M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 3

Aufgabe 9 Sei $\zeta := \zeta_3 := \exp(2\pi \mathrm{i}/3) \in \mathbb{C}$.

(1) Man bestimme $(\zeta - 1)(\zeta^2 + \zeta + 1)$. Man folgere: $\zeta^2 + \zeta + 1 = 0$.
Man berechne $|x + y\zeta|^2$ für $x,\, y \in \mathbb{R}$.

(2) Man zeige: Es ist $\mathbb{Z}[\zeta] := \{\, a + b\zeta \,:\, a,\, b \in \mathbb{Z} \,\} \subseteq \mathbb{C}$ ein Teilring.

(3) Seien $x,\, y \in \mathbb{R}$. Seien $a,\, b \in \mathbb{Z}$ gewählt mit $|x - a| \leqslant \frac{1}{2}$ und $|y - b| \leqslant \frac{1}{2}$. Man zeige:

$$|(x + y\zeta) - (a + b\zeta)|^2 \;\leqslant\; \frac{3}{4}\,.$$

(4) Sei $d : \mathbb{Z}[\zeta]^\times \to \mathbb{Z}_{\geqslant 0} : z \mapsto d(z) := |z|^2$.
Man zeige: d ist eine Gradfunktion und folglich $\mathbb{Z}[\zeta]$ ein euklidischer Ring.

Lösung.
Zu (1). Es wird $(\zeta - 1)(\zeta^2 + \zeta + 1) = \zeta^3 + \zeta^2 + \zeta - \zeta^2 - \zeta - 1 = \zeta^3 - 1 = 0$.
Da $\zeta \neq 1$, folgt $\zeta^2 + \zeta + 1 = 0$.
Zu (2). Es ist $1 = 1 \cdot 1 + 0 \cdot \zeta \in \mathbb{Z}[\zeta]$.
Seien $x = a + b\zeta$, $x' = a' + b'\zeta \in \mathbb{Z}[\zeta]$ gegeben, wobei $a,\, b,\, a',\, b' \in \mathbb{Z}$.
Es ist $x - x' = (a - a') + (b - b')\zeta \in \mathbb{Z}[\zeta]$.
Es ist

$$\begin{array}{rcl} x \cdot x' & = & (a + b\zeta) \cdot (a' + b'\zeta) \\ & = & aa' + (ab' + ba')\zeta + bb'\zeta^2 \\ & = & aa' + (ab' + ba')\zeta + bb'(-1 - \zeta) \\ & = & (aa' - bb') + (ab' + ba' - bb')\zeta \\ & \in & \mathbb{Z}[\zeta]\,. \end{array}$$

Also ist $\mathbb{Z}[\zeta] \subseteq \mathbb{C}$ ein Teilring.
Zu (3). Kürzen wir $s := x - a$ und $t := y - b$ ab, so ist $|s| \leqslant \frac{1}{2}$ und $|t| \leqslant \frac{1}{2}$. Dann ist auch $|s - \frac{1}{2}t| \leqslant \frac{3}{4}$.
Ferner erinnern wir an $\overline{\zeta} = \overline{\exp(2\pi \mathrm{i}/3)} = \exp(-2\pi \mathrm{i}/3) = \exp(4\pi \mathrm{i}/3) = \zeta^2$.
Damit wird

$$\begin{array}{rcl} |(x + y\zeta) - (a + b\zeta)|^2 & = & |s + t\zeta|^2 \\ & = & (s + t\zeta)\overline{(s + t\zeta)} \\ & = & (s + t\zeta)(s + t\zeta^2) \\ & = & s^2 + st\zeta + st\zeta^2 + t^2\zeta^3 \\ & = & s^2 + st\zeta + st(-1 - \zeta) + t^2 \\ & = & s^2 + t^2 - st \\ & = & (s - \frac{1}{2}t)^2 + \frac{3}{4}t^2 \\ & \leqslant & \frac{9}{16} + \frac{3}{4} \cdot \frac{1}{4} \\ & = & \frac{3}{4}\,. \end{array}$$

Zu (4). Sei $u \in \mathbb{Z}[\zeta]$. Sei $v \in \mathbb{Z}[\zeta]^\times$. Wir bilden $\frac{u}{v}$ in $\mathbb{C}$. Wir schreiben $\frac{u}{v} = x + y\zeta$ mit $x,\, y \in \mathbb{R}$.
Wir wählen $a \in \mathbb{Z}$ mit $|x - a| \leqslant \frac{1}{2}$. Wir wählen $b \in \mathbb{Z}$ mit $|y - b| \leqslant \frac{1}{2}$. Dies ist mit einer Rundung zu einer ganzen Zahl erreichbar.
Sei $q := a + b\zeta \in \mathbb{Z}[\zeta]$. Gemäß (3) ist $|\frac{u}{v} - q| \leqslant \frac{3}{4}$.
Sei $r := u - vq \in \mathbb{Z}[\zeta]$. Es wird

$$u \;=\; vq + r\,,$$

wobei

$$\begin{array}{rcl} d(r) & = & |r|^2 \\ & = & |u - vq|^2 \\ & = & |\frac{u}{v} - q|^2 \cdot |v|^2 \\ & \leqslant & \frac{3}{4}|v|^2 \\ & < & |v|^2 \\ & = & d(v) \; . \end{array}$$

Somit ist $\mathbb{Z}[\zeta]$, mit der Gradfunktion d, ein euklidischer Ring.

