3 Vom Zählen zur Induktion

3.1 Natürliche Zahlen und Induktions-Prinzip

Seit unserer Kindheit kennen wir die Zahlen 1, 2, 3, 4, usw. Diese Zahlen gebrauchen wir zum Zählen, und sie sind uns so vertraut, dass wir sie die „natürlichen Zahlen“ nennen. Man kann gar nicht über Logik, Mengenlehre oder Mathematik sprechen, ohne natürliche Zahlen zu verwenden. Als spezielle Dezimalbrüche sind die natürlichen Zahlen aber auch reelle Zahlen und damit Bestandteile unseres axiomatisch begründeten Systems von reellen Zahlen. Aber was zeichnet die natürlichen Zahlen in $\mathbb{R}$ aus?

Es ist ihr Bildungsgesetz. Mit der 1 fängt alles an, und die 1 ist auch in $\mathbb{R}$ durch ihre Eigenschaft als multiplikatives neutrales Element ausgezeichnet. Aus ihr gewinnt man sofort weitere natürliche Zahlen: $2 := 1+1$, $3 := 2+1$, $4 := 3+1$, $\ldots$. Und wenn wir irgend eine – auch noch so große – natürliche Zahl n konstruiert oder benannt haben, so erhalten wir aus ihr durch Addition der Eins wieder eine natürliche Zahl, ihren ***Nachfolger*** $n+1$. Da $1 > 0$ ist, ist stets $n+1 > n$. Die natürlichen Zahlen werden demnach größer und größer, und eine größte ist nicht in Sicht.

Die gerade herausgearbeitete Struktur der Menge der natürlichen Zahlen ist so charakteristisch für den Vorgang des Zählens, dass es naheliegt, nach allen Mengen mit dieser Eigenschaft zu suchen:

Definition

Eine Teilmenge $M \subset \mathbb{R}$ heißt ***induktiv***, falls gilt:

- $1 \in M$,
- $\forall x : \big(x \in M \implies (x+1) \in M \big)$.

Jede induktive Menge enthält die Zahlen 1, 2, 3, 4, ..., aber offensichtlich ist auch die Menge $\{x \in \mathbb{R} \mid x > 0\}$ induktiv, und das ist zu viel des Guten. Der Durchschnitt von zwei induktiven Mengen ist wieder induktiv, dabei wird die Menge höchstens kleiner. Suchen wir also nach der „kleinsten“ induktiven Menge! Das muss die Menge der natürlichen Zahlen sein.

Definition

Ein Element $n \in \mathbb{R}$ heißt ***natürliche Zahl***, falls n zu **jeder** induktiven Teilmenge von $\mathbb{R}$ (also zum Durchschnitt aller induktiven Teilmengen) gehört. Mit $\mathbb{N}$ wird die Menge aller natürlichen Zahlen in $\mathbb{R}$ bezeichnet.

Die Menge $\mathbb{N}$ ist natürlich selbst induktiv. Nun lässt sich eine sehr wichtige Folgerung ziehen:

3.1.1 (Induktionsprinzip) *Es sei $M \subset \mathbb{N}$ eine Teilmenge, und es gelte:*

- $1 \in M$.
- $\forall\, n : \big(n \in M \implies (n+1) \in M \big)$.

Dann ist bereits $M = \mathbb{N}$.

BEWEIS: Nach Voraussetzung ist M eine induktive Teilmenge von $\mathbb{N}$. Weil aber $\mathbb{N}$ schon die kleinste induktive Menge ist, muss sogar $M = \mathbb{N}$ gelten. ■

Warum ist das Induktionsprinzip wichtig? Es führt zu einem völlig neuen Beweisverfahren, dem „Beweis durch vollständige Induktion". Man kann dieses Verfahren immer dann benutzen, wenn natürliche Zahlen im Spiel sind:

Sei $A(n)$ eine Aussageform, bei der die natürlichen Zahlen einen zulässigen Objektbereich für die Variable n bilden. Dann kann man versuchen, die Aussage

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

durch vollständige Induktion zu beweisen. Und das geht so:

Sei $M := \{n \in \mathbb{N} \mid A(n)\}$. Dann ist die gewünschte Aussage äquivalent zu der Aussage „ $M = \mathbb{N}$ ". Der Beweis besteht – so er denn möglich ist – aus 2 Teilen.

1) **Induktionsanfang:** Man zeige, dass die Aussage $A(1)$ wahr ist. Das bedeutet, dass $1 \in M$ ist.

