Brückenkurs Mathematik für Studienanfänger:innen der Informatik und Mathematik

Beweise

Jonas Cleve, Freie Universität Berlin

03. – 14. April 2023

Beweise – Voraussetzungen & Begriffe

Was setzen wir als bekannt voraus?

- $\mathbb{N}$ sind die natürlichen Zahlen mit 0, $\mathbb{N}^+$ ohne 0
- Addition und Multiplikation auf natürlichen Zahlen

  Assoziativität: $(a + b) + c = a + (b + c)$
  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

  Kommutativität: $a + b = b + a$
  $a \cdot b = b \cdot a$

  Distributivität: $a \cdot (b + c) = a \cdot b + a \cdot c$

- $n \in \mathbb{N}$ ist durch $d \in \mathbb{N}^+$ teilbar („d teilt n“ oder $d|n$), wenn es ein $k \in \mathbb{N}$ mit $n = k \cdot d$ gibt.

  $d|n \equiv \exists k \in \mathbb{N} : n = k \cdot d \equiv D(n, d)$ ← Ein Prädikat

- $p > 1$ ist Primzahl, wenn sie nur Teiler 1 und p hat
- Jede Zahl $n \in \mathbb{N}$ mit $n > 1$ lässt sich als eindeutiges Produkt von Primzahlen (Primfaktoren) schreiben

  $84 = 2 \cdot 2 \cdot 3 \cdot 7$ $81 = 3 \cdot 3 \cdot 3 \cdot 3$ $97 = 97$

Arten von (beweisbaren) Aussagen:

Satz (eng. *Theorem*)

wichtige Hauptaussage

Lemma (eng. *Lemma*)

wichtiger Schlüsselgedanke / Hilfssatz

Korollar/Folgerung (eng. *Corollary*)

Folgerung aus Satz/Lemma, oft einfach genug, dass kein Beweis nötig ist

Beobachtung (eng. *Observation*)

Wahre Aussage, keine Beweis „benötigt“

Vermutung (eng. *Conjecture*)

Aussage, deren Wahrheitswert (noch) unbekannt ist (z.B. Goldbachsche Vermutung)

Beweise – Voraussetzungen & Begriffe

Was setzen wir als bekannt voraus?

- $\mathbb{N}$ sind die natürlichen Zahlen mit 0, $\mathbb{N}^+$ ohne 0
- Addition und Multiplikation auf natürlichen Zahlen

  Assoziativität: $(a + b) + c = a + (b + c)$
  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

  Kommutativität: $a + b = b + a$
  $a \cdot b = b \cdot a$

  Distributivität: $a \cdot (b + c) = a \cdot b + a \cdot c$

- $n \in \mathbb{N}$ ist durch $d \in \mathbb{N}^+$ teilbar („d teilt n“ oder $d|n$), wenn es ein $k \in \mathbb{N}$ mit $n = k \cdot d$ gibt.

  $d|n \equiv \exists k \in \mathbb{N} : n = k \cdot d \equiv D(n, d)$ ← Ein Prädikat

- $p > 1$ ist Primzahl, wenn sie nur Teiler 1 und p hat
- Jede Zahl $n \in \mathbb{N}$ mit $n > 1$ lässt sich als eindeutiges Produkt von Primzahlen (Primfaktoren) schreiben

  $84 = 2 \cdot 2 \cdot 3 \cdot 7$ $81 = 3 \cdot 3 \cdot 3 \cdot 3$ $97 = 97$

Buchempfehlung:

Beutelspacher, Albrecht
„Das ist o. B. d. A. trivial!“: Tipps und Tricks zur Formulierung mathematischer Gedanken
Vieweg + Teubner, 2009
kostenlos aus dem Uni-Netz

wichtiger Schlüsselgedanke / Hilfssatz

Korollar/Folgerung (eng. *Corollary*)

Folgerung aus Satz/Lemma, oft einfach genug, dass kein Beweis nötig ist

Beobachtung (eng. *Observation*)

Wahre Aussage, keine Beweis „benötigt“

Vermutung (eng. *Conjecture*)

Aussage, deren Wahrheitswert (noch) unbekannt ist (z.B. Goldbachsche Vermutung)

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.

Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1$, $r_1 \to r_2$, ..., $r_k \to t$

Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.

Grund: $(s \to r) \wedge (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

s	r	t	$s \to r$	$r \to t$	$(s \to r) \wedge (r \to t)$	$s \to t$	$(s \to r) \wedge (r \to t) \to (s \to t)$
0	0	0	1	1	1	1	1
0	0	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	0	1
1	0	1	0	1	0	1	1
1	1	0	1	0	0	0	1
1	1	1	1	1	1	1	1

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.

Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1$, $r_1 \to r_2$, ..., $r_k \to t$

Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.

Grund: $(s \to r) \wedge (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

Beispiel: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Ist m teilbar durch l und n teilbar durch m, dann ist auch n teilbar durch l. Also: $\forall l, m, n \in \mathbb{N}^+ : l|m \wedge m|n \to l|n$.

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.
Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1$, $r_1 \to r_2$, ..., $r_k \to t$
Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.
Grund: $(s \to r) \land (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

Beispiel: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Ist m teilbar durch l und n teilbar durch m, dann ist auch n teilbar durch l. Also: $\forall l, m, n \in \mathbb{N}^+ : l|m \land m|n \to l|n$.

Beweis: Seien $l, m, n \in \mathbb{N}^+$ gegeben.

Prämisse → Definition Teilbarkeit

$l|m \land m|n \equiv (\exists j \in \mathbb{N} : m = j \cdot l) \land (\exists k \in \mathbb{N} : n = k \cdot m)$

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.
Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1$, $r_1 \to r_2$, ..., $r_k \to t$
Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.
Grund: $(s \to r) \wedge (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

Beispiel: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Ist m teilbar durch l und n teilbar durch m, dann ist auch n teilbar durch l. Also: $\forall l, m, n \in \mathbb{N}^+ : l|m \wedge m|n \to l|n$.

Beweis: Seien $l, m, n \in \mathbb{N}^+$ gegeben.

Prämisse → Definition Teilbarkeit → Quantoren nach vorne ziehen

$l|m \wedge m|n$
$\equiv (\exists j \in \mathbb{N} : m = j \cdot l) \wedge (\exists k \in \mathbb{N} : n = k \cdot m)$
$\equiv \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : m = j \cdot l \wedge n = k \cdot m$

Einsetzen von $m = j \cdot l$

$\to \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : n = k \cdot (j \cdot l)$

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.
Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1$, $r_1 \to r_2$, ..., $r_k \to t$
Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.
Grund: $(s \to r) \wedge (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

Beispiel: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Ist m teilbar durch l und n teilbar durch m, dann ist auch n teilbar durch l. Also: $\forall l, m, n \in \mathbb{N}^+ : l|m \wedge m|n \to l|n$.

Beweis: Seien $l, m, n \in \mathbb{N}^+$ gegeben.

Prämisse	Definition Teilbarkeit	Quantoren nach vorne ziehen
$l\|m \wedge m\|n$	$\equiv (\exists j \in \mathbb{N} : m = j \cdot l) \wedge (\exists k \in \mathbb{N} : n = k \cdot m)$	$\equiv \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : m = j \cdot l \wedge n = k \cdot m$

Einsetzen von $m = j \cdot l$	Assoziativgesetz
$\to \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : n = k \cdot (j \cdot l)$	$\equiv \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : n = (k \cdot j) \cdot l$

Ersetze $k \cdot j$ durch k'	Definition Teilbarkeit
$\to \exists k' \in \mathbb{N} : n = k' \cdot l$	$\equiv l\|n$

Beweise – Direkte Beweise

Zu beweisende Aussagen haben (in der Regel) die Form „wenn s dann t“, also $s \to t$.
Wir können $s \to t$ in viele kleine Implikationen zerlegen: $s \to r_1, r_1 \to r_2, \ldots, r_k \to t$
Sind alle Implikationen `wahre` Aussagen, ist auch $s \to t$ `wahr`.
Grund: $(s \to r) \wedge (r \to t) \to (s \to t) \equiv 1$, ist also eine Tautologie.

Beispiel: Für beliebige $l, m, n \in \mathbb{N}^+$ gilt: Ist m teilbar durch l und n teilbar durch m, dann ist auch n teilbar durch l. Also: $\forall l, m, n \in \mathbb{N}^+ : l|m \wedge m|n \to l|n$.

Beweis: Seien $l, m, n \in \mathbb{N}^+$ gegeben.

