9. Lösung zu algebraischen Strukturen: Teilbarkeit in Integritätsbereichen

Lösung (9.1) (a) Wegen $a = 1 \cdot a$ gilt $a \mid a$.

(b) Gelten die Bedingungen $a \mid b$ und $b \mid c$, so gibt es Elemente $r, s \in R$ mit $b = ra$ und $c = sb$. Dann gilt $c = s(ra) = (sr)a$, so daß auch $a \mid c$ gilt.

(c) Wegen $a = 1 \cdot a$ gilt $a \sim a$ (Reflexivität). Gibt es eine Einheit u mit $b = ua$, so gibt es auch eine Einheit v (nämlich $v := u^{-1}$) mit $a = vb$; aus $a \sim b$ folgt also $b \sim a$ (Symmetrie). Gibt es Einheiten u und v mit $b = ua$ und $c = vb$, gilt $c = v(ua) = (vu)a$; es gibt also auch eine Einheit w (nämlich $w := vu$) mit $c = wa$. Aus $a \sim b$ und $b \sim c$ folgt also $a \sim c$ (Transitivität). Gilt $a \sim b$, so gibt es eine Einheit u mit $b = ua$ und $a = u^{-1}b$, so daß die Bedingungen $a \mid b$ und $b \mid a$ gelten. Sind umgekehrt diese beiden Bedingungen erfüllt. so gibt es Elemente $r, s \in R$ mit $b = ra$ und $a = sb$. Es gilt dann $a = s(ra) = (sr)a$, folglich $1 = sr$, so daß r und s Einheiten sind. Also gilt $a \sim b$.

(d) Gilt $a \sim 0$, so gibt es eine Einheit u mit $a = u \cdot 0 = 0$. Also ist das einzige zur Null assoziierte Ringelement die Null selbst. Da das Produkt zweier Einheiten wieder eine Einheit ist, ist jedes zu einer Einheit assoziierte Ringelement wieder eine Einheit. Umgekehrt ist wegen $1 = u^{-1}u$ jede Einheit u assoziiert zum Einselement. Also ist $R^\times$ genau die Äquivalenzklasse des Einselements unter der Relation $\sim$.

(e) Gilt $a \mid b$, sagen wir $b = ra$, so gilt auch $b = (u^{-1}r)(ua)$ und damit $ua \mid b$. Gilt $ua \mid b$, sagen wir $b = s(ua)$, so gilt auch $ub = (su^2)a$ und damit $a \mid ub$. Gilt $a \mid ub$, sagen wir $ub = ta$, so gilt auch $b = (u^{-1}t)a$ und damit $a \mid b$. Also sind alle drei Aussagen äquivalent.

(f) Genau dann gilt $ra|rb$, wenn es ein Element $x \in R$ gibt mit $rb = rax$. Wegen der Nullteilerfreiheit von R ist diese Gleichung äquivalent mit der Gleichung $b = ax$.

(g) Gelten die Bedingungen $c|a$ und $c|b$, so gibt es Elemente $x, y \in R$ mit $a = cx$ und $b = cy$. Wir erhalten dann $ra+sb = rcx+scy = c(rx+sy)$ und damit $c|ra+sb$.

Lösung (9.2) (a) Es sei x ein gemeinsamer Teiler von a_1/g, …, a_n/g. Dann ist gx ein gemeinsamer Teiler von $a_1, \ldots, a_n$, folglich ein Teiler von g, sagen wir $g = (gx)y$. Dann gilt aber $1 = xy$, so daß x eine Einheit ist. Nur die Einheiten sind also gemeinsame Teiler der Elemente a_1/g, …, a_n/g; diese Elemente sind daher teilerfremd.

(b) Da g ein ggT von $a_1, \ldots, a_n$ ist und g' ein gemeinsamer Teiler dieser Elemente, gilt $g' \mid g$. Analog gilt $g \mid g'$. Also gilt $g' \sim g$.

(c) Es gelte $g' \sim g$, sagen wir $g' = ug$ mit einer Einheit $u \in R^\times$. Dann ist g' ein gemeinsamer Teiler von $a_1, \ldots, a_n$, und ist d ein beliebiger gemeinsamer Teiler von $a_1, \ldots, a_n$, so ist d ein Teiler von g und damit auch von g'. Also ist g' ein ggT von $a_1, \ldots, a_n$.

(d) Da k ein kgV von $a_1, \ldots, a_n$ ist und k' ein gemeinsames Vielfaches dieser Elemente, gilt $k \mid k'$. Analog gilt $k' \mid k$. Also gilt $k' \sim k$.

(e) Es gelte $k' \sim k$, sagen wir $k' = uk$ mit einer Einheit $u \in R^\times$. Dann ist k' ein gemeinsames Vielfaches von $a_1, \ldots, a_n$, und ist v ein beliebiges gemeinsames Vielfaches von $a_1, \ldots, a_n$, so ist v ein Vielfaches von k und damit auch von k'. Also ist k' ein kgV von $a_1, \ldots, a_n$.