2) **Induktionsschluss:** Man beweise, dass für beliebiges $n \in \mathbb{N}$ die folgende Implikation wahr ist:

$$A(n) \quad \implies \quad A(n+1).$$

Beachte: Die **Implikation** muss wahr sein, nicht die Aussage $A(n+1)$! Das bedeutet dann: Wenn n in M liegt, so liegt auch $n+1$ in M. Mit dem Induktionsprinzip folgt daraus, dass $M = \mathbb{N}$ ist.

Wir wollen zunächst ein ganz simples Beispiel betrachten:

Behauptung. $\forall\, n \in \mathbb{N} : (n = 1) \vee (n > 1)$.

BEWEIS:
$\underline{n = 1}$ (Induktionsanfang): Für $n = 1$ ist die Aussage trivial. Das kann immer mal wieder vorkommen, aber umgekehrt kann auch schon mal der Induktionsanfang der schwierigste Teil des Beweises sein.

$\underline{n \to n+1}$ (Induktionsschluss): Für die natürliche Zahl n sei die Behauptung schon bewiesen. Unter dieser Voraussetzung muss nachgewiesen werden, dass die Behauptung auch für $n+1$ gilt. Dabei sind zwei Fälle zu unterscheiden:

1. Fall: $n = 1$. Dann ist $n + 1 = 1 + 1 > 1 + 0 = 1$.

2. Fall: Ist schon $n > 1$, so ist erst recht $n + 1 > n + 0 = n > 1$. ■

Genaugenommen ist ein Induktionsbeweis ein Beweis mit unendlich vielen Schritten. Man zeigt zunächst den Fall $n = 1$. Dann benutzt man diesen schon bewiesenen Fall, um den Fall $n = 2 = 1+1$ zu zeigen. Und dann benutzt man wiederum diesen Fall, um den Fall $n = 3 = 2+1$ zu zeigen. Und so fährt man fort. Unendlich viele Schritte kann man nicht aufschreiben, aber wenn die einzelnen Schritte formal alle gleich sind, dann kann man sie mit variablem n alle auf einen Schlag durchführen.

3.2 Einige Induktionsbeweise

1. Beispiel:

Gerne wird Induktion benutzt, um Summenformeln zu beweisen. Ich zeige das hier am Beispiel der Gauß'schen Summenformel.

3.2.1 Gauß'sche Summenformel: *Für jedes* $n \in \mathbb{N}$ *ist* $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$.

BEWEIS: Sei zunächst $n = 1$. Dann steht auf der linken Seite die Summe $\sum_{k=1}^{1} k = 1$, und rechts ergibt die Formel den Wert $1(1+1)/2 = 1$. Da beides übereinstimmt, ist der Induktionsanfang erledigt.

Jetzt nehmen wir an, die Formel sei für ein $n \geq 1$ schon bewiesen. Dann gilt:

$$\begin{aligned}
\sum_{k=1}^{n+1} k &= \sum_{k=1}^{n} k + (n+1) \\
&= \frac{n(n+1)}{2} + (n+1) \qquad \text{(nach Induktionsvoraussetzung)} \\
&= \frac{n(n+1) + 2(n+1)}{2} \qquad \text{(auf den Hauptnenner gebracht)} \\
&= \frac{(n+1)(n+2)}{2} = \frac{(n+1)\cdot\big((n+1)+1\big)}{2}.
\end{aligned}$$

Also gilt die Formel für $n+1$, und alles ist gezeigt. ∎

Viele Aussagen über natürliche Zahlen, die eigentlich selbstverständlich klingen, müssen erst mal bewiesen werden. Dabei ist das Induktions-Prinzip unverzichtbar. Ein typisches Beispiel ist die Aussage, dass die Summe von natürlichen Zahlen wieder eine natürliche Zahl ist.

3.2.2 Satz *Für alle* $n, m \in \mathbb{N}$ *ist auch* $n + m \in \mathbb{N}$.

BEWEIS: Es sei n beliebig vorgegeben. Dann kann man Induktion nach m führen.

Induktionsanfang ($m = 1$): Weil $\mathbb{N}$ induktiv ist, liegt mit n auch $n+1$ in $\mathbb{N}$.

