C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 2

Aufgabe 5 Sei R ein kommutativer Ring mit $\mathrm{char}(R) =: p$ prim.
Wir betrachten die Frobenius-Abbildung $F : R \to R : x \mapsto x^p$.
Man zeige oder widerlege.

(1) Es ist F ein Ringmorphismus.

(2) Es ist F injektiv.

(3) Falls R ein Körper ist, dann ist F injektiv.

(4) Falls R ein Körper ist, dann ist F bijektiv.

Lösung zu Aufgabe 5:

(1) Richtig. Beweis:

Zunächst ist $F(1) = 1^p = 1$. Weiterhin gilt für alle $x, y \in R$ $F(xy) = (xy)^p = x^p y^p = F(x)F(y)$, wobei die Anwendung des Potenzgesetzes aufgrund der Kommutativität von R erlaubt ist.

Interessanter ist die Additivität.

Sei dafür zunächst $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ der Binomialkoeffient. Ist $k < p$, so teilt p keine der Zahlen $1, 2 \ldots, k$, somit kann p auch kein Teiler von $1 \cdot 2 \cdot \ldots \cdot k = k!$ sein. Es ist andererseits klar, dass $p | p!$. Ist $0 < k < p$, so ist auch $p - k < p$, also gilt nach der obigen Feststellung, dass $p \nmid k!, (p-k)!$. Wir haben aber $p | p! = k!(p-k)!\binom{p}{k}$. Es muss p einen der letzteren drei Faktoren teilen; hierfür kommt aber nur $\binom{p}{k}$ in Frage. Damit gilt

$$p \mid \binom{p}{k} \quad (0 < k < p) \tag{1}$$

Unter Verwendung des binomischen Lehrsatzes (welcher in jedem kommutativen Ring gilt), berechnen wir nun für beliebige $x, y \in R$:

$$\begin{aligned} F(x+y) &= (x+y)^p \\ &= \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \\ &= \binom{p}{0} x^0 y^p + \sum_{k=0}^{p-1} \underbrace{\binom{p}{k} x^k y^{p-k}}_{=0(\text{ wegen (1)})} + \binom{p}{p} x^p y^0 \\ &= x^p + y^p = F(x) + F(y). \end{aligned}$$

(2) Falsch. Sei $R = \mathbb{F}_p[X]/(X^2)$, dann ist $\mathrm{char}(R) = p$.

Da $X \notin (X^2)$, ist $X + (X^2) \neq 0 + (X^2)$, allerdings ist $F(X + (X^2)) = (X + (X^2))^p = X^p + (X^2) = 0 + (X^2) = F(0 + (X^2))$. Folglich ist F nicht injektiv.

Anmerkung: Das Vorhandensein nilpotenter Elemente ist in der Grund dafür, dass F nicht injektiv ist: es gibt ein $a \neq 0$ mit $a^p = 0$, also mit $a \in \mathrm{Kern}(F)$. Nilpotente Elemente sind häufig Grund für eigenartige Phänomene.

(3) Richtig. Ist R ein Körper, so ist $F : R \to R$ ein Ringhomomorphismus. Es hat R nur die Ideale (0) und $R = (1)$, da jedes Ideal ungleich (0) ein invertierbares Element enthält und damit auch 1. Wegen $F(1) = 1$ ist $1 \notin \text{Kern}(F)$. Da $\text{Kern}(F)$ jedoch ein Ideal ist (Lemma 27.(2)) , muss $\text{Kern}(F) = (0)$ sein, sprich: F ist nach Lemma 27.(2) injektiv.

(4) Falsch. Der Körper $R = \mathbb{F}_p(X)$ ist hier ein Gegenbeispiel. Es ist R der Quotientenkörper des Rings $S = \mathbb{F}_p[X]$, welcher nach dem Satz von Gauß (Satz 65) faktoriell ist Da X irreduzibel in S, also auch prim ist, können wir folgendermaßen mit der Bewertung zum Primelement X argumentieren: gäbe es ein $q \in R$ mit $f(q) = q^p = X$, so wäre auch

$$1 = v_X(X) = v_X(q^p) = p \cdot v_X(q),$$

ein *Widerspruch*, schließlich ist v_X eine ganzzahlige Funktion! Somit ist F in diesem Fall nicht surjektiv und erst recht nicht bijektiv.

