Mathematik für Informatiker I

(Diskrete Mathematik)

– Vorlesungsskript WiSe 2016/17 –

Version: 4. November 2016

Universität Hamburg

Vorwort

Dies ist das Skript für die Vorlesung *Mathematik I für Studierende der Informatik (Diskrete Mathematik)* des Wintersemesters 2016/17. Das Skript ist eine leicht veränderte und angepasste Version des Skriptes von Stefan Geschke, welches sich wiederum an dem vom Thomas Andreae aus dem Wintersemester 2013/14 zur gleichen Vorlesung orientiert hat. Ziel der Vorlesung ist die Vermittlung allgemeiner mathematischer Grundlagen und Beweistechniken. Die folgenden Themen werden besprochen

- Grundlagen der Mathematik und Logik,
- Natürliche Zahlen und vollständige Induktion,
- Elementare Zahlentheorie,
- Elementare Kombinatorik,
- Graphentheorie,
- Algebraische Strukturen (Gruppen, Ringe und Körper).

Hamburg, Herbst 2016 Mathias Schacht

Ergänzende Literatur

[1] M. Aigner, *Diskrete Mathematik*, 5th ed., Vieweg Studium: Aufbaukurs Mathematik, Friedr. Vieweg & Sohn, Wiesbaden, 2004.

[2] G. Fischer, *Lineare Algebra*, 18th ed., Grundkurs Mathematik: Eine Einführung für Studienanfänger, Springer, 2014.

[3] J. Matoušek and J. Nešetřil, *Diskrete Mathematik: Eine Entdeckungsreise*, 2nd ed., Springer, 2007.

[4] A. Steger, *Diskrete Strukturen, Band 1: Kombinatorik, Graphentheorie, Algebra*, 2nd ed., Springer, 2007.

Inhaltsverzeichnis

KAPITEL 1

Mathematische Grundlagen und Logik

§1.1. Mengen

Definition 1.1. *Eine* Menge *ist eine Zusammenfassung bestimmter, wohlunterschiedener Objekte, die die* Elemente *der Menge genannt werden.*

Bei Mengen kommt es nicht auf die Reihenfolge der Elemente an. Auch können Elemente in einer Menge nicht mehrfach vorkommen. Eine Menge ist durch ihre Elemente eindeutig bestimmt. Daher schreiben wir $A = B$ für zwei Mengen A und B, wenn A und B dieselben Elemente haben.

Definition 1.2. *Ist x ein Element der Menge M, so schreiben wir $x \in M$. $x \notin M$ bedeutet, dass x kein Element von M ist. Sind A und B Mengen, so schreiben wir $A \subseteq B$, wenn A eine* Teilmenge *von B ist, also wenn jedes Element von A auch Element von B ist. Die (eindeutig bestimmte) Menge, die keine Elemente hat, heißt die* leere Menge. *Sie wird als $\{\}$ oder $\varnothing$ notiert.*

Mengen kann man notieren, indem man ihre Elemente in geschweiften Klammern angibt. $\{4, 7, 13\}$ bezeichnet zum Beispiel die Menge, deren Elemente die genau die Zahlen 4, 7 und 13 sind. Da es nur auf die Elemente selbst und nicht auf deren Reihenfolge ankommt, bezeichnen $\{3, 4, 5\}$ und $\{4, 5, 3\}$ dieselbe Menge. Wenn ein Element mehrfach genannt wird, so wird das ignoriert, da eine Menge jedes Element nur einmal enthält. Daher bezeichnen $\{1, 2, 1, 1\}$ und $\{1, 2\}$ dieselbe Menge. $\mathbb{Z} = \{\dots, -1, 0, 1, 2, \dots\}$ ist die Menge der ganzen Zahlen. $\mathbb{N}$ ist die Menge $\{1, 2, 3, \dots\}$ der natürlichen Zahlen. Viele Autoren lassen die natürlichen Zahlen bei 0 anfangen. Wir definieren $\mathbb{N}_0$ als die Menge der natürlichen Zahlen zusammen mit der 0, also $\mathbb{N}_0 = \{0, 1, 2, \dots\}$.

$$\{n\colon\ n \text{ ist eine natürliche Zahl mit } 5 < n < 10\}$$

ist die Menge der natürlichen Zahlen , die echte größer als 5 und echt kleiner als 10 sind, also die Menge $\{6, 7, 8, 9\}$. Auf diese Weise kann man auch unendliche Mengen notieren. So ist

$$\{n\colon\ n \text{ ist eine durch 2 teilbare natürliche Zahl}\}$$

die Menge der geraden natürlichen Zahlen.

§1.2. Elementare Logik

Definition 1.3. *Eine* Aussage *ist ein Satz, von dem man im Prinzip eindeutig feststellen kann, ob er wahr oder falsch ist. Ob eine Aussage wahr oder falsch ist, ist der* Wahrheitswert *der Aussage. Der Wahrheitswert „wahr“ wird dabei oft mit „w“ oder „1“ abgekürzt, der Wahrheitswert „falsch“ mit „f“ oder „0“.*

Der Satz „Die Straße ist nass“ ist eine Aussage. Ebenso sind „$2 + 5 = 7$“ und „$2 + 5 < 3$“ Aussagen, wobei die erste wahr und die zweite falsch ist. „Guten Abend!“ ist keine Aussage. Ebenso ist „$n^2 = 4$“ keine Aussage, da wir nicht feststellen können, ob diese Formel wahr oder falsch ist, solange wir nicht wissen, was n ist.

Aussagen können mit den logischen Verknüpfungen „und“, „oder“ und „nicht“ verknüpft werden. Allerdings ist die Bedeutung dieser Wörter in der Umgangssprache nicht immer ganz eindeutig. Daher ist es sinnvoll, diese Verknüpfungen für formale Zwecke zu präzisieren.

Definition 1.4. *Ist a eine Aussage, so ist die* Negation *von a die Aussage, die genau dann wahr ist, wenn a falsch ist. Die Negation von a wird $\neg a$ geschrieben und „nicht a“ gelesen. Sind a und b Aussagen, so ist die* Konjunktion *von a und b die Aussage, die genau dann wahr ist, wenn sowohl a als auch b wahr ist. Die Konjunktion von a und b wird $a \wedge b$ geschrieben und „a und b“ gelesen. Die* Disjunktion *von a und b ist die Aussage, die genau dann wahr ist, wenn mindestens eine der Aussagen a und b wahr ist. Die Disjunktion von a und b wird $a \vee b$ geschrieben und „a oder b“ gelesen.*

Den Wahrheitswert einer durch logische Verknüpfungen aus anderen Aussagen gebildeten Aussage in Abhängigkeit der Wahrheitswerte der Ausgangsaussagen kann man in Form einer *Wahrheitstafel* beschreiben:

a	$\neg a$
0	1
1	0

a	b	$a \wedge b$	$a \vee b$
0	0	0	0
0	1	0	1
1	0	0	1
1	1	1	1

Definition 1.5. *Weitere wichtige logische Verknüpfungen sind die* Implikation $\rightarrow$*, die* Äquivalenz $\leftrightarrow$ *und das exklusive Oder* xor*. Wir definieren diese Verknüpfungen mit Hilfe einer Wahrheitstafel.*

a	b	$a \rightarrow b$	$a \leftrightarrow b$	xor
0	*0*	*1*	*1*	*0*
0	*1*	*1*	*0*	*1*
1	*0*	*0*	*0*	*1*
1	*1*	*1*	*1*	*0*

Die Aussage $a \to b$ ist also immer dann wahr, wenn a falsch ist oder b wahr. Ist $a \to b$ wahr, so sagen wir „b folgt aus a“ oder „a impliziert b“. Die Aussage $a \leftrightarrow b$ ist immer dann wahr, wenn a und b entweder beide falsch oder beide wahr sind. Ist $a \leftrightarrow b$ wahr, so nennen wir a und b äquivalent. Die Zeichen $\to$ und $\leftrightarrow$ werden normalerweise nur in formalen Ausdrücken verwendet, während wir im normalen mathematischen Text $\Rightarrow$ und $\Leftrightarrow$ benutzen. Ein klassisches Beispiel ist die Aussage „wenn es regnet, ist die Straße nass“, die sich mit Hilfe von $\Rightarrow$ so schreiben lässt:

$$\text{Es regnet} \Rightarrow \text{Die Straße ist nass.}$$

(Wir ignorieren in diesem Beispiel das Problem, dass die Wahrheitswerte von „es regnet“ und „die Straße ist nass“ natürlich von Ort und Zeitpunkt abhängen. Wir können uns zum Beispiel vorstellen, dass wir Ort und Zeit schon fest gewählt haben.) Die Aussage $a \operatorname{xor} b$ ist genau dann wahr, wenn die Wahrheitswerte von a und b unterschiedlich sind.

Mit Hilfe von Wahrheitstafeln können wir die Wahrheitswerte komplizierterer Aussagen untersuchen, die durch Verknüpfungen einfacherer Aussagen entstanden sind. Seien zum Beispiel a, b und c Aussagen und e die Aussage $a \wedge (b \vee c)$. Falls die Wahrheitswerte von a, b und c bekannt sind, so können wir zunächst den Wahrheitswert von $b \vee c$ bestimmen und dann den von $a \wedge (b \vee c)$. Auf diese Weise erhält man folgende Wahrheitstafel:

a	b	c	$b \vee c$	$a \wedge (b \vee c)$
0	0	0	0	0
0	0	1	1	0
0	1	0	1	0
0	1	1	1	0
1	0	0	0	0
1	0	1	1	1
1	1	0	1	1
1	1	1	1	1

Wenn man eine entsprechende Wahrheitstafel für $(a \wedge b) \vee (a \wedge c)$ aufstellt, sieht man, dass $a \wedge (b \vee c)$ und $(a \wedge b) \vee (a \wedge c)$ äquivalent sind, unabhängig davon, welche Wahrheitswerte die Aussagen a, b und c haben. Aus diese Weise lassen sich Rechenregeln für $\vee$, $\wedge$ und $\neg$ nachweisen. Das ist das *Wahrheitstafelverfahren*. Wir halten zunächst folgenden Satz fest:

Satz 1.6. *Sind a, b und c Aussagen, so ist $a \wedge (b \vee c)$ äquivalent zu $(a \wedge b) \vee (a \wedge c)$.*

Eine weitere wichtige Regel ist die sogenannte *Kontraposition*, die man oft in Beweisen anwenden kann.

Satz 1.7. *Seien a und b Aussagen. Die Aussage $a \to b$ ist äquivalent zu $\neg b \to \neg a$.*

BEWEIS. Wir schreiben die entsprechende Wahrheitstafel auf.

a	b	$\neg a$	$\neg b$	$a \to b$	$\neg b \to \neg a$
0	0	1	1	1	1
0	1	1	0	1	1
1	0	0	1	0	0
1	1	0	0	1	1

Wie man leicht abliest, sind $a \to b$ und $\neg b \to \neg a$ in der Tat äquivalent. □

Beispiel 1.8. Der Satz „wenn es neblig ist, ist die Sicht schlecht“ ist äquivalent zu „wenn die Sicht nicht schlecht ist, dann ist es nicht neblig“.

Unter dem Stichwort „Boolesche Algebra“ werden später noch weitere Rechenregeln für logische Verknüpfungen festhalten.

Definition 1.9. *Eine* Aussageform *ist eine Aussage, in der eine Konstante durch eine Variable ersetzt wurde. So erhält man aus einer Aussage a eine Aussageform $a(x)$.*

„$2 + 5 = 7$“ ist eine Aussage. Daraus lässt sich zum Beispiel die Aussageform „$2 + x = 7$“ ableiten. Sei $a(x)$ diese Aussageform. Ein Wahrheitswert von $a(x)$ lässt sich nicht angeben, da wir nicht wissen, welchen Wert x hat. Wenn wir für x einen Wert einsetzen, dann erhalten wir wieder eine Aussage. So ist $a(5)$, also die ursprüngliche Aussage, wahr, während $a(2)$, also die Aussage „$2 + 2 = 7$“, falsch ist.

Auch Aussageformen können mittels logischer Verknüpfungen verknüpft werden. Ist $a(x)$ die Aussageform „$2+x \leqslant 7$“, so ist $\neg a(x)$ die Aussageform „$2+x \nleqslant 7$“ oder, anders geschrieben, „$2 + x > 7$“. Ist $a(x)$ die Aussageform „$x = 2$“ und $b(x)$ die Aussageform „$x^2 = 4$“, so verstehen wir, was „$a(x) \Rightarrow b(x)$“ bedeutet:

$$\text{Wenn } x = 2 \text{ ist, so ist } x^2 = 4.$$

Setzen wir für x konkrete natürliche Zahlen ein, so erhalten wir immer eine wahre Aussage. Mit anderen Worten, die Aussage

$$\text{Für alle natürlichen Zahlen } x \text{ gilt: } a(x) \Rightarrow b(x)$$

ist wahr. Den Satzteil „für alle natürlichen Zahlen x“ nennen wir einen *Quantor*. Mit Hilfe von Quantoren können wir aus Aussageformen wieder Aussagen machen.

Definition 1.10. *Sei $a(x)$ eine Aussageform und M eine Menge. Dann ist*

$$(\exists x \in M) a(x)$$

die Aussage, die genau dann wahr ist, wenn es mindestens ein Element x der Menge M gibt, so dass $a(x)$ gilt. $(\exists x \in M) a(x)$ wird „es gibt ein x in M mit $a(x)$“ gelesen. Das Zeichen $\exists$ ist der Existenzquantor.

$$(\forall x \in M) a(x)$$

ist die Aussage, die genau dann wahr ist, wenn $a(x)$ für alle Elemente x der Menge M gilt. $(\forall x \in M)a(x)$ *wird „für alle x in M gilt $a(x)$“ gelesen. Das Zeichen* $\forall$ *ist der* Allquantor.

Im Zusammenhang mit Quantoren, und auch sonst, werden wir Klammern immer so setzen, beziehungsweise weglassen, dass die Lesbarkeit optimal ist.

Ein typisches Beispiel einer *Existenzaussage*, also einer Aussage, die mit einem Existenzquantor beginnt, ist die Aussage $\exists x \in \mathbb{N}(x^2 = 4)$. Ein typisches Beispiel einer *Allaussage*, also einer Aussage, die mit einem Allquantor beginnt, ist die Aussage $\forall x \in \mathbb{N}(x^2 > 0)$.

Oft betrachten wir Aussageformen wie „$(n+1)^2 = n^2+2n+1$“. Bei dieser Aussageform ist klar, dass für n eine Zahl eingesetzt werden soll, und nicht anderes. Außerdem steht die Variable n üblicher Weise für eine natürliche Zahl. Unsere Erfahrung sagt uns also, dass wir, wenn wir „$(n + 1)^2 = n^2 + 2n + 1$“ hinschreiben, wir oft eigentlich „$\forall n \in \mathbb{N}((n + 1)^2 = n^2 + 2n + 1)$“ meinen.

