Übungsblatt 3

Aufgabe 1

1) Seien $u, v \in \mathbb{Z}[i]$

$q' = \frac{u}{v} = x + iy \in \mathbb{C}[i]$

Wähle $a, b \in \mathbb{Z}$ mit $|a - x| \leq \frac{1}{2}$ und $|b - y| \leq \frac{1}{2}$

und setze $q = a + bi \in \mathbb{Z}[i]$

Dann $N(q - q') = (a-x)^2 + (b-y)^2 \leq \frac{1}{4} + \frac{1}{4} \leq \frac{1}{2} < 1$

Wir haben : $u = vq + r$, wobei $r = u - vq =$

$= vq' - vq = v(q' - q)$

$N(r) = N(v)\, N(q' - q) < N(v)$. ∎

2) Eigenschaften : $z = a + bi \in \mathbb{C}$, $\bar{z} = a - bi$ $\rightsquigarrow$ $N(z) = z \cdot \bar{z} = a^2 + b^2 \in \mathbb{R}$

wenn $z \in \mathbb{Z}[i]$, dann $a^2 + b^2 \in \mathbb{Z}_{\geq 0}$

- $N(z_1 z_2) = z_1 z_2 \cdot \overline{z_1 z_2} = z_1 z_2\, \bar{z}_1 \bar{z}_2 = z_1 \bar{z}_1 \cdot z_2 \bar{z}_2 = N(z_1) N(z_2)$

$\cancel{z_1 z_2 \overline{z_1 z_2}}$

Wir zeigen : $z \in \mathbb{Z}[i]^* \iff N(z) = 1$

"$\Leftarrow$" $1 = N(z) = z \cdot \bar{z}$, $\bar{z} \in \mathbb{Z}[i] \Rightarrow z \in \mathbb{Z}[i]^*$

"$\Rightarrow$" Falls $\exists\, z^{-1} \in \mathbb{Z}[i]$, dann gilt $1 = z z^{-1}$ und

$1 = N(1) = N(z)\, N(z^{-1}) \Rightarrow \underset{\mathbb{Z}_{\geq 0}}{N(z)} = 1$.

$z = a + bi \in \mathbb{Z}[i]$

$N(z) = 1 \iff a^2 + b^2 = 1 \iff (a, b) \in \{(\pm 1, 0), (0, \pm 1)\}$

$\iff z \in \{\pm 1, \pm i\}$.

3) Sei π ein Primelement in $\mathbb{Z}[i]$.

$$\pi = a + bi\ ,\quad a, b \in \mathbb{Z} \qquad N(\pi) = \underbrace{a^2 + b^2}_{\in \mathbb{Z}} > 0$$

<u>Bmk</u>: $\overline{\pi} = a - bi$ ist auch ein Primelement in $\mathbb{Z}[i]$.

Angenommen, dass $N(\pi)$ keine Primzahl in $\mathbb{Z}$ ist.

$$N(\pi) = xy\ ,\quad x, y \in \mathbb{Z}\ ,\quad x > 1, y > 1$$

in $\underset{\substack{\uparrow \\ \text{faktoriell}}}{\mathbb{Z}[i]}$: $\quad \pi\overline{\pi} = N(\pi) = xy$

Nach der Eindeutigkeit der Primfaktorzerlegung in $\mathbb{Z}[i]$:

$$\pi\overline{\pi} = xy \implies \{\pi, \overline{\pi}\} \underset{\substack{\text{bis auf} \\ \text{Einheiten}}}{=} \{x, y\}$$

Es folgt: x und y sind prim in $\mathbb{Z}[i]$

$\Rightarrow$ irreduzibel in $\underset{\substack{\cup \\ \mathbb{Z}}}{\mathbb{Z}[i]}$ $\Rightarrow$ irreduzibel in $\mathbb{Z}$ $\Rightarrow$ x, y sind Primzahlen in $\mathbb{Z}$.

$$\{\pi, \overline{\pi}\} \overset{\substack{\text{bis auf...} \\ \downarrow}}{=} \{x, y\} \implies \pi = \text{Primzahl aus } \mathbb{Z} \text{ bis auf Einheiten.}$$

Aufgabe 2

1) p Primzahl aus $\mathbb{Z}$, $p \equiv 3 \mod 4$

Angenommen, p ist nicht prim in $\mathbb{Z}[i] \Rightarrow p$ ist reduzibel in $\mathbb{Z}[i]$

