Blatt 2, Aufgabe 4
Wir betrachten die folgende Teilmenge $\mathbb{Z}[i] := \{x + iy \in \mathbb{C}; x, y \in \mathbb{Z}\}$ der komplexen Zahlen.

a) Man zeige: $\mathbb{Z}[i]$ wird mit Addition und Multiplikation komplexer Zahlen zu einem Integritätsbereich. Er heißt der **Ring der Gaußschen Zahlen**.

b) Für $z = x + iy \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ sei $N(z) := z \cdot \overline{z} = x^2 + y^2$, wobei $\overline{z} := x - iy$ die komplexe Konjugation bezeichne. Man zeige: Für $0 \neq z \in \mathbb{C}$ gilt $z^{-1} = \frac{1}{N(z)} \cdot \overline{z}$.

c) Aus Teil b) folgere man: Die Einheitengruppe von $\mathbb{Z}[i]$ ist gegeben als

$$\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i]; N(z) = 1\} = \{\pm 1, \pm i\}.$$

Ist $\mathbb{Z}[i]$ ein Körper?

Lösung

a) Zunächst zeigen wir, dass die Abbildungen

$$+ : \mathbb{Z}[i] \times \mathbb{Z}[i] \to \mathbb{Z}[i]$$

und

$$\cdot : \mathbb{Z}[i] \times \mathbb{Z}[i] \to \mathbb{Z}[i]$$

wohldefiniert sind. Seien $a + bi$, $c + di \in \mathbb{Z}[i]$. Dann gilt $a + bi + c + di = (a+c) + (b+d)i \in \mathbb{Z}[i]$, da $a+c \in \mathbb{Z}$ und $b+d \in \mathbb{Z}$. Ebenso gilt $(a+bi) \cdot (c+di) = (ac - bd) + (ad + bc)i \in \mathbb{Z}[i]$, da $(ac - bd)$, $ad + bc \in \mathbb{Z}$.

Mithilfe der Tatsache, dass $\mathbb{C}$ ein Ring ist, rechnet man leicht nach, dass $(\mathbb{Z}[i], +, \cdot)$ selbst ein Ring ist. Dabei nutzt man im Wesentlichen aus, dass die Rechenregeln (Assoziativgesetze, Distributivgesetze und Kommutativität) bereits in $\mathbb{C}$ gelten und somit auch in der Teilmenge $\mathbb{Z}[i]$. Die Existenz neutraler Elemente folgt daraus, dass die neutralen Elemente der Addition und Multiplikation im Ring $\mathbb{C}$, also 0 und 1, bereits in $\mathbb{Z}[i]$ liegen. Außerdem sieht man leicht, dass additive Inverse von Elementen aus $\mathbb{Z}[i]$ wieder in $\mathbb{Z}[i]$ liegen.

Da $\mathbb{C}$ ein Integritätsbereich ist und $\mathbb{Z}[i] \subseteq \mathbb{C}$ gilt, so ist der Ring $\mathbb{Z}[i]$ ebenso ein Integritätsbereich.

b) Es gilt $z \cdot \overline{z} = N(z)$. Für $0 \neq z \in \mathbb{C}$ folgt also $z^{-1} = \frac{1}{N(z)} \cdot \overline{z}$.

c) i) Wir zeigen zunächst, dass $\mathbb{Z}^* = \{z \in \mathbb{Z}[i] \mid N(z) = 1\}$ gilt.
" $\subseteq$ " : Sei $0 \neq z = x + iy \in \mathbb{Z}[i]$ mit $z^{-1} \in \mathbb{Z}[i]$. Nach Teil b) gilt

$$z^{-1} = \frac{1}{N(z)} \cdot \overline{z} = \frac{x}{x^2 + y^2} - i\frac{y}{x^2 + y^2}.$$

Da $z^{-1} \in \mathbb{Z}[i]$, so gilt $\frac{x}{x^2+y^2} \in \mathbb{Z}$ und $\frac{y}{x^2+y^2} \in \mathbb{Z}$. Da $|x| \leq x^2 \leq x^2 + y^2$, so ist $\frac{x}{x^2+y^2} \in \mathbb{Z}$ genau dann, wenn $x = 0$ oder $x^2 + y^2 = 1$. Ebenso sieht man ein, dass $\frac{y}{x^2+y^2} \in \mathbb{Z}$ genau dann, wenn $y = 0$ oder $x^2 + y^2 = 1$. Da $0 \neq z$ ist, so muss also $N(z) = x^2 + y^2 = 1$ gelten.

