Sebastian Thomas

RWTH Aachen, WS 2016/17
24.11.2016–30.11.2016

Diskrete Strukturen

Vorlesungen 11 und 12 (vorläufig, wird fortgesetzt)

10 Teilbarkeitslehre

Ziel dieses Abschnitts ist es zu sehen, dass es starke formale Ähnlichkeiten zwischen dem Ring der ganzen Zahlen $\mathbb{Z}$ und dem Polynomring $K[X]$ über einem Körper K gibt.

Division mit Rest

Wir beginnen mit der (zumindest in Spezialfällen aus der Schule bekannten) Division mit Rest, für welche es sowohl eine Version für ganze Zahlen als auch für Polynome mit Koeffizienten in einem Körper gibt.

(10.1) Satz (Ganzzahldivision, Polynomdivision)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $\mathbb{Z}$ rekursiv definiert durch

$$q_i := \begin{cases} 0, & \text{für } i = 0, \\ q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b), & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1], \end{cases}$$

$$r_i := \begin{cases} a, & \text{für } i = 0, \\ r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin [0, |b| - 1], \\ r_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in [0, |b| - 1]. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$a = q_i b + r_i.$$

(ii) Es existiert ein $n \in [0, \max(0, |a| - |b| + 1)]$ mit $r_n \in [0, |b| - 1]$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$.

(b) Es seien ein Körper K und $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Ferner seien Folgen $(q_i)_{i\in\mathbb{N}_0}$ und $(r_i)_{i\in\mathbb{N}_0}$ in $K[X]$ rekursiv definiert durch

$$q_i := \begin{cases} 0, & \text{für } i = 0, \\ q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}, \end{cases}$$

$$r_i := \begin{cases} f, & \text{für } i = 0, \\ r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \notin K[X]_{<\deg g}, \\ r_{i-1}, & \text{für } i \in \mathbb{N} \text{ mit } r_{i-1} \in K[X]_{<\deg g}. \end{cases}$$

(i) Für alle $i \in \mathbb{N}_0$ gilt

$$f = q_i g + r_i.$$

(ii) Es existiert ein $n \in \mathbb{N}_0$ mit $r_n \in K[X]_{<\deg g}$ und $q_i = q_n$, $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \neq 0$ ist, dann kann $n \in \mathbb{N}_0$ so gewählt werden, dass zusätzlich $n \leq \max(0, \deg f - \deg g + 1)$ gilt.

Beweis.

(a) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i b + r_i = q_0 b + r_0 = 0 \cdot b + a = a.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $a = q_{i-1} b + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i b + r_i &= \begin{Bmatrix} (q_{i-1} + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b))b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1} b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1} b + (\operatorname{sgn} r_{i-1})(\operatorname{sgn} b)b + r_{i-1} - (\operatorname{sgn} r_{i-1})|b|, & \text{falls } r_{i-1} \notin [0, |b| - 1], \\ q_{i-1} b + r_{i-1}, & \text{falls } r_{i-1} \in [0, |b| - 1] \end{Bmatrix} \\ &= q_{i-1} b + r_{i-1} = a. \end{aligned}$$

Nach dem Induktionsprinzip gilt $a = q_i b + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin [0, |b| - 1]$ gegeben. Dann gilt

$$\begin{aligned} |r_i| = |r_{i-1} - (\operatorname{sgn} r_{i-1})|b|| &= \begin{Bmatrix} |r_{i-1} - |b||, & \text{falls } r_{i-1} > 0, \\ |r_{i-1} + |b||, & \text{falls } r_{i-1} < 0 \end{Bmatrix} = \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} > 0, \\ -(r_{i-1} + |b|), & \text{falls } r_{i-1} < 0 \end{Bmatrix} \\ &= \begin{Bmatrix} r_{i-1} - |b|, & \text{falls } r_{i-1} > 0, \\ -r_{i-1} - |b|, & \text{falls } r_{i-1} < 0 \end{Bmatrix} = |r_{i-1}| - |b| < |r_{i-1}|. \end{aligned}$$

Für $i \in \mathbb{N}$ mit $r_{i-1} \in [0, |b| - 1]$ gilt hingegen $r_i = r_{i-1}$ und damit $r_i \in [0, |b| - 1]$.
Falls $a \notin [0, |b| - 1]$ ist, erhalten wir induktiv $r_{|a|-|b|+1} \in [0, |b| - 1]$. Falls hingegen $a \in [0, |b| - 1]$ ist, gilt $r_0 = a \in [0, |b| - 1]$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in [0, |b| - 1]\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $a \notin [0, |b| - 1]$ ist, gilt $n \leq |a| - |b| + 1$, und wenn $a \in [0, |b| - 1]$ ist, gilt $n = 0$. Insgesamt gilt also stets $n \leq \max(0, |a| - |b| + 1)$ und damit $n \in [0, \max(0, |a| - |b| + 1)]$.

(b) (i) Wir führen Induktion nach i. Für $i = 0$ gilt

$$q_i g + r_i = q_0 g + r_0 = 0 \cdot g + f = f.$$

Nun sei $i \in \mathbb{N}$ so gegeben, dass $f = q_{i-1} g + r_{i-1}$ gilt. Dann erhalten wir auch

$$\begin{aligned} q_i g + r_i &= \begin{Bmatrix} (q_{i-1} + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g})g \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1} g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= \begin{Bmatrix} q_{i-1} g + \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g \\ \qquad + r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g, & \text{falls } r_{i-1} \notin K[X]_{<\deg g}, \\ q_{i-1} g + r_{i-1}, & \text{falls } r_{i-1} \in K[X]_{<\deg g} \end{Bmatrix} \\ &= q_{i-1} g + r_{i-1} = f. \end{aligned}$$

Nach dem Induktionsprinzip gilt $f = q_i g + r_i$ für alle $i \in \mathbb{N}_0$.

