Math Cheat Sheet

Natürliche Zahlen $\mathbb{N}$

Peano-Axiome

1. Die 0 ist eine natürliche Zahl: $0 \in \mathbb{N}$
2. Der Nachfolger einer natürliche Zahl n sei $\sigma(n)$: $n \in \mathbb{N} \Rightarrow \sigma(n) \in \mathbb{N}$
3. Die 0 ist kein Nachfolger: $\forall n \in \mathbb{N}\colon \sigma(n) \neq 0$
4. Zwei verschiedene Zahlen haben verschiedene Nachfolger: $\forall n, m \in \mathbb{N} : (n \neq m) \Rightarrow (\sigma(n) \neq \sigma(m))$
5. Für jede Teilmenge M von $\mathbb{N}$ gilt, wenn M die folgenden Eigenschaften erfüllt:
   a) 0 ist in M
   b) Für jedes n in M ist auch $\sigma(n)$ in M

   dass $M = \mathbb{N}$. Formal:
   $0 \in M \land \forall n \in \mathbb{N}\colon (n \in M \Rightarrow \sigma(n) \in M) \Rightarrow M \subseteq \mathbb{N}$
   (Schliesst parallele Strukturen aus.) Induktionsprinzip.

Addition

Die Addition ist rekursiv definiert:

1. Eine Zahl + 0 ist wieder die Zahl selbst. $n + 0 = n$
2. Wird zu einer Zahl, der Nachfolger einer anderen Zahl addiert, ist das so, wie wenn erst die beiden Zahlen addiert werden und dann der Nachfolger gebildet wird: $m + \sigma(n) = \sigma(m + n)$

Vollständige Induktion

$$(E(0) \land \forall n \in \mathbb{N}(E(n) \Rightarrow E(n+1))) \Leftrightarrow \forall n \in \mathbb{N}(E(n))$$

Man zeigt etwas für die 0, anschliessend nimmt man an, dass wenn es für eine natürliche Zahl gilt, dann auch für deren Nachfolger. Gilt es für 0 und alle Nachfolger, gilt es für alle.
Zu zeigen: $\forall n \in \mathbb{N}\colon n + 0 = n$
Problem: bisherige Theoreme lassen sich nicht anwenden.

Beweis: Vollständige Induktion über n.

$$\begin{aligned} n &= 0 && \text{(Induktionsanfang)} \\ 0 + 0 &= 0 && \text{(Addition 1: Für die 0 bewiesen)} \end{aligned}$$

Induktionschritt: Wir schliessen von $n = k$ auf $n = \sigma(k)$

$$\begin{aligned} k + 0 &= k && \text{Induktionsannahme; für } k \text{ gilt es bereits} \\ \sigma(k) + 0 &= \sigma(k) && \text{(Neu zu zeigen: gilt für Nachfolger)} \\ \sigma(k) + 0 &= \sigma(k + 0) && \text{(Addition 2)} \\ &= \sigma(k) && \text{(Induktionsannahme: für } \sigma(k) \text{ bewiesen)} \end{aligned}$$

□

Der Trick ist, die Induktionsannahme im Beweis zu verwenden. Es wird nur angenommen, dass die Formel für eine Zahl gilt. Bewiesen wird dann, wenn die Formel für eine Zahl gilt, gilt sie auch für alle anderen.

Direkter Beweis

Zu zeigen: $\forall n \in \mathbb{N}\colon n + 1 = \sigma(n)$

Beweis. Sei n fest, aber beliebig

$$\begin{aligned} n + 1 &= n + \sigma(0) && \text{Definition der 1} \\ &= \sigma(n + 0) && \text{Addition 2} \\ &= \sigma(n) && \text{Addition 1} \end{aligned}$$

□

Summen

$$\sum_{i=1}^{0} a_i = 0$$

$$\sum_{i=1}^{n+1} a_i = \left(\sum_{i=1}^{n} a_i\right) + a_{n+1}$$

Die Gaussche Summenformel

$$1 + 2 + \cdots + n = \Sigma_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$$

Zu zeigen: $\forall n \in \mathbb{N} \backslash \{0\}\colon \Sigma_{i=1}^{n} i = \frac{n \cdot (n+1)}{2}$

