Einführung in die Mathematik

Gernot Greschonig

Armin Rainer

Leo Summerer

Unterlagen zur Vorlesung

Bachelorstudium Unterrichtsfach Mathematik

Wintersemester 2019/20

Vorwort

Diese Unterlagen zur Vorlesung „Einführung in die Mathematik“ geben nur den unmittelbar in der Vorlesung behandelten Stoff in sehr knapper Form wieder.

Zur Vertiefung und Erweiterung sowie für Übungsbeispiele verweisen wir insbesondere auf das Werk „Einführung in das mathematische Arbeiten“ von Hermann Schichl und Roland Steinbauer, zweite Auflage erschienen im Springer Verlag.

Herzlicher Dank ergeht an Christoph Krall für zahlreiche nützliche Anregungen zur Verbesserung dieser Unterlagen.

Inhaltsverzeichnis

KAPITEL 1

Grundlagen

1. Die mathematische Sprache

Ein mathematischer Text setzt sich aus folgenden Bestandteilen zusammen:

- Axiome $\longrightarrow$
- $\updownarrow$
- Definitionen $\longrightarrow$

- Sätze (Theoreme) $\longrightarrow$
- Hilfssätze (Lemmata) $\longrightarrow$
- Propositionen $\longrightarrow$
- $\downarrow$
- Korollare (Folgerungen) $\longrightarrow$

- Beweise

- \+ Bemerkungen, Beispiele, Anwendungen...

Ein *Axiom* ist eine grundlegende Aussage, die vorausgesetzt und nicht bewiesen wird.

Beispiele. Axiome der Logik; Axiome der Mengentheorie.

Häufig wird jedoch die Existenz einer mathematischen Struktur entsprechend einem Axiom oder mehreren Axiomen aus allgemeineren Axiomen bewiesen.

Beispiele. Die Axiome der natürlichen Zahlen folgen aus den Axiomen der Mengentheorie; Konstruktion der reellen Zahlen entsprechend den Axiomen eines vollständigen geordneten Körpers.

Axiome können daher auf verschiedene Ebenen gezogen werden:

(i) Logik
(ii) Mengenlehre
...
(x) natürliche Zahlen
...
(y) reelle Zahlen

Eine *Definition* begründet einen neuen Begriff, oft mit Verweis auf einen bereits vorher definierten Oberbegriff, der weiter eingeschränkt wird. Der *Bezug* ist entscheidend.

Definition. Der Anstieg einer Geraden im xy-Koordinatensystem ist eine reelle Zahl, die angibt, wie sich y ändert, wenn x um 1 wächst.

Bezug: Gerade; Oberbegriff: reelle Zahl; einschränkender Halbsatz: __.

Diese Definition ist nur mit Bezug auf eine Geradenfunktion sinnvoll, jedoch nicht für eine beliebige Funktion im xy-Koordinatensystem.

Als weiteres Beispiel einer Definition betrachten wir den Begriff der Teilbarkeit ganzer Zahlen:

Definition (Teilbarkeit). Seien n und m ganze Zahlen. Die Zahl m heißt Teiler von n, wenn es eine ganze Zahl k gibt mit

$$n = mk$$

Wir schreiben dann $m \mid n$ (gesprochen m teilt n).

Folgerungen für die Teilbarkeit:

- $m \mid 0$ gilt für alle $m \in \mathbb{Z}$ $(0 = m0)$
- $0 \mid n$ gilt nur für $n = 0$ $(n = k0 \Longrightarrow n = 0)$

DEFINITION. Eine ganze Zahl n heißt *gerade*, falls $2 \mid n$. Andernfalls heißt die Zahl *ungerade*.

Ein *Satz* oder eine Proposition besteht aus einer Voraussetzung und einer Behauptung. Als *Proposition* bezeichnen wir ein weniger bedeutendes Resultat als einen Satz. Sätze, Propositionen und Hilfssätze werden bewiesen, wenn ein *Korollar* eine triviale Schlussfolgerung aus einem Satz ist, dann entfällt der Beweis auch häufig. Die Verwendung eines Lemmas kann einen Beweis klarer strukturieren, die Aussage des Lemmas ist meist für sich nicht interessant.

PROPOSITION 1.1. *Das Quadrat einer geraden Zahl ist ebenfalls gerade.*

BEWEIS. Sei n gerade, dann gilt nach der Definition $2 \mid n$ und somit $n = 2k$ für eine ganze Zahl k. Daher ist $n^2 = (2k)^2 = 4k^2 = 2(2k^2) = 2l$ für eine ganze Zahl $l = 2k^2$. Nach der Definition ist n^2 gerade. □

Der Beweis oben ist direkt (straight forward): $V \Longrightarrow \cdots \Longrightarrow \cdots \Longrightarrow \cdots \Longrightarrow B$
Ein Beweis besteht aus:

- Handlungsanleitungen
- logischen Schlussfolgerungen
- Rechnungen

Ein Beweis wird durch viele Handlungsanleitungen sowie detailliert ausgeführte logische Schlussfolgerungen und Rechnungen besser verständlich.

DEFINITION. Eine Primzahl ist eine natürliche Zahl p mit $p > 1$, die nur 1 und p als positive Teiler besitzt.

BEMERKUNG. -1 und $-p$ sind natürlich auch Teiler, daher die Einschränkung auf positive Teiler. Die Hinzunahme von 1 zu den Primzahlen würde beispielweise die Eindeutigkeit der Primfaktorenzerlegung (siehe später) zerstören. Die ersten Primzahlen sind daher $2, 3, 5, 7, 11, 13, 17, \ldots$.

SATZ 1.2 (Satz von Euklid). *Es gibt unendlich viele Primzahlen.*

Der Beweis des Satzes von Euklid erfordert ein Lemma:

LEMMA 1.3 (Existenz der Primfaktorenzerlegung). *Sei $n > 1$ eine natürliche Zahl. Dann gibt es eine Primzahl, die n teilt. Daher kann n als Produkt von Primzahlen geschrieben werden.*

BEWEIS. Angenommen, die Aussage wäre falsch und nicht alle natürlichen Zahlen haben einen Primteiler. Dann muss es eine kleinste solche Zahl ohne Primteiler geben (jede nichtleere Menge natürlicher Zahlen enthält eine kleinste Zahl). Sei a diese Zahl, dann ist a nicht prim (a teilt sich selbst). Da a nicht prim ist, besitzt es einen positiven Teiler m mit $m \neq 1$ und $m \neq a$. Es gilt $m < a$ und wegen der Minimalität von a besitzt m einen Primteiler. Dieser Primteiler teilt dann auch a, ein Widerspruch. Daher besitzt jede natürliche Zahl $n > 1$ einen Primteiler p und es gilt $n = pk$ mit einer natürlichen Zahl k. Wenn $k > 1$ gilt, dann besitzt auch k einen Primteiler. Wir setzen diesen Prozess fort und gewinnen bei jedem Schritt einen Primteiler. Da jede Primzahl ≥ 2 ist, bricht dieser Prozess schließlich ab. □

BEMERKUNG. Dies ist ein *indirekter* Beweis, es wird aus der Verneinung der zu beweisenden Behauptung ein Widerspruch geschlossen.

BEWEIS DES SATZES VON EUKLID. Wir nehmen an, dass es nur endlich viele Primzahlen $p_1, p_2, \cdots, p_r$ gäbe und bilden die natürliche Zahl $N = p_1 p_2 \cdots p_r + 1$. Nach dem Lemma besitzt $N > 1$ einen Primteiler, daher existiert eine Primzahl p_i unter allen Primzahlen $p_1, \ldots, p_r$, sodass $p_i \mid N$ gilt. Aus $N = p_i k$ mit einer natürlichen Zahl k folgt $N - p_1 \cdots p_r = p_i(k - p_1 \cdots p_{i-1} p_{i+1} \cdots p_r) = 1$. Daher gilt $p_i \mid 1$, im Widerspruch zu $p_i \geq 2$. Daher muss die Annahme endlich vieler Primzahlen $p_1, \ldots, p_r$ falsch gewesen sein. □

2. Die mathematische Schrift (Schreibweisen, Notationen, Ausdrücke)

Variablen stehen in der Mathematik stellvertretend für konkrete Zahlen. Wir führen eine Rechnung, einen Beweis etc. nicht für konkrete Zahlen sondern formal für beliebige Zahlen durch. Wir bezeichnen Variablen mit lateinischen oder griechischen Buchstaben:

$a, b, c, \ldots$
$\alpha, \beta, \gamma, \ldots$

Mittels der *Indexschreibweise* können jederzeit beliebig viele Variablen definiert werden, denn unterschiedliche Indices definieren hier unterschiedliche Variablen:

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

Indices werden auch in der linearen Algebra verwendet:

BEISPIELE. Vektoren:

$$\mathbf{x} = (x_1, x_2, \ldots, x_n) \quad \ldots \quad \text{Zeilenvektor}$$

$$\mathbf{y} = \begin{pmatrix} y_1 \\ . \\ . \\ . \\ y_n \end{pmatrix} \quad \ldots \quad \text{Spaltenvektor}$$

m gleich lange Zeilenvektoren $\mathbf{x}_1, \ldots, \mathbf{x}_m$ werden mittels doppelter Indices bezeichnet:

$$\mathbf{x}_1 = (x_{11}, x_{12}, \ldots, x_{1n}), \ldots, \mathbf{x}_m = (x_{m1}, x_{m2}, \ldots, x_{mn})$$

Ein Schema von doppelt indizierten Variablen wird als Matrix bezeichnet:

$$\begin{pmatrix} x_{11} & x_{12} & \ldots & x_{1n} \\ x_{21} & x_{22} & \ldots & x_{2n} \\ . & & & . \\ . & & & . \\ x_{m1} & x_{m2} & \ldots & x_{mn} \end{pmatrix} \quad \ldots \quad m \times n\text{-Matrix}$$

Hier bezeichnet x_{ij} den Eintrag in der i-ten Zeile und der j-ten Spalte.

BEISPIEL. Eine Folge reeller Zahlen $(x_i)_{i \geq 1}$ besteht aus den Folgengliedern $x_1, x_2, x_3, \ldots$. Wollen wir eine allgemeine Teilfolge von 5 beliebigen Folgengliedern angeben, empfehlen sich indizierte Indices:

$$(x_{i_1}, x_{i_2}, x_{i_3}, x_{i_4}, x_{i_5})$$

Hier ist $(x_1, x_2, x_3, x_4, x_5)$ eine spezielle Wahl mit $i_1 = 1, i_2 = 2, \ldots, i_5 = 5$.

BEMERKUNG. Indices dürfen grundsätzlich überall stehen:

$$A_i^j, \quad {}^{\alpha\beta}\Gamma, \ldots$$

DEFINITION. Das Kronecker δ ist gegeben durch

$$\delta_{ij} = \begin{cases} 1 & \text{für } i = j \\ 0 & \text{für } i \neq j \end{cases}$$

Dieses Kronecker δ definiert für jedes $m \geq 1$ eine quadratische $m \times m$-Matrix

$$(\delta_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq m}} = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ . & & & . \\ . & & & . \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

BEMERKUNG. Die Schreibweise von Indices ist immer zu beachten:

- Es gilt $x_{2+5} = x_7$, aber im Allgemeinen gilt $x_2 + x_5 \neq x_7$.
- Im Allgemeinen gilt $x_i + 1 \neq x_{i+1}$.

Das Summenzeichen wird zur geschlossenen Darstellung und Umformung von Ausdrücken der Form

$$a_2 + a_3 + a_4 + \cdots + a_7 = \sum_{i=2}^{7} a_i$$

verwendet. Dabei sind:

$\sum$	...	Summenzeichen
i	...	Laufindex bzw. Summationsindex in den Grenzen 2 bis 7
a_i	...	allgemeiner Term in der Summe

BEISPIELE. Verschiebung des Laufindex:

$$\sum_{j=0}^{4} x_{i,j+1} = x_{i1} + x_{i2} + \cdots + x_{i5} = \sum_{j=1}^{5} x_{i,j}$$

Triviale Summen:

$$\sum_{j=1}^{1} x_j = x_1, \quad \sum_{j=2}^{1} x_j = 0, \quad \sum_{j=2}^{7} x = \underbrace{x + \cdots + x}_{\text{6-mal}} = 6x$$

Wenn die obere Grenze kleiner als die untere Grenze ist, dann setzen wir die Summe 0.
Polynome:

$$a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{i=0}^{n} a_i x^i$$

Zusammenfassen und Herausheben:

$$\sum_{k=0}^{n} a_k + \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} (a_k + b_k), \quad \sum_{k=0}^{n} c a_k = c \sum_{k=0}^{n} a_k$$

Das Produktzeichen $\prod$ wird analog zum Summenzeichen $\sum$ zur Produktbildung verwendet:

$$a_2 \, a_3 \, a_4 \cdots a_7 = \prod_{i=2}^{7} a_i$$

Man setzt jedoch

$$\prod_{j=1}^{0} a_j = 1,$$

auch ganz generell bei einer oberen Grenze kleiner als die untere Grenze.

Beispiele.

$$\prod_{j=2}^{7} x = x^6, \quad \prod_{j=1}^{n} a_{2j} = \prod_{\substack{k=1 \\ k \text{ gerade}}}^{2n} a_k = a_2\, a_4 \cdots a_{2n-2}\, a_{2n}$$

Bei einer Doppelsumme werden alle Einträge einer Matrix summiert:

$$\mathbf{A} = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ a_{m1} & \dots & a_{mn} \end{pmatrix} \qquad \sum_{i=1}^{m} \left(\sum_{j=1}^{n} a_{ij} \right) = S = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} a_{ij} \right)$$

Hier wurde links zeilenweise und rechts spaltenweise summiert. Wenn die Reihenfolge keine Rolle spielt, dann schreibt man auch

$$S = \sum_{\substack{1 \le i \le m \\ 1 \le j \le n}} a_{ij}$$

Bemerkung. Bei unendlichen Summen (siehe Analysis) spielt die Reihenfolge der Summation im Allgemeinen eine Rolle.

Beispiele. Teleskopsumme, Teleskopprodukt:

$$\sum_{i=0}^{n-1} (a_i - a_{i+1}) = a_0 - a_n, \quad \prod_{i=0}^{n-1} \frac{a_i}{a_{i+1}} = \frac{a_0}{a_n}$$

Allgemeine Indexmengen:

$$I = \{2, 8, 13\}, \quad \sum_{i \in I} x_i = x_2 + x_8 + x_{13}$$

Definition (Fakultät, Faktorielle). Sein n eine natürliche Zahl ($n \in \mathbb{N}$). Wir definieren:

$$n! := \prod_{i=1}^{n} i$$

Es gilt: $0! = 1; 1! = 1; 2! = 2; 3! = 6; 4! = 24; 5! = 120; 6! = 720; \dots,$

Definition (Binomialkoeffizient). Seien n und k mit $k \le n$ natürliche Zahlen. Wir definieren den Binomialkoeffizienten durch

$$\binom{n}{k} := \frac{n!}{k!\,(n-k)!} = \frac{\prod_{i=n-k+1}^{n} i}{k!} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!}.$$

Weiters setzen wir für $k > n$ und ganze Zahlen $k < 0$ den Binomialkoeffizienten $\binom{n}{k} = 0$.

Proposition 2.1. *Es gelten für alle natürlichen Zahlen n und k mit $k \le n$ folgende Gleichungen:*

$$\binom{n}{0} = \binom{n}{n} = 1, \quad \binom{n}{k} = \binom{n}{n-k}, \quad \binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$$

BEWEIS. Die ersten beiden Gleichungen folgen unmittelbar aus der Definition.
Die dritte Gleichung folgt für $k = 0$ ebenfalls aus der Definition. Für $0 < k \leq n$ gilt

$$\binom{n}{k} + \binom{n}{k-1} = \frac{n!}{k!\,(n-k)!} + \frac{n!}{(k-1)!\,(n-k+1)!} =$$
$$= \frac{n!\,(n+1-k)}{k!\,(n-k+1)!} + \frac{n!\,k}{k!\,(n-k+1)!} = \frac{n!\,(n+1)}{k!\,((n+1)-k)!} = \binom{n+1}{k}$$

□

Das Pascalsche Dreieck wird in Form eines gleichschenkeligen Dreiecks durch die Zahl 1 an der Spitze und darunter liegende Zeilen gebildet. Die n-te Zeile besteht jeweils aus n Einträgen, die fiktiven Einträge außerhalb des Dreiecks werden 0 gesetzt. Jeder Eintrag ist gleich der Summe der beiden Einträge schräg links und schräg rechts darüber. Daher sind die Einträge am Rand alle gleich $1 = 0 + 1 = 1 + 0$. Die Summenformel in der Proposition entspricht der Bildungsvorschrift des Pascalschen Dreiecks und es gilt folgende Darstellung durch Binomialkoeffizienten:

$$\boxed{\tbinom{0}{0}=1}$$
$$\boxed{\tbinom{1}{0}=1}\quad\boxed{\tbinom{1}{1}=1}$$
$$\boxed{\tbinom{2}{0}=1}\quad\boxed{\tbinom{2}{1}=2}\quad\boxed{\tbinom{2}{2}=1}$$
$$\boxed{\tbinom{3}{0}=1}\quad\boxed{\tbinom{3}{1}=3}\quad\boxed{\tbinom{3}{2}=3}\quad\boxed{\tbinom{3}{3}=1}$$
$$\boxed{\tbinom{4}{0}=1}\quad\boxed{\tbinom{4}{1}=4}\quad\boxed{\tbinom{4}{2}=6}\quad\boxed{\tbinom{4}{3}=4}\quad\boxed{\tbinom{4}{4}=1}$$
$$\boxed{\tbinom{5}{0}=1}\quad\boxed{\tbinom{5}{1}=5}\quad\boxed{\tbinom{5}{2}=10}\quad\boxed{\tbinom{5}{3}=10}\quad\boxed{\tbinom{5}{4}=5}\quad\boxed{\tbinom{5}{5}=1}$$
$$\boxed{\tbinom{6}{0}=1}\quad\boxed{\tbinom{6}{1}=6}\quad\boxed{\tbinom{6}{2}=15}\quad\boxed{\tbinom{6}{3}=20}\quad\boxed{\tbinom{6}{4}=15}\quad\boxed{\tbinom{6}{5}=6}\quad\boxed{\tbinom{6}{6}=1}$$
$$\boxed{\tbinom{7}{0}=1}\quad\boxed{\tbinom{7}{1}=7}\quad\boxed{\tbinom{7}{2}=21}\quad\boxed{\tbinom{7}{3}=35}\quad\boxed{\tbinom{7}{4}=35}\quad\boxed{\tbinom{7}{5}=21}\quad\boxed{\tbinom{7}{6}=7}\quad\boxed{\tbinom{7}{7}=1}$$
$$\boxed{\tbinom{8}{0}=1}\quad\boxed{\tbinom{8}{1}=8}\quad\boxed{\tbinom{8}{2}=28}\quad\boxed{\tbinom{8}{3}=56}\quad\boxed{\tbinom{8}{4}=70}\quad\boxed{\tbinom{8}{5}=56}\quad\boxed{\tbinom{8}{6}=28}\quad\boxed{\tbinom{8}{7}=8}\quad\boxed{\tbinom{8}{8}=1}$$

In der n-ten Zeile des Pascalschen Dreiecks stehen daher die Binomialkoeffizienten $\binom{n-1}{k}$ für $k = 0, \ldots, n-1$. Insbesondere sind alle Binomialkoeffizienten natürliche Zahlen.

In diesem Argument haben wir erstmals (in informeller Weise) einen Beweis durch vollständige Induktion geführt. Der Name Binomialkoeffizient rührt vom binomischen Satz her.