(ii) Zunächst sei $i \in \mathbb{N}$ mit $r_{i-1} \notin K[X]_{<\deg g}$ gegeben. Dann gilt

$$\begin{aligned} \deg(\operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g) &= \deg X^{\deg r_{i-1} - \deg g} + \deg g \\ &= \deg r_{i-1} - \deg g + \deg g = \deg r_{i-1} \end{aligned}$$

nach Bemerkung (9.7)(b) und damit $r_i = 0$ oder $r_i \neq 0$ und

$$\begin{aligned} \deg r_i &= \deg(r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g) \\ &\leq \max(\deg r_{i-1}, \deg(\operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g)) = \deg r_{i-1} \end{aligned}$$

nach Bemerkung (9.7)(a). Da der Koeffizient von $r_i = r_{i-1} - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} X^{\deg r_{i-1} - \deg g} g$ an der Stelle $\deg r_{i-1}$ durch $\operatorname{lc}(r_{i-1}) - \operatorname{lc}(r_{i-1}) \operatorname{lc}(g)^{-1} \operatorname{lc}(g) = 0$ gegeben ist, gilt sogar $r_i = 0$ oder $r_i \neq 0$ und $\deg r_i < \deg r_{i-1}$, d.h. es ist $r_i \in K[X]_{<\deg r_{i-1}}$.

Für $i \in \mathbb{N}$ mit $r_{i-1} \in K[X]_{<\deg g}$ gilt hingegen $r_i = r_{i-1}$ und damit $r_i \in K[X]_{<\deg g}$.
Falls $f \notin K[X]_{<\deg g}$ ist, erhalten wir induktiv $r_{\deg f - \deg g + 1} \in K[X]_{<\deg g}$. Falls hingegen $f \in K[X]_{<\deg g}$ ist, gilt $r_0 = f \in K[X]_{<\deg g}$. Es sei $n := \min\{i \in \mathbb{N}_0 \mid r_i \in K[X]_{<\deg g}\}$. Per Induktion folgt $q_i = q_n$ und $r_i = r_n$ für $i \in \mathbb{N}_0$ mit $i \geq n$. Wenn $f \notin K[X]_{<\deg g}$ ist, gilt $n \leq \deg f - \deg g + 1$, und wenn $f \in K[X]_{<\deg g} \setminus \{0\}$ ist, gilt $n = 0$. Insgesamt gilt also, sofern $f \neq 0$ ist, stets $n \leq \max(0, \deg f - \deg g + 1)$. □

(10.2) Satz (Division mit Rest)**.**

(a) Für alle $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gibt es eindeutige $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit

$$a = qb + r.$$

(b) Es sei ein Körper K gegeben. Für alle $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gibt es eindeutige $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit

$$f = qg + r.$$

Beweis.

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben. Nach Satz (10.1)(a) gibt es $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ mit $a = qb + r$. Für die Eindeutigkeit seien $q, q' \in \mathbb{Z}$, $r, r' \in [0, |b| - 1]$ mit $x = qb + r = q'b + r'$ gegeben. Dann ist

$$|q - q'|\,|b| = |(q - q')b| = |qb - q'b| = |r' - r| < |b|.$$

Wegen $b \neq 0$ impliziert dies $|q - q'| < 1$, also $|q - q'| = 0$. Folglich ist $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = a - qb = a - q'b = r'$.

(b) Es seien $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben. Nach Satz (10.1)(b) gibt es $q \in K[X]$, $r \in K[X]_{<\deg g}$ mit $f = qg + r$. Für die Eindeutigkeit seien $q, q' \in K[X]$, $r, r' \in K[X]_{<\deg g}$ mit $f = qg + r = q'g + r'$ gegeben. Dann ist

$$(q - q')g = qg - q'g = r' - r \in K[X]_{<\deg g}$$

und damit $(q - q')g = 0$ nach Bemerkung (9.7)(b). Wegen $g \neq 0$ impliziert dies aber bereits $q - q' = 0$, d.h. es gilt $q = q'$ und damit auch $r = f - qg = f - q'g = r'$. □

(10.3) Definition (ganzer Anteil, Rest)**.**

(a) Es seien $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$ gegeben und es seien $q \in \mathbb{Z}$, $r \in [0, |b| - 1]$ die eindeutigen ganzen Zahlen mit $a = qb + r$. Dann heißt $a \operatorname{div} b := q$ der *ganzzahlige Anteil* (oder der *ganze Anteil*) und $a \bmod b := r$ der *Rest* bei der *Ganzzahldivision* von a durch b.

(b) Es seien ein Körper K sowie $f \in K[X]$, $g \in K[X] \setminus \{0\}$ gegeben und es seien $q, r \in K[X]$ die eindeutigen Polynome mit $f = qg + r$ und mit $r = 0$ oder $r \neq 0$, $\deg r < \deg g$. Dann heißt $f \operatorname{div} g := q$ der *ganze Anteil* und $f \bmod g := r$ der *Rest* bei der *Polynomdivision* von f durch g.

(10.4) Beispiel.

(a) In $\mathbb{Z}$ ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) In $\mathbb{Q}[X]$ ist $(6X^3 + X^2 + 7) \operatorname{div} (2X^2 + X - 3) = 3X - 1$ und $(6X^3 + X^2 + 7) \bmod (2X^2 + X - 3) = 10X + 4$.

Beweis.

(a) Eine Ganzzahldivision liefert

$$\begin{aligned} -47 &= 0 \cdot 9 + (-47) = (-1) \cdot 9 + (-38) = (-2) \cdot 9 + (-29) = (-3) \cdot 9 + (-20) = (-4) \cdot 9 + (-11) \\ &= (-5) \cdot 9 + (-2) = (-6) \cdot 9 + 7. \end{aligned}$$

Folglich ist $(-47) \operatorname{div} 9 = -6$ und $(-47) \bmod 9 = 7$.

(b) Eine Polynomdivision liefert

$$\begin{aligned} 6X^3 + X^2 + 7 &= 0 \cdot (2X^2 + X - 3) + 6X^3 + X^2 + 7 = 3X \cdot (2X^2 + X - 3) + (-2X^2 + 9X + 7) \\ &= (3X - 1) \cdot (2X^2 + X - 3) + (10X + 4). \end{aligned}$$

Folglich ist $(6X^3 + X^2 + 7) \operatorname{div} (2X^2 + X - 3) = 3X - 1$ und $(6X^3 + X^2 + 7) \bmod (2X^2 + X - 3) = 10X + 4$. □

Teilbarkeit

Als nächstes studieren wir die Teilbarkeitsrelation in $\mathbb{Z}$ und in $K[X]$ für einen Körper K.