Beweis. Induktion über n

$$\begin{aligned} n &= 1 && \text{(Induktionsanfang)} \\ \Sigma_{i=1}^{1} i = 1 &= \frac{2}{2} = \frac{1 \cdot 2}{2} = \frac{1 \cdot (1+1)}{2} && \text{Beweis für 1} \end{aligned}$$

Induktionsschritt: Wir schliessen von $n = k$ auf $n = k + 1$

$$\begin{aligned} \Sigma_{i=1}^{k} i &= \frac{k \cdot (k+1)}{2} && \text{Induktionsannahme} \\ \Sigma_{i=1}^{k+1} i &= \frac{(k+1) \cdot ((k+1)+1)}{2} && \text{Neu zu zeigen} \\ \Sigma_{i=1}^{k+1} i &= \Sigma_{i=1}^{k} i + (k+1) && \text{Summe um einen Term verkürzt} \\ &= \frac{k \cdot (k+1)}{2} + (k+1) && \text{Induktionsannahme} \\ &= \frac{k \cdot (k+1)}{2} + \frac{2 \cdot (k+1)}{2} && \text{Rechts um zwei erweitert} \\ &= \frac{k \cdot (k+1) + 2 \cdot (k+1)}{2} && \text{Zusammenzug} \\ &= \frac{(k+1) \cdot (k+2)}{2} && k + 1\text{ausklammern} \\ &= \frac{(k+1) \cdot ((k+1)+1)}{2} && \text{Terme vertauscht} \end{aligned}$$

□

Rechenregeln

Neutrales Element	$0 + n = n$
Kommutativität	$n + m = m + n$
Assoziativität	$(n+m)+k = n+(m+k)$
Kürzbarkeit	$(n+k = m+k) \Rightarrow n = m$

Multiplikation

Die Multiplikation ist rekursiv definiert:

1. Eine Zahl mal 0 ist 0: $n \cdot 0 = 0$
2. Wird eine Zahl mit dem Nachfolger einer anderen Zahl multipliziert, ist das so, wie wenn erst die beiden Zahlen multipliziert und anschliessend die ursprüngliche Zahl addiert wird: $m \cdot \sigma(n) = \sigma(m \cdot n) + m$

Potenzen

1. Eine Zahl hoch 0 ist 1: $n^0 = 1$
2. Eine Zahl hoch dem Nachfolger einer anderen Zahl ist die eigentliche Zahl multipliziert mit der eigentlichen Zahl hoch der anderen Zahl: $m^{\sigma(n)} = m \cdot (m^n)$

Fakultät

1. $0! = 1$
2. $\sigma(m)! = \sigma(m) \cdot m!$

Beispiel: $n! > 2^n$ für $n \geq 4$

Beweis. Anfang: $4! = 24 > 16 = 2^4$
Annahme: $k! > 2^k$
Zu zeigen: $(k+1)! > 2^{k+1}$

$$(k+1)! = (k+1) \cdot k! > (k+1) \cdot 2^k > 2 \cdot 2^k = 2^{k+1}$$

□

Beweisstrategie: Von Links und rechts der Mitte hin annähern.

Rechenregeln

Absorbtion	$0 \cdot n = 0$	
Neutrales Element	$1 \cdot n = n$	
Kommutativität	$n \cdot m = m \cdot n$	Partialsummen
Assoziativität	$(n \cdot m) \cdot k = n \cdot (m \cdot k)$	
Distributivität	$n \cdot (m+k) = n \cdot m + n \cdot k$	

$$\sum_{i=1}^{n} (c \cdot (a_1 + b_1)) = c \left(\sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i \right)$$

Produkte

$$\prod_{i=1}^{0} a_i = 1$$

$$\prod_{i=1}^{n+1} a_i = a_{n+1} \cdot \prod_{i=1}^{n} a_i$$

Die Ordnung der natürlichen Zahlen

Es sei A eine Menge und $\preceq$ eine Ordnung auf A.

1. Sei $X \subset A$, dann ist $m \in X$ dass minimale Element, wenn gilt: $\forall x \in X(m \preceq x)$.
2. Das Paar $(A, \preceq)$ heisst Wohlordnung, wenn jede nichtleere Teilmenge $X \subset A$ ein minimales Element besitzt.

Die 0 ist die kleinste natürliche Zahl.