Bemerkung: Wenn wir benutzen, dass die Normabbildung multiplikativ ist (siehe Aufgabe 4 von Blatt 3), so können wir einen einfacheren Beweis angeben: Sei $0 \neq z =\in \mathbb{Z}[i]$ mit $z^{-1} \in \mathbb{Z}[i]$. Dann gilt $1 = N(1) = N(z \cdot z^{-1}) = N(z)N(z^{-1})$. Also ist $N(z) \in \mathbb{Z}^* = \{\pm 1\}$. Somit gilt $N(z) = 1$.

" $\supseteq$ " : Sei $z \in \mathbb{Z}[i]$ mit $N(z) = 1$. Nach Teil b) gilt $z^{-1} = \overline{z} \in \mathbb{Z}[i]$.

ii) Wir zeigen nun $\{z \in \mathbb{Z}[i] \mid N(z) = 1\} = \{\pm 1, \pm i\}$.
" $\supseteq$ " : Es gilt $N(\pm 1) = N(\pm i) = 1$.

" $\subseteq$ " : Sei $z = x + iy \in \mathbb{Z}[i]$ mit $N(z) = x^2 + y^2 = 1$. Da $x, y \in \mathbb{Z}$, so muss $|x| \leq 1$ und $|y| \leq 1$ gelten. Man sieht nun leicht ein, dass

- $x = 0$, $y = 1$
- $x = 0$, $y = -1$
- $x = 1$, $y = 0$
- $x = -1$, $y = 0$

die einzigen ganzzahligen Lösungen der Gleichung $x^2 + y^2 = 1$ sind.

iii) Da $\mathbb{Z}[i]^* = \{\pm 1, \pm i\} \subsetneq \mathbb{Z}[i] \setminus \{0\}$, so ist $\mathbb{Z}[i]$ kein Körper.

Blatt 3, Aufgabe 4
Sei $\mathbb{Z}[i]$ der Ring der Gaußschen Zahlen und $N : \mathbb{Z}[i] \to \mathbb{N}_0$, $z \mapsto z \cdot \overline{z}$ die Normabbildung.

a) Zeigen Sie, dass für $z, z' \in \mathbb{Z}[i]$ gilt $N(zz') = N(z) \cdot N(z')$. Wir sagen, dass die Normabbildung N **multiplikativ** ist. Folgern Sie daraus, dass $u \in \mathbb{Z}[i]$ irreduzibel ist, wenn $N(u) \in \mathbb{Z}$ irreduzibel ist.

b) Zeigen Sie, dass $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der Bewertungsfunktion $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}_0$ ist.

Lösung

a) i) Seien $z = a + ib$, $y' = c + id \in \mathbb{C}$. Es gilt

$$\overline{z} \cdot \overline{z'} = (a - ib) \cdot (c - id) = (ac - bd) - i(ad + bc)i = \overline{z \cdot z'}.$$

Damit gilt nun

$$N(z) \cdot N(z') = z \cdot \overline{z} \cdot z' \cdot \overline{z'} = z \cdot z' \cdot \overline{z \cdot z'} = N(z \cdot z').$$

ii) Sei $u = z \cdot z'$ mit $z, z' \notin \mathbb{Z}[i]^*$. Dann gilt $N(u) = N(z) \cdot N(z')$. Da $z, z' \notin \mathbb{Z}[i]^*$, so gilt $N(z), N(z') \notin \mathbb{Z}^*$. Somit ist also $N(u)$ reduzibel.

b) Für $u \in \mathbb{Z}[i]$ und $0 \neq v \in \mathbb{Z}[i]$ definiere $s := \Re(uv^{-1}) \in \mathbb{Q}$ und $t := \Im(uv^{-1}) \in \mathbb{Q}$. Es gibt $a, b \in \mathbb{Z}$, so dass $|a - s| \leq \frac{1}{2}$ und $|b - t| \leq \frac{1}{2}$ gilt. Wir definieren $q := a + ib \in \mathbb{Z}[i]$ und $r := u - qv \in \mathbb{Z}[i]$. Dann gilt $u = qv + r$. Wir zeigen $N(r) < N(v)$. Zunächst gilt $N(r) = N(u - qv) = N(v) \cdot N(uv^{-1} - q)$ nach Teil a). Weiterhin gilt

$$N(uv^{-1} - q) = N((s+it) - (a+ib)) = (s-a)^2 + (t-b)^2 = |s-a|^2 + |t-b|^2 = (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2} < 1.$$

Somit also $N(r) = N(v) \cdot N(uv^{-1} - q) < N(v)$. die Monotonie der Bewertungsfunktion folgt direkt aus der Multiplikativität der Normfunktion. Dies zeigt, dass $\mathbb{Z}[i]$ ein euklidischer Ring bezüglich der Bewertungsfunktion $N : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}_0$ ist.