3. Beweismethoden und Beweistechniken

Direkter / indirekter Beweis. Den direkten Beweis haben wir in der Proposition 1.1 bereits kennengelernt. Die Voraussetzung wird bis zur Aussage (Behauptung) des Satzes hin umgeformt, dabei werden Gleichungen umgeformt bzw. verifiziert.

Sei beispielsweise $A = B$ zu beweisen:

- korrekt: $A = A_1 = A_2 = \cdots = A_n = B$
- falsch: $A = B \Longrightarrow A_1 = B_1 \Longrightarrow A_2 = B_2 \Longrightarrow \cdots \Longrightarrow C = C$

Im korrekten Beweisschema wird A umgeformt bis die Gleichheit zu B offensichtlich wird.

Im falschen Beweisschema wird „Wenn $A = B$ richtig ist, dann auch $C = C$“ geschlossen, jedoch nicht umgekehrt. Diese Vorgangsweise ist nur mit sog. Äquivalenzumformungen gestattet. Nur dann dürfen die Pfeile umgekehrt werden um aus der wahren Aussage $C = C$

auch die Aussage $A = B$ zu schließen. Wir raten daher dringend ab vom „Herunterrechnen“ von Gleichungen und empfehlen Umformungen in Gleichungsketten.

Eine ebenfalls korrekte Vorgangsweise:

$$\left.\begin{array}{l} A = A_1 = A_2 = \cdots = A_m = C \\ B = B_1 = B_2 = \cdots = B_n = C \end{array}\right\} \quad \Longrightarrow \quad A = B$$

Eine Äquivalenz von Aussagen $P \Leftrightarrow Q$ wird häufig in getrennten Richtungen $P \Rightarrow Q$ und $Q \Rightarrow P$ ($P \Leftarrow Q$) bewiesen. Analog gilt für zwei Mengen $A = B \Leftrightarrow A \subseteq B$ und $B \subseteq A$.

Fallunterscheidungen. Eine weitere wesentliche Beweistechnik sind Fallunterscheidungen. Hier stehen jeweils korrekte Beweisargumente unter mehreren zusätzlichen Annahmen zur Verfügung. Wesentlich ist, dass immer zumindest eine dieser zusätzlichen Annahmen erfüllt sein muss.

Beispiel. Jede Quadratzahl liefert bei Division durch 3 den Rest 0 oder 1.

Beweis. Sei $n = m^2$ eine Quadratzahl, dann kann m durch $m = 3k$, $m = 3k + 1$ oder $m = 3k + 2$ mit $k \in \mathbb{N}$ dargestellt werden. 1. Fall: $n = (3k)^2 = 9k^2 = 3(3k^2)$, daher Rest 0;
2. Fall: $n = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, daher Rest 1;
3. Fall: $n = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$, daher Rest 1. □

Beispiel. Für reelle Zahlen x, y gilt $\big||x| - |y|\big| \leq |x - y|$.

Beweis. 1. Fall: $x, y \geq 0$; 2. Fall: $x \geq 0, y < 0$; 3. Fall: $x < 0, y \geq 0$; 4. Fall: $x, y < 0$. Durch die Fallunterscheidungen können die Beträge $|x|$ bzw. $|y|$ jeweils durch x oder $-x$ bzw. y oder $-y$ dargestellt werden. □

Beispiel. Fallunterscheidungen sind auch beim Auflösen von Ungleichungen essentiell. Wir suchen die Lösungsmenge der Ungleichung $\frac{x-1}{x+2} < 3$. Im Fall $x < -2$ gilt $x - 1 > 3x + 6 \Leftrightarrow x < -\frac{7}{2}$, daher ist die Ungleichung für alle $x < -\frac{7}{2}$ erfüllt. Im Fall $x > -2$ gilt $x - 1 < 3x + 6 \Leftrightarrow x > -\frac{7}{2}$, daher ist die Ungleichung für alle $x > -2$ erfüllt. Daher gilt $L = (-\infty, -\frac{7}{2}) \cup (-2, \infty)$.

Häufige Fallunterscheidungen sind: endlich – unendlich, gerade – ungerade, positiv – 0 – negativ, etc.

Ein *indirekter Beweis* wurde bereits beim Satz von Euklid verwendet. Aus der Negation (Verneinung) der zu beweisenden Aussage wird durch Umformungen eine offensichtlich falsche Aussage oder ein Widerspruch gewonnen. Es sollte immer eine Formulierung „Angenommen ... “ vorkommen und der Widerspruch genau lokalisiert werden. Diese Methode beruht auf dem *Prinzip vom ausgeschlossenen Dritten* – es gibt nur zwei Wahrheitswerte „wahr“ und „falsch“ – und der *zweiwertigen (klassischen) Logik* – jede Aussage ist *entweder* wahr oder falsch.

Vollständige Induktion. Die Methode der vollständigen Induktion wird zum Beweis von Aussagen $A(n)$ für alle natürlichen Zahlen n (oder alle natürlichen Zahlen $n \geq n_0$) verwendet. Angenommen, wir können zeigen:

- $A(0)$ ist wahr
- $A(n + 1)$ ist wahr, wenn $A(n)$ wahr ist (d.h. $A(n) \Rightarrow A(n + 1)$)

Dann ist $A(n)$ für alle n wahr, denn

$$A(0) \Rightarrow A(1) \Rightarrow A(2) \Rightarrow \cdots \Rightarrow A(i) \Rightarrow A(i + 1) \Rightarrow \ldots.$$

Wir bezeichnen den Beweis von $A(0)$ als *Induktionsanfang*, die Voraussetzung von $A(n)$ als *Induktionsannahme* und den Schluss von $A(n)$ auf $A(n+1)$ als *Induktionsschritt*. Wesentlich ist, dass die Schlussfolgerung von $A(n)$ nach $A(n+1)$ für *alle* natürlichen Zahlen n zulässig ist! Auch der Induktionsanfang ist absolut essentiell, kann aber für eine positive natürliche Zahl n_0 erfolgen (dann gilt die Aussage $A(n)$ nur für $n \geq n_0$).

Die Methode der vollständigen Induktion ist vielseitig einsetzbar z.B. bei Gleichungen für natürliche Zahlen, jedoch muss zuerst die zu beweisende Formel aufgefunden werden.

BEISPIEL. Die geometrische Summenformel lautet für eine natürliche Zahl n und reelle Zahlen a_0 und $q \neq 1$

$$a_0 + a_0\,q + a_0\,q^2 + a_0\,q^3 + \cdots + a_0\,q^n = \sum_{i=0}^{n} a_0\,q^i = a_0\,\frac{1-q^{n+1}}{1-q}.$$

BEWEIS. *Induktionsanfang:* Für $n = 0$ besteht die Summe nur aus a_0 und stimmt mit dem Wert $a_0\frac{1-q^{0+1}}{1-q} = a_0$ überein.

Induktionsannahme: Wir setzen $\sum_{i=0}^{n} a_0\,q^i = a_0\frac{1-q^{n+1}}{1-q}$ voraus.

Induktionsschritt: Wir schließen

$$\sum_{i=0}^{n+1} a_0\,q^i = \left(\sum_{i=0}^{n} a_0\,q^i\right) + a_0 q^{n+1} \overset{\text{Induktionsannahme}}{=} a_0\frac{1-q^{n+1}}{1-q} + a_0 q^{n+1} =$$

$$= a_0\frac{1-q^{n+1}+q^{n+1}(1-q)}{1-q} = a_0\frac{1-q^{n+2}}{1-q}.$$

Die Kette von Gleichungen ergibt die zu beweisende Summenformel für den Summationsindex $n+1$, damit ist der Induktionsbeweis abgeschlossen. □

SATZ 3.1. *Seien a und b reelle Zahlen und $n \geq 1$ eine natürliche Zahl. Dann gilt*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

BEWEIS. Wir multiplizieren das Produkt $\underbrace{(a+b)\cdots(a+b)}_{\text{n-mal}}$ vollständig aus und erhalten insgesamt 2^n Summanden, denn bei jedem der Faktoren haben wir die Wahl zwischen a und b. Jeder dieser Summanden wird eindeutig durch eine Zeichenkette der Länge n bestehend aus den Symbolen a und b repräsentiert, als reelle Zahlen sind jedoch alle Zeichenketten mit k-mal a und $(n-k)$-mal b identisch. Daher bleibt nur noch die Aussage $A(n)$ zu beweisen, dass die Zahl derartiger Zeichenketten für alle $0 \leq k \leq n$ genau $\binom{n}{k}$ ist (d.h. $A(n)$ besteht eigentlich aus $n+1$ gleichzeitig erfüllten Aussagen). Wir führen diesen Beweis mit vollständiger Induktion nach n.

Induktionsanfang: Für $n = 1$ triff die Aussage $A(1)$ zu, denn es gibt genau eine Zeichenkette mit einem a und genau eine Zeichenkette mit einem b und es gilt $\binom{1}{0} = \binom{1}{1} = 1$.

Induktionsannahme: Wir nehmen nun an, dass für eine natürliche Zahl $n \geq 1$ und alle $0 \leq k \leq n$ die Zahl der Zeichenketten mit k-mal a und $(n-k)$-mal b genau $\binom{n}{k}$ ist.

Induktionsschritt: Wenn $1 \leq k \leq n$ gilt, dann kann jede Zeichenkette der Länge $n+1$ mit k-mal a und $(n+1-k)$-mal b auf genau eine der folgenden Arten gebildet werden:

- eine Zeichenkette der Länge n mit k-mal a und $(n-k)$-mal b, ergänzt um ein b am Ende,
- eine Zeichenkette der Länge n mit $(k-1)$-mal a und $(n+1-k)$-mal b, ergänzt um ein a am Ende.

Nach der Induktionsannahme und Proposition 2.1 gilt für die Anzahl $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$. In den Fällen $k = 0$ und $k = n + 1$ (d.h. die Zeichenkette enthält nur eines der Symbole a oder b) gibt es nur eine Möglichkeit der Bildung, die Anzahl ist wegen $\binom{n+1}{0} = \binom{n+1}{n+1} = 1$ auch dann korrekt. Daher gilt $A(n + 1)$ und der Induktionsbeweis ist fertig. □

Bei Beweisen von Ungleichungen ist die Richtung des Ungleichungszeichens zu beachten, weiters ist eine hinreichend gute Abschätzung wichtig:

Beispiel. Zeige $n^3 \leq 3^n$ für alle natürlichen Zahlen n.

Beweis. Für $n = 0, 1, 2$ wird die Aussage zuerst direkt verifiziert.
Induktionsanfang: Für $n = 3$ gilt $3^3 \leq 3^3$.
Induktionsannahme: Sei $n^3 \leq 3^n$ für eine natürliche Zahl $n \geq 3$.
Induktionsschritt: Es gilt $3^{n+1} = 3 \cdot 3^n \overset{\text{Induktionsannahme}}{\geq} 3 \cdot n^3 = n^3 + 2n^3 \overset{\text{wegen } n\geq 3}{\geq} n^3 + 6n^2 \overset{\text{wegen } n\geq 2}{\geq} n^3 + 3n^2 + 3n + 1 = (n + 1)^3$. □

Bemerkung. Die Induktionsanfang ist bei $n = 1$ ($1^3 \leq 3^1$) und $n = 2$ ($2^3 \leq 3^2$) durchführbar, aber der Induktionsschritt funktioniert erst ab $n = 3$.

Zum Abschluss wollen wir uns noch mit einem „falschen“ Induktionsbeweis befassen:

Satz 3.2. *Alle Menschen besitzen dieselbe Haarfarbe.*

Beweis. Wir beweisen induktiv für alle natürlichen Zahlen $k \geq 1$ die Aussage: „In allen Mengen von Menschen mit k Elementen tritt nur eine Haarfarbe auf.“
Induktionsanfang: Die Aussage ist für $k = 1$ offensichtlich.
Induktionsannahme: In jeder Menge von Menschen mit k Elementen gibt es nur eine Haarfarbe.
Induktionsschritt: Sei $M = \{m_1, \ldots, m_k, m_{k+1}\}$ eine Menge von Menschen mit $k + 1$ Elementen. Wir betrachten die beiden Teilmengen $\{m_1, \ldots, m_k\}$ und $\{m_2, \ldots, m_{k+1}\}$ mit jeweils k Elementen. Nach der Induktionsannahme tritt in beiden jeweils nur eine Haarfarbe auf. Da beide Mengen gemeinsame Elemente besitzen, tritt überhaupt nur eine Haarfarbe auf. □

Lokalisieren Sie den Fehler in diesem Beweis!

KAPITEL 2

Logik

Die Mathematik besteht überwiegend aus Aussagen (und nicht Zahlen, Rechnungen etc.). Die Verbindung zwischen diesen Aussagen ist wesentlich!
Aussagenlogik:

- Setzt einfache Aussagen zu komplexen zusammen (mittels sog. Junktoren),
- der Wahrheitsgehalt solcher Aussagen ist zu ermitteln.

Prädikatenlogik:

- Allgemeine Aussagen (Allquantor $\forall$)
- Existenzaussagen (Existenzquantor $\exists$)

Was ist eine Aussage? Eine Aussage ist ein sprachlicher Konstrukt, dem man prinzipiell einen Wahrheitswert zuordnen kann:

- Fragen oder Befehle sind daher keine Aussagen.
- Eine Aussage muss genau einen der Wahrheitswerte „wahr“ oder „falsch“ besitzen.

Wahrheitswerte im Rahmen eines Axiomensystems in der Mathematik:

- Noch unbewiesene Aussagen können wahr oder falsch sein und dies muss überprüfbar sein,
- sie können aber auch unentscheidbar sein, d.h. weder durch Hinzunahme der Aussage zum jeweiligen Axiomensystem ergibt sich ein Widerspruch noch durch Hinzunahme der Negation.

1. Aussagenlogik

Nicht / Und / Oder. Sei p eine Aussage. Dann kann die *Negation (Verneinung)* $\neg p$ sprachlich gebildet werden, indem man „es ist nicht der Fall, dass“ voranstellt.
Wahrheitswerte: p wahr $\Longrightarrow \neg p$ falsch
p falsch $\Longrightarrow \neg p$ wahr
Wir stellen die Wahrheitswerte von $\neg p$ und $\neg(\neg p)$ in Abhängigkeit vom Wahrheitswert von p in einer *Wahrheitstafel* dar:

p	$\neg p$	$\neg(\neg p)$
w	f	w
f	w	f

Beispiel. Sei p die Aussage $2 \mid 10$. Dann ist die Negation $\neg p$ die Aussage $2 \nmid 10$.

Auch die Verknüpfung zweier Aussagen ergibt eine neue Aussage.

Beispiele. Sei nun p die Aussage $3 \mid 18$ und sei q die Aussage $2 \mid 18$.

(1) Die Und-Verknüpfung $p \wedge q$ ist die Aussage „18 ist durch 2 und durch 3 teilbar“. Diese Aussage ist wahr. (Achtung: $p \wedge q$ ist vom rein logischen Standpunkt nicht dasselbe wie die Aussage „18 ist durch 6 teilbar“.)
(2) Die Oder-Verknüpfung $p \vee q$ ist die Aussage „18 ist durch 2 oder durch 3 teilbar“. Auch diese Aussage ist wahr.

(3) Die Aussage „18 ist entweder durch 2 oder durch 3 teilbar“ ist jedoch falsch. Formal ist das $(p \wedge \neg q) \vee (\neg p \wedge q)$ oder auch $p \veebar q$

Auch die Verknüpfungen zweier Aussagen werden durch Wahrheitstafeln beschrieben. Links stehen die möglichen Wahrheitswerte von p und q und rechts die sich daraus ergebenden Wahrheitswerte von $p \wedge q$, $p \vee q$ und $p \veebar q$:

p	q	$p \wedge q$
w	w	w
w	f	f
f	w	f
f	f	f

p	q	$p \vee q$
w	w	w
w	f	w
f	w	w
f	f	f

p	q	$p \veebar q$
w	w	f
w	f	w
f	w	w
f	f	f

Es folgt unabhängig vom Wahrheitswert der Aussage p:

- Die Aussage $p \vee \neg p$ ist immer wahr, d.h. eine *Tautologie*.
- Die Aussage $p \wedge \neg p$ ist immer falsch, d.h. eine *Kontradiktion*.

Implikation und Äquivalenz. Seien p und q Aussagen. Die Schlussfolgerung (Implikation) $p \Rightarrow q$: „Wenn p, dann q“ ist ebenfalls eine Aussage. In der Alltagssprache ist diese Aussage nur dann wahr, wenn sowohl die Voraussetzung p als auch die Schlussfolgerung q wahr sind. In der Logik definiert man $p \Rightarrow q$ auch immer dann als wahr, wenn die Voraussetzung p falsch ist:

Alltagssprache

p	q	$p \Rightarrow q$
w	w	w
w	f	f
f	w	n.a.
f	f	n.a.

Mathematik / Logik

p	q	$p \Rightarrow q$
w	w	w
w	f	f
f	w	w
f	f	w

- Aus einer falschen Aussage folgt jede beliebige Aussage.
- Eine wahre Aussage folgt aus jeder beliebigen Aussage.

Andere Umschreibungen für $p \Rightarrow q$ sind:

- p ist hinreichend für q
- q ist notwendig für p $(\neg q \Rightarrow \neg p)$

Seien wieder a und b Aussagen. $a \Leftrightarrow b$: „a genau dann, wenn b“ ist ebenfalls eine Aussage:

a	b	$a \Leftrightarrow b$
w	w	w
w	f	f
f	w	f
f	f	w

Nun können wir zeigen: $(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a)$ (indirekter Beweis!)

a	b	$a \Rightarrow b$	$\neg b$	$\neg a$	$\neg b \Rightarrow \neg a$	$(a \Rightarrow b) \Leftrightarrow (\neg b \Rightarrow \neg a)$
w	w	w	f	f	w	w
w	f	f	w	f	f	w
f	w	w	f	w	w	w
f	f	w	w	w	w	w

Es gelten folgende Rechenregeln:

- Kommutativgesetze: $a \wedge b \Leftrightarrow b \wedge a$, $a \vee b \Leftrightarrow b \vee a$
- Assoziativgesetze: $a \wedge (b \wedge c) \Leftrightarrow (a \wedge b) \wedge c$
  $a \vee (b \vee c) \Leftrightarrow (a \vee b) \vee c$
- Distributivgesetze: $a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c)$
  $a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c)$
- Gesetze von De Morgan: $\neg(a \wedge b) \Leftrightarrow \neg a \vee \neg b$
  $\neg(a \vee b) \Leftrightarrow \neg a \wedge \neg b$
- $(a \Rightarrow b) \Leftrightarrow (\neg a \vee b)$

Hier bindet $\neg$ am stärksten, $\wedge, \vee$ binden stärker als $\Leftrightarrow, \Rightarrow$. Der Beweis dieser Rechenregeln erfolgt mit Hilfe von Wahrheitstafeln. Wir beweisen eines der Distributivgesetze.

a	b	c	$b \wedge c$	$a \vee (b \wedge c)$	$a \vee b$	$a \vee c$	$(a \vee b) \wedge (a \vee c)$
w	w	w	w	w	w	w	w
w	w	f	f	w	w	w	w
w	f	w	f	w	w	w	w
w	f	f	f	w	w	w	w
f	w	w	w	w	w	w	w
f	w	f	f	f	w	f	f
f	f	w	f	f	f	w	f
f	f	f	f	f	f	f	f

Bei allen möglichen Wahrheitswerten von a, b und c stimmen die Wahrheitswerte in der fünften Spalte von links und in der rechten Spalte überein, daher gilt $a \vee (b \wedge c) \Leftrightarrow (a \vee b) \wedge (a \vee c)$.

Bemerkung. Die gesamte Aussagenlogik kann mit zwei Junktoren $\neg, \vee$ oder $\neg, \wedge$ aufgebaut werden.

Logische und sachbezogene Schlüsse.

