

Logik und Diskrete Strukturen

Kapitel 1: Grundlagen

Prof. Dr. Jasmin Blanchette

Lehr- und Forschungseinheit für Theoretische Informatik und Theorembeweisen

Sommersemester 2026

Basierend auf Folien von PD Dr. Jan Johannsen

Übersicht

Mengen

Relationen

Funktionen

Beweise

Induktion

Mengen

“Definition” (Georg Cantor)

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

Notation für Mengen:

- ▶ Aufzählung: $\{2, 3, 5, 8\}$
auch unvollständig: $\{0, 1, 2, \dots, 99\}$
oder unendlich: $\{1, 3, 5, 7, \dots\}$
- ▶ Komprehension: $\{x \mid \varphi(x)\}$ für Eigenschaft $\varphi(x)$
- ▶ Aussonderung: $\{x \in M \mid \varphi(x)\}$
- ▶ Bekannte Mengen: $\mathbb{N} = \{0, 1, \dots\}$, \mathbb{Z} , \mathbb{Q} , \mathbb{R} , \mathbb{C}
- ▶ $[n] = \{1, \dots, n\}$

Elemente und Teilmengen

Notation:

$a \in M$ a ist Element von M

$a \notin M$ a ist nicht Element von M

$A \subseteq B$ A ist Teilmenge von B

d.h.: für alle x gilt: aus $x \in A$ folgt $x \in B$.

Extensionalität

Mengen sind durch ihre Elemente bestimmt:

$A = B$ gdw. für alle x gilt: $x \in A$ gdw. $x \in B$
gdw. $A \subseteq B$ und $B \subseteq A$

Die **leere Menge** $\{\}$, auch als \emptyset notiert, enthält keine Elemente.

Operationen auf Mengen

Vereinigung

$$A \cup B := \{x \mid x \in A \text{ oder } x \in B\}$$

Schnitt

$$A \cap B := \{x \mid x \in A \text{ und } x \in B\}$$

Differenz

$$A \setminus B := \{x \mid x \in A \text{ und } x \notin B\}$$

Symmetrische Differenz

$$A \triangle B := (A \setminus B) \cup (B \setminus A)$$

Eigenschaften

Assoziativität

$$(A \cup B) \cup C = A \cup (B \cup C) \quad \text{und} \quad (A \cap B) \cap C = A \cap (B \cap C)$$

Kommutativität

$$A \cup B = B \cup A \quad \text{und} \quad A \cap B = B \cap A$$

Idempotenz

$$A \cup A = A \quad \text{und} \quad A \cap A = A$$

Distributivität

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \quad \text{und} \\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

Eigenschaften der leeren Menge

$$A \cup \emptyset = A \quad (\text{neutral})$$

$$A \cap \emptyset = \emptyset \quad (\text{absorbierend})$$

Verallgemeinerte Operationen

Sind A_1, \dots, A_n Mengen, so schreibt man

$$\bigcup_{i=1}^n A_i$$

für die Vereinigung $A_1 \cup A_2 \cup \dots \cup A_n$.

Allgemeiner: für eine (Index-)Menge I und Mengen A_i für $i \in I$:

$$\bigcup_{i \in I} A_i$$

Analog für \cap und andere (assoziative und kommutative) Operationen.

Kardinalität

Kardinalität (oder Mächtigkeit) von A :
Anzahl der Elemente von A , notiert $|A|$

Es ist $|\emptyset| = 0$.

A ist endlich gdw. $|A| \in \mathbb{N}$.

Unendliche Mengen sind beispielsweise $\mathbb{N}, \mathbb{Q}, \mathbb{R}$.

Theorem (Cantor)

Es ist $|\mathbb{Q}| = |\mathbb{N}|$, aber $|\mathbb{R}| > |\mathbb{N}|$.

Disjunktheit

Kardinalität der Vereinigung:

$$|A \cup B| = |A| + |B| - |A \cap B|$$

$$\text{Insbesondere } |A \cup B| \leq |A| + |B|$$

Mengen A, B heißen **disjunkt**, wenn $A \cap B = \emptyset$ ist.

Sind A, B disjunkt, dann schreibe $A \uplus B$ für $A \cup B$.

