Universität Konstanz
Fachbereich Mathematik und Statistik
O. Schnürer, A. Kunert
SS 2013

Übungen zur Vorlesung Lineare Algebra II

Blatt 12

Hinweis zu Aufgabe 45

(a) Es genügt zu zeigen, dass $\mathbb{Z}[i]$ multiplikativ abgeschlossen ist. Seien dazu $a, b, c, d \in \mathbb{Z}$. Dann ist

$$(a + bi)(c + di) = ab - bd + i(bc + ad).$$

Wegen $ab - bd, bc + ad \in \mathbb{Z}$ folgt $(a + bi)(c + di) \in \mathbb{Z}[i]$.

(b) Offensichtlich sind $1, -1, i, -i \in \mathbb{Z}[i]$. Im folgenden wird gezeigt, dass dies alle Einheiten sind. Zunächst beobachten wir das Verhalten des üblichen Absolutbetrages auf $\mathbb{Z}[i]$. Für $a, b \in \mathbb{Z}$ gilt.

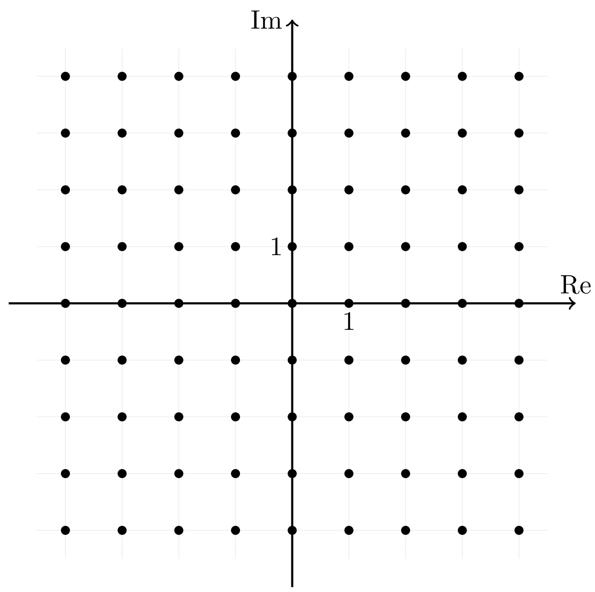
$$|a + bi|^2 = a^2 + b^2 \in \mathbb{Z}.$$

Angenommen $c, d \in \mathbb{Z}$ mit $c + di = (a + bi)^{-1}$. Dann gilt

$$1 = |1|^2 = |(a + bi)(c + di)|^2 = |a + bi|^2 |c + di|^2.$$

Daher muss $a^2 + b^2 \in \{-1, +1\}$ sein. Es folgt $a = \pm 1, b = 0$ oder $a = 0, b = \pm 1$.

(c) Im folgenden Bild sind die Punkte aus $\mathbb{Z}[i]$ innerhalb der Gaussschen Zahlenebene markiert.



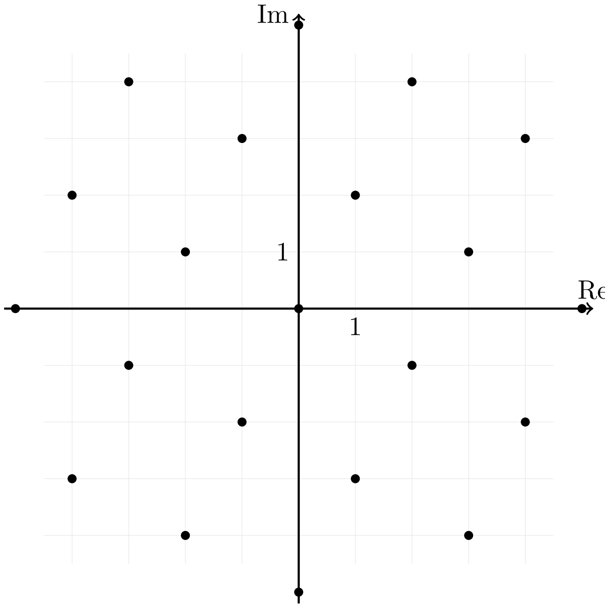
(d) Seien $z_1, z_2 \in \mathbb{R}$ mit $z = z_1 + iz_2$. Dann gibt es $x_1, x_2 \in \mathbb{Z}$ mit $|z_i - x_i| \leq \frac{1}{2}$. Es ist $x := x_1 + ix_2 \in \mathbb{Z}[i]$ und

$$|z - x| \leq \sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{1}{\sqrt{2}} < 1$$

(e) Seien $a, b \in \mathbb{Z}$. Dann gilt $(2-i)(a+bi) = 2a + b + i(2b - a)$. Identifiziert man die Gausssche Zahlenebene mit dem $\mathbb{R}^2$ gilt also

$$(2 - i) = \{(2a + b, 2b - a)^t \mid a, b \in \mathbb{Z}\}.$$

Also besteht das Hauptideal $(2-i)$ gerade aus allen $\mathbb{Z}$–Linearkombinationen der Vektoren $(2, -1)^t$ und $(1, 2)^t$. Wir erhalten also



(f) Nach Teil (d) existiert ein $q \in \mathbb{Z}[i]$ mit $\left|\frac{z}{a} - q\right| < |1| = 1$. Wir multiplizieren diese Ungleichung mit $|a|$ und erhalten das gewünschte Ergebnis.