Die Negation $\neg(\forall x \in M)a(x)$ der Allaussage $(\forall x \in M)a(x)$ ist äquivalent zu der Existenzaussage $(\exists x \in M)\neg a(x)$. Das wird an einem Beispiel schnell klar: „Alle Autos in Hamburg sind blau“ ist sicher falsch, es gilt vielmehr „nicht alle Auto in Hamburg sind blau“, was äquivalent zu der Aussage „es gibt in Hamburg (mindestens) ein Auto, das nicht blau ist“ ist. Analog ist $\neg(\exists x \in M)a(x)$ zu $(\forall x \in M)\neg a(x)$ äquivalent.

§1.3. Mengenoperationen

Wir definieren einige Verknüpfungen von Mengen, mit denen sich ganz ähnlich rechnen lässt wie mit den Verknüpfungen $\wedge$, $\vee$ und $\neg$ von Aussagen. Die Rechengesetze, die für die logischen Verknüpfungen (von Aussagen) und für die entsprechenden Verknüpfungen von Mengen gelten, fasst man unter dem Begriff „Boolesche Algebra“ zusammen.

Definition 1.11. *Seien A und B Mengen. Dann ist die* Vereinigung *von A und B definiert als*

$$A \cup B := \{x \colon x \in A \vee x \in B\}.$$

(Hier benutzen wir das Zeichen $:=$ um auszudrücken, dass es sich um eine Definition handelt.) Der Schnitt *oder* Durchschnitt *von A und B ist die Menge*

$$A \cap B := \{x \colon x \in A \wedge x \in B\}.$$

Zwei Mengen A und B heißen disjunkt, *falls $A \cap B = \varnothing$. Die* mengentheoretische Differenz *von A und B ist die Menge*

$$A \smallsetminus B := \{x \in A \colon x \notin B\}.$$

Schon anhand der Definition von $\cup$ und $\cap$ sieht man, dass $\cup$ etwas mit $\vee$ zu tun hat und $\cap$ mit $\wedge$. Und in der Tat verhalten sich $\cap$ und $\cup$ ähnlich wie $\wedge$ und $\vee$. Eine Operation auf Mengen, die sich analog zur Negation verhält, ist die Komplementbildung.

Definition 1.12. *Für eine Menge M sei*

$$\wp(M) := \{x \colon x \subseteq M\}$$

die Potenzmenge *von M. Wir fixieren M und betrachten nur Teilmengen von M. Für $A \in \wp(M)$ sei*

$$\overline{A} := \{x \in M \colon x \notin A\}$$

das Komplement *von A in M.*

Wir stellen fest, das $\wp(M)$ unter $\cup$, $\cap$ und Komplementbildung *abgeschlossen* ist. D.h., für alle $A, B \in \wp(M)$ sind $A \cap B$, $A \cup B$ und $\overline{A}$ wieder Elemente von $\wp(M)$.

Rechenregeln für die Mengenoperationen $\cap$, $\cup$ und Komplementbildung können wir wieder mit dem Wahrheitstafelverfahren herleiten. Seien zum Beispiel A, B und C Teilmengen einer Menge M.

Satz 1.13. *Es gilt $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.*

Beweis. Wir wissen schon, dass $A \cap (B \cup C)$ und $(A \cap B) \cup (A \cap C)$ Teilmengen von M sind. Also müssen wir nur zeigen, dass die beiden Mengen genau dieselben Elemente von M enthalten.

Es gilt

$$A \cap (B \cup C) = \{x \in M \colon x \in A \wedge (x \in B \vee x \in C)\}$$

sowie

$$(A \cap B) \cup (A \cap C) = \{x \in M \colon (x \in A \wedge x \in B) \vee (x \in A \vee x \in C)\}.$$

Wir fixieren nun ein beliebiges Element x von M. Sei a die Aussage $x \in A$, b die Aussage $x \in B$ und c die Aussage $x \in C$. Man beachte, dass wir hier so tun, als wären a, b und c Aussagen, da wir das x vorher fixiert haben und wir es jetzt wie eine Konstante behandeln können.

Nach Satz 1.6 sind $a \wedge (b \vee c)$ und $(a \wedge b) \vee (a \wedge c)$ äquivalent. Damit gilt

$$x \in A \cap (B \cup C) \Leftrightarrow a \wedge (b \vee c) \Leftrightarrow (a \wedge b) \vee (a \wedge c) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$$

Also haben $A \cap (B \cup C)$ und $(A \cap B) \cup (A \cap C)$ dieselben Elemente und sind damit gleich. □

Wir haben bisher die Frage nach der Gleichheit zweier Mengen auf die Frage zurückgeführt, ob zwei Aussagen äquivalent sind. Die letztere Frage ließ sich mit Hilfe des Wahrheitstafelverfahrens klären. Damit lässt sich das Wahrheitstafelverfahren manchmal einsetzen, um die Gleichheit zweier Mengen nachzuweisen. Im allgemeinen

ist es allerdings meistens ratsam, die Gleichheit zweier Mengen A und B nachzurechnen, indem man zunächst $A \subseteq B$ und dann $B \subseteq A$ zeigt.

Beispiel 1.14. Wir beweisen die Gleichung $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ ohne das Wahrheitstafelverfahren. Als erstes zeigen wir $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Dazu müssen wir zeigen, dass jedes Element von $A \cap (B \cup C)$ auch ein Element von $(A \cap B) \cup (A \cap C)$ ist.

Sei also $x \in A \cap (B \cup C)$. Dann ist x sowohl in A als auch in $B \cup C$ enthalten. Also ist x in B oder in C enthalten. Ist x in B enthalten, so gilt $x \in A \cap B$. Ist x in C enthalten, so gilt $x \in A \cap C$. Damit ist x in $A \cap B$ oder in $A \cap C$ enthalten. Also gilt $x \in (A \cap B) \cup (A \cap C)$.

Das zeigt $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$. Wir zeigen nun $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$.

Sei $x \in (A \cap B) \cup (A \cap C)$. Dann ist x in $A \cap B$ oder in $A \cap C$ enthalten. Wir nehmen zunächst an, dass $x \in A \cap B$ gilt. Dann ist x in A und in B enthalten. Damit ist x aber auch in $B \cup C$ enthalten. Es folgt $x \in A \cap (B \cup C)$.

Nun nehmen wir an, dass $x \in A \cap C$ gilt. Wie eben sehen wir, dass $x \in A \cap (B \cup C)$ gilt.

Also gilt $x \in A \cap (B \cup C)$ unabhängig davon, ob x ein Element von $A \cap B$ oder $A \cap C$ ist.

Das zeigt $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$. Insgesamt folgt nun die Gleichheit $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Definition 1.15. *Sind A und B Mengen, so bezeichnet man mit $A \times B$ die Menge $\{(a, b) \colon a \in A \text{ und } b \in B\}$ aller geordneten Paare (a, b), deren erste Komponente a ein Element von A ist und deren zweite Komponente b ein Element von B sind. $A \times B$ heißt das* kartesische Produkt *der Mengen A und B. Mit A^2 bezeichnet man die Menge $A \times A$.*

*A^3 ist die Menge $\{(a_1, a_2, a_3) \colon a_1, a_2, a_3 \in A\}$ aller Tripel von Elementen von A. Analog ist für jede natürliche Zahl $n \geqslant 1$ A^n die Menge $\{(a_1, \ldots, a_n) \colon a_1, \ldots, a_n \in A\}$ aller n-*Tupel *von Elementen von A.*

Zum Beispiel ist

$$\{1, 2, 3\} \times \{4, 5\} = \{(1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5)\}.$$

§1.4. Abbildungen

Definition 1.16. *Eine* Abbildung *von einer Menge A in eine Menge B ist eine Zuordnung, die jedem Element von A ein Element von B zuordnet. Abbildungen werden oft auch* Funktionen *genannt. Ist f eine Abbildung von A nach B, so schreiben wir $f \colon A \to B$. Dabei wird A der* Definitionsbereich *von f genannt und B der* Wertevorrat. *Auch der Begriff* Vorbereich *für A und* Nachbereich *für B ist sinnvoll. Schließlich wird*

B manchmal auch der Wertebereich *von f genannt, wobei das zu Verwechslungen mit dem* Bild *von f führen kann, welches wir weiter unten definieren.*

Für jedes $a \in A$ bezeichnen wir mit $f(a)$ das Element von B, das die Funktion f dem Element a zuordnet. Falls f einem Element $a \in A$ also $b \in B$ zuordnet, so schreiben wir $f(a) = b$ und sagen „f bildet a auf b ab“. Das Element b heißt der Wert *oder der* Funktionswert *von f an der Stelle a. Man kann anstelle von $f(a) = b$ auch $a \mapsto b$ schreiben, wenn klar ist, welche Funktion f gemeint ist.*

Das Bild *von f ist die Menge $\{f(x) \colon x \in A\}$.*

Der Name *Wertebereich* wird von manchen Autoren für das Bild einer Funktion verwendet und von anderen für den Wertevorrat. Um Missverständnissen vorzubeugen, verwenden wir diesen Begriff gar nicht.

Beispiel 1.17. (1) Eine Funktion f von der Menge $\mathbb{N}$ der natürlichen Zahlen in die natürlichen Zahlen kann zum Beispiel durch eine Formel gegeben sein: $f(n) = n^2$. Ein Schreibweise, die alle wesentlichen Informationen beinhaltet, wäre dann

$$f \colon \mathbb{N} \to \mathbb{N}; n \mapsto n^2.$$

(2) Der Ausdruck $g \colon \mathbb{N}^2 \to \mathbb{N}, (m, n) \mapsto m + n$ beschreibt eine Funktion von der Menge der Paare natürlicher Zahlen in die Menge der natürlichen Zahlen, die der Gleichung $g((m, n)) = m + n$ genügt. Anstelle von $g((m, n))$ schreiben wir auch $g(m, n)$.

(3) Funktionen mit endlichem Definitionsbereich kann man auch in Form einer Tabelle angeben. Sei zum Beispiel $A = \{1, 2, 3, 4, 5\}$ und $B = \{q, w, e, r, t, z\}$. Dann definiert die folgende Tabelle die Funktion $f \colon A \to B$:

a	1	2	3	4	5
f(a)	w	q	t	w	e

Es gilt nun $f(1) = w$, $f(2) = q$ und so weiter.

Definition 1.18. *Eine Abbildung $f \colon A \to B$ heißt*

(1) injektiv, *falls für alle $x, y \in A$ gilt: Ist $x \neq y$, so ist $f(x) \neq f(y)$.*

(2) surjektiv, *falls es für alle $b \in B$ mindestens ein $a \in A$ gibt, so dass $f(a) = b$ gilt.*

(3) bijektiv, *falls sie injektiv und surjektiv ist.*

Beispiel 1.19. (1) Sei $A = \{1, 2, 3\}$ und $B = \{1, 2, 3\}$. Die Abbildung $f \colon A \to B$ mit $f(1) = 1$, $f(2) = 1$ und $f(3) = 2$ ist weder injektiv noch surjektiv.

(2) Seien A und B wie in (1). Die Funktion $g \colon A \to B$ mit $g(1) = 2$, $g(2) = 3$ und $g(3) = 1$ ist sowohl injektiv als auch surjektiv, also bijektiv.

(3) Sei wieder $A = \{1, 2, 3\}$ aber $B = \{3, 7\}$. Die Abbildung $f \colon A \to B$ mit $f(1) = 3$, $f(2) = 7$ und $f(3) = 3$ ist surjektiv, aber nicht injektiv.

(4) Sei nun A wie in (1)–(3) und $B = \{1, 2, 3, 4\}$. Die Funktion $f\colon A \to B$ mit $f(1) = 2$, $f(2) = 1$, $f(3) = 4$ ist injektiv, aber nicht surjektiv.

(5) Die Abbildung $h\colon \mathbb{N} \to \mathbb{N}; n \mapsto n^2$ ist nicht surjektiv, da es zum Beispiel kein $a \in \mathbb{N}$ gibt, für das $h(a) = 3$ gilt.

Das kann man wie folgt einsehen: Angenommen, es gäbe doch ein $a \in \mathbb{N}$ mit $h(a) = a^2 = 3$. Dann ist a entweder $\sqrt{3}$ oder $-\sqrt{3}$. Beide Zahlen, $\sqrt{3}$ und $-\sqrt{3}$, sind aber keine Elemente von $\mathbb{N}$. Das widerspricht der Annahme $a \in \mathbb{N}$.

Eine andere MÃűglichkeit zu zeigen, dass 3 nicht im Bild von f liegt ist die folgende: Es gelten $1^2 = 1 < 3$ und $2^2 = 4 > 3$. Für alle $n \geqslant 2$ ist $n^2 \geqslant 2^2$ und damit $n^2 > 3$. Damit gibt es kein $n \in \mathbb{N}$ mit $n^2 = 3$.

Die Abbildung h ist aber injektiv. Seien nämlich $x, y \in \mathbb{N}$ mit $x \neq y$. Dann ist entweder $x < y$ oder $y < x$. Wir betrachten nur den ersten Fall, der zweite Fall kann genauso behandelt werden. Wir nehmen also $x < y$ an. (Später werden wir in so einer Situation zum Beispiel schreiben „ohne Beschränkung der Allgemeinheit (o.B.d.A.) können wir $x < y$ annehmen“.) Sei $a = y - x$. Dann ist $y = x + a$ und $y^2 = x^2 + 2xa + a^2$. Wegen $x, a > 0$ gilt $2xa + a^2 > 0$ und damit ist $y^2 > x^2$. Insbesondere gilt

$$h(x) = x^2 \neq y^2 = h(y).$$

Das zeigt, dass h injektiv ist.

Definition 1.20. *Für eine natürliche Zahl n versteht man unter einer n-*stelligen Verknüpfung *oder einer n-*stelligen Operation *auf einer Menge M eine Abbildung $f\colon M^n \to M$.*

Der wichtigste Spezialfall ist der einer *binären* Verknüpfung $f\colon M^2 \to M$. Beispiele binärer Verknüpfungen sind die Addition $+\colon \mathbb{N}^2 \to \mathbb{N}; (m, n) \mapsto m + n$ und die Multiplikation $\cdot\colon \mathbb{N}^2 \to \mathbb{N}; (m, n) \mapsto m \cdot n$.

§1.5. Boolesche Algebra

Wir haben schon gesehen, dass sich die Mengenoperationen $\cap$, $\cup$ und Komplementbildung ganz analog zu den logischen Verknüpfungen $\wedge$, $\vee$ und $\neg$ verhalten. Und in der Tat kann man die Mengenoperationen und die logischen Verknüpfungen mit einem gemeinsamen Begriff beschreiben.

Definition 1.21. *Gegeben sei eine Menge B, die mindestens die zwei verschiedene Elemente 1 und 0 enthält, zusammen mit der einstelligen Verknüpfung $\neg\colon B \to B$ und den zwei zweistelligen Verknüpfungen $\sqcap, \sqcup\colon B^2 \to B$. $(B, \sqcap, \sqcup, \neg, 0, 1)$ heißt eine* Boolesche Algebra, *wenn für alle $a, b, c \in B$ die folgenden Gleichungen gelten:*

(A1) Assoziativgesetze:

- $a \sqcap (b \sqcap c) = (a \sqcap b) \sqcap c$

- $a \sqcup (b \sqcup c) = (a \sqcup b) \sqcup c$

(A2) Kommutativgesetze:

- $a \sqcap b = b \sqcap a$
- $a \sqcup b = b \sqcup a$

(A3) Distributivgesetze:

- $a \sqcap (b \sqcup c) = (a \sqcap b) \sqcup (a \sqcap c)$
- $a \sqcup (b \sqcap c) = (a \sqcup b) \sqcap (a \sqcup c)$

(A4) Beschränkheit:

- $a \sqcap 1 = a$
- $a \sqcup 0 = a$

(A5) Komplementierung:

- $a \sqcap \neg a = 0$
- $a \sqcup \neg a = 1$

Die Aussagen (A1)–(A5) in Definition 1.21 sind die *Axiome* für Boolesche Algebren.