- Logischer Schluss: $p \wedge q \Rightarrow p$
  ist wahr unabhängig von den Wahrheitswerten von p und q.
- Sachbezogener Schluss: $p \Rightarrow q$
  ist wahr oder falsch, je nach der Definition der Aussagen p und q, hängt daher von Wahrheitswerten ab.

Achtung: $6 \mid n \Rightarrow 3 \mid n$ ist „logisch“ im Sinne von leicht, jedoch ein sachbezogener Schluss.

Wir verwenden folgende logischen Schlüsse beim Beweisen:

- Indirekter Beweis: $p \Rightarrow q$ wird gezeigt durch: $\neg q \Rightarrow \neg p$
- Fallunterscheidung: „Es gilt p“ wird gezeigt durch: Fall $q \Rightarrow p$, Fall $\neg q \Rightarrow p$

- Beweis durch Widerspruch: „Es gilt p“ wird gezeigt durch:

$$\left.\begin{array}{l}\text{Annahme } \neg p \Rightarrow q \\ \text{Annahme } \neg p \Rightarrow \neg q\end{array}\right\} \implies \text{Widerspruch}$$

Zum Abschluss wollen wir den Unterschied zwischen logischen und sachbezogenen Schlüssen noch anhand von zwei Bauernregeln illustrieren:

> „Kräht der Hahn früh auf dem Mist, ändert sich das Wetter, oder es bleibt, wie es ist.“

Die Aussage $p \Rightarrow q \vee \neg q$ ist eine Tautologie, daher handelt es sich um einen logischen Schluss.

> „Wenn's zu Silvester stürmt und schneit, ist das neue Jahr nicht weit.“

Der Schluss $p \wedge q \Rightarrow t$ ist sachbezogen, denn Silvester ist der letzte Tag im (alten) Jahr.

2. Prädikatenlogik

Diese Logik handelt von Aussageformen (=Prädikaten), d.h. von Aussagen, die eine oder mehrere *freie* Variablen enthalten.

Beispiele. 12 ist durch 3 teilbar: Aussage
n ist gerade: Aussageform

Eine Aussageform hat per se keinen Wahrheitswert, dieser hängt von den eingesetzten Objekten ab. Durch das Versehen jeder freien Variable mit einem *Quantor* wird die Aussageform zu einer Aussage (die Variablen werden gebunden) und deren Wahrheitswert gibt dann Aufschluss, ob und gegebenenfalls welche Objekte eingesetzt werden dürfen.

Beispiele.

- $k \mid n$ ist eine Aussageform und
$$\forall n : \exists k : k \mid n$$
ergibt eine wahre Aussage (setze $k = n$).
Ebenso ergibt
$$\exists k : \forall n : k \mid n$$
eine wahre Aussage (setze $k = 1$).
- $5 \mid 12$ ist eine falsche Aussage.
- $3 \mid 12$ ist eine wahre Aussage.

Wir verwenden den	Bedeutung
• Allquantor $\forall$	für alle...
• Existenzquantor $\exists$	es existiert mindestens ein...

Weiters werwenden wir $\exists!$ für „es existiert genau ein“. Dies ist kein neuer Quantor, sondern $\exists! x : A(x)$ ist lediglich eine Abkürzung für

$$\exists x : A(x) \wedge (\forall x_1 \forall x_2 : A(x_1) \wedge A(x_2) \Rightarrow x_1 = x_2)$$

Beispiel (Existenz der n-ten Wurzel einer positiven reellen Zahl). Für alle $a \in \mathbb{R}$ mit $a > 0$ und alle $n \in \mathbb{N}$ mit $n > 0$ gibt es (genau) ein $x \in \mathbb{R}$ mit $x > 0$ und $x^n = a$:

$$\forall a : a \in \mathbb{R} \wedge a > 0 \Rightarrow (\forall n : n \in \mathbb{N} \wedge n > 0 \Rightarrow \exists(!) x : x \in \mathbb{R} \wedge x > 0 \wedge x^n = a).$$

Bemerkung. Häufig treten Quantoren versteckt auf. Die Aussage $f : \mathbb{R} \to \mathbb{R}$ ist konstant entspricht

$$\exists y \in \mathbb{R} : \forall x \in \mathbb{R} : f(x) = y.$$

Eine Variable mit Quantor ist keine freie Variable mehr! Der Name einer Variablen ist egal:

$$\forall x \in \mathbb{N} : x \geq 0 \quad \text{ist dasselbe wie} \quad \forall y \in \mathbb{N} : y \geq 0$$

Beispiele (Freie und gebundene Variablen). Seien $A(x)$ und $B(x, y)$ Aussageformen:

- $A(x)$ — x ist frei
- $\forall x : A(x)$ — x ist gebunden
- $\exists y : B(x, y)$ — y gebunden, x frei

Meist kommen Quantoren in Beweisen „versteckt“ vor, die Formulierungen lauten z.B:

- $\forall x \in M : A(x)$ — Sei $x \in M$ (beliebig). ... Dann gilt $A(x)$.
- $\exists x \in M : A(x)$ — Wähle $x := \ldots$ Dann gilt $A(x)$.
- $\exists! x \in M : A(x)$ — Wähle $x := \ldots$ Dann gilt $A(x)$. Seien $x_1, x_2 \in M$ mit $A(x_1)$ und $A(x_2)$. Dann gilt $x_1 = x_2$.

Beispiele (Verneinung von Aussagen mit Quantoren).

$$\neg\big(\forall x : A(x)\big) = \big(\exists x : \neg A(x)\big)$$
$$\neg\big(\exists x : A(x)\big) = \big(\forall x : \neg A(x)\big)$$
$$\neg\big(\exists! x : A(x)\big) = \big(\forall x : \neg A(x)\big) \vee \big(\exists x_1, x_2 : x_1 \neq x_2 \wedge A(x_1) \wedge A(x_2)\big)$$

Beispiele (Äquivalente Umformungen mit Quantoren).

$$\big(\exists x : P(x) \vee Q(x)\big) = \big(\exists x : P(x)\big) \vee \big(\exists x : Q(x)\big)$$
$$\big(\forall x : P(x) \wedge Q(x)\big) = \big(\forall x : P(x)\big) \wedge \big(\forall x : Q(x)\big)$$

Beispiele (Nicht äquivalente Umformungen mit Quantoren).

$$\big(\exists x : P(x) \wedge Q(x)\big) \Rightarrow \big(\exists x : P(x)\big) \wedge \big(\exists x : Q(x)\big)$$
$$\big(\forall x : P(x) \vee Q(x)\big) \Leftarrow \big(\forall x : P(x)\big) \vee \big(\forall x : Q(x)\big)$$

Man setze z.B. für ganze Zahlen $P(x) \ldots x$ gerade, $Q(x) \ldots x$ ungerade.

Das Verwenden mehrerer Quantoren hintereinander:

- gleiche Quantoren sind vertauschbar. Seien $a, b \in \mathbb{R}$:

  $$\big(\forall a : \forall b : (a+b)^2 = a^2 + 2ab + b^2\big) = \big(\forall b : \forall a : (a+b)^2 = a^2 + 2ab + b^2\big)$$

  Wir schreiben daher auch $\forall a, b : (a+b)^2 = a^2 + 2ab + b^2$.
- verschiedene Quantoren sind nicht vertauschbar:

  $$\forall a \in \mathbb{R} : \exists (f : \mathbb{R} \longrightarrow \mathbb{R}) : f(a) = 0$$

  z.B. $f(x) = x - a$. Für jedes a gibt es viele Funktionen, die a als Nullstelle haben. Auch die folgende Aussage ist wahr:

  $$\exists (f : \mathbb{R} \longrightarrow \mathbb{R}) : \forall a \in \mathbb{R} : f(a) = 0$$

  Jedoch gilt dies nur für die Funktion $f = 0$.

Beispiel (Konvergenz von Folgen). Sei $x \in \mathbb{R}$, $x_0, x_1, x_2, x_3, \ldots$ eine Folge reeller Zahlen. Die Folge $(x_n)_{n \in \mathbb{N}}$ konvergiert gegen x, wenn gilt:

$$\forall \varepsilon > 0 : \exists N \in \mathbb{N} : \forall n \geq N : |x - x_n| < \varepsilon$$

Die Negation lautet:

$$\exists \varepsilon > 0 : \forall N \in \mathbb{N} : \exists n \geq N : |x - x_n| \geq \varepsilon$$

KAPITEL 3

Mengenlehre

1. Naive Mengenlehre

Wir verwenden den „naiven“ Mengenbegriff von Georg Cantor:

> „Unter einer Menge verstehen wir jede Zusammenfassung M von bestimmten wohlunterschiedenen Objekten m unserer Anschauung oder unseres Denkens (welche die Elemente von M genannt werden) zu einem Ganzen.“

Beispiele. Menge der Studierenden im HS, Menge der ganzen Zahlen, Menge der Punkte auf dem Einheitskreis.

Wie kann man Mengen definieren, angeben oder spezifizieren?

- Aufzählen der Elemente bei endlichen Mengen: $5 \in M$ heißt 5 liegt in M.
  $M = \{0, 2, 5\} = \{0, 2, 2, 5, 5, 5\} \ldots 3$ Elemente.
  M darf auch andere Mengen als Elemente haben.
- Spezifizieren der Elemente einer Menge durch eine charakteristische Eigenschaft – eignet sich auch für unendliche Mengen:

$$A := \{x \mid x \in X \wedge A(x)\} = \{x \in X \mid A(x)\} \quad \text{oder} \quad A := \{x \in X : A(x)\}$$

Beispiele. Die Menge der Quadratzahlen:

$$A = \{x \mid x \in \mathbb{N} \wedge (\exists y \in \mathbb{N} : y^2 = x)\} = \{x \in \mathbb{N} \mid \exists y \in \mathbb{N} : y^2 = x)\}$$

Implizite – explizite Beschreibung:

$$L = \{x \in \mathbb{R} \mid x^3 - 6x^2 + 11x - 6 = 0\} = \{1, 2, 3\}$$

Wesentliche Begriffe aus der naiven Mengenlehre:

- Gleichheit von Mengen (Extensionalitätsprinzip):

$$A = B :\Leftrightarrow \forall x : (x \in A \Leftrightarrow x \in B)$$

- Leere Menge:

$$\emptyset := \{x \mid x \neq x\} \quad \text{(eventuell auch } \{\}\text{)}$$

  Achtung: $\{\emptyset\}$ ist nicht die leere Menge! $\{\emptyset\}$ ist die Menge, deren einziges Element die leere Menge ist. $\emptyset$ ist eindeutig bestimmt!
- Teilmengen:

$$B \subseteq A :\Leftrightarrow \forall x : (x \in B \Rightarrow x \in A)$$

  Insbesondere gilt daher $A \subseteq A$ für alle Mengen A.

Proposition 1.1. *Für jede Menge A gilt $\emptyset \subseteq A$.*

Beweis. Zu zeigen ist $x \in \emptyset \Rightarrow x \in A$. Da aber die Voraussetzung $x \in \emptyset$ nie erfüllt ist, folgt $x \in A$ unabhängig von x. □

Die Mengen $\emptyset$ und A bezeichen wir auch als triviale Teilmengen von A, alle anderen Teilmengen als echte Teilmengen von A. Wenn $B \subseteq A$ und $B \neq A$, dann schreiben wir $B \subset A$ oder noch eindeutiger $B \subsetneqq A$ bzw. $B \subsetneq A$. Mitunter wird beim Symbol $B \subset A$ auch die Gleichheit zugelassen und dann für echte Teilmengen $B \subsetneqq A$ verwendet.

PROPOSITION 1.2. *Sei A eine endliche Menge mit $n \in \mathbb{N}$ Elementen (wir schreiben dann $|A| = n$). Dann gibt es 2^n verschiedene Teilmengen von A.*

BEWEIS. Seien $x_1, \ldots, x_n$ die Elemente von A. Jede Teilmenge von A ist eindeutig durch diejenigen x_i bestimmt, welche in der Teilmenge liegen. Daher besteht für jedes Element x_i die Möglichkeit in A zu liegen (1) oder nicht (0). Es gilt:

$$\#TM \quad = \quad \#\text{Funktionen von } \{x_1, \ldots, x_n\} \longrightarrow \{0,1\} \quad = \quad 2^n$$

□

PROPOSITION 1.3. *Seien A und B Mengen. Dann gilt $A = B \quad \Leftrightarrow \quad A \subseteq B \wedge B \subseteq A$.*

BEWEIS.

$$\begin{aligned} A = B &\Leftrightarrow \forall x : (x \in A \Leftrightarrow x \in B) \\ &\Leftrightarrow \forall x : \big((x \in A \Rightarrow x \in B) \wedge (x \in B \Rightarrow x \in A)\big) \\ &\Leftrightarrow (\forall x : x \in A \Rightarrow x \in B) \wedge (\forall x : x \in B \Rightarrow x \in A) \\ &\Leftrightarrow A \subseteq B \wedge B \subseteq A \end{aligned}$$

□

Mengenoperationen. Die Mengenoperationen werden durch Aussagen über Elemente und die logischen Junktoren definiert, daher die Ähnlichkeiten der Symbole mit den logischen Symbolen.

$$\begin{aligned} A \cup B &:= \{x \mid x \in A \vee x \in B\} && \ldots \text{ Vereinigung, die Existenz wird per Axiom postuliert} \\ A \cap B &:= \{x \mid x \in A \wedge x \in B\} = \{x \in A \cup B \mid x \in A \wedge x \in B\} && \ldots \text{ Durchschnitt} \\ A \setminus B &:= \{x \mid x \in A \wedge x \notin B\} && \ldots \text{ Mengendifferenz} \\ A \Delta B &:= \{x \mid x \in A \wedge x \notin B\} \cup \{x \mid x \in B \wedge x \notin A\} \\ &= (A \setminus B) \cup (B \setminus A) = (A \cup B) \setminus (A \cap B) && \ldots \text{ symmetrische Differenz} \end{aligned}$$

Zwei Mengen A und B mit $A \cap B = \emptyset$ heißen *disjunkt*. Die Operationen $\cup$ und $\cap$ können auf beliebig viele Mengen (eine Mengenfamilie, d.h. eine Menge von Mengen) ausgedehnt werden. Meist verwenden wir dazu eine Indexmenge I.

DEFINITION. Sei $(A_i)_{i \in I}$ eine Mengenfamilie:

$$\bigcup_{i \in I} A_i := \{x \mid \exists i \in I : x \in A_i\}$$

$$\bigcap_{i \in I} A_i := \{x \mid \forall i \in I : x \in A_i\}$$

BEISPIELE. $M \cup \emptyset = M, \quad M \setminus \emptyset = M, \quad M \cap \emptyset = \emptyset$

$$\mathbb{Z} = \bigcup_{n \in \mathbb{N}} \{-n, n\}$$

$$\mathbb{Q} = \bigcup_{n \in \mathbb{Z}} \bigcup_{m \in \mathbb{N} \setminus \{0\}} \left\{\frac{n}{m}\right\}$$

BEMERKUNG. Meist arbeitet man mit einer vorgegebenen Grundmenge (Universum, Universalmenge) und spezifiziert verschieden Teilmengen davon, z.B.

$U = \mathbb{R}^n$

TM: $(n-1)$-dimensionale Teilräume (auch Hyperebenen)

Innerhalb einer solchen Grundmenge wird der Begriff des Komplements definiert:

DEFINITION. Sei U eine Grundmenge und $A \subseteq U$. Dann heißt $A^c := U \setminus A$ das Komplement von A (in U).

BEISPIEL. $U = \mathbb{R}, \quad A = [1,2] \quad \Rightarrow \quad A^c = (-\infty, 1) \cup (2, \infty)$.

Rechenregeln für Mengenoperationen. Diese sind analog den betreffenden Rechenregeln für logische Junktoren. Komplementierungen (in einer vorgegebenen Grundmenge U) werden als $A^c = U \setminus A$ angeschrieben und in die Negation übersetzt.

- Kommutativgesetze: $A \cap B = B \cap A$, $A \cup B = B \cup A$
- Assoziativgesetze: $A \cap (B \cap C) = (A \cap B) \cap C$
  $A \cup (B \cup C) = (A \cup B) \cup C$
- Distributivgesetze: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
  $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- Gesetze von De Morgan: $C \setminus (A \cap B) = (C \setminus A) \cup (C \setminus B)$, $(A \cap B)^c = A^c \cup B^c$
  $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$, $(A \cup B)^c = A^c \cap B^c$

BEISPIEL. Zu zeigen ist $C \setminus (A \cup B) = (C \setminus A) \cap (C \setminus B)$.

$$\begin{aligned}
x \in C \setminus (A \cup B) &\Leftrightarrow x \in C \wedge x \notin A \cup B \\
&\Leftrightarrow x \in C \wedge \neg(x \in A \cup B) \\
&\Leftrightarrow x \in C \wedge \neg(x \in A \vee x \in B) \\
&\Leftrightarrow x \in C \wedge (\neg x \in A \wedge \neg x \in B) \\
&\Leftrightarrow (x \in C \wedge \neg x \in A) \wedge (x \in C \wedge \neg x \in B) \\
&\Leftrightarrow (x \in C \wedge x \notin A) \wedge (x \in C \wedge x \notin B) \\
&\Leftrightarrow (x \in C \setminus A) \wedge (x \in C \setminus B) \\
&\Leftrightarrow x \in (C \setminus A) \cap (C \setminus B)
\end{aligned}$$

BEISPIEL. Zu zeigen ist $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

$$\begin{aligned}
x \in A \cap (B \cup C) &\Leftrightarrow x \in A \wedge x \in B \cup C \\
&\Leftrightarrow x \in A \wedge (x \in B \vee x \in C) \\
&\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \in C) \\
&\Leftrightarrow x \in A \cap B \vee x \in A \cap C \\
&\Leftrightarrow x \in (A \cap B) \cup (A \cap C)
\end{aligned}$$

BEMERKUNG. Die De Morgan Gesetze gelten auch für beliebige Vereinigungen und Durchschnitte:

$$C \setminus \Big(\bigcup_{i \in I} A_i\Big) = \bigcap_{i \in I} (C \setminus A_i) \qquad C \setminus \Big(\bigcap_{i \in I} A_i\Big) = \bigcup_{i \in I} (C \setminus A_i)$$

Wenn eine Universalmenge U existiert, dann gilt:

$$\Big(\bigcup_{i \in I} A_i\Big)^c = \bigcap_{i \in I} A_i^c \qquad \Big(\bigcap_{i \in I} A_i\Big)^c = \bigcup_{i \in I} A_i^c$$

Wir zeigen die zweite Identität:

$$\begin{aligned} x \in C \setminus \Big(\bigcap_{i\in I} A_i\Big) &\Leftrightarrow x \in C \wedge \neg x \in \Big(\bigcap_{i\in I} A_i\Big) \\ &\Leftrightarrow x \in C \wedge \neg\big(\forall i \in I : x \in A_i\big) \\ &\Leftrightarrow x \in C \wedge \exists i \in I : \neg x \in A_i \\ &\Leftrightarrow \exists i \in I : (x \in C \wedge \neg x \in A_i) \\ &\Leftrightarrow \exists i \in I : (x \in C \setminus A_i) \\ &\Leftrightarrow x \in \bigcup_{i\in I} (C \setminus A_i) \end{aligned}$$

Potenzmenge.

DEFINITION. Sei M eine Menge. Dann definieren wir $\mathcal{P}(M) := \{A \mid A \subseteq M\}$.

BEISPIELE. (1) $\mathcal{P}(\emptyset) = \{\emptyset\}$
(2) $M = \{1,2,3\} \Rightarrow \mathcal{P}(M) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, M\}$
(3) $|M| = n \Rightarrow |\mathcal{P}(M)| = 2^n$
(4) Auch bei unendlichen Mengen besitzt die Potenzmenge eine größere Kardinalität.

