

Mathematik für Informatiker I

(Diskrete Mathematik)

– Vorlesungsskript WiSe 2016/17 –
Version: 21. Oktober 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, Beweistechniken und Themen aus der Diskreten Mathematik

- 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

Vorwort	iii
Ergänzende Literatur	v
Kapitel 1. Mathematische Grundlagen und Logik	1
1.1. Mengen	1
1.2. Elementare Logik	2
1.3. Mengenoperationen	5
1.4. Abbildungen	7
1.5. Boolesche Algebra	9
1.6. Summen- und Produktzeichen	12
Kapitel 2. Natürliche Zahlen und vollständige Induktion	15
2.1. Natürliche Zahlen	15
2.2. Prinzip der vollständigen Induktion	15
2.3. Peano Axiome	22
Notation	25

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 \emptyset 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 $\mathbb{N}_0 = \{0, 1, 2, \dots\}$.

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

ist die Menge der natürlichen Zahlen, die echt 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

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

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 $a \rightarrow b$ ist also immer dann wahr, wenn a falsch ist oder b wahr. Ist $a \rightarrow b$ 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 \rightarrow 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:

Es regnet \Rightarrow 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 $a \text{ xor } b$ 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. Auf 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 $a \rightarrow b$ ist äquivalent zu $\neg b \rightarrow \neg a$.*

BEWEIS. Wir schreiben die entsprechende Wahrheitstafel auf.

a	b	$\neg a$	$\neg b$	$a \rightarrow b$	$\neg b \rightarrow \neg a$
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 $a \rightarrow b$ und $\neg b \rightarrow \neg a$ in der Tat äquivalent. \square

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 „ $2 + x \leq 7$ “, so ist $\neg a(x)$ die Aussageform „ $2 + x \not\leq 7$ “ 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:

Wenn $x = 2$ 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

Für alle natürlichen Zahlen x 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

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

(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

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

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

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

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

$$\mathcal{P}(M) := \{x : x \subseteq M\}$$

die Potenzmenge von M . Wir fixieren M und betrachten nur Teilmengen von M . Für $A \in \mathcal{P}(M)$ sei

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

das Komplement von A in M .

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

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

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

sowie

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

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. \square

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 $\{(a, b) : a \in A \text{ und } b \in B\}$ 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 $\{(a_1, a_2, a_3) : a_1, a_2, a_3 \in A\}$ aller Tripel von Elementen von A . Analog ist für jede natürliche Zahl $n \geq 1$ A^n die Menge $\{(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}$ 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 $f: A \rightarrow B$. 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 $\{f(x) : x \in A\}$.

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

$$f: \mathbb{N} \rightarrow \mathbb{N}; n \mapsto n^2.$$

- (2) Der Ausdruck $g: \mathbb{N}^2 \rightarrow \mathbb{N}, (m, n) \mapsto m + n$ 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 $f: A \rightarrow B$:

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 $f: A \rightarrow B$ 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 $f: A \rightarrow B$ 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 $g: A \rightarrow B$ 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 $f: A \rightarrow B$ 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 $f: A \rightarrow B$ mit $f(1) = 2, f(2) = 1, f(3) = 4$ ist injektiv, aber nicht surjektiv.
- (5) Die Abbildung $h: \mathbb{N} \rightarrow \mathbb{N}; n \mapsto n^2$ 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 Möglichkeit 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 $n \geq 2$ ist $n^2 \geq 2^2$ 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 $f: M^n \rightarrow M$.

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

§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 $\neg: B \rightarrow B$ und den zwei zweistelligen Verknüpfungen $\sqcap, \sqcup: B^2 \rightarrow B$. $(B, \sqcap, \sqcup, \neg, 0, 1)$ heißt eine Boolesche Algebra, wenn für alle $a, b, c \in B$ die folgenden Gleichungen gelten:

(A1) Assoziativgesetze:

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

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

(A2) *Kommutativgesetze:*

$$\bullet a \sqcap b = b \sqcap a$$

$$\bullet a \sqcup b = b \sqcup a$$

(A3) *Distributivgesetze:*

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

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

(A4) *Beschränktheit:*

$$\bullet a \sqcap 1 = a$$

$$\bullet a \sqcup 0 = a$$

(A5) *Komplementierung:*

$$\bullet a \sqcap \neg a = 0$$

$$\bullet a \sqcup \neg a = 1$$

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 $0 := \emptyset$ 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 $a = (a_1, \dots, a_8)$ und $b = (b_1, \dots, b_8)$ sei

