Mathematical Reasoning

Chapter 7. Complex Numbers

7.2. The Gaussian Integers—Proofs of Theorems

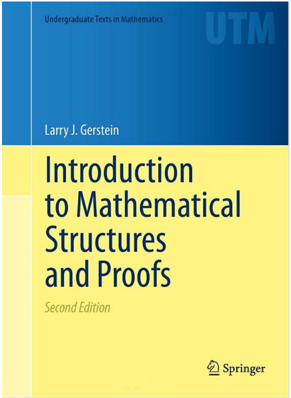

Table of contents

1 Theorem 7.14. Division Algorithm

Theorem 7.14

Theorem 7.14. Division Algorithm in $\mathbb{Z}[i]$.
Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta + r$, with $0 \leq N(r) < N(\beta)$.

Proof. The quotient α/β is of the form $u + vi$, with $u, v \in \mathbb{Q}$, since $\dfrac{\alpha}{\beta} = \dfrac{\alpha}{\beta}\dfrac{\overline{\beta}}{\overline{\beta}} = \dfrac{\alpha\overline{\beta}}{|\beta|^2}$ and the real and imaginary parts of α and $\overline{\beta}$ are integers. Thus $\alpha = \beta(u + vi)$. Sine u and v are rational, then there are integers x and y such that $|x - u| \leq 1/2$ and $|y - v| \leq 1/2$ (when u or v is $1/2$, then there are two choices, respectively, for x or y). So $x + yi$ is a Gaussian integer closest to α/β. Define $q = x + yi$ and $r = \alpha - \beta q$. So $\alpha = \beta q + r$, as needed. It remains to confirm that $N(r) < N(\beta)$. Now

$$r = \alpha - \beta q = \beta(u + vi) - \beta(x + yi) = \beta((u - x) + (v - y)i),$$

and, with $\gamma = (u - x) + (v - y)i$ for which $N(\gamma) = (u - x)^2 + (v - y)^2 \leq 1/2$, $N(r) = N(\beta)N(\gamma) = N(\beta)/2 < N(\beta)$, as claimed. □

Theorem 7.14

Theorem 7.14. Division Algorithm in $\mathbb{Z}[i]$.
Let $\alpha, \beta \in \mathbb{Z}[i]$, with $\beta \neq 0$. Then there exist $q, r \in \mathbb{Z}[i]$ such that $\alpha = \beta + r$, with $0 \leq N(r) < N(\beta)$.

Proof. The quotient α/β is of the form $u + vi$, with $u, v \in \mathbb{Q}$, since $\dfrac{\alpha}{\beta} = \dfrac{\alpha}{\beta}\dfrac{\overline{\beta}}{\overline{\beta}} = \dfrac{\alpha\overline{\beta}}{|\beta|^2}$ and the real and imaginary parts of α and $\overline{\beta}$ are integers. Thus $\alpha = \beta(u + vi)$. Sine u and v are rational, then there are integers x and y such that $|x - u| \leq 1/2$ and $|y - v| \leq 1/2$ (when u or v is $1/2$, then there are two choices, respectively, for x or y). So $x + yi$ is a Gaussian integer closest to α/β. Define $q = x + yi$ and $r = \alpha - \beta q$. So $\alpha = \beta q + r$, as needed. It remains to confirm that $N(r) < N(\beta)$. Now

$$r = \alpha - \beta q = \beta(u + vi) - \beta(x + yi) = \beta((u - x) + (v - y)i),$$

and, with $\gamma = (u - x) + (v - y)i$ for which $N(\gamma) = (u - x)^2 + (v - y)^2 \leq 1/2$, $N(r) = N(\beta)N(\gamma) = N(\beta)/2 < N(\beta)$, as claimed. □