Geordnete Paare, geordnete n-Tupel. Für $a, b \in M$ gilt $\{a,b\} = \{b,a\}$, d.h. die Ordnung wird nicht beachtet. Wir definieren geordnete Paare durch $(a,b) := \{\{a\}, \{a,b\}\}$. Es gilt

$$(a_1, b_1) = (a_2, b_2) \Leftrightarrow a_1 = a_2 \wedge b_1 = b_2.$$

DEFINITION. Seien A, B Mengen. Wir definieren die Produktmenge durch

$$A \times B := \{(a,b) \mid a \in A, b \in B\}.$$

Für endlich viele Mengen $A_1, A_2, \ldots, A_n$ setzen wir

$$\prod_{i=1}^{n} A_i = \{(a_1, \ldots, a_n) \mid a_i \in A_i \text{ für } i = 1, \ldots, n\}.$$

Für $A \times A$ schreiben wir auch A^2, analog auch A^n. Bei beliebig vielen Mengen $(A_i)_{i\in I}$ benötigen wir den Begriff der Abbildung:

$$x \in \prod_{i\in I} A_i \text{ entspricht einer Abbildung } f : I \longrightarrow \bigcup_{i\in I} A_i \text{ mit } \forall i \in I : f(i) \in A_i$$

BEMERKUNG. Die Produktmenge ist zu unterscheiden vom Mengenprodukt bei Verknüpfungen:

$$AB := \{x \mid \exists a \in A, b \in B \text{ mit } x = ab\}.$$

2. Relationen

DEFINITION. Seien X, Y Mengen. Eine Relation zwischen X und Y ist ein Tripel (X, Y, R) mit $R \subseteq X \times Y$. Im Fall $X = Y$ sprechen wir auch von einer Relation auf X. Für $(x,y) \in R$ schreiben wir auch xRy.

BEISPIEL.
M: Menge der Menschen
R: ... raucht die selbe Zigarettenmarke wie ...

DEFINITION (Eigenschaften von Relationen). Sei X eine Menge und $R \subseteq X \times X$ eine Relation auf X. R heißt

(R)	reflexiv	$:\Leftrightarrow \forall x \in X : xRx$
(S)	symmetrisch	$:\Leftrightarrow \forall x, y \in X : xRy \Rightarrow yRx$
(T)	transitiv	$:\Leftrightarrow \forall x, y, z \in X : xRy \wedge yRz \Rightarrow xRz$
(AS)	antisymmetrisch	$:\Leftrightarrow \forall x, y \in X : xRy \wedge yRx \Rightarrow x = y$

Eine Relation mit den Eigenschaften (R), (S), (T) bezeichen wir als *Äquivalenzrelation.* Bei einer Äquivalenzrelation schreiben wir $x \sim y$ (statt xRy).
Eine Relation mit den Eigenschaften (R), (AS), (T) bezeichen wir als *Ordnungsrelation.*

BEISPIELE.
... ist verwandt mit ... $\longrightarrow$ nicht transitiv
... ist Bruder von ... $\longrightarrow$ nicht symmetrisch
... wohnt im selben Ort wie ... $\longrightarrow$ Äquivalenzrelation

BEISPIEL. Die Kongruenzrelation $\equiv$ auf $\mathbb{Z}$ definiert durch $k \equiv l :\Leftrightarrow n \mid k - l$ mit einer festen Zahl $n \in \mathbb{N} \setminus \{0\}$ ist eine Äquivalenzrelation. Wir schreiben $k \equiv l(n)$. Beweis als Übung.

DEFINITION. Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Für $a \in M$ heißt

$$[a] := \{b \in M \mid b \sim a\} \quad \text{(oder auch } \bar{a}\text{)}$$

die Äquivalenzklasse von a.

PROPOSITION 2.1 (Eigenschaften von Äquivalenzklassen).
(1) $\forall a \in M : [a] \neq \emptyset$
(2) $\bigcup_{a \in M} [a] = M$
(3) $\forall a, b \in M : [a] \cap [b] \neq \emptyset \Rightarrow [a] = [b]$

BEWEIS. (1): Wegen (R) gilt $a \in [a]$.
(2): Es gilt $M = \bigcup_{a \in M} \{a\} \subseteq \bigcup_{a \in M} [a] \subseteq M$.
(3): Aus $c \in [a] \cap [b]$ folgt mit (S) und (T) $c \sim a \wedge c \sim b \Rightarrow a \sim c \wedge c \sim b \Rightarrow a \sim b$. Für $d \in [a]$ folgt mit (T) $d \sim a \wedge a \sim b \Rightarrow d \sim b$, daher $[a] \subseteq [b]$. Wegen (S) gilt auch $b \sim a$ und es folgt analog $[b] \subseteq [a]$ und damit $[a] = [b]$. □

DEFINITION (Quotientenmenge). Sei $\sim$ eine Äquivalenzrelation auf M. Die Menge

$$\{[a] \mid a \in M\} =: M/\sim$$

heißt die *Quotientenmenge* oder *Faktormenge* von M nach $\sim$.

BEMERKUNG. Eine Äquivalenzrelation auf M erzeugt eine Familie von

- *nichtleeren* Teilmengen von M,
- die ganz M überdecken (die Vereinigung ist ganz M),
- sodass zwei verschiedene Mitglieder immer disjunkt sind.

Eine derartige Familie von Mengen nennt man eine Partition von M.

DEFINITION (Disjunktheit von Mengen).
A, B disjunkt $:\Leftrightarrow A \cap B = \emptyset$ (Achtung: $\emptyset$ und $\emptyset$ sind gleich und disjunkt!)
Nun sei $(A_i)_{i \in I}$ eine Familie von Mengen:

- $(A_i)_{i \in I}$ disjunkt $:\Leftrightarrow \bigcap_{i \in I} A_i = \emptyset$
- $(A_i)_{i \in I}$ *paarweise* disjunkt $:\Leftrightarrow \forall i, j \in I : i \neq j \Rightarrow A_i \cap A_j = \emptyset$ (Wenn $|I| \geq 2$ gilt, dann folgt aus paarweiser Disjunktheit die Disjunktheit.)

SATZ 2.2. *Sei M eine Menge und $(U_i)_{i\in I}$ eine Partition von M. Dann definiert*

$$x \sim y \quad :\Leftrightarrow \quad \exists i \in I : x \in U_i \wedge y \in U_i$$

eine Äquivalenzrelation auf M.

BEWEIS. Jedes Element $x \in M = \bigcup_{i\in I} U_i$ ist in einer Menge U_i mit $i \in I$ enthalten, daher folgt $x \sim x$ und es gilt (R).

Die Definition von $\sim$ ist offensichtlich symmetrisch, daher gilt (S).

Wenn $x \sim y$ und $y \sim z$ gelten, dann existieren $i, j \in I$ mit $x, y \in U_i$ und $y, z \in U_j$. Wegen $y \in U_i \cap U_j$ folgt aus der paarweisen Disjunktheit $i = j$ und damit $x \sim z$, daher gilt (T). □

BEMERKUNG. Die Konstruktionen in Proposition 2.1 und Satz 2.2 sind invers zueinander, eine Äquivalenzrelation erzeugt eine Partition und umgekehrt.

BEISPIEL. Sei $\sim$ definiert durch $\equiv (n)$ mit einer Zahl $n \in \mathbb{N} \setminus \{0\}$ (auch mit $\equiv (\mathrm{mod}\, n)$ bezeichnet). Die Äquivalenzklassen (auch Kongruenzklassen) sind $[0], [1], \ldots, [n-1]$. Wir schreiben $\mathbb{Z}_n := \mathbb{Z}/\sim$. Damit ist $\mathbb{Z}_n$ als Menge definiert, später werden wir noch Operationen $+$ und $\cdot$ auf $\mathbb{Z}_n$ definieren und $\mathbb{Z}_n$ zum Restklassenring machen.

DEFINITION. Sei M eine Menge und $\leq$ eine Relation auf M mit den Eigenschaften (R), (AS) und (T). Dann heißt $\leq$ eine Ordnungsrelation oder *partielle Ordnung* auf M und $(M, \leq)$ heißt eine *geordnete Menge*.

Wenn zwei beliebige Elemente $x, y \in M$ immer vergleichbar sind, d.h.

$$\forall x, y \in M : x \leq y \vee y \leq x$$

gilt, dann bezeichnen wir $\leq$ als *Totalordnung* oder *lineare Ordnung*.

BEMERKUNG. Wir definieren $x \geq y :\Leftrightarrow y \leq x$ und $x < y :\Leftrightarrow x \leq y \wedge x \neq y$.

BEISPIELE.
- $\leq$ ist eine Totalordnung auf den reellen Zahlen $\mathbb{R}$.
- $\subseteq$ liefert eine partielle Ordnung auf $\mathcal{P}(M)$.
- $|$ definiert eine partielle Ordnung auf $\mathbb{N}$.
- Seien $(A, \leq)$ und $(B, \preceq)$ zwei geordnete Mengen. Dann ist durch

$$(a, b) \trianglelefteq (a', b') :\Leftrightarrow a < a' \vee (a = a' \wedge b \preceq b')$$

eine Ordnungsrelation auf $A \times B$ definiert.

DEFINITION. Sei $(M, \leq)$ eine geordnete Menge und sei $E \subseteq M$.

(1) Ein Element $\beta \in M$ heißt obere Schranke von E, falls $\forall x \in E : x \leq \beta$ gilt $(E \leq \beta)$.
(2) Ein Element $\alpha \in M$ heißt untere Schranke von E, falls $\forall x \in E : \alpha \leq x$ gilt $(\alpha \leq E)$.

Die Menge E heißt nach oben bzw. nach unten beschränkt, wenn eine obere bzw. eine untere Schranke von E existieren.

BEISPIELE (Intervalle in $\mathbb{R}$). Seien $a, b \in \mathbb{R}$ mit $a < b$:

$$(a, b) = \{x \in \mathbb{R} \mid a < x < b\}$$
$$[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$$
$$[a, b) = \{x \in \mathbb{R} \mid a \leq x < b\}$$
$$(a, b] = \{x \in \mathbb{R} \mid a < x \leq b\}$$

$E := [0, 1]$: jedes $x \geq 1$ ist eine obere Schranke.
$M := \{\frac{1}{n} \mid n = 1, 2, \ldots\}$: 1 ist eine obere Schranke, 0 ist eine untere Schranke.
Primzahlen $\mathbb{P}$: nach oben nicht beschränkt, 2 ist eine untere Schranke.

Eine obere bzw. untere Schranke sind nicht notwendigerweise eindeutig definiert, jedoch sind das Supremum und das Infimum (sofern sie existieren) eindeutig.

DEFINITION. Sei $(M, \leq)$ eine geordnete Menge und sei $E \subseteq M$.

(1) Ein Element $\beta = \sup E \in M$ ist die *kleinste obere Schranke (Supremum)* von E, wenn die Bedingungen $E \leq \beta$ und $\forall \gamma \in M : E \leq \gamma \Rightarrow \beta \leq \gamma$ gelten.
(2) Ein Element $\alpha = \inf E \in M$ ist die *größte untere Schranke (Infimum)* von E, wenn die Bedingungen $\alpha \leq E$ und $\forall \gamma \in M : \gamma \leq E \Rightarrow \gamma \leq \alpha$ gelten.

BEMERKUNGEN. Supremum und Infimum müssen nicht existieren! Z.B. bei einer partiellen Ordnung wegen mangelnder Vergleichbarkeit von Elementen. Auch bei der Totalordnung auf dem Intervall $M = (-1, 1)$ hat die Menge $E = (0, 1)$ ein Infimum $\inf E = 0$ aber kein Supremum (dieses muss ein Element von M sein).

Die Eindeutigkeit von Supremum bzw. Infimum folgt (so sie existieren) aus (AS).

Wenn das Supremum bzw. Infimum Elemente von E sind, dann bezeichnet man sie als Maximum bzw. Minimum.

BEISPIELE.
- $M = \mathbb{R}$, $E = (0, 1)$: $\sup E = 1, \inf E = 0$.
- $E = \{x \in \mathbb{Q} \mid x > 0 \wedge x^2 < 2\}$: $\sup E = \sqrt{2}$ bei $M = \mathbb{R}$, aber kein Supremum bei $M = \mathbb{Q}$.
- $E = \{\frac{1}{n} \mid n = 1, 2, 3 \dots\}$: $\max E = 1$, kein Minimum.

3. Abbildungen (Funktionen)

Seien A und B Mengen. Eine Abbildung $f : A \longrightarrow B$ ist eine Vorschrift, die jedem $a \in A$ genau ein $b \in B$ zuordnet.

- Für $a \in A$ bezeichnen wir $f(a)$ als das *Bild (Funktionswert)* von a unter f.
- $a \dots$ *Argument*
- Wenn $f(a) = b$, dann ist a ein *Urbild* von b unter f.
- $A \dots$ *Definitionsbereich*, $B \dots$ *Zielbereich*; beide gehören zur Abbildung!

$$\begin{aligned} f : & A \longrightarrow B \\ & a \longmapsto b \end{aligned}$$

- Die Funktion f ist zu unterscheiden vom Funktionswert $f(a)$ bei $a \in A$.

Was bedeutet Vorschrift? Darf man die Funktionswerte „würfeln“?

DEFINITION. Eine Abbildung ist ein Tripel (A, B, G) bestehend aus Mengen A (Definitionsbereich) und B (Zielbereich) und einer Relation $G \subseteq A \times B$ zwischen A und B mit den folgenden Eigenschaften:

(1) $\forall a \in A : \exists b \in B : (a, b) \in G$ (jedes $a \in A$ besitzt ein Bild)
(2) $\forall a \in A : \forall b_1, b_2 \in B : (a, b_1) \in G \wedge (a, b_2) \in G \Rightarrow b_1 = b_2$ (Eindeutigkeit)

Wir schreiben dann $G = G(f) = \{(a, f(a)) \mid a \in A\}$ und bezeichnen mit G den Graphen von f.

BEMERKUNGEN. Die beiden Bedingungen können durch die Bedingung (1) mit dem Quantor $\exists!$ ersetzt werden.

Eine Abbildung kann auch als Relation R zwischen A und B mit der Bedingung

$$\forall a \in A : \exists! b \in B : aRb$$

eingeführt werden.

BEISPIELE. $A = B = \mathbb{R}, f(x) = x^2 \Rightarrow G(f) = \{(x, x^2) \mid x \in \mathbb{R}\}$
$A = B = \mathbb{R}^+, g(x) = x^2 \Rightarrow G(g) = \{(x, x^2) \mid x \in \mathbb{R}^+\}$
Die Funktionen f und g sind verschieden!

DEFINITION (Quotientenabbildung). Sei M eine Menge und $\sim$ eine Äquivalenzrelation auf M. Die Quotientenabbildung

$$\begin{aligned} q : M &\longrightarrow M/\sim \\ a &\longmapsto [a] \end{aligned}$$

ordnet jedem $a \in M$ seine Äquivalenzklasse zu.

DEFINITION (Bild und Urbild von Mengen). Sei $f : A \longrightarrow B$ eine Abbildung. Für eine Teilmenge $M \subseteq A$ definieren wir das *Bild* von M unter f als

$$f(M) := \{b \in B \mid \exists a \in M : f(a) = b\} \quad (= \{f(a) \mid a \in M\})$$

und für eine Teilmenge $N \subseteq B$ definieren wir das *Urbild* von N unter f als

$$f^{-1}(N) := \{a \in A \mid f(a) \in N\}.$$

BEISPIELE. Sei $f : \mathbb{R} \longrightarrow \mathbb{R}$ mit $f(x) = x^2$.
$M := [-1, 1] \Rightarrow f(M) = [0, 1]$
$N := [-4, 4] \Rightarrow f^{-1}(N) = [-2, 2]$
$N := \{9\} \Rightarrow f^{-1}(N) = \{-3, 3\}$

SATZ 3.1 (Kompatibilität mit Mengenoperationen). *Sei $f : A \longrightarrow B$ eine Abbildung und seien $A_i \subseteq A$ und $B_i \subseteq B$. Dann gelten folgende Aussagen:*

(1) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$
(2) $f(A_1 \cap A_2) \subseteq f(A_1) \cap f(A_2)$
(3) $f(A_1 \setminus A_2) \supseteq f(A_1) \setminus f(A_2)$
(4) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$
(5) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$
(6) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$

BEWEIS. (1): $b \in f(A_1 \cup A_2) \Leftrightarrow \exists a \in A_1 \cup A_2 : f(a) = b \Leftrightarrow$
$\Leftrightarrow \exists a : (a \in A_1 \vee a \in A_2) \wedge f(a) = b \Leftrightarrow \exists a : (a \in A_1 \wedge f(a) = b) \vee (a \in A_2 \wedge f(a) = b) \Leftrightarrow$
$\Leftrightarrow (\exists a : a \in A_1 \wedge f(a) = b) \vee (\exists a : a \in A_2 \wedge f(a) = b) \Leftrightarrow b \in f(A_1) \vee b \in f(A_2) \Leftrightarrow$
$\Leftrightarrow b \in f(A_1) \cup f(A_2)$
(2): $b \in f(A_1 \cap A_2) \Leftrightarrow \exists a \in A_1 \cap A_2 : f(a) = b \Leftrightarrow \exists a : (a \in A_1 \wedge a \in A_2) \wedge f(a) = b \Leftrightarrow$
$\Leftrightarrow \exists a : (a \in A_1 \wedge f(a) = b) \wedge (a \in A_2 \wedge f(a) = b) \Rightarrow$
$\Rightarrow (\exists a : a \in A_1 \wedge f(a) = b) \wedge (\exists a : a \in A_2 \wedge f(a) = b) \Leftrightarrow b \in f(A_1) \wedge b \in f(A_2) \Leftrightarrow$
$\Leftrightarrow b \in f(A_1) \cap f(A_2)$
(3): $b \in f(A_1) \setminus f(A_2) \Leftrightarrow b \in f(A_1) \wedge b \notin f(A_2) \Leftrightarrow$
$\Leftrightarrow (\exists a \in A_1 : f(a) = b) \wedge \neg(\exists a' \in A_2 : f(a') = b) \Leftrightarrow$
$\Leftrightarrow (\exists a \in A_1 : f(a) = b) \wedge (\forall a' : a' \notin A_2 \vee f(a') \neq b) \overset{\text{setze } a'=a}{\Rightarrow} \exists a \in A_1 : f(a) = b \wedge a \notin A_2 \Leftrightarrow$
$\Leftrightarrow \exists a \in A_1 \setminus A_2 : f(a) = b \Leftrightarrow b \in f(A_1 \setminus A_2)$
(4): $a \in f^{-1}(B_1 \cup B_2) \Leftrightarrow f(a) \in B_1 \cup B_2 \Leftrightarrow f(a) \in B_1 \vee f(a) \in B_2 \Leftrightarrow$
$\Leftrightarrow a \in f^{-1}(B_1) \vee a \in f^{-1}(B_2) \Leftrightarrow a \in f^{-1}(B_1) \cup f^{-1}(B_2)$
(5): $a \in f^{-1}(B_1 \cap B_2) \Leftrightarrow f(a) \in B_1 \cap B_2 \Leftrightarrow f(a) \in B_1 \wedge f(a) \in B_2 \Leftrightarrow$
$\Leftrightarrow a \in f^{-1}(B_1) \wedge a \in f^{-1}(B_2) \Leftrightarrow a \in f^{-1}(B_1) \cap f^{-1}(B_2)$
(6): $a \in f^{-1}(B_1 \setminus B_2) \Leftrightarrow f(a) \in B_1 \setminus B_2 \Leftrightarrow f(a) \in B_1 \wedge f(a) \notin B_2 \Leftrightarrow$
$\Leftrightarrow a \in f^{-1}(B_1) \wedge a \notin f^{-1}(B_2) \Leftrightarrow a \in f^{-1}(B_1) \setminus f^{-1}(B_2)$ □

BEMERKUNG. Für die Urbilder gilt immer die Gleichheit der betreffenden Mengen, für die Bilder nur bei der Vereinigung.