$\Rightarrow p = z_1 z_2$, $z_1, z_2 \in \mathbb{Z}[i]$ und $z_1, z_2 \notin \mathbb{Z}[i]^* \Leftrightarrow N(z_{1,2}) \neq 1$

$$p^2 = N(p) = \underbrace{N(z_1) N(z_2)}_{\substack{\text{liegen in } \mathbb{Z}, \\ > 1, \text{ da nicht für } z_{1,2} \notin \mathbb{Z}[i]^* \\ \text{Aufgabe 1.2}}} \Rightarrow N(z_1) = N(z_2) = p$$

Wir schreiben $z_1 = a + bi$, $a, b \in \mathbb{Z}$

Dann $a^2 + b^2 = p \Rightarrow a^2 + b^2 = 0$ in $\mathbb{Z}/p\mathbb{Z}$

$\Rightarrow a^2 = -b^2$ in $\mathbb{Z}/p\mathbb{Z} \Rightarrow \left(\frac{a}{b}\right)^2 = -1$ in $\mathbb{Z}/p\mathbb{Z}$

Aber -1 ist kein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$ nach der Aufgabe 1.5 Tblatt 3

Widerspruch.

2) Sei $p = 1 \mod 4$ prim oder $p = 2$. Nach Aufgabe 1.5 Tblatt 3 ist -1 ein Quadrat in $(\mathbb{Z}/p\mathbb{Z})^*$.

$\exists\, m \in \mathbb{Z}$ mit $m^2 + 1 = pl$ in $\mathbb{Z}$., $l \in \mathbb{Z}$

Dann gilt (*) $(m+i)(m-i) = pl$ in $\mathbb{Z}[i]$.

Wir annehmen, dass p prim in $\mathbb{Z}[i]$ ist.

Nach (*) $p \mid (m+i)(m-i) \Rightarrow p \mid (m+i)$ oder $p \mid (m-i)$

aber $m \pm i \neq p \cdot (a + bi)$ mit $a, b \in \mathbb{Z}$. Widerspruch.

Es folgt: p ist nicht prim in $\mathbb{Z}[i]$ $\Rightarrow p$ ist reduzibel in $\mathbb{Z}[i]$

$\Rightarrow p = z_1 z_2$ in $\mathbb{Z}[i]$ mit $N(z_1), N(z_2) \neq 1$

$\Rightarrow p^2 = N(p) = N(z_1) \cdot N(z_2) \Longrightarrow N(z_1) = N(z_2) = p$

Wenn $z_1 = a + ib \in \mathbb{Z}[i]$, dann $p = N(z_1) = a^2 + b^2$

3) Die Elemente wie in 1) und 2) ($a+ib$ mit $a^2+b^2=p \equiv 1 \bmod 4$ oder $p=2$) sind prim in $\mathbb{Z}[i]$.

Es gibt keine andere nach Aufgabe 1.3

<u>Aufgabe 3</u> : (1) Sei $a \in R \setminus \{0\}$. z.z.: a ist invertierbar

$$\begin{aligned} \varphi : (R,+) &\longrightarrow (R,+) \quad \text{Gruppenhom.} \\ x &\longmapsto a \cdot x \end{aligned}$$

$\operatorname{Ker} \varphi = \{0\}$, da R ein Integritätsbereich ist

$\Rightarrow \varphi$ ist injektiv $\underset{R \text{ endlich}}{\Longrightarrow}$ φ ist ~~bijektiv~~ surjektiv

$\Rightarrow \exists\, x \in R$ mit $\varphi(x) = 1 \rightsquigarrow x$ ist das Inverse von a in R.

(2) $\mathfrak{p}$ Primideal in A

$A/\mathfrak{p}$ Integritätsbereich $\underset{\text{nach } 1)}{\Longrightarrow}$ Körper $\Rightarrow \mathfrak{p}$ ist maximal

<u>Aufgabe 4</u> : $1+x = 1-(\overset{y}{\widetilde{-x}})$, $y^n = 0$

auch nilpotent.

$$1 = 1-y^n = (1-y)\underbrace{(1+y+\dots+y^{n-1})}_{\text{Inverse von } (1-y)}$$