich f nicht surjektiv, so gälte $f(R) \subsetneq R$, also $\neg(\#R \leq \#f(R))$. Dann ergäbe der Direcletsche Schubfächersatz 2.26 die Existenz eines Elementes von R, das zwei verschiedene Urbilder unter f besitzt, im Widerspruch zur Injektivität von f.

Beweis. Sei $\chi := \mathrm{Char}(\Bbbk)$ keine Primzahl, d.h. $\chi = m \cdot n$ mit $m, n \in \mathbb{N}$ und $1 < m, n < \chi$. (Beachte, daß $\chi = 1$ nach 4.22 nicht möglich ist!) Dann folgt aus

$$0 = \chi \cdot 1 = m \cdot n \cdot 1 = (m \cdot 1) \cdot (n \cdot 1)$$

und der Nullteilerfreiheit von $\Bbbk$: $m \cdot 1 = 0$ oder $n \cdot 1 = 0$, im Widerspruch zur Minimalität von $\chi \in \mathbb{N}_+$ mit $\chi \cdot 1 = 0$. □

Komplexe Zahlen

Die Gleichung $x^2 = -1$ besitzt im Körper $\mathbb{R}$ der reellen Zahlen keine Lösung x. Wir definieren die *komplexen Zahlen* als die Menge $\boxed{\mathbb{C}}$ aller geordneten Paare (x, y) mit $x, y \in \mathbb{R}$ zusammen mit den folgenden Verknüpfungen

$$+ \colon \mathbb{C} \longrightarrow \mathbb{C}, \quad ((x_1, y_1), (x_2, y_2)) \longmapsto (x_1 + x_2, y_1 + y_2),$$

und

$$\cdot \colon \mathbb{C} \longrightarrow \mathbb{C}, \quad ((x_1, y_1), (x_2, y_2)) \longmapsto (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + y_1 \cdot x_2).$$

Satz 4.27. *$\mathbb{C}$ ist ein Körper.*

Beweis als Übung. □

Die Abbildung

$$\mathbb{R} \hookrightarrow \mathbb{C}, \quad x \longmapsto (x, 0),$$

definiert einen unitären Ringhomomorphismus, der injektiv ist. Wir können jedes $x \in \mathbb{R}$ daher mit $(x, 0) \in \mathbb{C}$ identifizieren und $\mathbb{R}$ als *Teilkörper* von $\mathbb{C}$ auffassen. Wir setzen

$$\boxed{\mathrm{i}} := (0, 1) \in \mathbb{C}.$$

Dann gilt

$$\mathrm{i}^2 = (0, 1) \cdot (0, 1) = (-1, 0) = -1.$$

Hierdurch erklät sich durch Ausmultiplikation auch die oben eingeführte Multiplikation: Für alle $(x_1, y_1), (x_2, x_2) \in \mathbb{C}$ gilt $(x_k, y_k) = x_k + \mathrm{i}\, y_k$ für $k \in \{1, 2\}$ und

$$\begin{aligned} (x_1, y_1) \cdot (x_2, y_2) &= (x_1 + \mathrm{i}\, y_1) \cdot (x_2 + \mathrm{i}\, y_2) \\ &= (x_1 \cdot x_2 - y_1 \cdot y_2) + \mathrm{i}\, (x_1 \cdot y_2 + y_1 \cdot x_2) \\ &= (x_1 \cdot x_2 - y_1 \cdot y_2,\, x_1 \cdot y_2 + y_1 \cdot x_2). \end{aligned}$$

Die geometrische Veranschaulichung der Addition und der Multiplikation erfolgt in den Vorlesungen *Lineare Algebra I* und *Analysis I*: Faßt man komplexe Zahlen als *Vektoren im* $\mathbb{R}^2$ auf, so addieren sich die Komponenten bei Addition. Bei Multplikaton addieren sich die Winkel zur ersten Koordinatenachse, und die *Längen der Vektoren* multiplizieren sich.

Literatur

[1] A. Beutelspacher: *Das ist o. B. d. A. trivial!*, Vieweg (2004).

[2] P.J. Davis, R. Hersch: *Erfahrung Mathematik*, Birkhäuser (1994).

[3] O. Deiser: *Einführung in die Mengenlehre*, Springer (2002).

[4] H.-D. Ebbinghaus et al.: *Zahlen*, Springer (1983).

[5] G. Fischer: *Lineare Algebra*, Vieweg (1995).

[6] K. Fritzsche: *Mathematik für Einsteiger*, Spektrum Akademischer Verlag (1995).

Index