Homework x

Kevin Le

Friday 13th June, 2025

Exercise 0.1. Verify that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or by using the fact that $N(a+bi = (a+bi)(a-bi)$. Conclude that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

Proof. Writing $\alpha = a + bi$ and $\beta = c + di$, we have

$$\begin{aligned} N(\alpha\beta) &= N((a+bi)(c+di)) \\ &= N((ac-bd)+(ab+cd)i) \\ &= (ac-bd)^2 + (ab+cd)^2 \\ &= a^2c^2 - 2abcd + b^2d^2 + a^2b^2 + 2abcd + c^2d^2 \\ &= a^2c^2 + b^2d^2 + a^2b^2 + c^2d^2 \\ &= (a^2+b^2)(c^2+d^2) \\ &= N(\alpha)N(\beta). \end{aligned}$$

If $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then for some β, $\alpha\beta = \gamma$. Hence, $N(\gamma) = N(\alpha\beta) = N(\alpha)N(\beta)$ which means $N(\alpha) \mid N(\gamma)$. $\square$

Exercise 0.2. Let $\alpha \in \mathbb{Z}[i]$. Show that α is a unit iff $N(\alpha) = 1$. Conclude that the only units are ± 1 and $\pm i$.

Proof. If is a unit, then for some $\alpha^{-1} \in \mathbb{Z}[i]$, we have $\alpha\alpha^{-1} = 1$. Hence $N(\alpha\alpha^{-1}) = 1$ and by exercise 1, this implies that $N(\alpha)N(\alpha^{-1}) = 1$. Since the range of N is $\mathbb{Z}$, we have $N(\alpha) = \pm 1$. Writing $\alpha = a^2 + b^2$, this means $a = \pm 1$ and $b = 0$ or $a = 0$ and $b = \pm 1$. $\square$

Exercise 0.3. Let $\alpha \in \mathbb{Z}[i]$. Show that if $N(\alpha)$ is a prime in $\mathbb{Z}$ then α is irreducible in $\mathbb{Z}[i]$. Show that the same conclusion holds if $N(\alpha) = p^2$, where p is a prime in $\mathbb{Z}$, $p \equiv 3 \pmod 4$.

Proof. Suppose $N(\alpha)$ is a prime in $\mathbb{Z}$ and α is not irreducible in $\mathbb{Z}[i]$. Then, we have $\alpha = \beta\gamma$ for $\beta, \gamma \in \mathbb{Z}[i]$ with $N(\beta) \neq 1$ and $N(\gamma) \neq 1$. By Exercise 1 again, this implies that $N(\beta)N(\gamma) = p$. Since p is prime this implies that $N(\beta) = p$ and $N(\gamma) = 1$ or $N(\beta) = 1$ and $N(\gamma) = p$. This is a contradiction. $\square$