§ 4. ggT und kgV

(4.1) DEF: Eine ganze Zahl g heißt **größter gemeinsamer Teiler (ggT)** zweier ganzer Zahlen a und b, wenn gilt:

GGT$_0$) $g \geq 0$

GGT$_1$) $g \mid a$ und $g \mid b$

GGT$_2$) Für alle $t \in Z$ mit $t \mid a$ und $t \mid b$ folgt $t \mid g$.

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

GGT$_0$) hat die Eindeutigkeit des ggT's zur Folge (s. Bem. (4.2)).

GGT$_1$) besagt, daß g ein gemeinsamer Teiler von a und b ist.

GGT$_2$) bedeutet, daß g von jedem gemeinsamen Teiler von a und b geteilt wird.

(4.2) BEM: Zu je zwei ganzen Zahlen gibt es höchstens einen ggT.

(4.3) SATZ: Zu je zwei ganzen Zahlen a und b existiert immer ein eindeutig bestimmter ggT g, und es gibt $x, y \in \mathbb{Z}$ mit der Eigenschaft

$$g = xa + yb,$$

(d.h. g läßt sich als **ganzzahlige Linearkombination** von a und b darstellen).

Bew: **1) Eindeutigkeit** folgt aus (4.2)

2) Existenz Seien $a, b \in \mathbb{Z}$. Da $\mathbb{Z}$ ein HIB ist, ist das Summenideal $\mathbb{Z}a + \mathbb{Z}b$ ein Hauptideal, d.h. es gibt (genau ein) $g \in \mathbb{N}_0$ mit der Eigenschaft

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}g.$$

GGT$_1$) und GGT$_2$) folgen dann sofort mit Hilfe von (3.17).

Wegen $g \in \mathbb{Z}a + \mathbb{Z}b$ ergibt sich dann die behauptete Darstellung für g. •

(4.4) LEMMA: **Rechenregeln für den ggT**

Für alle $a, b \in \mathbb{Z}$ gilt:

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

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

c) $\mathrm{ggT}(a, 0) = |a|$

d) $\mathrm{ggT}(0, 0) = 0$

e) $\mathrm{ggT}(a, b) = 0 \iff (a = b = 0)$

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

(4.5) BEM: zur Namensgebung "ggT":

Für $a, b \in \mathbb{Z}$ sei $GT^+(a,b) := T^+(a) \cap T^+(b)$ die Menge der nichtnegativen gemeinsamen Teiler. Im Falle $a, b \in \mathbb{N}$ ist $GT^+(a,b)$ endlich und nichtleer und besitzt daher ein bzgl. $\leq$ größtes Element. Dieses ist gerade

$$\mathrm{ggT}(a,b) \;=\; \max((GT^+(a,b), \leq)) \,.$$

Dagegen gilt im Falle $a = b = 0$

$$GT^+(a,b) \;=\; T^+(a) \cap T^+(b) \;=\; \mathbb{N}_0 \cap \mathbb{N}_0 \;=\; \mathbb{N}_0 \,,$$

d.h. $\mathrm{ggT}(a,b) = 0$ ist nicht mehr die (bzgl. $\leq$) größte Zahl in der Menge der (nichtnegativen) gemeinsamen Teiler von a und b.

In der geordneten Menge $(\mathbb{N}_0, |\,)$ ist jedoch $\mathrm{ggT}(a,b)$ für alle $a, b \in \mathbb{N}_0$ das (bzgl. $|$) größte Element in der Menge der nichtnegativen gemeinsamen Teiler von a und b, d.h.

$$\mathrm{ggT}(a,b) \;=\; \max((GT^+(a,b), |\,)) \,.$$

Das Nullelement spielt also keine Sonderrolle mehr.

Ein effizientes Verfahren zur Berechnung des ggT's zweier natürlicher Zahlen liefert der allen bekannte **euklidische Algorithmus (EA)**. Grundlage dafür ist das folgende

(4.6) LEMMA: Für $a \in \mathbb{Z}$ und $b \in \mathbb{N}$ gilt $\mathrm{ggT}(a,b) = \mathrm{ggT}(b, a \bmod b)$.

(4.7) Der euklidische Algorithmus (EA)

Seien $a, b \in \mathbb{N}$. Die Folgen $(r_k)_{k \geq 0}$, $(q_k)_{k \geq 1}$ 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.