Relationen

$a \leq b \quad \Leftrightarrow \exists k \in \mathbb{N}(m = k + n)$
$a < b \quad \Leftrightarrow (n \leq m \wedge n \neq m)$
Die Kleiner-als-Relation wird rekursiv definiert:

1. Keine Zahl ist kleiner als null: $\forall n \in \mathbb{N}\colon \neg n < 0$
2. Eine Zahl ist kleiner als der Nachfolger einer anderen Zahl genau dann, wenn beide Zahlen gleich gross oder die erste Zahl kleiner als die zweite ist: $\forall m, n \in \mathbb{N}\colon m < \sigma(n) \Leftrightarrow (m = n) \vee (m < n)$

Zu zeigen: $3 < 5$

Beweis.

$$\begin{aligned}
(3 < 5) = (3 < \sigma(4)) & \quad \text{(Definition der 5)}\\
\Leftrightarrow (3 = 4) \vee (3 < 4) & \quad \text{(Kleiner 2: links falsch)}\\
(3 < 4) = (3 < \sigma(3)) & \quad \text{(Definition der 4)}\\
\Leftrightarrow (3 = 3) \vee (3 < 3) & \quad \text{(Kleiner 2: (3 = 3) ist wahr)}
\end{aligned}$$

□

Das Paar $(\mathbb{N}, \leq)$ ist eine Wohlordnung.

Rechenregeln

$$\begin{aligned}
n < m &\Leftrightarrow (n + 1) \leq m\\
n < m &\Leftrightarrow (n + k) < (m + k)\\
n \leq m &\Leftrightarrow (n + k) \leq (m + k)\\
(n \leq n') \wedge (m \leq m') &\Leftrightarrow (n + m) \leq (n' + m')
\end{aligned}$$

Ganze Zahlen

$\mathbb{Z} = \{\cdots - 2, -1, 0, 1, 2, \dots\}$
Es gilt: $x < y \Leftrightarrow \exists n \in \mathbb{N} > 0 \mid x + n = y$

Rechenregeln

	$-1\dot{z} = -z$
	$-(-z) = z$
Inverses Element bzgl. +	$-z + z = 0$
Absorbtion	$0 \cdot z = 0$
Neutrales Element bzgl. +	$0 + z = z$
Neutrales Element bzgl. ·	$1 cdot z = z$
Assoziativität bzgl. +	$a+(b+c) = (a+b)+c$
Assoziativität bzgl. ·	$a \cdot (b \cdot c) = (a \cdot b) \cdot c$
Kommutativität bzgl. +	$a + b = b + a$
Kommutativität bzgl. ·	$a \cdot b = b \cdot a$
Distributiviät	$a \cdot (b+c) = a \cdot b + a \cdot c$

Definitionen

Subtraktion

$$a - b = a + (-b)$$

Betrag

$$|z| = \begin{cases} z & \text{falls } z \in \mathbb{N} \\ -1 \cdot z & \text{sonst} \end{cases}$$

Teilbarkeit

$$x \mid y \Leftrightarrow \exists q \in \mathbb{Z}(y = x \cdot q)$$

Teilbarkeit ist transitiv: $x \mid y \wedge y \mid z \Rightarrow x \mid z$.
Beispiel: $\forall a, b, c, d \in \mathbb{Z}\ (a \mid b) \wedge (a \mid d) \Rightarrow (a \cdot c) \mid (b \cdot d)$

Beweis. Es seien a, b, c, d fest, aber beliebig.
Es gelte $a \mid b$ und $c \mid d$
Zeige: $a \cdot c \mid b \cdot d$

$$\begin{aligned}
a \mid b &\Leftrightarrow \exists q_1 \in \mathbb{Z}\ b = a \cdot q_1\\
c \mid d &\Leftrightarrow \exists q_2 \in \mathbb{Z}\ d = c \cdot q_2\\
(a \cdot q_1) \cdot (c \cdot q_2) = b \cdot d &\\
\text{Mit } q_3 = q_1 \cdot q_2 \text{ gilt:} a \cdot c \cdot q_3 = b \cdot d \Rightarrow (a \cdot c) \mid (b \cdot d)
\end{aligned}$$

□

Beispiel: $\forall a, b, c \in \mathbb{Z}\ a \mid b \wedge a \nmid c \Rightarrow a \nmid (b + c)$