(10.5) Definition (Teilbarkeit)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen a *teilt* b (oder dass a ein *Teiler* von b ist oder dass a ein *Faktor* von b ist oder dass b ein *Vielfaches* von a ist), geschrieben $a \mid b$, falls ein $q \in R$ mit $b = qa$ existiert. Wenn a kein Teiler von b ist, so schreiben wir $a \nmid b$.

(10.6) Beispiel.

(a) In $\mathbb{Z}$ gilt $3 \mid 6$ und $4 \nmid 6$.

(b) In $\mathbb{Q}[X]$ gilt $X - 1 \mid X^2 - 1$ und $X \nmid X^2 - 1$.

Beweis.

(a) Es gilt $6 = 2 \cdot 3$, also $3 \mid 6$. Wegen $6 = 1 \cdot 4 + 2$ gibt es nach dem Satz über die Division mit Rest (10.2)(a) kein $q \in \mathbb{Z}$ mit $6 = q \cdot 4$, so dass $4 \nmid 6$ folgt.

(b) Es gilt $X^2 - 1 = (X + 1)(X - 1)$, also $X - 1 \mid X^2 - 1$. Wegen $X^2 - 1 = X \cdot X + (-1)$ gibt es nach dem Satz über die Division mit Rest (10.2)(b) kein $q \in \mathbb{Q}[X]$ mit $X^2 - 1 = q \cdot X$, so dass $X \nmid X^2 - 1$ folgt. □

(10.7) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R \setminus \{0\}$, $b \in R$ gegeben. Genau dann gilt $a \mid b$, wenn $b \bmod a = 0$ ist.

Beweis. Wenn $a \mid b$ gilt, dann gibt es ein $q \in R$ mit $b = qa = qa + 0$ und nach dem Satz über die Division mit Rest (10.2) folgt $b \bmod a = 0$. Gilt umgekehrt $b \bmod a = 0$, so folgt $b = (b \operatorname{div} a)a + (b \bmod a) = (b \operatorname{div} a)a$ und damit $a \mid b$. □

(10.8) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Die Teilbarkeitsrelation $\mid$ auf R ist eine Präordnung.

Beweis. Es seien $a, b, c \in R$ mit $a \mid b$ und $b \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qb$. Dann folgt

$$c = qb = q(pa) = (qp)a,$$

also $a \mid c$. Folglich ist $\mid$ transitiv.
Für $a \in R$ gilt $a = 1 \cdot a$, also $a \mid a$. Folglich ist $\mid$ reflexiv.
Insgesamt ist $\mid$ eine Präordnung auf R. □

Wir studieren weitere Eigenschaften der Teilbarkeitsrelation.

(10.9) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K.

(a) Für $a, b, c \in R$ gilt: Wenn $a \mid b$ und $a \mid c$, dann auch $a \mid b + c$.

(b) Für $a \in R$ gilt $a \mid 0$.

(c) Für $a, b, c \in R$ gilt: Wenn $a \mid b$, dann auch $a \mid cb$.

Beweis.

(a) Es seien $a, b, c \in R$ mit $a \mid b$ und $a \mid c$ gegeben, d.h. es gebe $p, q \in R$ mit $b = pa$ und $c = qa$. Dann folgt

$$b + c = pa + qa = (p + q)a,$$

also $a \mid b + c$.

(b) Für $a \in R$ gilt $0 = 0 \cdot a$, also $a \mid 0$.

(c) Es seien $a, b, c \in R$ gegeben und es gelte $a \mid b$. Da auch $b \mid cb$ gilt, folgt $a \mid cb$ nach Proposition (10.8). □

Assoziiertheit

Nach Proposition (10.8) ist die Teilbarkeitsrelation | eine Präordnung auf $\mathbb{Z}$ bzw. auf $K[X]$ für einen Körper K. Im Allgemeinen gilt jedoch keine Antisymmetrie, es kann in diesen Ringen Elemente a und b mit $a \mid b$ und $b \mid a$ und $a \neq b$ geben. Wir vergeben folgende Terminologie:

(10.10) Definition (assoziierte Elemente)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Wir sagen, dass a *assoziiert* zu b ist, wenn $a \mid b$ und $b \mid a$ gilt.

(10.11) Beispiel.

(a) In $\mathbb{Z}$ ist 3 assoziiert zu -3.

(b) In $\mathbb{Q}[X]$ ist $X - 1$ assoziiert zu $2X - 2$.

Beweis.

(a) Wegen $-3 = (-1) \cdot 3$ gilt $3 \mid -3$ und wegen $3 = (-1) \cdot (-3)$ gilt $-3 \mid 3$. Folglich ist 3 assoziiert zu -3.

(b) Wegen $2X - 2 = 2(X - 1)$ gilt $X - 1 \mid 2X - 2$ und wegen $X - 1 = \frac{1}{2}(2X - 2)$ gilt $-3 \mid 3$. Folglich ist $X - 1$ assoziiert zu $2X - 2$. □

(10.12) Proposition. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Die folgenden Aussagen sind äquivalent.

(a) Es ist a assoziiert zu b.

(b) Es gibt ein $u \in R^\times$ mit $b = ua$.

(c) Im Fall $R = \mathbb{Z}$ gilt $|a| = |b|$. Im Fall $R = K[X]$ gilt entweder $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$.