Induktionsschluss ($m \to m+1$): Es sei $n+m \in \mathbb{N}$ (Induktionsvoraussetzung). Dann ist $n + (m+1) = (n+m) + 1 \in \mathbb{N}$, weil $\mathbb{N}$ induktiv ist. ∎

Ganz interessant ist auch das folgende Ergebnis:

3.2.3 Satz *Es gibt keine Zahl* $n \in \mathbb{N}$ *mit* $1 < n < 2$.

BEWEIS: Sei $M := \{1\} \cup \{x \in \mathbb{R} : x \geq 2\}$. Definitionsgemäß liegt 1 in M. Ist $x \in M$, so ist entweder $x = 1$ und $x + 1 = 2 \in M$, oder es ist $x \geq 2$ und $x + 1 \geq 2 + 1 > 2 + 0 = 2$. Also ist M induktiv und deshalb $\mathbb{N} \subset M$. Damit gilt für jede natürliche Zahl $n \in \mathbb{N}$: $n = 1$ oder $n \geq 2$. ∎

Für jede Zahl $n \in \mathbb{N}$ folgt dann auch, dass es keine natürliche Zahl m mit $n < m < n + 1$ gibt. Und das wiederum bedeutet für beliebige natürliche Zahlen n und m: Ist $m < n + 1$, so ist $m \leq n$.

2. Beispiel:

Die Gauß'sche Summenformel konnte auch ohne Induktion bewiesen werden. Eher sinnvoll ist die Anwendung des Induktionsprinzips bei Ungleichungen.

3.2.4 (Bernoulli'sche Ungleichung)

$$(1 + x)^n > 1 + nx \text{ \textit{für} } x > -1,\ x \neq 0 \text{ \textit{und} } n \geq 2.$$

BEWEIS: Induktion nach n:

Induktionsanfang: Im Falle $n = 2$ ist die Ungleichung $(1 + x)^2 = 1 + 2x + x^2 > 1 + 2x$ offensichtlich erfüllt.

Induktionsschluss: Nach Voraussetzung ist $1 + x > 0$. Ist die Behauptung für n bewiesen, so folgt:

$$\begin{aligned}
(1 + x)^{n+1} &= (1 + x)(1 + x)^n \\
&> (1 + x)(1 + nx) \text{ (nach Induktionsvoraussetzung)} \\
&= 1 + (n + 1)x + nx^2 \ > \ 1 + (n + 1)x.
\end{aligned}$$

∎

3.3 Teilbarkeit und Primzahlen

Wir benötigen in diesem Abschnitt folgendes Ergebnis:

3.3.1 Wohlordnungssatz *Jede nicht-leere Teilmenge M von $\mathbb{N}$ besitzt ein kleinstes Element.*

n_0 ist kleinstes Element von M, falls gilt:

$$n_0 \in M \quad \text{und für alle } n \in M \text{ gilt: } n_0 \leq n.$$

Zum Beispiel ist 5 das kleinste Element der Menge $\{5, 7, {}^{89}/_{7}, 100\}$ und 0 das kleinste Element der Menge $\{m \in \mathbb{Z} \mid m > -{}^{1}/_{3}\}$. Die Menge $M = \{x \in \mathbb{R} \mid x > 0\}$ besitzt dagegen kein kleinstes Element: Wäre nämlich x_0 das kleinste Element von M, so wäre $x_0 > 0$ und auch $y_0 := x_0/2$ ein Element von M. Weil $y_0 < x_0$ ist, kann das nicht sein.

BEWEIS (des Wohlordnungssatzes): Wir würden gerne Induktion benutzen, aber es fehlt eine Variable dafür. Der Trick dieses Beweises besteht darin, dass wir künstlich eine Variable einführen. Wir beweisen nämlich die folgende Aussage $A(n)$:

Jede Teilmenge $M \subset \mathbb{N}$, die die Zahl n enthält, besitzt ein kleinstes Element.

Haben wir die Aussage $A(n)$ durch vollständige Induktion für jedes $n \in \mathbb{N}$ bewiesen, so haben wir auch den Satz bewiesen.

A(1): Ist $1 \in M$, so ist natürlich 1 das kleinste Element.

A(n) $\Longrightarrow$ **A(n+1)**: Es sei $M \subset \mathbb{N}$ eine Teilmenge, die die Zahl $n+1$ enthält. Die Aussage $A(n)$ sei schon bewiesen.

Wir müssen die Aussage $A(n)$ irgendwie benutzen. Da wir nicht wissen, ob n in M liegt, machen wir eine Fallunterscheidung:

a) Ist $n \in M$, so hat M nach Induktionsvoraussetzung ein kleinstes Element, und wir sind fertig.

b) Ist $n \notin M$, müssen wir uns etwas einfallen lassen. Wir basteln uns eine neue Menge, die n enthält: Sei $H := M \cup \{n\}$ unsere „Hilfsmenge". Offensichtlich ist $H \subset \mathbb{N}$ und $n \in H$. Nach Induktionsvoraussetzung besitzt H ein kleinstes Element a, und es muss dann $a \leq n$ sein.

