

Übungsblatt № 9

Aufgabe 62

Beweisen Sie, dass für alle natürlichen Zahlen $a, b \in \mathbb{N}$ die Gleichung $ab = \text{ggT}(a, b) \cdot \text{kgV}(a, b)$ gilt.

Sei $d = \text{ggT}(a, b)$, dann gibt es teilerfremde $a_0, b_0 \in \mathbb{N}$, sodass $a_0d = a$ und $b_0d = b$. Offensichtlich teilt a_0b_0d sowohl a als auch b . Sei $m \in \mathbb{N}$ mit $m|a$ und $m|b$. Wir wollen zeigen, dass $a_0b_0d|m$. Da m ein gemeinsames Vielfaches von a und b ist, gibt es ein $k \in \mathbb{N}$, sodass $m = ka = kb_0d$. Des Weiteren teilt $b m$, sprich b_0d teilt ka_0d . Daraus folgt durch einfaches Kürzen, dass $b_0|ka_0$. Da a_0 und b_0 teilerfremd sind, folgt $b_0|k$. Es gibt also ein $l \in \mathbb{N}$, sodass $b_0l = k$:

$$m = ka_0d = la_0b_0d \implies a_0b_0d|m$$

Damit teilt a_0b_0d alle gemeinsamen Vielfachen von a und b , insbesondere also auch das kleinste gemeinsame Vielfache, womit gilt $da_0b_0 = \text{kgV}(a, b)$. Damit erhalten wir direkt:

$$\text{ggT}(a, b)\text{kgV}(a, b) = a_0b_0d^2 = a_0db_0d = ab$$

Aufgabe 63

Sei p eine Primzahl. Für $n \in \mathbb{Z} \setminus \{0\}$ sei

$$v_p(n) = \max\{k \in \mathbb{N}_0 : p^k|n\}$$

Wie kann man k aus der Primfaktorzerlegung von $|n|$ ablesen?

Ist $r \in \mathbb{Q} \setminus \{0\}$ und sind $a, b, c, d \in \mathbb{Z} \setminus \{0\}$ mit $r = \frac{a}{b} = \frac{c}{d}$, so gilt $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. Wir können daher durch

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b)$$

für $a, b \in \mathbb{Z} \setminus \{0\}$ eine wohldefinierte Funktion $v_p: \mathbb{Q} \setminus \{0\} \rightarrow \mathbb{Z}$ definieren. Zeigen Sie, dass v_p die folgenden Eigenschaften besitzt:

- a) $v_p(rs) = v_p(r) + v_p(s)$ für $r, s \in \mathbb{Q} \setminus \{0\}$
- b) Für $r \in \mathbb{Q} \setminus \{0\}$ gilt genau dann $r \in \mathbb{Z}$, wenn $v_p(r) \geq 0$ für alle Primzahlen p ist.
- c) Sind $r, s \in \mathbb{Q} \setminus \{0\}$ mit $r + s \neq 0$, so gilt $v_p(r + s) \geq \min\{v_p(r), v_p(s)\}$. Ist $v_p(r) \neq v_p(s)$, so gilt die Gleichheit.

Es sei

$$|n| = \prod_{i=1}^d p_i^{k_i}$$

die Primfaktorzerlegung von $|n|$. Dann gilt $v_{p_i}(n) = k_i$ für $i = 1, \dots, d$, da offensichtlich $p_i^{k_i}|n$ und $p_i^{k_i+1} \nmid n$. Kommt p nicht in der Primfaktorzerlegung vor, so ist offensichtlich $v_p(n) = 0$, da $p^0 = 1|n$.

Sei nun $r \in \mathbb{Q} \setminus \{0\}$ mit $r = \frac{a}{b} = \frac{c}{d}$. Es seien a, b oBdA teilerfremd. Für den Fall $a = c$ und $b = d$ ist der Beweis trivial. Wir können somit annehmen, dass $l = \text{ggT}(c, d) > 1$, also c und d nicht teilerfremd sind. Es folgt somit

$$\frac{a}{b} = \frac{la}{lb} = \frac{c}{d}$$

Seien $a, b \in \mathbb{Z} \setminus \{0\}$ und $v_p(a) = k_1$ sowie $v_p(b) = k_2$:

$$p^{k_1} | a \implies p^{k_1} p^{k_2} | ab \iff p^{k_1+k_2} | ab \implies v_p(ab) = v_p(a) + v_p(b)$$

weil k_1 und k_2 jeweils maximal sind. Daraus folgt direkt:

$$v_p\left(\frac{c}{d}\right) = v_p(la) - v_p(lb) = v_p(l) + v_p(a) - v_p(l) - v_p(b) = v_p(a) - v_p(b) = v_p\left(\frac{a}{b}\right)$$

