Aufgabe F14T3A3 (2+5+8 Punkte)

Wir betrachten die Teilmenge $R = \{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\}$ von $\mathbb{C}$.

(a) Zeigen Sie, dass R ein Unterring von $\mathbb{C}$ ist.

(b) Beweisen Sie, dass R ein euklidischer Ring ist bezüglich der Normfunktion $d(\alpha) = |\alpha|^2$.

(c) Geben Sie alle möglichen Faktorisierungen von $8 - i\sqrt{2}$ in irreduzible Elemente von R an (bis auf Reihenfolge).

Lösung:

zu (a) Das Einselement $1 \in \mathbb{C}$ ist in R enthalten, denn es gilt $1 = 1 + 0i\sqrt{2} \in R$. Seien nun $\alpha, \beta \in R$ vorgegeben. Zu zeigen ist $\alpha - \beta \in R$ und $\alpha\beta \in R$. Wegen $\alpha, \beta \in R$ gibt es $a, b, c, d \in \mathbb{Z}$ mit $\alpha = a + bi\sqrt{2}$ und $\beta = c + di\sqrt{2}$. Es folgt $\alpha - \beta = (a + bi\sqrt{2}) - (c + di\sqrt{2}) = (a - c) + (b - d)i\sqrt{2} \in R$ und

$$\alpha\beta \quad = \quad (a + bi\sqrt{2})(c + di\sqrt{2}) \quad = \quad (ac - 2bd) + (ad + bc)i\sqrt{2} \in R.$$

zu (b) Dieser Beweis ist aus der Vorlesung bekannt. Zunächst einmal ist R als Teilring des Körper $\mathbb{C}$ ein Integritätsbereich. Außerdem gilt für alle $a, b \in \mathbb{Z}$ jeweils

$$d(a + bi\sqrt{2}) \quad = \quad |a + bi\sqrt{2}|^2 \quad = \quad a^2 + 2b^2 \in \mathbb{N}_0$$

und $d(a + ib\sqrt{2}) = 0$ nur für $a = b = 0$, also ist durch d eine Funktion $R \setminus \{0\} \to \mathbb{N}$ definiert. Seien nun $\alpha, \beta \in R$ mit $\beta \neq 0$ vorgegeben. Zu zeigen ist, dass es Elemente $\gamma, \rho \in R$ mit $\alpha = \gamma\beta + \rho$ gibt, wobei $\rho = 0$ oder $d(\rho) < d(\beta)$ erfüllt ist. Seien $a, b, c, d \in \mathbb{Z}$ mit $\alpha = a + bi\sqrt{2}$ und $\beta = c + di\sqrt{2}$. Wegen $\beta \neq 0$ ist $(c, d) \neq (0, 0)$. Es gilt dann

$$\frac{\alpha}{\beta} \quad = \quad \frac{a + bi\sqrt{2}}{c + di\sqrt{2}} \quad = \quad \frac{(a + bi\sqrt{2})(c - di\sqrt{2}}{(c + di\sqrt{2})(c - di\sqrt{2})} \quad = \quad \frac{(ac + 2bd) + (bc - ad)i\sqrt{2}}{c^2 + 2d^2} \quad = \quad r + si\sqrt{2}$$

mit

$$r = \frac{ac + 2bd}{c^2 + 2d^2} \in \mathbb{Q} \qquad \text{und} \qquad s = \frac{bc - ad}{c^2 + 2d^2} \in \mathbb{Q}.$$

Seien nun $r_0, s_0 \in \mathbb{Z}$ so gewählt, dass $|r - r_0| \leq \frac{1}{2}$ und $|s - s_0| \leq \frac{1}{2}$ gilt. Setzen wir $\gamma = r_0 + s_0 i\sqrt{2}$, dann erhalten wir

$$\begin{aligned} \left|\frac{\alpha}{\beta} - \gamma\right|^2 \quad &= \quad |(r - r_0) + (s - s_0)i\sqrt{2}|^2 \quad = \quad (r - r_0)^2 + 2(s - s_0)^2 \\ &\leq \quad \tfrac{1}{4} + 2 \cdot \tfrac{1}{4} \quad = \quad \tfrac{3}{4} \quad < \quad 1. \end{aligned}$$