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

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

und

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

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, insbesondere 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

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

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

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

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

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 $a \sqcup 1 = 1$ folgt aus $a \sqcap 0 = 0$ nach dem Dualitätsprinzip. \square

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 nachrechnen. 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, \dots, a_n sei

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

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:

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

Falls $a_1 = \dots = a_n = a$ 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, \dots, b_n ist

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

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

$$(a_1 + \dots + a_m)(b_1 + \dots + b_n) = a_1 b_1 + \dots + a_1 b_n + \dots + a_m b_1 + \dots + a_m b_n.$$

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, \dots, a_n reelle Zahlen, so setzt man

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

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 $\forall n \in \mathbb{N}: A(n)$ 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 $A(n)$:

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

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. \square

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

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

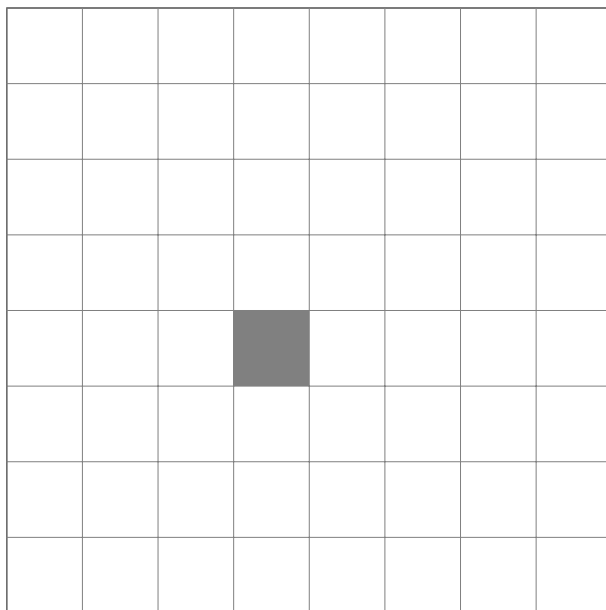
Der erste Summand der rechten Seite dieser Gleichung, $n^3 - n$, ist nach Induktionsannahme durch 3 teilbar. Der Rest, $3n^2 + 3n$, ist offenbar auch durch 3 teilbar. Das zeigt $3|(n+1)^3 - (n+1)$ und damit $A(n+1)$.

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 $n \in \mathbb{N}$. \square

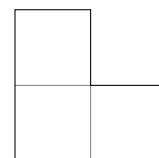
Als nächstes diskutieren wir ein Beispiel, das zeigt, dass der Erfolg einer Induktion von der geschickten Wahl des Induktionsanfangs abhängen kann. Außerdem liefert der folgende Beweis einen Algorithmus, also ein Verfahren, zur Lösung des vorgelegten Problems.

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 Seitenlänge 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.

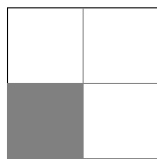
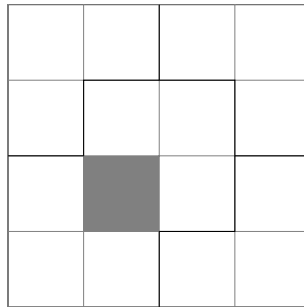


Hof



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.“

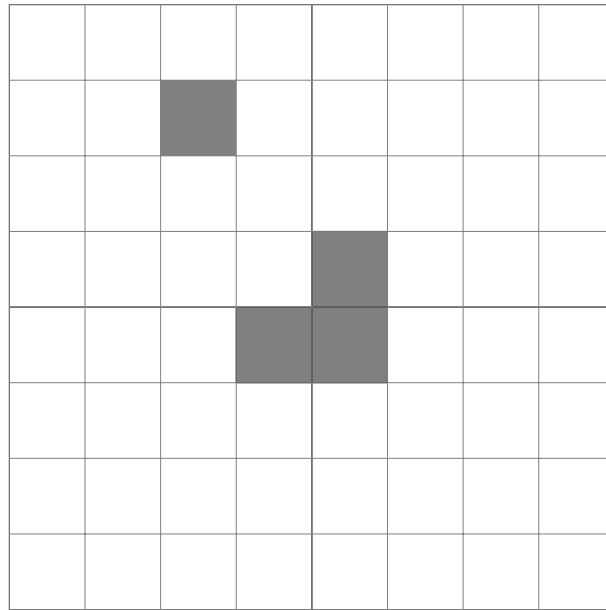
Es stellt sich heraus, dass wir Schwierigkeiten haben, die gewünschte Induktion mit dieser Induktionsannahme durchzuführen. Einen Hof der Kantenlänge 2^{n+1} können wir in vier quadratische Teile mit der Kantenlänge 2^n zerlegen, aber das fehlende Quadrat in der Mitte des Quadrats mit Kantenlänge 2^{n+1} liegt nun am Rand eines der Quadrate mit Kantenlänge 2^n . Bei den anderen drei Quadraten 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 $n \geq n_0$, wenn $A(n_0)$ wahr ist und die Implikation $A(n) \Rightarrow A(n+1)$ für alle $n \geq n_0$ gilt.