Dann gilt: $|A \uplus B| = |A| + |B|$.

Potenzmenge

Die **Potenzmenge** $\mathcal{P}(M)$ einer Menge M ist

$$\{A \mid A \subseteq M\}$$

Beispiel: $M = \{a, b, c\}$

$$\mathcal{P}(M) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

Es gibt auch die Notation $2^M = \mathcal{P}(M)$.

Es ist $\mathcal{P}(\emptyset) = \{\emptyset\}$ und $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$.

Ist M endlich, so ist $|\mathcal{P}(M)| = 2^{|M|}$.

Kartesisches Produkt

Geordnetes Paar: (a, b)

Eigenschaft: $(a, b) = (c, d)$ gdw. $a = c$ und $b = d$

Kartesisches Produkt

$$A \times B := \{(x, y) \mid x \in A \text{ und } y \in B\}$$

Es gilt: $|A \times B| = |A| \cdot |B|$.

Definiere induktiv:

$$\begin{aligned} A^1 &= A \\ A^{i+2} &= A \times A^{i+1} \end{aligned}$$

Notation: $(a_1, \dots, a_k) \in A^k$

Ende der 1. Vorlesung

Relationen

Relation R zwischen zwei Mengen A und B

$$R \subseteq A \times B$$

Ist $A = B$, also $R \subseteq A \times A$,

spricht man von einer Relation auf A

Ist R eine Relation auf A und $a, b \in A$,

schreibt man auch $a R b$ statt $(a, b) \in R$

Allgemeiner: n -stellige Relation $R \subseteq A^n$.

Beispiele für Relationen

A	B	$a R b$
\mathbb{N}	\mathbb{N}	$a < b$
\mathbb{N}	\mathbb{N}	$a \text{ teilt } b$
Menschen	Menschen	$a \text{ kennt } b$
Katzen	Menschen	$a \text{ gehört } b$
M	$\mathcal{P}(M)$	$a \in b$

Eigenschaften von Relationen

Eine Relation R auf A heißt

▶ **reflexiv**

für alle $a \in A$ gilt: $a R a$

▶ **transitiv**

für alle $a, b, c \in A$ gilt: wenn $a R b$ und $b R c$, dann $a R c$

▶ **symmetrisch**

für alle $a, b \in A$ gilt: wenn $a R b$, dann $b R a$

▶ **antisymmetrisch**

für alle $a, b \in A$ gilt: wenn $a R b$ und $b R a$, dann $a = b$

Besondere Relationen

Eine Relation R auf A heißt

- ▶ **Quasiordnung**
wenn sie reflexiv und transitiv ist
- ▶ **partielle Ordnung**
wenn sie reflexiv, transitiv und antisymmetrisch ist
- ▶ **totale** oder **lineare Ordnung**
wenn sie partielle Ordnung ist,
und für alle $a, b \in A$ gilt $a R b$ oder $b R a$
- ▶ **Äquivalenzrelation**
wenn sie reflexiv, transitiv und symmetrisch ist

Beispiele für besondere Relationen

- ▶ Totale Ordnungen:
das übliche \leq auf \mathbb{R}
- ▶ Partielle Ordnungen:
Teilbarkeit $a \mid b$ auf $\mathbb{N} \setminus \{0\}$
Teilmengen \subseteq auf $\mathcal{P}(A)$
- ▶ Quasiordnungen:
 $|A| \leq |B|$ auf $\mathcal{P}(\mathbb{N})$
- ▶ Äquivalenzrelationen:
 $|A| = |B|$ auf $\mathcal{P}(\mathbb{N})$
 $x \bmod 7 = y \bmod 7$ auf \mathbb{N}

Äquivalenzklassen

Partition einer Menge A :

Familie von Teilmengen A_1, \dots, A_k mit

- ▶ $A_i \neq \emptyset$ für alle i
- ▶ $A_i \cap A_j = \emptyset$ für $i \neq j$
- ▶ $A_1 \cup \dots \cup A_k = A$

Sei \equiv eine Äquivalenzrelation auf A .

Für $a \in A$ ist

$$[a] := \{x \in A \mid x \equiv a\}$$

die Äquivalenzklasse von a .

