Multiplicative Norms

Let us point out again that for an integral domain D, *the arithmetic concepts of irreducibles and units are not affected in any way by a norm that may be defined on the domain*. However, as the preceding section and our work thus far in this section show, a suitably defined norm may be of help in determining the arithmetic structure of D. This is strikingly illustrated in *algebraic number theory*, where for a domain of *algebraic integers* we consider many different norms of the domain, each doing its part in helping to uncover the arithmetic structure of the domain. In a domain of algebraic integers, we have essentially one norm for each irreducible (up to associates), and each such norm gives information concerning the behavior in the integral domain of the irreducible to which it corresponds. This is an example of the importance of studying properties of elements in an algebraic structure by means of mappings associated with them.

Let us study integral domains that have a multiplicative norm satisfying Properties 2 and 3 of N on $\mathbb{Z}[i]$ given in Lemma 36.2.

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

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

■

36.7 Theorem 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 such that $|N(\alpha)| = 1$ is a unit in D, then an element π 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

$$N(1) = N((1)(1)) = N(1)N(1)$$

shows that $N(1) = 1$. Also, if u is a unit in D, then

$$1 = N(1) = N(uu^{-1}) = N(u)N(u^{-1}).$$

Since $N(u)$ is an integer, this implies that $|N(u)| = 1$.

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 is a prime in $\mathbb{Z}$. Then if $\pi = \alpha\beta$, we have

$$p = |N(\pi)| = |N(\alpha)N(\beta)| = |N(\alpha)||N(\beta)|,$$

so either $|N(\alpha)| = 1$ or $|N(\beta)| = 1$. By assumption, this means that either α or β is a unit of D. Thus π is an irreducible of D. ◆

36.8 Example On $\mathbb{Z}[i]$, the function N defined by $N(a + bi) = a^2 + b^2$ gives a multiplicative norm in the sense of our definition. We saw that the function ν given by $\nu(\alpha) = N(\alpha)$ for nonzero $\alpha \in \mathbb{Z}[i]$ is a Euclidean norm on $\mathbb{Z}[i]$, so the units are precisely the elements α of $\mathbb{Z}[i]$ with $N(\alpha) = N(1) = 1$. Thus the second part of Theorem 36.7 applies in $\mathbb{Z}[i]$. We saw in Example 36.5 that 5 is not an irreducible in $\mathbb{Z}[i]$, for $5 = (1 + 2i)(1 - 2i)$. Since $N(1 + 2i) = N(1 - 2i) = 1^2 + 2^2 = 5$ and 5 is a prime in $\mathbb{Z}$, we see from Theorem 36.7 that $1 + 2i$ and $1 - 2i$ are both irreducibles in $\mathbb{Z}[i]$. ▲

As an application of mutiplicative norms, we shall now give another example of an integral domain that is *not* a UFD. We saw one example in Example 34.17. The following is the standard illustration.

36.9 Example Let $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$. As a subset of the complex numbers closed under addition, subtraction, and multiplication, and containing 0 and 1, $\mathbb{Z}[\sqrt{-5}]$ is an integral

domain. Define N on $\mathbb{Z}[\sqrt{-5}]$ by

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

(Here $\sqrt{-5} = i\sqrt{5}$.) Clearly, $N(\alpha) = 0$ if and only if $\alpha = a + b\sqrt{-5} = 0$. That $N(\alpha\beta) = N(\alpha)N(\beta)$ is a straightforward computation that we leave to the exercises (see Exercise 12). Let us find all candidates for units in $\mathbb{Z}[\sqrt{-5}]$ by finding all elements α in $\mathbb{Z}[\sqrt{-5}]$ with $N(\alpha) = 1$. If $\alpha = a + b\sqrt{-5}$, and $N(\alpha) = 1$, we must have $a^2 + 5b^2 = 1$ for *integers* a and b. This is possible only if $b = 0$ and $a = \pm 1$. Hence ± 1 are the only candidates for units. Since ± 1 are units, they are then precisely the units in $\mathbb{Z}[\sqrt{-5}]$.