Als Beispiel beweisen wir eine einfache Ungleichung.

Satz 2.4. Für alle natürlichen Zahlen $n \geq 3$ 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 $n \geq 3$ gilt: $A(n) \rightarrow A(n + 1)$

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

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

Das zeigt $A(n + 1)$.

Es folgt, dass $A(n)$ für alle $n \geq 3$ 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 $\sum_{i=0}^n q^i = 1 + q + \dots + q^n$ 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 $n \geq 0$ gilt (Induktionsannahme). Dann gilt sie auch für $n + 1$:

$$\begin{aligned} \sum_{i=0}^{n+1} q^i &= \sum_{i=0}^n q^i + q^{n+1} \stackrel{\text{I.A.}}{=} \frac{1 - q^{n+1}}{1 - q} + q^{n+1} = \frac{1 - q^{n+1}}{1 - q} + \frac{q^{n+1}(1 - q)}{1 - q} \\ &= \frac{1 - q^{n+1} + q^{n+1} - q^{n+2}}{1 - q} = \frac{1 - q^{n+2}}{1 - q} \end{aligned}$$

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

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: $A(1) \wedge \dots \wedge A(n) \Rightarrow A(n + 1)$.

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

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

Beispiel 2.6. Wir definieren eine 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 $n \geq 1$ sei $f_{n+1} = f_{n-1} + f_n$.

Die Zahlen f_0, f_1, f_2, \dots heißen Fibonacci-Zahlen. Die ersten 10 Glieder der Folge f_0, f_1, f_2, \dots 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 $n \geq 1$, 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 $n \geq 1$ 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 $n \geq 1$. Dazu nehmen wir an, dass für ein gewisses $n \geq 1$ 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

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

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 natürlichen 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 $S = \{n \in \mathbb{N} : A(n) \text{ ist wahr}\}$ 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.

- (1) $1 \in \mathbb{N}$
- (2) $n \in \mathbb{N} \Rightarrow n' \in \mathbb{N}$
- (3) $n \in \mathbb{N} \Rightarrow n' \neq 1$
- (4) $m, n \in \mathbb{N} \Rightarrow (m' = n' \Rightarrow m = n)$
- (5) $(1 \in S \wedge \forall n \in \mathbb{N}(n \in S \Rightarrow n' \in S)) \Rightarrow \mathbb{N} \subseteq S$

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

- (1) 1 ist eine natürliche Zahl.
- (2) Der Nachfolger einer natürlichen Zahl ist wieder eine natürliche Zahl.
- (3) 1 ist nicht Nachfolger einer natürlichen Zahl.
- (4) Die Nachfolgerfunktion $n \mapsto n'$ ist injektiv.
- (5) Jede induktive Menge enthält alle natürlichen Zahlen.

Auf Basis dieser Axiome kann man nun die bekannte Operationen $+$ und \cdot sowie die Relation \leq 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 $A \neq \emptyset$. 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 $1, \dots, n$ Elemente von B sind, dass also $P(1), \dots, P(n)$ 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 $A = \emptyset$, im Widerspruch zu $A \neq \emptyset$. Damit hat A ein kleinstes Element. \square

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: $\forall k \in \mathbb{N} (k \leq n \Rightarrow k \in B)$

Dann kann man an Stelle der Induktionsannahme $P(1) \wedge \dots \wedge P(n)$ einfach $Q(n)$ schreiben. Man beweist dann im Induktionsschritt nicht $(P(1) \wedge \dots \wedge P(n)) \Rightarrow P(n')$, 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 $(\forall n \in \mathbb{N})P(n)$.

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 $\{A: A \subseteq M\}$

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

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

\mathbb{R} : reelle Zahlen