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

Dann gibt es eine Zahl $n \in \mathbb{N}$ mit $r_n \neq 0$ und $r_{n+1} = 0$, wobei gilt

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

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

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

Annahme: $r_k > 0$ für alle $k \ge 2$. Dann folgt $b = r_1 > r_2 > r_3 > r_4 > \ldots > r_k > \ldots > 0$, d.h. es gibt unendlich viele natürliche Zahlen $< b$. **Widerspruch!** Folglich gibt es ein $n \in \mathbb{N}$ mit $r_{n+1} = 0$ und $r_n \neq 0$. Die letzten beiden Gleichungen des obigen Schemas lauten damit

$$\begin{array}{rcll}
r_{n-2} &=& q_{n-1} \cdot r_{n-1} + r_n & \text{mit} \quad 0 \le r_n < r_{n-1} \\
r_{n-1} &=& q_n \cdot r_n &
\end{array}$$

Mit Hilfe von (4.6) ergibt sich nun

$$\mathrm{ggT}(a,b) = \mathrm{ggT}(r_0, r_1) = \mathrm{ggT}(r_1, r_2) = \ldots = \mathrm{ggT}(r_{n-2}, r_{n-1}) = \mathrm{ggT}(r_{n-1}, r_n) = r_n \,.$$

Dabei gilt die letzte Gleichheit wegen $r_n \mid r_{n-1}$. •

Eine Modifizierung des EA zum erweiterten euklidischen Algorithmus ermöglicht es, auch Koeffizienten für die Darstellung des ggT's als ganzzahlige Linearkombination zu berechnen:

(4.8) Der erweiterte euklidische Algorithmus (EEA)

Seien $a, b \in \mathbb{N}$. Die Zahlen r_k und q_k seien wie in (4.7) definiert, dh .

$(\star)$ $$r_k = q_{k+1} \cdot r_{k+1} + r_{k+2} \quad (0 \le r_{k+2} < r_{k+1})$$

Die Folgen $(x_k)_{k \ge 0}$ und $(y_k)_{k \ge 0}$ seien rekursiv definiert durch

$x_0 := 1 \,,\; x_1 := 0$

$(\star\star)$ $$x_{k+1} := x_{k-1} - q_k \cdot x_k \quad (k \ge 1)$$

$y_0 := 0 \,,\; y_1 := 1$

$(\star\star\star)$ $$y_{k+1} := y_{k-1} - q_k \cdot y_k \quad (k \ge 1)$$

Dann gilt $$r_k = x_k \cdot a + y_k \cdot b \quad \text{für alle } k \in \mathbb{N}_0$$

und insbesondere für $k = n$

$$\mathrm{ggT}(a,b) \;=\; r_n \;=\; x_n \cdot a + y_n \cdot b \,,$$

Bew: Die Behauptung läßt sich leicht durch vollständige Induktion nach $k \in \mathbb{N}_0$ beweisen. •

Wir wollen jetzt die Definition des ggT's verallgemeinern:

(4.9) DEF: Eine ganze Zahl g heißt **größter gemeinsamer Teiler (ggT)** von endlich vielen ganzen Zahlen $a_1, a_2, \ldots, a_n$ $(n \geq 2)$, wenn gilt:

GGT$_0$) $g \geq 0$

GGT$_1$) $g \mid a_i$ $(\forall\, i = 1, 2, \ldots, n)$

GGT$_2$) Für alle $t \in Z$ mit $t \mid a_i$ $(\forall\, i = 1, 2, \ldots, n)$ folgt $t \mid g$.

Bezeichnung: $g = \mathrm{ggT}(a_1, a_2, \ldots, a_n)$.

(4.10) SATZ: Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ $(n \geq 2)$. Dann existiert ein eindeutig bestimmter ggT von $a_1, a_2, \ldots, a_n$, und dieser läßt sich als ganzzahlige Linearkombination von $a_1, a_2, \ldots, a_n$ darstellen.