Beispiel 1.22. (1) Die *Schaltalgebra* ist die Menge $\{0, 1\}$ der Wahrheitswerte mit den Verknüpfungen $\wedge$, $\vee$ und $\neg$. Die Schaltalgebra ist eine Boolesche Algebra, wie man mit Hilfe des Wahrheitstafelverfahrens leicht nachrechnen kann.

(2) Ist M eine Menge, so ist $\wp(M)$ mit den Verknüpfungen $\cap$, $\cup$ und Komplementbildung sowie den Konstanten $1 := M$ und $0 := \varnothing$ eine Boolesche Algebra, die *Potenzmengenalgebra* von M. Dass Potenzmengenalgebren wirklich Boolesche Algebren sind, folgt aus der Tatsache, dass die Schaltalgebra die Axiome einer Booleschen Algebra erfüllt, zusammen mit der Übersetzung von Fragen der Gleichheit von Mengen in Fragen der Äquivalenz von Aussagen, die wir oben schon diskutiert haben.

(3) Wir betrachten noch einen speziellen Fall, nämlich eine Boolesche Algebra, die im wesentlichen genau die Potenzmengenalgebra auf einer achtelementigen Menge ist, die wir aber anders aufschreiben. Es sei $B := \{w, f\}^8$, also die Menge aller 8-Tupel der Wahrheitswerte w und f. Man kann B zum Beispiel als Menge aller möglichen Bytes interpretieren. Weiter sei

$$1 := (w, w, w, w, w, w, w, w)$$

und

$$0 = (f, f, f, f, f, f, f, f).$$

Die Operationen definieren wir jetzt wie folgt:

Für $a, b \in B$ mit $a = (a_1, \ldots, a_8)$ und $b = (b_1, \ldots, b_8)$ sei

$$a \sqcap b := (a_1 \wedge b_1, \ldots, a_8 \wedge b_8),$$

$$a \sqcup b := (a_1 \vee b_1, \ldots, a_8 \vee b_8)$$

und

$$\neg a := (\neg a_1, \ldots, \neg a_8).$$

Dann ist $(B, \sqcap, \sqcup, \neg, 0, 1)$ eine Boolesche Algebra, wie man leicht nachrechnet.

Alle Aussagen, die sich aus (A1)–(A5) ableiten lassen, gelten für alle Booleschen Algebren, inbesondere also für die Schaltalgebra und alle Potenzmengenalgebren. Diese Allgemeinheit ist die Stärke der *axiomatischen Methode*, bei der Sätze aus Axiomen gefolgert werden und nicht nur für bestimmte Strukturen, wie zum Beispiel die natürlichen Zahlen oder eine bestimmte Boolesche Algebra, bewiesen werden.

Wir geben Beispiele für die axiomatische Methode und beweisen ein paar einfache Regeln für Boolesche Algebren. Sei $(B, \sqcap, \sqcup, \neg, 0, 1)$ eine Boolesche Algebra.

Satz 1.23. *Für alle $a \in B$ gilt $a \sqcap a = a$ und $a \sqcup a = a$.*

Beweis. Es gilt

$$a \sqcap a \overset{(A4)}{=} (a \sqcap a) \sqcup 0 \overset{(A5)}{=} (a \sqcap a) \sqcup (a \sqcap \neg a) \overset{(A3)}{=} a \sqcap (a \sqcup \neg a) \overset{(A5)}{=} a \sqcap 1 \overset{(A4)}{=} a.$$

Auf dieselbe Weise rechnen wir $a \sqcup a = a$ nach.

$$a \sqcup a \overset{(A4)}{=} (a \sqcup a) \sqcap 1 \overset{(A5)}{=} (a \sqcup a) \sqcap (a \sqcup \neg a) \overset{(A3)}{=} a \sqcup (a \sqcap \neg a) \overset{(A5)}{=} a \sqcup 0 \overset{(A4)}{=} a.$$

Damit haben wir die beiden Gleichung aus den Axiomen (A1)–(A5) hergeleitet. □

In diesem Beweis fällt auf, dass wir den Beweis der Gleichung $a \sqcap a = a$ in den Beweis der Gleichung $a \sqcup a = a$ übersetzen können, indem wir $\sqcap$ und $\sqcup$ vertauschen und ebenso 0 und 1. Das funktioniert, da die Axiome (A1)–(A5) aus Paaren von Gleichungen bestehen, die jeweils durch diese Vertauschungen auseinander hervorgehen.

Satz 1.24 (Dualitätsprinzip für Boolesche Algebren)**.** *Jede Aussage, die eine Folgerung aus den Axiomen (A1)–(A5) ist, geht in eine gültige Aussage über, wenn man in ihr überall die Zeichen $\sqcap$ und $\sqcup$ sowie die Zeichen 0 und 1 vertauscht.*

Satz 1.25. *Für alle $a \in B$ gilt $a \sqcap 0 = 0$ und $a \sqcup 1 = 1$.*

Beweis. Es gilt

$$a \sqcap 0 = a \sqcap (a \sqcap \neg a) = (a \sqcap a) \sqcap \neg a = a \sqcap \neg a = 0.$$

Die Behauptung $a \sqcap 1 = 1$ folgt aus $a \sqcap 0 = 0$ nach dem Dualitätsprinzip. □

Wir schließen diesen Abschnitt mit zwei wichtigen Regeln für Boolesche Algebren, die aus den Axiomen folgen, deren Beweis wir aber nicht angeben.

Satz 1.26 (De Morgansche Regeln)**.** *Für alle $a, b \in B$ gilt $\neg(a \sqcap b) = \neg a \sqcup \neg b$ und $\neg(a \sqcup b) = \neg a \sqcap \neg b$.*

Der Beweis der de Morganschen Regeln aus den Axiomen (A1)–(A5) ist deutlich aufwendiger als die Beweise der Sätze 1.23 und 1.25. Mit Hilfe des Wahrheitstafelverfahrens lassen sich die de Morganschen Regeln für die Schaltalgebra leicht nachrechen. Man

kann zeigen, dass alle Gleichungen, wie zum Beispiel die de Morganschen Regeln, die in der Schaltalgebra gelten, auch in allen anderen Booleschen Algebren gelten. Damit kann das Wahrheitstafelverfahren für Gleichungen, in denen nur die Konstanten 0 und 1 auftreten, in beliebigen Booleschen Algebren eingesetzt werden.

§1.6. Summen- und Produktzeichen

Bevor wir uns eingehend mit den bekannten Zahlenbereichen $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$ befassen führen wir eine Notation ein, die sich bald als nützlich erweisen wird. Die *reellen Zahlen* $\mathbb{R}$ sind die bekannten Zahlen auf der Zahlengerade wie -1, 0, 2.5, $-\frac{10}{7}$, e und π, für die die üblichen Rechenregeln gelten.

Definition 1.27. *Für reelle Zahlen $a_1, \ldots, a_n$ sei*

$$\sum_{i=1}^{n} a_i = a_1 + a_2 + \ldots + a_n.$$

Dabei heißt i der Laufindex*, 1 ist die* untere Summationsgrenze *und n die* obere Summationsgrenze*.*

Der Laufindex muss nicht mit i bezeichnet werden und die untere Summationsgrenze muss nicht 1 sein. So ist zum Beispiel

$$\sum_{j=0}^{4} 2^j = 2^0 + 2^1 + 2^2 + 2^3 + 2^4 = 31.$$

Summen mit wechselnden Vorzeichen, wie zum Beispiel $a_1 - a_2 + a_3 - a_4$ kann man bequem mit Hilfe von Potenzen von -1 schreiben. Dabei muss man aber genau aufpassen, welche Vorzeichen man erzeugt:

$$\sum_{i=1}^{4} (-1)^i a_i = -a_1 + a_2 - a_3 + a_4$$

$$\sum_{i=1}^{4} (-1)^{i+1} a_i = a_1 - a_2 + a_3 - a_4$$

Falls $a_1 = \cdots = a_n = a$ gilt, so ist $\sum_{i=1}^{n} a_i = na$.

Das bekannte Distributivgesetz lautet $a(b + c) = ab + ac$. Das Gesetz gilt auch für mehr als zwei Summanden. Für alle reellen Zahlen $a, b_1, \ldots, b_n$ ist

$$a \sum_{i=1}^{n} b_i = a(b_1 + \ldots + b_n) = ab_1 + \ldots + ab_n = \sum_{i=1}^{n} ab_i.$$

Mit Hilfe des Distributivgesetzes können wir Ausdrücke wie $(a + b)(c + d)$ ausmultiplizieren und erhalten

$$(a + b)(c + d) = ac + ad + bc + bd.$$

Allgemein gilt

$$(a_1 + \ldots + a_m)(b_1 + \ldots + b_n) = a_1b_1 + \ldots + a_1b_n + \ldots + a_mb_1 + \ldots + a_mb_n.$$

Mit dem Summenzeichen geschrieben erhalten wir

$$\left(\sum_{i=1}^{m} a_i\right)\left(\sum_{j=1}^{n} b_j\right) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j.$$

Da wir nach dem Kommutativgesetz für die Addition die Summanden vertauschen können ohne den Wert der Summe zu ändern, ist

$$\sum_{i=1}^{m}\sum_{j=1}^{n} a_i b_j = \sum_{j=1}^{n}\sum_{i=1}^{m} a_i b_j.$$

Auf der Änderung der Summationsreihenfolge beruht auch die Gleichung

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i.$$

Oft kann man dieselben Summen unterschiedlich aufschreiben. So ist zum Beispiel

$$\sum_{i=0}^{3} a_{2i+1} = a_1 + a_3 + a_5 + a_7 = \sum_{i=1}^{4} a_{2i-1}.$$

Bemerkung 1.28. Analog zum Summenzeichen kann man auch das Produktzeichen definieren. Sind $a_1, \ldots, a_n$ reelle Zahlen, so setzt man

$$\prod_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

KAPITEL 2

Natürliche Zahlen und vollständige Induktion

§2.1. Natürliche Zahlen

Auf den natürlichen Zahlen $\mathbb{N} = \{1, 2, 3, \dots\}$ gelten die bekannten Rechengesetze:

(1) Assoziativgesetze:
- $a + (b + c) = (a + b) + c$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(2) Kommutativgesetze:
- $a + b = b + a$
- $a \cdot b = b \cdot a$

(3) Distributivgesetz:
- $a \cdot (b + c) = a \cdot b + a \cdot c$

(4) Existenz eines neutralen Elements der Multiplikation:
- $a \cdot 1 = a$

Eine weitere wichtige Eigenschaft von $\mathbb{N}$ ist das Funktionieren der *vollständigen Induktion*.

§2.2. Prinzip der vollständigen Induktion

Sei $A(n)$ eine Aussageform. Dann gilt $\forall n \in \mathbb{N}\colon A(n)$ genau dann, wenn folgende zwei Bedingungen erfüllt sind:

(1) *Induktionsanfang*: $A(1)$ ist wahr.
(2) *Induktionsschritt*: Für jedes $n \in \mathbb{N}$ gilt: Falls $A(n)$ wahr ist, so ist auch $A(n+1)$ wahr.

Kompakt geschrieben gilt also für jede Aussageform $A(n)$:

$$(A(1) \wedge \forall n \in \mathbb{N}(A(n) \Rightarrow A(n+1))) \Rightarrow \forall n \in \mathbb{N}\colon A(n)$$

Als Beispiel beweisen wir einen Satz über die Summe der ersten n natürlichen Zahlen.

Satz 2.1. *Für alle $n \in \mathbb{N}$ gilt:*

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

Beweis. Sei $A(n)$ die Aussageform $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Wir wollen zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt.

Induktionsanfang. A(1) ist wahr.

A(1) ist nämlich die Aussage $\sum_{i=1}^{1} i = \frac{1\cdot(1+1)}{2}$. Es gilt $\sum_{i=1}^{1} i = 1 = \frac{1\cdot(1+1)}{2}$. Das zeigt $A(1)$.

Induktionsschritt. Für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$

Um das zu zeigen, nehmen wir uns ein beliebiges $n \in \mathbb{N}$ her und zeigen $A(n) \Rightarrow A(n+1)$. Wir müssen also zeigen, dass $A(n+1)$ wahr ist, falls $A(n)$ wahr ist. Wenn $A(n)$ falsch ist, ist nichts zu zeigen.

Wir können also annehmen, dass $A(n)$ wahr ist. Das ist die *Induktionsannahme*. Nun zeigen wir $A(n+1)$ unter dieser Annahme. $A(n+1)$ ist die Aussage

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

also

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

Es gilt

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

Nach der Induktionsannahme ist $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Mit dieser Information erhalten wir

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

Das zeigt $A(n+1)$.

Damit haben wir den Induktionsanfang und den Induktionsschritt bewiesen. Es folgt, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt. □

Wir geben ein weiteres Beispiel. Für ganze Zahlen a und b schreiben wir $a|b$, falls a ein Teiler von b ist.

Satz 2.2. *Für alle $n \in \mathbb{N}$ ist $n^3 - n$ durch 3 teilbar.*

Beweis. Sei $A(n)$ die Aussageform „3 teilt $n^3 - n$“. Wir wollen zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt.

Induktionsanfang. A(1) ist wahr.

A(1) ist nämlich die Aussage $3|1^3 - 1$, also $3|0$. Diese Aussage ist wahr.

Induktionsschritt. Für alle $n \in \mathbb{N}$ gilt: $A(n) \Rightarrow A(n+1)$

Sei also $n \in \mathbb{N}$. Wieder nehmen wir an, dass $A(n)$ wahr ist, und zeigen $A(n+1)$. Die Induktionsannahme ist also $3|n^3 - n$.

$A(n+1)$ ist die Aussage $3|(n+1)^3 - (n+1)$. Wir vereinfachen:

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = n^3 + 3n^2 + 2n$$

Wir wollen zeigen, dass $n^3 + 3n^2 + 2n$ durch 3 teilbar ist, und dürfen benutzen, dass $n^3 - n$ durch 3 teilbar ist. Es gilt

$$n^3 + 3n^2 + 2n = (n^3 - n) + 3n^2 + 3n.$$

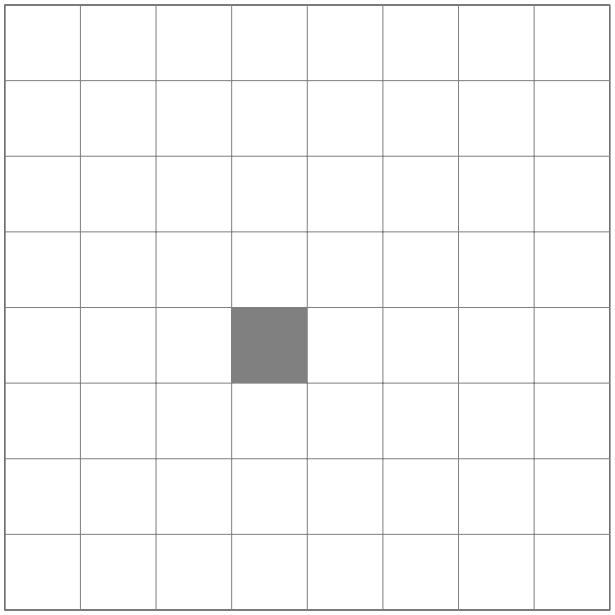
Der erste Summand der rechten Seite dieser Gleichung, $n^3 - n$, ist nach Induktionsannahme durch 3 teilbar. Der Rest, $3n^2 + 3n$, ist offenbar auch durch 3 teilbar. Das zeigt $3|(n+1)^3 - (n+1)$ und damit $A(n+1)$.

