(9.6) SATZ: Division mit Rest

Zu $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ existieren eindeutig bestimmte ganze Zahlen q und r mit

$$a = qn + r \quad \text{und} \quad 0 \le r < n$$

Hierbei heißt q der **Quotient** bei Division von a durch n und r der **Rest** bei Division von a durch n.

Bew: Idee: Subtrahiere von $a > 0$ solange n, bis eine Zahl zwischen 0 und $n-1$ übrigbleibt.

Setze $\quad q := \left\lfloor \frac{a}{n} \right\rfloor \quad$ und $\quad r := a - qn$.

Dann gilt: $q, r \in \mathbb{Z}$ und $a = qn + r$. Noch z.z.: $0 \le r < n$.

Für alle $x \in \mathbb{R}$ gilt: $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$, woraus $0 \le x - \lfloor x \rfloor < 1$ folgt. Für $x = \frac{a}{n}$ ergibt sich dann: $\quad 0 \le \frac{a}{n} - \left\lfloor \frac{a}{n} \right\rfloor = \frac{a}{n} - q < 1 \quad \Big| \cdot n \quad \Longrightarrow \quad 0 \le \underbrace{a - qn}_{=r} < n$

Bezeichnungen: Gelte $a = qn + r$ mit $0 \le r < n$. Dann setzen wir $q =: a \text{ div } n$ und $r =: a \bmod n$.

(9.7) FOLG: Für $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ gilt: $n|a \iff a \bmod n = 0$

Eine rationale Zahl r ist ein Bruch zweier ganzer Zahlen

$$r = \frac{a}{b} \qquad (a, b \in \mathbb{Z}, b \ne 0)$$

Für jede rationale Zahl gibt es unendlich viele solcher Darstellungen der Form

$$r = \frac{ak}{bk} \qquad (k \in \mathbb{Z} \setminus \{0\})$$

Um zu einer möglichst einfachen Darstellung zu kommen, kürzt man gemeinsame Faktoren von Zähler und Nenner heraus, z.B.

$$\frac{36}{42} = \frac{\cancel{2} \cdot 18}{\cancel{2} \cdot 21} = \frac{\cancel{3} \cdot 6}{\cancel{3} \cdot 7} = \frac{6}{7}$$

Die Zahlen 6 und 7 haben jetzt keinen gemeinsamen Teiler $\ne \pm 1$, sie sind teilerfremd. Mit einem Schlage erhält man diese Darstellung, indem man den größten gemeinsamen Teiler von Zähler und Nenner herauskürzt. Man kommt dann zu der eindeutigen Darstellung einer rationalen Zahl

$$r = \frac{c}{d} \quad \text{mit } c \in \mathbb{Z}, d \in \mathbb{N}, \ c \text{ und } d \text{ teilerfremd}$$

Die folgende Definition für den ggT ist so formuliert, daß sie leicht auf andere Bereiche (z.B. für Polynome) übertragen werden kann.

(9.8) DEF: Seien a und b ganze Zahlen. Eine Zahl $g \in \mathbb{Z}$ heißt **größter gemeinsamer Teiler** (ggT) von a und b, wenn folgendes gilt:

i) $g \geq 0$

ii) $g \mid a$ und $g \mid b$

iii) $\forall\, t \in \mathbb{Z} \;:\; t \mid a$ und $t \mid b \implies t \mid g$

Bezeichnung: $g = \mathrm{ggT}(a, b)$

(9.9) BEM: a) i) liefert die Eindeutigkeit des ggT's (s.b)) , ii) bedeutet, daß g ein **gemeinsamer Teiler** von a und b ist und iii) besagt, daß g von jedem gemeinsamen Teiler von a und b geteilt wird.

b) Zu $a, b \in \mathbb{Z}$ gibt es höchstens einen ggT.

Bew: Seien g und g' ggT's von a und b. Dann folgt aus (9.8), daß g und g' sich gegenseitig teilen, woraus nach (9.3c) $|g| = |g'|$ folgt. Wegen i) ergibt sich hieraus $g = g'$.

c) Im Falle $g = \mathrm{ggT}(a, b) \neq 0$ ist g auch wirklich der größte unter den gemeinsamen Teilern von a und b .

Bew: Ist $t \in \mathbb{Z}$ ein beliebiger gemeinsamer Teiler von a und b, so folgt aus iii) $t \mid g$, woraus sich mit (1.3b) ergibt $t \leq |t| \leq |g| = g$.

d) $\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$

e) $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$

f) $\mathrm{ggT}(a, b) = |a| \iff a \mid b$.