(g) Wir wählen den Absolutbetrag als Gradfunktion. In der Lösung zu Teil (b) wurde gezeigt, dass $|x| \in \mathbb{N}$ für alle $x \in \mathbb{Z}[i]$ gilt. Sei nun $z \in \mathbb{Z}[i]$ und $a \in \mathbb{Z}[i] \setminus \{0\}$. Wir wählen q gemäß Teil (g) und $r := z - aq$. Dann gilt $z = aq + r$ und $|r| = |z - aq| < |a|$. Dies zeigt, dass $\mathbb{Z}[i]$ ein euklidischer Ring ist.

(h) Wir definieren

$$\begin{aligned} \psi \colon \mathbb{Z}[t]/(t^2 + 1) &\longrightarrow \mathbb{Z}[i] \\ \overline{p} &\longmapsto p(i). \end{aligned}$$

Zunächst zeigen wir, dass ψ wohldefiniert ist. Seien also $p, q \in \mathbb{Z}[t]$ mit $p - q \in (t^2 + 1)$. Dann ist $q = p + (t^2 + 1) \cdot f$ für ein $f \in \mathbb{Z}[t]$ und daher

$$\psi(\overline{q}) = \psi(\overline{p + f \cdot (t^2 + 1)}) = (p + f \cdot (t^2 + 1))(i) = p(i) + f(i)(i^2 + 1) = p(i) = \psi(\overline{p}),$$

woraus die Wohldefiniertheit von ψ folgt. Offensichtlich ist ψ ein Ringhomomorphismus. Weiter gilt $\text{im}\psi = \mathbb{Z}[i]$, da $1, i \in \text{im}\psi$. Bleibt zu zeigen, dass ψ injektiv ist. Nehmen wir dazu an, dass $\psi(\overline{p}) = 0$ ist. Wegen $\overline{t^2} = \overline{-1}$ können wir annehmen, dass $p = a + bt$ mit $a, b \in \mathbb{Z}$ ist. Dann ist $\psi(\overline{p}) = a + bi = 0$ daraus folgt $a = b = 0$ und somit $p = 0$.

Hinweis zu Aufgabe 46

Es gilt

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

Bleibt zu zeigen, dass die entsprechenden Elemente aus $R := \mathbb{Z}[\sqrt{-5}]$ paarweise nicht assoziiert und irreduzibel sind. Seien $a, b \in \mathbb{Z}$. Wir beobachten zunächst, dass

$$|a + bi|^2 = (a + ib)(a - ib) = a^2 + 5b^2 \in \mathbb{Z}.$$

Dies zeigt, dass $a + bi \in R^*$, genau dann, wenn $|a + bi| = 1$ gilt. Es ist also $R^* = \{-1, 1\}$. Es gilt

$$\begin{aligned} |2|^2 &= 4 \\ |3|^2 &= 9 \\ |1 + \sqrt{-5}|^2 &= 6 \\ |1 + \sqrt{-5}|^2 &= 6. \end{aligned}$$

Hätte eines dieser Elemente $x \in \{2, 3, 1 + \sqrt{-5}, 1 - \sqrt{5}\}$ einen echten Teiler d, so teilt $|d|^2$ auch $|x|^2$. Allerdings gibt es kein Element in R, mit Normquadrat 2 oder 3. Dies zeigt, dass x irreduzibel ist. Weiter folgt daraus, dass weder 2 noch 3 zu $(1 \pm \sqrt{-5})$ assoziiert ist. Dies zeigt, dass die Zerlegung in irreduzible Elemente in R nicht eindeutig ist. Also kann R kein Hauptidealring sein.

Hinweis zu Aufgabe 47

Wir berechnen den größten gemeinsamen Teiler mithilfe des euklidischen Algorithmus. Sei $f := x^6 + x^5 + 2x^4 + x^2 + x + 2$ und $g := x^3 + x + 1$. Zunächst gilt

$$f = (x^3 + x^2 + x + 1)g - (x^2 + x + 2).$$

Es folgt $\mathrm{ggT}(f, g) = \mathrm{ggT}(g, x^2 + x + 2)$. Weiter ist $x^2 + x + 2 \mid g$. Es folgt $\mathrm{ggT}(f, g) = x^2 + x + 2$.

Hinweis zu Aufgabe 48

Wir verwenden die Notation und den Algorithmus aus Bemerkung 4.3.15. Dabei gilt

$$\begin{aligned} b_1 &= 3 \\ b_2 &= 5 \\ b_3 &= 14. \end{aligned}$$

Es ist

$$\begin{aligned} c_1 &= 5 \cdot 14 = 70 \\ c_2 &= 3 \cdot 14 = 42 \\ c_3 &= 3 \cdot 5 = 15 \end{aligned}$$

Wegen $\mathrm{ggT}(b_i, c_i) = 1$, gibt es u_i, v_i mit $1 = u_i b_i + v_i c_i$. Diese berechnen sich zu.

$$\begin{aligned} 1 &= -3 \cdot 23 + 1 \cdot 70 \\ 1 &= 17 \cdot 5 - 2 \cdot 42 \\ 1 &= -14 + 15. \end{aligned}$$

Also ist $v_1 = 1$, $v_2 = -2$, $v_3 = 1$. Entsprechend der Bemerkung ist damit

$$2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot (-2) + 6 \cdot 15 \cdot 1 = -22$$

eine Lösung obiges Systems. Alle weiteren Lösungen davon unterscheiden sich um ein Vielfaches von 210 von dieser Lösung.