(f) Jedenfalls ist rg ein gemeinsamer Teiler von $a_1, \ldots, a_n$. Ist also g' ein ggT von $ra_1, \ldots, ra_n$, so gilt $rg \mid g'$, sagen wir $g' = (rg)x$. Dann ist gx ein gemeinsamer Teiler von $a_1, \ldots, a_n$, folglich ein Teiler von g, sagen wir $g = (gx)y$. Hieraus folgt aber $xy = 1$, so daß x eine Einheit ist. Wegen $g' = (rg)x$ gilt daher $g' \sim rg$; da g' ein ggT von $ra_1, \ldots, ra_n$, ist folglich auch rg ein ggT von $ra_1, \ldots, ra_n$.

Lösung (9.3) (a) Setzen wir $x = a + b\sqrt{-5}$ und $y = c + d\sqrt{-5}$, so gilt $xy = ac - 5bd + ad\sqrt{-5} + bc\sqrt{-5} = (ac - 5bd) + (ad + bc)\sqrt{-5}$. Hieraus folgt

$$\begin{aligned} N(xy) &= (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= a^2c^2 - 10abcd + 25b^2d^2 + 5a^2d^2 + 10abcd + 5b^2c^2 \\ &= a^2c^2 + 5(a^2d^2 + b^2c^2) + 25b^2d^2 \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \;=\; N(x)N(y). \end{aligned}$$

(b) Es gebe Elemente $r, s \in R$ mit $x = ra$ und $y = sa$. Wir haben dann $N(x) = N(ra) = N(r)N(a)$ und $N(y) = N(sa) = N(s)N(a)$, so daß $N(a)$ ein gemeinsamer Teiler von $N(x)$ und $N(y)$ ist.

(c) Es gebe Elemente $r, s \in R$ mit $a = rx$ und $a = sy$. Wir haben dann $N(a) = N(rx) = N(r)N(x)$ und $N(a) = N(sy) = N(s)N(y)$, so daß $N(a)$ ein gemeinsames Vielfaches von $N(x)$ und $N(y)$ ist.

(d) Wir betrachten $x := 2$ und $y := 1 + \sqrt{-5}$. Es sei $a + b\sqrt{-5}$ ein gemeinsamer Teiler von x und y. Dann ist $N(a + b\sqrt{-5}) = a^2 + 5b^2$ ein gemeinsamer Teiler von $N(x) = 4$ und $N(y) = 6$, folglich ein Teiler von 2. Da die Gleichung $a^2 + 5b^2 = 2$ keine ganzzahligen Lösungen hat, folgt hieraus $a^2+5b^2 = 1$ und damit $a+b\sqrt{-5} = \pm 1$. Also haben x und y nur die gemeinsamen Teiler ± 1 in R; diese sind dann automatisch größte gemeinsame Teiler.

Nun sei $a + b\sqrt{-5}$ ein kleinstes gemeinsames Vielfaches von x und y. Dann ist $N(a + b\sqrt{-5}) = a^2 + 5b^2$ ein gemeinsames Vielfaches von $N(x) = 4$ und $N(y) = 6$, folglich ein Vielfaches von 12. Andererseits muß $a + b\sqrt{-5}$ jedes gemeinsame Vielfache von x und y teilen, insbesondere also $xy = 2 + 2\sqrt{-5}$ und $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$. Dann muß $N(a + b\sqrt{-5})$ auch $N(2 + 2\sqrt{-5}) = 24$ und $N(6) = 36$ teilen, damit also ein Teiler von 12 sein. Insgesamt führt dies auf die Gleichung $a^2 + 5b^2 = 12$, die aber keine ganzzahlige Lösung hat. Also kann es ein kleinstes gemeinsames Vielfaches von x und y nicht geben.

(e) Wir betrachten die Elemente $x := 6$ und $y := 2 + 2\sqrt{-5}$. Ist $a + b\sqrt{-5}$ ein gemeinsamer Teiler x und y, so ist $N(a+b\sqrt{-5}) = a^2+5b^2$ ein gemeinsamer Teiler von $N(x) = 36$ und $N(y) = 24$, also ein Teiler von 12. Dies

liefert für (a,b) nur die Möglichkeiten $(\pm1,0)$, $(\pm2,0)$ und $(\pm1,\pm1)$. Da $\pm(1-\sqrt{-5})$ keine Teiler von $2+2\sqrt{-5}$ sind, sind die gemeinsamen Teiler von x und y genau die sechs Elemente ±1, ±2 und $\pm(1+\sqrt{-5})$. Keines dieser Elemente von R ist durch alle andern teilbar; also besitzen x und y keinen größten gemeinsamen Teiler.