Man kann alternativ auch rechnerisch argumentieren, daß X nicht im Bild von F liegt. Denn *wäre* $X = \left(\frac{a(X)}{b(X)}\right)^p$ mit $a(X), b(X) \in \mathbb{F}_p[X]^\times$, dann wäre $X \cdot b(X)^p = a(X)^p$. Der Grad des Polynoms links ist $\equiv_p 1$, der Grad des Polynoms rechts ist $\equiv_p 0$. *Widerspruch.*

Aufgabe 6 Wir betrachten den kommutativen Ring $\mathbb{Z}$. Seien $a, b \in \mathbb{Z}^\times$.
Zu zeigen ist folgendes.

(1) Es ist $(a, b) = (\text{ggT}(a, b))$.

(2) Es ist $(a) \cap (b) = (\text{kgV}(a, b))$.

Lösung zu Aufgabe 6:

(1) Schreibe $g := \text{ggT}(a, b)$.

Wir haben $(a, b) \stackrel{!}{=} (g)$ zu zeigen.

$\subseteq$: Da a und b Vielfache von g sind, ist $a \in (g)$ und $b \in (g)$. Also ist auch $(a, b) \subseteq (g)$.

$\supseteq$: Schreibe $g = sa + tb$, was nach dem Euklidschen Algorithmus möglich ist. Es ist also $g \in (a, b)$ und somit auch $(g) \subseteq (a, b)$.

> Erste alternative Lösung zu $\supseteq$, ohne Euklidschen Algorithmus:
> Es ist $\mathbb{Z}$ ein Hauptidealbereich. Also können wir $(a, b) = (c)$ schreiben für ein $c \in \mathbb{Z}$, o.E. mit $c > 0$. Es ist also $c = xa + yb$ für gewisse $x, y \in \mathbb{Z}$.
> Es teilt c sowohl a als auch b.
> Sei umgekehrt d ein gemeinsamer Teiler von a und von b. Dann teilt d auch $xa + yb = c$.
> Somit ist c der größte gemeinsame Teiler von a und von b.
>
> Zweite alternative Lösung zu $\supseteq$, ohne Euklidschen Algorithmus:
> Sei $(a, b) = (c)$ mit $c > 0$. Es gilt für alle $d \in \mathbb{Z}$:
>
> $$d|c \Leftrightarrow (c) \subseteq (d) \Leftrightarrow (a, b) \subseteq (d) \Leftrightarrow (a \in (d)) \wedge (b \in (d)) \Leftrightarrow ((a) \subseteq (d)) \wedge (b \subseteq (d))$$
> $$\Leftrightarrow (d|a) \wedge (d|b) \Leftrightarrow d|\text{ggT}(a, b).$$
>
> Wegen $c|c$ folgt damit $c|\text{ggT}(a, b)$. Andererseits folgt aus $\text{ggT}(a, b)|\text{ggT}(a, b)$, dass $\text{ggT}(a, b)|c$. Da $\text{ggT}(a, b)$ und c beide positiv sind, gilt $\text{ggT}(a, b) = c$.

(2) Sei $(c) := (a) \cap (b)$, wobei $c \geq 0$. Dann gilt für alle $d \in \mathbb{Z}$:

$$c|d \Leftrightarrow (d) \subseteq (c) \Leftrightarrow ((d) \subseteq (a)) \wedge ((d) \subseteq (b)) \Leftrightarrow (a|d) \wedge (b|d) \Leftrightarrow \mathrm{kgV}(a,b)|d.$$

Wegen $c|c$ folgt damit $c|\mathrm{kgV}(a,b)$. Andererseits folgt aus $\mathrm{kgV}(a,b)|\mathrm{kgV}(a,b)$, dass $\mathrm{kgV}(a,b)|c$. Da $\mathrm{kgV}(a,b)$ und c beide $\geqslant 0$ sind, gilt $\mathrm{kgV}(a,b) = c$.