Beweis. Zunächst gelte Bedingung (a), d.h. es sei a assoziiert zu b. Dann gilt $a \mid b$ und $b \mid a$, d.h. es gibt $p, q \in R$ mit $b = pa$ und $a = qb$. Wir erhalten

$$a = qb = q(pa) = (qp)a.$$

Da R nach Beispiel (6.51) bzw. nach Korollar (9.9) ein Integritätsbereich ist, folgt $a = 0$ oder $qp = 1$ nach Bemerkung (6.52). Wenn $a = 0$ ist, dann ist $b = pa = 0 = 1 \cdot a$ und es ist $1 \in R^\times$ nach Proposition (6.30)(b) auf Grund der Kommutativität des Rings R. Wenn $qp = 1$ ist, dann ist $p \in R^\times$. In jedem Fall gibt es ein $u \in R^\times$ mit $b = ua$, d.h. es gilt Bedingung (b).
Umgekehrt, wenn Bedingung (b) gilt, d.h. wenn es ein $u \in R^\times$ mit $b = ua$ gibt, dann gilt auch $a = u^{-1}b$ und damit $a \mid b$ und $b \mid a$, d.h. auch Bedingung (a) gilt.
Wir haben gezeigt, dass Bedingung (a) und Bedingung (b) äquivalent sind.
Um zu zeigen, dass Bedingung (b) und Bedingung (c) äquivalent sind, betrachten wir zunächst den Fall $R = \mathbb{Z}$. Dann ist $R^\times = \mathbb{Z}^\times = \{1, -1\}$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $|a| = |b|$ gilt, d.h. Bedingung (b) und Bedingung (c) sind in diesem Fall äquivalent.
Schließlich betrachten wir den Fall $R = K[X]$ für einen Körper K. Dann ist $R^\times = K[X]^\times = K^\times$. Folglich gibt es genau dann ein $u \in R^\times$ mit $b = ua$, wenn $a = b = 0$ oder $\mathrm{lc}(a)^{-1}a = \mathrm{lc}(b)^{-1}b$ gilt, d.h. Bedingung (b) und Bedingung (c) sind auch in diesem Fall äquivalent.
Wir haben gezeigt, dass Bedingung (b) und Bedingung (c) äquivalent sind.
Insgesamt sind Bedingung (a), Bedingung (b) und Bedingung (c) äquivalent. □

Teilbarkeit und Nullstellen von Polynomen

Mit Hilfe der Teilbarkeitsrelation lassen sich Nullstellen von Polynomen über einem Körper charakterisieren:

(10.13) Definition (Linearfaktor)**.** Es seien ein Körper K und ein $f \in K[X]$ gegeben. Ein *Linearfaktor* von f ist ein lineares Polynom über K, welches ein Teiler von f ist.

Ein Linearfaktor eines Polynoms f über einem Körper K ist also ein Polynom von der Form $aX + b$ für gewisse $a \in K \setminus \{0\} = K^\times$, $b \in K$.

(10.14) Proposition. Es seien ein Körper K, $f \in K[X]$ und $a \in K$ gegeben. Genau dann ist a eine Nullstelle von f, wenn $X - a$ ein Linearfaktor von f ist.

Beweis. Es sei $q := f \operatorname{div} (X - a)$ und $r := f \bmod (X - a)$. Dann gilt

$$f = (f \operatorname{div} (X - a)) \cdot (X - a) + f \bmod (X - a) = q \cdot (X - a) + r$$

und damit

$$f(a) = q(a) \cdot (a - a) + r(a) = r(a).$$

Wegen $\deg(X - a) = 1$ ist $r \in K[X]_{<\deg(X-a)} = K[X]_{<1} = K$, also $r = r(a) = f(a)$. Somit ist a genau dann eine Nullstelle von f, wenn $r = 0$ ist, d.h. wenn $X - a$ ein Linearfaktor von f ist. □

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Als nächstes thematisieren wir die aus der Schule bekannten Begriffe des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, wobei wir diese über die Teilbarkeitsrelation definieren.

(10.15) Definition (gemeinsamer Teiler, gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *gemeinsamer Teiler* von a und b ist ein $d \in R$ so, dass $d \mid a$ und $d \mid b$ gilt.

(b) Ein *gemeinsames Vielfaches* von a und b ist ein $m \in R$ so, dass $a \mid m$ und $b \mid m$ gilt.

(10.16) Beispiel.

(a) (i) In $\mathbb{Z}$ sind 1, 2, -6 gemeinsame Teiler von 12 und 18.

(ii) In $\mathbb{Q}[X]$ sind 1, $X + 1$, $2X + 2$ gemeinsame Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.

(b) (i) In $\mathbb{Z}$ sind 12 und -24 gemeinsame Vielfache von 4 und 6.

(ii) In $\mathbb{Q}[X]$ sind $X^3 - X^2 - X + 1$ und $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ gemeinsame Vielfache von $X^2 - 2X + 1$ und $X^2 - 1$.

Beweis.

(a) (i) Wegen $12 = 12 \cdot 1$ gilt $1 \mid 12$ und wegen $18 = 18 \cdot 1$ gilt $1 \mid 18$. Folglich ist 1 ein gemeinsamer Teiler von 12 und 18.
Wegen $12 = 6 \cdot 2$ gilt $2 \mid 12$ und wegen $18 = 9 \cdot 2$ gilt $2 \mid 18$. Folglich ist 2 ein gemeinsamer Teiler von 12 und 18.
Wegen $12 = (-2) \cdot (-6)$ gilt $-6 \mid 12$ und wegen $18 = (-3) \cdot (-6)$ gilt $-6 \mid 18$. Folglich ist -6 ein gemeinsamer Teiler von 12 und 18.

(ii) Wegen $X^2 - 1 = (X^2 - 1) \cdot 1$ gilt $1 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (X^2 + 2X + 1) \cdot 1$ gilt $1 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.
Wegen $X^2 - 1 = (X - 1)(X + 1)$ gilt $X + 1 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (X + 1)(X + 1)$ gilt $X + 1 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.
Wegen $X^2 - 1 = (\frac{1}{2}X - \frac{1}{2})(2X + 2))$ gilt $2X + 2 \mid X^2 - 1$ und wegen $X^2 + 2X + 1 = (\frac{1}{2}X + \frac{1}{2})(2X + 2)$ gilt $2X + 2 \mid X^2 + 2X + 1$. Folglich ist 1 ein gemeinsamer Teiler von $X^2 - 1$ und $X^2 + 2X + 1$.

(b) (i) Wegen $12 = 3 \cdot 4$ gilt $4 \mid 12$ und wegen $12 = 2 \cdot 6$ gilt $6 \mid 12$. Folglich ist 12 ein gemeinsames Vielfaches von 4 und 6.
Wegen $-24 = (-6) \cdot 4$ gilt $4 \mid -24$ und wegen $-24 = (-4) \cdot 6$ gilt $6 \mid -24$. Folglich ist -24 ein gemeinsames Vielfaches von 4 und 6.

