N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 4

Aufgabe 13

(1) Man finde in $\mathbb{Z}[\mathrm{i}]$ zwei nicht assoziierte Primelemente von Grad 13; vgl. Beispiel 47.(3).

(2) In $\mathbb{F}_5[X]$ bestimme man je ein normiertes irreduzibles Polynom von Grad 1, von Grad 2 und von Grad 3.

Lösung zu Aufgabe 13:

(1) Wir betrachten die Gradfunktion $d : \mathbb{Z}[\mathrm{i}]^\times \to \mathbb{Z}_{\geqslant 0} : z \mapsto d(z) = |z^2|$, vgl. Beispiel 47.(3).

Für $z = a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]^\times$ mit $a, b \in \mathbb{Z}$ ist somit $d(a + b\mathrm{i}) = a^2 + b^2$. Beachte, dass für $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ gilt:

$$d(z_1 z_2) = |z_1 z_2|^2 = (|z_1| \cdot |z_2|)^2 = |z_1|^2 \cdot |z_2|^2 = d(z_1)d(z_2) \ .$$

Wir zeigen: Für $a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]^\times$ sind die folgenden Aussagen äquivalent.

(I) $a + b\mathrm{i} \in \mathrm{U}(\mathbb{Z}[\mathrm{i}])$

(II) $d(a + b\mathrm{i}) = 1$

(III) $a + b\mathrm{i} \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$

(I) $\Rightarrow$ (II): Für $u \in \mathrm{U}(\mathbb{Z}[\mathrm{i}])$ ist

$$1 = d(1) = d(u \cdot u^{-1}) = \underbrace{d(u)}_{\in \mathbb{Z}_{\geqslant 0}} \underbrace{d(u^{-1})}_{\in \mathbb{Z}_{\geqslant 0}} \ .$$

Also $d(u) = 1$, da $d(u) \geqslant 0$ und $d(u) \in \mathrm{U}(\mathbb{Z}) = \{-1, 1\}$.

(II) $\Rightarrow$ (III): Für $a, b \in \mathbb{Z}$ mit

$$1 = d(a + b\mathrm{i}) = \underbrace{a^2}_{\in \mathbb{Z}_{\geqslant 0}} + \underbrace{b^2}_{\in \mathbb{Z}_{\geqslant 0}}$$

folgt $(a, b) \in \{(1, 0), (0, 1), (-1, 0), (0, -1)\}$, d.h. $a + b\mathrm{i} \in \{1, \mathrm{i}, -1, -\mathrm{i}\}$.

(III) $\Rightarrow$ (I): Gilt, da $1 = 1 \cdot 1 = (-1) \cdot (-1) = \mathrm{i} \cdot (-\mathrm{i}) = (-\mathrm{i}) \cdot \mathrm{i}$.

Somit sind die Aussagen äquivalent.

Es ist

$$13 = 9 + 4 = (3 + 2\mathrm{i})(3 - 2\mathrm{i}) \ .$$

Zusätzlich ist $3 + 2\mathrm{i} \neq u \cdot (3 - 2\mathrm{i})$ für $u \in \mathrm{U}(\mathbb{Z}[\mathrm{i}]) = \{1, \mathrm{i}, -1, -\mathrm{i}\}$.

Es sind also $3 + 2\mathrm{i}$ und $3 - 2\mathrm{i}$ zwei Elemente von Grad 13, die nicht assoziiert sind.

Wir zeigen, dass $3+2\mathrm{i}$ prim ist. Da $\mathbb{Z}[\mathrm{i}]$ ein Hauptidealbereich ist (Beispiel 52.(3)), genügt es zu zeigen, dass $3 + 2\mathrm{i}$ irreduzibel ist, vgl. Lemma 58.

Angenommen $3 + 2\mathrm{i}$ ist nicht irreduzibel. Dann gibt es $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ mit $z_1, z_2 \notin \mathrm{U}(\mathbb{Z}[\mathrm{i}])$ so, dass $z_1 z_2 = 3 + 2\mathrm{i}$ ist. Nun ist

$$13 = d(3 + 2\mathrm{i}) = d(z_1 z_2) = \underbrace{d(z_1)}_{\in \mathbb{Z}_{\geqslant 0}} \cdot \underbrace{d(z_2)}_{\in \mathbb{Z}_{\geqslant 0}}$$

und also $d(z_1) = 1$ oder $d(z_2) = 1$, da 13 irreduzibel in $\mathbb{Z}$ ist. Dann ist aber z_1 oder z_2 eine Einheit. *Widerspruch.*

Wir zeigen, dass $3 - 2\mathrm{i}$ prim ist. Es genügt zu zeigen, dass $3 - 2\mathrm{i}$ irreduzibel ist.