Äquivalenzklassen

Lemma

$a \equiv b$ gdw. $[a] = [b]$.

Beweis.

Wir zeigen nur eine Richtung: wenn $a \equiv b$, dann $[a] = [b]$.

Um $[a] = [b]$ zu zeigen, reicht es, $[a] \subseteq [b]$ und $[b] \subseteq [a]$ zu zeigen.

Durch Symmetrie reicht es, $[a] \subseteq [b]$ zu beweisen.

Sei $c \in [a]$.

Dann ist $c \equiv a$.

Da $a \equiv b$, ist auch $c \equiv b$ (durch die Transitivität von \equiv).

Also ist $c \in [b]$.

Somit $[a] \subseteq [b]$.



Äquivalenzklassen

Die Äquivalenzklassen $[a]$ für $a \in A$ bilden eine Partition von A :

Lemma

1. für $a, b \in A$ ist $[a] = [b]$ oder $[a] \cap [b] = \emptyset$
2. $A = \bigcup_{a \in A} [a]$

Beweis.

Wir zeigen Punkt 1: Wenn $[a] \cap [b] \neq \emptyset$, dann gilt $[a] = [b]$.

Es gibt $c \in [a] \cap [b]$.

Da $c \in [a]$, ist $c \equiv a$.

Da $c \in [b]$, ist $c \equiv b$.

Also ist $a \equiv b$ (durch die Transitivität von \equiv).

Somit $[a] = [b]$ (mit dem vorherigen Lemma). □

Quasiordnung

Ist \succsim eine Quasiordnung auf A , so ist

$$a \simeq b \text{ gdw. } a \succsim b \text{ und } b \succsim a$$

eine Äquivalenzrelation.

Induzierte Ordnung auf Äquivalenzklassen von \simeq :

$$[a] \preceq [b] \text{ gdw. } a \succsim b$$

Quasiordnung

Lemma

Die Relation \preceq ist wohldefiniert.

Mit anderen Worten, wenn $a \preceq b$, $[a] = [a']$ und $[b] = [b']$, dann $a' \preceq b'$.

Beweis.

Da $[a] = [a']$, ist $a \simeq a'$, d.h. $a \preceq a'$ und $a' \preceq a$.

Da $[b] = [b']$, ist $b \simeq b'$, d.h. $b \preceq b'$ und $b' \preceq b$.

Daher $a' \preceq a \preceq b \preceq b'$.

Daher $a' \preceq b'$ (durch die Transitivität von \preceq).



Quasiordnung

Lemma

\preceq ist eine partielle Ordnung auf der Menge der Äquivalenzklassen von \simeq .

Beweis.

Wir müssen zeigen, dass \preceq reflexiv, transitiv und antisymmetrisch ist.

- ▶ **Reflexivität:** $[a] \preceq [a]$, da $a \simeq a$.
- ▶ **Transitivität:** Wir nehmen $[a] \preceq [b]$ und $[b] \preceq [c]$ an und zeigen $[a] \preceq [c]$.
Aus den Annahmen folgen $a \simeq b$ sowie $b \simeq c$.
Daher $a \simeq c$ (durch die Transitivität).
- ▶ **Antisymmetrie:** Wir nehmen $[a] \preceq [b]$ und $[b] \preceq [a]$ an und zeigen $[a] = [b]$.
Aus den Annahmen folgen $a \simeq b$ sowie $b \simeq a$.
Daher $a \simeq b$.
Somit $[a] = [b]$ (mit einem vorherigen Lemma).



Funktionen

Eine Relation $R \subseteq A \times B$ heißt **Funktion** von A nach B , wenn für alle $a \in A$ gilt $|\{b \in B \mid a R b\}| = 1$.

