# 8. Musterlösung zu Mathematik für Informatiker II, SS 2004

MARTIN LOTZ & MICHAEL NÜSKEN

**Aufgabe 8.1** (Polynomdivision). (8 Punkte)

Dividiere $a$ mit Rest durch $b$ für

(i) $a = x^7 - 5x^6 + 3x^2 + 1$, $b = x^2 + 1$ in $\mathbb{R}[x]$.

**Lösung.** $x^7 - 5x^6 + 3x^2 + 1 = (x^5 - 5x^4 - x^3 + 5x^2 + x - 2)(x^2 + 1) + (-x + 3)$. ○

(ii) $a = x^6 + 2$, $b = x^2 + x + 1$ in $\mathbb{F}_3[x]$.

**Lösung.** $x^6 + 2 = x^6 - 1 = (x^4 - x^3 + x - 1)(x^2 + x + 1)$. ○

(iii) $a = x^{10} - 1$, $b = x^4 - 1$ in $\mathbb{F}_3[x]$.

**Lösung.** $x^{10} - 1 = (x^6 + x^2)(x^4 - 1) + x^2 - 1$. ○

(iv) $a = x^5 + x - 2$, $b = x^3 + 3x - 1$ in $\mathbb{R}[x]$.

**Lösung.** $x^5 + x - 2 = (x^2 - 3)(x^3 + 3x - 1) + (x^2 + 10x - 5)$. ○

Berechne den größten gemeinsamen Teiler der Polynome

(v) $a = x^7 - 5x^6 + 3x^2 + 1$, $b = x^2 + 1$ in $\mathbb{R}[x]$.

**Lösung.** Wir führen den Euklidischen Algorithmus mit $x^7 - 5x^6 + 3x^2 + 1$ und $x^2 + 1$ durch:

$$x^7 - 5x^6 + 3x^2 + 1 = (x^5 - 5x^4 - x^3 + 5x^2 + x - 2)(x^2 + 1) + (-x + 3)$$
$$x^2 + 1 = (-x - 3)(-x + 3) + 10$$

Der letzte Rest ist eine reelle Zahl, also ist der grösste gemeinsame Teiler die Eins. Man sagt dann auch, die Polynome seien teilerfremd. ○

(vi) $a = x^{10} - 1$, $b = x^4 - 1$ in $\mathbb{F}_3[x]$.

**Lösung.** Wir führen den Euklidischen Algorithmus mit $x^{10} - 1$ und $x^4 - 1$ durch:

$$x^{10} - 1 = (x^6 + x^2)(x^4 - 1) + x^2 - 1$$
$$x^4 - 1 = (x^2 + 1)(x^2 - 1)$$

Der größte gemeinsame Teiler ist hier das Polynom $x^2 - 1$. ○

**Lexikon.** Sei $F$ ein Körper. Ein Polynom $a = a_d x^d + \cdots + a_1 x + a_0 \in F[x]$ heißt *normiert*, wenn $a_d = 1$ gilt. Der *größte gemeinsame Teiler* $\mathrm{ggT}(a, b)$ von $a, b \in F[x]$ ist das eindeutige normierte Polynom $g \in F[x]$ mit den folgenden Eigenschaften: (i) $g$ ist ein *gemeinsamer Teiler*, dh. $g$ teilt $a$ und $b$, (ii) wenn $f \in F[x]$ ein gemeinsamer Teiler von $a$ und $b$ ist (also die Polynome $a$ und $b$ teilt), so teilt $f$ auch $g$. Der ggT ist das normierte Polynom größten Grades, welches $a$ und $b$ teilt. Wie bei den ganzen Zahlen kann der ggT mit Hilfe des Euklidischen Algorithmus berechnet werden.

**Aufgabe 8.2** (Erweiterter Euklidischer Algorithmus). (7 Punkte)

Wir untersuchen den Erweiterten Euklidischen Algorithmus für Polynome über einem Körper $F$.

**Algorithmus.** Erweiterter Euklidischer Algorithmus.

Eingabe: $a, b \in F[x]$ mit $\deg a \geq \deg b$.
Ausgabe: $\ell \in \mathbb{N}$, $g, s, t \in F[x]$ wie unten berechnet.

