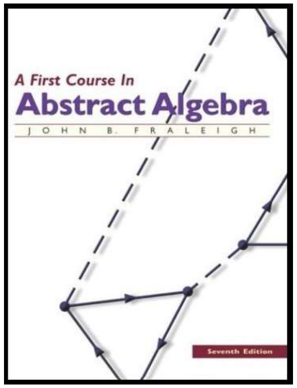
Introduction to Modern Algebra

Part IX. Factorization

IX.47. Gaussian Integers and Multiplicative Norms



Lemma 47.3

Lemma 47.3. $\mathbb{Z}[i]$ is an integral domain.

Proof. "Cleary" $\mathbb{Z}[i]$ is a commutative ring with unity 1. We now show that $\mathbb{Z}[i]$ has no divisors of 0. If $\alpha\beta = 0$ then by Lemma 47.2 Parts (2) and (3)

$$N(\alpha)N(\beta) = N(\alpha\beta) = N(0) = 0 \tag{1}$$

Since $N(\alpha)$ and $N(\beta)$ are nonnegative real numbers then either $N(\alpha) = 0$ or $N(\beta) = 0$. By Lemma 47.2 Part (2), this means that either $\alpha = 0$ or $\beta = 0$. So $\mathbb{Z}[i]$ is a commutative ring with unity and no divisors of 0; that is, $\mathbb{Z}[i]$ is an integral domain. □

Theorem 47.4

Theorem 47.4. The function v given by $v(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm in $\mathbb{Z}[i]$ and so $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. For all $\beta = b_1 + b_2 i \neq 0$ in $\mathbb{Z}[i]$ we have $N(b_1 + b_2 i) = b_1^2 + b_2^2 = 1$. Then for all $\alpha, \beta in \mathbb{Z}[i]$ where $\alpha \neq 0 \neq \beta$ we have

$$\begin{aligned} N(\alpha) &\leq N(\alpha)N(\beta) \text{ since } N(\beta) \geq 1 \\ &= N(\alpha\beta) \text{ by Lemma 47.2(3)} \end{aligned} \tag{2}$$

so Condition 2 for a Euclidean norm in Definition 46.1 holds.

Theorem 47.4 (continued 1)

Theorem 47.4. The function v given by $v(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm in $\mathbb{Z}[i]$ and so $\mathbb{Z}[i]$ is a Euclidean domain.

Proof (Continued). We now show that N satisfies Condition 1 (the division algorithm). Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\alpha = a_1 + a_2 i$ and $\beta = b_1 + b_2 i$ where $\beta \neq 0$. We need to find σ and ρ in $\mathbb{Z}[i]$ such that $\alpha = \beta\sigma + \rho$ where either $\rho = 0$ or $N(\rho) < N(\beta) = b_1^2 + b_2^2$. Let $\alpha/\beta = r + si$ where $r = (a_1 b_1 + a_2 b_2)/(b_1^2 + b_2^2)$ (see equation (7) on page 15 of the book), so $r, s \in \mathbb{Q}$. Let q_1 and q_2 be integers as close as possible to r and s, respectively (so q_1 is either $\lfloor r \rfloor$ or $\lceil r \rceil$ and q_2 is either $\lfloor s \rfloor$ or $\lceil s \rceil$). Let $\sigma = q_1 + q_2 i$ and $\rho = \alpha - \beta\sigma$. Then $\alpha = \beta\sigma + \rho$.

Theorem 47.4. (continued 2)

Theorem 47.4. The function v given by $v(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm in $\mathbb{Z}[i]$ and so $\mathbb{Z}[i]$ is a Euclidean domain.

Proof (Continued). If $\rho = 0$ we are done. Otherwise, by construction of σ we have $|r - q_1| \leq 1/2$ and $|s - q_2| \leq 1/2$, so $N(\alpha/\beta - \sigma) = N((r + si) - (q_1 + q_2 i)) = N((r - q_1) + (s - q_2)i) \leq \frac{1}{2}^2 + \frac{1}{2}^2 = \frac{1}{2}$. Thus

$$\begin{aligned} N(\rho) &= N(\alpha - \beta\sigma) = N(\beta(\alpha/\beta - \sigma)) \\ &= N(\beta)N(\alpha/\beta - \sigma) \text{ by Lemma 47.2(3)} \\ &\leq N(\beta) \cdot \frac{1}{2} \end{aligned} \tag{3}$$

So $N(\rho) < N(\beta)$ and Condition 2 follows. □

Theorem 47.7

Theorem 47.7. If D is an integral domain with a multiplicative norm N, then $N(1) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every α satisfying $|N(\alpha)| = 1$ is a unit in D, then an element $\pi \in D$ with $|N(\pi)| = p$ for a prime $p \in \mathbb{Z}$ is an irreducible of D.

Proof. Let D be an integral domain with a multiplicative norm N. Then $N(1) = N((1)(1)) = N(1)N(1)$ and so $N(1)$ is either 0 or 1. By Property 1 of the definition of the multiplicative norm, we have that $N(1) = 1$. If $u \in D$ is a unit then $1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1})$. Since $N(u)$ is an integer then $N(u) = \pm 1$ and $|N(u)| = 1$.