Aufgabe 7 Sei $\zeta_3 := \exp(2\pi\mathrm{i}/3) = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3} \in \mathbb{C}$.

(1) Man bestätige $\zeta_3^2 + \zeta_3 + 1 = 0$.

(2) Wir betrachten den Teilring $\mathbb{Z}[\zeta_3] := \{\, a + b\zeta_3 \,:\, a,\, b \,\in\, \mathbb{Z} \,\} \,\subseteq\, \mathbb{C}$.
Sei $d : \mathbb{Z}[\zeta_3]^\times \to \mathbb{Z}_{\geqslant 0} : z = a + b\zeta_3 \mapsto |z|^2 = a^2 - ab + b^2$.
Man zeige, daß d eine Gradfunktion auf $\mathbb{Z}[\zeta_3]$ ist, mithin $\mathbb{Z}[\zeta_3]$ ein euklidischer Ring.

(3) Ist 3 prim in $\mathbb{Z}[\zeta_3]$?

Lösung zu Aufgabe 7:

(1) Es ist $\zeta_3^3 = \exp(2\pi\mathrm{i}/3)^3 = \exp(2\pi\mathrm{i}) = 1$, d.h. ζ_3 ist eine Nullstelle des Polynoms $f(x) = x^3 - 1 \in \mathbb{C}[x]$.
Wegen $f(x) = x^3 - 1 = (x-1)(x^2 + x + 1)$ ist ζ_3 entweder eine Nullstelle von $x - 1$ oder von $x^2 + x + 1$. Da $\zeta_3 \neq 1$ ist, kann ζ_3 keine Nullstelle von $x - 1$ sein, folglich ist ζ_3 eine Nullstelle von $x^2 + x + 1$, was die Gleichung $\zeta_3^2 + \zeta_3 + 1 = 0$ nach sich zieht.

(2) **Vorbemerkung.** *Für alle $z \in \mathbb{C}$ gibt es $a, b \in \mathbb{Z}$ so, dass $|z - (a + b\zeta_3)|^2 < 1$.*
Beweis: 1 und ζ_3 sind linear unabhängig über $\mathbb{R}$. Da $\mathbb{C}$ ein 2-dimensionaler Vektorraum über $\mathbb{R}$ ist, bilden $1, \zeta_3$ folglich eine Basis.
Sei nun $z \in \mathbb{C}$. Dann gibt es also $u, v \in \mathbb{R}$ so, dass $z = u + v\zeta_3$. Wir wählen nun $a, b \in \mathbb{Z}$ mit $|u - a| \leq \frac{1}{2}$ und $|v - b| \leq \frac{1}{2}$. Damit gilt

$$\begin{aligned} |z - (a + b\zeta_3)|^2 &= |(u + v\zeta_3) - (a + b\zeta_3)|^2 \\ &= |(u - a) + (v - b)\zeta_3|^2 \\ &= (u-a)^2 - (u-a)(v-b) + (v-b)^2 \\ &\leq \left(\frac{1}{2}\right)^2 + \frac{1}{2}\cdot\frac{1}{2} + \left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1. \end{aligned}$$

□

Nachfolgend schreiben wir $R := \mathbb{Z}[\zeta_3]$.
Seien nun $x \in R$, $y \in R^\times$.
Gibt es nun ein $q \in R$ so, dass $x = qy$ ist, so ist nichts zu tun.
Andernfalls finden wir nach obigem Lemma $a, b \in \mathbb{Z}$ so, dass $\left|\frac{x}{y} - (a + b\zeta_3)\right|^2 < 1$ ist. Beidseitiges Multiplizieren mit $|y|^2$ ergibt:

$$\begin{aligned} & |y|^2 \cdot \left|\frac{x}{y} - (a + b\zeta_3)\right|^2 < |y|^2 \\ \Leftrightarrow \quad & |x - y(a + b\zeta_3)|^2 < |y|^2 \\ \Leftrightarrow \quad & d(x - y(a + b\zeta_3)) < d(y). \end{aligned}$$