1. $r_0 \leftarrow a, \quad r_1 \leftarrow b.$
2. $s_0 \leftarrow 1, \quad t_0 \leftarrow 0.$
3. $s_1 \leftarrow 0, \quad t_1 \leftarrow 1.$
4. $i \leftarrow 1.$
5. Solange $r_i \neq 0$ erledige 6–10
6. $\quad q_i \leftarrow r_{i-1} \operatorname{quo} r_i.$
7. $\quad r_{i+1} \leftarrow r_{i-1} - q_i r_i.$
8. $\quad s_{i+1} \leftarrow s_{i-1} - q_i s_i.$
9. $\quad t_{i+1} \leftarrow t_{i-1} - q_i t_i.$
10. $\quad i \leftarrow i + 1.$
11. $\ell \leftarrow i - 1.$
12. Antworte $\ell$, $g = r_\ell / \operatorname{lc}(r_\ell)$, $s = s_\ell / \operatorname{lc}(r_\ell)$, $t = t_\ell / \operatorname{lc}(r_\ell)$.

Hierbei bezeichnet $\operatorname{lc}(f)$ den *Leitkoeffizient* von $f$. Dies ist der Koeffizient des Terms höchsten Grades von $f$. Zeige:

(i) Für $1 \leq i < \ell$ gilt $\deg r_{i+1} < \deg r_i$.

**Lösung.** Wir beweisen dies mit Induktion. Nach Voraussetzung haben wir $\deg r_0 \geq \deg r_1$. Gilt $\deg r_0 > \deg r_1$, so können wird dies als Induktionsverankerung nehmen. Ansonsten ist $r_0 = \alpha r_1 + r_2$, wobei $\alpha = \operatorname{lc}(r_0)/\operatorname{lc}(r_1)$, und $\deg r_2 < \deg r_1$. Dies nehmen wir dann als Induktionsverankerung.

Angenommen $\deg r_i < \deg r_{i-1}$ sei gezeigt. Bei Division mit Rest von $r_{i-1}$ durch $r_i$ erhalten wir $r_{i-1} = r_i q_i + r_{i+1}$. Aus der Polynomdivision ist bekannt, dass der Rest $r_{i+1}$ kleineren Grad hat als das Polynom $r_i$, durch das geteilt wird. Daraus folgt die Behauptung. ◯

(ii) Der Algorithmus terminiert nach höchstens $\deg b + 1$ Schleifendurchläufen.

**Lösung.** Nach dem $i$-ten Schleifendurchlauf erhalten wir einen Rest $r_{i+1}$, dessen Grad mindestens eins kleiner ist als der Grad von $r_i$. Der Grad von $r_1$ ist $\deg b$, also folgt $\deg r_{i+1} \leq \deg b - i$. Am Ende des Algorithmus haben wir $r_{\ell+1} = 0$. Nach $\ell - 1$ Schleifendurchläufen, haben wir $0 \leq \deg r_\ell \leq \deg b - \ell + 1$. Daraus folgt $\ell \leq \deg b + 1$, was zu beweisen war. ◯

(iii) Für alle $0 \leq i < \ell$ gilt: $g = \mathrm{ggT}(r_i, r_{i+1}) = \mathrm{ggT}(a, b)$. [*Hinweis.* Zeige $\mathrm{ggT}(r_{i-1}, r_i) = \mathrm{ggT}(r_i, r_{i+1})$ und benutze dann Induktion].

**Lösung.** Nach Definition gilt $\mathrm{ggT}(a, b) = \mathrm{ggT}(r_0, r_1)$. Betrachte nun $r_{i-1}$ und $r_i$. Wir haben

$$r_{i-1} = q_i r_i + r_{i+1},$$

woraus folgt, dass die gemeinsamen Teiler von $r_{i-1}$ und $r_i$ genau die gemeinsamer Teiler von $r_i$ und $r_{i+1}$ sind. Ist $g$ der größte gemeinsame Teiler von $r_{i-1}$ und $r_i$, so muss $g$ nach Definition des ggT und der eben aufgestellten Beobachtung auch der größte gemeinsame Teiler von $r_i$ und $r_{i+1}$ sein. Schließlich folgt per Induktion $g = r_\ell / \operatorname{lc}(r_\ell) = \mathrm{ggT}(r_\ell, r_{\ell+1}) = \mathrm{ggT}(a, b)$. ◯

(iv) Für $0 \leq i \leq \ell$ gilt $r_i = s_i a + t_i b$. Insbesondere ist $g = sa + tb$.