Notation:

- ▶ $f(a)$ ist das eindeutige $b \in B$ mit $(a, b) \in f$.
- ▶ $f : A \rightarrow B$
- ▶ $f^{-1}(b) = \{a \in A \mid f(a) = b\}$ **Urbild** von b
- ▶ $f(A') = \{f(a) \mid a \in A'\}$ für $A' \subseteq A$
- ▶ $f^{-1}(B') = \bigcup_{b \in B'} f^{-1}(b) = \{a \in A \mid f(a) \in B'\}$ für $B' \subseteq B$

Eigenschaften von Funktionen

Eine Funktion $f : A \rightarrow B$ heißt

- ▶ **injektiv**, wenn $f(a_1) = f(a_2)$ nur gilt, wenn $a_1 = a_2$,
also für alle $b \in B$ gilt $|f^{-1}(b)| \leq 1$
- ▶ **surjektiv**, wenn es für jedes $b \in B$ ein $a \in A$ gibt mit $f(a) = b$,
also für alle $b \in B$ gilt $|f^{-1}(b)| \geq 1$,
also wenn $f(A) = B$
- ▶ **bijektiv**, wenn f injektiv und surjektiv ist,
also für alle $b \in B$ gilt $|f^{-1}(b)| = 1$

Sind A, B endlich und $f : A \rightarrow B$ bijektiv, so ist $|A| = |B|$.

Eigenschaften von Funktionen

Theorem

Ist $|A| = |B|$ endlich und $f : A \rightarrow B$, so gilt:

f ist injektiv gdw. f ist surjektiv gdw. f ist bijektiv

Beweis.

Wir beweisen: f ist injektiv gdw. f ist surjektiv. Daraus folgt die zweite Biimplikation direkt.

Falls f injektiv ist, dann gilt $|f(A)| = |A|$.

Durch die Annahme gilt $|A| = |B|$. Da $|A|, |B|$ endlich sind, muss jedes Element von B von einem Element von A getroffen sein.

Somit ist f surjektiv.

Falls f surjektiv ist, dann gilt $f(A) = B$.

Wenn f nicht injektiv wäre, hätten wir $|f(A)| < |A|$ (da $|A|$ endlich ist).

Aber dann $|f(A)| = |B| = |A|$. Widerspruch. □

Funktionskomposition

Seien $f : B \rightarrow C$ und $g : A \rightarrow B$ Funktionen.

Die **Komposition** $f \circ g : A \rightarrow C$ ist definiert durch

$$(f \circ g)(x) = f(g(x)) \quad \text{für } x \in A$$

Man schreibt auch $f \circ g = x \mapsto f(g(x))$.

Die **Identitätsfunktion** $id : A \rightarrow A$ ist gegeben durch

$$id(x) = x \quad \text{für alle } x \in A$$

Es gilt: $id \circ f = f \circ id = f$ für jede Funktion f .

Definition: für eine Funktion $f : A \rightarrow A$

- ▶ $f^0 = id$
- ▶ $f^{i+1} = f \circ f^i$
- ▶ $f^{-k} = (f^{-1})^k$

Bijektive Funktionen

Lemma

Sind f und g beide injektiv, so ist $f \circ g$ injektiv.

Beweis (durch Kontraposition).

Nehmen wir an, dass $f \circ g$ nicht injektiv ist.

Dann gibt es $x_1, x_2 \in A$, sodass $x_1 \neq x_2$ und $(f \circ g)(x_1) = (f \circ g)(x_2)$.

Das heißt, $f(g(x_1)) = f(g(x_2))$.

Sei $y_1 = g(x_1)$ und $y_2 = g(x_2)$.

► **Fall 1:** $y_1 \neq y_2$.

Da $f(y_1) = f(y_2)$, ist f nicht injektiv.

► **Fall 2:** $y_1 = y_2$.

Da $g(x_1) = y_1 = y_2 = g(x_2)$, ist g nicht injektiv.



Bijektive Funktionen

Lemma

Sind f und g beide surjektiv, so ist $f \circ g$ surjektiv.

Beweis (durch Kontraposition).

Nehmen wir an, dass $f \circ g$ nicht surjektiv ist.

Dann gibt es $z \in C$, sodass $f(g(x)) \neq z$ für alle $x \in A$.

- ▶ **Fall 1:** Es gibt $y \in B$ mit $f(y) = z$.
Dann gilt $g(x) \neq y$ für alle $x \in A$. (Sonst hätten wir $f(g(x)) = z$.)
Also ist g nicht surjektiv.
- ▶ **Fall 2:** Es gibt kein $y \in B$ mit $f(y) = z$.
Dann ist f nicht surjektiv.