(ii) Wegen $X^3 - X^2 - X + 1 = (X + 1) \cdot (X^2 - 2X + 1)$ gilt $X^2 - 2X + 1 \mid X^3 - X^2 - X + 1$ und wegen $X^3 - X^2 - X + 1 = (X - 1) \cdot (X^2 - 1)$ gilt $X^2 - 1 \mid X^3 - X^2 - X + 1$. Folglich ist $X^3 - X^2 - X + 1$ ein gemeinsames Vielfaches von $X^2 - 2X + 1$ und $X^2 - 1$.
Wegen $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2} = (-\frac{1}{2}X^2 + \frac{1}{2}) \cdot (X^2 - 2X + 1)$ gilt $X^2 - 2X + 1 \mid -\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ und wegen $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2} = (-\frac{1}{2}X^2 + X - \frac{1}{2}) \cdot (X^2 - 1)$ gilt $X^2 - 1 \mid -\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$. Folglich ist $-\frac{1}{2}X^4 + X^3 - X + \frac{1}{2}$ ein gemeinsames Vielfaches von $X^2 - 2X + 1$ und $X^2 - 1$. □

(10.17) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Ein *größter gemeinsamer Teiler* von a und b ist ein gemeinsamer Teiler g von a und b derart, dass jeder gemeinsame Teiler d von a und b auch ein Teiler von g ist.

(b) Ein *kleinstes gemeinsames Vielfaches* von a und b ist ein gemeinsames Vielfaches l von a und b derart, dass jedes gemeinsame Vielfache m von a und b auch ein Vielfaches von l ist.

Ein größter gemeinsamer Teiler ist also ein größtes Element in der prägeordneten Menge der gemeinsamen Teiler zusammen mit der Teilbarkeitsrelation, vgl. Definition (7.10)(b)(ii).

(10.18) Beispiel.

(a) In $\mathbb{Z}$ ist -6 ein größter gemeinsamer Teiler von 12 und 18.

(b) In $\mathbb{Z}$ ist 12 ein kleinstes gemeinsames Vielfaches von 4 und 6.

Beweis.

(a) Es sei $T := \{d \in \mathbb{Z} \mid d \mid 12 \text{ und } d \mid 18\}$ die Menge der gemeinsamen Teiler von 12 und 18. Nach Beispiel (10.16)(a)(i) ist $-6 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 12$ stets $|a| \leq |12| = 12$ folgt, gilt ferner $T \subseteq [-12, 12]$. Durch Ausrechnen ergibt sich

$$T = \{-6, -3, -2, -1, 1, 2, 3, 6\}.$$

Da für alle $d \in T$ auch $d \mid -6$ gilt, ist -6 somit ein größter gemeinsamer Teiler von 12 und 18.

(b) Es sei $I := \{m \in \mathbb{Z} \mid 4 \mid m \text{ und } 6 \mid m\}$ die Menge der gemeinsamen Vielfache von 4 und 6. Nach Beispiel (10.16)(b)(i) ist $12 \in I$. Es sei ein beliebiges gemeinsames Vielfaches m von 4 und 6 gegeben. Dann gilt $4 \mid m$ und $6 \mid m$, nach Proposition (10.9)(a) also auch $4 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$ und $6 \mid m - (m \operatorname{div} 12) \cdot 12 = m \bmod 12$. Folglich ist $m \bmod 12 \in I$. Durch Ausrechnen ergibt sich ferner $[0, 11] \cap I = \{0\}$, so dass $m \bmod 12 = 0$ folgt. Somit ist m ein Vielfaches von 12. Insgesamt ist 12 daher ein kleinstes gemeinsames Vielfaches von 4 und 6. □

Im Beweis von Beispiel (10.18) haben wir an entscheidender Stelle benutzt, dass die ganzzahligen Intervalle $[-12, 12]$ bzw. $[0, 11]$ endliche Mengen sind. Eine effizientere Methode zur Berechnung von größten gemeinsamen Teilern, welche sich auch für Polynome über Körpern eignet, werden wir in Satz (10.24) kennenlernen. Unter Ausnutzung von Satz (10.22) wird dies auch eine Möglichkeit zur effizienten Berechnung von kleinsten gemeisamen Vielfachen liefern.

(10.19) Bemerkung. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei ein größter gemeinsamer Teiler g von a und b sowie $g' \in R$ gegeben. Genau dann ist g' ein größter gemeinsamer Teiler von a und b, wenn g assoziiert zu g' ist.

(b) Es sei ein kleinstes gemeinsames Vielfaches l von a und b sowie $l' \in R$ gegeben. Genau dann ist l' ein kleinstes gemeinsames Vielfaches von a und b, wenn l assoziiert zu l' ist.

Beweis.

(a) Zunächst sei g' ein größter gemeinsamer Teiler von a und b. Dann ist g' insbesondere ein gemeinsamer Teiler von a und b und g ein größter gemeinsamer Teiler von a und b, wir haben also $g' \mid g$. Andererseits ist aber auch g ein gemeinsamer Teiler von a und b und g' ein größter gemeinsamer Teiler von a und b, wir haben also auch $g \mid g'$. Folglich ist g assoziiert zu g'.

Umgekehrt sei nun $g' = ug$ für ein $u \in R^\times$. Nach Proposition (10.12) ist mit g dann auch $g' = ug$ ein gemeinsamer Teiler von a und b, und für jeden gemeinsamen Teiler d von a und b folgt aus $d \mid g$ auch $d \mid ug$. Insgesamt ist g' ein größter gemeinsamer Teiler von a und b.

(b) Dies lässt sich dual zu (a) beweisen. □

(10.20) Lemma (Lemma von Bézout)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben.

(a) Es sei $I := \{d \in R \mid \text{es gibt } x, y \in R \text{ mit } d = xa + yb\}$.

(i) Falls $(a, b) = (0, 0)$, sei $g = 0$. Falls $(a, b) \neq (0, 0)$ sei $g \in I$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|g| = \min\{|d| \mid d \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg g = \min\{\deg d \mid d \in I \setminus \{0\}\}.$$

Dann ist g ein größter gemeinsamer Teiler von a und b. Insbesondere existiert ein größter gemeinsamer Teiler von a und b.