**Lösung.** Am Anfang haben wir $r_0 = s_0 a + t_0 b = a$ und $r_1 = s_1 a + t_1 b = b$. Angenommen, die entsprechende Aussage gilt bereits für $r_{i-1}$ und $r_i$. Aus den Formeln in der Schleife folgt

$$\begin{aligned} r_{i+1} &= r_{i-1} - q_i r_i \\ &= s_{i-1} a + t_{i-1} b - q_i (s_i a + t_i b) \\ &= (s_{i-1} - q_i s_i) a + (t_{i-1} - q_i t_i) b \\ &= s_{i+1} a + t_{i+1} b. \end{aligned}$$

Durch Induktion schließen wir nun auf die Behauptung. ◯

(v) Ist $\mathrm{ggT}(a, b) = 1$, so folgt $sa \equiv 1 \bmod b$.

**Lösung.** Im Fall $\mathrm{ggT}(a, b) = 1$ liefert der erweiterte Euklidische Algorithmus Polynome $s, t$ mit $sa + tb = 1$. Also $sa \equiv 1 \bmod b$. ◯

**Aufgabe 8.3** (Irreduzible Polynome). (5+1 Punkte)

Sei $F$ ein Körper. Ein Polynom $f \in F[x] \setminus F$ heißt *irreduzibel*, wenn aus $f = gh$ entweder $g \in F \setminus \{0\}$ oder $h \in F \setminus \{0\}$ folgt. Andernfalls heißt $f$ *zerlegbar*.

In dieser Aufgabe wollen wir irreduzible Polynome untersuchen.

(i) Zeige, dass Polynome der Form $\alpha x + \beta$, $\alpha \neq 0, \beta \in F$, irreduzibel sind.

**Lösung.** Wir beweisen dies durch Widerspruch. Angenommen, wir hätten $\alpha x + \beta = fg$, mit $\deg f = d \geq 1$ und $\deg g = e \geq 1$. (Seien $\gamma x^d$ und $\delta x^e$ die Terme größten Grades in $f$ und $g$. Dann ist der Leitterm von $fg$ gleich $\gamma\delta x^{d+e}$. Da $F$ ein Körper ist, besitzt $F$ insbesondere keine Nullteiler, woraus $\gamma\delta \neq 0$ folgt.) Also ist $\deg fg = d + e \geq 2 > 1$ und wir haben einen Widerspruch zur Tatsache, dass der Grad von $\alpha x + \beta$ eins ist. ◯

(ii) Zeige, dass wenn $a$ eine Nullstelle eines Polynomes $f \in F[x]$ ist, d.h. wenn $f(a) = 0$ gilt, das Polynom $f$ von $x - a$ geteilt wird. Ist der Grad von $f$ echt größer als eins, so folgt insbesondere, dass $f$ nicht irreduzibel ist.

**Lösung.** Wir führen Division mit Rest durch:

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

wobei $\deg r < \deg(x - a) = 1$ gilt. Also ist $r \in F$ eine Konstante. Wäre nun $r \neq 0$, so müsste $f(a) = r \neq 0$ gelten, im Widerspruch zur Annahme, dass $a$ eine Nullstelle von $f$ ist. Also folgt $r = 0$ und $f = q \cdot (x - a)$. ◯

(iii) Zeige anhand eines Beispiels in $\mathbb{R}[x]$, dass die Umkehrung nicht gilt, d.h., gib ein *zerlegbares* Polynom in $\mathbb{R}[x]$ an, welches keine reelle Nullstelle besitzt.

**Lösung.** Das Polynom $(x^2 + 1)^2$ hat keine Nullstelle in $\mathbb{R}$ (welche reelle Zahl erfüllt $x^2 = -1$?), ist aber definitiv nicht irreduzibel. ◯

(iv) Beweise: Hat $f \in F[x]$ Grad zwei oder drei, so ist $f$ *genau dann* zerlegbar, wenn es eine Nullstelle in $F$ besitzt.