Bew: Die eindeutig bestimmte nichtnegative Zahl g, die das Summenideal

$$\mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n = \{\, x_1a_1 + x_2a_2 + \ldots + x_na_n \mid a_1, a_2, \ldots, a_n \in \mathbb{Z}\,\}$$

erzeugt, ist der ggT von $a_1, a_2, \ldots, a_n$. $g \in \mathbb{Z}a_1 + \mathbb{Z}a_2 + \ldots + \mathbb{Z}a_n$ läßt sich dann aus $a_1, a_2, \ldots, a_n$ ganzzahlig linear kombinieren. •

(4.11) DEF: Seien $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ $(n \geq 2)$.

a) Die Zahlen $a_1, a_2, \ldots, a_n$ heißen **teilerfremd**, wenn $\mathrm{ggT}(a_1, a_2, \ldots, a_n) = 1$ gilt.

b) Die Zahlen $a_1, a_2, \ldots, a_n$ heißen **paarweise teilerfremd**, wenn gilt:

$$\mathrm{ggT}(a_i, a_k) = 1 \ \forall\, i, k \in \{1, 2, \ldots, n\} \text{ mit } i \neq k\,.$$

(4.12) BEM: a) Die Zahlen $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ sind genau dann teilerfremd, wenn es Zahlen $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ gibt mit $x_1a_1 + x_2a_2 + \ldots + x_na_n = 1$.

b) Paarweise teilerfremde Zahlen sind auch teilerfremd, aber nicht umgekehrt.

(4.13) SATZ: Für $a, b, c \in \mathbb{Z}$ gelten die folgenden Aussagen:

a) $a \mid c$ und $b \mid c$ und $\mathrm{ggT}(a, b) = 1 \implies (a \cdot b) \mid c$

b) $a \mid (b \cdot c)$ und $\mathrm{ggT}(a, b) = 1 \implies a \mid c$.

BEM: Ohne die Voraussetzung, daß die Zahlen a und b teilerfremd sind, gelten die obigen Aussagen i.a. nicht:

Gegenbeispiel zu **a)** : $4 \mid 12$ und $6 \mid 12$, aber $4 \cdot 6 = 24$ ist kein Teiler von 12.

b) $6 \mid (4 \cdot 9)$, aber $6 \nmid 4$ und $6 \nmid 9$.

Dual zum Begriff des ggT's definieren wir jetzt den Begriff des kgV's.

(4.14) DEF: Eine ganze Zahl k heißt **kleinstes gemeinsames Vielfaches (kgV)** zweier ganzer Zahlen a und b, wenn gilt:

KGV$_0$) $k \geq 0$

KGV$_1$) $a \mid k$ und $b \mid k$

KGV$_2$) Für alle $v \in Z$ mit $a \mid v$ und $b \mid v$ folgt $k \mid v$.

Bezeichnung: $k = \mathrm{kgV}(a,b)$.

KGV$_0$) hat die Eindeutigkeit des kgV's zur Folge (s. Bem. (4.15)).

KGV$_1$) besagt, daß k ein gemeinsames Vielfaches von a und b ist.

KGV$_2$) bedeutet, daß k Teiler eines jeden gemeinsamen Vielfachen von a und b ist.

(4.15) BEM: Zu je zwei ganzen Zahlen a und b gibt es höchstens ein kgV.

(4.16) SATZ: Zu je zwei ganzen Zahlen existiert ein eindeutig bestimmtes kgV.

Bew: **1) Eindeutigkeit** folgt aus (4.15)

2) Existenz Seien $a, b \in \mathbb{Z}$. Da $\mathbb{Z}$ ein HIB ist, ist das Ideal $\mathbb{Z}a \cap \mathbb{Z}b$ ein Hauptideal, d.h. es gibt (genau ein) $k \in \mathbb{N}_0$ mit der Eigenschaft

$$\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}k .$$

KGV$_1$) und KGV$_2$) folgen dann sofort mit Hilfe von (3.17), d.h.

$$k = \mathrm{kgV}(a,b) .$$

•

(4.17) LEMMA: Rechenregeln für das kgV

Für alle $a, b \in \mathbb{Z}$ gilt:

a) $\mathrm{kgV}(a,b) = \mathrm{kgV}(b,a)$	**b)** $\mathrm{kgV}(a,b) = \mid a \mid \iff b \mid a$
c) $\mathrm{kgV}(a,0) = 0$	**d)** $\mathrm{kgV}(0,0) = 0$
e) $\mathrm{kgV}(a,b) = 0 \iff (a = 0 \vee b = 0)$	**f)** $\mathrm{kgV}(a,b) = \mathrm{kgV}(\mid a \mid, \mid b \mid)$