Es sei $a+b\sqrt{-5}$ ein kleinstes gemeinsames Vielfaches von x und y. Dann ist $N(a+b\sqrt{-5})=a^2+5b^2$ ein gemeinsames Vielfaches von $N(x)=36$ und $N(y)=24$, also ein Vielfaches von 12. Andererseits teilt $a+b\sqrt{-5}$ jedes gemeinsame Vielfache von x und y, also beispielsweise $12=2(1+\sqrt{-5})(1-\sqrt{-5})$ und $6+6\sqrt{-5}$. Dann teilt $N(a+b\sqrt{-5})=a^2+5b^2$ auch $N(12)=144$ und $N(6+6\sqrt{-5})=216$ und muß damit ein Teiler von 72 sein. Insgesamt erhalten wir $a^2+5b^2\in\{12,24,36,72\}$. Dies liefert für (a,b) nur die Möglichkeiten $(\pm2,\pm2)$, $(\pm4,\pm2)$ und $(\pm6,\pm0)$. Nun ist 6 nicht teilbar durch $2+2\sqrt{-5}$, und $2\pm2\sqrt{-5}$ und $4\pm2\sqrt{-5}$ sind nicht teilbar durch 6. Die Annahme, $a+b\sqrt{-5}$ sei ein kleinstes gemeinsames Vielfaches von 6 und $2+2\sqrt{-5}$ führt also auf einen Widerspruch. (Durch Anwendung von Satz (2.5)(a) ließe sich das Argument noch etwas abkürzen.)

(f) Ist $d=a+b\sqrt{-5}$ ein gemeinsamer Teiler von 3 und $2+\sqrt{-5}$, so ist $N(a+b\sqrt{-5})=a^2+5b^2$ ein gemeinsamer Teiler von $N(3)=9$ und $N(2+\sqrt{-5})=9$, also 1, 3 oder 9. Dies liefert die Möglichkeiten $(a,b)=(\pm1,0)$, $(a,b)=(\pm3,0)$ und $(a,b)=(\pm2,\pm1)$; also sind die Ringelemente ±1, ±3 und $\pm2\pm\sqrt{-5}$ die einzig möglichen Kandidaten für gemeinsame Teiler von 3 und $2+\sqrt{-5}$. Nun ist 3 nicht durch $\pm2\pm\sqrt{-5}$ teilbar, und $2+\sqrt{-5}$ ist nicht durch ±3 teilbar; also sind ±1 die einzigen gemeinsamen Teiler (und damit zwangsläufig die größten gemeinsamen Teiler) von 3 und $2+\sqrt{-5}$. Wir behaupten, daß sich 1 (und damit auch -1) nicht als R-Linearkombination von 3 und $2+\sqrt{-5}$ schreiben läßt. Wäre

$$\begin{aligned}1 &= 3(a+b\sqrt{-5})+(2+\sqrt{-5})(c+d\sqrt{-5})\\ &= (3a+2c-5d)+(3b+c+2d)\sqrt{-5},\end{aligned}$$

so gälten die Gleichungen $3a+2c-5d=1$ und $3b+c+2d=0$, nach Addition dieser Gleichungen dann auch $3a+3b+3c-3d=1$, was modulo 3 sofort einen Widerspruch liefert. Also kann es keine R-lineare Darstellung der angegebenen Art geben.

Lösung (9.4) (a) Eine echte Zerlegung von X^2+1 wäre eine in zwei Polynome ersten Grades. Eine solche ist in $\mathbb{R}[X]$ nicht möglich, da X^2+1 keine reelle Nullstelle hat; in $\mathbb{R}[X]$ ist X^2+1 also irreduzibel. Wegen $X^2+1=(X+i)(X-i)$ ist X^2+1 dagegen reduzibel in $\mathbb{C}[X]$.

(b) Wegen $2X+2=2(X+1)$ ist $2X+2$ reduzibel in $\mathbb{Z}[X]$, denn weder 2 noch $X+1$ ist eine Einheit in $\mathbb{Z}[X]$. Dagegen ist 2 eine Einheit in $\mathbb{Q}[X]$, so daß $2X+2\sim X+1$ in $\mathbb{Q}[X]$ irreduzibel ist.

(c) Die Zerlegung $X^2-X-2=(X+1)(X-2)$ ist in $\mathbb{Z}[X]$ eine Zerlegung in echte Faktoren, so daß X^2-X-2 in $\mathbb{Z}[X]$ reduzibel ist. In $\mathbb{Z}[[X]]$ ist dagegen sowohl $X+1$ als auch $X-2$ (und damit auch X^2-X-2) eine Einheit.

(d) Die Zerlegung

$$X^4+4 \;=\; (X^2+2)^2-4X^2 \;=\; (X^2+2-2X)(X^2+2+2X)$$

zeigt, daß X^4+4 über jedem der Ringe $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ reduzibel ist.

Lösung (9.5) Die irreduziblen Elemente in $\mathbb{C}[X]$ sind nach dem Fundamentalsatz der Algebra genau die Polynome ersten Grades. Die irreduziblen Polynome in $\mathbb{R}[X]$ sind genau die Polynome ersten Grades und die nullstellenfreien Polynome zweiten Grades, also die von der Form $c\cdot\big((X+a)^2+b^2\big)$ mit $b\neq0$ und $c\neq0$.

Lösung (9.6) Wir nehmen an, $a+b\sqrt{-5}$ sei ein Teiler von $1-\sqrt{-5}$. Dann ist $N(a+b\sqrt{-5})=a^2+5b^2$ ein Teiler von $N(1-\sqrt{-5})=6$. Dies ist nur möglich für $(a,b)=(\pm1,0)$ oder $(a,b)=(\pm1,\pm1)$. Man rechnet sofort nach, daß $1-\sqrt{-5}$ kein Teiler von $1+\sqrt{-5}$ ist; also sind die einzigen Teiler von $1+\sqrt{-5}$ die Elemente ±1 und $\pm(1+\sqrt{-5})$, also Einheiten oder Assoziierte von $1+\sqrt{-5}$. Also hat $1+\sqrt{-5}$ keine echten Teiler und ist daher irreduzibel. Der Nachweis für 2, 3 und $1-\sqrt{-5}$ erfolgt völlig analog.