Bijektive Funktionen

Lemma

Sind f und g beide bijektiv, dann ist $f \circ g$ bijektiv.

Beweis.

Das Lemma folgt aus den letzten zwei Lemmata. □

Bijektive Funktionen

Ist $f : A \rightarrow B$ bijektiv, dann gilt $|f^{-1}(b)| = 1$ für alle $b \in B$.

Schreibe $f^{-1}(b) = a$ statt $f^{-1}(b) = \{a\}$ (**Umkehrfunktion**).

Die Umkehrfunktion ist die bijektive Funktion $f^{-1} : B \rightarrow A$.

Eine bijektive Funktion $f : A \rightarrow A$ heißt **Permutation**.

Struktur von Permutationen

Sei $f : A \rightarrow A$ eine Permutation.

Definition: für $a, b \in A$

$$a \equiv_f b \quad \text{gdw.} \quad b = f^z(a) \quad \text{für ein } z \in \mathbb{Z}$$

Struktur von Permutationen

Lemma

\equiv_f ist eine Äquivalenzrelation auf A .

Beweis.

Wir müssen zeigen, dass \equiv reflexiv, transitiv und symmetrisch ist.

- ▶ **Reflexivität:** Folgt aus $a = f^0(a)$.
- ▶ **Transitivität:** Aus $a \equiv_f b$ und $b \equiv_f c$ folgt $a = f^z(b)$ sowie $b = f^{z'}(c)$.
Daher $a = f^{z+z'}(c)$.
- ▶ **Symmetrie:** $a = f^z(b)$ gdw. $b = f^{-z}(a)$.



Struktur von Permutationen

Für die Äquivalenzklassen gilt:

- ▶ Ist $|[a]| = k$ endlich, dann ist

$$[a] = \{a, f(a), \dots, f^{k-1}(a)\} \quad \text{und} \quad f^k(a) = a$$

- ▶ Ist $[a]$ unendlich, dann ist

$$[a] = \{\dots, f^{-2}(a), f^{-1}(a), a, f(a), f^2(a), \dots\}$$

Die Äquivalenzklassen heißen **Zyklen** von f .

Exkurs: Kardinalität formal

Definiere $A \simeq B$ gdw. es eine bijektive Funktion $f : A \rightarrow B$ gibt.

Lemma

\simeq ist eine Äquivalenzrelation.

Beweis.

Wir müssen zeigen, dass \simeq reflexiv, transitiv und symmetrisch ist.

- ▶ **Reflexivität:** Die Identitätsfunktion $A \rightarrow A$ ist bijektiv.
- ▶ **Transitivität:** Wenn $f : A \rightarrow B$ und $g : B \rightarrow C$ bijektiv sind, dann ist $f \circ g$ bijektiv.
- ▶ **Symmetrie:** Wenn $f : A \rightarrow B$ bijektiv ist, dann ist $f^{-1} : B \rightarrow A$ bijektiv. □

Exkurs: Kardinalität formal

Die Äquivalenzklassen von \simeq sind Kardinalzahlen.

Für endliche Mengen A definiere

$$|A| = n \quad \text{gdw.} \quad A \simeq [n]$$

Theorem (Cantor)

Es ist $\mathbb{Q} \simeq \mathbb{N}$, aber $\mathbb{R} \not\simeq \mathbb{N}$.

Ende der 2. Vorlesung

Mathematische Aussagen

Mathematische Aussagen sind zusammengesetzt aus einfacheren Aussagen mit den folgenden Operationen:

Bezeichnung	Notation	Bedeutung
Konjunktion	$A \wedge B$	A und B
Disjunktion	$A \vee B$	A oder B
Implikation	$A \rightarrow B$	wenn A gilt, dann auch B
Biimplikation	$A \leftrightarrow B$	A gilt gdw. B gilt
Negation	$\neg A$	A gilt nicht
Allquantifikation	$\forall x \in M A$	A gilt für alle $x \in M$
Existenzquantifikation	$\exists x \in M A$	A gilt für ein $x \in M$

Viele mathematische Sätze sind von der Form

$$\forall a_1 \in S_1 \dots \forall a_n \in S_n (A_1 \wedge \dots \wedge A_m \rightarrow B)$$