Setzen wir also $q = a + b\zeta_3$ und $r = x - y(a + b\zeta_3)$, so gilt einerseits $d(r) < d(y)$ und andererseits $x = y(a + b\zeta_3) + (x - y(a + b\zeta_3)) = q \cdot y + r$. Folglich ist R euklidisch.

(3) Ein Element von $\mathbb{Z}[\zeta_3]$ ist $\mathrm{i}\sqrt{3} = 1 + 2 \cdot \left(-\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}\right) = 1 + 2\zeta_3$, somit kann man 3 in $\mathbb{Z}[\zeta_3]$ als $3 = -\mathrm{i}\sqrt{3} \cdot \mathrm{i}\sqrt{3}$ zerlegen.

Jedoch sind $\pm\mathrm{i}\sqrt{3}$ keine Einheiten in $\mathbb{Z}[\zeta_3]$. Wäre z.B. $\mathrm{i}\sqrt{3}$ eine Einheit, so wäre auch $(\mathrm{i}\sqrt{3})^{-1} = \frac{-\mathrm{i}}{3}\sqrt{3} \in \mathbb{Z}[\zeta_3]$. Wir haben jedoch die (eindeutige!) reelle Linearkombination $\frac{-\mathrm{i}}{3}\sqrt{3} = -\frac{1}{3} - \frac{2}{3}\zeta_3 \notin \mathbb{Z}[\zeta_3]$. Gleichermaßen ist auch $-\mathrm{i}\sqrt{3}$ keine Einheit. 3 ist in $\mathbb{Z}[\zeta_3]$ nicht irreduzibel, also auch nicht prim (Bemerkung 52.(3)).

Alternativ kann man so argumentieren: Es ist $d(z_1 z_2) = d(z_1)d(z_2)$ (vgl. Aufgabe 4). Wäre aber $1 + 2\zeta_3$ eine Einheit, so gäbe es ein $r \in \mathbb{Z}[\zeta_3]$ mit $(1 + 2\zeta_3)r = 1$. Also wäre $d(1+2\zeta_3)d(r) = 1$ bzw. $(1^2 - 1 \cdot 2 + 2^2)d(r) = 3d(r) = 1$. Dann kann $d(r)$ aber keine ganze Zahl sein.

Aufgabe 8 Wir betrachten den faktoriellen Ring $\mathbb{Z}[\mathrm{i}]$.
Man finde eine Primfaktorzerlegung von x in $\mathbb{Z}[\mathrm{i}]$.

(1) $x = 5$.

(2) $x = 4$.

(3) $x = 3$.

(4) $x = 5\mathrm{i}$.

Lösung zu Aufgabe 8: Wir greifen auf die Gradfunktion $d : \mathbb{Z}[\mathrm{i}]^\times \to \mathbb{Z}_{\geq 0} : z \mapsto d(z) = |z|^2$ zurück (Beispiel 44.(3)).
Für $a, b \in \mathbb{Z}$ gilt $d(a + \mathrm{i}b) = |a + \mathrm{i}b|^2 = a^2 + b^2$.
Weiterhin ist d multiplikativ: für alle $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ gilt $d(z_1 z_2) = |z_1 z_2|^2 = (|z_1| \cdot |z_2|)^2 = |z_1|^2 \cdot |z_2|^2 = d(z_1) \cdot d(z_2)$.
Ist zudem $z \in \mathbb{Z}[i]$ so gilt $d(z) = 1 \Leftrightarrow z \in U(\mathbb{Z}[\mathrm{i}])$:
Ist nämlich $d(a + \mathrm{i}b) = a^2 + b^2 = 1$, so kommen für a, b nur die Optionen $a = \pm 1, b = 0$ und $a = 0, b = \pm 1$ in Frage, d.h. $a + \mathrm{i}b \in \{1, -1, \mathrm{i}, -\mathrm{i}\}$.
Ist andererseits $z \in U(\mathbb{Z}[\mathrm{i}])$, so haben wir

$$1 = d(1) = d(zz^{-1}) = d(z)d(z^{-1}).$$

Da aber beide Faktoren natürliche Zahlen sind, muss $d(z) = 1$ sein.