Die Gleichung $2\cdot3=6=(1+\sqrt{-5})(1-\sqrt{-5})$ zeigt, daß $1+\sqrt{-5}$ ein Teiler von $2\cdot3$. Andererseits teilt $1+\sqrt{-5}$ weder 2 noch 3, wie man entweder durch Betrachten der Norm sieht oder aber durch die Beobachtung, daß die Elemente $2/(1+\sqrt{-5})=(1+\sqrt{-5})/3$ und $3/(1+\sqrt{-5})=(1+\sqrt{-5})/2$, die man in $\mathbb{Q}+\mathbb{Q}\sqrt{-5}$ bilden kann, nicht in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$ liegen. Also ist $1+\sqrt{-5}$ kein Primelement in $\mathbb{Z}+\mathbb{Z}\sqrt{-5}$. Der Nachweis für die Elemente 2, 3 und $1-\sqrt{-5}$ ist vollkommen analog.

Lösung (9.7) Gilt $m+n=2$, so haben wir $m=n=1$, und die Behauptung gilt trivialerweise. Die Behauptung sei richtig für einen Wert $m+n$, und wir betrachten eine Gleichung der Form $p_1\cdots p_m p_{m+1}=q_1\cdots q_n$. (Wird statt m die Zahl n um 1 erhöht, so ist der Beweis vollkommen analog.) Dann teilt p_{m+1} die rechte Seite der Gleichung, folglich einen der Faktoren, sagen wir q_i. Es gilt dann $q_i=rp_{m+1}$ mit einem Element $r\in R$. Da q_i prim ist, folgt hieraus $q_i\mid r$ oder $q_i\mid p_{m+1}$. Aber $q_i\mid r$ ist unmöglich; sonst gälte $r=sq_i$ mit einem $s\in R$, damit $q_i=rp_{m+1}=sq_ip_{m+1}$ und damit $1=sp_{m+1}$, so daß p_{m+1} eine Einheit wäre. Also gilt $q_i\mid p_{m+1}$; da auch $p_{m+1}\mid q_i$ gilt, sind also p_{m+1} und q_i assoziiert, sagen wir $q_i=up_{m+1}$ mit einer Einheit $u\in R^\times$. Dividieren wir die Gleichung $p_1\cdots p_mp_{m+1}=q_1\cdots q_n$ durch p_{m+1}, so ergibt sich $p_1\cdots p_m=(uq_1)q_2\cdots\widehat{q_i}\cdots q_n$. Nach Induktionsannahme gilt $m=n-1$ und $p_j\sim q_{\sigma(j)}$ für eine Bijektion $\sigma:\{1,2,\ldots,i-1,i+1,\ldots,n\}\to\{1,\ldots,m\}$. Setzen wir noch $\sigma(i):=m+1$, so folgt die Behauptung.

Lösung (9.8) (a) Es gelten die folgenden Ä]quivalenzen: $a\mid b\Leftrightarrow b\in Ra\Leftrightarrow b\in\langle\!\langle a\rangle\!\rangle\Leftrightarrow\langle\!\langle b\rangle\!\rangle\subseteq\langle\!\langle a\rangle\!\rangle$.

(b) Genau dann sind a und b assoziiert, wenn die Bedingungen $a\mid b$ und $b\mid a$ gelten. Nach Teil (a) ist dies

genau dann der Fall, wenn die Inklusionen $\langle\!\langle a\rangle\!\rangle \supseteq \langle\!\langle b\rangle\!\rangle$ und $\langle\!\langle b\rangle\!\rangle \supseteq \langle\!\langle a\rangle\!\rangle$ gelten, also genau dann, wenn die Gleichheit $\langle\!\langle a\rangle\!\rangle = \langle\!\langle b\rangle\!\rangle$ gilt.

(c) Diese Aussage ist trivial.

(d) Ist x eine Einheit und ist $r \in R$ ein beliebiges Ringelement, so gilt $r = (rx^{-1})x \in Rx = \langle\!\langle x\rangle\!\rangle$. Da $r \in R$ beliebig war, gilt also $R \subseteq \langle\!\langle x\rangle\!\rangle$ und damit $\langle\!\langle x\rangle\!\rangle = R$. Gilt umgekehrt $\langle\!\langle x\rangle\!\rangle = R$, so gilt $1 \in \langle\!\langle x\rangle\!\rangle$; es gibt dann also ein Element $r \in R$ mit $1 = rx$, und diese Gleichung zeigt, daß x eine Einheit ist.