Prämisse → Definition Teilbarkeit → Quantoren nach vorne ziehen

$l|m \wedge m|n \equiv (\exists j \in \mathbb{N} : m = j \cdot l) \wedge (\exists k \in \mathbb{N} : n = k \cdot m) \equiv \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : m = j \cdot l \wedge n = k \cdot m$

Einsetzen von $m = j \cdot l$ → Assoziativgesetz

$\to \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : n = k \cdot (j \cdot l) \equiv \exists j \in \mathbb{N} : \exists k \in \mathbb{N} : n = (k \cdot j) \cdot l$

Ersetze $k \cdot j$ durch k' → Definition Teilbarkeit

$\to \exists k' \in \mathbb{N} : n = k' \cdot l \equiv l|n$

□

Beweise – Indirekte Beweise

Statt (über Zwischenschritte) $s \to t$, beweisen wir eine der logisch äquivalenten Aussagen:

- *Kontraposition:* $\neg t \to \neg s$
- *Widerspruch:* $(s \wedge \neg t) \to 0$

s	t	$s \to t$	$\neg t$	$\neg s$	$\neg t \to \neg s$	$s \wedge \neg t$	$(s \wedge \neg t) \to 0$
0	0	1	1	1	1	0	1
0	1	1	0	1	1	0	1
1	0	0	1	0	0	1	0
1	1	1	0	0	1	0	1

Beweise – Indirekte Beweise

Statt (über Zwischenschritte) $s \to t$, beweisen wir eine der logisch äquivalenten Aussagen:

– *Kontraposition:* $\neg t \to \neg s$

– *Widerspruch:* $(s \wedge \neg t) \to 0$

Beispiel: Für jede natürliche Zahl n gilt: Ist n^2 ungerade, so ist auch n ungerade.

$$\forall n \in \mathbb{N} : \boxed{n^2 \text{ ungerade} \to n \text{ ungerade}}$$

logisch äquivalente Aussagen

Beweis durch Kontraposition:

$$\forall n \in \mathbb{N} : \boxed{n \text{ gerade} \to n^2 \text{ gerade}}$$

Dafür jetzt ein direkter Beweis:

Sei ein beliebiges $n \in \mathbb{N}$ gegeben.

Prämisse
n gerade

Definition „gerade“
$\equiv \exists k \in \mathbb{N} : n = 2 \cdot k$

Quadrieren
$\to \exists k \in \mathbb{N} : n^2 = (2 \cdot k)^2 = 4k^2 = 2 \cdot 2k^2$

Neuer Platzhalter k' für $2k^2$
$\to \exists k' \in \mathbb{N} : n^2 = 2 \cdot k'$

Definition „gerade“
$\equiv n^2$ gerade

□

Beweise – Indirekte Beweise

Statt (über Zwischenschritte) $s \to t$, beweisen wir eine der logisch äquivalenten Aussagen:

– *Kontraposition:* $\neg t \to \neg s$

– *Widerspruch:* $(s \wedge \neg t) \to 0$

Beispiel: Seien m und n natürliche Zahlen, $m \geq n$, sodass $3|m+n$ und $3|m-n$ gilt.
Dann ist m durch 3 teilbar.

$$\forall m, n \in \mathbb{N}: \underbrace{m \geq n \ \wedge \ 3|m+n \ \wedge \ 3|m-n}_{s} \quad \to \quad \underbrace{3|m}_{t}$$

Beweis durch Widerspruch:

Seien beliebige $m, n \in \mathbb{N}$ gegeben.

Nehmen an, dass $\underbrace{m \geq n, 3|m+n \text{ und } 3|m-n}_{s}$ gilt, sowie, dass $\underbrace{m \text{ **nicht** durch 3 teilbar ist.}}_{\neg t}$

$\to$ $\exists k, k' \in \mathbb{N}$, sodass $m+n = 3k$ und $m-n = 3k'$ **und** es gibt **kein** $k'' \in \mathbb{N}$, sodass $m = 3k''$

Sei $x = 2m$

$x = 2m = m + m + n - n = (m+n) + (m-n)$

$x = 3k + 3k' = 3(k+k')$

$\to x$ ist durch 3 teilbar

Primfaktoren: $m = p_1 \cdot p_2 \cdot \ldots \cdot p_l$ und alle $p_i \neq 3$

Primfaktoren: $x = 2 \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_l$ und alle $p_i \neq 3$

$\to x$ ist nicht durch 3 teilbar

x ist durch 3 teilbar und x ist nicht durch 3 teilbar $\equiv 0$ ↯ Hier ist der Widerspruch $\square$

Beweise – Beweis durch Fallunterscheidung

Um $s \to t$ zu beweisen, betrachten wir verschiedene Fälle für s.

$$s \to t \equiv ((s \wedge r) \to t) \wedge ((s \wedge \neg r) \to t)$$

Beispiel: Ist $n \in \mathbb{N}$ ungerade, so ist $n^2 - 1$ durch 8 teilbar.