DEFINITION. Sei $f : A \longrightarrow B$ eine Abbildung.

(1) f heißt *injektiv*, wenn

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2)$$
$$(\Leftrightarrow \quad \forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2).$$

(2) f heißt *surjektiv*, wenn

$$\forall b \in B : \exists a \in A : f(a) = b.$$

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

BEISPIELE.

$f_1 : \mathbb{R} \longrightarrow \mathbb{R}$	$x \longmapsto x^2$	weder injektiv noch surjektiv
$f_2 : \mathbb{R}_0^+ \longrightarrow \mathbb{R}$	$x \longmapsto x^2$	injektiv
$f_3 : \mathbb{R} \longrightarrow \mathbb{R}_0^+$	$x \longmapsto x^2$	surjektiv
$f_4 : \mathbb{R}_0^+ \longrightarrow \mathbb{R}_0^+$	$x \longmapsto x^2$	bijektiv

DEFINITION (Einschränkung einer Abbildung). Sei $f : A \longrightarrow B$ eine Abbildung und sei $A_1 \subseteq A$. Wir definieren $f|_{A_1} : A_1 \longrightarrow B$ durch $f|_{A_1}(a) := f(a)$ für alle $a \in A_1$, das heißt

$$f|_{A_1} = (A_1, B, G(f) \cap (A_1 \times B)).$$

BEISPIELE. In den vorangehenden Beispielen ist f_2 die Einschränkung von f_1 auf $\mathbb{R}_0^+$, f_4 ist die Einschränkung von f_3 auf $\mathbb{R}_0^+$.

BEMERKUNG. Man kann auch den Zielbereich einer nicht surjektiven Abbildung einschränken und sie a fortiori surjektiv machen:

$$f : A \longrightarrow f(A)$$
$$a \longmapsto f(a)$$

DEFINITION. Für Abbildungen $f : A \longrightarrow B$ und $g : B \longrightarrow C$ ist die *Verknüpfung (Komposition)* durch

$$g \circ f : A \longrightarrow C$$
$$a \longmapsto g(f(a))$$

definiert.

BEISPIELE. Seien

$$f : \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto x^2 \end{array} \qquad g : \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto x + 2. \end{array}$$

Dann gilt

$$g \circ f : \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto x^2 + 2 \end{array} \qquad f \circ g : \begin{array}{l} \mathbb{R} \longrightarrow \mathbb{R} \\ x \longmapsto (x + 2)^2 \end{array}$$

LEMMA 3.2. *Seien $f : A \longrightarrow B$ und $g : A \longrightarrow B$ zwei Abbildungen. Dann gilt:*

$$f = g \quad \Leftrightarrow \quad \forall a \in A : f(a) = g(a)$$

BEWEIS. Der Definitions- und Zielbereich stimmen nach Voraussetzung überein. Daher gilt $f = g \Leftrightarrow G(f) = G(g) \Leftrightarrow \forall a \in A : (a, f(a)) = (a, g(a)) \Leftrightarrow \forall a \in A : f(a) = g(a)$. □

KOROLLAR 3.3. *Seien $f : A \longrightarrow B$, $g : B \longrightarrow C$ und $h : C \longrightarrow D$ Abbildungen. Dann gilt $(h \circ g) \circ f = h \circ (g \circ f)$.*

PROPOSITION 3.4. *Seien $f : A \longrightarrow B$ und $g : B \longrightarrow C$ zwei Abbildungen. Es gilt:*

(1) $g \circ f$ injektiv $\Rightarrow$ f injektiv
(2) $g \circ f$ surjektiv $\Rightarrow$ g surjektiv
(3) f und g injektiv $\Rightarrow$ $g \circ f$ injektiv
(4) f und g surjektiv $\Rightarrow$ $g \circ f$ surjektiv

BEWEIS. (1): $f(a_1) = f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \overset{g\circ f \text{ injektiv}}{\Rightarrow} a_1 = a_2$.
(2): $\forall c \in C : \exists a \in A : g \circ f(a) = g(f(a)) = c \overset{\text{setze } b=f(a)\in B}{\Rightarrow} \forall c \in C : \exists b \in B : g(b) = c$.
(3): $g \circ f(a_1) = g \circ f(a_2) \Rightarrow g(f(a_1)) = g(f(a_2)) \overset{g \text{ injektiv}}{\Rightarrow} f(a_1) = f(a_2) \overset{f \text{ injektiv}}{\Rightarrow} a_1 = a_2$.
(4): $(\forall c \in C : \exists b \in B : g(b) = c) \wedge (\forall b \in B : \exists a \in A : f(a) = b) \Rightarrow$
$\Rightarrow \forall c \in C : \exists b \in B : g(b) = c \wedge \exists a \in A : f(a) = b \Rightarrow \forall c \in C : \exists a \in A : g(f(a)) = c$. □

DEFINITION (Umkehrabbildung). Sei die Abbildung $f : A \longrightarrow B$ bijektiv. Dann gilt

$$\forall b \in B : \exists! a \in A : f(a) = b,$$

denn die Injektivität von f entspricht genau der zusätzlichen Bedingung beim Quantor $\exists!$. Wir definieren mit diesen Elementen $b \in B$ und $a \in A$ eine Abbildung:

$$\begin{aligned} f^{-1} : B &\longrightarrow A \\ b &\longmapsto a \end{aligned}$$

BEMERKUNG. Die Notation f^{-1} wird ganz allgemein für das Urbild und bei bijektiven Abbildungen für die Umkehrabbildung verwendet. Bei einer bijektiven Abbildung f stimmt für jede Teilmenge $B_1 \subseteq B$ das Urbild unter f

$$f^{-1}(B_1) = \{a \in A \mid f(a) \in B_1\}$$

überein mit dem Bild von B_1 unter der Umkehrabbildung f^{-1}

$$(f^{-1})(B_1) = \{a \in A \mid \exists b \in B_1 : f^{-1}(b) = a\}.$$

DEFINITION (Identitätsabbildung). Für eine beliebige Menge A definieren wir

$$\begin{aligned} \mathrm{id}_A : A &\longrightarrow A \\ a &\longmapsto a \end{aligned}$$

Diese Abbildung ist offensichtlich bijektiv.

LEMMA 3.5. *Sei $f : A \longrightarrow B$ eine Abbildung.*

(1) Wenn f bijektiv ist, dann gelten $f^{-1} \circ f = \mathrm{id}_A$ und $f \circ f^{-1} = \mathrm{id}_B$.
(2) Ist $g : B \longrightarrow A$ eine Abbildung mit $g \circ f = \mathrm{id}_A$ und $f \circ g = \mathrm{id}_B$, dann sind f und g bijektiv und es gelten $g = f^{-1}$ und $f = g^{-1}$.

BEWEIS. (1): Nach der Definition von f^{-1} gilt $\forall a \in A : f^{-1}(f(a)) = a$, daher $f^{-1} \circ f = \mathrm{id}_A$. Ebenso gilt für $b \in B$ und $a = f^{-1}(b)$ nach der Definition $f(a) = b$, daher $f \circ f^{-1} = \mathrm{id}_B$.
(2): Aus der Bijektivität von $g \circ f$ folgt nach Proposition 3.4 die Surjektivität von g und die Injektivität von f. Aus der Bijektivität von $f \circ g$ folgt ebenso die Surjektivität von f und die Injektivität von g. Weiters gelten:

$$\begin{aligned} g = g \circ \mathrm{id}_B = g \circ (f \circ f^{-1}) = (g \circ f) \circ f^{-1} = \mathrm{id}_A \circ f^{-1} = f^{-1} \\ f = f \circ \mathrm{id}_A = f \circ (g \circ g^{-1}) = (f \circ g) \circ g^{-1} = \mathrm{id}_B \circ g^{-1} = g^{-1} \end{aligned}$$

□

BEMERKUNG. Aus dem Lemma folgt für eine bijektive Abbildung $f = (f^{-1})^{-1}$

DEFINITION. Seien X und Y Mengen und $R \subseteq X \times X$ sowie $S \subseteq Y \times Y$ Relationen. Die Abbildung $f : X \longrightarrow Y$ *respektiert die Relationen R und S*, wenn

$$\forall x_1, x_2 \in X : x_1 R x_2 \Rightarrow f(x_1) S f(x_2).$$

Besonders wichtig ist der Fall zweier Ordnungsrelationen.

DEFINITION. Seien $(X, \leq)$ und $(Y, \trianglelefteq)$ geordnete Mengen. Eine Abbildung $f : X \longrightarrow Y$ heißt *monoton wachsend* (auch isoton), wenn

$$\forall x_1, x_2 \in X : x_1 \leq x_2 \Rightarrow f(x_1) \trianglelefteq f(x_2),$$

und *monoton fallend* (auch antiton), wenn

$$\forall x_1, x_2 \in X : x_1 \leq x_2 \Rightarrow f(x_1) \trianglerighteq f(x_2) \qquad (\text{d.h. } f(x_2) \trianglelefteq f(x_1)).$$

BEISPIEL. Die Funktion $f : \mathbb{R}_0^+ \longrightarrow \mathbb{R}, x \mapsto x^2$ ist monoton wachsend (auf $\mathbb{R}_0^-$ monoton fallend).

DEFINITION. Sei X eine Menge. Eine *X-wertige Folge* ist eine Abbildung $f : \mathbb{N} \longrightarrow X$. Für $f(0), f(1), f(2), \ldots$ schreiben wir auch $x_0, x_1, x_2, \ldots$.

DEFINITION. Seien A und B Mengen. Wir definieren

$$B^A := \{f : A \longrightarrow B\}.$$

Für endliche Mengen A, B ist die Anzahl der Funktionen von A nach B genau $|B|^{|A|}$, denn jede Funktion wird durch die Gesamtheit ihrer Funktionswerte bestimmt.

BEISPIEL. Die Menge $X^{\mathbb{N}} := \{f : \mathbb{N} \longrightarrow X\}$ entspricht den X-wertigen Folgen.

DEFINITION (Mengenprodukt). Sei $(M_i)_{i \in I}$ eine Familie von Mengen. Wir definieren:

$$\prod_{i \in I} M_i := \left\{ f : I \longrightarrow \bigcup_{i \in I} M_i \middle| \forall j \in I : f(j) \in M_j \right\}$$

BEISPIELE.
- Sei $I = \{1, \ldots, n\}$ endlich, dann ist f durch $f(1), \ldots, f(n)$ bestimmt mit $f(k) \in M_k$ für $k = 1, \ldots, n$. Jede Funktion f entspricht einem n-Tupel und das Produkt entspricht $X_1 \times \cdots \times X_n$.
- Sei $M_i = M$ für alle $i \in I$. Dann gilt $\prod_{i \in I} M_i = \{f : I \longrightarrow M\} = M^I$.

4. Die „Größe“ (Mächtigkeit, Kardinalität) von Mengen

Für endliche Mengen bestimmen wir die Anzahl der Elemente durch Abzählen, d.h. mittels einer bijektiven Abbildung auf die Menge $\{1, 2, 3, \ldots, n\}$ mit einem passenden $n \in \mathbb{N}$.

Ganz generell wird die Mächtigkeit von Mengen mittels (bijektiver) Abbildungen definiert. Bei unendlichen Mengen treten der Intuition widersprechende Fakten auf:

$$\begin{aligned} f : \mathbb{N} &\longrightarrow 2\mathbb{N} = \{k \in \mathbb{N} \mid \exists n \in \mathbb{N} : k = 2n\} \\ n &\longmapsto 2n \end{aligned}$$

ist eine bijektive Abbildung, aber $\mathbb{N} \supsetneqq 2\mathbb{N}$.

DEFINITION. Seien A und B zwei Mengen.

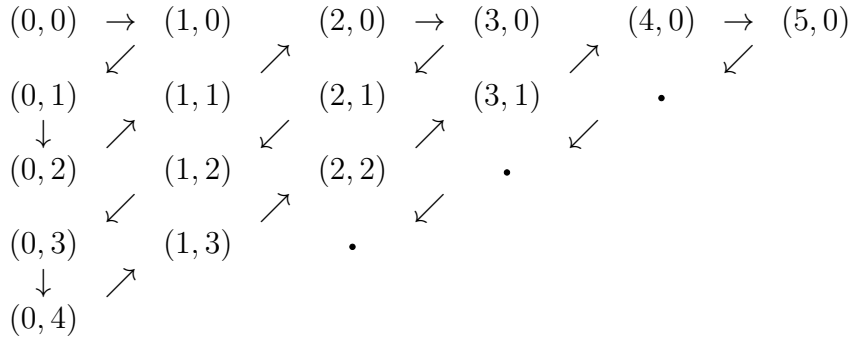
(1) Die Mengen A und B heißen *gleichmächtig* genau dann, wenn eine bijektive Abbildung $f : A \longrightarrow B$ existiert. Wir schreiben auch $|A| = |B|$.
(2) Wenn eine bijektive Abbildung $g : A \longrightarrow B_1$ auf eine Teilmenge $B_1 \subseteq B$ existiert, dann heißt A *höchstens gleichmächtig* zu B ($|A| \leq |B|$). Wenn zusätzlich *keine* bijektive Abbildung $f : A \longrightarrow B$ existiert, dann heißt A *weniger mächtig* als B ($|A| < |B|$).

DEFINITION. (1) Eine Menge A heißt endlich, wenn $|A| = |\{1, 2, 3, \ldots, n\}|$ für eine natürliche Zahl n gilt.
(2) Eine Menge A heißt abzählbar unendlich, wenn $|A| = |\mathbb{N}|$ gilt.
(3) Eine Menge A heißt überabzählbar, falls weder endlich noch abzählbar unendlich.

BEMERKUNG. Man definiert auch für unendliche Mengen ein Maß für die Mächtigkeit, die Kardinalzahl. Die erste unendliche (transfinite) Kardinalzahl wird mit dem Hebräischen Buchstaben $\aleph$ und dem Index 0 bezeichnet, d.h. $|\mathbb{N}| = \aleph_0$.

PROPOSITION 4.1. *Es gilt* $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0$.

BEWEIS. Cantorsches Diagonalverfahren:



□

PROPOSITION 4.2. *Für die rationalen Zahlen* $\mathbb{Q}$ *gilt* $|\mathbb{Q}| = |\mathbb{N}| = \aleph_0$.

BEWEIS. Im ersten Schritt zeigen wir $|\mathbb{Q}^+| = \aleph_0$ mit dem Cantorschen Diagonalverfahren, angewandt auf die Zähler und Nenner in $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$). Die Erweiterungen bereits aufgetretener Brüche werden einfach übersprungen. Im zweiten Schritt fügen wir 0 an den Anfang und die negativen rationalen Zahlen in die Zwischenräume ein. □

PROPOSITION 4.3. *Es gilt* $|\mathbb{N}| < |\mathbb{R}|$*, daher ist* $\mathbb{R}$ *überabzählbar.*

BEWEIS. Wegen $\mathbb{N} \subseteq \mathbb{R}$ gilt $|\mathbb{N}| \leq |\mathbb{R}|$ ($\mathrm{id}_{\mathbb{N}}$ ist eine bijektive Abbildung auf eine Teilmenge von $\mathbb{R}$). Es bleibt zu zeigen, dass keine Abbildung von $\mathbb{N}$ nach $\mathbb{R}$ bijektiv sein kann.

Wir nehmen an, dass eine bijektive Abbildung $f : \mathbb{N} \longrightarrow \mathbb{R}$ existiert. Die Elemente der Folge $f(0), f(1), f(2), \ldots$ werden in der Dezimalentwicklung mit ganzen Zahlen $m_i \in \mathbb{Z}$ und Ziffern $a_{ij} \in \{0, 1, 2, \ldots, 9\}$ für $i, j \in \mathbb{N}$ dargestellt:

$$f(i) = m_i, a_{i0}a_{i1}a_{i2}a_{i3}\ldots$$

Wir definieren eine Zahl $\tilde{x} \in (0, 1)$ durch die Dezimalentwicklung $0, a_0a_1a_2a_3\ldots$ mit

$$a_i = \begin{cases} 1 & \text{wenn } a_{ii} \neq 1 \\ 2 & \text{wenn } a_{ii} = 1. \end{cases}$$

Diese Zahl besitzt keine Periode 9 und unterscheidet sich für jedes $i \in \mathbb{N}$ an der i-ten Stelle der Dezimalentwicklung von $f(i)$, im Widerspruch zur Surjektivität von f gilt $\tilde{x} \notin f(\mathbb{N})$. □

SATZ 4.4 (Cantor). *Für jede Menge* $A \neq \emptyset$ *gilt* $|A| < |\mathcal{P}(A)|$.

BEWEIS. Es gilt $|A| \leq |\mathcal{P}(A)|$, denn die Abbildung $f : A \longrightarrow \mathcal{P}(A), a \mapsto \{a\}$ ist injektiv.
Wir nehmen an, dass eine bijektive Abbildung $g : A \longrightarrow \mathcal{P}(A)$ existiert und setzen

$$(*) \qquad S := \{a \in A \mid a \notin g(a)\} \in \mathcal{P}(A)$$

Da g surjektiv ist, gilt $S = g(a_0)$ für ein $a_0 \in A = S \cup (A \setminus S)$. Aus $a_0 \in S = g(a_0)$ und $(*)$ folgt der Widerspruch $a_0 \notin S$. Aus $a_0 \notin S = g(a_0)$ und $(*)$ folgt der Widerspruch $a_0 \in S$. Da jedenfalls ein Widerspruch auftritt, kann kein bijektives $g : A \longrightarrow \mathcal{P}(A)$ existieren. □

KAPITEL 4

Algebraische Strukturen

Eine algebraische Struktur (auch universelle Algebra) besteht aus einer Menge und einer Verknüpfung.

DEFINITION. Sei M eine Menge. Eine *binäre Verknüpfung* ist eine Abbildung

$$\circ : M \times M \longrightarrow M$$
$$(x, y) \longmapsto x \circ y$$

BEMERKUNG. Es gibt auch unäre Verknüpfungen, ternäre Verknüpfungen etc.

BEISPIELE.
- Auf $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \ldots$ $+$: Addition, $\cdot$: Multiplikation
- Auf $X^X = \{f : X \longrightarrow X\}$, $\circ$: Komposition von Abbildungen
- Auf $\mathbb{Z}_n$: $[x] + [y] := [x + y]$, $[x] \cdot [y] := [xy]$ sind wohldefiniert (d.h. wenn $[x] = [x']$ und $[y] = [y']$ gelten, dann folgen $[x + y] = [x] + [y] = [x'] + [y'] = [x' + y']$ und $[xy] = [x] \cdot [y] = [x'] \cdot [y'] = [x'y']$).
- Auf den $n \times n$-Matrizen $\mathrm{M}_{n\times n}(\mathbb{R})$ mit reellen Einträgen, $\circ$ Matrizenmultiplikation:

$$(\mathbf{A} \circ \mathbf{B})_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} = \sum_{k=1}^{n} (\mathbf{A})_{ik} (\mathbf{B})_{kj}$$

- Verknüpfungen auf endlichen Mengen können mittels einer Verknüpfungstafel angegeben werden, hier beispielsweise für $\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Durch die linke Spalte wird das linke Argument der Verknüpfung definiert, durch die erste Zeile das rechte Argument.

