

Monoid = Halbgruppe mit neutralem Element

Es ist zu zeigen:

$$1 \cdot u = u = u \cdot 1$$

neutrales Element

$$(h \cdot m) \cdot u = h \cdot (u \cdot u)$$

Halbgruppe

$$m \cdot n = n \cdot m$$

kommutativ

$$k \cdot u = k \cdot u \Rightarrow u = n$$

Kürzungsregel

$$h(u+v) = h \cdot u + h \cdot v$$

Distributivität

$$m < n \Rightarrow h \cdot m < h \cdot n$$

Monotonie

1. Neutrales Element

1.) Ist rechtsneutral nach Definition $1 \cdot m$ durch Ind. nach m

J.A. $1 \cdot 1 = 1 \cdot 1$

J.S. $1 \cdot S(m) = 1 + (1 \cdot m) \stackrel{J.V.}{=} 1 + m = m + 1 = S(m)$

2. Halbgruppe

$S(n) \cdot m = m + (n \cdot m)$ durch Induktion nach m

J.A. $S(u) \cdot 1 = S(u) = 1 + u = 1 + (1 \cdot u)$

J.S. $S(u) \cdot S(m) = S(n) + (S(m) \cdot m) \stackrel{J.V.}{=} S(n) + m + (n \cdot m) =$
 $= m + 1 + u + (n \cdot m) = S(m) + n \cdot m =$
 $= S(u) + (n \cdot S(m))$

$$S(n) \cdot m = m + (m \cdot n)$$

31.10.05

Beweis der Kommutativität durch Induktion nach n

J.A. $m \cdot 1 = m = 1 \cdot m$

J.S. $m \cdot S(n) = m + (m \cdot n) \stackrel{J.V.}{=} m + (n \cdot m) \stackrel{*}{=} S(n) \cdot m$

Distributivität durch Induktion nach m

J.A. $h(1+m) = h \cdot S(n) = h + (h \cdot n) = (h \cdot 1) + (h \cdot n)$

J.S. $h \cdot (S(n) + n) = h \cdot S(m+n) = h + (h \cdot (u+v)) \stackrel{J.V.}{=}$
 $= h + ((h \cdot u) + (h \cdot v)) \stackrel{Ass.}{=} (h + (h \cdot m)) + (h \cdot u) =$

$$= (k \cdot (sm)) + (k \cdot u)$$

Assoziativität durch Induktion nach n:

$$J.A. \quad (k \cdot m) \cdot 1 = k \cdot m = k \cdot (m \cdot 1)$$

$$\begin{aligned} J.S. \quad (k \cdot m) \cdot S(n) &= (k \cdot m)(u+1) \stackrel{\text{Dist.}}{=} ((k \cdot m) \cdot n) + ((k \cdot m) \cdot 1) = \\ &\stackrel{J.V.}{=} (k \cdot (m \cdot n)) + k \cdot (m \cdot 1) \stackrel{\text{Dist.}}{=} k((m \cdot n) + m) = \\ &= k \cdot (m + (m \cdot n)) = k \cdot (m \cdot S(n)) \end{aligned}$$

Monotonie durch Induktion nach k:

$$J.A. \quad m < n \Rightarrow 1 \cdot m = m < n = 1 \cdot n$$

$$\begin{aligned} J.S. \quad m < n &\Rightarrow \underline{S(k) \cdot m} = (k+1) \cdot m \stackrel{\text{Dist.}}{=} (k \cdot m) + 1 \cdot m < \\ &\stackrel{J.V.}{<} (k \cdot n) + 1 \cdot m = (k \cdot u) + u < (k \cdot u) + u + 1 = \\ &= (k \cdot u) + (1 \cdot n) = (k+1) \cdot n = \underline{S(k) \cdot n} \end{aligned}$$

Kürzungsregel durch Kontraposition

Sei $k \cdot m = k \cdot n$. Angenommen $m \neq n$. O.B.d.A. $m < n$
 $\Rightarrow$ Monotonie $k \cdot m < k \cdot n \Rightarrow k \cdot m \neq k \cdot n$ Widerspruch $\Rightarrow m = n$