Damit ist für alle $n \in \mathbb{N}$ die Implikation $A(n) \Rightarrow A(n+1)$ bewiesen. Zusammen mit dem Induktionsanfang folgt $3|n^3 - n$ für alle $n \in \mathbb{N}$. □

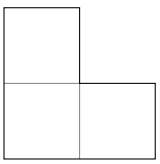
Als nächstes diskutieren wir ein Beispiel, das zeigt, dass der Erfolg einer Induktion von der geschickten Wahl des Induktionsanfangs abhängen kann. Außerdem liefert der folgende Beweis einen Algorithmus, also ein Verfahren, zur Lösung des vorgelegten Problems.

Problem 2.3. Ein quadratischer Hof mit der Seitenlänge 2^n soll mit L-förmigen Fliesen gefliest werden. Dabei soll ein Quadrat mit der Seitenlänge 1 in der Mitte des Hofes frei bleiben, weil da eine Statue aufgestellt werden soll. Die Fliesen haben die Form von drei aneinander gesetzten Quadraten mit Seitenänge eins, so wie in der Skizze. Ist es möglich, den Hof bis auf das Quadrat in der Mitte vollständig mit den Fliesen zu überdecken, ohne dass die Fliesen sich überlappen und ohne Fliesen zu zerschneiden?

Im Folgenden betrachten wir nur Quadrate, deren Seitenlängen ganzzahlig sind. Auch stellen wir uns immer vor, dass die Quadrate in der Ebene liegen, wobei die Koordinaten der Ecken der Quadrate alle ganzzahlig sind.

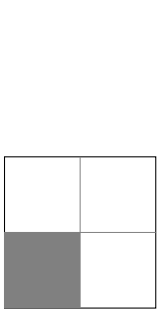


Hof

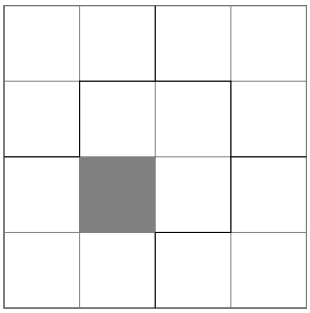


Fliese

Wir betrachten zunächst die Fälle $n = 1$ und $n = 2$ und sehen, dass wir den Hof wie gewünscht fliesen können. Schon der Fall $n = 1$ genügt für den Induktionsanfang.



$n = 1$



$n = 2$

Eine naheliegende Induktionsannahme wäre die Aussageform $A(n)$: „Jeder quadratische Hof mit der Kantenlänge 2^n kann bis auf ein fehlendes Quadrat der Kantenlänge 1 in der Mitte vollständig mit L-förmigen Fliesen gefliest werden."

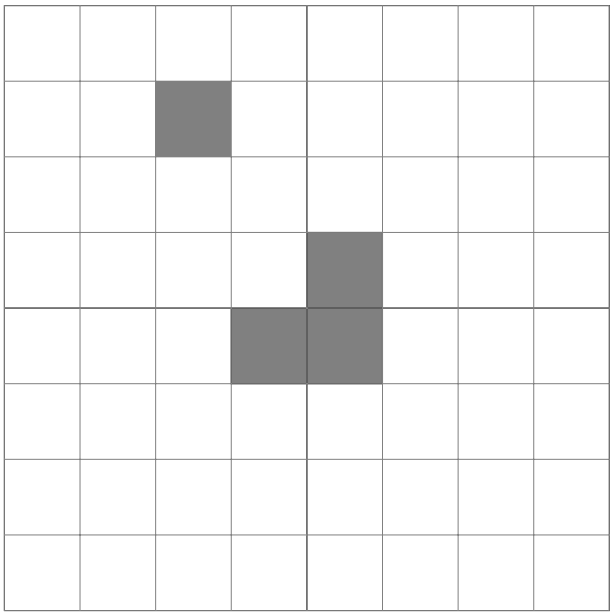
Es stellt sich heraus, dass wir Schwierigkeiten haben, die gewünschte Induktion mit dieser Induktionsannahme durchzuführen. Einen Hof der Kantenlänge 2^{n+1} können wir in vier quadratische Teile mit der Kantenlänge 2^n zerlegen, aber das fehlende Quadrat in der Mitte des Quadrats mit Kantenlänge 2^{n+1} liegt nun am Rand eines der Quadrate mit Kantenlänge 2^n. Bei den anderen drei Qudraten mit Kantenlänge fehlt kein Quadrat.

Eine Verstärkung von $A(n)$ führt schließlich zum Erfolg. $B(n)$ sei die Aussageform „Jeder quadratische Hof mit der Kantenlänge 2^n kann bis auf ein beliebig vorgegebenes fehlendes Quadrat der Kantenlänge 1 vollständig mit L-förmigen Fliesen gefliest werden".

Wir zeigen, dass $B(n)$ für alle $n \in \mathbb{N}$ gilt. Der Induktionsanfang ist einfach: $B(1)$ gilt, da von einem Quadrat der Kantenlänge 2 nach Entfernen eines Quadrates der Kantenlänge 1 eine L-förmige Fliese übrig bleibt.

Induktionsschritt: Wir zeigen, dass für alle $n \in \mathbb{N}$ die Implikation $B(n) \Rightarrow B(n+1)$ gilt. Sei also $n \in \mathbb{N}$. Wir nehmen an, dass $B(n)$ gilt. Sei nun ein Quadrat mit Kantenlänge 2^{n+1} vorgegeben, in dem ein Quadrat der Kantenlänge 1 markiert ist, welches beim Überdecken ausgelassen werden soll.

Wir zerlegen dieses Quadrat in vier Quadrate der Kantenlänge 2^n. Das markierte Quadrat der Kantenlänge 1 liegt in einem dieser vier Quadrate. Nun legen wir eine der L-förmigen Fliesen so in die Mitte des Quadrats mit Kantenlänge 2^{n+1}, dass die drei Quadrate der Fliese alle in je einem der vier Quadrate der Kantenlänge 2^n zum liegen kommen, wobei dasjenige der vier Quadrate, das das markierte Quadrat enthält, nicht getroffen wird.



Zerlegung des Quadrats der Kantenlänge 2^{n+1} und Lage der ersten Fliese

Nun genügt es, jedes der vier Quadrate mit Kantenlänge 2^n mit L-förmigen Fliesen zu überdecken, wobei jeweils ein Quadrat der Kantenlänge 1 ausgelassen werden muss. Das ist aber nach der Induktionsannahme $B(n)$ möglich. Das zeigt die Implikation $B(n) \Rightarrow B(n+1)$. Also gilt $B(n)$ für alle $n \in \mathbb{N}$. Das löst Problem 2.3.

Wir bemerken noch, dass diese Lösung des Problems auch ein Verfahren liefert, den Hof wie gewünscht zu fliesen:

- Wenn der Hof die Kantenlänge 2 hat, so bleibt neben dem markierten Quadrat genau Platz für eine L-förmige Fliese.
- Wenn der Hof für ein $n > 1$ die Kantenlänge 2^n hat, so unterteile den Hof in vier Quadrate der Kantenlänge 2^{n-1} und lege eine Fliese so in die Mitte des Hofes, dass sie genau die drei Quadrate der Kantenlänge 2^{n-1} trifft, die nicht das markierte Quadrat enthalten.
- Führe den Algorithmus für die vier Quadrate der Kantenlänge 2^{n-1} durch, wobei das ursprünglich markierte Quadrat und die drei Quadrate, die von der ersten Fliese überdeckt werden, markiert werden.

Wir betrachten zwei weitere Varianten der vollständigen Induktion. So muss man zum Beispiel den Induktionsanfang nicht unbedingt bei $n = 1$ machen. Ein Induktionsanfang bei $n = 0$ kommt recht häufig vor, andere Startwerte sind aber auch möglich.

2.2.1. Vollständige Induktion mit beliebigem Startwert. Es sei n_0 eine ganze Zahl und $A(n)$ eine Aussageform. Dann gilt $A(n)$ genau dann für alle ganzen Zahlen $n \geqslant n_0$, wenn $A(n_0)$ wahr ist und die Implikation $A(n) \Rightarrow A(n+1)$ für alle $n \geqslant n_0$ gilt.

Als Beispiel beweisen wir eine einfache Ungleichung.

Satz 2.4. *Für alle natürlichen Zahlen $n \geqslant 3$ gilt $2n + 1 < 2^n$.*

BEWEIS. $A(n)$ sei die Aussageform $2n + 1 < 2^n$.
Induktionsanfang. $A(3)$ gilt.

Um das zu sehen, setzen wir 3 für n ein. Es ist $2 \cdot 3 + 1 = 7 < 8 = 2^3$.
Induktionsschritt. Für alle $n \geqslant 3$ gilt: $A(n) \to A(n + 1)$

Wie nehmen an, dass $A(n)$ für ein gewisses $n \geqslant 3$ gilt, und haben $A(n + 1)$ nachzuweisen. Es ist

$$2(n + 1) + 1 = 2n + 3 = 2n + 1 + 2 \overset{\text{I.A.}}{<} 2^n + 2 \overset{n\geqslant 2}{<} 2^n + 2^n = 2^{n+1}.$$

Das zeigt $A(n + 1)$.

Es folgt, dass $A(n)$ für alle $n \geqslant 3$ gilt. □

Wir beweisen noch eine Formel, die sich in der Analysis als nützlich erweisen wird. Sei q eine reelle Zahl $\neq 1$ und $n \in \mathbb{N}_0$. Wir wollen einen einfachen Ausdruck für die Summe $\sum_{i=0}^{n} q^i = 1 + q + \ldots + q^n$ herleiten. Dazu formen wir die Summe um:

$$\begin{aligned}\sum_{i=0}^{n} q^i = 1 + \sum_{i=1}^{n} q^i = 1 + q\sum_{i=1}^{n} q^{i-1} = 1 + q\sum_{i=0}^{n-1} q^i = 1 + q\sum_{i=0}^{n-1} q^i + q^{n+1} - q^{n+1} \\ = 1 + q\left(\sum_{i=0}^{n-1} q^i + q^n\right) - q^{n+1} = 1 + q\sum_{i=0}^{n} q^i - q^{n+1}\end{aligned}$$

Wenn man den Term $q\sum_{i=0}^{n} q^i$ auf die linke Seite dieser Gleichung bringt, erhält man

$$(1 - q)\sum_{i=0}^{n} q^i = 1 - q^{n+1}.$$

Da $q \neq 1$ ist, können wir auf beiden Seiten durch $1 - q$ teilen und erhalten so die *geometrische Summenformel*:

Satz 2.5 (Geometrische Summenformel)**.** *Sei q eine reelle Zahl $\neq 1$ und $n \in \mathbb{N}_0$. Dann gilt*

$$\sum_{i=0}^{n} q^i = \frac{1 - q^{n+1}}{1 - q}.$$

BEWEIS. Wir haben die geometrische Summenformel zwar korrekt hergeleitet, geben aber trotzdem noch einen Beweis mittels vollständiger Induktion an.
Induktionsanfang. Für $n = 0$ stimmt die geometrische Summenformel, denn es gilt

$$\sum_{i=0}^{0} q^i = 1 = \frac{1 - q^1}{1 - q}.$$

Induktionsschritt. Wir nehmen an, dass die geometrische Summenformeln für ein gewisses $n \geqslant 0$ gilt (Induktionsannahme). Dann gilt sie auch für $n+1$:

$$\sum_{i=0}^{n+1} q^i = \sum_{i=0}^{n} q^i + q^{n+1} \overset{\text{I.A.}}{=} \frac{1-q^{n+1}}{1-q} + q^{n+1} = \frac{1-q^{n+1}}{1-q} + \frac{q^{n+1}(1-q)}{1-q}$$
$$= \frac{1-q^{n+1}+q^{n+1}-q^{n+2}}{1-q} = \frac{1-q^{n+2}}{1-q}$$

Damit ist die geometrische Summenformel für alle $n \in \mathbb{N}_0$ bewiesen. □

2.2.2. Vollständige Induktion mit mehreren Vorgängern. Wieder sei $A(n)$ eine Aussageform. Dann gilt $A(n)$ genau dann für alle natürlichen Zahlen n, wenn $A(1)$ wahr ist und für alle $n \in \mathbb{N}$ die folgende Implikation gilt: $A(1) \wedge \cdots \wedge A(n) \Rightarrow A(n+1)$.

Bei dieser Variante ist die Induktionsannahme die Annahme, dass $A(1), \ldots, A(n)$ wahr sind.

Eng mit der vollständigen Induktion verwandt sind *rekursive Definitionen.*

Beispiel 2.6. Wir definieren einen Folge natürlicher Zahlen a_n wie folgt:

(1) $a_1 = 1$
(2) $a_{n+1} = 2a_n + 1$

Dadurch ist a_n für jede natürliche Zahl n eindeutig bestimmt. Nach (1) gilt $a_1 = 1$. Wenden wir (2) auf den Fall $n = 1$ an, so erhalten wir $a_2 = 2 \cdot 1 + 1 = 3$. Wenden wir (2) auf den Fall $n = 2$ an, so ergibt sich $a_3 = 2 \cdot 3 + 1 = 7$.

Ein weiteres Beispiel für eine rekursive Definition sind die bekannten Fibonacci-Zahlen.

Definition 2.7. *Es sei $f_0 = 0$ und $f_1 = 1$. Für alle $n \geqslant 1$ sei $f_{n+1} = f_{n-1} + f_n$.*

Die Zahlen $f_0, f_1, f_2, \ldots$ heißen Fibonacci-Zahlen. *Die ersten 10 Glieder der Folge $f_0, f_1, f_2, \ldots$ lauten $0, 1, 1, 2, 3, 5, 8, 13, 21, 34$.*

Man kann für die n-te Fibonacci-Zahl f_n eine geschlossene Formel angeben, also einen Ausdruck, der keine Rekursion benutzt.

Satz 2.8. *Für alle $n \in \mathbb{N}_0$ gilt*

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

Beweis. Wir beweisen den Satz durch vollständige Induktion, wobei wir Induktion mit mehreren Vorgängern anwenden. Das liegt daran, dass in der rekursiven Definition von f_{n+1} auch auf mehrere Vorgänger zurückgegriffen wird.