1. Monoide und Gruppen

DEFINITION. Ein Paar $(G, \circ)$, wobei G eine Menge und $\circ$ eine Verknüpfung, heißt *Gruppe*, wenn folgende Axiome gelten:

(A) $\forall g, h, k \in G : (g \circ h) \circ k = g \circ (h \circ k)$ (Assoziativgesetz)
(N) $\exists e \in G : \forall g \in G : g \circ e = e \circ g = g$ (neutrales Element)
(I) $\forall g \in G : \exists g^{-1} \in G : g^{-1} \circ g = g \circ g^{-1} = e$ (inverses Element)

Falls nur (A) und (N) gelten, so heißt $(G, \circ)$ ein *Monoid*. Falls aber zusätzlich zu (A),(N) und (I) auch

(K) $\forall g, h \in G : g \circ h = h \circ g$ (Kommutativgesetz)

gilt, so heißt die Gruppe $(G, \circ)$ *kommutativ* (auch *abelsch*).

BEMERKUNG. Wenn die Verknüpfung einer Gruppe als Addition notiert wird, dann ist diese Gruppe immer kommutativ und e wird mit 0 sowie g^{-1} mit $-g$ bezeichnet.

BEISPIELE. Beispiele für Monoide sind $\mathbb{N}$ mit der Multiplikation und $e = 1$, die $n \times n$-Matrizen $\mathrm{M}_{n\times n}(\mathbb{R})$ mit der Einheitsmatrix $e = \mathbf{I}$ mit $(\mathbf{I})_{ij} = \delta_{ij}$.

SATZ 1.1 (Gruppeneigenschaften). *Sei $(G, \circ)$ eine Gruppe und seien $g, h, k \in G$ beliebig.*

(1) e ist eindeutig bestimmt.
(2) g^{-1} ist eindeutig bestimmt.
(3) $(g^{-1})^{-1} = g$
(4) $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$
(5) $h \circ g = k \circ g \Rightarrow h = k$
$g \circ h = g \circ k \Rightarrow h = k$
(6) Die Gleichung $g \circ x = h$ hat die eindeutige Lösung $x = g^{-1} \circ h$.

BEWEIS. (1): Seien $e, \tilde{e} \in G$, beide erfüllen Axiom (N). Aus $e \circ g = g$ folgt für $g = \tilde{e}$ die Gleichung $e \circ \tilde{e} = \tilde{e}$ und aus $g \circ \tilde{e} = g$ folgt für $g = e$ die Gleichung $e \circ \tilde{e} = e$, daher $e = \tilde{e}$.

(2): Seien $g^{-1}, \tilde{g} \in G$, beide erfüllen Axiom (I) für $g \in G$. Aus $g^{-1} \circ g = g \circ g^{-1} = e$ und $\tilde{g} \circ g = g \circ \tilde{g} = e$ folgt $\tilde{g} = \tilde{g} \circ e = \tilde{g} \circ (g \circ g^{-1}) = (\tilde{g} \circ g) \circ g^{-1} = e \circ g^{-1} = g^{-1}$.

(3): Das Element g erfüllt $g \circ g^{-1} = g^{-1} \circ g = e$ und damit alle Eigenschaften von $(g^{-1})^{-1}$. Aufgrund der Eindeutigkeit von $(g^{-1})^{-1}$ gilt $(g^{-1})^{-1} = g$.

(4): Es folgt mit (A), (I) und (N), dass $(g \circ h) \circ (h^{-1} \circ g^{-1}) = ((g \circ h) \circ h^{-1}) \circ g^{-1} = (g \circ (h \circ h^{-1})) \circ g^{-1} = (g \circ e) \circ g^{-1} = e$. Analog folgt $(h^{-1} \circ g^{-1}) \circ (g \circ h) = e$, aufgrund der Eindeutigkeit gilt $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

(5): Aus $h \circ g = k \circ g$ folgt $(h \circ g) \circ g^{-1} = (k \circ g) \circ g^{-1}$, mit (A) und (I) folgt daher $h \circ e = k \circ e$ und $h = k$. Die zweite Aussage folgt analog $g \circ h = g \circ k \Rightarrow g^{-1} \circ (g \circ h) = g^{-1} \circ (g \circ k) \Rightarrow e \circ h = e \circ k \Rightarrow h = k$.

(6): Das Element $x = g^{-1} \circ h$ erfüllt $g \circ x = h$, die Eindeutigkeit folgt aus (5). □

BEISPIELE (Beispiele von Gruppen). $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{Z}_n, +), (\mathbb{R}^n, +)$ und die triviale Gruppe $(\{e\}, \circ)$ sind kommutative Gruppen.

$(\mathbb{Z}_n \setminus \{0\}, \cdot)$ ist im Allgemeinen keine Gruppe! Z.B. hat [2] kein multiplikativ Inverses in $\mathbb{Z}_6$.

Nicht kommutative Gruppen sind $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$ mit der Matrizenmultiplikation $\circ$ und die Permutationsgruppen $\mathcal{S}_n = \{f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\} \mid f \text{ ist bijektiv}\}$ mit der Komposition $\circ$ für $n \in \mathbb{N}, n \geq 3$.

BEISPIEL. Die Permutationsgruppe $\mathcal{S}_3 = \{\mathrm{id}, (1, 2), (1, 3), (2, 3), (1, 2, 3), (1, 3, 2)\}$, dabei bedeutet die Zyklenschreibweise $(1, 2)$ die Abbildung $1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3$ und $(1, 3, 2)$ bedeutet $1 \mapsto 3, 3 \mapsto 2, 2 \mapsto 1$. Es gelten $(2, 3) \circ (1, 2) = (1, 3, 2)$ und $(1, 2) \circ (2, 3) = (1, 2, 3)$, daher ist $\mathcal{S}_3$ nicht kommutativ.

Die Gruppe $(\mathbb{Z}_6, +)$ ist eine weitere (jedoch kommutative) Gruppe mit 6 Elementen.

DEFINITION. Sei $(G, \circ)$ eine Gruppe und sei $H \subseteq G$. Wenn für alle $g, h \in H$ auch $g \circ h \in H$ gilt und $(H, \circ|_{H\times H})$ ebenfalls eine Gruppe ist, so heißt $(H, \circ_H)$ eine *Untergruppe* von $(G, \circ)$. Wir schreiben $H \leqslant G$.

PROPOSITION 1.2. *Sei $(H, \circ_H)$ eine Untergruppe von $(G, \circ)$.*

(1) Es gilt $e_G = e_H$.

(2) Für alle $h \in H$ gilt $(h^{-1})_G = (h^{-1})_H$.

BEWEIS. (1): Es gilt $e_H \circ e_H = e_H \circ_H e_H = e_H = e_H \circ e_G$, nach Satz 1.1 (5) folgt $e_H = e_G$.

(2): Es gilt $h \circ (h^{-1})_H = h \circ_H (h^{-1})_H = e_H = e_G = h \circ (h^{-1})_G$, wiederum folgt $(h^{-1})_H = (h^{-1})_G$. □

BEISPIELE (Beispiele von Untergruppen). $\{e\} \leqslant G$ und $G \leqslant G$ sind die trivialen Untergruppen von G; mit $\circ = +$ gilt $2\mathbb{Z} \leqslant \mathbb{Z} \leqslant \mathbb{Q} \leqslant \mathbb{R}$; mit der Matrizenmultiplikation $\circ$ gilt $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{M}_{n\times n}(\mathbb{R}) \mid \det(A) = 1\} \leqslant \mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_{n\times n}(\mathbb{R}) \mid \det(A) \neq 0\}$.

LEMMA 1.3. *Sei $(G, \circ)$ eine Gruppe und sei $H \neq \emptyset$ eine Teilmenge von G. Folgende Aussagen sind äquivalent:*

(1) $H \leqslant G$

(2) $(\forall x, y \in H : x \circ y \in H) \wedge (\forall x \in H : x^{-1} \in H)$

(3) $\forall x, y \in H : x \circ y^{-1} \in H$

BEWEIS. (1)⇒(2): Folgt aus der Definition und Proposition 1.2 (2).

(2)⇒(1): $\circ$ ist eine Verknüpfung auf H $(\forall x, y \in H : x \circ y \in H)$ und (A) wird von G auf H vererbt. H ist nichtleer und für $x \in H$ gilt $x^{-1} \in H$ und mit (2) auch $x \circ x^{-1} = e \in H$.

(2)⇒(3): trivial.

(3)⇒(2): H ist nichtleer und für $x \in H$ folgt $x \circ x^{-1} = e \in H$. Daher gilt $\forall y \in H : e \circ y^{-1} = y^{-1} \in H$, wegen $(y^{-1})^{-1} = y$ folgt aus (3) auch $\forall x, y \in H : x \circ (y^{-1})^{-1} = x \circ y \in H$. □

DEFINITION. Seien $(G, \circ)$ und $(H, \diamond)$ Gruppen. Eine Abbildung $f : G \longrightarrow H$ heißt *Gruppenhomomorphismus*, wenn gilt:

$$\forall x, y \in G : f(x \circ y) = f(x) \diamond f(y)$$

Die Abbildung f ist mit $\circ$ und $\diamond$ verträglich. Wir bezeichnen einen injektiven Gruppenhomomorphismus als *Monomorphismus*, einen surjektiven als *Epimorphismus*, einen bijektiven als *Isomorphismus*. Im Fall $H = G$ bezeichnen wir einen Gruppenhomomorphismus als *Endomorphismus* und wenn bijektiv als *Automorphismus*.

BEISPIELE.

$f : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}, +)$, $n \longmapsto 3n$	Endomorphismus
$q : (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$, $n \longmapsto [n]$	Quotientenabbildung ⇒ Epimorphismus
$\exp : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$, $x \longmapsto e^x$	Isomorphismus ($\exp^{-1} = \log$)

PROPOSITION 1.4. *Sei $f : (G, \circ) \longrightarrow (H, \diamond)$ ein Gruppenhomomorphismus. Dann gelten:*

(1) $f(e_G) = e_H$

(2) $\forall g \in G : f((g^{-1})_G) = (f(g)^{-1})_H$

BEWEIS. (1): $f(e_G) = f(e_G \circ e_G) = f(e_G) \diamond f(e_G)$. Daher gilt $f(e_G) \diamond e_H = f(e_G) = f(e_G) \diamond f(e_G)$ und nach Satz 1.1 (5) folgt $f(e_G) = e_H$.

(2): Sei $g \in G$ beliebig, dann gilt $e_H = f(e_G) = f(g \circ g^{-1}) = f(g) \diamond f(g^{-1})$. Ebenso gilt $e_H = f(g) \diamond f(g)^{-1}$, nach der Kürzungsregel folgt $f(g^{-1}) = f(g)^{-1}$. □

BEMERKUNG. Der *Kern* $\ker(f) := \{x \in G : f(x) = e_H\}$ ist immer eine Untergruppe von G und es gilt $\ker(f) = \{e_G\} \Leftrightarrow f$ injektiv. Beweis als Übung.

2. Ringe

Bei einem Ring handelt es sich um eine Struktur mit zwei Verknüpfungen auf ein und derselben Menge.

DEFINITION. Eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$ heißt *Ring*, falls

- $(R, +)$ eine kommutative (abelsche) Gruppe mit neutralem Element 0 und inversem Element $-a$ ist,
- $(R, \cdot)$ die Eigenschaft (A) erfüllt (und dann auch als Halbgruppe bezeichnet wird),
- (D) gilt: $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c \wedge (b + c) \cdot a = b \cdot a + c \cdot a$.

Die Verknüpfung $\cdot$ bindet stärker als $+$. Der Ring heißt *kommutativ*, wenn zusätzlich gilt:

$$\forall a, b \in R : a \cdot b = b \cdot a$$

Der Ring besitzt ein *Einselement* 1, wenn

$$\exists 1 \in R : 1 \neq 0 \wedge \forall a \in R : 1 \cdot a = a \cdot 1 = a.$$

SATZ 2.1 (Ringeigenschaften). *Sei $(R, +, \cdot)$ ein Ring. Dann gelten:*

(1) $\forall a \in R : a \cdot 0 = 0 \cdot a = 0$
(2) $\forall a, b \in R : (-a) \cdot b = -(a \cdot b) = a \cdot (-b)$
(3) $\forall a, b \in R : (-a) \cdot (-b) = a \cdot b$

BEWEIS. (1): Es gilt $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$, aus $a \cdot 0 + 0 = a \cdot 0$ und Satz 1.1 (5) folgt $a \cdot 0 = 0$. Der Beweis von $0 \cdot a = 0$ erfolgt analog.

(2): $(-a) \cdot b + a \cdot b = (-a + a) \cdot b = 0 \cdot b = 0$ und $+$ ist kommutativ, daher gilt $(-a) \cdot b = -(a \cdot b)$. Der Beweis von $a \cdot (-b) = -(a \cdot b)$ erfolgt analog.

(3): Aus (2) folgt $(-a) \cdot (-b) = -(a \cdot (-b)) = -(-(a \cdot b)) = a \cdot b$. □

BEMERKUNG. Der kleinste Ring ist $\{0\}$, der kleinste Ring mit 1 ist $\{0, 1\}$.

BEISPIELE (Beispiele von Ringen). Kommutative Ringe mit 1 sind beispielsweise $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ und $(\mathbb{Z}_n, +, \cdot)$. Die Polynome mit reellen Koeffizienten bilden mit der Addition und Multiplikation (Faltung) ebenfalls einen kommutativen Ring mit 1.

Die Menge der Matrizen $\mathrm{M}_{n \times n}(\mathbb{R})$ mit der koordinatenweisen Addition und dem Matrizenprodukt ergibt bei $n \geq 2$ einen nicht kommutativen Ring mit Eins $\mathbf{I}$ (Einheitsmatrix).

Die geraden ganzen Zahlen $(2\mathbb{Z}, +, \cdot)$ sind ein kommutativer Ring ohne Einselement.

DEFINITION (Teilring). Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$. Wenn $\forall a, b \in S : a + b \in S \wedge a \cdot b \in S$ gilt und $(S, +|_{S \times S}, \cdot|_{S \times S})$ selbst wieder ein Ring ist, so heißt $(S, +_S, \cdot_S)$ ein *Teilring* von R. Wir schreiben $S \leqslant R$.

PROPOSITION 2.2. *Sei $(R, +, \cdot)$ ein Ring und sei $S \subseteq R$ eine nichtleere Teilmenge. Dann ist S ein Teilring von R genau dann, wenn gilt:*

$$\forall a, b \in S : a - b \in S \wedge a \cdot b \in S$$

BEWEIS. Die Eigenschaft (A) wird für $+$ und $\cdot$ von R auf S vererbt, ebenso (K) für $+$. Auch (D) wird von R auf S vererbt. Daher ist nach Lemma 1.3 $(S, +)$ eine kommutative Gruppe genau dann, wenn $\forall a, b \in S : a - b \in S$. Ebenso ist $(S, \cdot)$ eine Halbgruppe genau dann, wenn $\forall a, b \in S : a \cdot b \in S$. □

BEMERKUNG. Aus Proposition 1.2 folgen $0_S = 0_R$ und $(-a)_S = (-a)_R$. Wenn R und S Ringe mit Einselementen sind, dann verlangt man $1_S = 1_R$.

BEISPIEL. Der Ring $(\mathbb{Z}, +, \cdot)$ besitzt ein Einselement 1 und es gilt $(2\mathbb{Z}, +, \cdot) \leqslant (\mathbb{Z}, +, \cdot)$, aber $(2\mathbb{Z}, +, \cdot)$ besitzt kein Einselement.

DEFINITION. Seien $(R, +, \cdot)$ und $(S, \oplus, \odot)$ Ringe. Eine Abbildung $f : R \longrightarrow S$ heißt Ringhomomorphismus, falls gilt:

$$\forall a, b \in R : f(a + b) = f(a) \oplus f(b) \wedge f(a \cdot b) = f(a) \odot f(b)$$

Wenn R und S Ringe mit Einselementen sind, dann verlangt man noch $f(1_R) = 1_S$.

BEISPIELE. Die Quotientenabbildung $q : \mathbb{Z} \longrightarrow \mathbb{Z}_n, k \mapsto [k]$ ist ein Ringhomomorphismus.

Die Abbildung $f : 2\mathbb{Z} \longrightarrow \mathbb{Z}, 2k \mapsto 2k$ ist ein Ringhomomorphismus (nicht surjektiv).

Die Abbildung $g : 2\mathbb{Z} \longrightarrow \mathbb{Z}, 2k \mapsto k$ ist *kein* Ringhomomorphismus. Aus der Definition würde einerseits $g(4) = g(2 \cdot 2) = g(2) \cdot g(2) = 1 \cdot 1 = 1$ und andererseits $g(4) = g(2 + 2) = 1 + 1 = 2$ folgen, ein Widerspruch.

DEFINITION. Sei $(R, +, \cdot)$ ein Ring. Ein Element $a \in R \setminus \{0\}$ heißt Nullteiler, wenn $\exists b \in R \setminus \{0\} : a \cdot b = 0$.

BEISPIEL. Das Element [2] ist ein Nullteiler in $\mathbb{Z}_6$, denn $[2] \cdot [3] = [6] = [0]$.

DEFINITION. Ein kommutativer Ring $(R, +, \cdot)$ mit Einselement heißt *Integritätsbereich*, wenn R keine Nullteiler besitzt.

Ein Element $a \in R$ heißt *Einheit*, wenn $\exists b \in R : a \cdot b = b \cdot a = 1$. Wir bezeichnen die Menge der Einheiten mit R^*.

BEMERKUNG. Die Eins 1 ist von Einheiten zu unterscheiden! Die Eins (das Einselement) ist immer eine Einheit, aber nicht umgekehrt.

BEISPIELE. Die Ringe $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ $(\mathbb{R}, +, \cdot)$ sind Integritätsbereiche.

Der Ring $(\mathbb{Z}_n, +, \cdot)$ ist ein Integritätsbereich genau dann, wenn n eine Primzahl.

3. Körper

DEFINITION. Eine Menge K mit zwei Verknüpfungen + und $\cdot$ heißt *Körper*, falls

- $(K, +)$ eine kommutative (abelsche) Gruppe mit neutralem Element 0 und inversem Element $-a$ ist,
- $(K \setminus \{0\}, \cdot)$ eine kommutative (abelsche) Gruppe mit neutralem Element 1 und inversem Element a^{-1} ist,
- (D) gilt: $\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c \wedge (b + c) \cdot a = b \cdot a + c \cdot a$.

Auch hier bindet die Verknüpfung $\cdot$ stärker als +.

BEMERKUNGEN. Analog zu dieser Definition ist $(K, +, \cdot)$ ein kommutativer Ring mit 1, sodass jedes Element ungleich 0 bezüglich $\cdot$ ein Inverses besitzt. Insbesondere gilt $1 \neq 0$.

SATZ 3.1 (Rechenregeln für Körper). *Sei $(K, +, \cdot)$ ein Körper und $K^* = K \setminus \{0\}$.*

(1) Für $a, b \in K^*$ gilt $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$.

(2) Für $a \in K^*$ gilt $(-a)^{-1} = -(a^{-1})$, daher $(-1)^{-1} = -1$.

(3) Für $a, b \in K$ gilt $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0$ (d.h. ein Körper ist nullteilerfrei).

(4) Für $a, b \in K$ mit $a \neq 0$ hat die Gleichung $a \cdot x = b$ die eindeutige Lösung $x = a^{-1} \cdot b$.

BEWEIS. Die Beweise erfolgen mittels der Gruppeneigenschaften von $(K^*, \cdot))$ und (K).

(1): Folgt aus Satz 1.1 (4) und (K).

(2): Es gilt $-a \in K^*$, denn sonst würde $a = -(-a) = -0 = 0$ nach Satz 2.1 (3) folgen. Weiters gilt $(-a) \cdot (-(a^{-1})) = a \cdot a^{-1} = 1$, daher folgt $(-a)^{-1} = -(a^{-1})$ mit (K).