Beweis. Es seien a, b, c fest, aber beliebig.
Es gelte $a \mid b$ und $a \nmid b$.
Zeige: $a \nmid (b + c)$. Anmerkung: Beweis durch Widerspruch:
$\neg(a \mid b \wedge a \nmid c \Rightarrow a \nmid (b + c)) = a \mid b \wedge a \nmid c \wedge a \mid (b + c)$
Annahme: $a \mid (b + c)$

$$\begin{aligned}
a \mid b &\Leftrightarrow a \cdot q_1 = b\\
a \mid (b + c) &\Leftrightarrow a \cdot q_2 = b + c\\
a \cdot q_2 &= a \cdot q_1 + c\\
a(q_2 - q_1) = c &\Leftrightarrow a \mid c. \text{Widerspruch zum geltenden}
\end{aligned}$$

□

Hilfssätze

$s \mid t \wedge s \mid u \Rightarrow s \mid (t + u)$
$s \mid t \wedge s \mid u \Rightarrow s \mid (t - u)$

Teilen mit Rest

Sind $x, y \in \mathbb{N} \setminus \{0\}$, dann gibt es eindeutig bestimmte Zahlen, so dass:

1. $y = q \cdot x + r$
2. $r < x$

Kleinstes gemeinsames Vielfaches (KGV)

(engl. *least common multiple*, zum erweitern von Brüchen)

$$\text{kgV}(x, y) = \min\{q \in \mathbb{N} \mid x \mid q \wedge y \mid q\}$$

Grösster gemeinsamer Teiler (GGT)

(engl. *greatest common divisor*, zum kürzen von Brüchen)

$$\text{ggT}(x, y) = \max\{q \in \mathbb{N} \mid q \mid n \wedge q \mid y\}$$

$$\text{kgV}(x, y) = \min\{q \in \mathbb{N} \mid n \mid q \wedge m \mid k\}$$

$$\text{kgV}(x, y) \cdot \text{ggT}(x, y) = x \cdot y$$

Euklidischer Algorithmus

$$\text{ggt}(n, m) = \text{ggt}(n, m - n) = \text{ggt}(m, m - n)$$

Teilerfremdheit

Zahlen sind teilerfremd, wenn $\text{ggt}(m, n) = 1 \Leftrightarrow k \cdot x + k' \cdot y$.

Zahlentheorie

Satz vom kleinsten Teiler

Der kleinste Teiler $d > 1$ einer natürlichen Zahl $n \geq 2$ ist eine Primzahl.

Beweis. Sei $T(n)$ die Menge aller Teiler von n.
$T(n) \backslash \{1\}$ ist nicht leer, weil $n \in T(n)$
dann gibt es nach dem Wohlordnungsprinzip[1] eine kleinste Zahl d in $T(n) \backslash \{1\}$.
Zu zeigen: d ist eine Primzahl
Annahme: d ist keine Primzahl
Dann: $\exists a, b \in \mathbb{N} \setminus \{1, d\}\colon a \cdot b = d \wedge a, b < d$
$\Rightarrow a \mid d$
Da a kleiner als d sein muss, kann d nicht das kleinste Element in $T(n) \backslash 1$ sein.
Das ist ein Widerspruch zur Annahme. Die Annahme muss falsch sein, dann muss aber d eine Primzahl sein. □

Hauptsatz

Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige Primfaktorzerlegung. Die Reihenfolge der Primfaktoren kann variieren.

Beweis. Sei $n \in \mathbb{N} \setminus \{1\}$
Fall I: n ist eine Primzahl, ein eindeutiger Primfaktor gefunden (n).
Fall II: n ist keine Primzahl

$$\Rightarrow \exists d_1, q_1 \in \mathbb{N} \setminus \{1\}\colon d_1 \cdot q_1 = n$$

und d_1 ist das kleinste Element in $T(n) \setminus \{1\}$, also d_1 ist Primzahl
Betrachte q_1: Fall I: q_1 ist eine Primzahl, eindeutige Primfaktorzerlegung gefunden.
Fall II: q_1 ist keine Primzahl, dann wiederhole diesen Prozess mit q_1

□

Revision: 1.0, Datum: 6. Januar 2013

[1] In jeder nicht-leeren Teilmenge der natürlichen Zahlen gibt es eine kleinste Zahl