Um die Rechnung übersichtlicher zu gestalten, führen wir zwei Abkürzungen ein. Es seien $\varphi := \frac{1+\sqrt{5}}{2}$ und $\psi := \frac{1-\sqrt{5}}{2}$. Sei $A(n)$ die Aussageform

$$f_n = \frac{\varphi^n - \psi^n}{\sqrt{5}}.$$

Wir wollen also zeigen, dass $A(n)$ für alle $n \in \mathbb{N}_0$ gilt.

Als Induktionsannahme wählen wir $A(n-1) \wedge A(n)$. Das können wir natürlich nur annehmen, falls n mindestens 1 ist, da f_{-1} ja nicht definiert ist und wir nicht wissen, was $A(-1)$ bedeutet. Im Induktionsschritt zeigen wir dann für alle $n \geqslant 1$, dass aus $A(n-1)$ und $A(n)$ zusammen $A(n+1)$ folgt.

Wenn wir für den Induktionsanfang nur $A(0)$ zeigen, dann haben wir aber das Problem, dass wir nicht wissen, ob $A(1)$ überhaupt gilt, da im Induktionsschritt $A(n-1) \wedge A(n) \Rightarrow A(n+1)$ nur für $n \geqslant 1$ wird. Daher müssen wir beim Induktionsanfang auch noch $A(1)$ explizit zeigen.

Induktionsanfang. Es gilt

$$\frac{\varphi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = f_0$$

sowie

$$\frac{\varphi^1 - \psi^1}{\sqrt{5}} = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = \frac{1}{\sqrt{5}} \cdot \frac{2\sqrt{5}}{2} = 1 = f_1.$$

Induktionsschritt. Wir zeigen $A(n-1) \wedge A(n) \Rightarrow A(n+1)$ für alle $n \geqslant 1$. Dazu nehmen wir an, dass für ein gewisses $n \geqslant 1$ die Aussage $A(n-1) \wedge A(n)$ gilt. Dann ist

$$f_{n+1} = f_{n-1} + f_n = \frac{\varphi^{n-1} - \psi^{n-1} + \varphi^n - \psi^n}{\sqrt{5}} = \frac{\varphi^n\left(1+\frac{1}{\varphi}\right) - \psi^n\left(1+\frac{1}{\psi}\right)}{\sqrt{5}}.$$

Es gilt

$$1 + \frac{1}{\varphi} = 1 + \frac{2}{1+\sqrt{5}} = \frac{1+\sqrt{5}+2}{1+\sqrt{5}}$$
$$= \frac{(3+\sqrt{5})(1-\sqrt{5})}{(1+\sqrt{5})(1-\sqrt{5})} = \frac{-2-2\sqrt{5}}{1-5} = \frac{1+\sqrt{5}}{2} = \varphi$$

und analog $1 + \frac{1}{\psi} = \psi$. Damit ergibt sich

$$f_{n+1} = \frac{\varphi^{n+1} - \psi^{n+1}}{\sqrt{5}},$$

also $A(n+1)$.

Insgesamt gilt $A(n)$ für alle $n \in \mathbb{N}_0$. □

§2.3. Peano Axiome

Wir haben bisher noch nicht diskutiert, warum die vollständige Induktion überhaupt funktioniert. Unsere intuitive Vorstellung von den natürlich Zahlen ist die folgende: Wenn wir bei 1 anfangen zu zählen und dann in Einerschritten immer weiter zählen, so erreichen wir schließlich jede natürliche Zahl. Oder anders gesagt, die natürlichen

Zahlen sind genau die Zahlen, die wir erreichen können, wenn wir bei 1 anfangen zu zählen und dann in Einerschritten immer weiter zählen.

Ist $A(n)$ eine Aussageform und gelten $A(1)$ und $\forall n \in \mathbb{N}(A(n) \Rightarrow A(n+1))$, so können wir die Menge $S = \{n \in \mathbb{N} \colon A(n) \text{ ist wahr}\}$ betrachten und stellen Folgendes fest:

(1) $1 \in S$
(2) $n \in S \Rightarrow n + 1 \in S$

Eine Menge mit den Eigenschaften (1) und (2) nennen wir *induktiv*. Wir können also bei 1 anfangen, in Einerschritten zu zählen, ohne jemals die Menge S zu verlassen. Nach unserer Intuition über die natürlichen Zahlen erreichen wir dabei alle natürlichen Zahlen. Also gilt $\mathbb{N} \subseteq S$. Andererseits ist $S \subseteq \mathbb{N}$. Es folgt $S = \mathbb{N}$. Also gilt $A(n)$ für alle $n \in \mathbb{N}$.

Die folgende Axiome präzisieren unsere Intuition über die natürlichen Zahlen. Hierbei steht n' für den Nachfolger von n in den natürlichen Zahlen, also für $n + 1$.

Definition 2.9. *Die folgenden Axiome sind die* Peano-Axiome *für die natürlichen Zahlen.*

(*P1*) $1 \in \mathbb{N}$
(*P2*) $n \in \mathbb{N} \Rightarrow n' \in \mathbb{N}$
(*P3*) $n \in \mathbb{N} \Rightarrow n' \neq 1$
(*P4*) $m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n)$
(*P5*) $(1 \in S \wedge \forall n \in \mathbb{N}(n \in S \Rightarrow n' \in S)) \Rightarrow \mathbb{N} \subseteq S$

Das Axiom (5) ist das *Induktionsaxiom*, welches garantiert, dass wir Sätze mittels vollständiger Induktion beweisen können. Normalsprachlich lauten die Axiome wie folgt:

(*P1*) 1 ist eine natürliche Zahl.
(*P2*) Der Nachfolger einer natürlichen Zahl ist wieder eine natürliche Zahl.
(*P3*) 1 ist nicht Nachfolger einer natürlichen Zahl.
(*P4*) Die Nachfolgerfunktion $n \mapsto n'$ ist injektiv.
(*P5*) Jede induktive Menge enthält alle natürlichen Zahlen.

Auf Basis dieser Axiome kann man nun die bekannte Operationen $+$ und $\cdot$ sowie die Relation $\leqslant$ auf $\mathbb{N}$ rekursiv definieren, was wir aber nicht im einzelnen durchführen wollen.

Vollständige Induktion liefert uns interessante Informationen über die Menge der natürlichen Zahlen.

Satz 2.10. *Jede nichtleere Menge natürlicher Zahlen hat ein kleinstes Element.*

Beweis. Sei A eine nichtleere Menge natürlicher Zahlen, also $A \subseteq \mathbb{N}$ und $A \neq \varnothing$. Falls A kein kleinstes Element hat, so betrachte $B = \mathbb{N} \setminus A$. Wir zeigen mittels

vollständiger Induktion, dass B alle natürlichen Zahlen enthält und A damit leer ist, im Widerspruch zur Annahme.

Sei $P(n)$ die Aussageform $n \in B$. 1 ist das kleinste Element von $\mathbb{N}$. Also gilt $1 \notin A$, da sonst 1 das kleinste Element von A wäre. Damit ist $1 \in B$. Das zeigt $P(1)$. Das ist der Induktionsanfang.

Nun nehmen wir an, dass die Zahlen $1, \ldots, n$ Elemente von B sind, dass also $P(1), \ldots, P(n)$ gelten. Die Zahl n' kann nicht in A liegen, da n' dann das kleinste Element von A wäre. Also liegt n' in B. Das zeigt $P(n')$. Das ist der Induktionsschritt.

Damit gilt $\mathbb{N} \subseteq B$. Also ist $A = \varnothing$, im Widerspruch zu $A \neq \varnothing$. Damit hat A ein kleinstes Element. □

Wir haben hier die Induktion mit mehreren Vorgängern durchgeführt. Um zu sehen, dass das wirklich dasselbe ist, wie die Standardform der Induktion, kann man zum Beispiel anstelle der Aussageform $P(n)$ die folgende Aussageform $Q(n)$ betrachten: $\forall k \in \mathbb{N}(k \leqslant n \Rightarrow k \in B)$

Dann kann man an Stelle der Induktionsannahme $P(1) \wedge \cdots \wedge P(n)$ einfach $Q(n)$ schreiben. Man beweist dann im Induktionsschritt nicht $(P(1) \wedge \cdots \wedge P(n)) \Rightarrow P(n')$, sondern $Q(n) \Rightarrow Q(n')$. Der Beweis selbst bleibt aber eigentlich derselbe.

Wir haben dann gezeigt, dass $Q(n)$ für alle $n \in \mathbb{N}$ gilt, und zwar mit der Standardform der Induktion. Aber $(\forall n \in \mathbb{N})Q(n)$ ist natürlich äquivalent zu $(\forall n \in \mathbb{N})P(n)$.

KAPITEL 3

Elementare Zahlentheorie

§3.1. Relationen

In Definition 1.15 haben wir das kartesische Produkt $A \times B$ zweier Mengen A und B als die Menge aller Paare (a, b) mit $a \in A$ und $b \in B$ definiert.

Definition 3.1. *Eine* Relation *von A nach B ist eine Teilmenge R von $A \times B$. Eine Relation auf A ist eine Teilmenge von $A \times A$. Für $(a, b) \in R$ schreiben wir auch aRb.*

Beispiel 3.2. (1) Sei $A = \{1, 2, 3\}$ und $B = \{0, 1\}$. Dann sind $R_1, \ldots, R_4$ Relationen von A nach B:

(a) $R_1 = \{(1, 0), (2, 0), (2, 1)\}$.

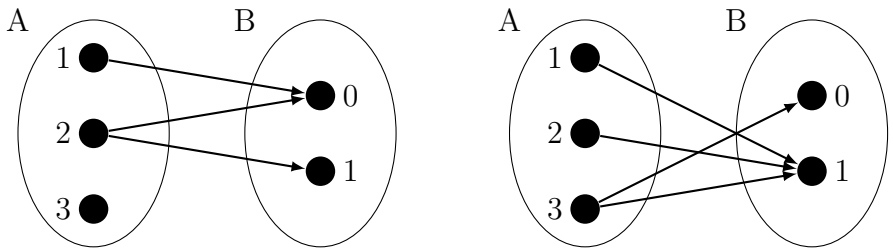
(b) $R_2 = \{(1, 1), (2, 1), (3, 0), (3, 1)\}$

(c) $R_3 = A \times B$

(d) $R_4 = \varnothing$.

(2) $R = \{(a, b) \colon a, b \in \mathbb{N} \wedge a < b\}$, $S = \{(a, b) \colon a, b \in \mathbb{N} \wedge a \leqslant b\}$ und $T = \{(a, b) \colon a, b \in \mathbb{N} \wedge a = b\}$ sind Relationen auf $\mathbb{N}$. Üblicher Weise identifizieren wir $<$ mit R, $\leqslant$ mit S und T mit $=$.

Wir können Relationen ähnlich wie Funktionen mit Hilfe von Pfeildiagrammen notieren. Hier sind zwei Diagramme für die Relationen R_1 und R_2.



Definition 3.3. *Sei A eine Menge und sei R eine Relation auf A.*

(1) R heißt reflexiv, *falls für alle $a \in A$ das Paar (a, a) in R ist.*

(2) R heißt irreflexiv, *falls R kein Paar der Form (a, a) enthält.*

(3) R heißt symmetrisch, *falls für alle $(a, b) \in R$ auch $(b, a) \in R$ gilt.*

(4) R heißt antisymmetrisch, *falls aus $(a, b) \in R$ und $a \neq b$ stets $(b, a) \notin R$ folgt.*

(5) R heißt transitiv, *falls aus $(a, b) \in R$ und $(b, c) \in R$ stets $(a, c) \in R$ folgt.*

Man beachte, dass irreflexiv nicht dasselbe ist wie nicht reflexiv. Ebenso ist antisymmetrisch nicht dasselbe wie nicht symmetrisch.

3.1.1. Partitionen und Äquivalenzrelationen.

Definition 3.4. *Eine Relation R auf einer Menge A heißt Äquivalenzrelation, falls R reflexiv, transitiv und symmetrisch ist.*

Ist R eine Äquivalenzrelation auf A so bezeichnen wir für jedes $a \in A$ mit $[a]_R$ die Menge $\{b \in A \colon (a,b) \in R\}$ und nennen diese Menge die Äquivalenzklasse *von a.*

Satz 3.5. *Sei A eine Menge und R eine Äquivalenzrelation auf A. Dann gilt für alle $a, b \in A$ entweder $[a]_R \cap [b]_R = \varnothing$ oder $[a]_R = [b]_R$. Der zweite Fall tritt genau dann ein, wenn aRb gilt.*

Beweis. Seien $a, b \in A$ mit $[a]_R \cap [b]_R \neq \varnothing$. Sei $c \in [a]_R \cap [b]_R$. Dann gilt aRc und bRc. Wegen Symmetrie und Transitivität von R folgt daraus aRb. Wieder wegen Symmetrie und Transitivität von R ist jedes Element von A, das zu a äquivalent ist, auch zu b äquivalent und umgekehrt. Damit sind $[a]_R$ und $[b]_R$ gleich. □

Für eine Äquivalenzrelation R auf einer Menge A ist $\{[a]_R \colon a \in A\}$ eine *Partition* von A.

Definition 3.6. *Sei A eine Menge, I eine Indexmenge und für alle $i \in I$ sei $K_i \subseteq A$. $P = \{K_i \colon i \in I\}$ ist eine* Partition *von A, falls gilt:*

(1) Für alle $i, j \in I$ mit $i \neq j$ ist $K_i \cap K_j = \varnothing$.
(2) Es gilt $\bigcup_{i \in I} K_i = A$.

Dabei ist $\bigcup_{i \in I} K_i$ die Menge $\{x \colon \exists i \in I (x \in K_i)\}$.

Umgekehrt kann man einer Partition $P = \{K_i \colon i \in I\}$ von A eine Äquivalenzrelation auf A zuordnen, deren Äquivalenzklassen genau die Mengen K_i sind. Sei nämlich $P = \{K_i \colon i \in I\}$ eine Partition von A. Sei

$$R := \{(a,b) \in A \times A \colon \exists i \in I (a, b \in K_i)\}.$$

Wir nennen also zwei Elemente a und b von A äquivalent, wenn sie in derselben Menge K_i liegen.

Wegen $\bigcup_{i \in I} K_i = A$ gibt es für jedes $a \in A$ ein $i \in I$ mit $a \in K_i$. Damit steht jedes $a \in A$ zu sich selbst in Relation. R ist also reflexiv. Gilt $a, b \in K_i$, so gilt auch $b, a \in K_i$. Damit ist R symmetrisch. Seien schließlich $a, b, c \in A$ mit aRb und bRc. Dann gibt es $i, j \in I$ mit $a, b \in K_i$ und $b, c \in K_j$. Nun gilt $b \in K_i \cap K_j$. Da die Mengen in der Partition paarweise disjunkt sind, muss $K_i = K_j$ gelten. Also gilt $a, c \in K_i$. Damit ist aRc. Das zeigt die Transitivität von R.

Korollar 3.7. *Es sei A eine Menge. Für jede Äquivalenzrelation auf A bilden die Äquivalenzklassen eine Partition von A. Umgekehrt gibt es für jede Partition von A eine Äquivalenzrelation, deren Äquivalenzklassen genau die Mengen in der Partition sind.*

Beispiel 3.8. Sei $m \in \mathbb{N}$ und $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \colon a \equiv b (\mathrm{mod}\ m)\}$. Dann ist R eine Äquivalenzrelation auf $\mathbb{Z}$, deren Äquivalenzklassen genau die Restklassen modulo m sind.