Im folgenden zeigen wir, daß zu je zwei ganzen Zahlen stets der ggT existiert. Dies geschieht dadurch, daß wir ein Verfahren zur Berechnung des ggT's angeben (euklidischer Algorithmus). Das folgende Lemma ist Grundlage für eine Berechnungsmethode des ggT's:

(9.10) LEMMA: Seien $a, b, q, r \in \mathbb{Z}$ mit $a = qb + r$. Dann gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, r)$.

Im Falle $b > 0$ gilt insbesondere $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a \bmod b)$

Bew: Die Aussage ist so zu verstehen, daß $\mathrm{ggT}(b, r)$ existiert und gleich $\mathrm{ggT}(a, b)$ ist, wenn $\mathrm{ggT}(a, b)$ existiert und umgekehrt.

Gezeigt wird, daß die Zahlenpaare (a, b) und (b, r) dieselben gemeinsamen Teiler haben.

Für ein beliebiges $t \in \mathbb{Z}$ mit $t \mid a$ und $t \mid b$ folgt mit (9.3f) auch $t \mid (a - qb)$, d.h. $t \mid r$. Umgekehrt folgt aus $t \mid b$ und $t \mid r$ auch $t \mid (qb + r)$, also $t \mid a$.

Existiere nun $g := \mathrm{ggT}(a, b)$. Dann gilt **i)** $g \geq 0$.

ii) Nach obiger Überlegung ist g auch ein gemeinsamer Teiler von b und r .

iii) Sei $t \in \mathbb{Z}$ ein beliebiger gemeinsamer Teiler von b und r. Dann ist t auch ein gemeinsamer Teiler von a und b, also $t \mid g$, da $g := \mathrm{ggT}(a, b)$.

Damit ist g auch ggT von b und r. Die Umkehrung geht analog. Ξ

Beispiel: Wir wollen den ggT von $a = 48$ und $b = 18$ berechnen.

Division mit Rest ergibt $48 = 2 \cdot 18 + 12$, also $\text{ggT}(48, 18) = \text{ggT}(18, 12)$ nach (9.10)

Division mit Rest ergibt $18 = 1 \cdot 12 + 6$, also $\text{ggT}(18, 12) = \text{ggT}(12, 6)$ nach (9.10).

Nun gilt nach (1.9f) $\text{ggT}(12, 6) = 6$, da $6 \mid 12$.

Insgesamt erhalten wir: $\text{ggT}(48, 18) \;=\; \text{ggT}(18, 12) \;=\; \text{ggT}(12, 6) \;=\; 6$,

womit wir den ggT berechnet haben. Wir werden sehen, daß dieses Verfahren immer den ggT zweier ganzer Zahlen liefert (euklidischer Algorithmus). Indem wir die Divisionsgleichungen jeweils nach dem Rest auflösen und in die vorhergehende Gleichung einsetzen, erhalten wir

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ &= 18 - (48 - 2 \cdot 18) \;=\; 3 \cdot 18 - 48 \end{aligned}$$

Damit haben wir den ggT von 48 und 18 als ganzzahlige Linearkombination von 48 und 18 dargestellt:

$$6 \;=\; \text{ggT}(48, 18) \;=\; (-1) \cdot 48 + 3 \cdot 18$$

Auch diese Möglichkeit der Darstellung des ggT's ist immer gegeben, wie wir gleich sehen werden.

(9.11) Der erweiterte euklidische Algorithmus

Seien $a, b \in \mathbb{N}$. Die Folgen $(r_k)_{k \geq 0}$, $(q_k)_{k \geq 1}$, $(x_k)_{k \geq 0}$, $(y_k)_{k \geq 0}$ seien rekursiv definiert durch:

$r_0 := a$, $r_1 := b$. Für $k \in \mathbb{N}_0$ sei q_{k+1} der Quotient und r_{k+2} der Rest bei Division von r_k durch r_{k+1} , falls $r_{k+1} \neq 0$, d.h.

$$(\star) \quad r_k \;=\; q_{k+1} \cdot r_{k+1} + r_{k+2} \quad \text{mit} \quad 0 \leq r_{k+2} < r_{k+1}$$

$$x_0 := 1 \;,\; x_1 := 0 \qquad (\star\star) \quad x_{k+1} := x_{k-1} - q_k \cdot x_k \quad \forall\, k \geq 1$$

$$y_0 := 0 \;,\; y_1 := 1 \qquad (\star\star\star) \quad y_{k+1} := y_{k-1} - q_k \cdot y_k \quad \forall\, k \geq 1$$

