Solutions to the book: *Jürgen Neukirch, Algebraic Number Theory*

Meng-Gen Tsai
plover@gmail.com

July 12, 2021

Contents

Chapter I: Algebraic Integers

I.1. The Gaussian Integers

Exercise I.1.1.

$\alpha \in \mathbb{Z}[i]$ is a unit if and only if $N(\alpha) = 1$.

Proof.

(1) *Show that for all $\alpha, \beta \in \mathbb{Z}[i]$, $N(\alpha\beta) = N(\alpha)N(\beta)$, either by direct computation or 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 $\mathbb{Z}$.*

(2) (Direct computation.) Write $\alpha = a + bi, \beta = c + di$ where $a, b, c, d \in \mathbb{Z}$. Thus,

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

Therefore, $N(\alpha\beta) = N(\alpha)N(\beta)$. (Note that we also get the identity $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$.)

(3) (Using the fact that $N(a+bi) = (a+bi)(a-bi)$, or $N(\alpha) = \alpha\overline{\alpha}$ for any $\alpha \in \mathbb{Z}[i]$.)

$$\begin{aligned} N(\alpha\beta) &= \alpha\beta\overline{\alpha\beta} \\ &= \alpha\beta\overline{\alpha}\,\overline{\beta} \\ &= \alpha\overline{\alpha}\beta\overline{\beta} \\ &= N(\alpha)N(\beta). \end{aligned}$$

(4) *Show that if $\alpha \mid \gamma$ in $\mathbb{Z}[i]$, then $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.* Write $\gamma = \alpha\beta$ for some $\beta \in \mathbb{Z}[i]$. So $N(\gamma) = N(\alpha)N(\beta) \in \mathbb{Z}$, or $N(\alpha) \mid N(\gamma)$ in $\mathbb{Z}$.

(5) ($\Longrightarrow$) Since α is a unit, there is $\beta \in \mathbb{Z}[i]$ such that $\alpha\beta = 1$. By (1), $N(\alpha\beta) = N(1)$, or $N(\alpha)N(\beta) = 1$. Since the image of N is nonnegative integers, $N(\alpha) = 1$.

(6) ($\Longleftarrow$) By (1), $N(\alpha) = \alpha\overline{\alpha}$, or $1 = \alpha\overline{\alpha}$ since $N(\alpha) = 1$. That is, $\overline{\alpha} \in \mathbb{Z}[i]$ is the inverse of $\alpha \in \mathbb{Z}[i]$. (Or we solve the equation $N(\alpha) = a^2 + b^2 = 1$, and show that all four solutions (± 1 and $\pm i$) are unit.)

(7) Conclusion: a unit $\alpha = a + bi$ of $\mathbb{Z}[i]$ is satisfying the equation $N(\alpha) = a^2 + b^2 = 1$ by (5)(6). That is, the only unit of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

□