(3): Der Beweis erfolgt indirekt durch $a \in K^* \wedge b \in K^* \Rightarrow a \cdot b \in K^*$.

(4): Im Fall $b = 0$ folgt $x = 0 = a^{-1} \cdot b$ aus (3) und Satz 2.1 (1), im Fall $b \neq 0$ folgt die Aussage aus Satz 1.1 (6), wobei nach Satz 2.1 (1) $x = 0$ keine Lösung sein kann. □

LEMMA 3.2. *Jeder endliche Integritätsbereich $(R, +, \cdot)$ ist ein Körper.*

BEWEIS. Sei $a \in R \setminus \{0\}$ fest gewählt. Wir betrachten die Abbildung $f_a : R \longrightarrow R$ mit $x \mapsto a \cdot x$. Die Abbildung ist injektiv, denn für $ax_1 = ax_2$ folgt $a(x_1 - x_2) = 0$ und aufgrund der Nullteilerfreiheit $x_1 = x_2$. Da die Menge R endlich ist, muss f_a auch surjektiv sein und $\exists x \in R : a \cdot x = 1$. Da $a \neq 0$ beliebig war, ist $(R, +, \cdot)$ ist ein Körper. □

PROPOSITION 3.3. *Der Ring $\mathbb{Z}_m$ ist ein Körper genau dann, wenn $m \in \mathbb{P}$.*

BEWEIS. $\Rightarrow$: Sei $m \notin \mathbb{P}$, dann gilt $m = ab$ mit $a, b \in \mathbb{Z} \setminus \{1, -1, m, -m\}$ und es folgt $[a] \cdot [b] = [m] = [0]$. Wegen $[a] \neq 0$ und $[b] \neq 0$ sind beide Nullteiler und $\mathbb{Z}_m$ ist kein Körper.
$\Leftarrow$: Für $m \in \mathbb{P}$ und $k, l \in \{0, 1, \ldots, m-1\}$ mit $[k] \cdot [l] = [k \cdot l] = [0]$ gilt $m \mid k \cdot l$. Nach Korollar 1.6 in Kapitel 5 (Zahlenmengen) gilt $m \mid k \vee m \mid l$, daher $[k] = [0] \vee [l] = [0]$. Somit ist $\mathbb{Z}_m$ nullteilerfrei und nach dem Lemma ein Körper. □

BEISPIELE (Beispiele von Körpern). $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ sind Körper. Nach der Proposition ist $(\mathbb{Z}_p, +, \cdot)$ für $p \in \mathbb{P}$ ein Körper. Der kleinste Körper ist $(\mathbb{Z}_2, +, \cdot)$.

DEFINITION. Die Definition eines Teilkörpers $E \leqslant K$ erfolgt analog einem Teilring mit 1, zusätzlich muss für $a \in E^*$ auch $a^{-1} \in E$ gelten.

PROPOSITION 3.4. *Sei $(K, +, \cdot)$ ein Körper und sei $E \subseteq K$ eine nichtleere Teilmenge mit $E \neq \{0\}$. Dann ist E ein Teilkörper von K genau dann, wenn gilt:*

$$\big(\forall a, b \in E : a - b \in E\big) \wedge \big(\forall a, b \in E^* : a \cdot b^{-1} \in E\big)$$

BEWEIS. $\Rightarrow$: Ergibt sich aus den Körpereigenschaften von E.
$\Leftarrow$: Aus der zweiten Bedingung folgt für $a = b \in E^*$ auch $a \cdot a^{-1} = 1 \in E$. Für $a = 1$ folgt nun $\forall b \in E^* : b^{-1} \in E$. Wegen $a - a = 0 \in E$ und $\forall a \in E : a \cdot 0 = 0$ folgt gemeinsam mit $(b^{-1})^{-1} = b$ nun $\forall a, b \in E : a \cdot b \in E$. Nach Proposition 2.2 ist E ein Teilring mit 1 und zusätzlich gilt $\forall a \in E^* : a^{-1} \in E$, daher ist E ein Teilkörper. □

BEISPIELE. $(\mathbb{Q}, +, \cdot) \leqslant (\mathbb{R}, +, \cdot)$.
Für die *quadratischen Zahlkörper* $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ gilt $(\mathbb{Q}(\sqrt{d}), +, \cdot) \leqslant (\mathbb{R}, +, \cdot)$, hier ist $d \in \mathbb{Q}$ kein Quadrat einer rationalen Zahl.

DEFINITION. Seien $(K, +, \cdot)$ und $(K', \oplus, \odot)$ Körper. Eine Abbildung $f : K \longrightarrow K'$ heißt Körperhomomorphismus, falls f ein Ringhomomorphismus ist und $f(1_K) \neq 0_{K'}$ gilt.

PROPOSITION 3.5. *Jeder Körperhomomorphismus $f : K \longrightarrow K'$ ist injektiv und ein Gruppenhomomorphismus von $(K^*, \cdot)$ nach $((K')^*, \odot)$.*

BEWEIS. Für $a \in K^*$ gilt $f(a) \odot f(a^{-1}) = f(a \cdot a^{-1}) = f(1_K) \neq 0_{K'}$ und daher $f(a) \neq 0_{K'}$ nach Satz 2.1 (1). Es gilt $f(K^*) \subseteq (K')^*$ und damit ist f ein Gruppenhomomorphismus von $(K^*, \cdot)$ nach $((K')^*, \odot)$ mit $f(1_K) = 1_{K'}$ nach Proposition 1.4 (1).
Für $a, b \in K$ mit $f(a) = f(b)$ folgt nun mittels Proposition 1.4 (2) die Gleichung $0_{K'} = f(a) \oplus (-f(b)) = f(a) \oplus f(-b) = f(a + (-b))$, daher $\Rightarrow a + (-b) = 0_K$ bzw. $a = b$. □

BEISPIELE. $(\mathbb{R}, \oplus, \odot)$ mit den Verknüpfungen $a \oplus b := a + b - 3$ und $a \odot b := ab - 3a - 3b + 12$ ist ein zu $(\mathbb{R}, +, \cdot)$ isomorpher Körper, denn $f : \mathbb{R} \longrightarrow \mathbb{R}, x \mapsto x + 3$ ist ein Körperisomorphismus von $(\mathbb{R}, +, \cdot)$ nach $(\mathbb{R}, \oplus, \odot)$.
Die Körper $\mathbb{Q}(\sqrt{2})$ und $\mathbb{Q}(\sqrt{3})$ sind nicht isomorph. Für einen bijektiven Körperhomomorphismus f müsste sowohl $f(2) = f(1 + 1) = f(1) + f(1) = 1 + 1 = 2$ als auch $f(2) = f(\sqrt{2} \cdot \sqrt{2}) = f(\sqrt{2}) \cdot f(\sqrt{2})$ gelten. Angenommen, es existieren $a, b \in \mathbb{Q}$ mit $f(\sqrt{2}) = a + b\sqrt{3}$, dann folgt $2 = (a + b\sqrt{3})^2 = a^2 + 3b^2 + 2ab\sqrt{3}$. Dies ist nur bei $a = 0 \vee b = 0$ möglich, aber $a^2 = 2$ als auch $3b^2 = 2$ sind in $\mathbb{Q}$ nicht lösbar.

KAPITEL 5

Zahlenmengen

1. Die natürlichen Zahlen $\mathbb{N}$

Die natürlichen Zahlen $\mathbb{N}$ wurden 1889 von Giuseppe Peano axiomatisiert.

Definition. Sei $\mathbb{N}$ eine Menge. Die *Peano Axiome* lauten:

(1) $0 \in \mathbb{N}$
(2) $\forall n \in \mathbb{N} : \exists S(n)$ ($S(n)$ ist der Nachfolger von n, $S : \mathbb{N} \longrightarrow \mathbb{N}$)
(3) $\forall n \in \mathbb{N} : S(n) \neq 0$ (0 ist kein Nachfolger)
(4) $\forall n_1, n_2 \in \mathbb{N} : n_1 \neq n_2 \Rightarrow S(n_1) \neq S(n_2)$ (S ist injektiv)
(5) $\forall M \subseteq \mathbb{N} : (0 \in M \wedge \forall n \in M : S(n) \in M) \Rightarrow M = \mathbb{N}$ (Eine Teilmenge von $\mathbb{N}$, die 0 und mit jedem ihrer Elemente auch dessen Nachfolger enthält, ist gleich $\mathbb{N}$.)

Diese Axiome definieren die natürlichen Zahlen bis auf eine Isomorphie.

Satz 1.1 (Dedekind). *Wenn* $(\mathbb{N}, S, 0)$ *und* $(\tilde{\mathbb{N}}, \tilde{S}, \tilde{0})$ *beide die Axiome (1) bis (5) erfüllen, dann existiert ein bijektive Abbildung* $\phi : \mathbb{N} \longrightarrow \tilde{\mathbb{N}}$ *mit*

- $\phi(0) = \tilde{0}$,
- $\forall n \in \mathbb{N} : \phi(S(n)) = \tilde{S}(\phi(n))$.

Bemerkungen. Die Konstruktion der natürlichen Zahlen erfolgt in der axiomatischen Mengenlehre mittels des Unendlichkeitsaxioms in ZFC (Zermelo-Fraenkel-Axiomensystem der Mengentheorie): Es gibt eine Menge, welche die leere Menge $\emptyset$ und mit jedem Element x auch die Menge $x \cup \{x\}$ als Element enthält.

Wir definieren den Nachfolger von x durch $S(x) := x \cup \{x\} = x + 1$ und setzen dann: $0 := \emptyset, \quad 1 := \{\emptyset\}, \quad 2 := \{\emptyset, \{\emptyset\}\}, \quad 3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \ldots$.
Es gilt ganz allgemein $n = \{0, 1, 2, \ldots, n-1\}$.

Beweise mit vollständiger Induktion basieren auf (5) mit $M = \{n \in \mathbb{N} \mid A(n) \text{ ist wahr}\}$. Der Induktionsanfang entspricht $0 \in M$, der Induktionsschritt $\forall n \in M : S(n) \in M$.

Definition. Die Ordnung auf den natürlichen Zahlen $\mathbb{N}$ wird durch

$$n \leq m :\Leftrightarrow n \subseteq m$$

definiert. Die Axiome (R) und (T) folgen aus der Definition, (AS) kann mittels des Regularitätsaxioms in ZFC bewiesen werden. Diese Ordnung ist eine Totalordnung auf $\mathbb{N}$.

Satz 1.2 (Wohlordnungsprinzip). *Jede nichtleere Teilmenge von* $\mathbb{N}$ *besitzt ein kleinstes Element.*

Beweis. Angenommen, es sei $T \subseteq \mathbb{N}$ eine nichtleere Menge ohne kleinstes Element. Wir zeigen mit vollständiger Induktion nach n, dass $\forall n \in \mathbb{N} : k \leq n \Rightarrow k \notin T$.

Induktionsanfang: Für $n = 0$ gilt $k \leq 0 \Rightarrow k = 0$ und es gilt $0 \notin T$, sonst ist 0 kleinstes Element von T ($0 \leq m$ für alle $m \in T$).

Induktionsannahme: Es gelte für alle $k \in \mathbb{N}$ mit $k \leq n$, dass $k \notin T$.

Induktionsschritt: Für jedes $m \in T$ gilt $n + 1 \leq m \vee m \leq n + 1$ (Totalordnung). Laut Induktionsannahme gilt $k \notin T$ für alle $k \in \mathbb{N}$ mit $k < n + 1$, daher trifft die linke Bedingung

immer zu und es folgt $\forall m \in T : n+1 \leq m$. Wenn $n+1 \in T$, dann ist $n+1$ kleinstes Element von T, ein Widerspruch. Daher gilt auch für alle $k \in \mathbb{N}$ mit $k \leq n+1$, dass $k \notin T$.

Wir erhalten $\forall n \in \mathbb{N} : k \leq n \Rightarrow k \notin T$, insbesondere $\forall n \in \mathbb{N} : n \notin T$ bzw. $T = \emptyset$. □

KOROLLAR 1.3. *Jede nichtleere, nach unten beschränkte Teilmenge von $\mathbb{Z}$ besitzt ein kleinstes Element.*

BEWEIS. Sei $T \subseteq \mathbb{Z}$ und $T \geq -m$. Die Menge

$$T_1 = T + m = \{k \in \mathbb{Z} \mid \exists l \in T : k = l + m\} \subseteq \mathbb{N}$$

ist nichtleer und besitzt ein kleinstes Element n. Dann ist $n - m$ das kleinste Element von T, denn die Ordnungsrelation ist mit der Addition verträglich. □

SATZ 1.4 (q-adische Darstellung einer natürlichen Zahl). *Sei $q \in \mathbb{N}$ mit $q > 1$. Dann kann jede natürliche Zahl $n > 0$ eindeutig in der Form*

$$n = \sum_{i=0}^{k} a_i q^i$$

mit $k \in \mathbb{N}$, $a_i \in \{0, 1, \ldots, q-1\}$ für $0 \leq i \leq k$ und $a_k \neq 0$ geschrieben werden.

BEWEIS. Induktion nach dem größten $k \geq 0$ mit $q^k \leq n$.

Induktionsanfang: Für $k = 0$ gilt $n < q$ und $n = a_0$.

Induktionsannahme: Die Behauptung gelte für alle n mit $q^k \leq n < q^{k+1}$.

Induktionsschritt: Sei n mit $q^{k+1} \leq n < q^{k+2}$ gegeben. Dann existieren natürliche Zahlen a_{k+1} und $0 \leq r < q^{k+1}$ mit $n = a_{k+1}q^{k+1} + r$. Es gilt $a_{k+1} \in \{1, \ldots, q-1\}$, denn für $a_{k+1} \geq q$ folgt der Widerspruch $q^{k+2} > n = a_{k+1}q^{k+1} + r \geq a_{k+1}q^{k+1} \geq q^{k+2}$. Ebenso folgt für $a_{k+1} = 0$ ein Widerspruch $n = 0q^{k+1} + r = r < q^{k+1}$. Wir wenden die Induktionsannahme auf r an und erhalten $a_i \in \{0, 1, \ldots, q-1\}$ für $0 \leq i \leq k$ mit $r = \sum_{i=0}^{k} a_i q^i$. Wenn $r = 0$, dann setzen wir $a_i = 0$ für $0 \leq i \leq k$. Es folgt nun $n = a_{k+1}q^{k+1} + \sum_{i=0}^{k} a_i q^i$ und der Induktionsbeweis ist fertig.

Zum Beweis der Eindeutigkeit seien a_i und b_i zwei verschiedene Darstellungen von n. Wir ergänzen ggf. durch Koeffizienten 0, sodass beide Darstellungen dieselbe Zahl $k+1$ von Koeffizienten besitzen. Nun sei $0 \leq l \leq k$ die größte natürliche Zahl mit $a_l \neq b_l$. Nach der geometrischen Summenformel gilt $q^l = 1 + \sum_{i=0}^{l-1}(q-1)q^i$. Wir nehmen $a_l < b_l$ an und schließen aus $a_i = b_i$ für $i \in \{l+1, \ldots, k\}$

$$n = \sum_{i=0}^{l} a_i q^i + \sum_{i=l+1}^{k} a_i q^i = \sum_{i=0}^{l} b_i q^i + \sum_{i=l+1}^{k} a_i q^i,$$

daher $\sum_{i=0}^{l} a_i q^i = \sum_{i=0}^{l} b_i q^i$. Jedoch gilt

$$\sum_{i=0}^{l} b_i q^i = b_l q^l + \underbrace{\sum_{i=0}^{l-1} b_i q^i}_{\geq 0} \overset{b_l \geq a_l + 1}{\geq} a_l q^l + q^l = a_l q^l + 1 + \sum_{i=0}^{l-1}(q-1)q^i \geq$$

$$\overset{0 \leq a_i \leq q-1}{\geq} a_l q^l + 1 + \sum_{i=0}^{l-1} a_i q^i = \sum_{i=0}^{l} a_i q^i + 1 > \sum_{i=0}^{l} a_i q^i,$$

ein Widerspruch. □

Größter gemeinsamer Teiler (ggT), Euklidischer Algorithmus und Eindeutigkeit der Primfaktorenzerlegung.

DEFINITION. Seien $a, b \in \mathbb{N}$. Eine Zahl $d \in \mathbb{N}$ heißt $\mathrm{ggT}(a, b)$, wenn:

(1) $d \mid a \wedge d \mid b$
(2) $\forall d' \in \mathbb{N} : d' \mid a \wedge d' \mid b \Rightarrow d' \mid d$

SATZ 1.5 (Euklidischer Algorithmus). *Für zwei natürliche Zahlen $a, b \in \mathbb{N}$ existiert immer ein $\mathrm{ggT}(a, b)$, dieser kann durch den Euklidischen Algorithmus ermittelt werden. Ohne Beeinträchtigung der Allgemeinheit sei $a > b$:*

$$\begin{aligned}
a &= q_0 b + r_1 && (0 \leq r_1 < b)\\
b &= q_1 r_1 + r_2 && (0 \leq r_2 < r_1)\\
r_1 &= q_2 r_2 + r_3 && (0 \leq r_3 < r_2)\\
&\vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && (0 \leq r_n < r_{n-1})\\
r_{n-1} &= q_n r_n + r_{n+1} && (0 = r_{n+1} < r_n)
\end{aligned}$$

Die Folge r_i ist streng monoton fallend und nach unten durch 0 beschränkt, daher existiert ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$. Dann gilt $r_n = \mathrm{ggT}(a, b)$ und es existieren ganze *Zahlen $s, t \in \mathbb{Z}$ mit $as + bt = \mathrm{ggT}(a, b)$*

BEWEIS. Aus $r_{n-1} = q_n r_n$ folgt $r_n \mid r_{n-1}$. Aus $r_{n-2} = q_{n-1} r_{n-1} + r_n$ folgt $r_n \mid r_{n-2}$, induktiv erhalten wir schließlich $r_n \mid r_2$ und $r_n \mid r_1$. Daraus ergeben sich $r_n \mid b$ und $r_n \mid a$, daher ist r_n ein gemeinsamer Teiler von a und b.

Wenn $r' \mid a, b$ gilt, dann folgt $r' \mid r_1 = a - q_0 b$. Aus $r' \mid r_1$ folgt nun $r' \mid r_2 = b - q_1 r_1$ und aus $r_3 = r_1 - q_2 r_2$ folgt $r' \mid r_3$. Induktiv ergibt sich $r' \mid r_n$, somit ist r_n der $\mathrm{ggT}(a, b)$.