Theorem 47.7 (continued)

Theorem 47.7. If D is an integral domain with a multiplicative norm N, then $N(1) = 1$ and $|N(u)| = 1$ for every unit $u \in D$. If, furthermore, every α satisfying $|N(\alpha)| = 1$ is a unit in D, then an element $\pi \in D$ with $|N(\pi)| = p$ for a prime $p \in \mathbb{Z}$ is an irreducible of D.

Proof (continued). Now suppose that the units of D are exactly the elements of norm ± 1. Let $\pi \in D$ be such that $|N(\pi)| = p$ where $p \in \mathbb{Z}$ is prime. Then if $\pi = \alpha\beta$ we have $p = |N(\pi)| = |N(\alpha)N(\beta)|$ so either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$ since p is prime. By hypothesis then either α or β is a unit of D. So $\pi = \alpha\beta$ implies either α or β is a unit; that is, π is irreducible. □

Theorem 47.10. Fermat's $p = a^2 + b^2$ Theorem

Theorem 47.10. Fermat's $\mathbf{p = a^2 + b^2}$ Theorem. Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod{4}$.

Proof. First, suppose $p = a^2 + b^2$. Now a and b cannot both be even or both be odd since this would give p even (notice that we hypothesize an odd prime). If $a = 2r$ (even) and $b = 2s + 1$ (odd), then $a^2 + b^2 = 4r^2 + r(s^2 + s) + 1 \equiv 1 \pmod{4}$ and $p \equiv 1 \pmod{4}$.

Theorem 47.10. Fermat's $p = a^2 + b^2$ Theorem (continued 1)

Theorem 47.10. Fermat's $\mathbf{p = a^2 + b^2}$ Theorem. Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \pmod 4$.

Proof (continued). Second, assume $p \equiv 1 \pmod 4$. Now consider the multiplicative group of nonzero elements of $\mathbb{Z}_p$. This is a cyclic group and has order $p - 1$. Since 4 is a divisor of $p - 1$, then this cyclic group has an element n of multiplicative order 4 (the multiplicative group is isomorphic to U_{p-1} and $exp(2\pi i(p-1)/4)$ is of order 4. Then n^2 is of multiplicative order 2. So $n^2 = -1$ in $\mathbb{Z}_p$ (or $n^2 = p - 1$). So in $\mathbb{Z}$ we have $n^2 \equiv -1 \pmod p$ and $n^2 + 1 \in \mathbb{Z}$ is a multiple of p.

Theorem 47.10. Fermat's $p = a^2 + b^2$ Theorem (continued 2)

Theorem. 47.10. Fermat's $\mathbf{p = a^2 + b^2}$ Theorem Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \, (mod\, 4)$.

Proof (continued). Viewing p and $n^2 + 1$ in $\mathbb{Z}[i]$ we see that p divides $n^2 + 1 = (n+1)(n-i)$. ASSUME p is irreducible in $\mathbb{Z}[i]$. Then p would have to divide either $n + 1$ or $n - i$ by Lemma 45.13 (since $\mathbb{Z}$ is a PID. see papge 391 of the book). If p divides $n + i$, then $n + i \equiv p(a + bi)$ for some $a, b\mathbb{Z}$. But then we need $pb = 1$ (equating imaginary parts). An irreducible is, by definition, not a unit; since p is irreducible by assumption, then p is not a unit so $1 = pb$ is a contradiction. Similarly, if p divides $n - i$ then we need $-1 = pb$ or $1 \equiv p(-b)$, again a contradiction. These CONTRADICTIONS imply that the assumption that p is irreducible in $\mathbb{Z}[i]$ is false, and p is not irreducible.

Theorem 47.10. Fermat's $p = a^2 + b^2$ Theorem (continued 3)

Theorem 47.10. Fermat's $\mathbf{p = a^2 + b^2}$ Theorem. Let p be an odd prime in $\mathbb{Z}$. Then $p = a^2 + b^2$ for integers $a, b \in \mathbb{Z}$ if and only if $p \equiv 1 \, (mod\, 4)$.

Proof (continued). Since p is not irreducible in $\mathbb{Z}[i]$, then $p = (a + bi)(c + di)$ where neither $a + bi$ nor $c + di$ is a unit. Using the multiplicative norm on $\mathbb{Z}[i]$ we have $N(p) = N(a + bi)N(c + di)$ or $p^2 = (a^2 + b^2)(c^2 + d^2)$ where, by Theorem 47.7, neither $a^2 + b^2 = 1$ nor $c^2 + d^2 = 1$. But we hypothesized that p is a prime in $\mathbb{Z}$, so we must have that $p = a^2 + b^2$. [We also have $p = c^2 + d^2$. Since $p = (a + bi)(c + di) = a^2 + b^2 = (a + bi)(a - bi)$, it must be that $a - bi = c + di$ and $c = a$ and $d = b$. Of course, if $p = a^2 + b^2$ then $p = (\pm a)^2 + (\pm b)^2$.] □