Dann gilt :

a) $\forall\, k \geq 0 \;:\; r_k \;=\; x_k \cdot a + y_k \cdot b$

b) Es gibt eine Zahl $m \in \mathbb{N}$ mit $r_m \neq 0$ und $r_{m+1} = 0$, und es ist

$$r_m \;=\; \text{ggT}(a, b) \;=\; x_m \cdot a + y_m \cdot b$$

BEM: Zur Berechnung des ggT's mit Hilfe des einfachen **euklidischen Algorithmus (EA)** benötigt man nur die beiden Hilfsfolgen $(r_k)_{k \geq 0}$ und $(q_k)_{k \geq 1}$. Der **erweiterte euklidische Algorithmus (EEA)** liefert zusätzlich die Darstellung des ggT's von a und b als ganzzahlige Linearkombination der beiden Zahlen a und b .

Bew: **a)** Wir führen Induktion nach $k \in \mathbb{N}_0$:

(IA) $\underline{k=0}$ $\quad x_0 \cdot a + y_0 \cdot b \;=\; 1 \cdot a + 0 \cdot b \;=\; a \;=\; r_0$

$\underline{k=1}$ $\quad x_1 \cdot a + y_1 \cdot b \;=\; 0 \cdot a + 1 \cdot b \;=\; b \;=\; r_1$

(IV) Sei $k \in \mathbb{N}$ beliebig und gelte die Behauptung für $k-1$ und k, d.h.

$r_{k-1} = x_{k-1}a + y_{k-1}b \qquad$ und $\qquad r_k = x_k a + y_k b$

(IB) $r_{k+1} = x_{k+1}a + y_{k+1}b$

Nach $(\star)$ für $k-1$ gilt $\; r_{k+1} \;=\; r_{k-1} - q_k r_k$. Setzt man für r_{k-1} und r_k die IV ein, so erhält man:

$$\begin{aligned} r_{k+1} &= (x_{k-1}a + y_{k-1}b) - q_k(x_k a + y_k b) \\ &= \underbrace{(x_{k-1} - q_k x_k)}_{=x_{k+1} \quad (\star\star)} a + \underbrace{(y_{k-1} - q_k y_k)}_{=y_{k+1} \quad (\star\star\star)} b \\ &= x_{k+1}a + y_{k+1}b \end{aligned}$$

b) Wir führen wiederholte Division mit Rest aus. Dies ist solange möglich, wie die Zahl, durch die geteilt ist, von 0 verschieden ist.

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_0 &= q_1 \cdot r_1 + r_2 \quad \text{mit} \quad 0 \le r_2 < r_1 \\ r_1 &= q_2 \cdot r_2 + r_3 \quad \text{mit} \quad 0 \le r_3 < r_2 \\ r_2 &= q_3 \cdot r_3 + r_4 \quad \text{mit} \quad 0 \le r_4 < r_3 \\ &\vdots \\ r_k &= q_{k+1} \cdot r_{k+1} + r_{k+2} \quad \text{mit} \quad 0 \le r_{k+2} < r_{k+1} \\ &\vdots \end{aligned}$$

Annahme: $\quad r_k > 0 \quad \forall\, k \ge 2. \qquad$ Dann folgt $\quad b = r_1 > r_2 > r_3 > r_4 > \ldots > r_k > \ldots > 0$

d.h. es gibt unendlich viele natürliche Zahlen $< b$. Widerspruch!

Folglich gibt es ein $m \in \mathbb{N}$ mit $r_{m+1} = 0$ und $r_m \neq 0$. Zu zeigen bleibt, daß r_m wirklich der ggT von a und b ist. Dazu schreiben wir noch einmal das Divisionsschema auf:

$$\begin{aligned} r_0 &= a \\ r_1 &= b \\ r_0 &= q_1 \cdot r_1 + r_2 \quad \text{mit} \quad 0 < r_2 < r_1 \\ r_1 &= q_2 \cdot r_2 + r_3 \quad \text{mit} \quad 0 < r_3 < r_2 \\ r_2 &= q_3 \cdot r_3 + r_4 \quad \text{mit} \quad 0 < r_4 < r_3 \\ &\vdots \\ r_k &= q_{k+1} \cdot r_{k+1} + r_{k+2} \quad \text{mit} \quad 0 < r_{k+2} < r_{k+1} \\ &\vdots \\ r_{m-2} &= r_{m-1} \cdot q_{m-1} + r_m \quad \text{mit} \quad 0 < r_m < r_{m-1} \\ r_{m-1} &= r_m \cdot q_m + \underbrace{r_{m+1}}_{=0} \end{aligned}$$