(ii) Es sei $g \in R$ ein größter gemeinsamer Teiler von a und b. Dann ist $g \in I$.

(b) Es sei $I := \{m \in R \mid \text{es gibt } x, y \in R \text{ mit } m = xa \text{ und } m = yb\}$.

(i) Falls $(a, b) = (0, 0)$, sei $l = 0$. Falls $(a, b) \neq (0, 0)$ sei $l \in I$ so, dass folgendes gilt: Im Fall $R = \mathbb{Z}$ gelte

$$|l| = \min\{|m| \mid m \in I \setminus \{0\}\}.$$

Im Fall $R = K[X]$ für einen Körper K gelte

$$\deg l = \min\{\deg m \mid m \in I \setminus \{0\}\}.$$

Dann ist l ein kleinstes gemeinsames Vielfaches von a und b. Insbesondere existiert ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Es sei $l \in R$ ein kleinstes gemeinsames Vielfaches von a und b. Dann ist $l \in I$.

Beweis.

(a) (i) Wenn $(a, b) = (0, 0)$ ist, so ist $g = 0$ ein größter gemeinsamer Teiler von a und b. Im Folgenden sei daher $(a, b) \neq (0, 0)$, so dass auch $g \neq 0$ gilt. Da $g \in I$ ist, gibt es $x, y \in R$ mit $g = xa + yb$. Folglich ist

$$a \bmod g = a - (a \operatorname{div} g)g = a - (a \operatorname{div} g)(xa + yb) = (1 - (a \operatorname{div} g)x)a + (a \operatorname{div} g)yb \in I,$$

also $a \bmod g = 0$ nach Wahl von g. Somit ist g ein Teiler von a. Analog lässt sich zeigen, dass g ein Teiler von b ist. Ferner ist jeder gemeinsame Teiler d von a und b nach Proposition (10.9)(a), (c) auch ein Teiler von $xa + yb = g$. Insgesamt ist g daher ein größter gemeinsamer Teiler von a und b.

(ii) Nach (i) gibt es einen größten gemeinsamen Teiler g' von a und b mit $g' \in I$, also derart, dass $g' = x'a + y'b$ für gewisse $x', y' \in R$. Da sowohl g als auch g' ein größter gemeinsamer Teiler von a und b ist, sind g und g' nach Bemerkung (10.19)(a) zueinander assoziiert. Nach Proposition (10.12) gibt es ein $u \in R^\times$ mit

$$g = ug' = u(x'a + y'b) = (ux')a + (uy')b.$$

Folglich ist auch $g \in I$. □

(b) (i) Wenn $(a, b) = (0, 0)$ ist, so ist $l = 0$ ein kleinstes gemeinsames Vielfaches von a und b. Im Folgenden sei daher $(a, b) \neq (0, 0)$. Da $l \in I$ ist, gibt es $x, y \in R$ mit $l = xa = yb$, d.h. l ist ein gemeinsames Vielfaches von a und b. Es sei ein beliebiges gemeinsames Vielfaches m von a und b gegeben. Dann gilt $a \mid m$ und $b \mid m$, nach Proposition (10.9)(a), (c) also auch $a \mid m - (m \operatorname{div} l)l = m \bmod l$ und $b \mid m - (m \operatorname{div} l)l = m \bmod l$. Folglich ist $m \bmod l \in I$, also $m \bmod l = 0$ nach Wahl von l. Somit ist m ein Vielfaches von l. Insgesamt ist l daher ein kleinstes gemeinsames Vielfaches von a und b.

(ii) Da l als kleinstes gemeinsames Vielfaches von a und b insbesondere ein gemeinsames Vielfaches von a und b ist, gibt es $x, y \in R$ mit $l = xa = yb$. Folglich ist $l \in I$.

Nach dem Lemma von Bézout (10.20) gibt es für jedes Paar ganzer Zahlen bzw. von Polynomen über einem Körper einen größten gemeinsamen Teiler sowie ein kleinstes gemeinsames Vielfaches, und nach Bemerkung (10.19) sind diese eindeutig bis auf Assoziiertheit. Im Folgenden geben wir einem ausgezeichneten größten gemeinsamen Teiler und einem ausgezeichneten kleinsten gemeinsamen Vielfachen eine feste Bezeichnung.

(10.21) Definition (größter gemeinsamer Teiler, kleinstes gemeinsames Vielfaches)**.**

(a) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Wir bezeichnen mit $\gcd(a, b)$ den eindeutig bestimmten nicht-negativen größten gemeinsamen Teiler von a und b.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $(f, g) = (0, 0)$, so setzen wir $\gcd(f, g) := 0$. Andernfalls bezeichnen wir mit $\gcd(f, g)$ den eindeutig bestimmten normierten größten gemeinsamen Teiler von f und g.

(b) (i) Es seien $a, b \in \mathbb{Z}$ gegeben. Wir bezeichnen mit $\operatorname{lcm}(a, b)$ das eindeutig bestimmte nicht-negative kleinste gemeinsame Vielfache von a und b.

(ii) Es seien ein Körper K und $f, g \in K[X]$ gegeben. Falls $(f, g) = (0, 0)$, so setzen wir $\operatorname{lcm}(f, g) := 0$. Andernfalls bezeichnen wir mit $\operatorname{lcm}(f, g)$ das eindeutig bestimmte normierte kleinste gemeinsame Vielfache von f und g.

Wir haben also in den Fällen $R = \mathbb{Z}$ und $R = K[X]$ für einen Körper K wohldefinierte Abbildungen

$$\gcd\colon R \times R \to R,$$
$$\operatorname{lcm}\colon R \times R \to R$$

konstruiert.

(10.22) Satz. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a, b \in R$ gegeben. Dann ist ab assoziiert zu $\gcd(a, b) \operatorname{lcm}(a, b)$.