Die Anzahl der Restklassen modulo m ist genau m. Die verschiedenen Restklassen sind die Mengen

$$\{m \cdot q + 0 \colon q \in \mathbb{Z}\}, \quad \{m \cdot q + 1 \colon q \in \mathbb{Z}\}, \quad \ldots, \quad \{m \cdot q + (m-1) \colon q \in \mathbb{Z}\}.$$

3.1.2. Ordnungsrelationen.

Definition 3.9. *Sei A eine Menge und R eine Relation auf A. Dann ist R eine* Ordnungsrelation, *falls R reflexiv, antisymmetrisch und transitiv ist. Ordnungsrelationen nennt man auch* Halbordnungen *oder* partielle Ordnungen. *Das Paar (A, R) ist eine* halbgeordnete *oder* partiell geordnete Menge.

Ordnungsrelationen werden oft mit $\leqslant$ oder einem ähnlichen Zeichen bezeichnet. Man schreibt dann praktisch immer $a \leqslant b$ anstelle von $(a, b) \in \leqslant$. Man beachte, dass dabei nicht unbedingt die bekannte $\leqslant$-Relation auf den reellen Zahlen gemeint ist.

Beispiel 3.10. Sei $A := \{a, b, c, d\}$ und

$$R := \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, d), (c, d)\}.$$

Wie man leicht sieht, ist R reflexiv, transitiv und antisymmetrisch.

Beispiel 3.11. Sei $A := \{a, b, c, d\}$ und

$$R := \{(a, a), (b, b), (c, c), (d, d), (a, b), (a, c), (a, d), (b, c), (b, d), (c, d)\}.$$

Wieder sieht man leicht, dass R reflexiv, transitiv und antisymmetrisch ist.

Beispiel 3.12.
(1) Die Relation $\leqslant$ ist eine Ordnungsrelation of $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$.
(2) Für jede Menge M ist $\subseteq$ eine Ordnungsrelation auf $\wp(M)$.
(3) Die Teilbarkeitsrelation $\mid$ ist eine Ordnungsrelation auf $\mathbb{N}$.

Definition 3.13. *Ein Ordnungsrelation R auf einer Menge R heißt* lineare Ordnung, *falls für alle $a, b \in A$ mit $a \neq b$ entweder aRb oder bRa gilt. Lineare Ordnungen nennt man auch* totale Ordnungen.

Beispiel 3.14. Die Relation $\leqslant$ auf $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ ist jeweils eine lineare Ordnung. Die Relation R aus Beispiel 3.11 ist ebenfalls eine lineare Ordnung, während die Relation aus Beispiel 3.10 keine lineare Ordnung ist, da die Element b und c nicht *vergleichbar* sind, also da weder (b, c) noch (c, b) in R ist. Ebenso ist $\subseteq$ keine lineare Ordnung auf $\wp(M)$, falls M mindestens zwei Elemente hat.

§3.2. Ganze und rationale Zahlen

Im Abschnitt über Mengen hatten wir bereits die Menge

$$\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$$

der ganzen Zahlen eingeführt. Die Menge $\mathbb{Q}$ der *rationalen Zahlen* ist die Menge aller Brüche $\frac{m}{n}$ mit $m, n \in \mathbb{Z}$ und $n \neq 0$.

Da wir jede ganzen Zahl m mit dem Bruch $\frac{m}{1}$ identifzieren können, fassen wir $\mathbb{Z}$ als eine Teilmenge von $\mathbb{Q}$ auf. Wir erinnern uns kurz daran, wie man Brüche addiert und multipliziert:

$$\frac{m}{n} + \frac{m'}{n'} = \frac{m \cdot n' + m'n}{n \cdot n'}$$
$$\frac{m}{n} \cdot \frac{m'}{n'} = \frac{m \cdot m'}{n \cdot n'}$$

Die folgenden Rechenregeln für rationale Zahlen a, b, c setzen wir als bekannt voraus:

(K1) Assoziativgesetze
- $a + (b + c) = (a + b) + c$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

(K2) Kommutativgesetze
- $a + b = b + a$
- $a \cdot b = b \cdot a$

(K3) Distributivgesetz
- $a \cdot (b + c) = a \cdot b + a \cdot c$

(K4) Existenz neutraler Elemente bezüglich der Addition und der Multiplikation
- $a + 0 = a$
- $1 \cdot a = a$

(K5) Existenz inverser Elemente bezüglich der Addition und der Multiplikation
- Es gibt ein Element $-a$ mit $a + (-a) = 0$.
- Falls $a \neq 0$ ist, so gibt es ein Element a^{-1} mit $a \cdot a^{-1} = 1$.

Da diese Rechengesetze so wichtig sind, bekommen Strukturen, in denen diese Gesetze erfüllt sind, einen eigenen Namen.

Definition 3.15. *Sei K eine Menge, 0 und 1 zwei verschiedene Elemente von K und $+ \colon K \times K \to K$ und $\cdot \colon K \times K \to K$ Abbildungen. Dann heißt K zusammen mit 0, 1, $+$ und $\cdot$ ein* Körper, *falls die Axiome (K1)–(K5) erfüllt sind.*

Wie oben schon bemerkt, erfüllt $\mathbb{Q}$ mit der üblichen Addition und Multiplikation und mit den bekannten Konstanten 0 und 1 die Körperaxiome (K1)–(K5). Die ganzen Zahlen $\mathbb{Z}$ mit den üblichen Rechenoperationen erfüllen zwar (K1)–(K4), aber sie bilden keinen Körper, da zum Beispiel 2 in $\mathbb{Z}$ kein multiplikatives Inverses besitzt: Es gibt keine ganze Zahl n mit $2 \cdot n = 1$.

Neben der Struktur eines Körpers, haben die rationalen Zahlen noch eine weitere wichtige Eigenschaft. Sie werden durch die Kleiner-Beziehung $<$ *angeordnet*. Für je zwei verschiedene rationale Zahlen a und b gilt entweder $a < b$ („a kleiner b“) oder $a > b$ („a größer b“). Es gelten folgende Regeln:

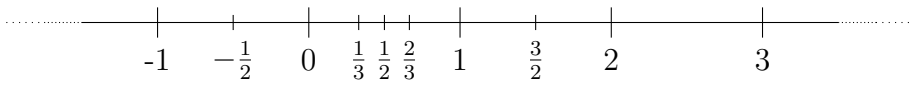
(1) $a < b \wedge b < c \Rightarrow a < c$
(2) $a < b \Rightarrow a + c < b + c$
(3) $a < b \Rightarrow a \cdot c < b \cdot c$, falls $c > 0$.
(4) $a < b \Rightarrow a \cdot c > b \cdot c$, falls $c < 0$.

Wir schreiben $a \leqslant b$ für $(a < b \vee a = b)$ und lesen $\leqslant$ als „kleiner-gleich“ und $\geqslant$ als „größer-gleich“.

Für $\leqslant$ gelten ähnliche Regeln wie für $<$.

(1) $a \leqslant b \wedge b \leqslant c \Rightarrow a \leqslant c$
(2) $a \leqslant b \Rightarrow a + c \leqslant b + c$
(3) $a \leqslant b \Rightarrow a \cdot c \leqslant b \cdot c$, falls $c \geqslant 0$.
(4) $a \leqslant b \Rightarrow a \cdot c \geqslant b \cdot c$, falls $c \leqslant 0$.

Die ganzen und die rationalen Zahlen lassen sich gut auf dem Zahlenstrahl veranschaulichen. Wir stellen uns vor, dass die Gerade horizontal von links nach rechts verläuft. Nun markieren wir einen Punkt auf der Geraden und nennen ihn 0. Rechts von der 0 markieren wir einen weiteren Punkt und nennen ihn 1. Ist nun n eine natürlich Zahl, so entspricht n dem Punkt auf der Geraden, den man erreicht, wenn man von der 0 ausgehend n-mal die Strecke von der 0 zur 1 abträgt. Sind m und n natürliche Zahlen, so erhält den Punkte auf der Geraden, der $\frac{m}{n}$ entspricht, in dem man die Strecke von 0 nach m in n gleiche Teile unterteilt. Damit finden wir alle rationalen Zahlen > 0 auf der Zahlengeraden. Für natürliche Zahlen m und n finden wir den Punkt auf der Geraden, der $-\frac{m}{n}$ entspricht, indem man von 0 ausgehend nach links die Länge der Strecke von 0 bis $\frac{m}{n}$ abträgt.



Offenbar kann man zum Beispiel $\frac{3}{2}$ auch erreichen, indem man zuerst die Strecke von 0 nach 1 halbiert, um $\frac{1}{2}$ zu erhalten, und dann dreimal von 0 ausgehend nach rechts die Länge der Strecke von 0 bis $\frac{1}{2}$ abträgt.

Die rationalen Zahlen liegen *dicht* auf der Zahlengeraden. D.h., zwischen je zwei verschiedenen Punkten auf der Geraden liegt eine rationale Zahl. Wir werden jedoch gleich sehen, dass es Punkte auf der Geraden gibt, die keiner rationalen Zahlen entsprechen, dass die rationalen Zahlen also Lücken haben.

§3.3. Die reellen Zahlen

Mit $\sqrt{2}$ bezeichnen wir die positive Lösung der Gleichung $x^2 = 2$. Es stellt sich heraus, dass $\sqrt{2}$ keine rationale Zahl ist.

Bevor wir das beweisen können, müssen stellen wir Folgendes fest.

Lemma 3.16. *Sei m eine ganze Zahl. Falls m^2 gerade ist, so ist auch m selbst gerade.*

BEWEIS. Wir beweisen die Kontraposition dieser Aussage: Wenn m ungerade ist, so ist auch m^2 ungerade.

Sei m ungerade. Dann ist $m-1$ gerade. Also gibt es eine ganze Zahl k mit $2k = m-1$. Es gilt also $m = 2k+1$. Nun ist $m^2 = (2k+1)^2 = 4k^2+4k+1$. Da $4k^2+4k$ gerade ist, ist $4k^2+4k+1$ ungerade. Also ist m^2 ungerade. □

Satz 3.17. *Es gibt keine rationale Zahl a mit $a^2 = 2$.*

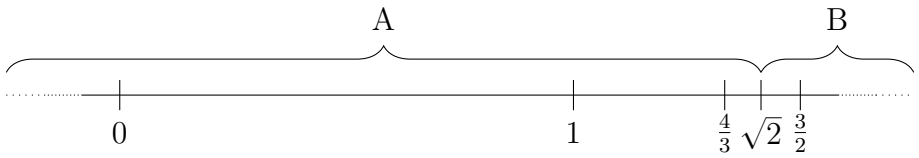
BEWEIS. Der Beweis dieses Satzes ist ein sogenannter *Widerspruchsbeweis*. Wir nehmen dazu an, dass es eine rationale Zahl a mit $a^2 = 2$ gibt und folgern daraus eine offensichtlich falsche Aussage. Sei A die Aussage „ es gibt eine rationale Zahl a mit $a^2 = 2$“ und B eine falsche Aussage. Wenn wir $A \Rightarrow B$ zeigen können und B falsch ist, so muss A falsch sein, was wir leicht der Wahrheitstafel für $\rightarrow$ entnehmen können. Wir haben also $\neg A$ bewiesen.

Zum eigentlichen Beweis. Wie eben schon angekündigt, nehmen wir an, dass es eine rationale Zahl a mit $a^2 = 2$ gibt. Die Zahl a lässt sich als Bruch $\frac{m}{n}$ schreiben, wobei m und n ganze Zahlen sind und $n \neq 0$ gilt. Gilt $a^2 = 2$, so gilt auch $(-a)^2 = 2$. Daher können wir annehmen, dass a positiv ist und dass m und n natürliche Zahlen sind. Schließlich können wir noch annehmen, dass der Bruch $\frac{m}{n}$ gekürzt ist, dass also m und n keine gemeinsame Teiler > 1 haben. Es gilt $a^2 = \frac{m^2}{n^2} = 2$. Multiplikation mit n^2 liefert $m^2 = 2n^2$. Also ist m^2 durch 2 teilbar. Nach Lemma 3.16 ist damit auch m durch 2 teilbar.

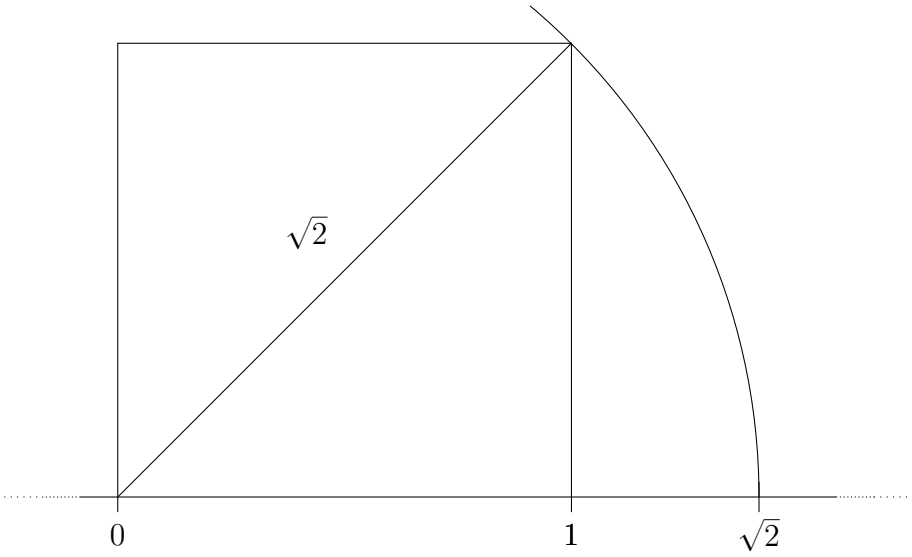
Wenn aber m von 2 geteilt wird, so wird m^2 von 4 geteilt. Wegen $m^2 = 2n^2$ wird dann aber auch n^2 von 2 geteilt. Wie oben für m ergibt sich, dass n gerade ist. Das heißt aber, dass man den Bruch $\frac{m}{n}$ durch 2 kürzen kann, ein Widerspruch zur Annahme, dass der Bruch bereits gekürzt ist.

Die Aussage „der Bruch $\frac{m}{n}$ ist gekürzt und der Bruch $\frac{m}{n}$ lässt sich kürzen“ ist offenbar falsch. Also haben wir aus der Aussage „es gibt eine rationale Zahl a mit $a^2 = 2$“ eine falsche Aussage abgeleitet. Damit ist diese Aussage selbst falsch und es gilt stattdessen, was wir zeigen wollten: Es gibt keine rationale Zahl a mit $a^2 = 2$. □

Trotzdem finden wir einen Punkt auf der Zahlengeraden, der der Zahl $\sqrt{2}$ entspricht, nämlich den eindeutig bestimmten Punkt, der rechts von alle Zahlen in der Menge $A := \{x \in \mathbb{Q} : x < 0 \vee x^2 < 2\}$ und links von alle Zahlen in der Menge $B := \{x \in \mathbb{Q} : x > 0 \wedge x^2 > 2\}$ liegt.