Aufgabe 10

(1) Man finde $q,\, r \;\in\; \mathbb{Z}[\mathrm{i}]$ mit $2 - 3\mathrm{i} = (1 + 2\mathrm{i})q + r$, wobei $|r|^2 < |1 + 2\mathrm{i}|^2$.

(2) Man zeige: Für $u \in \mathrm{U}(\mathbb{Z}[\mathrm{i}])$ ist $|u|^2 \in \mathrm{U}(\mathbb{Z})$. Man bestimme $\mathrm{U}(\mathbb{Z}[\mathrm{i}])$.

(3) Sei $\zeta := \zeta_3 := \exp(2\pi\mathrm{i}/3) \in \mathbb{C}$.
Man finde $q,\, r \;\in\; \mathbb{Z}[\zeta]$ mit $2 - 3\zeta = (1 + 2\zeta)q + r$, wobei $|r|^2 < |1 + 2\zeta|^2$.

Lösung.
Zu (1). Wir berechnen $\frac{2-3\mathrm{i}}{1+2\mathrm{i}} = \frac{(2-3\mathrm{i})(1-2\mathrm{i})}{(1+2\mathrm{i})(1-2\mathrm{i})} = \frac{-4-7\mathrm{i}}{5} = -\frac{4}{5} - \frac{7}{5}\mathrm{i}$.
Runden des Real- und des Imaginärteils gibt $q := -1 - \mathrm{i}$.
Dann wird $r := (2 - 3\mathrm{i}) - (1 + 2\mathrm{i})(-1 - \mathrm{i}) = 2 - 3\mathrm{i} + 1 + \mathrm{i} + 2\mathrm{i} - 2 = 1$.
Alles in allem ist

$$(2 - 3\mathrm{i}) = (1 + 2\mathrm{i})(-1 - \mathrm{i}) + 1 \; ,$$

wobei $|1|^2 = 1 < 5 = |1 + 2\mathrm{i}|^2$.
Zu (2). Sei $u \in \mathrm{U}(\mathbb{Z}[\mathrm{i}])$. Dann ist auch $v := u^{-1} \in \mathbb{Z}[\mathrm{i}]$, und insbesondere $|v|^2 = v \cdot \overline{v} \in \mathbb{Z}$.
Aus $1 = u \cdot u^{-1}$ folgt $1 = |1|^2 \;=\; |u|^2 \cdot |v|^2$. Da $|v|^2 \in \mathbb{Z}$ ist, folgt $|u|^2 \in \mathrm{U}(\mathbb{Z}) = \{-1, +1\}$.
Es folgt wegen $|u|^2 \geqslant 0$ auch noch $|u|^2 = 1$.
Schreiben wir $u = a + b\mathrm{i}$, so ist also $|u|^2 = a^2 + b^2 = 1$. Da $a,\, b, \in\, \mathbb{Z}$ sind, folgt

$$(a, b) \;\in\; \{(1, 0), (-1, 0), (0, 1), (0, -1)\} \; .$$

Diese 4 Paare liefern alle auch eine Einheit. Somit ist

$$\mathrm{U}(\mathbb{Z}[\mathrm{i}]) \;=\; \{1, -1, \mathrm{i}, -\mathrm{i}\} \; .$$

Zu (3). Wir berechnen, unter Berücksichtigung von $\overline{\zeta} = \zeta^2$,

$$\frac{2 - 3\zeta}{1 + 2\zeta} \;=\; \frac{(2 - 3\zeta)(1 + 2\zeta^2)}{(1 + 2\zeta)(1 + 2\zeta^2)} \;=\; \frac{2 + 4\zeta^2 - 3\zeta - 6\zeta^3}{1 + 2\zeta^2 + 2\zeta + 4\zeta^3} \;=\; \frac{-4 + 4(-1 - \zeta) - 3\zeta}{1 + 2(-1 - \zeta) + 2\zeta + 4} \;=\; \frac{-8 - 7\zeta}{3} \;=\; -\frac{8}{3} - \frac{7}{3}\zeta \; .$$

Runden der Koeffizienten gibt $q := -3 - 2\zeta$.
Dann wird $r := (2 - 3\zeta) - (1 + 2\zeta)(-3 - 2\zeta) = 2 - 3\zeta + 3 + 6\zeta + 2\zeta + 4\zeta^2 = 5 + 5\zeta + 4(-1 - \zeta) = 1 + \zeta$.
Alles in allem ist

$$(2 - 3\zeta) = (1 + 2\zeta)(-3 - 2\zeta) + (1 + \zeta) \; ,$$

wobei $|1 + \zeta|^2 = (1 + \zeta)(1 + \zeta^2) = (-\zeta^2)(-\zeta) = 1 < 3 = |1 + 2\zeta|^2$.