**Lösung.** Sei $f \in F[X]$ von Grad zwei oder drei. Wir wissen bereits: Hat $f \in F[x]$ eine Nullstelle, so ist $f$ zerlegbar. Sei umgekehrt $f$ zerlegbar. Dann lässt sich $f$ schreiben als Produkt $f = gh$, wobei $\deg g = d \geq 1$ und auch $\deg h = e \geq 1$. Währen sowohl $d$ wie auch $e$ vom Grad größer als 1, so hätte das Produkt $gh$ Grad größer als drei, im Wiederspruch zur Annahme. Also ist einer der Faktoren linear, d.h. von der Form $\alpha x + \beta$. Dann ist aber $-\beta/\alpha$ eine Nullstelle von $f$ und wir sind fertig. ◯

(v) Bestimme alle irreduziblen Polynome vom Grad 3 in $\mathbb{F}_2[x]$. [*Hinweis:* Jedes Polynom in $\mathbb{F}_2[x]$ vom Grad 3 ist von der Form $x^3 + \alpha x^2 + \beta x + \gamma$ mit $\alpha, \beta, \gamma \in \mathbb{F}_2$. Benutze nun das Nullstellenkriterium aus (iv).]

**Lösung.** Sei $f = x^3 + \alpha x^2 + \beta x + \gamma \in \mathbb{F}_2[x]$. Ist $\gamma = 0$, so ist 0 eine Nullstelle von $f$ und nach (iv) ist $f$ dann zerlegbar. Als Kandidaten für irreduzible Polynome kommen also nur Polynome der Form $f = x^3 + \alpha x^2 + \beta x + 1$ in Frage. Es gibt vier Stück davon, je nachdem wie wir $\alpha$

und $\beta$ mit Werten 1 und 0 belegen. Im Fall $\alpha = \beta$ sehen wir, dass 1 eine Nullstelle von $f$ in $\mathbb{F}_2$ ist, also sind diese Polynome zerlegbar. Schließlich haben wir die Polynome

$$x^3 + x^2 + 1 \text{ und } x^3 + x + 1,$$

welche keine Nullstellen in $\mathbb{F}_2$ besitzen und somit irreduzibel sind. ◯

(vi*) Eine Form des Fundamentalsatzes der Algebra besagt, dass jedes irreduzible Polynom in $\mathbb{C}[x]$ linear, d.h. von der Form $\alpha x + \beta$, mit $\alpha \neq 0, \beta \in \mathbb{C}$, ist. Benutze dies um zu folgern, dass jedes Polynom vom Grad $d \geq 1$ in $\mathbb{C}[x]$ sich als Produkt von $d$ Linearfaktoren schreiben läßt.

**Lösung.** Wir beweisen dies durch Induktion nach dem Grad des Polynoms. Der Fall $\deg f = 1$ ist klar, sei also $\deg f = d > 1$ und nimm an, die Aussage sei für Grade kleiner als $d$ bereits bewiesen. Nach dem Fundamentalsatz der Algebra folgt, dass $f$ nicht irreduzibel ist. Es gibt also Polynome $g, h$ mit $\deg g = e < d$, $\deg h = d - e < d$ so, dass $f = gh$. Nach Induktionsvoraussetzung lassen sich $g$ und $h$ als Produkte von jeweils $e$ und $d - e$ linearen Faktoren schreiben. Es folgt, dass $f$ sich als Produkt von $d$ linearen Faktoren schreiben lässt. ◯

**Aufgabe 8.4** ($\mathbb{F}_8$). (8 Punkte)

Wir wollen hier den Körper mit acht Elementen kennenlernen.

(i) Zeige, dass $x^3 + x + 1$ über $\mathbb{F}_2$ irreduzibel ist, sich also nicht als ein nichttriviales Produkt schreiben lässt.

**Lösung.** Dies wurde bereits in Aufgabe 8.3(v) gezeigt. ◯

Für $g \in \mathbb{F}_2[x]$ besteht der Ring $\mathbb{F}_2[x]/\langle g \rangle$ aus den Resten $f \operatorname{rem} g$ ($f \in \mathbb{F}_2[x]$); Addition und Multiplikation erfolgen modulo $g$.

(ii) Bestimme eine Liste aller Elemente in $\mathbb{F}_8 = \mathbb{F}_2[x]/\langle x^3 + x + 1 \rangle$. [Bezeichne mit $a$ das zu $x \in \mathbb{F}_2[x]$ gehörige Element in $\mathbb{F}_8$.]

**Lösung.** Jedes Element in $\mathbb{F}_8$ ist ein Polynom in $a$ vom Grad höchstens zwei. Es gibt acht Stück davon:

$$0,\ 1,\ a,\ a+1,\ a^2,\ a^2+1,\ a^2+a,\ a^2+a+1.$$

Jedes dieser Elemente ist verschieden modulo $a^3 + a + 1$. ◯

(iii) Berechne $a(a^2 + a + 1)$, $a^2(a^2 + a + 1)$ und $a^{-1}$ in $\mathbb{F}_8$.