Now in $\mathbb{Z}[\sqrt{-5}]$, we have $21 = (3)(7)$ and also

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}).$$

If we can show that 3, 7, $1 + 2\sqrt{-5}$, and $1 - 2\sqrt{-5}$ are all irreducibles in $\mathbb{Z}[\sqrt{-5}]$, we will then know that $\mathbb{Z}[\sqrt{-5}]$ cannot be a UFD, since neither 3 nor 7 is $\pm(1 + 2\sqrt{-5})$.

Suppose that $3 = \alpha\beta$. Then

$$9 = N(3) = N(\alpha)N(\beta)$$

shows that we must have $N(\alpha) = 1$, 3, or 9. If $N(\alpha) = 1$, then α is a unit. If $\alpha = a + b\sqrt{-5}$, then $N(\alpha) = a^2 + 5b^2$, and for no choice of integers a and b is $N(\alpha) = 3$. If $N(\alpha) = 9$, then $N(\beta) = 1$, so β is a unit. Thus from $3 = \alpha\beta$, we can conclude that either α or β is a unit. Therefore, 3 is an irreducible in $\mathbb{Z}[\sqrt{-5}]$. A similar argument shows that 7 is also an irreducible in $\mathbb{Z}[\sqrt{-5}]$.

If $1 + 2\sqrt{-5} = \gamma\delta$, we have

$$21 = N(1 + 2\sqrt{-5}) = N(\gamma)N(\delta).$$

so $N(\gamma) = 1$, 3, 7, or 21. We have seen that there is no element of $\mathbb{Z}[\sqrt{-5}]$ of norm 3 or 7. Thus either $N(\gamma) = 1$, and γ is a unit, or $N(\gamma) = 21$, so $N(\delta) = 1$, and δ is a unit. Therefore, $1 + 2\sqrt{-5}$ is an irreducible in $\mathbb{Z}[\sqrt{-5}]$. A parallel argument shows that $1 - 2\sqrt{-5}$ is also an irreducible in $\mathbb{Z}[\sqrt{-5}]$.

In summary, we have shown that

$$\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$$

is an integral domain but not a UFD. In particular, there are two *different* factorizations

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$$

of 21 into irreducibles. These irreducibles cannot be primes, for the property of a prime enables us to prove uniqueness of factorization (see the proof of Theorem 34.18). ▲

We conclude with a classical application, determining which primes p in $\mathbb{Z}$ are equal to a sum of squares of two integers in $\mathbb{Z}$. For example, $2 = 1^2 + 1^2, 5 = 1^2 + 2^2$, and $13 = 2^2 + 3^2$ are sums of squares. Since we have now answered this question for the only even prime number, 2, we can restrict ourselves to odd primes.

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

Proof First, suppose that $p = a^2 + b^2$. Now a and b cannot both be even or both be odd since p is an odd number. If $a = 2r$ and $b = 2s + 1$, then $a^2 + b^2 = 4r^2 + 4(s^2 + s) + 1$, so $p \equiv 1 \pmod 4$. This takes care of one direction for this "if and only if" theorem.

For the other direction, we assume that $p \equiv 1 \pmod 4$. Now the multiplicative group of nonzero elements of the finite field $\mathbb{Z}_p$ is cyclic, and has order $p - 1$. Since

4 is a divisor of $p-1$, we see that $\mathbb{Z}_p$ contains an element n of multiplicative order 4. It follows that n^2 has multiplicative order 2, so $n^2 = -1$ in $\mathbb{Z}_p$. Thus in $\mathbb{Z}$, we have $n^2 \equiv -1 \pmod{p}$, so p divides $n^2 + 1$ in $\mathbb{Z}$.