Beweise mit Konjunktion und Disjunktion

Um zu zeigen, dass $A \wedge B$ gilt,

beweise A und beweise B

Um die Annahme $A \wedge B$ zu verwenden,

verwende Annahme A und verwende Annahme B

Um zu zeigen, dass $A \vee B$ gilt,

beweise A oder beweise B

Um die Annahme $A \vee B$ zu verwenden,

beweise C unter der Annahme A

beweise C unter der Annahme B

verwende Annahme C

(Fallunterscheidung)

Beweise mit Implikation

Um zu zeigen, dass $A \rightarrow B$ gilt,

beweise B unter der Annahme A

Um die Annahme $A \rightarrow B$ zu verwenden,

beweise A

verwende Annahme B

Um zu zeigen, dass $A \leftrightarrow B$ gilt,

beweise B unter der Annahme A und

beweise A unter der Annahme B

Um die Annahme $A \leftrightarrow B$ zu verwenden,

verwende Annahme $A \rightarrow B$ und

verwende Annahme $B \rightarrow A$

Beweise mit Quantoren

Um zu zeigen, dass $\forall x \in M A(x)$ gilt,

beweise $A(m)$ für ein festes, aber beliebiges $m \in M$

Um die Annahme $\forall x \in M A(x)$ zu verwenden,

wähle ein $m_0 \in M$ und verwende die Annahme $A(m_0)$

Um zu zeigen, dass $\exists x \in M A(x)$ gilt,

wähle ein $m_0 \in M$ und beweise $A(m_0)$

Um die Annahme $\exists x \in M A(x)$ zu verwenden,

verwende die Annahme $A(m)$ für ein festes, aber beliebiges $m \in M$

Beweise mit Quantoren

Beispiel

Für alle $n \in \mathbb{N}$ gilt: ist n ungerade, dann ist auch n^2 ungerade.

Beweis.

Zu zeigen: $\forall n \in \mathbb{N}, n \text{ ungerade} \rightarrow n^2 \text{ ungerade}$.

Das heißt, $\forall n \in \mathbb{N}, (\exists k \in \mathbb{N}, n = 2k + 1) \rightarrow (\exists k' \in \mathbb{N}, n^2 = 2k' + 1)$.

Anmerkung: $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$.

Wir wählen $2k^2 + 2k$ für k' , woraus sich $n^2 = 2k' + 1$ ergibt. □

Beweis durch Kontraposition

Um zu zeigen, aus A folgt B ,

beweise $\neg A$ unter der Annahme $\neg B$

Beispiel

Für alle $n \in \mathbb{N}$ gilt: ist n^2 gerade, dann ist auch n gerade.

Beweis (durch Kontraposition).

Wir zeigen: ist n nicht gerade, dann ist auch n^2 nicht gerade.

Siehe letztes Beispiel. □

Beweise mit Negation

Um zu zeigen, dass $\neg A$ gilt,

zeige unter der Annahme A einen Widerspruch

Um zu zeigen, dass A gilt,

zeige unter der Annahme $\neg A$ einen Widerspruch

Beweis mit Negation

Beispiel

$\sqrt{2}$ ist irrational, d.h. $\sqrt{2} \notin \mathbb{Q}$.

Beweis.

Wir nehmen an, dass $\sqrt{2} \in \mathbb{Q}$.

Das heißt, es gibt $p, q \in \mathbb{N}$, sodass $\sqrt{2} = \frac{p}{q}$ und $\text{ggT}(p, q) = 1$.

Das heißt, $(\frac{p}{q})^2 = 2$, also $\frac{p^2}{q^2} = 2$, also $p^2 = 2q^2$.

Insbesondere ist p^2 gerade, und daher ist p gerade (d.h. $\exists p' \in \mathbb{N}, p = 2p'$).

Es gibt also p' , sodass $(2p')^2 = 2q^2$. Das heißt, $4p'^2 = 2q^2$, also $2p'^2 = q^2$.

Insbesondere ist q^2 gerade, und daher ist q gerade.

Das heißt, 2 ist ein Teiler von p und von q .