**Lösung.** Wir rechnen mit Polynomen in $\mathbb{F}_2[x]$:

$$x(x^2+x+1) = x^3+x^2+x \equiv x^2+1 \bmod x^3+x+1,$$
$$x^2(x^2+x+1) = x^4+x^3+x^2 \equiv 1 \bmod x^3+x+1.$$

Daraus folgt $a(a^2+a+1) = a^2+1$ und $a^2(a^2+a+1) = 1$ in $\mathbb{F}_8$. Das Element $a^{-1}$ kann mit dem erweiterten Euklidischen Algorithmus, angewandt auf $x$ und $x^3+x+1$, berechnet werden (siehe Aufgabe 8.2(v)). Wegen

$$x^3+x+1 = x(x^2+1)+1$$

folgt $x(x^2+1) \equiv 1 \bmod x^3+x+1$ und folglich $a^{-1} = a^2+1$. ◯

(iv) Ist $\mathbb{F}_8$ ein Körper?

**Lösung.** Die Menge $\mathbb{F}_8$ ist ein Körper. Wir wissen bereits (oder gehen davon aus), dass $\mathbb{F}_8$ ein Ring ist (die Axiome lassen sich leicht nachprüfen). Wir müssen also nur noch nachweisen, dass $\mathbb{F}_8$ keine Nullteiler besitzt und jedes Element ein Inverses besitzt. Wir können so argumentieren: Da $x^3+x+1$ irreduzibel ist, gilt für jedes $f \in \mathbb{F}_2[x]$ mit $\deg f < 3$, dass $\mathrm{ggT}(f, x^3+x+1) = 1$. Also kann mit dem EEA ein $s \in \mathbb{F}_2[x]$ berechnet werden, welches $sf \equiv 1 \bmod x^3+x+1$ erfüllt. Dieses $s$ liefert das inverse Element $s \bmod x^3+x+1$ zu $f$ in $\mathbb{F}_8$. Wir folgern, dass jedes Element $z \neq 0$ aus $\mathbb{F}_8$ ein inverses Element besitzt. Insbesondere hat $\mathbb{F}_8$ keine Nullteiler: aus $yz = 0$ würde $y^{-1}yz = z = 0$ folgen. Wir schließen, dass $\mathbb{F}_8$ ein Körper ist. ◯

(v) Zeige, dass für alle $z \in \mathbb{F}_8 \setminus \{0\}$ die Gleichung $z^7 = 1$ gilt. Das verallgemeinert den kleinen Satz von Fermat.

**Lösung.** Da $\mathbb{F}_8$ ein Körper ist, ist $\mathbb{F}_8 \setminus \{0\}$ eine Gruppe bezüglich der Multiplikation. Diese hat 7 Elemente. Nach dem Satz von Lagrange teilt die Ordnung der von $z$ erzeugten Untergruppe die Ordnung von $\mathbb{F}_8 \setminus \{0\}$, also 7. Folglich hat jedes Element $z$ Ordnung 1 oder 7 und insbesondere gilt $z^7 = 1$. ◯

(vi) Zeige, dass $z^{-1} = z^6$ für $z \neq 0$.

**Lösung.** Aus (v) folgt $z \cdot z^6 = 1 = z^6 \cdot z$. Angenommen, es gibt ein zweites Element $y$ mit $zy = yz = 1$. Dann hätten wir $z(y - z^6) = 1 - 1 = 0$. Da $\mathbb{F}_8$ keine Nullteiler enthält, folgt $y = z^6$. Dies ist dann auch das eindeutig bestimmte inverse Element $z^{-1}$ zu $z$. ◯

(vii) Ist $\mathbb{Z}_8$ ein Körper?

**Lösung.** Der Ring $\mathbb{Z}_8$ ist kein Körper. Das Element $2 \bmod 8$ ist ein Nullteiler in $\mathbb{Z}_8$ ($2 \cdot 4 \equiv 0 \bmod 8$), und hat somit auch kein inverses Element. ◯

***Aufgabe 8.5** (Nicht alltäglich, knifflig). (0+5 Punkte)

Ein Ring $R$ heißt *euklidisch*, wenn er eine Division mit Rest erlaubt, dh. es gibt eine *euklidische Normfunktion* $\nu\colon R \setminus \{0\} \to \mathbb{N}$ so, dass es für alle $a, b \in R$ mit $b \neq 0$ passende $q, r \in R$ gibt mit $a = q \cdot b + r$ und $r = 0$ oder $\nu(r) < \nu(b)$.