(e) Das Element x sei irreduzibel, und es gelte $\langle\!\langle x\rangle\!\rangle \subseteq \langle\!\langle a\rangle\!\rangle$. Dann gilt $a \mid x$. Da x keine echten Teiler hat, muß daher a eine Einheit oder zu x assoziiert sein; im ersten Fall gilt $\langle\!\langle a\rangle\!\rangle = R$, im zweiten Fall gilt $\langle\!\langle a\rangle\!\rangle = \langle\!\langle x\rangle\!\rangle$. Es gibt also in diesem Fall kein Element $a \in R$ mit $\langle\!\langle x\rangle\!\rangle \subsetneqq \langle\!\langle a\rangle\!\rangle \subsetneqq R$. Umgekehrt gelte diese Bedingung. Es sei a ein Teiler von x, so daß $\langle\!\langle x\langle\!\langle \subseteq \langle\!\langle a\rangle\!\rangle$. Nach Voraussetzung muß dann $\langle\!\langle a\rangle\!\rangle = \langle\!\langle x\rangle\!\rangle$ gelten. Im ersten Fall ist x assoziiert zu a, im zweiten Fall ist x eine Einheit. Damit ist gezeigt, daß x keine echten Teiler hat und folglich irreduzibel ist.

(f) Genau dann gilt $\langle\!\langle x\rangle\!\rangle \subseteq \bigcap_i \langle\!\langle a_i\rangle\!\rangle$, wenn x in jedem der Ideale $\langle\!\langle a_i\rangle\!\rangle = Ra_i$ liegt, wenn also x ein gemeinsames Vielfaches der Elemente a_i ist.

(g) Es gelte $\langle\!\langle x\rangle\!\rangle = \bigcap_i \langle\!\langle a_i\rangle\!\rangle$. Nach (h) ist dann x ein gemeinsames Vielfaches von $a_1, \ldots, a_n$. Jedes andere gemeinsame Vielfache von $a_1, \ldots, a_n$ ist dann enthalten in $\bigcap_i \langle\!\langle a_i\rangle\!\rangle = \langle\!\langle x\rangle\!\rangle$ und ist damit durch x teilbar. Damit ist gezeigt, daß x ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$ ist.

Umgekehrt sei x ein kleinstes gemeinsames Vielfaches von $a_1, \ldots, a_n$. Wegen (h) gilt dann zunächst $\langle\!\langle x\rangle\!\rangle \subseteq \bigcap_i \langle\!\langle a_i\rangle\!\rangle$. Zum Nachweis der umgekehrten Inklusion betrachten wir ein Element $y \in \langle\!\langle a_i\rangle\!\rangle$. Dieses ist dann ein gemeinsames Vielfaches von $a_1, \ldots, a_n$, folglich ein Vielfaches von x und damit ein Element von $\langle\!\langle x\rangle\!\rangle$.

(h) Genau dann gilt $\sum_i \langle\!\langle a_i\rangle\!\rangle \subseteq \langle\!\langle x\rangle\!\rangle$, wenn $\langle\!\langle a_i\rangle\!\rangle \subseteq \langle\!\langle x\rangle\!\rangle$ bzw. $a_i \in \langle\!\langle x\rangle\!\rangle$ für alle i gilt, wenn also x ein gemeinsamer Teiler von $a_1, \ldots, a_n$ ist.

(i) Es gelte $\langle x\rangle\!\rangle = \sum_i \langle\!\langle a_i\rangle\!\rangle$. Nach (j) ist dann x ein gemeinsamer Teiler von $a_1, \ldots, a_n$. Ist ferner y ein anderer gemeinsamer Teiler von $a_1, \ldots, a_n$, so liegt jedes der Elemente a_i in $\langle\!\langle y\rangle\!\rangle$; hieraus folgt dann $\sum_i \langle\!\langle a_i\rangle\!\rangle \subseteq \langle\!\langle y\rangle\!\rangle$ und damit $\langle\!\langle x\rangle\!\rangle \subseteq \langle\!\langle y\rangle\!\rangle$, also $x \in \langle\!\langle y\rangle\!\rangle$, so daß y ein Teiler von x ist. Damit ist gezeigt, daß x ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ ist.

Lösung (9.9) Wir berechnen

$$\frac{127+9i}{19+113i} \;=\; \frac{127+9i}{19+113i}\cdot\frac{19-113i}{19-113i} \;=\; \frac{343}{1313} - \frac{1418}{1313}i.$$

Das am dichtesten bei dieser Zahl liegende Element von $\mathbb{Z}+i\mathbb{Z}$ ist $0-i=-i$; wir schreiben also

$$(1) \qquad 127+9i \;=\; (-i)\cdot(19+113i)+(14+28i)\,.$$

Als nächstes berechnen wir

$$\frac{19+113i}{14+28i} \;=\; \frac{1}{14}\cdot\frac{19+113i}{1+2i}\cdot\frac{1-2i}{1-2i} \;=\; \frac{7}{2}+\frac{15}{14}i.$$

Hier gibt es zwei Elemente in $\mathbb{Z}+i\mathbb{Z}$, die von dieser Zahl minimalen Abstand haben, nämlich $3+i$ und $4+i$. Es ist egal, welche davon wir wählen; wir nehmen $3+i$ und schreiben daher

$$(2) \qquad 19+113i \;=\; (3+i)\cdot(14+28i)+(5+15i)\,.$$

Im nächsten Schritt berechnen wir

$$\frac{14+28i}{5+15i} \;=\; \frac{14}{5}\cdot\frac{1+2i}{1+3i}\cdot\frac{1-3i}{1+3i} \;=\; \frac{49}{25}-\frac{7}{25}i.$$