Die Existenz eines Punktes auf der Zahlengeraden, dessen Abstand von 0 genau $\sqrt{2}$ ist, sieht man wie folgt: Auf der Strecke von 0 nach 1 errichte man ein Quadrat mit der Kantenlänge 1. Die Diagonale dieses Quadrats hat nach dem Satz von Pythagoras die Länge $\sqrt{2}$. Wenn wir von 0 ausgehend nach rechts die Länge der Diagonalen des Quadrats auf der Zahlengeraden abtragen, so erreichen wir den Punkt, der $\sqrt{2}$ entspricht.



Es gibt viele Punkte auf der Zahlengeraden, denen keine rationale Zahl entspricht. Wir können $\mathbb{Q}$ aber so zur Menge $\mathbb{R}$ der *reellen Zahlen* erweitern, dass jedem Punkt auf der Zahlengeraden eine reelle Zahl entspricht und umgekehrt jede reelle Zahl einem Punkt auf der Zahlengeraden. Wir können reelle Zahlen addieren und multiplizieren, wobei wir bei Einschränkung dieser Operationen auf $\mathbb{Q}$ genau die bekannten Operationen auf den rationalen Zahlen erhalten. Mit diesen Operationen bilden die reellen Zahlen einen Körper, wie die rationalen Zahlen auch.

Die Kleiner-Beziehung $<$ zwischen reellen Zahlen ist so erklärt, dass für reelle Zahlen a und b die Beziehung $a < b$ genau dann gilt, wenn der Punkt auf der Zahlengeraden, der a entspricht, links von dem Punkt liegt, der b entspricht. Es gelten dieselben Rechenregeln für $<$ auf $\mathbb{R}$ wie auf $\mathbb{Q}$.

Es gibt verschiedene Möglichkeiten, die reellen Zahlen ausgehend von den rationalen Zahlen zu konstruieren. Wir werden allerdings nicht näher auf die Konstruktion eingehen. Alle reellen Zahlen lassen sich als (eventuell unendliche) Dezimalbrüche darstellen. Die rationalen Zahlen entsprechen den Dezimalbrüchen, die entweder nach endlich vielen Nachkommastellen abbrechen oder periodisch werden.

Die reellen Zahlen, die nicht rational sind, heißen *irrational*. Beispiele für irrationale Zahlen sind $\sqrt{2}$, $\sqrt{3}$, e, π und $\sqrt[3]{5}$.

§3.4. Die Abzählbarkeit von $\mathbb{Q}$ und die Überabzählbarkeit von $\mathbb{R}$

Wir haben schon gesehen, dass es reelle Zahlen gibt, die nicht rational sind, wie zum Beispiel $\sqrt{2}$. In diesem Abschnitt werden wir sehen, dass es sogar viel mehr reelle als rationale Zahlen gibt.

Definition 3.18. *Zwei Mengen A und B heißen* gleichmächtig, *wenn es eine Bijektion $f\colon A \to B$ gibt.*

Diese Definition ist auch für unendliche Mengen sinnvoll. So ist

$$f\colon \mathbb{Z} \to \{a \in \mathbb{Z}\colon a \text{ ist gerade}\}; a \mapsto 2a$$

eine Bijektion zwischen den ganzen Zahlen und den (positiven sowie negativen) geraden Zahlen. $\mathbb{Z}$ und die Menge aller geraden Zahlen sind also gleichmächtig.

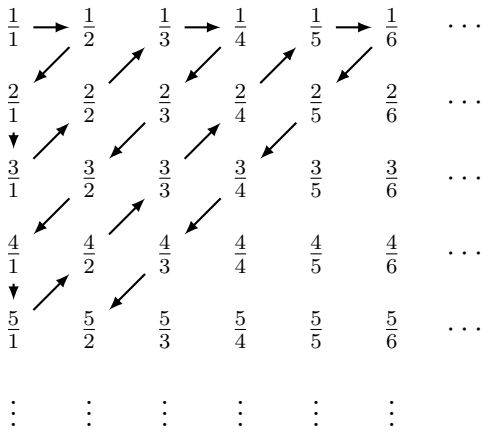
Definition 3.19. *Eine Menge M heißt abzählbar, wenn M entweder endlich ist oder es eine Bijektion $f\colon \mathbb{N} \to M$ gibt. Eine Menge, die nicht abzählbar ist, heißt überabzählbar.*

Man kann leicht zeigen, dass eine Menge genau dann M abzählbar ist, wenn M entweder leer ist oder es eine surjektive Abbildung $f\colon \mathbb{N} \to M$ gibt. Eine Surjektion $f\colon \mathbb{N} \to M$ nennt man eine *Aufzählung* von M. Eine Aufzählung f von M kann man einfach in der Form $f(1), f(2), \dots$ notieren.

So ist zum Beispiel $0, 1, -1, 2, -1, \dots$ eine Aufzählung von $\mathbb{Z}$. Die Menge der ganzen Zahlen ist also abzählbar. Etwas verblüffender ist folgender Satz, der von Cantor bewiesen wurde.

Satz 3.20. *Die Menge $\mathbb{Q}$ der rationalen Zahlen ist abzählbar.*

Beweis. Wir geben zunächst eine Aufzählung $q_1, q_2, \dots$ der Menge der rationalen Zahlen > 0 an. Man erhält die Aufzählung, indem man im folgenden Bild bei den Bruch $\frac{1}{1}$ beginnt und den Pfeilen folgt.



Die Aufzählung lautet also

$$q_1 = \frac{1}{1}, \quad q_2 = \frac{1}{2}, q_3 = \quad q_3 = \frac{2}{1}, \quad q_4 = \frac{3}{1}, \quad q_5 = \frac{2}{2}, \dots$$

Die Tatsache, das viele rationale Zahlen hierbei doppelt auftreten, zum Beispiel 1 als $\frac{1}{1}$ und $\frac{2}{2}$ spielt keine Rolle, da eine Aufzählung nicht injektiv sein muss. Es ist aber klar, das jede rationale Zahl > 0 in dieser Aufzählung irgendwann einmal auftritt.

Mit dieser Aufzählung der rationalen Zahlen > 0 können wir nun aber leicht eine Aufzählung aller rationalen Zahlen angeben:

$$0, q_1, -q_1, q_2, -q_2, \dots$$

leistet das Gewünschte. □

Satz 3.21. *Die Menge* $\mathbb{R}$ *der reellen Zahlen ist überabzählbar.*

Beweis. Wir zeigen, dass die schon die Menge der reellen Zahlen, die echt größer als 0 und echt kleiner als 1 sind, überabzählbar sind. Wir führen einen Widerspruchsbeweis.

Angenommen, es gibt eine Aufzählung $s_1, s_2, s_3, \dots$ der reellen Zahlen s mit $0 < s < 1$. Die Zahlen s_n, $n \in \mathbb{N}$ lassen sich als Dezimalzahlen ohne Vorzeichen mit einer 0 vor dem Dezimalpunkt schreiben. Für alle $i, j \in \mathbb{N}$ sei s_{ij} die Ziffer, die in der j-ten Nachkommastelle der Dezimaldarstellung von s_i steht. Dann können wir die Aufzählung $s_1, s_2, \dots$ wie folgt notieren:

$$\begin{aligned} s_1 &= 0.s_{11}s_{12}s_{13}\dots \\ s_2 &= 0.s_{21}s_{22}s_{23}\dots \\ s_3 &= 0.s_{31}s_{32}s_{33}\dots \\ \vdots &\qquad\qquad \vdots \end{aligned}$$

Nun definieren wir eine weitere reelle Zahl a, die echt zwischen 0 und 1 liegt, die in der Aufzählung aber nicht auftritt. Das widerspricht der Annahme, dass $s_1, s_2, s_3, \dots$ eine Aufzählung der reellen Zahlen ist, die echt zwischen 0 und 1 liegen.

Wir geben die Nachkommastellen $a_1a_2a_3\dots$ der Zahl a an. Für $i \in \mathbb{N}$ sei

$$a_i := \begin{cases} 4, \text{ falls } s_{ii} \neq 4 \text{ ist und} \\ 5, \text{ sonst.} \end{cases}$$

Es ist klar, dass $a = 0.a_1a_2a_3\dots$ echt zwischen 0 und 1 liegt. a ist so gewählt, dass es sich an der i-ten Nachkommastelle von s_i unterscheidet. Da die Nachkommastellen von a nicht irgendwann konstant 0 oder konstant 9 werden, ist a damit von allen s_i, $i \in \mathbb{N}$ verschieden. □

§3.5. Teilbarkeit, Primzahlen und der euklidische Algorithmus

Wir haben bereits Teilbarkeit durch 2 betrachtet. Dennoch wiederholen wir die formale Definition von Teilbarkeit.

Definition 3.22. *Eine ganze Zahl a ist ein* Teiler *einer ganzen Zahl b, falls eine ganze Zahl c mit $b = a \cdot c$ existiert. Wenn a ein Teiler von b ist, so nennt man b ein* Vielfaches

von a. Ist a ein Teiler von b, so schreiben wir $a \mid b$. Ist a kein Teiler von b, so schreiben wir $a \nmid b$.

Man beachte, dass jede ganze Zahl a die 0 teilt. Es ist nämlich $0 = 0 \cdot a$. Umgekehrt teilt 0 nur sich selber und keine andere ganze Zahl. Ebenso beachte man, dass für alle ganzen Zahlen a und b Folgendes gilt:

$$a \mid b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow a \mid -b$$

Damit kann man die Teilbarkeitsbeziehung zwischen ganzen Zahlen immer auf die Teilbarkeitsbeziehung zwischen natürlichen Zahlen zurückführen.

Satz 3.23. *Die Teilbarkeitsbeziehung $\mid$ hat folgende Eigenschaften:*

(1) Gilt $a \mid b$ und $b \mid c$, so gilt auch $a \mid c$.
(2) Aus $a_1 \mid b_1$ und $a_2 \mid b_2$ folgt $a_1 \cdot a_2 \mid b_1 \cdot b_2$.
(3) Aus $a \cdot b \mid a \cdot c$ und $a \neq 0$ folgt $b \mid c$.
(4) Aus $a \mid b_1$ und $a \mid b_2$ folgt für alle $c_1, c_2 \in \mathbb{Z}$ die Beziehung $a \mid b_1 \cdot c_1 + b_2 \cdot c_2$.

Beweis. (1)–(4) lassen sich leicht nachrechnen. Zum Beispiel kann man (4) wie folgt nachrechnen:

Wegen $a \mid b_1$ und $a \mid b_2$ existieren $d_1, d_2 \in \mathbb{Z}$ mit $b_1 = a \cdot d_1$ und $b_2 = a \cdot d_2$. Für alle $c_1, c_2 \in \mathbb{Z}$ gilt nun

$$b_1 \cdot c_1 + b_2 \cdot c_2 = a \cdot d_1 \cdot c_1 + a \cdot d_2 \cdot c_2 = a \cdot (d_1 \cdot c_1 + d_2 \cdot c_2).$$

Das zeigt $a \mid b_1 \cdot c_1 + b_2 \cdot c_2$. □

Definition 3.24. *Eine natürliche Zahl $n \geqslant 2$ heißt* Primzahl, *wenn n nur durch -1, 1, n und $-n$ teilbar ist. Die Zahlen ± 1 und $\pm n$ nennt man die* trivialen *Teiler von n.*

Satz 3.25 (Euklid)**.** *Es gibt unendlich viele Primzahlen.*

Beweis. Wir führen wieder einen Widerspruchsbeweis. Angenommen, es gibt nur endlich viele Primzahlen $p_1, \ldots, p_n$. Betrachte das Produkt $a = p_1 \cdot \ldots \cdot p_n$.

Sei p die kleinste natürliche Zahl $\geqslant 2$, die $a + 1$ teilt. Dann ist p eine Primzahl. Hat nämlich p einen Teiler q, der von -1, 1, p und $-p$ verschieden ist, so ist q oder $-q$ eine natürliche Zahl $\geqslant 2$, die $a + 1$ teilt und kleiner als p ist. Das widerspricht aber der Wahl von p als kleinsten Teiler von $a + 1$ mit $p \geqslant 2$.

Da p eine Primzahl ist, existiert ein $i \in \{1, \ldots, n\}$ mit $p = p_i$. Damit teilt p sowohl a als auch $a + 1$. Also teilt p auch $1 = (a + 1) - a$. Das widerspricht aber der Wahl von p als einer ganzen Zahl $\geqslant 2$. □

Ohne Beweis geben wir einen wichtigen Satz über die Darstellung natürlicher Zahlen als Produkte von Primzahlen an.

Satz 3.26. *Jede natürliche Zahl $n \geqslant 2$ ist ein Produkt der Form $p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ wobei k eine natürliche Zahl $\geqslant 1$ ist, $p_1, \ldots, p_k$ paarweise verschiedene Primzahlen sind und*

$\alpha_1, \ldots, \alpha_k$ natürliche Zahlen sind. Dabei ist die Produktdarstellung $n = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ bis auf die Reihenfolge der Faktoren eindeutig.

Zum Beispiel ist $12 = 2^2 \cdot 3$ und $500 = 2^2 \cdot 5^3$.

Eine wichtige Folgerung aus diesem Satz ist die Folgende:

Korollar 3.27. *Teilt eine Primzahl p ein Produkt $a \cdot b$ natürlicher Zahlen, so teilt p eine der beiden Zahlen a und b.*

BEWEIS. Wir schreiben a und b als Produkte von Primzahlen, $a = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ und $b = q_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_m}$. Dann ist

$$a \cdot b = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \cdot q_1^{\beta_1} \cdot \ldots \cdot q_m^{\beta_m}.$$

Gilt $p \mid a \cdot b$, so existiert eine natürliche Zahl c mit $a \cdot b = p \cdot c$. Schreibt man nun c als Produkt von Primzahlen, so erhält man eine Darstellung von $a \cdot b$ als Produkt von Primzahlen, in dem der Faktor p auftritt. Wegen der Eindeutigkeit der Darstellung von $a \cdot b$ als Produkt von Primzahlen ist der Faktor p ein Element der Menge $\{p_1, \ldots, p_n, q_1, \ldots, q_m\}$. Damit teilt p die Zahl a oder die Zahl b. □

Die Aussage dieses Korollars wird falsch, wenn man die Bedingung weglässt, dass p eine Primzahl ist. Zum Beispiel teilt 6 das Produkt $4 \cdot 9$, während 6 weder 4 noch 9 teilt.

§3.6. Grösster gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Definition 3.28. *Seien a und b natürliche Zahlen. Der* größte gemeinsame Teiler *von a und b ist die größte natürliche Zahl c, die sowohl a als auch b teilt. Der größte gemeinsame Teiler von a und b wird mit $\mathrm{ggT}(a, b)$ bezeichnet. Das* kleinste gemeinsame Vielfache *von a und b ist die kleinste natürliche Zahl, die sowohl von a als auch von b geteilt wird. Das kleinste gemeinsame Vielfache von a und b wird mit $\mathrm{kgV}(a, b)$ bezeichnet.*

Der größte gemeinsame Teiler zweier natürlicher Zahlen a und b existiert, da es einerseits nur endliche viele gemeinsame Teiler von a und b gibt und andererseits 1 ein gemeinsamer Teiler von a und b ist. Das kleinste gemeinsame Vielfache von a und b existiert, da es mindestens ein gemeinsames Vielfaches gibt, nämlich $a \cdot b$, und jede nichtleere Menge natürlicher Zahlen ein kleinstes Element hat.