Ist $a < n$, so muss a schon in M liegen und dort erst recht das kleinste Element sein. So bleibt nur noch der Fall zu betrachten, dass $a = n$ ist. Aber dann kommt a in M nicht vor, und es muss $a < m$ für alle $m \in M$ gelten. Also ist $n+1 = a+1 \leq m$ für alle $m \in M$. Das bedeutet, dass $n+1$ das kleinste Element von M ist. ∎

Übrigens besitzt die Menge $\mathbb{N}$ kein größtes Element: Wäre nämlich $a \in \mathbb{N}$ das größte Element von $\mathbb{N}$, so wäre jede natürliche Zahl $n \leq a$. Aber mit a liegt auch $a+1$ in $\mathbb{N}$, und es ist $a+1 > a+0 = a$. Das ist ein Widerspruch!

Anmerkung: Der Beweis des Wohlordnungssatzes wurde nicht in der Vorlesung vorgeführt!

Sind $a, b \in \mathbb{Z}$, $b \neq 0$, so ist normalerweise $q := a \cdot b^{-1}$ keine ganze Zahl. Liegt q jedoch in $\mathbb{Z}$, so ist $a = q \cdot b$ ein ganzzahliges Vielfaches von b. Diese Situation ist so wichtig, dass man dafür eine neue Bezeichnung eingeführt hat:

Definition

Seien $a, b \in \mathbb{Z}$, $b \neq 0$. b heißt ***Teiler*** von a, falls es eine ganze Zahl q gibt, so dass $a = q \cdot b$ ist.

Man schreibt dann: $b \mid a$ (in Worten „b teilt a").

Beispiele.

1. $3 \mid 12, \quad (-7) \mid 49, \quad (-5) \mid (-20)$.
2. $b \mid 0$ gilt für jede ganze Zahl b.
3. $1 \mid a$ gilt für jede ganze Zahl a.

Ist b **kein** Teiler von a, so schreibt man: $b \nmid a$.

3.3.2 (Teilbarkeitsregeln) *Für $a, b, c, d \in \mathbb{Z}$ gelten folgende Aussagen:*

1. $a \mid b \implies a \mid bc$,
2. $(a \mid b) \wedge (b \mid c) \implies a \mid c$,
3. $(a \mid b) \wedge (a \mid c) \implies a \mid (b + c)$.

BEWEIS: 1) $b = q \cdot a \implies bc = (qc) \cdot a$.

2) $(b = q \cdot a) \wedge (c = p \cdot b) \implies c = (pq) \cdot a$.

3) $(b = q \cdot a) \wedge (c = r \cdot a) \implies b + c = (q + r) \cdot a$. ∎

Definition

Sei $a \in \mathbb{Z}$. Dann heißen die Zahlen 1, -1, a und $-a$ die ***trivialen Teiler*** von a. Alle anderen Teiler von a nennt man ***echte Teiler*** von a. Eine natürliche Zahl $p > 1$ heißt ***Primzahl***, falls sie keine echten Teiler besitzt.

In der Schule wird oft die Frage gestellt, warum 1 keine Primzahl sei. Aus Gründen, die erst in der höheren Algebra verständlich werden, definiert man das einfach so!

Jede natürliche Zahl ist Summe von endlich vielen Einsen. Multiplikativ gesehen bilden jedoch die Primzahlen die elementaren Bausteine der natürlichen Zahlen. Das wollen wir in den nächsten Sätzen vertiefen:

3.3.3 Satz (Existenz eines Primteilers): *Jede natürliche Zahl $a > 1$ besitzt mindestens einen Primteiler (also eine Primzahl p mit $p \mid a$), und zwar ist der kleinste Teiler $p > 1$ von a eine Primzahl.*

BEWEIS: Sei $M := \{n \in \mathbb{N} \mid (n > 1) \wedge (n \mid a)\}$. Da a selbst in M liegt, ist M nicht leer. Also gibt es in M ein kleinstes Element p. Nach Konstruktion ist $p > 1$. Hätte p einen echten Teiler, so wäre dieser auch ein Teiler von a. Das kann aber nicht sein, also ist p eine Primzahl. ∎