(1) Wir haben $5 = 2^2 + 1^2 = (2 + \mathrm{i})(2 - \mathrm{i})$. Weiterhin ist $2 + \mathrm{i}$ irreduzibel (also prim): gäbe es Nichteinheiten $z_1, z_2 \in \mathbb{Z}[\mathrm{i}]$ mit $z_1 z_2 = 2 + \mathrm{i}$, so wäre $d(z_1)d(z_2) = d(2 + \mathrm{i}) = 5$, also wäre entweder $d(z_1) = 1$ oder $d(z_2) = 1$, d.h. entweder z_1 oder z_2 eine Einheit.

Genauso begründet man, dass $2 - \mathrm{i}$ irreduzibel ist.

Eine komplexe Division (oder Durchtesten der Einheiten $\pm 1, \pm i$) zeigt, dass $2 + \mathrm{i}$ und $2 - \mathrm{i}$ nicht zueinander assoziiert sind.

Also ist

$$5 \;=\; (2 + \mathrm{i})(2 - \mathrm{i})$$

eine Primfaktorzerlegung.

(2) Wir zerlegen zunächst $x = 4 = 2 \cdot 2$. Weiterhin ist $2 = 1^2 + 1^2 = (1 + \mathrm{i})(1 - \mathrm{i})$. Wie bei (1) folgert man aus $d(1 \pm \mathrm{i}) = 2$, dass $1 \pm \mathrm{i}$ irreduzibel, also prim, sind. Allerdings ist $1 - \mathrm{i} = \mathrm{i} \cdot (1 - \mathrm{i})$, d.h. $1 + \mathrm{i}$ und $1 - \mathrm{i}$ sind zueinander assoziiert. Damit erhält man die Primfaktorzerlegung von 4 folgendermaßen:

$$4 = 2^2 = ((1 + \mathrm{i})(1 - \mathrm{i}))^2 = (1 + \mathrm{i})^2(1 - \mathrm{i})^2 = (1 + \mathrm{i})^2 \cdot \mathrm{i}^2(1 + \mathrm{i})^2 = (-1) \cdot (1 + \mathrm{i})^4.$$

(3) Für $x = 3$ ist $d(x) = 9$. Gibt es Nichteinheiten z_1, z_2 mit $z_1 z_2 = 3$, so ist $d(z_1)d(z_2) = 9$. D.h. es muss $d(z_1) = d(z_2) = 3$ sein. Aber es gibt kein $z =: a + b\mathrm{i} \in \mathbb{Z}[\mathrm{i}]$ mit $d(z) = 3$, da sonst $d(z) = a^2 + b^2 = 3$ wäre. Es gibt aber keine $a, b \in \mathbb{Z}$, die diese Gleichung erfüllen. Folglich ist 3 bereits irreduzibel, also auch prim. Die Primfaktorzerlegung ist also einfach

$$3 \;=\; 3\,.$$

(4) Wir verwenden unser Ergebnis aus Teil (1):

$$5\mathrm{i} \;=\; \mathrm{i} \cdot (2 + \mathrm{i}) \cdot (2 - \mathrm{i})$$

ist eine Primfaktorzerlegung, denn $2 + \mathrm{i}$, $2 - \mathrm{i}$ sind nichtassoziierte Primelemente und i ist eine Einheit.

Alternativ kann man auch i in einen der Faktoren hineinziehen, z.B. als
$5 = (-1 + 2\mathrm{i})(2 - \mathrm{i})$.