Angenommen $3 - 2\mathrm{i}$ ist nicht irreduzibel. Dann gibt es $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ mit $z_1, z_2 \notin \mathrm{U}(\mathbb{Z}[\mathrm{i}])$ so, dass $z_1 z_2 = 3 - 2\mathrm{i}$ ist. Nun ist

$$13 = d(3 - 2\mathrm{i}) = d(z_1 z_2) = \underbrace{d(z_1)}_{\in \mathbb{Z}_{\geqslant 0}} \cdot \underbrace{d(z_2)}_{\in \mathbb{Z}_{\geqslant 0}}$$

und also $d(z_1) = 1$ oder $d(z_2) = 1$, da 13 irreduzibel in $\mathbb{Z}$ ist. Dann ist aber z_1 oder z_2 eine Einheit. *Widerspruch.*

(2) Jedes Polynom von Grad 1 ist irreduzibel. Z.B. ist $X - 1 \in \mathbb{F}_5[X]$ irreduzibel.

Es ist $X^2 - 2 \in \mathbb{F}_5[X]$ irreduzibel, da es keine Nullstelle in $\mathbb{F}_5$ besitzt und folglich nicht in zwei Faktoren von Grad 1 zerfallen kann.

Es ist $X^3 + X + 1 \in \mathbb{F}_5[X]$ irreduzibel, da es keine Nullstelle in $\mathbb{F}_5$ besitzt und folglich nicht in einen Faktor von Grad 1 und einen Faktor von Grad 2 zerfallen kann.

Aufgabe 14 Sei R ein faktorieller Ring und $K = \mathrm{Quot}(R)$. Sei $p \in R$ prim.
Man zeige folgendes.

(1) Seien $x,\, y \in R^\times$. Sei $g \in R^\times$ ein größter gemeinsamer Teiler von x und y. Dann ist 1 ein größter gemeinsamer Teiler von $\frac{x}{g}$ und $\frac{y}{g}$.

(2) Für $x, y \in K$ ist $\mathrm{v}_p(x \cdot y) = \mathrm{v}_p(x) + \mathrm{v}_p(y)$.

(3) Für $x, y \in K$ ist $\mathrm{v}_p(x + y) \geqslant \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\}$.
Ist $\mathrm{v}_p(x) \neq \mathrm{v}_p(y)$, dann gilt $\mathrm{v}_p(x + y) = \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\}$.

Lösung zu Aufgabe 14:

(1) Sei $h \in R^\times$ ein größter gemeinsamer Teiler von $\frac{x}{g}$ und $\frac{y}{g}$. Dann ist $\frac{x}{g} = h \cdot s$ für ein $s \in R^\times$ und $\frac{y}{g} = h \cdot t$ für ein $t \in R^\times$. Es folgt $x = g \cdot h \cdot s$ und $y = g \cdot h \cdot t$. Also ist gh ein gemeinsamer Teiler von x und y. Da g größter gemeinsamer Teiler von x und y ist, folgt $gh | g$. Also ist h eine Einheit und daher assoziiert zu 1. Folglich ist 1 ein größter gemeinsamer Teiler von $\frac{x}{g}$ und $\frac{y}{g}$.