Das ist aber unmöglich, da $\text{ggT}(p, q) = 1$. Widerspruch. □

Vollständige Induktion

Um zu zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt, zeige

Induktionsanfang: $A(0)$ gilt

Induktionsschritt: für alle $n \in \mathbb{N}$ gilt:
wenn $A(n)$ gilt, dann auch $A(n + 1)$

D.h. zeige: für beliebiges $n \in \mathbb{N}$ gilt $A(n + 1)$
unter Verwendung der Induktionshypothese $A(n)$.

Vollständige Induktion

Beispiel (Gauß)

Für alle $n \in \mathbb{N}$ gilt: $\sum_{i=0}^n i = \frac{1}{2}n(n+1)$.

Beweis (durch vollständige Induktion über n).

- ▶ **Induktionsanfang:** $\sum_{i=0}^0 i = 0 = \frac{1}{2}0(0+1)$.
- ▶ **Induktionsschritt:** Wir müssen zeigen, dass $\sum_{i=0}^{n+1} i = \frac{1}{2}(n+1)(n+2)$, unter Verwendung der Induktionshypothese $\sum_{i=0}^n i = \frac{1}{2}n(n+1)$.

$$\begin{aligned}\sum_{i=0}^{n+1} i &= \sum_{i=0}^n i + (n+1) \\ &= \frac{1}{2}n(n+1) + (n+1) \quad (\text{durch die Induktionshypothese}) \\ &= \left(\frac{1}{2}n + 1\right)(n+1) \\ &= \frac{1}{2}(n+2)(n+1) \\ &= \frac{1}{2}(n+1)(n+2).\end{aligned}$$



Starke Induktion

Um zu zeigen, dass $A(n)$ für alle $n \in \mathbb{N}$ gilt, zeige

Induktionsschritt: für alle $n \in \mathbb{N}$ gilt:
wenn $A(k)$ für alle $k < n$ gilt, dann auch $A(n)$

D.h. zeige: für beliebiges $n \in \mathbb{N}$ gilt $A(n)$
unter Verwendung der Induktionshypothese $A(k)$ für alle $k < n$.

Starke Induktion

Beispiel

Für alle $n \in \mathbb{N} \setminus \{0\}$ gilt: n ist Produkt von Primzahlen.

Beweis (durch starke Induktion über n).

▶ **Induktionsschritt:**

▶ **Fall 1:** $n = 0$.

Unmöglich, da $0 \notin \mathbb{N} \setminus \{0\}$.

▶ **Fall 2:** $n = 1$.

Das leere Produkt ergibt 1.

▶ **Fall 3:** $n \geq 2$.

Falls n eine Primzahl ist, ist n ein Produkt von Primzahlen.

Sonst gibt es $k, m \in \mathbb{N}$ mit $2 \leq k, m < n$ mit $n = km$.

Durch die Induktionshypothese sind $k = p_1 \cdots p_r$ und $m = q_1 \cdots q_s$.

Damit ist $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$ ein Produkt von Primzahlen.



Starke Induktion

Beispiel

Seien n Mannschaften M_1, \dots, M_n .

Nehmen wir an, dass jede Mannschaft einmal gegen jede andere Mannschaft gespielt hat.

Es gibt eine Anordnung M_{i_1}, \dots, M_{i_n} , sodass: M_{i_j} hat gegen $M_{i_{j+1}}$ verloren für alle $j \in \{1, \dots, n-1\}$.

Beweis (durch starke Induktion über n).

▶ Induktionsschritt:

▶ **Fall 1:** $n = 0$. Trivial.

▶ **Fall 2:** $n \geq 1$.

Seien $V = \{M_i \mid M_i \text{ hat gegen } M_n \text{ verloren}\}$ und $S = \{M_i \mid M_i \text{ hat gegen } M_n \text{ gewonnen}\}$.

Da $|V| < n$ und $|S| < n$, können wir sie rekursiv sortieren:

$M_{i_1}, \dots, M_{i_{|V|}}$ bzw. $M_{j_1}, \dots, M_{j_{|S|}}$.

Die Anordnung $M_{i_1}, \dots, M_{i_{|V|}}, M_n, M_{j_1}, \dots, M_{j_{|S|}}$ hat die gewünschte Eigenschaft. □