Ist die Zerlegung von a und b in Primfaktoren gegeben, so können wir $\mathrm{ggT}(a, b)$ und $\mathrm{kgV}(a, b)$ leicht berechnen. Sei p eine Primzahl, c ein gemeinsamer Teiler von a und b und $\alpha \in \mathbb{N}$, so dass $p^\alpha \mid c$ gilt. Dann gilt auch $p^\alpha \mid a$ und $p^\alpha \mid b$. Damit können wir den größten gemeinsamen Teiler von a und b wie folgt bestimmen:

In der Primfaktorzerlegung des größten gemeinsamen Teilers von a und b treten für jede Primzahl p die höchsten Potenzen p^α auf, die sowohl a als auch b teilen. Genauer: Sei $\{p_1, \ldots, p_n\}$ die Menge der Primzahlen, die sowohl a als auch b teilen. Für jedes $i \in \{1, \ldots, n\}$ sei α_i die größte natürliche Zahl, so dass $p_i^{\alpha_i}$ sowohl a als auch b teilt. Dann ist $p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ der größte gemeinsame Teiler von a und b.

Das kleinste gemeinsame Vielfache von a und b lässt sich auf ähnliche Weise finden. Ist nämlich c ein Vielfaches von a und von b, so gilt für jede Primzahl p und jede natürliche Zahl α: Wenn p^α die Zahl a oder die Zahl b teilt, so teilt p^α auch c. Sei nun $\{p_1, \ldots, p_n\}$ die Menge der Primzahlen, die a oder b teilen. Für jedes $i \in \{1, \ldots, n\}$ sei $\alpha_i \in \mathbb{N}$ die größte natürliche Zahl, so dass $p_i^{\alpha_i} \mid a$ oder $p_i^{\alpha_1} \mid b$ gilt. Dann ist $p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ das kleinste gemeinsame Vielfache von a und b.

Man beachte, dass man $\mathrm{ggT}(a, b)$ aus $\mathrm{kgV}(a, b)$ berechnen kann und umgekehrt. Es gilt nämlich die Beziehung

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

Beispiel 3.29. (1) Sei $a = 60$ und $b = 70$. Dann ist $a = 2^2 \cdot 3 \cdot 5$ and $b = 2 \cdot 5 \cdot 7$. Es gilt $\mathrm{ggT}(a, b) = 2 \cdot 5 = 10$ und $\mathrm{kgV}(a, b) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420$.

(2) Sei

$$a = 2^4 \cdot 3 \cdot 5^2 \cdot 7 \cdot 13^4$$

und

$$b = 2^2 \cdot 5 \cdot 7^2 \cdot 13^3 \cdot 17 \cdot 23.$$

Dann ist

$$\mathrm{ggT}(a, b) = 2^2 \cdot 5 \cdot 7 \cdot 13^3$$

und

$$\mathrm{kgV}(a, b) = 2^4 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 13^4 \cdot 17 \cdot 23.$$

Die Zerlegung ganzer Zahlen in ihre Primfaktoren dauert bei Zahlen mit sehr großen Primfaktoren unter Umständen sehr lange. Diese Tatsache ist zum Beispiel wichtig für das weit verbreitete Verschlüsselungsverfahren RSA.

Es gibt aber einen schnellen Algorithmus, mit dem den größten gemeinsamen Teiler zweier natürlicher Zahlen bestimmen kann, der auf Euklid zurückgeht und damit seit über 2000 Jahren bekannt ist. Der Algorithmus benutzt die Division mit Rest.

Satz 3.30. *Für alle $m \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ gibt es eindeutig bestimmte Zahlen q und r mit $0 \leqslant r < n$ und $m = q \cdot n + r$.*

In der Darstellung $m = q \cdot n + r$ nennt man q den *Quotienten* von m und n und r den *Rest*. Die Funktion, die m und n den Quotienten q zuordnet wird mit div bezeichnet. Die Funktion, die m und n den Rest r zuordnet heißt mod. Es gilt also für alle $m \in \mathbb{Z}$ und alle $n \in \mathbb{N}$ die Gleichung

$$m = (m \operatorname{div} n) \cdot n + (m \bmod n).$$

Beispiel 3.31. (1) Sei $m = 27$ und $n = 12$. Dann ist $27 = 2 \cdot 12 + 3$. Der Quotient ist also 2 und der Rest 3.

(2) Sei $m = -10$ und $n = 3$. Dann ist $-10 = -4 \cdot 3 + 2$. Wir haben also $q = -4$ und $r = 2$. Es gilt zwar auch $-10 = -3 \cdot 3 - 1$, aber die Zahlen q und r werden bei der Division mit Rest immer so gewählt, dass $0 \leqslant r < n$ gilt.

Wir stellen Folgendes fest: Ist a ein gemeinsamer Teiler von m und n und gilt $m = q \cdot n + r$, so ist a auch ein Teiler von $r = m - q \cdot n$. Umgekehrt ist jeder gemeinsame Teiler von n und r auch ein Teiler von m. Es folgt, dass die beiden Zahlen m und n dieselben gemeinsamen Teiler haben wie die beiden Zahlen n und r. Für jede natürliche Zahl n ist $\mathrm{ggT}(n, 0) = n$. Das erklärt, warum der folgende Algorithmus zur Berechnung des größten gemeinsamen Teilers zweier natürlicher Zahlen funktioniert.

Der euklidische Algorithmus. Seien $m, n \in \mathbb{N}_0$ mit $m > n$.

(1) Falls $n = 0$ ist, so gib m als den größten gemeinsamen Teiler aus.
(2) Falls $n \neq 0$ ist, so bestimme ganze Zahlen q und r mit $0 \leqslant r < n$ und $m = q \cdot n + r$.
(3) Setze $m := n$ und $n := r$ gehe zurück zu (1).

Nach unserer Vorbemerkung haben m und n in jedem Durchlauf der Schleife in diesem Algorithmus denselben größten gemeinsamen Teiler. Auf der anderen Seite wird n in jedem Durchlauf der Schleife echt kleiner. Also ist nach endlich vielen Schritten $n = 0$ und der Algorithmus terminiert.

Beispiel 3.32. (1) Wir berechnen wieder den größten gemeinsamen Teiler von 70 und 60, aber diesmal mit dem euklidischen Algorithmus. Setze zunächst $m = 70$ und $n = 60$. Wegen $n \neq 0$, führen wir eine Division mit Rest durch. Es gilt $70 = 1 \cdot 60 + 10$. Wir setzen $m := 60$ und $n := 10$. Immer noch gilt $n \neq 0$. Division mit Rest liefert $60 = 6 \cdot 10 + 0$. Wir setzen $m := 10$ und $n := 0$. Nun ist $n = 0$ und der größte gemeinsame Teiler von 10 und 0 ist 10. Die ursprünglichen Zahlen 70 und 60 haben denselben größten gemeinsamen Teiler und daher gilt $\mathrm{ggT}(70, 60) = 10$.

(2) Sei $m = 816$ und $n = 294$. Die Rechnung lautet nun wie folgt:

$$\begin{aligned} 816 &= 2 \cdot 294 + 228 \\ 294 &= 1 \cdot 228 + 66 \\ 228 &= 3 \cdot 66 + 30 \\ 66 &= 2 \cdot 30 + 6 \\ 30 &= 5 \cdot 6 + 0 \end{aligned}$$

Damit ergibt sich $\mathrm{ggT}(816, 294) = 6$.

§3.7. Modulare Arithmetik

Definition 3.33. *Es sei m eine natürliche Zahl. Zwei ganze Zahlen a und b sind* kongruent modulo m, *falls a und b denselben Rest bei Division durch m haben. Ist a kongruent zu b modulo m, so schreiben wir $a \equiv b \,(\mathrm{mod}\, m)$.*

Wir stellen kurz fest, dass $a \equiv b \,(\mathrm{mod}\, m)$ genau dann gilt, wenn $a - b$ durch m teilbar ist. Ist $a \equiv b \,(\mathrm{mod}\, m)$, so existieren ganze Zahlen q_a, q_b und r mit $a = q_a \cdot m + r$, $b = q_b \cdot m + r$ und $0 \leqslant r < m$. Es gilt $a - b = (q_a \cdot m + r) - (q_b \cdot m + r) = (q_a - q_b) \cdot m$. Also ist $a - b$ durch m teilbar.

Sei umgekehrt $a - b$ durch m teilbar. Es gibt ganze Zahlen q_a, q_b, r_a und r_b mit $a = q_a \cdot m + r_a$, $b = q_b \cdot m + r_b$, $0 \leqslant r_a < m$ und $0 \leqslant r_b < m$. Es gilt

$$a - b = (q_a \cdot m + r_a) - (q_b \cdot m + r_b) = (q_a - q_b) \cdot m + (r_a - r_b).$$

Da $a - b$ durch m teilbar ist, ist auch $r_a - r_b$ durch m teilbar. Wegen $0 \leqslant r_a, r_b < m$ gilt $-m < r_a - r_b < m$. Wenn aber eine ganze Zahl, die echt größer als $-m$ und echt kleiner als m ist, durch m teilbar ist, so kann diese Zahl nur 0 sein. Damit ist $r_a - r_b = 0$. Also gilt $a \equiv b \,(\mathrm{mod}\, m)$.

Beispiel 3.34.
(1) $23 \equiv 8 \,(\mathrm{mod}\, 5)$, da $23 - 8 = 15$ durch 5 teilbar ist. Außerdem ist $23 = 4 \cdot 5 + 3$ und $8 = 1 \cdot 5 + 3$, also $23 \,\mathrm{mod}\, 5 = 3 = 8 \,\mathrm{mod}\, 5$.
(2) $-7 \equiv 2 \,(\mathrm{mod}\, 3)$, da $-7 = -3 \cdot 3 + 2$ und $2 = 0 \cdot 3 + 2$, also $-7 \,\mathrm{mod}\, 3 = 2 = 2 \,\mathrm{mod}\, 3$.
(3) $8227 \not\equiv 11 \,(\mathrm{mod}\, 3)$, da $8227 - 11 = 8216$ nicht durch 3 teilbar ist.

Wir betrachten die Menge aller ganzen Zahlen, die modulo m kongruent zu einer festen Zahl sind.

Beispiel 3.35. Sei $m = 3$. Die Menge der Zahlen, deren Rest bei Division durch 3 genau 0 ist, ist die Menge

$$K_0 = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

Die Menge der Zahlen, bei denen der Rest genau 1 ist, ist

$$K_1 = \{\ldots, -5, -2, 1, 4, 7, 10, \ldots\}.$$

Für den Rest 2 erhalten wir die Menge

$$K_2 = \{\ldots, -4, -1, 2, 5, 8, 11, \ldots\}.$$

Definition 3.36. *Für jede natürliche Zahl m und jede ganze Zahl a heißt die Menge* $[a]_m := \{b \in \mathbb{Z} \colon b \,\mathrm{mod}\, m = a \,\mathrm{mod}\, m\}$ *die* Restklasse von a modulo m.

Wir stellen fest, dass es für jede natürliche Zahl m genau m verschiedene Restklassen modulo m gibt, nämlich $[0]_m, \ldots, [m-1]_m$. Diese Restklassen sind paarweise disjunkt und es gilt $\mathbb{Z} = [0]_m \cup \cdots \cup [m-1]_m$.

Folgender Satz sammelt die wichtigsten Regeln für das Rechnen mit Kongruenzen.

Satz 3.37. *Für alle $m \in \mathbb{N}$ und alle $a, b, c, d \in \mathbb{Z}$ gilt:*

(1) $a \equiv a \,(\mathrm{mod}\, m)$
(2) $a \equiv b \,(\mathrm{mod}\, m) \Rightarrow b \equiv a \,(\mathrm{mod}\, m)$
(3) $a \equiv b \,(\mathrm{mod}\, m) \wedge b \equiv c \,(\mathrm{mod}\, m) \Rightarrow a \equiv c \,(\mathrm{mod}\, m)$
(4) $a \equiv b \,(\mathrm{mod}\, m) \Rightarrow -a \equiv -b \,(\mathrm{mod}\, m)$

(5) $a \equiv b \,(\mathrm{mod}\, m) \wedge c \equiv d \,(\mathrm{mod}\, m) \Rightarrow a + c \equiv b + d \,(\mathrm{mod}\, m)$

(6) *Gilt* $\mathrm{ggT}(c, m) = 1$, *so folgt aus* $c \cdot a \equiv c \cdot b \,(\mathrm{mod}\, m)$ *die Kongruenz* $a \equiv b \,(\mathrm{mod}\, m)$.

Diese Rechenregeln kann man direkt mit Hilfe der Definition von $a \equiv b \,(\mathrm{mod}\, m)$ nachrechnen

Beispiel 3.38. In Satz 3.37 (6) muss man wirklich $\mathrm{ggT}(c, m) = 1$ voraussetzen. Zum Beispiel gilt $8 \cdot 3 \equiv 8 \cdot 6 \,(\mathrm{mod}\, 6)$ aber nicht $3 \equiv 6 \,(\mathrm{mod}\, 6)$.

Nützliche Operationen auf den reellen Zahlen, mit deren Hilfe man zum Beispiel auch die Funktionen div und mod berechnen kann, sind das Auf- und Abrunden.

Definition 3.39. *Für eine reelle Zahl* r *ist* $\lceil r \rceil$ *die kleinste ganze Zahl* $\geqslant r$. *Analog ist* $\lfloor r \rfloor$ *die größte ganze Zahl* $\leqslant r$. *Man nennt* $\lceil \quad \rceil$ *die* obere Gaußklammer *und* $\lfloor \quad \rfloor$ *die* untere Gaußklammer.

Beispiel 3.40. Es gilt

$$\begin{array}{rclrcl} \lceil 3.14 \rceil & = & 4, & \lfloor 3.14 \rfloor & = & 3, \\ \lceil \sqrt{2} \rceil & = & 2, & \lfloor \sqrt{2} \rfloor & = & 1, \\ \lceil 5 \rceil & = & 5, & \lfloor 5 \rfloor & = & 5, \\ \lceil -1.2 \rceil & = & \text{-1}, & \lfloor -1.2 \rfloor & = & \text{-2}. \end{array}$$

Für alle $m \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt $m \,\mathrm{div}\, n = \lfloor \frac{m}{n} \rfloor$ sowie $m \bmod n = m - n \cdot \lfloor \frac{m}{n} \rfloor$.

$$\begin{cases} a \\ b \end{cases}$$

□

Notation

$\mathbb{N}$: natürliche Zahlen $\{1, 2, 3, \dots\}$

$\mathbb{N}_0$: natürliche Zahlen mit Null $\{0, 1, 2, 3, \dots\}$

$[n]$: ersten n natürliche Zahlen $\{1, 2, 3, \dots, n\}$

$\mathcal{P}(M)$: Potenzmenge von M $\{A\colon A \subseteq M\}$

$\mathbb{Z}$: ganze Zahlen $\{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q}$: rationale Zahlen $\left\{\frac{a}{b}\colon a \in \mathbb{Z} \text{ und } b \in \mathbb{Z} \setminus \{0\}\right\}$

$\mathbb{R}$: reelle Zahlen