Beweis. Zunächst gelte $\gcd(a, b) = 1$. Nach dem Lemma von Bézout (10.20) gibt es dann $x, y \in R$ mit $1 = xa + yb$. Da $\operatorname{lcm}(a, b)$ ein gemeinsames Vielfaches von a und b ist, gibt es ferner $p, q \in R$ mit $\operatorname{lcm}(a, b) = pa = qb$. Es folgt

$$(xq + yp)ab = xqab + ypab = qbxa + payb = \operatorname{lcm}(a, b)xa + \operatorname{lcm}(a, b)yb = \operatorname{lcm}(a, b)(xa + yb) = \operatorname{lcm}(a, b),$$

also $ab \mid \operatorname{lcm}(a, b)$. Andererseits ist aber auch ab ein gemeinsames Vielfaches von a und b, und da $\operatorname{lcm}(a, b)$ ein kleinstes gemeinsames Vielfaches von a und b ist, folgt $\operatorname{lcm}(a, b) \mid ab$. Folglich ist ab assoziiert zu $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(a, b)$.
Nun sei $\gcd(a, b)$ beliebig. Wenn $(a, b) = (0, 0)$ ist, so gilt

$$ab = 0 \cdot 0 = \gcd(a, b) \operatorname{lcm}(a, b).$$

Es sei also im Folgenden $(a, b) \neq (0, 0)$, so dass $\gcd(a, b) \neq 0$ ist. Da $\gcd(a, b)$ ein gemeinsamer Teiler von a und b ist, gibt es $p, q \in R$ mit $a = p \gcd(a, b)$ und $b = q \gcd(a, b)$. Es gilt $\gcd(p, q) = 1$ und $\operatorname{lcm}(a, b) = \gcd(a, b) \operatorname{lcm}(p, q)$. Nach dem bereits bewiesenen Spezialfall ist pq assoziiert zu $\gcd(p, q) \operatorname{lcm}(p, q) = \operatorname{lcm}(p, q)$. Folglich ist auch $ab = p \gcd(a, b)\, q \gcd(a, b) = \gcd(a, b)^2\, pq$ assoziiert zu $\gcd(a, b)^2 \operatorname{lcm}(p, q) = \gcd(a, b) \operatorname{lcm}(a, b)$. □

Alternativer Beweis von Beispiel (10.18)(b). Es sei $T := \{d \in \mathbb{Z} \mid d \mid 4 \text{ und } d \mid 6\}$ die Menge der gemeinsamen Teiler von 4 und 6. Wegen $4 = 2 \cdot 2$ und $6 = 3 \cdot 2$ ist $2 \in T$. Da für $a \in \mathbb{Z}$ aus $a \mid 6$ stets $|a| \leq |6| = 6$ folgt, gilt ferner $T \subseteq [-6, 6]$. Durch Ausrechnen ergibt sich

$$T = \{-2, -1, 1, 2\}.$$

Da für alle $d \in T$ auch $d \mid 2$ gilt und $2 \geq 0$ gilt, ist somit $\gcd(4, 6) = 2$.
Nach Satz (10.22) folgt

$$\operatorname{lcm}(4, 6) = \frac{4 \cdot 6}{\gcd(4, 6)} = \frac{4 \cdot 6}{2} = 12.$$ □

Der euklidische Algorithmus

Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Nach dem Lemma von Bézout (10.20)(a)(ii) wissen wir, dass es für $a, b \in R$ stets $x, y \in R$ mit $\gcd(a, b) = xa + yb$ gibt. Wir wollen nun einen Algorithmus herleiten, welcher zum einen $\gcd(a, b)$ und zum anderen eine solche Darstellung $(x, y) \in R \times R$ berechnet.

(10.23) Lemma. Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Für $a \in R$, $b \in R \setminus \{0\}$ ist

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

Beweis. Es seien $a, b \in R$ gegeben. Für $d \in R$ mit $d \mid b$ gilt nach Proposition (10.9)(a), (c) genau dann $d \mid a$, wenn $d \mid a - (a \operatorname{div} b)b = a \bmod b$ gilt. Somit sind die gemeinsamen Teiler von a und b genau die gemeinsamen Teiler von b und $a \bmod b$. Als größte Elemente in der prägeordneten Menge der gemeinsamen Teiler von a und b mit der Teilbarkeitsrelation sind dann aber auch die größten gemeinsamen Teiler von a und b genau die größten gemeinsamen Teiler von b und $a \bmod b$. Folglich gilt auch $\gcd(a, b) = \gcd(b, a \bmod b)$. □

(10.24) Satz (erweiterter euklidischer Algorithmus)**.** Es sei $R = \mathbb{Z}$ oder $R = K[X]$ für einen Körper K. Ferner seien $a \in R$, $b \in R \setminus \{0\}$ gegeben. Es seien Folgen $(r_i)_{i\in\mathbb{N}_0}$, $(x_i)_{i\in\mathbb{N}_0}$, $(y_i)_{i\in\mathbb{N}_0}$ in R rekursiv definiert durch

$$r_i := \begin{cases} a, & \text{für } i = 0, \\ b, & \text{für } i = 1, \\ r_{i-2} \bmod r_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$x_i := \begin{cases} 1, & \text{für } i = 0, \\ 0, & \text{für } i = 1, \\ x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0, \end{cases}$$

$$y_i := \begin{cases} 0, & \text{für } i = 0, \\ 1, & \text{für } i = 1, \\ y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} \neq 0, \\ 0, & \text{für } i \in \mathbb{N}_0 \text{ mit } i \geq 2, \text{ falls } r_{i-1} = 0. \end{cases}$$

(a) Für alle $i \in \mathbb{N}_0$ gilt

$$r_i = x_i a + y_i b.$$

(b) Es existiert ein $n \in \mathbb{N}$ so, dass r_n assoziiert zu $\gcd(a, b)$ ist und $r_i = 0$ für $i > n$ gilt. Im Fall $R = \mathbb{Z}$ kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq |b| + 1$ gilt. Im Fall $R = K[X]$ für einen Körper K kann $n \in \mathbb{N}$ so gewählt werden, dass $n \leq \deg b + 2$ gilt.

Beweis.