Aufgabe 11

(1) Wir betrachten das Ideal $(8, 20, 36) \subseteq \mathbb{Z}$. Man finde ein $z \in \mathbb{Z}$ mit $(z) = (8, 20, 36)$.

(2) Man finde zwei Elemente $f(X),\, g(X) \;\in\; \mathbb{Z}[X]$ mit
$(f(X)) \subset (f(X), g(X))$ und $(g(X)) \subset (f(X), g(X))$.

(3) Man zeige folgende Gleichheit von Idealen in $\mathbb{Q}[X, Y]$.

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

Lösung.
Zu (1). Wir behaupten, daß $(4) = (8, 20, 36)$ ist.
Zu $\supseteq$. Es ist $8a_1 + 20a_2 + 36a_3$ durch 4 teilbar für alle $a_1,\, a_2,\, a_3 \in \mathbb{Z}$.
Zu $\subseteq$. Es ist $4 = (-2)\cdot 8 + 1\cdot 20 + 0 \cdot 36 \in (8, 20, 36)$, und also auch $(4) \subseteq (8, 20, 36)$.
Alternativ kann man mit Bemerkung 66 auch $(8, 20, 36) = (\mathrm{ggT}(8, 20, 36)) = (4)$ anführen.
Zu (2). Wir behaupten, daß $(2) \subset (2, X)$ und $(X) \subset (2, X)$ ist.
Ersteres gilt, da $X \notin (2)$ liegt, denn das Polynom X in $\mathbb{Z}[X]$ nicht durch 2 teilbar ist.
Zweiteres gilt, da $2 \notin (X)$ liegt, denn 2 hat Grad 0, und die Polynome in (X) haben Grad $\geqslant 1$, als Vielfache von X.
Zu (3). Sei $I := (X^2 + Y,\ X + Y^2)$. Sei $J := (Y - XY^2,\ X - YX^2,\ X^2 + XY^2)$.
Zu $I \overset{!}{\subseteq} J$. Es ist $X^2 + Y = (Y - XY^2) + (X^2 + XY^2) \in J$.
Es ist zudem $X + Y^2 = (X - YX^2) + Y(Y - XY^2) + Y(X^2 + XY^2) \in J$.
Also ist auch $I \subseteq J$.
Zu $I \overset{!}{\supseteq} J$. Es ist $Y - XY^2 = (X^2 + Y) - X(X + Y^2) \in I$.
Es ist zudem $X - YX^2 = (X + Y^2) - Y(X^2 + Y) \in I$.
Es ist schließlich $X^2 + XY^2 = X(X + Y^2) \in I$.
Also ist auch $J \subseteq I$.

Aufgabe 12

(1) Sei R ein Integritätsbereich.
Man verifiziere: In $K := \mathrm{Quot}(R)$ gilt (Ring 2), also das Assoziativgesetz der Addition.

(2) Man finde $a,\, b,\, c \in \mathbb{F}_5$ mit
$$\frac{1}{X^3 + 2X^2} \;=\; \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X+2} \;\in\; \mathbb{F}_5(X)\ .$$
Sind die Elemente a, b und c in $\mathbb{F}_5$ dadurch eindeutig bestimmt?

Lösung.
Zu (1). Seien $u,\, u',\, u'' \in R$ und $v,\, v',\, v'' \in R^\times$ gegeben.
Zum einen wird
$$\left(\frac{u}{v} + \frac{u'}{v'}\right) + \frac{u''}{v''} \;=\; \frac{uv' + u'v}{vv'} + \frac{u''}{v''} \;=\; \frac{(uv' + u'v)v'' + u''(vv')}{(vv')v''} \;=\; fracuv'v'' + u'vv'' + u''vv'vv'v''\ .$$
Zum anderen wird
$$\frac{u}{v} + \left(\frac{u'}{v'} + \frac{u''}{v''}\right) \;=\; \frac{u}{v} + \frac{u'v'' + u''v'}{v'v''} \;=\; \frac{u(v'v'') + (u'v'' + u''v')v}{v(v'v'')} \;=\; fracuv'v'' + u'vv'' + u''vv'vv'v''\ .$$
Das ist dasselbe.
Zu (2). Wir multiplizieren mit $X^3 + 2X^2 = X^2(X+2)$ auf beiden Seiten und haben dann folgende Gleichung zu erfüllen.
$$1 \;=\; a(X^2 + 2X) + b(X+2) + cX^2 \;=\; (a+c)X^2 + (2a+b)X + 2b\ .$$
Koffizientenvergleich gibt das folgende lineare Gleichungssystem über $\mathbb{F}_5$.
$$\left(\begin{array}{ccc|c} 1 & 0 & 1 & 0 \\ 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 1 \end{array}\right)$$
Dies hat eine eindeutige Lösung, nämlich $\left(\begin{smallmatrix} a \\ b \\ c \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 \\ -2 \\ -1 \end{smallmatrix}\right)$, d.h. $a = 1$, $b = -2$, $c = -1$.
Es ist also
$$\frac{1}{X^3 + 2X^2} \;=\; \frac{1}{X} - \frac{2}{X^2} - \frac{c}{X+2} \;\in\; \mathbb{F}_5(X)\ .$$