Sei nun $\rho = \alpha - \gamma\beta$. Setzen wir voraus, dass $\rho \neq 0$ ist, dann gilt zumindest

$$d(\rho) \quad = \quad |\rho|^2 \quad = \quad |\alpha - \gamma\beta|^2 \quad = \quad |\beta|^2 \cdot \left|\frac{\alpha}{\beta} - \gamma\right|^2 \quad < \quad |\beta|^2 \quad = \quad d(\beta).$$

Damit ist die oben angegebene Eigenschaft nachgewiesen.

zu (c) Als euklidischer Ring ist R insbesondere faktoriell. Dies bedeutet, dass jede Zerlegung von $8 - i\sqrt{2}$ in irreduzible Faktoren bis auf Einheiten und Reihenfolge eindeutig bestimmt ist. Aus der Vorlesung ist bekannt, dass die Normfunktion d multiplikativ ist, dass ein Element $\alpha \in R$ genau dann in der Einheitengruppe $R^\times$ liegt, wenn $d(\alpha) = 1$ ist, und dass α irreduzibel ist, wenn es sich bei $d(\alpha)$ um eine Primzahl handelt. Da die einzigen Lösungen von $a^2 + 2b^2 = 1$ die Paare $(\pm 1, 0)$ sind, ist $R^\times = \{\pm 1\}$.

Es gilt $d(8 - i\sqrt{2}) = 8^2 + 2 \cdot 1 = 66 = 2 \cdot 3 \cdot 11$. Dies deutet darauf hin, dass $8 - i\sqrt{2}$ aus Elementen der Norm 2, 3 und 11 zusammengesetzt ist. Durch Lösen der Gleichungen $x^2 + 2y^2 = 2, 3, 11$ sieht man, dass $\pm i\sqrt{2}$ die Elemente mit Norm 2, $\pm 1 \pm i\sqrt{2}$ die Elemente der Norm 3 und $\pm 3 \pm i\sqrt{2}$ die Elemente der Norm 11 in R sind. Durch probeweises Multiplizieren findet man die Zerlegung $8 - i\sqrt{2} = \alpha\beta\gamma$ mit $\alpha = -i\sqrt{2}$, $\beta = 1 + i\sqrt{2}$ und $\gamma = 3 + i\sqrt{2}$. Auf Grund der oben erwähnten Eindeutigkeit hat jede weitere Zerlegung die Form

$$8 - i\sqrt{2} \quad = \quad (\varepsilon_1\alpha)(\varepsilon_2\beta)(\varepsilon_3\gamma) \qquad \text{mit} \quad \varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{\pm 1\}.$$

Außerdem muss $\varepsilon_1\varepsilon_2\varepsilon_3 = 1$ gelten, damit auf der linken Seite der Gleichung das richtige Vorzeichen steht. Damit gibt es genau vier Zerlegungen von $8 - i\sqrt{2}$ in irreduzible Elemente, nämlich

$$\begin{aligned} 8 - i\sqrt{2} &= (-i\sqrt{2})(1 + i\sqrt{2})(3 + i\sqrt{2}) \\ 8 - i\sqrt{2} &= (i\sqrt{2})(-1 - i\sqrt{2})(3 + i\sqrt{2}) \\ 8 - i\sqrt{2} &= (i\sqrt{2})(1 + i\sqrt{2})(-3 - i\sqrt{2}) \\ 8 - i\sqrt{2} &= (-i\sqrt{2})(-1 - i\sqrt{2})(-3 - i\sqrt{2}). \end{aligned}$$