$\forall n \in \mathbb{N} : n$ ungerade $\to 8 | (n^2 - 1)$

Beweis: Gegeben ein ungerades $n \in \mathbb{N}$.

Beobachtungen:
- Wissen, dass $n^2 - 1 = (n-1)(n+1)$
- Sowohl $(n-1)$ als auch $(n+1)$ sind gerade, also durch 2 teilbar
- Also ist $n^2 - 1$ durch 4 teilbar
- Ist $(n-1)$ oder $(n+1)$ durch 4 teilbar, dann ist $n^2 - 1$ durch 8 teilbar

Fall 1: $(n-1)$ ist durch 4 teilbar

$\to n - 1 = 4k$ (für ein $k \in \mathbb{N}$)

$\to n + 1 = 4k + 2 = 2(2k + 1)$

$\to n^2 - 1 = 4k \cdot 2(2k + 1) = 8 \cdot k(2k + 1)$

$\to n^2 - 1$ ist durch 8 teilbar

Fall 2: $(n-1)$ ist nicht durch 4 teilbar

$\to n - 1 = 2(2m + 1) = 4m + 2$ (für ein $m \in \mathbb{N}$)

$\to n + 1 = 2(2m + 1) + 2 = 4m + 4 = 4(m + 1)$

$\to n^2 - 1 = 2(2m + 1) \cdot 4(m + 1) = 8 \cdot (2m + 1)(m + 1)$

$\to n^2 - 1$ ist durch 8 teilbar $\square$

Beweise – Exkurs Summen

Für beliebiges $n \in \mathbb{N}$ wollen wir alle natürlichen Zahlen von 0 bis n aufsummieren.

$$0 + 1 + 2 + \ldots + (n-1) + n = ?$$

Können wir das nicht schöner / kompakter / eindeutiger aufschreiben?

$$0 + 1 + 2 + \ldots + (n-1) + n = \sum_{i=0}^{n} i$$

- n: Endwert (inklusive)
- i: Was soll aufsummiert werden?
- $\sum$: Sigma („griechisches S“)
- $i=0$: Platzhalter und Startwert

Weitere Beispiele:

$$\sum_{i=1}^{k} i^2 = 1^2 + 2^2 + \ldots + (k-1)^2 + k^2 \qquad \sum_{i=5}^{7} (i-2) = (5-2) + (6-2) + (7-2) = 3 + 4 + 5 = 12$$

Wichtige Eigenschaft: Summen können wir beliebig aufteilen (Addition ist assoziativ)!

$$1 + 2 + \ldots + n = (1 + 2) + (3 + \ldots + n) = (1 + \ldots + (n-1)) + n = (1 + \ldots + k) + ((k+1) + \ldots + n)$$

$$\sum_{i=1}^{n} i \qquad = 1 + 2 + \sum_{i=3}^{n} i \qquad = \left(\sum_{i=1}^{n-1} i \right) + n \qquad = \left(\sum_{i=1}^{k} i \right) + \left(\sum_{i=k+1}^{n} i \right)$$

Beweise – Induktion I

Wir wollen im Folgenden zeigen, dass $\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$ gilt, auch als Gaußsche Summenformel bekannt.

Wir wollen dies mit dem Prinzip der *vollständigen Induktion* beweisen.

Zuerst wollen wir uns eine Analogie des Prinzips anschauen.

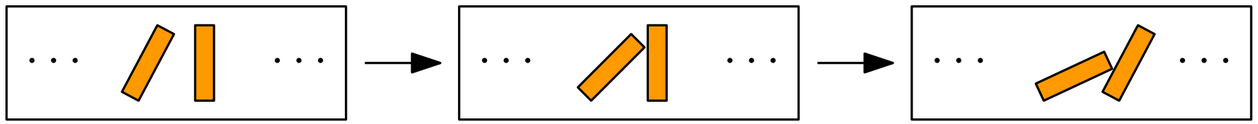
Beweise – Induktion II

Freie Universität Berlin

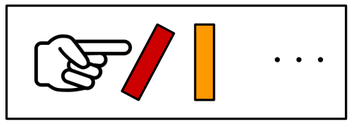
Angenommen, wir haben unendlich viele Dominosteine, perfekt aufgestellt:

Was wissen wir über die Steine?

1. Wenn ein Stein umgestoßen wird, dann stößt er den nächsten Stein um



2. Wir können den Startstein umstoßen (und tun dies auch)



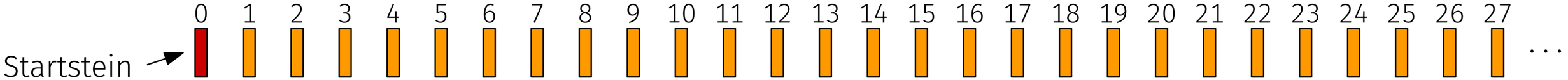
Aus 1. und 2. folgt: *Jeder* Stein fällt um!