Aus der letzten Gleichung folgt $r_m \,|\, r_{m-1}$, so daß nach (9.9f) gilt: $\quad r_m = \mathrm{ggT}(r_m, r_{m-1})$. Mit (9.10) und den obigen Gleichungen ergibt sich

$$\underline{\underline{\mathrm{ggT}(a,b)}} \;=\; \mathrm{ggT}(r_0,r_1) \;=\; \mathrm{ggT}(r_1,r_2) \;=\; \mathrm{ggT}(r_2,r_3) \;=\; \ldots \;=\; \mathrm{ggT}(r_{m-1},r_m) \;=\; \underline{\underline{r_m}}$$

Die Darstellung des ggT's ergibt sich unmittelbar aus a). Danach gilt

$$\underline{\underline{\mathrm{ggT}(a,b)}} = r_m = \underline{\underline{x_m \cdot a + y_m \cdot b}} \quad \text{mit} \quad x_m, y_m \in \mathbb{Z}$$

Ξ

Beispiel: Seien $a := 3473$, $b := 1311$. Es sollen der ggT und die Darstellung des ggT's bestimmt werden.

(EA)

k	$r_{k-2} = q_{k-1} r_{k-1} + r_k$	
0	$r_0 = a$	$r_0 = 3473$
1	$r_1 = b$	$r_1 = 1311$
2	$r_0 = q_1 \cdot r_1 + r_2$	$3473 = 2 \cdot 1311 + 851$
3	$r_1 = q_2 \cdot r_2 + r_3$	$1311 = 1 \cdot 851 + 460$
4	$r_2 = q_3 \cdot r_3 + r_4$	$851 = 1 \cdot 460 + 391$
5	$r_3 = q_4 \cdot r_4 + r_5$	$460 = 1 \cdot 391 + 69$
6	$r_4 = q_5 \cdot r_5 + r_6$	$391 = 5 \cdot 69 + 46$
7	$r_5 = q_6 \cdot r_6 + r_7$	$69 = 1 \cdot 46 + \boxed{23}$
8	$r_6 = q_7 \cdot r_7 + r_8$	$46 = 2 \cdot 23 + 0$

Es ist also $r_8 = 0$. Folglich $\boxed{23 = r_7 = \mathrm{ggT}(3473, 1311)}$

(EEA)

k	0	1	2	3	4	5	6	7	8
r_k	3473	1311	851	460	391	69	46	$\boxed{\boxed{23}}$	0
q_k	–	2	1	1	1	5	1	2	–
x_k	1	0	1	−1	2	−3	17	$\boxed{-20}$	–
y_k	0	1	−2	3	−5	8	−45	$\boxed{53}$	–

$$\boxed{23 = \mathrm{ggT}(3473, 1311) = (-20) \cdot 3473 + 53 \cdot 1311}$$

Aus (9.11) erhält man nun das folgende Ergebnis:

(9.12) SATZ: Zu je zwei ganzen Zahlen a und b existiert der eindeutig bestimmte ggT. Außerdem gibt es Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = x \cdot a + y \cdot b$. (Diese Zahlen x und y sind nicht eindeutig bestimmt).

Bew: 1. Fall: $a, b \in \mathbb{N}$ Die Behauptung ergibt sich aus (9.11) und (9.9b)

2. Fall: $a = 0, b \in \mathbb{Z}$ bel. Hier gilt $\mathrm{ggT}(a,b) = |b| = 0 \cdot a + \mathrm{sign}\,(b) \cdot b$

3. Fall: $a \in \mathbb{Z}$ bel. $, b = 0$ Hier gilt $\mathrm{ggT}(a,b) = |a| = \mathrm{sign}\,(a) \cdot a + 0 \cdot b$

4. Fall: $a, b \in \mathbb{Z}$ bel. Nach (9.9d) gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(|a|,|b|)$, und $\mathrm{ggT}(|a|,|b|)$ existiert nach den vorherigen Fällen, da $|a|, |b| \in \mathbb{N}_0$. Außerdem gibt es $x', y' \in \mathbb{Z}$ mit

$$\begin{aligned} \underline{\underline{\mathrm{ggT}(a,b)}} &= \mathrm{ggT}(|a|,|b|) = x' \cdot |a| + y' \cdot |b| = \underbrace{(x' \cdot \mathrm{sign}\,(a))}_{=:x} \cdot a + \underbrace{(y' \cdot \mathrm{sign}\,(b))}_{=:y} \cdot b \\ &= \underline{\underline{x \cdot a + y \cdot b}} \quad \text{mit } x, y \in \mathbb{Z} \end{aligned}$$