Blatt 6, Aufgabe 4

Sei $\mathbb{Z}[\mathrm{i}] := \{f(\mathrm{i}) \mid f \in \mathbb{Z}[X]\} \subset \mathbb{C}$, wobei $\mathrm{i} \in \mathbb{C}$ die imaginäre Einheit bezeichne.

Behauptung (a)**.** $\mathbb{Z}[\mathrm{i}] = \{u + \mathrm{i}v \mid u, v \in \mathbb{Z}\}$.

Beweis. Für die Richtung „$\supset$" seien $u, v \in \mathbb{Z}$ beliebig gegeben. Für $f := u + vX \in \mathbb{Z}[X]$ gilt dann $u + \mathrm{i}v = f(\mathrm{i})$, also liegt $u + \mathrm{i}v$ in der Tat in $\mathbb{Z}[\mathrm{i}]$.

Für die Richtung „$\subset$" sei $f \in \mathbb{Z}[X]$ beliebig gegeben. Die komplexe Zahl $f(\mathrm{i})$ ist dann also eine Linearkombination der Zahlen $\mathrm{i}^0, \mathrm{i}^1, \mathrm{i}^2, \mathrm{i}^3, \ldots$ mit ganzzahligen Koeffizienten. Jede dieser Zahlen liegt in der rechten Menge:

$$\begin{aligned}
\mathrm{i}^0 = \mathrm{i}^4 = \mathrm{i}^8 &= \mathrm{i}^{12} = \cdots = 1 + \mathrm{i} \cdot 0 \\
\mathrm{i}^1 = \mathrm{i}^5 = \mathrm{i}^9 &= \mathrm{i}^{13} = \cdots = 0 + \mathrm{i} \cdot 1 \\
\mathrm{i}^2 = \mathrm{i}^6 = \mathrm{i}^{10} &= \mathrm{i}^{14} = \cdots = -1 + \mathrm{i} \cdot 0 \\
\mathrm{i}^3 = \mathrm{i}^7 = \mathrm{i}^{11} &= \mathrm{i}^{15} = \cdots = 0 + \mathrm{i} \cdot (-1)
\end{aligned}$$

Damit liegt auch $f(\mathrm{i})$ in der rechten Menge. □

Sei die Funktion

$$\varphi\colon \quad \mathbb{Z}[\mathrm{i}] \setminus \{0\} \longrightarrow \mathbb{N}_0, \qquad z \longmapsto |z|^2,$$

definiert, wobei die Betragsstriche den komplexen Betrag bezeichnen (also $\varphi(u + \mathrm{i}v) = (\sqrt{u^2 + v^2})^2 = u^2 + v^2$ für $u, v \in \mathbb{Z}$).

Behauptung (b)**.** *Der Ring* $\mathbb{Z}[\mathrm{i}]$ *ist vermöge* φ *ein euklidischer Ring.*

Beweis. Dazu müssen wir die Teilaussagen (e1) und (e2) der Aufgabenstellung zeigen:

1. Seien $a, b \in \mathbb{Z}[\mathrm{i}]$ mit $ab \neq 0$. Dann ist insbesondere b nicht null und es gilt $\varphi(b) = |b|^2 \geq 1$. Somit folgt $\varphi(ab) = |ab|^2 = |a|^2|b|^2 \geq |a|^2 = \varphi(a)$.
2. Seien $a, b \in \mathbb{Z}[\mathrm{i}]$ mit $b \neq 0$. Dann ist der Quotient $x := a/b$ eine gewisse komplexe Zahl. Sei u der Real- und v der Imaginärteil von x, d. h. gelte $x = u + \mathrm{i}v$ mit $u, v \in \mathbb{R}$.

   Wir wählen nun ganzzahlige Näherungen $\tilde{u}, \tilde{v} \in \mathbb{Z}$ von u bzw. v, also ganze Zahlen mit $|u - \tilde{u}|, |v - \tilde{v}| \leq \frac{1}{2}$, und setzen $q := \tilde{u} + \mathrm{i}\tilde{v} \in \mathbb{Z}[\mathrm{i}]$, $r := a - qb$.

   Dann ist entweder der Rest r null (das passiert genau dann, wenn u und v selbst schon ganzzahlig waren), oder er ist nicht null; dann gilt die Abschätzung

   $$\begin{aligned}
   \varphi(r) = |a - qb|^2 = |b(x - q)|^2 &= |b|^2 \cdot ((u - \tilde{u})^2 + (v - \tilde{v})^2) \\
   &\leq |b|^2 \cdot (\tfrac{1}{4} + \tfrac{1}{4}) = \tfrac{1}{2}\varphi(b) < \varphi(b).
   \end{aligned}$$

□