Das am dichtesten bei dieser Zahl liegende Element von $\mathbb{Z}+\mathbb{Z}i$ ist $2+0\cdot i=2$; wir schreiben also

$$(3) \qquad 14+28i \;=\; 2\cdot(5+15i)+(4-2i)\,.$$

Der nächste Schritt liefert

$$\frac{5+15i}{4-2i} \;=\; \frac{5}{2}\cdot\frac{1+3i}{2-i}\cdot\frac{2+i}{2+i} \;=\; \frac{-1}{2}+\frac{7}{2}i\,.$$

Hier gibt es sogar vier Elemente in $\mathbb{Z}+i\mathbb{Z}$, die von dieser Zahl minimalen Abstand haben, nämlich $-1+3i$, $-1+4i$, $0+3i$ und $0+4i$. Es ist egal, welche davon wir wählen; nehmen wir $3i$, so schreiben wir

$$(4) \qquad 5+15i \;=\; 3i\cdot(4-2i)+(-1+3i)\,.$$

Nun gilt

$$\frac{4-2i}{-1+3i} \;=\; \frac{4-2i}{-1+3i}\cdot\frac{-1-3i}{-1-3i} \;=\; -1-i.$$

Diese Zahl liegt selbst schon in $\mathbb{Z}+i\mathbb{Z}$. Wir erhalten also

$$(5) \qquad 4-2i \;=\; (-1-i)(-1+3i)\,.$$

Da jetzt kein Rest mehr auftritt, ist das Ende des Euklidischen Algorithmus erreicht; ein größter gemeinsamer Teiler von a und b ist also $-1+3i$, da dies der letzte von Null verschiedene Rest ist, der im Euklidischen Algorithmus auftritt. (Da ein ggT nur bis auf die Multiplikation mit Einheiten eindeutig bestimmt ist, sind daher die vier Zahlen $-1+3i$, $1-3i$, $-3-i$ und $3+i$ die sämtlichen größten gemeinsamen Teiler von a und b.) Um eine lineare Darstellung des ggT zu erhalten, lesen wir die gefundenen Gleichungen rückwärts und erhalten

$$\begin{aligned}
-1+3i &\overset{(4)}{=} (5+15i) - 3i(4-2i)\\
&\overset{(3)}{=} (5+15i) - 3i\cdot\big((14+28i) - 2\cdot(5+15i)\big)\\
&= (1+6i)(5+15i) - 3i\cdot(14+28i)\\
&\overset{(2)}{=} (1+6i)\big((19+113i) - (3+i)(14+28i)\big) - 3i\cdot(14+28i)\\
&= (1+6i)(19+113i) + (3-22i)(14+28i)\\
&\overset{(1)}{=} (1+6i)\cdot(19+113i) + (3-22i)\big((127+9i) + i\cdot(19+113i)\big)\\
&= (23+9i)(19+113i) + (3-22i)(127+9i).
\end{aligned}$$

Lösung (9.10) (a) Es sei p reduzibel in R. Dann gibt es eine Darstellung $p = (a + ib)(c + id)$, wobei $a + ib$ und $c + id$ keine Einheiten sind. Komplexe Konjugation dieser Gleichung liefert $p = (a - ib)(c - id)$ und damit $p^2 = (a+ib)(a-ib)(c+id)(c-id) = (a^2+b^2)(c^2+d^2)$. Da $a+ib$ und $c + id$ keiune Einheiten sind, haben wir $a^2 + b^2 > 1$ und $c^2 + d^2 > 1$; also muß $a^2 + b^2 = p = c^2 + d^2$ gelten. In der Darstellung $p = (a + ib)(c + id)$ haben also die beiden Faktoren den gleichen Betrag. Da ihr Produkt eine positive reelle Zahl ist, erzwingt dies $c + id = \overline{a + ib} = a - ib$. Also gilt $p = (a + ib)(a - ib) = a^2 + b^2$. Gilt umgekehrt $p = a^2+b^2$, so gilt $p = (a+ib)(a-ib)$, so daß p reduzibel in R ist. Eine Primzahl $p \in \mathbb{N}$ ist also genau dann reduzibel in R, wenn sie als Summe zweier Quadrate darstellbar ist. Dies ist genau dann der Fall, wenn entweder $p = 2$ oder aber $p \equiv 1$ moduzlo 4 gilt.

(b) Die Zahl $(a+ib)(a-ib) = a^2+b^2$ besitzt eine Primfaktorzerlegung in $\mathbb{Z}$. Diese ist zugleich eine Zerlegung in R. Zerlegen wir diejenigen der auftretenden Primfaktoren, die nicht selbst schon prim in R sind, gemäß Teil (a) in der Form $p = (x + iy)(x - iy)$, so erhalten wir eine Primfaktorzerlegung. Ist nun $a+ib$ irreduzibel und daher prim, so muß wegen der Eindeutigkeit der Primfaktorzerlegung entweder $a + ib$ selbst eine der Primzahlen p oder einer der auftretenden Faktoren $x+iy$ sein (jeweils bis auf Multiplikation mit einer Einheit). Damit ist die Behauptung beweisen.