Gesetzmäßigkeiten zur Verteilung der Primzahlen zu finden, gehört zu den schwersten Problemen in der Mathematik. Ob die Folge der Primzahlen eventuell sogar ganz abbricht, beantwortete Euklid schon um 300 v.Chr.:

3.3.4 Satz von Euklid: *Es gibt unendlich viele Primzahlen.*

BEWEIS: Wir nehmen an, es gibt nur endlich viele Primzahlen, etwa $p_1, p_2, \ldots, p_n$, und bilden die Zahl $P := p_1 \cdot p_2 \cdot \ldots \cdot p_n$. Dann besitzt die Zahl $P + 1$ einen kleinsten Primteiler q, der natürlich unter den Zahlen $p_1, \ldots, p_n$ vorkommen muss, also auch ein Teiler von P ist. Wenn jedoch q ein Teiler von P und von $P + 1$ ist, dann muss q auch Teiler von 1 sein. Das ist unmöglich! ∎

Tatsächlich hat Euklid niemals den Begriff „unendlich“ benutzt. Er sagte vielmehr: „Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen“.

Geht eine Division von ganzen Zahlen nicht auf, so braucht man folgendes Ergebnis:

3.3.5 Satz (von der Division mit Rest) *Seien $a, b \in \mathbb{N}$, $1 \leq b \leq a$. Dann gibt es eindeutig bestimmte Zahlen $q, r \in \mathbb{N}_0$, so dass gilt:*

1. $a = q \cdot b + r$.
2. $0 \leq r < b$.

BEWEIS: Das Verfahren ist ganz simpel. b wird so oft von a subtrahiert, bis nur noch ein Rest $r < b$ übrig bleibt:

$$\begin{aligned} \text{Sei } S &:= \{a,\ a-b,\ a-2b,\ \ldots\} \cap \mathbb{N}_0 \\ &= \{n \in \mathbb{N}_0 \,:\, \exists\, x \in \mathbb{N}_0 \text{ mit } n = a - x \cdot b\}. \end{aligned}$$

Da $a = a - 0 \cdot b$ in S liegt, ist $S \neq \varnothing$. Als Teilmenge von $\mathbb{N}_0$ besitzt S ein kleinstes Element r. Dieses hat dann auch die Gestalt $r = a - q \cdot b$.

Wir müssen nur noch nachprüfen, ob alle Eigenschaften erfüllt sind.

Nach Konstruktion ist $r \geq 0$. Wäre $r \geq b$, so wäre auch noch $r - b = a - (q+1) \cdot b \in S$, im Widerspruch zur Minimalität von r. Das bedeutet, dass $r < b$ ist.

Der Beweis der Eindeutigkeit konnte aus Zeitgründen nicht in der Vorlesung erbracht werden, das soll hier nachgeholt werden:

Es gebe Zahlen $q_1, q_2 \in \mathbb{N}_0$ und $r_1, r_2 \in \mathbb{N}_0$, so dass $a = q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ ist, mit $0 \leq r_1 < b$ und $0 \leq r_2 < b$. Dann ist $(q_1 - q_2) \cdot b = r_2 - r_1$. Ist $r_1 = r_2$, so ist die rechte Seite der Gleichung $= 0$, und es muss auch $q_1 = q_2$ sein. Dann ist man fertig. Ist $r_1 \neq r_2$, so muss eine der beiden Zahlen größer sein. O.B.d.A.[1] sei $r_2 > r_1$. Dann ist die rechte Seite der Gleichung $(q_1 - q_2) \cdot b = r_2 - r_1$ positiv, und $q_1 - q_2$ muss ebenfalls > 0 sein.

Da $r_2 < b$ und $0 \leq r_1 < r_2$ ist, ist $0 < r_2 - r_1 < b$ und damit $b \cdot (q_1 - q_2) < b$. Das geht nur, wenn $q_1 - q_2 < 1$ ist, aber für eine positive ganze Zahl ist das nicht möglich. ∎

Ist zum Beispiel $a = 57$ und $b = 9$, so ist

$$S = \{57,\ 57 - 9,\ 57 - 2 \cdot 9,\ \ldots,\ 57 - 6 \cdot 9\}$$

und $3 = 57 - 6 \cdot 9$ das kleinste Element von S, slso $57 = 6 \cdot 9 + 3$ die gesuchte Division mit Rest.

[1] „Ohne Beschränkung der Allgemeinheit“ sagt man, wenn man eine Zusatzannahme macht, welche die Allgemeingültigkeit des Beweises nicht beeinträchtigt, wohl aber die Schreibarbeit verkürzt.