**Satz.** *Der Ring $\mathbb{Z}[x]$ der Polynome mit ganzzahligen Koeffizienten ist nicht euklidisch, erlaubt also keine Division mit Rest.*

Dafür müssen wir zeigen, dass egal welche Funktion $\nu$ wir versuchen, es nie für alle $a, b \in \mathbb{Z}[x]$ mit $b \neq 0$ passende $q, r \in \mathbb{Z}[x]$ geben wird mit $a = q \cdot b + r$ und $r = 0$ oder $\nu(r) < \nu(b)$.

(i*) Division mit Rest bezüglich des Grades $\nu = \deg$ ist nicht möglich. [Finde $a, b \in \mathbb{Z}[x]$ mit $b \neq 0$ so, dass ...]

**Lösung.** Wir nehmen einfach $a = x$ und $b = 2$. Angenommen, wir finden $q, r \in \mathbb{Z}[x]$ mit $a = qb + r$ mit $\deg r < 0 = \deg b$. Dann ist $r \in \mathbb{Z}$ und $q = q_1 x + q_0$. Durch Koeffizientenvergleich bekommen wir also $1 = q_1 2$. Aber das kann nicht sein, da es ein solches $q_1$ in $\mathbb{Z}$ nicht gibt. ◯

(ii*) Bestimme *alle* Teiler von $2 \in \mathbb{Z}[x]$ und *alle* Teiler von $x \in \mathbb{Z}[x]$.

**Lösung.** Die Teiler von 2 haben sicher alle Grad 0, sind also Konstanten. Und in $\mathbb{Z}$ sind die Teiler von 2 bekannt, es gibt vier Stück: $\{\pm 1, \pm 2\}$.

Die Teiler von $x$ haben sicher Grad 0 oder Grad 1. Aus $x = (ax + b)c$ findet man ganz leicht die einzigen vier Teiler $\{\pm 1, \pm x\}$. ◯

(iii*) Angenommen $\nu\colon \mathbb{Z}[x] \setminus \{0\} \to \mathbb{N}$ ist gegeben. Zeige: Dann gibt es ein Element $g = a \cdot 2 + b \cdot x$ mit $g \neq 0$, $a, b \in \mathbb{Z}[x]$ und $\nu(g)$ minimal unter allen solchen Elementen, also $\nu(g) \leq \nu(h)$ für alle $h = a' \cdot 2 + b' \cdot x \neq 0$, $a', b' \in \mathbb{Z}[x]$.

**Lösung.** Es gibt unter all diesen Paaren eins mit minimalem Wert $\nu(a \cdot 2 + b \cdot x)$, weil die Werte von $\nu$ ja in $\mathbb{N}$ liegen und dort jede Menge ein kleinstes Element hat (das ist das Induktionsprinzip!). Unter allen $(a, b)$ nehmen wir dann einfach eines, dass diesen kleinsten Wert auch liefert. ◯

(iv*) Nimm nun an, dass $\nu$ eine euklidische Normfunktion ist. Zeige: Dann gilt $g \mid 2$ und $g \mid x$ in $\mathbb{Z}[x]$.

**Lösung.** Unter diesen Voraussetzungen können wir 2 mit Rest durch $g$ teilen: wir erhalten $q, r \in \mathbb{Z}[x]$ mit $2 = q \cdot g + r$ und $\nu(r) < \nu(g)$. Aber dieses $r = (1 - a)2 - bx$ ist auch eine Linearkombination von 2 und $x$.

Wäre $r \neq 0$, so müsste wegen der Minimalität von $\nu(g)$ ja $\nu(g) \leq \nu(r)$ sein. Also kann nur $r = 0$ sein. Und dann ist $2 = q \cdot g$, also $g \mid 2$.

Ganz analog erhalten wir $g \mid x$. ◯

(v*) Führe dies zum Widerspruch.

**Lösung.** Wie wir gerade gesehen haben, muss $g$ ein gemeinsamer Teiler von 2 und $x$ sein. Die einzigen gemeinsamen Teiler von 2 und $x$ in $\mathbb{Z}[x]$ sind $\pm 1$. Also muss $g = 1$ oder $g = -1$ sein. Aber das ist unmöglich, weil $g(0) = a(0)2 + b(0)0$ auf jeden Fall gerade ist. ◯