– Es gibt einen eindeutigen Startstein
– Jeder Stein hat *einen eindeutigen* Nachfolger-Stein (rechts von ihm)
– Jeder Stein (außer der Startstein) hat *einen eindeutigen* Vorgänger-Stein (links von ihm)

Beweise – Induktion II

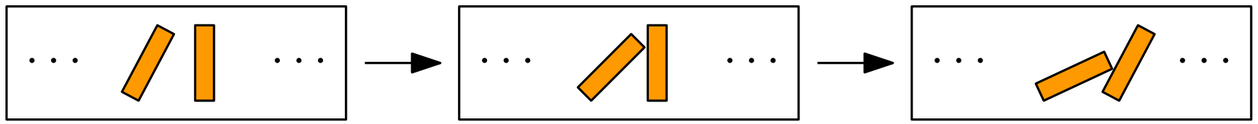
Freie Universität Berlin

Angenommen, wir haben unendlich viele Dominosteine, perfekt aufgestellt:

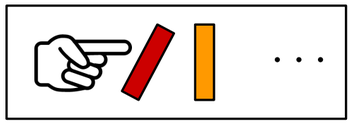


Was wissen wir über die Steine?

1. Wenn ein Stein umgestoßen wird, dann stößt er den nächsten Stein um



2. Wir können den Startstein umstoßen (und tun dies auch)



Aus 1. und 2. folgt: *Jeder* Stein fällt um!

- Es gibt einen eindeutigen Startstein
- Jeder Stein hat *einen eindeutigen* Nachfolger-Stein (rechts von ihm)
- Jeder Stein (außer der Startstein) hat *einen eindeutigen* Vorgänger-Stein (links von ihm)

Steine entsprechen den natürlichen Zahlen

Beweise – Induktion III

Was hat das mit Beweisen zu tun?

Wollen zeigen: $\forall n \in \mathbb{N} : P(n)$ (für alle natürlichen Zahlen gilt ein Prädikat P)

	Formell	Sprachlich	Dominos
Aussage	**Induktionsbehauptung (I.B.):** $\forall n \in \mathbb{N} : P(n)$	P gilt für alle natürlichen Zahlen	alle Steine fallen um
Beweis	**Induktionsanfang (I.A.):** $P(0)$	P gilt für die natürliche Zahl 0	 können Startstein umstoßen
Beweis	**Induktionsschritt (I.S.):** $P(k) \rightarrow P(k+1)$	wenn P für eine natürliche Zahl k gilt, dann gilt P auch für $k+1$	 ein fallender Stein k stößt den nächsten Stein $k+1$ um
	Induktionsvoraussetzung (I.V.): $\exists k \in \mathbb{N} : P(k)$	für irgendeine natürliche Zahl gilt P	 irgendein Stein fällt um

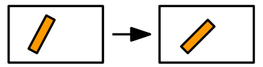
$P(0)$ gilt, dann gilt aber auch $P(1)$, dann gilt aber auch $P(2)$, dann gilt aber auch $P(3)$, ...

Beweise – Induktion IV

Induktionsbehauptung (I.B.): $\forall n \in \mathbb{N} : \sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

Induktionsanfang (I.A.): 

$$\sum_{i=0}^{0} i = 0 = \frac{0}{2} = \frac{0(0+1)}{2}$$ ✓

Induktionsvoraussetzung (I.V.): 

Nehmen an, dass $\sum_{i=0}^{k} i = \frac{k(k+1)}{2}$ für ein beliebiges $k \in \mathbb{N}$ gilt

Induktionsschritt (I.S.): 

Wir zeigen, dass aus der Induktionsvoraussetzung auch folgt, das die Aussage für $k+1$ gilt

$$\sum_{i=0}^{k+1} i = \left(\sum_{i=0}^{k} i\right) + (k+1) = \left(\frac{k(k+1)}{2}\right) + (k+1) = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} = \frac{k(k+1)+2(k+1)}{2}$$

Summe aufteilen — I.V. einsetzen — Bruch mit 2 erweitern — Auf einen Bruch bringen

$$= \frac{(k+2)(k+1)}{2} = \frac{(k+1)((k+1)+1)}{2}$$ ✓ (entspricht für $n = k+1$ der Behauptung)

Distributivgesetz — Umstellen

□