(c) Es gilt $30 = 2 \cdot 3 \cdot 5$. Dabei sind $2 = 1^2 + 1^2$ und $5 = 2^2+1^2$ jeweils als Summe zweier Quadrate darstellbar, 3 dagegen nicht. Die (bis auf Reihenfoilge und Multiplikation mit Einheiten eindeutige) Primfaktorzerlegung von 30 in $\mathbb{Z} + i\mathbb{Z}$ ist daher

$$30 \;=\; (1 + i) \cdot (1 - i) \cdot 3 \cdot (2 + i) \cdot (2 - i).$$

Weiter gilt $(17 + 4i)(17 - 4i) = 17^2 + 4^2 = 305 = 5 \cdot 61$. Dabei sind $5 = 2^2 + 1^2$ und $61 = 5^2 + 6^2$ als Summen je zweier Quadrate darstellbar. Dies liefert in R die Primfaktorzerlegung $305 = (2 + i)(2 - i)(5 + 6i)(5 - 6i)$. Folglich besitzt $17+4i$ einen zu $2\pm i$ und einen zu $5\pm6i$ assoziierten Primteiler; mit anderen Worten, eines der vier Produkte $(2 \pm i)(5 \pm 6i)$ muß zu $17 + 4i$ assoziiert sein. Durchprobieren der Möglichkeiten liefert die Primfaktorzerlegung

$$17 + 4i \;=\; (2 - i) \cdot (5 - 6i) \cdot i \;=\; (2 - i) \cdot (6 + 5i).$$

Schließlich gilt $8+6i = 2\cdot(4+3i) = (1+i)(1-i)(4+3i)$. Um die Primfaktorzerlegung von $4+3i$ zu finden, schreiben wir $(4+3i)(4-3i) = 25 = 5\cdot5$ und beobachten, daß $5 = 2^2+1^2$ als Summe zweier Quadrate darstellbar ist. Wir erhalten also $(4+3i)(4-3i) = (2+i)(2-i)(2+i)(2-i)$. Hieraus folgt, daß $4+3i$ assoziiert zu $(2+i)^2 = 3+4i$ oder $(2-i)^2 = 3-4i$ sein muß; es gilt $4 + 3i = i \cdot (3 - 4i) = i \cdot (2 - i)^2$. Dies liefert die Primfaktorzerlegung

$$\begin{aligned} 8 + 6i \;&=\; (1 + i) \cdot (1 - i) \cdot (2 - i)^2 \cdot i \\ &=\; (1 + i) \cdot (1 - i) \cdot (2 - i) \cdot (1 + 2i). \end{aligned}$$

Lösung (9.x) Wir nehmen an, es gebe eine Zerlegung von f in zwei Polynome $f_1(X) = \sum_{k=0}^{r} a_k X^k$ und $f_2(X) = \sum_{k=0}^{s} b_k X^k$ (wobei $r + s = n$). Da nach Voraussetzung p prim und ein Teiler von $c_0 = a_0 b_0$ ist, gilt $p \mid a_0$ oder $p \mid b_0$; o.B.d.A. gelte $p|a_0$. Wegen $p^2 \nmid c_0$ gilt dann $p \nmid b_0$. Wieder nach Voraussetzung ist p ein Teiler von $c_1 = a_0 b_1 + a_1 b_0$, folglich ein Teiler von $a_1 b_0$, folglich ein Teiler von a_1. Weiter ist p ein Teiler von $c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$, folglich ein Teiler von $a_2 b_0$, folglich ein Teiler von a_2. Fahren wir in dieser Weise fort, so sehen wir, daß p alle Koeffizienten von f teilt, insbesondere auch c_n, was der Voraussetzung widerspricht. Die Annahme, f sei zerlegbar, führt also auf einen Widerspruch.

Lösung (9.y) (a) Das Polynom ist irreduzibel nach dem Eisenstein-Kriterium mit $p = 3$.

(b) Das Polynom ist irreduzibel nach dem Eisenstein-Kriterium mit $p = 3$.

(c) Da das Polynom keine Nullstelle in $\mathbb{Z}_2$ hat, kann es keine Zerlegung in ein Polynom vom Grad 1 und eines vom Grad 3 geben; wenn es also überhaupt in zwei Polynome kleineren Grades zerlegbar ist, dann in zwei irreduzible Polynome vom Grad 2. Da das Absolutglied 1 ist, kommen als potentielle Faktoren nur $X^2 + 1$ und $X^2 + X + 1$ in Frage. Da $X^2 + 1 = (X + 1)^2$ reduzibel ist, bleibt nur $X^2 + X + 1$ als möglicher Faktor. Das Polynom müßte also gleich $(X^2 + X + 1)^2 = X^4 + X^2 + 1$ sein, was aber nicht der Fall ist.