(2) (I) Seien $r, \tilde{r} \in R^\times$.
Es gibt t, $\tilde{t}$, $s \in R^\times$ mit

$$\begin{aligned} r &= p^{\mathrm{v}_p(r)} \cdot t\,, \\ \tilde{r} &= p^{\mathrm{v}_p(\tilde{r})} \cdot \tilde{t}\,, \\ r \cdot \tilde{r} &= p^{\mathrm{v}_p(r \cdot \tilde{r})} \cdot s \end{aligned}$$

und $p \nmid t$, $\tilde{t}$, s.
Nun ist

$$p^{\mathrm{v}_p(r \cdot \tilde{r})} \cdot s = r \cdot \tilde{r} = p^{\mathrm{v}_p(r)} \cdot t \cdot p^{\mathrm{v}_p(\tilde{r})} \cdot \tilde{t}\,.$$

Es teilt $p^{\mathrm{v}_p(r) + \mathrm{v}_p(\tilde{r})}$ das Element $r \cdot \tilde{r}$. Also ist $\mathrm{v}_p(r) + \mathrm{v}_p(\tilde{r}) \leqslant \mathrm{v}_p(r \cdot \tilde{r})$ nach Definition.
Es wird

$$p^{\mathrm{v}_p(r \cdot \tilde{r}) - \mathrm{v}_p(r) - \mathrm{v}_p(\tilde{r})} \cdot s = t \cdot \tilde{t}\,.$$

Da $p \nmid t$, $\tilde{t}$, ist $\mathrm{v}_p(r \cdot \tilde{r}) - \mathrm{v}_p(r) - \mathrm{v}_p(\tilde{r}) = 0$.
Somit gilt $\mathrm{v}_p(r \cdot \tilde{r}) = \mathrm{v}_p(r) + \mathrm{v}_p(\tilde{r})$.

(II) Falls $x = 0$ oder $y = 0$ ist, dann sind beide Seiten der behaupteten Gleichung gleich ∞. Sei im Weiteren also $x \neq 0$ und $y \neq 0$.

(III) Schreibe $x = \frac{a}{b}$, $y = \frac{c}{d}$ mit $a, b, c, d \in R^\times$. Dann ist

$$\begin{aligned} \mathrm{v}_p(x \cdot y) = \mathrm{v}_p\left(\tfrac{a \cdot c}{b \cdot d}\right) &= \mathrm{v}_p(a \cdot c) - \mathrm{v}_p(b \cdot d) \\ &\overset{\text{(I)}}{=} \mathrm{v}_p(a) + \mathrm{v}_p(c) - (\mathrm{v}_p(b) + \mathrm{v}_p(d)) \\ &= \mathrm{v}_p(a) - \mathrm{v}_p(b) + \mathrm{v}_p(c) - \mathrm{v}_p(d) \\ &= \mathrm{v}_p(x) + \mathrm{v}_p(y) \ . \end{aligned}$$

(3) (I) Seien $r, \tilde{r} \in R^\times$. Schreibe $k := \min\{\mathrm{v}_p(r), \mathrm{v}_p(\tilde{r})\}$.
Aus $r \in (p^{\mathrm{v}_p(r)}) \subseteq (p^k)$ und $\tilde{r} \in (p^{\mathrm{v}_p(\tilde{r})}) \subseteq (p^k)$ folgt, da $(p^k) \trianglelefteq R$, auch $r + \tilde{r} \in (p^k)$.
Also ist $\mathrm{v}_p(r + \tilde{r}) \geqslant k = \min\{\mathrm{v}_p(r), \mathrm{v}_p(\tilde{r})\}$.

(II) Falls $x = 0$ ist, dann ist $\mathrm{v}_p(x + y) = \mathrm{v}_p(y) = \min\{\infty, \mathrm{v}_p(y)\} = \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\}$.
Falls $y = 0$ ist, dann ist $\mathrm{v}_p(x + y) = \mathrm{v}_p(x) = \min\{\mathrm{v}_p(x), \infty\} = \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\}$.
Sei im Weiteren also $x \neq 0$ und $y \neq 0$.

(III) Schreibe $x = \frac{a}{b}$, $y = \frac{c}{d}$ mit $a, b, c, d \in R^\times$.
Es ist