(a) Um $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$ zu zeigen, führen wir Induktion nach i. Zunächst gilt

$$x_0 a + y_0 b = 1 \cdot a + 0 \cdot b = a = r_0,$$
$$x_1 a + y_1 b = 0 \cdot a + 1 \cdot b = b = r_1,$$

also $x_i a + y_i b = r_i$ für $i \in \{0, 1\}$. Es sei also ein $i \in \mathbb{N}_0$ mit $i \geq 2$ gegeben und gelte $x_{i-2}a + y_{i-2}b = r_{i-2}$ sowie $x_{i-1}a + y_{i-1}b = r_{i-1}$. Wenn $r_{i-1} \neq 0$ ist, erhalten wir

$$\begin{aligned} x_i a + y_i b &= (x_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1})a + (y_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1})b \\ &= x_{i-2}a - (r_{i-2} \operatorname{div} r_{i-1})x_{i-1}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})y_{i-1}v \\ &= x_{i-2}a + y_{i-2}b - (r_{i-2} \operatorname{div} r_{i-1})(x_{i-1}a + y_{i-1}b) = r_{i-2} - (r_{i-2} \operatorname{div} r_{i-1})r_{i-1} = r_i. \end{aligned}$$

Wenn $r_{i-1} = 0$ ist, erhalten wir ebenfalls

$$x_i a + y_i b = 0 \cdot a + 0 \cdot b = 0 = r_i.$$

Nach dem Induktionsprinzip gilt $x_i a + y_i b = r_i$ für alle $i \in \mathbb{N}_0$.

(b) Im Fall $R = \mathbb{Z}$ gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $|r_i| = |r_{i-2} \bmod r_{i-1}| < |r_{i-1}|$, per Induktion also $r_{|b|+1} = 0$. Im Fall $R = K[X]$ für einen Körper K gilt für $i \geq 2$ stets $r_i = 0$ oder $r_i \neq 0$, $\deg r_i = \deg(r_{i-2} \bmod r_{i-1}) < \deg r_{i-1}$, per Induktion also $r_{(\deg b)+2} = 0$.

Wir setzen $n := \min\{i \in \mathbb{N} \mid r_i = 0\} - 1$. Dann ist $r_{n+1} = 0$, induktiv also $r_i = 0$ für alle $i \in \mathbb{N}_0$ mit $i > n$. Nach Lemma (10.23) gilt ferner

$$\gcd(r_{i-2}, r_{i-1}) = \gcd(r_{i-1}, r_{i-2} \bmod r_{i-1}) = \gcd(r_{i-1}, r_i)$$

für $i \in \mathbb{N}_0$, $i \geq 2$ mit $r_{i-1} \neq 0$. Induktiv erhalten wir

$$\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0).$$

Nun ist aber r_n assoziiert zu $\gcd(r_n, 0) = \gcd(a, b)$. □

(10.25) Beispiel.

(a) In $\mathbb{Z}$ ist $\gcd(2238, 168) = 6$ und

$$6 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) In $\mathbb{Q}[X]$ ist $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1) = X - 1$ und

$$X - 1 = \frac{1}{4}(X^3 + X^2 - X - 1) + (-\frac{1}{4}X - \frac{3}{4})(X^2 - 2X + 1).$$

Beweis.

(a) Wir berechnen $\gcd(2238, 168)$ mittels euklidischem Algorithmus:

$$\begin{aligned} 2238 &= 13 \cdot 168 + 54, \\ 168 &= 3 \cdot 54 + 6, \\ 54 &= 9 \cdot 6 + 0. \end{aligned}$$

Nach Satz (10.24)(b) ist $\gcd(2238, 168) = 6$. Wir setzen

$$\begin{aligned} r_0 &:= 2238, & & \\ r_1 &:= 168, & q_1 &:= 13, \\ r_2 &:= 54, & q_2 &:= 3, \\ r_3 &:= 6, & q_3 &:= 9, \end{aligned}$$

und berechnen $x_i, y_i \in \mathbb{Z}$ für $i \in \{0, 1, 2, 3\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} x_0 &:= 1, & y_0 &:= 0, \\ x_1 &:= 0, & y_1 &:= 1, \\ x_2 &:= x_0 - q_1 x_1 = 1 - 13 \cdot 0 = 1, & y_2 &:= y_0 - q_1 y_1 = 0 - 13 \cdot 1 = -13, \\ x_3 &:= x_1 - q_2 x_2 = 0 - 3 \cdot 1 = -3, & y_3 &:= y_1 - q_2 y_2 = 1 - 3 \cdot (-13) = 40. \end{aligned}$$

Nach Satz (10.24)(b) ist

$$6 = r_3 = x_3 \cdot 2238 + y_3 \cdot 168 = (-3) \cdot 2238 + 40 \cdot 168.$$

(b) Wir berechnen $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1)$ mittels euklidischem Algorithmus:

$$\begin{aligned} X^3 + X^2 - X - 1 &= (X + 3)(X^2 - 2X + 1) + 4X - 4, \\ X^2 - 2X + 1 &= (\frac{1}{4}X - \frac{1}{4})(4X - 4) + 0. \end{aligned}$$

Nach Satz (10.24)(b) ist $\gcd(X^3 + X^2 - X - 1, X^2 - 2X + 1) = X - 1$. Wir setzen

$$\begin{aligned} r_0 &:= X^3 + X^2 - X - 1, \\ r_1 &:= X^2 - 2X + 1, & q_1 &:= X + 3, \\ r_2 &:= 4X - 4, & q_2 &:= \frac{1}{4}X - \frac{1}{4}, \end{aligned}$$

und berechnen $h_i, k_i \in \mathbb{Q}[X]$ für $i \in \{0, 1, 2\}$ mit dem erweiterten euklidischen Algorithmus:

$$\begin{aligned} h_0 &:= 1, & k_0 &:= 0, \\ h_1 &:= 0, & k_1 &:= 1, \\ h_2 &:= h_0 - q_1 h_1 = 1 - (X + 3) \cdot 0 = 1, & k_2 &:= k_0 - q_1 k_1 = 0 - (X + 3) \cdot 1 = -X - 3. \end{aligned}$$

Nach Satz (10.24)(b) ist

$$4X - 4 = r_2 = h_2 f_2 + k_2 g_2 = 1(X^3 + X^2 - X - 1) + (-X - 3)(X^2 - 2X + 1)$$

und damit

$$X - 1 = \frac{1}{4}(4X - 4) = \frac{1}{4}(X^3 + X^2 - X - 1) + (-\frac{1}{4}X - \frac{3}{4})(X^2 - 2X + 1). \qquad \square$$