Viewing p and $n^2 + 1$ in $\mathbb{Z}[i]$, we see that p divides $n^2 + 1 = (n + i)(n - i)$. Suppose that p is irreducible in $\mathbb{Z}[i]$; then p would have to divide $n + i$ or $n - i$. If p divides $n + i$, then $n + i = p(a + bi)$ for some $a, b \in \mathbb{Z}$. Equating coefficients of i, we obtain $1 = pb$, which is impossible. Similarly, p divides $n - i$ would lead to an impossible equation $-1 = pb$. Thus our assumption that p is irreducible in $\mathbb{Z}[i]$ must be false.

Since p is not irreducible in $\mathbb{Z}[i]$, we have $p = (a + bi)(c + di)$ where neither $a + bi$ nor $c + di$ is a unit. Taking norms, we have $p^2 = (a^2 + b^2)(c^2 + d^2)$ where neither $a^2 + b^2 = 1$ nor $c^2 + d^2 = 1$. Consequently, we have $p = a^2 + b^2$, which completes our proof. [Since $a^2 + b^2 = (a + bi)(a - bi)$, we see that this is the factorization of p, that is, $c + di = a - bi$.] ◆

Exercise 10 asks you to determine which primes p in $\mathbb{Z}$ remain irreducible in $\mathbb{Z}[i]$.

EXERCISES 36

Computations

In Exercises 1 through 4, factor the Gaussian integer into a product of irreducibles in $\mathbb{Z}[i]$. [*Hint:* Since an irreducible factor of $\alpha \in \mathbb{Z}[i]$ must have norm >1 and dividing $N(\alpha)$, there are only a finite number of Gaussian integers $a + bi$ to consider as possible irreducible factors of a given α. Divide α by each of them in $\mathbb{C}$, and see for which ones the quotient is again in $\mathbb{Z}[i]$.]

1. 5 **2.** 7 **3.** $4 + 3i$ **4.** $6 - 7i$

5. Show that 6 does not factor uniquely (up to associates) into irreducibles in $\mathbb{Z}[\sqrt{-5}]$. Exhibit two different factorizations.

6. Consider $\alpha = 7 + 2i$ and $\beta = 3 - 4i$ in $\mathbb{Z}[i]$. Find σ and ρ in $\mathbb{Z}[i]$ such that

$$\alpha = \beta\sigma + \rho \qquad \text{with} \qquad N(\rho) < N(\beta).$$

[*Hint:* Use the construction in the proof of Theorem 36.4.

7. Use a Euclidean algorithm in $\mathbb{Z}[i]$ to find a gcd of $8 + 6i$ and $5 - 15i$ in $\mathbb{Z}[i]$. [*Hint:* Use the construction in the proof of Theorem 36.4.]

Concepts

8. Determine whether each of the following is true or false.

a. $\mathbb{Z}[i]$ is a PID.

b. $\mathbb{Z}[i]$ is a Euclidean domain.

c. Every integer in $\mathbb{Z}$ is a Gaussian integer.

d. Every complex number is a Gaussian integer.

e. A Euclidean algorithm holds in $\mathbb{Z}[i]$.

f. A multiplicative norm on an integral domain is sometimes an aid in finding irreducibles of the domain.

g. If N is a multiplicative norm on an integral domain D, then $|N(u)| = 1$ for every unit u of D.

h. If F is a field, then the function N defined by $N(f(x)) = (\text{degree of } f(x))$ is a multiplicative norm on $F[x]$.

i. If F is a field, then the function defined by $N(f(x)) = 2^{(\text{degree of } f(x))}$ for $f(x) \neq 0$ and $N(0) = 0$ is a multiplicative norm on $F[x]$ according to our definition.

j. $\mathbb{Z}[\sqrt{-5}]$ is an integral domain but not a UFD.

9. Let D be an integral domain with a multiplicative norm N such that $|N(\alpha)| = 1$ for $\alpha \in D$ if and only if α is a unit of D. Let π be such that $|N(\pi)|$ is minimal among all $|N(\beta)| > 1$ for $\beta \in D$. Show that π is an irreducible of D.