$$\begin{aligned} \mathrm{v}_p(x + y) = \mathrm{v}_p(\tfrac{a \cdot d + b \cdot c}{b \cdot d}) &= \mathrm{v}_p(a \cdot d + b \cdot c) - \mathrm{v}_p(b \cdot d) \\ &\overset{\text{(I)}}{\geqslant} \min\{\mathrm{v}_p(a \cdot d), \mathrm{v}_p(b \cdot c)\} - \mathrm{v}_p(b \cdot d) \\ &\overset{(2)}{=} \min\{\mathrm{v}_p(a) + \mathrm{v}_p(d), \mathrm{v}_p(b) + \mathrm{v}_p(c)\} - \mathrm{v}_p(b) - \mathrm{v}_p(d) \\ &= \min\{\mathrm{v}_p(a) + \mathrm{v}_p(d) - \mathrm{v}_p(b) - \mathrm{v}_p(d), \mathrm{v}_p(b) + \mathrm{v}_p(c) - \mathrm{v}_p(b) - \mathrm{v}_p(d)\} \\ &= \min\{\mathrm{v}_p(a) - \mathrm{v}_p(b), \mathrm{v}_p(c) - \mathrm{v}_p(d)\} \\ &= \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} \ . \end{aligned}$$

Sei nun $\mathrm{v}_p(x) \neq \mathrm{v}_p(y)$.
Sei ohne Einschränkung $\mathrm{v}_p(x) < \mathrm{v}_p(y)$. Beachte: Es ist $\mathrm{v}_p(y) = \mathrm{v}_p(-y)$. Nun ist

$$\mathrm{v}_p(y) > \mathrm{v}_p(x) = \mathrm{v}_p((x + y) + (-y)) \geqslant \min\{\mathrm{v}_p(x + y), \mathrm{v}_p(y)\} \ .$$

Da $\mathrm{v}_p(y) > \min\{\mathrm{v}_p(x + y), \mathrm{v}_p(y)\}$ ist, ist $\min\{\mathrm{v}_p(x + y), \mathrm{v}_p(y)\} = \mathrm{v}_p(x + y)$.
Somit folgt $\mathrm{v}_p(x) \geqslant \mathrm{v}_p(x + y) \geqslant \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} = \mathrm{v}_p(x)$ und damit Gleichheit.
Alternativ: Schreibe $x = p^{\mathrm{v}_p(x)} \cdot s$ und $y = p^{\mathrm{v}_p(y)} \cdot t$ mit $s, t \in R \setminus (p)$.
Sei ohne Einschränkung $\mathrm{v}_p(x) < \mathrm{v}_p(y)$ und $d := \mathrm{v}_p(y) - \mathrm{v}_p(x) > 0$. Nun ist

$$\mathrm{v}_p(x + y) = \mathrm{v}_p(p^{\mathrm{v}_p(x)}(s + tp^d)) \overset{(2)}{=} \mathrm{v}_p(p^{\mathrm{v}_p(x)}) + \mathrm{v}_p(s + tp^d) \ .$$

Es ist $\mathrm{v}_p(s + tp^d) = 0$, da $s \notin (p)$ und $t \cdot p^d \in (p^d) \subseteq (p)$. *Wäre* $s + tp^d \in (p)$, dann wäre auch $s = s + tp^d + p \cdot (-tp^{d-1}) \in (p)$, da $(p) \trianglelefteq R$ ein Ideal ist. Aber das ist *nicht* der Fall.
Also ist

$$\mathrm{v}_p(x + y) = \mathrm{v}_p(p^{\mathrm{v}_p(x)}) + \mathrm{v}_p(s + tp^d) = \mathrm{v}_p(x) = \min\{\mathrm{v}_p(x), \mathrm{v}_p(y)\} \ .$$

Aufgabe 15

(1) In $\mathbb{Z}$ bestimme man $\mathrm{ggT}(65, 169)$ zunächst via Primfaktorzerlegung und anschließend mit Hilfe des Euklidischen Algorithmus.

(2) In $\mathbb{Q}[X]$ bestimme man $\mathrm{ggT}(X^6-1,\, X^4-2X^2+1)$.

(3) In $\mathbb{F}_2[X]$ bestimme man $\mathrm{ggT}(X^3+X+1,\, X^5+X^2)$.

(4) In $\mathbb{Q}[X,Y]$ bestimme man $\mathrm{ggT}(X^2Y+X^2,\, XY^2+XY)$.

Lösung zu Aufgabe 15:

(1) Es ist $65 = 5 \cdot 13$ und $169 = 13^2$. Somit ist $\mathrm{ggT}(65, 169) = 13$.

Der Euklidische Algorithmus liefert folgendes.