Rechenregeln

$$1) \quad p, q \in \mathbb{N}, p \cdot q = 1 \Rightarrow p = q = 1$$

Beweis: Annahme $p \neq 1 \Rightarrow 1 < p \Rightarrow 1 \leq p < pq \Rightarrow 1 < pq$. Widerspruch

$$2) \quad m < n \Rightarrow k(n-m) = (k \cdot n) - (k \cdot m)$$

$$\begin{aligned} \text{Beweis:} \quad (k \cdot (n-m)) + (k \cdot m) &\stackrel{\text{Dist.}}{=} k((n-m) + m) = k \cdot n = \\ &= ((k \cdot n) - (k \cdot m)) + (k \cdot m) \stackrel{\text{Kürz.R.}}{\Rightarrow} k(n-m) = (k \cdot n) - (k \cdot m) \end{aligned}$$

3) Allgemeines Assoziativgesetz:

Definition: $a_1 \cdot a_2 \cdot \dots \cdot a_n = (\dots ((a_1 \cdot a_2) \cdot a_3) \dots) \cdot a_n$

Gesetz: $a_1 \cdot \dots \cdot a_n = (a_1 \cdot a_2 \cdot \dots \cdot a_k) \cdot (a_{k+1} \cdot \dots \cdot a_n)$

Schreibweise: $a_1 \cdot a_2 \cdot \dots \cdot a_n = \prod_{i=1}^n a_i$ (analog $a_1 + a_2 + \dots + a_n = \sum_{i=1}^n a_i$)

Konventionen: „Punkt vor Strich“

Treten in einem ohne Klammern geschriebenen Term Additionen und Multiplikation auf, so sind die Multiplikationen zuerst durchzuführen:

$$l + m \cdot n = l + (m \cdot n)$$

Distributivgesetze: $h \cdot (m + n) = hm + hn$, $(m + n) \cdot h = mh + nh$

Das Multiplikationszeichen kann weggelassen werden, wenn das Aufheben einer Multiplikation aus dem Zusammenhang klar ist, also vor einer Variablen, oder vor einer Klammer (weglassen nach einer Klammer ist unüblich)

$$l + m \cdot n = l + mn \quad ; \quad 3 \cdot m = 3m$$

$$h(m + n) = hm + hn$$

Ein nicht geschriebener Malpunkt bindet stärker als ein geschriebener!

z.B.

$$6a : 3a = \begin{cases} 2 \\ 2a^2 \end{cases} \Rightarrow (6a : 3) \cdot a \quad \downarrow$$

Teilbarkeit

Definition:

$$m, n \in \mathbb{N}$$

m Teiler von $n \iff \exists q: m \cdot q = n$ in Zeichen $m|n$

Kürzungsregel $\Rightarrow$ Wenn q existiert, so ist es eindeutig

$$\text{bestimmt: } q = \frac{n}{m}$$

Satz:

Die Teilbarkeit ist eine reflexive (partiell oder teilweise) Ordnung auf $\mathbb{N}$, derart dass die Multiplikation monoton ist.

Beweis:

1.) Reflexivität:

$$m \cdot 1 = m \Rightarrow m/m$$

2.) Transitivität:

$$h/m \text{ und } m/n \Rightarrow h \cdot p = m, m \cdot q = n$$

$$\Rightarrow h \cdot (p \cdot q) = (h \cdot p) \cdot q = m \cdot q = n \Rightarrow h/n$$

3.) Antisymmetrie:

$$m/n \text{ und } n/m \Rightarrow m \cdot q = n, n \cdot p = m$$

$$\Rightarrow m(pq) = (mq)p = np = m = m \cdot 1$$

kurz R

$$\Rightarrow qp = 1 \Rightarrow q = p = 1$$

$$\Rightarrow m = n$$

4.) Monotonie:

$$m/n \Rightarrow m \cdot q = n \Rightarrow (h \cdot m) \cdot q = h(mq)$$

$$= h \cdot n \Rightarrow h \cdot m \mid h \cdot n$$

Bemerkung:

1 ist das „kleinste“ Element von $\mathbb{N}$ bezüglich der

Teilbarkeit: $1 \cdot m = m \Rightarrow 1/m$ für alle $m \in \mathbb{N}$

„teilt“ ist keine lineare Ordnung, die Trichotomie gilt nicht

$$2 \nmid 3, 3 \nmid 2, 3 \neq 2 \quad m/n \Rightarrow m \leq n$$

Beweis:

$$m \cdot q = n$$

$$1. \text{ Fall: } q = 1 \Rightarrow m = n$$

$$2. \text{ Fall } 1 < q \Rightarrow m = m \cdot 1 < m \cdot q = n$$

Definition:

Eine natürliche Zahl p heißt Primzahl, wenn sie

genau zwei Teile besitzt: $1/p, p/p \Rightarrow 1 \neq p$

Beispiele: 2, 3, 5, 7, ...

Definition:

$p, n \in \mathbb{N}$ p ist Primteiler von n , wenn p Primzahl ist und n teilt.

Satz

Jede natürliche Zahl besitzt einen Primteiler ($n \neq 1$)

Beweis:

Sei $n > 1$ gegeben. Setze $M = \{m \in \mathbb{N} \mid 1 \neq m \wedge m/n\}$

$$m \in M \Rightarrow M \neq \emptyset \xrightarrow[\text{wohlgeordnet}]{\mathbb{N}} \text{Es gilt } m_0 = \min M$$

Behauptung:

m_0 ist Primzahl. Annahme: Es gilt m_1 mit $m_1 \mid m_0$

$$\text{und } m_1 \neq m_0 \xrightarrow{*} m_1 < m_0 \xrightarrow{\text{Trans.}} m_1 \mid m \Rightarrow m_1 \in M$$

$\Rightarrow$ Widerspruch zu $m_0 = \min M$ q.e.d.

Folgerung:

Jede natürliche Zahl $n > 1$ ist ein Produkt von (endlich vielen) Primzahlen.

Beweis:

Beweis durch Induktion nach n

J.A. $n=2$ klar

Induktionsvoraussetzung: Behauptung richtig für alle $m < n$

J.S. Sei p ein Primteiler von n , $n = p \cdot q$

1. Fall: n Primzahl, $n = p$, $q = 1$ nichts zu beweisen

2. Fall n keine Primzahl $\Rightarrow p < n$

$$q | n \Rightarrow 1 < q < n$$

J.V.
 $\Rightarrow q$ Produkt von Primzahlen

$\Rightarrow n = pq$ Produkt aus Primzahlen

Hauptsatz der elementaren Zahlentheorie

Jede natürliche Zahl $n > 1$ besitzt bis auf die Reihenfolge eindeutige Primzahlenzerlegung.

Beweis:

Methode des „kleinsten Verbrechers“

Annahme: $n = p_1 \cdot p_2 \cdot \dots \cdot p_r = q_1 \cdot q_2 \cdot \dots \cdot q_s$, p_i, q_j Primzahlen,

$p_i \neq p_j$ für alle i, j ; o.B.d.A. $q_1 < p_1$

Setze $m = n - q_1 \cdot p_2 \cdot \dots \cdot p_r = (p_1 - q_1) \cdot p_2 \cdot \dots \cdot p_r < n$

n kleinster Verbrecher $\Rightarrow m$ besitzt eindeutig Primzahlenzerlegung:

$$m = q_1 (q_2 \cdot \dots \cdot q_s - p_2 \cdot \dots \cdot p_r) \Rightarrow p_1 | (p_1 - q_1)$$

$$\Rightarrow p_1 - q_1 = q_1 t \Rightarrow p_1 = q_1 + q_1 t = q_1 (1 + t) \Rightarrow q_1 | p_1$$

$$\Rightarrow q_1 = p_1 \Rightarrow \text{Widerspruch}$$