Zu a): Wir haben den Fall für $a, b \in \mathbb{Z} \setminus \{0\}$ bereits gezeigt. Sei $r = \frac{a}{b}$ und $s = \frac{c}{d}$ mit $\text{ggT}(a, b) = 1$ und $\text{ggT}(c, d) = 1$:

$$\begin{aligned} v_p(rs) &= v_p(ac) - v_p(bd) = v_p(a) + v_p(c) - v_p(b) - v_p(d) \\ &= \underbrace{v_p(a) - v_p(b)}_{=v_p(r)} + \underbrace{v_p(c) - v_p(d)}_{=v_p(s)} = v_p(r) + v_p(s) \end{aligned}$$

Zu b):

$$v_p(r) = v_p(a) - v_p(b) \geq 0 \iff v_p(a) \geq v_p(b)$$

Für $r \in \mathbb{Z}$ folgt $b = 1$ sprich $v_p(b) = 0$ und somit $v_p(a) \geq 0$, was per Definition von v_p erfüllt ist. Sei nun $v_p(r) \geq 0$. Wir nehmen oBdA an $\text{ggT}(a, b) = 1$. Angenommen $b \neq 1$, dann gibt es $p \in \mathbb{P}$ mit $v_p(b) \geq 1$ und $v_p(a) = 0$, da p nicht in der Primfaktorzerlegung von a vorkommt, da $\text{ggT}(a, b) = 1$, was aber ein Widerspruch zu $v_p(r) \geq 0$ ist.

Zu c): Seien $a, b \in \mathbb{Z} \setminus \{0\}$ mit $v_p(a) = k_1$ und $v_p(b) = k_2$. Wir zeigen zuerst, dass $v_p(a+b) \geq \min(v_p(a), v_p(b))$. Sei oBdA $k_1 = \min(k_1, k_2)$ und $k = k_2 - k_1$:

$$a + b = l_1 p^{k_1} + l_2 p^{k_2} = p^{k_1} (l_1 + l_2 p^k) \implies v_p(a+b) \geq k_1 = \min(k_1, k_2)$$

Wir zeigen noch $\min(a, b) - c = \min(a - c, b - c)$. Sei $a = \min(a, b)$:

$$a \leq b \implies \min(a - c, b - c) = a - c = \min(a, b) - c$$

Seien nun $r, s \in \mathbb{Q} \setminus \{0\}$ mit $r = \frac{a}{b}$ und $s = \frac{c}{d}$, sodass $\text{ggT}(a, b) = 1$ sowie $\text{ggT}(c, d) = 1$:

$$\begin{aligned} v_p(r+s) &= v_p\left(\frac{ad+bc}{bd}\right) = v_p(ad+bc) - v_p(bd) \geq \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) \\ &= \min(v_p(a) + v_p(d) - v_p(b) - v_p(d), v_p(b) + v_p(c) - v_p(d) - v_p(b)) \\ &= \min(v_p(a) - v_p(b), v_p(c) - v_p(d)) = \min(v_p(r), v_p(s)) \end{aligned}$$

Bekanntermaßen folgt aus $p|a$ und $p|b$, dass $p|(a+b)$. Gilt nun $p|a+b$ und $p|a$, dann gilt $p|a$ und somit auch $p|(a+b) - a = b$, sprich $p|b$. Sei nun $v_p(a) \neq v_p(b)$, sprich es gibt $k \in \mathbb{N}$ sowie $k_1 \in \mathbb{N}_0$ mit $a = l_1 p^{k_1}$ und $b = l_2 p^{k_1+k}$:

$$a + b = p^{k_1} (l_1 + l_2 p^k)$$

Angenommen $p|l_1 + l_2 p^k$, dann folgt aus unserer vorherigen Überlegung, dass $p|l_1$, womit $a + b = p^{k_1+1} (l'_1 + l_2 p^{k-1})$. Das ist aber ein Widerspruch dazu, dass $v_p(a) = k_1$. Daraus folgt aber $v_p(a+b) = k_1 = \min(v_p(a), v_p(b))$, womit

$$v_p(r+s) = v_p(ad+bc) - v_p(bd) = \min(v_p(ad), v_p(bc)) - v_p(b) - v_p(d) = \min(v_p(r), v_p(s))$$