3 Zahlen und Zahlendarstellungen

3.1 Die Menge IN der natürlichen Zahlen

3.1.1 Axiomatische Charakterisierung

Axiome von Peano (1891)

1) Null ist eine natürliche Zahl ($0 \in$ IN).
2) Jede natürliche Zahl n besitzt genau einen unmittelbaren Nachfolger $n' = \sigma(n)$.
3) Jede natürliche Zahl m ist unmittelbarer Nachfolger höchstens einer natürlichen Zahl ($m = \sigma(n)$).
4) Null ist kein unmittelbarer Nachfolger einer natürlichen Zahl.
5) Induktionsaxiom: Besitzt eine Menge M die Zahl 0 und mit einer Zahl n auch deren Nachfolger n', so gilt: IN $\subseteq M$.

Darstellungen von natürlichen Zahlen: IN = {0, 1, 2, ... , 10, 11, ...} = {I, II, III, IV, V, ... , X, ... , L, ... , C, ... , D, ..., M, ...} $\cup$ {0} = {|, ||, |||, ||||, ...}

3.1.2 Addition und Multiplikation

Addition		**Multiplikation**
$m + 0 = m$ $m + n' = (m + n)'$	**rekursive Definition**	$m * 0 = 0$ $m * n' = m * n + m$
$m + n = n + m$	**Kommutativität**	$m * n = n *$ m
$(m + n) + p = m + (n + p)$	**Assoziativität**	$(m * n) * p = m * (n * p)$
$m + 0 = 0 + m = m$ **0 ist neutrales Element bez. + Nullelement**		$m * 1 = 1 * m = m$ **1 ist neutrales Element bez. * Einselement**
$m + n = 0 \Leftrightarrow m = 0$ und $n = 0$		$m * n = 1 \Leftrightarrow m = 1$ und $n = 1$ $m * n = 0 \Leftrightarrow m = 0$ oder $n = 0$
$m + a = m + b \Rightarrow a = b$	**Kürzungsregeln**	Für $m \neq 0$ gilt: $m * a = m * b \Rightarrow a = b$
	Distributivität $(m + n) * p$ $= m * p + n * p$ * ist distributiv bez. +	

3.1.3 Relationen

Kleinergleichrelation		**Teilbarkeitsrelation**
$m \leq n$: $\Leftrightarrow$ es gibt eine natürliche Zahl s mit $m + s = n$	**Definition**	$m \mid n$: $\Leftrightarrow$ es gibt eine natürliche Zahl p mit $m * p = n$
$m \leq m$ f. a. $m \in$ IN Beweis: $m + 0 = m$	**Reflexivität**	$m \mid m$ f. a. $m \in$ IN Beweis: $m * 1 = m$

$m \le n$ und $n \le m \Rightarrow m = n$ Beweis: nach Vor. gilt $m + r = n$ und $n + s = m$, $\Rightarrow (m + r) + s = m \Rightarrow m + (r + s) = m$ $\Rightarrow r + s = 0 \Rightarrow r = 0$ und $s = 0$ $\Rightarrow m = n$	**Antisymmetrie**	$m \mid n$ und $n \mid m \Rightarrow m = n$ Beweis: Übungsaufgabe
$m \le n$ und $n \le p \Rightarrow m \le p$	**Transitivität**	$m \mid n$ und $n \mid p \Rightarrow m \mid p$
f. a. m, n gilt: $m \le n$ oder $n \le m$ $\le$ ist **linear** **Totalordnung**		Es gibt unvergleichbare Elemente, z. B. 3 teilt nicht 5 und 5 teilt auch nicht 3, d. h. $\mid$ ist **nicht linear** **Ordnung**
		weitere wichtige Eigenschaft $m \mid n$ und $m \mid p \Rightarrow m \mid (n + p)$

Weil $0' = 1$, gilt $n' = (n + 0)' = n + 0' = n + 1$.

3.1.4 Subtraktion und Division

Subtraktion	**Division**
Die Gleichung $m + x = n$ ist in IN genau dann lösbar, wenn $m \le n$	Die Gleichung $m * x = n$ ist in IN genau dann lösbar, wenn $m \mid n$
x bezeichnen wir dann mit $n - m$	x bezeichnen wir dann mit $\frac{n}{m}$

Während die Addition und die Multiplikation natürlicher Zahlen uneingeschränkt ausführbar sind, sind also Subtraktion und Division nur **eingeschränkt ausführbar**!

3.1.5 Das Beweisprinzip der vollständigen Induktion

Satz
Sei H eine Aussage über natürliche Zahlen. Gilt diese Aussage für die Zahl 0 und folgt aus der Gültigkeit der Aussage für eine beliebige natürliche Zahl k die Gültigkeit für den Nachfolger $k + 1$, so gilt H für alle natürlichen Zahlen n.

