Der Fundamentalsatz der Arithmetik

Unter $\mathbb{N}_0$ verstehen wir in diesem Dokument die natürlichen Zahlen mit Null, also $\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$.

Definition 1 Seien $n, m \in \mathbb{N}_0$. Wir sagen n *ist teilbar durch* m (oder auch m *teilt* n), in Zeichen $m \mid n$, wenn es ein $k \in \mathbb{N}_0$ gibt mit $n = mk$. Wir sagen n und m sind *teilerfremd*, wenn unter allen $x \in \mathbb{N}_0$ nur $x = 1$ sowohl $x \mid n$ als auch $x \mid m$ erfüllt, wenn n und m also nur den trivialen Teiler 1 gemeinsam haben.

Für den Spezialfall der Null stellen wir fest, dass Null durch jede Zahl teilbar ist, aber keine Zahl $n > 0$ durch Null teilbar ist, denn $n = 0 \cdot k$ kann nur für $n = 0$ eintreten.

Lemma 2 *Es gelten die folgenden Rechenregeln für alle* $a, b, c, m, n \in \mathbb{N}_0$*:*

1. $a \mid 0$, $a \mid a$, $1 \mid a$ *und der einzige Teiler von* 1 *ist* 1.
2. *Wenn* $a \mid b$ *und* $b \mid c$ *gelten, dann gilt auch* $a \mid c$.
3. *Es sei* $c \neq 0$. *Dann gilt* $a \mid b$ *genau dann, wenn* $ca \mid cb$ *gilt.*
4. *Es sei* $a \mid b$ *und* $a \mid c$. *Dann ist* $a \mid mb + nc$ *für alle* $m, n \in \mathbb{N}_0$.
5. *Aus* $a \mid m$ *und* $b \mid n$ *folgt* $ab \mid mn$.
6. *Wenn* $a \mid b$ *und* $b \neq 0$ *gelten, dann ist* $a \leq b$.
7. *Aus* $a \mid b$ *und* $b \mid a$ *folgt* $a = b$.
8. *Ist* $a = b + c$, $n \mid a$ *und* $n \mid b$, *dann ist auch* $n \mid c$.
9. *Es seien* $0 < a < b \leq c$ *und* $b \mid c$. *Dann ist* $b \nmid c + a$.

Beweis. Wir beweisen nur (2), (6) und (8), der Rest sind Übungsaufgaben.
(2): Es sei $a \mid b$ und $b \mid c$. Dann gibt es ein $x \in \mathbb{N}_0$ mit $ax = b$ und ein $y \in \mathbb{N}_0$ mit $by = c$. Daher ist $c = axy = a(xy)$. Da $xy \in \mathbb{N}_0$ ist, muss also a ein Teiler von c sein.
(6): Es sei a ein Teiler von b und $b \neq 0$. Dann gibt es eine ganze Zahl x mit $ax = b$ und $x \neq 0$. Sei nun $y \in \mathbb{N}_0$ mit $y + 1 = x$ (dieses y existiert, weil $x \neq 0$ ist), dann ist $b = a(y + 1) = ay + a$, also $a \leq b$.
(8): Nach Voraussetzung gibt es $x, y \in \mathbb{N}_0$ mit $a = nx$ und $b = ny$. Eingesetzt gilt also $nx = ny + c$. Nehmen wir an, $x < y$. Dann ist $nx < ny \leq ny + c$, was nicht sein kann. Folglich ist $y \leq x$, und damit gibt es ein $z \in \mathbb{N}_0$ mit $y + z = x$. Daraus folgt $ny + c = nx = n(y + z) = ny + nz$ und damit $c = nz$. Also ist auch c durch n teilbar. □

Definition 3 Eine natürliche Zahl $n > 1$, die nur durch 1 und sich selbst teilbar ist, heißt *prim* oder *Primzahl*. Ein *Primteiler* einer Zahl $a \in \mathbb{N}_0$ ist ein Teiler von a, der prim ist.

Die ersten Primzahlen lauten $2, 3, 5, 7, 11, 13, 17, 19$. Insbesondere wird die 1 üblicherweise nicht als Primzahl gezählt, und so wollen wir es auch hier handhaben. Die Null ist keine Primzahl, da sie durch jede natürliche Zahl teilbar ist. Andere Zahlen lassen sich als Produkt von Primzahlen schreiben, z.B. $21 = 3 \cdot 7$. Wir nennen dies eine *Primfaktorzerlegung*:

Definition 4 Eine *Primfaktorzerlegung* einer Zahl $n \in \mathbb{N}_0$ ist die Darstellung von n als Produkt von endlich vielen Primzahlen.

Ein Beispiel für eine Primfaktorzerlegung ist $250 = 2 \cdot 5^3 = 2 \cdot 5 \cdot 5 \cdot 5$. Keine Primfaktorzerlegung im obigen Sinn sind $21 = 1 \cdot 21$ oder $21 = (-3) \cdot (-7)$. Zerlegungen in genau eine Primzahl sind erlaubt, beispielsweise ist $7 = 7$ eine Primfaktorzerlegung der Zahl 7. Damit eröffnen sich zwei Fragen: Besitzt jede natürliche Zahl eine Primfaktorzerlegung? Und gibt es natürliche Zahlen mit mehr als einer Primfaktorzerlegung?