Es ist $169 = 65 \cdot 2 + 39$. Also ist $\mathrm{ggT}(169, 65) = \mathrm{ggT}(65, 39)$.

Es ist $65 = 39 + 26$. Also ist $\mathrm{ggT}(65, 39) = \mathrm{ggT}(39, 26)$.

Es ist $39 = 26 + 13$. Also ist $\mathrm{ggT}(39, 26) = \mathrm{ggT}(26, 13)$.

Es ist $26 = 13 \cdot 2 + 0$. Also ist $\mathrm{ggT}(26, 13) = \mathrm{ggT}(13, 0) = 13$.

Insgesamt ist $\mathrm{ggT}(169, 65) = 13$.

(2) Der Euklidische Algorithmus liefert folgendes.

Es ist $X^6-1 = (X^4-2X^2+1)\cdot(X^2+2)+3X^2-3$. Also ist $\mathrm{ggT}(X^6-1,\, X^4-2X^2+1) = \mathrm{ggT}(X^4-2X^2+1, 3X^2-3)$.

Es ist $X^4-2X^2+1 = (3X^2-3)\cdot\frac{1}{3}(X^2-1)+0$. Also ist $\mathrm{ggT}(X^4-2X^2+1, 3X^2-3) = \mathrm{ggT}(3X^2-3, 0) = X^2-1$.

Insgesamt ist $\mathrm{ggT}(X^6-1,\, X^4-2X^2+1) = X^2-1$.

(3) Der Euklidische Algorithmus liefert folgendes.

Es ist $X^5+X^2 = (X^3+X+1)\cdot(X^2+1)+X+1$. Also ist $\mathrm{ggT}(X^5+X^2,\, X^3+X+1) = \mathrm{ggT}(X^3+X+1, X+1)$.

Es ist $X^3+X+1 = (X+1)\cdot(X^2+X)+1$. Also ist $\mathrm{ggT}(X^3+X+1, X+1) = \mathrm{ggT}(X+1, 1) = 1$.

Insgesamt ist $\mathrm{ggT}(X^5+X^2,\, X^3+X+1) = 1$.

Alternativ: Es ist $X^3+X+1 \in \mathbb{F}_2[X]$ irreduzibel, da es keine Nullstelle in $\mathbb{F}_2$ hat und daher nicht in ein Polynom von Grad 2 und eins von Grad 1 zerfallen kann. Es besitzt also nur die Teiler 1 und X^3+X+1. Das Polynom X^5+X^2 ist nicht ohne Rest duch X^3+X+1 teilbar. Somit ergibt sich $\mathrm{ggT}(X^5+X^2,\, X^3+X+1) = 1$.

(4) Da $\mathbb{Q}[X,Y]$ kein Hauptidealbereich ist, ist der Euklidische Algorithmus nicht anwendbar. Es ist

$$\begin{aligned} X^2Y+X^2 &= Y^0\cdot(Y+1)^1\cdot X^2 \\ XY^2+XY &= Y^1\cdot(Y+1)^1\cdot X^1\ . \end{aligned}$$

Somit ist $\mathrm{ggT}(X^2Y+X^2,\, XY^2+XY) = Y^0\cdot(Y+1)^1\cdot X^1 = XY+X$.

Aufgabe 16

(1) Man bestimme in S_4

$$(1,2,3)\circ(1,4)(2,3).$$

(2) Man bestimme in S_4

$$(1,2,3)\circ(1,4,2,3).$$

(3) Sei $f := (1,4,2,3)$. Man bestimme ein $g \in \mathrm{S}_4$ so, dass $f\circ g = \mathrm{id}$ ist.

(4) Sei $h := (1,2)(3,4) \in \mathrm{S}_4$. Man bestimme ein $i \in \mathrm{S}_4$ so, dass $i \circ h$ aus einem Zykel der Länge 4 besteht.

Lösung zu Aufgabe 16:

(1) Es ist $(1,2,3) \circ (1,4)(2,3) = (1,4,2)$.

(2) Es ist $(1,2,3) \circ (1,4,2,3) = (1,4,3,2)$.

(3) Es ist $(1,4,2,3) \circ (1,3,2,4) = \mathrm{id}$.

(4) Es ist z.B. $(1,3) \circ (1,2)(3,4) = (1,2,3,4)$.