(4.18) BEM: Für beliebige ganze Zahlen a, b bezeichne $GV^+(a,b) := V^+(a) \cap V^+(b) \subseteq \mathbb{N}_0$ die Menge der nichtnegativen gemeinsamen Vielfachen von a und b. Es sei $k := \mathrm{kgV}(a,b)$. Im Falle $a = 0$ oder $b = 0$ ist $0 = k = \min(GV^+(a,b), \leq)$. Im Falle $a \neq 0$ und $b \neq 0$ ist dagegen $k > 0$ und deshalb

$$k := \min((GV^+(a,b) \cap \mathbb{N}, \leq)) .$$

Für alle $a, b \in \mathbb{Z}$ gilt aber $k = \min((GV^+(a,b), \mid))$.

(4.19) DEF: $a_1, a_2, \dots, a_n$ $(n \geq 2)$ seien ganze Zahlen. Eine ganze Zahl k heißt **kleinstes gemeinsames Vielfaches (kgV) von** $a_1, a_2, \dots, a_n$, wenn gilt:

KGV$_0$) $k \geq 0$

KGV$_1$) $a_1 \,|\, k$, $a_2 \,|\, k$, $\dots$, $a_n \,|\, k$

KGV$_2$) Für alle $v \in \mathbb{Z}$ mit $a_1 \,|\, v$, $a_2 \,|\, v$, $\dots$, $a_n \,|\, v$ folgt $k \,|\, v$.

Bezeichnung: $k = \mathrm{kgV}(a_1, a_2, \dots, a_n)$

(4.20) SATZ: Zu je n ganzen Zahlen existiert immer ein eindeutig bestimmtes kgV .

Bew: Die Zahl $k \in \mathbb{N}_0$ mit $\mathbb{Z}a_1 \cap \mathbb{Z}a_2 \cap \ldots \cap \mathbb{Z}a_n = (k)$ ist kgV von $a_1, a_2, \dots, a_n$. •

(4.21) BEM: Sind $r_1 = \dfrac{a_1}{b_1}, r_2 = \dfrac{a_2}{b_2}, \dots, r_n = \dfrac{a_n}{b_n}$ rationale Zahlen, so ist ihr **Hauptnenner** gerade das kgV der einzelnen Nenner $b_1, b_2, \dots, b_n$. Diese Bildung ist wichtig für die Addition rationaler Zahlen. Ist $k = \mathrm{kgV}(b_1, b_2, \dots, b_n)$ und gilt $b_i \cdot c_i = k$ für alle $i = 1, 2, \dots, n$, so folgt

$$r_1 + r_2 + \ldots + r_n \;=\; \frac{a_1}{b_1} + \frac{a_2}{b_2} + \ldots + \frac{a_n}{b_n} \;=\; \frac{a_1 \cdot c_1 + a_2 \cdot c_2 + \ldots + a_n \cdot c_n}{k} \,.$$

Zum Abschluß untersuchen wir den Zusammenhang zwischen dem ggT und dem kgV zweier ganzer Zahlen:

(4.22) SATZ: Für ganze Zahlen a und b gilt

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) \;=\; |\, a \cdot b \,| \,.$$

Bew: Es genügt, die Behauptung für $a > 0$ und $b > 0$ zu beweisen.
Ist $k = \mathrm{kgV}(a,b)$, so folgt $k \,|\, a \cdot b$. Für den zu k komplementären Teiler g von $a \cdot b$ läßt sich $g = \mathrm{ggT}(a,b)$ zeigen. Folglich gilt $g \cdot k = a \cdot b$. •

(4.23) BEM: **Berechnungsverfahren für das kgV**

Sind a und b ganze Zahlen , für die $\mathrm{ggT}(a,b) \neq 0$ gilt, so folgt

$$\mathrm{kgV}(a,b) \;=\; \frac{|\, a \cdot b \,|}{\mathrm{ggT}(a,b)} \,,$$

wobei sich $\mathrm{ggT}(a,b)$ (leicht!) mit Hilfe des euklidischen Algorithmus berechnen läßt .