(d) Es gilt $p(X) = (X^5 - 1)/(X - 1)$. Wäre p reduzibel, dann auch $q(X) := p(X + 1) = \big((X + 1)^5 - 1\big)/X = X^4 + 5X^3 + 10X^2 + 10X^1 + 5$. Aber q ist irreduzibel nach dem Eisenstein-Kriterium (mit $p = 5$). Andere Begründung: Wäre p reduzibel über $\mathbb{Z}$, dann erst recht über $\mathbb{Z}_2$, was aber nach Teil (c) nicht der Fall ist.

(e) In $\mathbb{Z} + i\mathbb{Z}$ gelten die Gleichungen $-1 + 3i = (1 + i)(1 + 2i)$ und $2 = (1 + i)(1 - i)$. Da $1 + i$ ein Primelement in $\mathbb{Z} + i\mathbb{Z}$ ist, ist das Eisenstein-Kriterium mit $p := 1 + i$ anwendbar.

(f) Wir behaupten zunächst, daß $p(X, Y) := X^2 + Y^3$ irreduzibel (und daher prim) in $K[X, Y]$ ist. Ist dies gezeigt, so können wir auf $X^2 + Y^3 + Z^5 = Z^5 + p \in K[X, Y][Z]$ das Eisenstein-Kriterium anwenden une erkennen, daß dann auch $X^2 + Y^3 + Z^5$ irreduzibel ist (und zwar in $K[X, Y][Z] \cong K[X, Y, Z]$). Wir nehmen an, p sei irreduzibel. Es gibt dann eine Darstellung $X^2 + Y^3 = (A_0 + A_1)(B_0 + B_1 + B_2)$, wobei A_i bzw. B_i jeweils ein Polynom in X und Y bezeichnet, das homogen vom Grad i ist. Ausmultiplizieren ergibt

$$X^2 + Y^3 \;=\; A_0 B_0 + (A_0 B_1 + A_1 B_0) + (A_0 B_2 + A_1 B_1) + A_1 B_2.$$

Da die homogenen Anteil eines Polynoms eindeutig bestimmt sind, führt dies auf die Gleichungen $A_0 B_0 = 0$, $A_0 B_1 + A_1 B_0 = 0$, $A_0 B_2 + A_1 B_1 = X^2$ und $A_1 B_2 = Y^3$. Wir unterscheiden zwei Fälle.

Erster Fall: $A_0 = 0$. Dann ist $A_1 B_0 = 0$, folglich $B_0 = 0$, weiter $A_1 B_1 = X^2$ und $A_1 B_2 = Y^3$. Hieraus folgt einerseits $A_1 = cX$ mit einer Einheit c, andererseits $A_1 = dY$ mit einer Einheit d, was sich natürlich widerspricht.

Zweiter Fall: $B_0 = 0$. Dann ist $A_0 B_1 = 0$; wir dürfen dann $B_1 = 0$ annehmen (denn den Fall $A_0 = 0$ haben wir bereits ausgeschlossen). Weiter gelten die Gleichungen $A_0 B_2 = X^2$ und $A_1 B_2 = Y^3$. Hieraus folgt einerseits $B_2 = uX^2$ mit einer Einheit u, andererseits $B_2 = vY^2$ mit einer Einheit v, was sich natürlich widerspricht.

Lösung (9.z) Über einem Körper der Charakteristik 3 haben wir $(X + Y)^3 = X^3 + 3X^2 Y + 3XY^2 + Y^3 = X^3 + Y^3$ und induktiv dann $X_1^3 + \cdots + X_n^3 = (X_1 + \cdots + X_n)^3$, so daß f in diesem Fall reduzibel ist. Wir nehmen nun an, die Charakteristik von K sei von 3 verschieden. Für $n = 1$ ist f reduzibel, denn $X^3 = X \cdot X \cdot X$. Für $n = 2$ ist f ebenfalls reduzibel, denn

$$X^3 + Y^3 \;=\; (X + Y)(X^2 - XY + Y^2).$$

Wir behaupten, daß f für $n = 3$ irreduzibel ist. Dazu fassen wir f als Polynom in Z über dem Ring $R := K[X, Y]$ auf und schreiben

$$X^3 + Y^3 + Z^3 \;=\; Z^3 + (X + Y)(X^2 - XY + Y^2).$$

Das Primelement $p := X + Y \in R$ erfüllt nun die Voraussetzungen des Eisenstein-Kriteriums, denn $X + Y$ ist kein Teiler von $X^2 - XY + Y^2 =: q(X, Y)$, denn es gilt $q(X, -X) = 3X^2 \neq 0$. (Hier geht ein, daß K nicht die Charakteristik 3 hat!) Also ist f irreduzibel in $K[X, Y][Z] \cong K[X, Y, Z]$. Für $n \geq 3$ folgt die Behauptung dann mit vollständiger Induktion. Ist nämlich $p := X_1^3 + \cdots + X_n^3$ irreduzibel nach Induktionsannahme und daher prim, so ist $X_1^3 + \cdots + X_n^3 + X_{n+1}^3 = X_{n+1}^3 + p$ irreduzibel in $K[X_1, \ldots, X_n][X_{n+1}] \cong K[X_1, \ldots, X_n, X_{n+1}]$ nach dem Eisenstein-Kriterium.