Section IX.47. Gaussian Integers and Multiplicative Norms

Note. In this section, we give another example of a Euclidean domain (other than $\mathbb{Z}$ and $F[x]$), namely the Gaussian integers. We define a multiplicative norm on in integral domain and give an application of it to number theory and prime numbers.

Definition 47.1. A *Gaussian integer* is a complex number $a + bi$ where $a, b \in \mathbb{Z}$. For Gaussian integer $\alpha = a + bi$, define the *norm* of α as $N(\alpha) = a^2 + b^2$.

Note. To an analyst, the above definition of "norm" is rather weird! Traditionally, the norm on $\mathbb{C}$ is $\|a + bi\| = \sqrt{a^2 + b^2}$ and we then show that this norm satisfies certain properties such as the triangle inequality. however, here our agenda is very different and we will use N for the Euclidean norm of an integral domain (namely, the integral domain is the Gaussian integers).

Note. We denote the Gaussian integers as $\mathbb{Z}[i]$ (not to be confused with an extension field [hey, $\mathbb{Z}$ is not a field!], group action on a set, or any of the other wonderful things we've represented with square brackets). We will show that $\mathbb{Z}[i]$ is a Euclidean domain. Notice that the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Lemma 47.2. In $\mathbb{Z}[i]$, the following properties of the norm function N hold for all $\alpha, \beta \in \mathbb{Z}[i]$:

1. $N(\alpha) \geq 0$,
2. $N(\alpha) = 0$ if and only if $\alpha = 0$, and
3. $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. The proof is Exercise 47.11. □

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

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.

Definition 47.6. Let D be an integral domain. A *multiplicative norm* N on D is a function mapping D onto the integers $\mathbb{Z}$ such that the following conditions are satisfied:

1. $N(\alpha) = 0$ if and only if $\alpha = 0$, and
2. $N(\alpha\beta) = N(\alpha)N(\beta)$ for all $\alpha, \beta \in D$.

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.

Example 47.8. On $\mathbb{Z}[i]$, the Euclidean norm $N(a + bi) = a^2 + b^2$ is also a multiplicative norm. So Theorem 47.7 applies to $\mathbb{Z}[i]$. As commented above, the unites of $\mathbb{Z}[i]$ are ± 1 and $\pm i$ (as the first claim in Theorem 47.7 verifies). Notice that $5 \in \mathbb{Z}[i]$ is not irreducible since $5 = (1 + 2i)(1 - 2i)$. But, by the second claim of Theorem 47.7, $N(1 + 2i) = N(1 - 2i) = 5$ and so $1 + 2i$ and $1 = 2i$ are irreducible in $\mathbb{Z}[i]$.

Note. The following example, which Fraleigh calls a "standard illustration," is another example of an integral domain which is not a UFD.

Example 47.9. Let $\mathbb{Z}[\sqrt{5}i] = \{a + b\sqrt{5}i \mid a, b \in \mathbb{Z}\}$. Then $\mathbb{Z}[\sqrt{5}i]$ is an integral domain (commutative ring with unity and not divisors of 0). Define N as $N(a + b\sqrt{5}i) = a^2 + b^2$. Then $N(\alpha) = 0$ if and only if $\alpha = 0$. We have $N(\alpha\beta) = M(\alpha)N(\beta)$ (Exercise 47.12). Now e consider the units of $\mathbb{Z}[i\sqrt{5}]$. Suppose $N(\alpha) = 1$ where $\alpha = a_b\sqrt{5}i$. Then $a^2 + 5b^2 = 1$ for integers a and b and it must be that $a = \pm 1$ and $b = 0$. So the units in $\mathbb{Z}[\sqrt{5}i]$ are 1 and -1.

In $\mathbb{Z}[\sqrt{5}i]$ we have $21 = (3)(7) = (1 + 2\sqrt{5}i)(1 - 2\sqrt{5}i)$. Below we show that 3, 7, $1 + 2\sqrt{5}i$, and $1 - 2\sqrt{5}i$ are irreducibles in $\mathbb{Z}[\sqrt{5}i]$ and hence $\mathbb{Z}[\sqrt{5}i]$ is not a UFD.

To show 3 is irreducible, suppose $3 = \alpha\beta$. Then $9 = N(3) = N(\alpha)N(\beta)$ and so $B(\alpha)$ is 1, 3, or 9. If $N(\alpha) = 1$, then α is a unit by Theorem 47.7. If $\alpha = a + b\sqrt{5}i$ then $N(\alpha) = a^2 + 5b^2 = 3$ but there are no such integers a and b so $N(\alpha) \neq 3$. If $N(\alpha) = 9$ then $N(\beta) = 1$ and β is a unit by Theorem 47.7. So if $3 = \alpha\beta$ then either α or β is a unit. That is, 3 is irreducible. Similarly, 7 is irreducible.

If $1 + 2\sqrt{5}i = \gamma\delta$ then $21 = N(1 + 2\sqrt{5}i) = N(\gamma)N(\delta)$, so $N(\gamma)$ is either 1, 3, 7, or 21. By the previous paragraph, there is no element of $\mathbb{Z}[i]$ of norm 3 or 7. So either $N(\gamma) = 1$ and γ is a unit, or $N(\gamma) = 21$, $N(\delta) = 1$, and δ is a unit. So $1 + 2\sqrt{5}i$ is irreducible. Similarly, $1 - 2\sqrt{5}i$ is irreducible.

So $\mathbb{Z}[\sqrt{5}i]$ is not a UFD. Notice that the irreducibles 3, 7, $1+2\sqrt{5}i$, and $1-2\sqrt{5}i$ are irreducibles but they cannot be primes. This is because a property of primes involves unique factorization (see the proof of Theorem 45.17).

Note. The following is an example from "algebraic number theory."

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 $p \equiv 1 \pmod{4}$.

Example. As a quick example, notice that $p = 601$ is a prime which is 1 (mod 4). The corresponding a and b are 5 and 24.

Revised: 3/30/2024