Induktions- Induktionsschritt (I. S.)
anfang (I. A.) Ind.-Vor. Ind.-Beh.

$$[H(0) \text{ und f. a. } k \in \mathbb{N}: (H(k) \Rightarrow H(k+1))] \Rightarrow H(n) \text{ f. a. } n \in \mathbb{N}$$

1. Vor. 2. Vor.

Voraussetzung Behauptung

Beispiel: *H*: Für beliebige natürliche Zahlen *m*, *n*, *p* gilt das folgende Assoziativgesetz:
$(m+n)+p=m+(n+p)$.

Beweis durch vollständige Induktion über *p* (bei festem *m* und *n*):

I. A.: Man zeigt zunächst, dass *H* für $p = 0$ gilt. Wegen der ersten Rekursionsgleichung für die Addition gilt $(m + n) + 0 = m + n = m + (n + 0)$.

I. S.: Man nimmt an, dass für ein beliebiges *p* die Aussage *H* schon gelte und zeigt dann, dass sie auch für den Nachfolger $p + 1$ gilt.
Durch wiederholte Anwendung der zweiten Rekursionsgleichung für die Addition und unter Ausnutzung der Induktionsvoraussetzung erhält man:
$(m+n)+(p+1)=((m+n)+p)+1=(m+(n+p))+1=m+((n+p)+1)=m+(n+(p+1))$.

3.1.6 Primzahlen

p ist **Primzahl**: $\Leftrightarrow$ *p* ist natürliche Zahl und $p > 1$, und *p* ist nur durch sich und 1 teilbar.
Beispiele: 2, 3, 5, 7, 11, 13, 17, 23, ...

Folgerungen und Sätze

- 2 ist die einzige gerade Primzahl.
- Jede natürliche Zahl $n > 1$ ist entweder Primzahl oder zusammengesetzte Zahl, z. B. $n = 150 = 10 * 15$.
- **Fundamentalsatz der Zahlentheorie:**
  Jede natürliche Zahl $n > 1$ ist (bis auf die Reihenfolge der Faktoren) eindeutig als Produkt von Primzahlen darstellbar: $n = p_1 * p_2 * p_3 * ... * p_k$.
  Beispiele:
  150 = 2 * 3 * 5 *5; 224 = $2^5 * 7$;
  2144 = $2^5 * 67$; 3856 = $2^4 * 241$;
  3813 = 3 * 31 * 41; 8260 = 2 * 2 * 5 * 7 * 59;
  40250= 2 * 5^3 * 7 * 23; 2813 = 29 * 97;
- Ist *p* Primzahl und $p \mid m * n \Rightarrow p \mid m$ oder $p \mid n$.
- **Es gibt unendlich viele Primzahlen.**
  Beweis indirekt:
  Angenommen, die Menge P aller Primzahlen ist endlich, d. h. $P = \{p_1, p_2, ..., p_n\}$. Wir bilden daraus die natürliche Zahl $m = p_1 * p_2 * ... * p_n + 1$. Da $m > 1$ lässt sich *m* nach dem Fundamentalsatz eindeutig in Primfaktoren zerlegen. Sei *p* ein beliebiger Faktor aus diesem Produkt. Dann teilt *p* die Zahl *m*, aber $p \notin P$, denn der Rest bei Division von *m* durch p_i ($i = 1, 2, ..., n$) ist immer 1. Also waren in P nicht alle Primzahlen enthalten, was zum Widerspruch zur Annahme und mithin zur Richtigkeit des Satzes führt.

3.1.7 Induktive Definitionen

Addition	$m + 0 = m$;	
	$m + (n + 1) = (m + n) + 1$;	(mittels Nachfolger)
Multiplikation	$m * 0 = 0$;	
	$m * (n + 1) = m * n + m$;	(mittels Addition)
Potenz	$m^0 = 1$;	
	$m^{n+1} = m^n * m$;	(mittels Multiplikation)

Potenzgesetze:

$m^{n_1+n_2} = m^{n_1} * m^{n_2}$

$m^{n_1*n_2} = (m^{n_1})^{n_2}$

$(m_1 * m_2)^n = m_1^{\,n} * m_2^{\,n}$

$(m_1 + m_2)^n = ?$

$m_1 \le m_2 \Rightarrow m_1^{\,n} \le m_2^{\,n}$

$n_1 \le n_2 \Rightarrow m^{n_1} \le m^{n_2}$

Anmerkungen:

- Beweise werden durch vollständige Induktion geführt
- Assoziativ- und Kommutativgesetz gelten im Allgemeinen nicht

Allgemeine Summe

$$\sum_{i=0}^{0} a_i = a_0$$

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

Beispiele: $1+2+3+...+127 = \sum_{i=1}^{127} i$; $\quad 1+4+9+16+...+125 = \sum_{j=1}^{15} j^2$.

Allgemeines Produkt

$$\prod_{i=0}^{0} a_i = a_0$$

$$\prod_{i=0}^{n+1} a_i = \prod_{i=0}^{n} a_i \cdot a_{n+1}$$

Beispiel: $1 \cdot 2 \cdot 3 \cdot ... \cdot n = n! = \prod_{i=1}^{n} i$

***n*-Fakultät**

$0! = 1$

$(n + 1)! = n! * (n + 1)$