Für $i \in \{3, \ldots, n\}$ kann der Rest $r_i = r_{i-2} - q_{i-1} r_{i-1}$ durch r_{i-1} und r_{i-2} ausgedrückt werden. Rekursives Einsetzen liefert eine Darstellung $r_n = r_1 c + r_2 d$ mit $c, d \in \mathbb{Z}$, mittels $r_1 = a - q_0 b$ sowie $r_2 = b - q_1 r_1 = b(1 + q_0 q_1) - q_1 a$ erhalten wir die Darstellung $\mathrm{ggT}(a, b) = as + bt$ durch geeignete Zahlen $s, t \in \mathbb{Z}$. □

KOROLLAR 1.6 (Lemma von Euklid). *Wenn eine Primzahl p ein Produkt zweier natürlicher Zahlen a und b teilt, dann teilt p zumindest einen der Faktoren.*

BEWEIS. Wenn $p \nmid a$ gilt, dann folgt $\mathrm{ggT}(p, a) = 1$ und es existieren $s, t \in \mathbb{Z}$ mit $ps + at = 1$. Es folgt $b = b \cdot 1 = pbs + abt$ und aus $p \mid ab$ ergibt sich $p \mid b$. □

SATZ 1.7. *Eine natürliche Zahl $n > 1$ kann eindeutig als Produkt von endlich vielen der Größe nach geordneten Primzahlen dargestellt werden.*

BEWEIS. Die Existenz einer Faktorisierung wurde bereits im Lemma 1.3, Kapitel 1 gezeigt. Wenn es natürliche Zahlen $n > 1$ mit jeweils zwei verschiedenen Primfaktorenzerlegungen gibt, dann gibt es nach dem Wohlordnungsprinzip eine kleinste derartige natürliche Zahl a. Wir stellen diese Zahl durch $a = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s$ mit $r, s \geq 2$ dar, wobei die Primzahlen p_i und q_j jeweils aufsteigend geordnet sind, mit möglichen Wiederholungen von Primzahlen mit höherer Potenz in der Faktorisierung. Die Mengen $\{p_1, p_2, \ldots, p_r\}$ und $\{q_1, q_2, \ldots, q_s\}$ sind disjunkt, denn jede gemeinsame Primzahl könnte mit dem Ergebnis einer nicht eindeutig faktorisierbaren Zahl a' mit $1 < a' < a$ gekürzt werden, im Widerspruch zur Minimalität von a. Es gelten $p_1 \mid q_1 \ldots q_s$ und $p_1 \nmid q_1$, da p_1 und q_1 verschiedene Primzahlen sind, und nach dem Korollar 1.6 folgt $p_1 \mid q_2 \ldots q_s$. Durch Induktion folgt $p_1 \mid q_i \ldots q_s$ für alle $i \in \{2, \ldots, s\}$, somit auch $p_1 \mid q_s$, ein Widerspruch. Daher ist die Primfaktorenzerlegung einer natürlichen Zahl $n > 1$ eindeutig bestimmt. □

BEMERKUNG. In $\mathbb{N}$ können wir über die Primfaktorenzerlegung der Zahlen $a > 1$ und $b > 1$ den $\mathrm{ggT}(a, b)$ bestimmen:

$$a = \prod p_i^{\nu_i} \wedge b = \prod p_j^{\mu j} \quad \Rightarrow \quad \mathrm{ggT}(a, b) = \prod p_i^{min\{\nu_i, \mu_i\}}$$

2. Die ganzen Zahlen $\mathbb{Z}$

Die Konstruktion der ganzen Zahlen erfolgt mittels einer Äquivalenzrelation auf $\mathbb{N} \times \mathbb{N}$:

$$(m, n) \sim (p, q) :\Leftrightarrow m + q = p + n$$

Wir definieren $\mathbb{Z}$ als die Menge

$$\mathbb{Z} := \mathbb{N} \times \mathbb{N}/\sim,$$

die Äquivalenzklasse $\overline{(m, n)}$ repräsentiert die ganze Zahl $m - n$, wobei $m, n \in \mathbb{N}$.

Die Operationen $+$ und $\cdot$ sind definiert durch

$$\overline{(m_1, n_1)} + \overline{(m_2, n_2)} := \overline{(m_1 + m_2, n_1 + n_2)},$$
$$\overline{(m_1, n_1)} \cdot \overline{(m_2, n_2)} := \overline{(m_1 m_2 + n_1 n_2, m_1 n_2 + n_1 m_2)}.$$

Das Nullelement und das additiv inverse Element sind definiert durch

$$0 := \overline{(0, 0)},$$
$$-\overline{(m, n)} := \overline{(n, m)}$$

und das Einselement ist definiert durch $\overline{(1, 0)}$.

BEMERKUNGEN. Die Addition ist wohldefiniert und erfüllt (A) und (K). Aus $(m_1, n_1) \sim (p_1, q_1) \Leftrightarrow m_1 + q_1 = p_1 + n_1$ und $(m_2, n_2) \sim (p_2, q_2) \Leftrightarrow m_2 + q_2 = p_2 + n_2$ folgt

$$m_1 + m_2 + q_1 + q_2 = p_1 + p_2 + n_1 + n_2,$$

daher

$$(m_1 + m_2, n_1 + n_2) \sim (p_1 + p_2, q_1 + q_2).$$

Das Nullelement $\overline{(0, 0)}$ erfüllt $\overline{(m, n)} + \overline{(0, 0)} = \overline{(m, n)}$ und das additiv inverse Element $\overline{(n, m)}$ erfüllt $\overline{(m, n)} + \overline{(n, m)} = \overline{(m + n, m + n)} = \overline{(0, 0)}$ für alle $m, n \in \mathbb{N}$.

Die Multiplikation ist ebenfalls wohldefiniert (Übung) und erfüllt (A) und (K), das Einselement $\overline{(1, 0)}$ erfüllt $\overline{(1, 0)} \cdot \overline{(m, n)} = \overline{(m, n)} \cdot \overline{(1, 0)} = \overline{(m, n)}$ für alle $m, n \in \mathbb{N}$.

Die Distributivgesetze (D) können direkt verifiziert werden.

Somit ist $\mathbb{Z}$ ein kommutativer Ring mit Eins. Weiters ist $\mathbb{Z}$ nullteilerfrei, daher ein Integritätsbereich (ohne Beweis).

Der Monoid $(\mathbb{N}, +)$ kann durch einen injektiven Monoidhomomorphismus in $(\mathbb{Z}, +)$ *eingebettet* werden:

$$\iota : \mathbb{N} \longrightarrow \mathbb{Z}$$
$$n \longmapsto \overline{(n, 0)}$$

Wir identifizieren von nun an $\iota(\mathbb{N})$ mit $\mathbb{N}$.

Eine Totalordnung auf $\mathbb{Z}$ wird (mittels der Totalordnung auf $\mathbb{N}$) durch

$$\overline{(m_1, n_1)} \leq \overline{(m_2, n_2)} :\Leftrightarrow m_1 + n_2 \leq m_2 + n_1$$

definiert, diese Definition ist ebenfalls wohldefiniert auf den Äquivalenzklassen.

3. Die rationalen Zahlen $\mathbb{Q}$

Die mengentheoretische Konstruktion der rationalen Zahlen $\mathbb{Q}$ abstrahiert die bekannten Regeln des Bruchrechnens. Wir definieren auf $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ eine Äquivalenzrelation

$$(a, b) \sim (c, d) :\Leftrightarrow ad = bc$$

und definieren die rationalen Zahlen $\mathbb{Q}$ als die Menge

$$\mathbb{Q} := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim .$$

Im Sinne des Bruchrechnens entspricht eine Äquivalenzklasse allen möglichen Erweiterungen und Kürzungen eines gegebenen Bruches.

Die Operationen $+$ und $\cdot$ sind definiert durch

$$\overline{(a, b)} + \overline{(c, d)} := \overline{(ad + bc, bd)},$$
$$\overline{(a, b)} \cdot \overline{(c, d)} := \overline{(ac, bd)}.$$

Das Nullelement und das additiv inverse Element sind definiert durch

$$0 := \overline{(0, 1)},$$
$$-\overline{(a, b)} := \overline{(-a, b)}.$$

Das Einselement und das multiplikativ inverse Element von $\overline{(a, b)} \neq 0$ ($\Leftrightarrow a \neq 0$) sind definiert durch

$$1 := \overline{(1, 1)},$$
$$\left(\overline{(a, b)}\right)^{-1} := \overline{(b, a)}.$$

Bemerkung. Alle Operationen sind wohldefiniert und erfüllen (A) und (K), weiters gilt auch (D). Der Beweis dieser Gesetze erfolgt durch Nachrechnen. Daher ist $(\mathbb{Q}, +, \cdot)$ ein Körper.

Definition. Sei K eine Menge mit zwei Verknüpfungen $+, \cdot$ und einer Relation $\leq$. Dann heißt $(K, +, \cdot, \leq)$ ein *geordneter Körper*, wenn

- $(K, +, \cdot)$ ein Körper ist,
- $(K, \leq)$ eine totalgeordnete Menge ist,
- die Ordnung mit $+, \cdot$ verträglich ist:
  (14) $\forall x, y, z \in K : x \leq y \Rightarrow x + z \leq y + z$ (Monotoniegesetz d. Addition)
  (15) $\forall x, y, z \in K : x \leq y \wedge z \geq 0 \Rightarrow x \cdot z \leq y \cdot z$ (Monotonieges. d. Multiplikation)

Bemerkung. Ein geordneter Körper wird durch insgesamt 15 Axiome definiert: (A), (N), (I) und (K) jeweils für die Gruppen $(K, +)$ und $(K \setminus \{0\}, \cdot)$ sowie (D), dann die Axiome (R), (T), (AS) und das Totalordnungsaxiom für $(K, \leq)$, schließlich die Axiome (14) und (15).

Definition (Ordnung auf $\mathbb{Q}$). Wir definieren die *positiven rationalen Zahlen* durch

$$\mathbb{Q}_+ := \{\overline{(a, b)} \mid a, b \in \mathbb{Z} \text{ mit } (a > 0 \wedge b > 0) \vee (a < 0 \wedge b < 0)\}.$$

Auch diese Definition ist unabhängig von den Repräsentanten einer Äquivalenzklasse. Mit $P = \mathbb{Q}_+ \cup \{0\}$ und $-P = \{-\overline{(a, b)} \mid \overline{(a, b)} \in P\}$ erhalten wir $P \cup (-P) = \mathbb{Q}$ und $P \cap (-P) = \{0\}$. Weiters gelten für alle $x, y \in P$ die Inklusionen $x + y \in P$ und $x \cdot y \in P$. Wir setzen

$$\overline{(a, b)} \leq \overline{(r, s)} :\Leftrightarrow \overline{(r, s)} - \overline{(a, b)} \in P.$$

Diese Definition ergibt eine Totalordnung auf $\mathbb{Q}$ entsprechend den Axiomen (14) und (15), daher ist $\mathbb{Q}$ ein geordneter Körper (Übung).

PROPOSITION 3.1. *In einem geordneten Körper $(K, +, \cdot, \leq)$ gelten mit $x, y, z \in K$ folgende Rechenregeln:*

(1) $x \leq y \Leftrightarrow y - x \geq 0$
(2) $x \leq 0 \Leftrightarrow -x \geq 0$
(3) $x \leq y \Leftrightarrow -x \geq -y$
(4) $z \leq 0 \wedge x \leq y \Rightarrow x \cdot z \geq y \cdot z$
(5) $x \neq 0 \Rightarrow x^2 > 0 \qquad (\Rightarrow 1 > 0)$
(6) $0 < x < y \Rightarrow 0 < y^{-1} < x^{-1}$

BEWEIS. (1), (2), (3): Man addiert beidseitig $-x$ bzw. $-x - y$ und verwendet Axiom (14), für die Gegenrichtung addiert man beidseitig x bzw. $x + y$.

(4): Mit (15) folgt $z \leq 0 \Rightarrow -z \geq 0 \Rightarrow x{\cdot}(-z) \leq y{\cdot}(-z) \Rightarrow -(x{\cdot}z) \leq -(y{\cdot}z) \Rightarrow y{\cdot}z \leq x{\cdot}z$.

(5): Folgt aus Axiom (15) mittels Fallunterscheidung nach $x > 0 \Rightarrow x^2 = x \cdot x \geq 0$ und $x < 0 \Rightarrow x^2 = (-x) \cdot (-x) \geq 0$. Aus der Nullteilerfreiheit folgt nun $x^2 \neq 0$, daher $x^2 > 0$.

(6): Es gilt $\forall x > 0 : x^{-1} > 0$, denn $x^{-1} \leq 0$ ergibt mit Axiom (15) einen Widerspruch $1 = x^{-1} \cdot x \leq 0 \cdot x = 0$. Aus $0 < x < y$ und (15) folgt nun $x \cdot y \geq 0$ und mit der Nullteilerfreiheit $x \cdot y > 0$, daher $x^{-1} \cdot y^{-1} = (x \cdot y)^{-1} > 0$. Die Ungleichung $x < y$ und (15) ergeben $y^{-1} = x \cdot (x^{-1} \cdot y^{-1}) \leq y \cdot (x^{-1} \cdot y^{-1}) = x^{-1}$. Zusammen mit $x \neq y \Rightarrow x^{-1} \neq y^{-1}$ (denn $(x^{-1})^{-1} = x$) folgt die Aussage. □

4. Die reellen Zahlen $\mathbb{R}$

Bei den reellen Zahlen wird zu den Axiomen eines geordneten Körpers ein weiteres hinzugefügt:

DEFINITION (Ordnungsvollständigkeit).
(16) Jede nichtleere und nach oben beschränkte Teilmenge von $\mathbb{R}$ besitzt ein Supremum.

BEMERKUNG. Äquivalent zu (16) ist folgendes Axiom: Jede nichtleere und nach unten beschränkte Teilmenge besitzt ein Infimum. Für eine nichtleere und nach unten beschränkte Teilmenge M von $\mathbb{R}$ ist $-M$ nach oben beschränkt und es gilt $\sup(-M) = -\inf M$.

BEWEIS. Sei $M \neq \emptyset$. Dann gilt $s \leq M \Leftrightarrow -s \geq -M \Leftrightarrow -M \leq -s$, daher existiert nach (16) ein Supremum $\alpha = \sup(-M)$. Dieses Supremum erfüllt $-M \leq \alpha$ und $\forall \gamma \in \mathbb{R}$ mit $-M \leq \gamma$ gilt $\alpha \leq \gamma$. Dies ist äquivalent zu $-\alpha \leq M$ und $\forall \gamma \in \mathbb{R}$ mit $M \geq -\gamma$ gilt $-\alpha \geq -\gamma$. Wenn wir $\delta = -\gamma$ setzen, dann ist dies äquivalent zu $-\alpha \leq M$ und $\forall \delta \in \mathbb{R}$ mit $M \geq \delta$ gilt $-\alpha \geq \delta$. Daher ist $-\alpha$ das Infimum von M, somit besitzt jede nichtleere nach unten beschränkte Teilmenge ein Infimum.

Der Beweis der Gegenrichtung erfolgt analog, daher sind die beiden Axiome äquivalent. □

Das Axiom (16) beseitigt den Makel der Nicht-Vollständigkeit von $\mathbb{Q}$, es gilt:

$$\forall \alpha \in \mathbb{R} : \alpha = \sup\{x \in \mathbb{Q} \mid x < \alpha\} = \inf\{x \in \mathbb{Q} \mid \alpha < x\}$$

SATZ 4.1 (Dedekind). *Es existiert bis auf Isomorphie genau ein ordnungsvollständiger Körper, welcher $\mathbb{Q}$ als Teilkörper enthält.*

BEWEIS. Der Beweis erfolgt mittels der mengentheoretischen Konstruktion der reellen Zahlen durch die sog. Dedekind-Schnitte. □

SATZ 4.2 (Archimedische Eigenschaft). *Für beliebige $x, y \in \mathbb{R}$ mit $x > 0$ und $y > 0$ existiert ein $n \in \mathbb{N}$ mit $nx > y$.*

BEWEIS. Sei $A := \{nx \mid n \in \mathbb{N}\}$. Angenommen, für alle $n \in \mathbb{N}$ gilt $nx \leq y$, dann ist A durch y nach oben beschränkt und besitzt nach dem Axiom der Ordnungsvollständigkeit ein Supremum $\alpha = \sup A$. Aus $x > 0$ folgt $\alpha - x < \alpha$, daher ist $\alpha - x$ keine obere Schranke von A und $\exists n \in \mathbb{N} : nx > \alpha - x$. Dann folgt jedoch $\alpha < (n+1)x \in A$, ein Widerspruch. □

SATZ 4.3. *Seien $x, y \in \mathbb{R}$ mit $x < y$, dann existieren ein $q \in \mathbb{Q}$ und ein $r \in \mathbb{R} \setminus \mathbb{Q}$ mit $x < q < y$ und $x < r < y$.*

BEWEIS. Aus $x < y$ folgt $y - x > 0$ und nach der Archimedischen Eigenschaft $\exists n \in \mathbb{N} : n(y-x) > 1$. Wir wählen $m_1, m_2 \in \mathbb{Z}$ mit $m_1 > nx$ und $m_2 > -nx$, daher gilt $-m_2 < nx < m_1$. Wir setzen $M := \{k \in \mathbb{Z} \mid nx < k\}$. Da M nichtleer und nach unten beschränkt ist, existiert ein kleinstes Element $m \in M$. Aus $m - 1 \notin M$ folgt $m - 1 \leq nx$, daher $nx < m \leq nx + 1 < nx + n(y-x) = ny$. Die rationale Zahl $q = \frac{m}{n}$ erfüllt $x < q < y$.

Durch eine weitere Anwendung des vorangehenden Arguments können wir zwei rationale Zahlen q_1, q_2 mit $x < q_1 < q_2 < y$ finden. Da $\frac{\sqrt{2}}{2} \in (0,1)$ eine irrationale Zahl ist, erfüllt die irrationale Zahl $r = q_1 + (q_2 - q_1)\frac{\sqrt{2}}{2}$ die Ungleichungen $x < q_1 < r < q_2 < y$. □

DEFINITION (Absolutbetrag, Abstand, Vorzeichen). Seien $x, y \in \mathbb{R}$. Wir definieren:

$$|x| := \begin{cases} x & \text{wenn } x \geq 0 \\ -x & \text{wenn } x < 0 \end{cases} \qquad \text{(Absolutbetrag)}$$

$$d(x,y) := |x - y| \qquad \text{(Abstand)}$$

$$\operatorname{sgn}(x) := \begin{cases} 1 & \text{wenn } x > 0 \\ 0 & \text{wenn } x = 0 \\ -1 & \text{wenn } x < 0 \end{cases} \qquad \text{(Vorzeichen, Signum)}$$

PROPOSITION 4.4. *Es gelten für alle $x, y, z \in \mathbb{R}$ folgende Aussagen:*

(1) $|x| = |-x| \geq 0$, $|x| \geq x$, $|x| \geq -x$ *und* $|x| = 0 \Leftrightarrow x = 0$.
(2) $d(x,y) = d(y,x) \geq 0$ *und* $d(x,y) = 0 \Leftrightarrow x = y$.
(3) $|x + y| \leq |x| + |y|$; $d(x,z) \leq d(x,y) + d(y,z)$. *(Dreiecksungleichung)*
(4) $|x \cdot y| = |x| \cdot |y|$.

BEWEIS. Die Aussagen (1) folgen durch Fallunterscheidungen $x > 0 \Leftrightarrow -x < 0 \Rightarrow x = |x| = -(-x) = |-x| > 0 > -x$; $x = 0 \Leftrightarrow |x| = |-x| = x = -x = 0$; $x < 0 \Leftrightarrow -x > 0 \Rightarrow -x = |x| = |-x| > 0 > x$. Die Gleichung $|x| = 0$ kann daher nur bei $x = 0$ erfüllt sein,

Die Aussagen (2) folgen nun aus (1) und der Definition von $d(\cdot,\cdot)$.

Im Beweis von (3) verwenden wir $x \leq |x|$ und $-x \leq |x|$ sowie die Fallunterscheidungen $x + y \geq 0 \Rightarrow |x+y| = x + y \leq |x| + |y|$ bzw. $x + y < 0 \Rightarrow |x+y| = -x - y \leq |x| + |y|$. Es folgt nun $d(x,z) = |x - z| = |(x-y) + (y-z)| \leq |x-y| + |y-z| = d(x,y) + d(y,z)$.

Im Beweis von (4) verwenden wir die Fallunterscheidungen $x, y \geq 0 \Rightarrow |x \cdot y| = x \cdot y = |x| \cdot |y|$; $x \geq 0 \wedge y < 0 \Rightarrow |x \cdot y| = -(x \cdot y) = x \cdot (-y) = |x| \cdot |y|$; $x < 0 \wedge y \geq 0 \Rightarrow |x \cdot y| = -(x \cdot y) = (-x) \cdot y = |x| \cdot |y|$; $x, y < 0 \Rightarrow |x \cdot y| = (x \cdot y) = (-x) \cdot (-y) = |x| \cdot |y|$. □