Satz 5 (Existenz der Primfaktorzerlegung) *Jede natürliche Zahl $n > 1$ besitzt eine Primfaktorzerlegung.*

Beweis. Ist die Behauptung falsch, so gibt es eine kleinste Zahl n_0, die sich nicht in Primfaktoren zerlegen lässt. Diese Zahl n_0 ist dann jedenfalls keine Primzahl, besitzt also eine Zerlegung in zwei von 1 verschiedene Faktoren, $n_0 = pq$. Hier sind p und q beide kleiner als n_0 und besitzen daher nach Annahme eine Zerlegung in endlich viele Primfaktoren. Somit besitzt auch n_0 eine solche Zerlegung, im Widerspruch zur Definition von n_0. □

Für die Eindeutigkeit der Primfaktorzerlegung benötigen wir einen kleinen Hilfssatz:

Lemma 6 *Jede natürliche Zahl $n > 1$ besitzt einen Primteiler.*

Beweis. Sei T die Menge aller Teiler t von n mit $t > 1$. T ist eine Menge natürlicher Zahlen und nicht leer, da $n \in T$ ist. Also gibt es ein kleinstes Element $p \in T$. Angenommen, p ist keine Primzahl, und $m \in \mathbb{N}_0 \setminus \{1, p\}$ ein Teiler von p. Dann ist m auch ein Teiler von n nach Lemma 2(2) und $m < p$ nach 2(6). Das widerspricht aber der Definition von p als kleinstem Element in T. □

Wir haben im Beweis nicht nur irgend einen Primteiler von n konstruiert, sondern den kleinsten Primteiler von n. Die Definition des kleinsten Primteilers erlaubt auch eine sehr einfache Formulierung des klassischen Beweises von Euklid zur unendlichen Anzahl der Primzahlen; bevor wir zum Fundamentalsatz schreiten, wollen wir uns daher noch kurz den Satz von Euklid anschauen:

Satz 7 (Satz von Euklid) *Es gibt unendlich viele Primzahlen.*

Beweis. Sei P die Menge aller Primzahlen. Angenommen, P ist endlich. Es sei n das Produkt aller Zahlen aus P und $m := n + 1$. Damit ist m größer als jede Zahl in P, und daher $m \notin P$. Nach Lemma 2(9) ist $p \nmid m$ für alle $p \in P$, aber nach Lemma 6 besitzt m einen Primteiler: Widerspruch. □

Satz 8 (Fundamentalsatz der Arithmetik) *Jede natürliche Zahl $n > 1$ besitzt eine bis auf Reihenfolge eindeutige Primfaktorzerlegung (d.h. zwei unterschiedliche Zerlegungen unterscheiden sich nur in der Reihenfolge der Faktoren).*

Beweis. Die Existenz haben wir bereits in Satz 5 gezeigt. Bleibt noch die Eindeutigkeit zu zeigen: Angenommen, $n \in \mathbb{N}_0$ besitzt eine nicht-eindeutige Primfaktorzerlegung, und nehmen wir weiter an, n ist die kleinste natürliche Zahl mit nicht-eindeutiger Primfaktorzerlegung. Sei p_1 der kleinste Primteiler von n. Indem wir $n = p_1 m$ für ein $m \in \mathbb{N}_0$ schreiben, können wir eine Primfaktorzerlegung von n finden, in der p_1 auftritt: $n = p_1 p_2 \cdots p_s$ mit $s \in \mathbb{N}_0$ und Primzahlen $p_1, \ldots, p_s$. Sei $n = q_1 q_2 \cdots q_t$ mit $t \in \mathbb{N}_0$ und Primzahlen $q_1, \ldots, q_t$ eine andere Primfaktorzerlegung von n. Wenn eines der q_j gleich p_1 wäre, müsste $p_2 \cdots p_s$ zwei unterschiedliche Primfaktorzerlegungen haben, was der Annahme widerspricht, dass n die kleinste solche Zahl ist. Folglich ist $p_1 \neq q_j$ für alle $j \in \{1, \ldots, t\}$, und da p_1 der kleinste Primteiler von n ist, muss sogar $p_1 < q_j$ für alle j gelten. Sei nun $d \in \mathbb{N}_0$ mit $q_1 = p_1 + d$ und

$$\begin{aligned} n_1 &:= p_1 \cdot q_2 q_3 \cdots q_t \,, \\ n_2 &:= d \cdot q_2 q_3 \cdots q_t \,. \end{aligned}$$

Aus dem Distributivgesetz folgt damit $n = n_1 + n_2$. Da sowohl n_1 als auch n durch p teilbar sind, muss auch n_2 durch p_1 teilbar sein. Da n_2 kleiner ist als n, muss darüber hinaus die Primfaktorzerlegung von n_2 eindeutig sein. Da keine der Zahlen q_2, q_3, …, q_t durch p_1 teilbar sein kann (es sind von p_1 verschiedene Primzahlen), muss die Primfaktorzerlegung von d ein p_1 enthalten, insbesondere ist also $p_1 \mid d$. Da $q_1 = p_1 + d$ ist, muss dann aber auch q_1 durch p_1 teilbar sein; das widerspricht aber der Annahme, dass q_1 eine von p_1 verschiedene Primzahl ist. □