Therefore, $M \subseteq C \subseteq D$. However, since $M$ is maximal and $r + M \neq M$, it follows that $C = D$, and so $B = D/M$. Thus, there exists an element $s + M \in D/M$ for which $(r + M)(s + M) = 1 + M$, and so $r + M$ has an inverse in $D/M$. Therefore, $D/M$ is a field. Now, suppose $D/M$ is a field. Let $B$ be an ideal of $D$ for which $M \subseteq B \subseteq D$. We know by Proposition 1.8 that $\varphi(B)$ is an ideal of $D/M$, and since the only ideals in a field are the field itself and $\{0\}$, it follows that either $\varphi(B) = M$ or $\varphi(B) = D/M$. Thus, either $B = M$ or $B = D$, and $M$ is maximal. ■

By combining the results of Theorems 1.11 and 1.12, we obtain the following theorem.

**Theorem 1.13** *Suppose $a$ is an element in a Euclidean domain $D$. Then the following statements are equivalent.*

1. *$a$ is irreducible in $D$.*
2. *$(a)$ is maximal in $D$.*
3. *$D/(a)$ is a field.*

## 1.4 Finite Fields

Finite fields play an important role in several of the applications that we will present in this book. In this section, we will describe the theoretical basis of constructing finite fields.

It can easily be shown that the ring $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ for prime $p$ is a field with the usual operations of addition and multiplication modulo $p$ (i.e., divide the result by $p$ and take the remainder). This shows that there are finite fields of order $p$ for every prime $p$. In the following discussion, we show how the fields $\mathbb{Z}_p$ can be used to construct finite fields of order $p^n$ for every prime $p$ and positive integer $n$.

Suppose $m$ is an irreducible element in a Euclidean domain $D$, and let $B = (m)$. Then by Theorem 1.13, we know that $D/B$ must be a field. If $D$ is the ring $\mathbb{Z}$ of integers and $m > 0$, then $m$ must be a prime $p$. Note that if we perform the addition and multiplication operations in $D/B$ without including $B$ in the notation, these operations will be exactly the addition and multiplication operations in $\mathbb{Z}_p$. Thus, we can view $D/B$ as $\mathbb{Z}_p$.

Now, suppose $D$ is the integral domain $\mathbb{Z}_p[x]$ of polynomials over $\mathbb{Z}_p$ for prime $p$, and let $B = (f(x))$ for some irreducible polynomial $f(x)$ of degree $n$ in $D$. Then again by Theorem 1.13, we know that $D/B$ must be a field. Each element in $D/B$ is a coset of the form $g(x) + B$ for some $g(x) \in \mathbb{Z}_p[x]$. Since $\mathbb{Z}_p[x]$ is a Euclidean domain, there exists $r(x) \in \mathbb{Z}_p[x]$ for which

$g(x)+B = r(x)+B$ with either $r(x) = 0$ or $\deg(r(x)) < n$. Therefore, each element in $D/B$ can be expressed as $r(x) + B$ for some $r(x) \in \mathbb{Z}_p[x]$ with either $r(x) = 0$ or $\deg(r(x)) < n$. Since a polynomial $r(x) \in \mathbb{Z}_p[x]$ with either $r(x) = 0$ or $\deg(r(x)) < n$ can contain up to $n$ terms, and each of these terms can have any of $p$ coefficients (the $p$ elements in $\mathbb{Z}_p$), there are $p^n$ polynomials $r(x) \in \mathbb{Z}_p[x]$ with either $r(x) = 0$ or $\deg(r(x)) < n$. Thus, the field $D/B$ will contain $p^n$ distinct elements. The operations on this field are the usual operations of addition and multiplication modulo $f(x)$ (i.e., divide the result by $f(x)$ and take the remainder). For convenience, when we write elements and perform the addition and multiplication operations in $D/B$, we will not include $B$ in the notation. That is, we will express the elements $r(x) + B$ in $D/B$ as just $r(x)$.

Because it is possible to find an irreducible polynomial of degree $n$ over $\mathbb{Z}_p$ for every prime $p$ and positive integer $n$, the comments in the preceding paragraph indicate that there are finite fields of order $p^n$ for every prime $p$ and positive integer $n$. It is also true that all finite fields have order $p^n$ for some prime $p$ and positive integer $n$ (see Theorem 1.14).

**Example 1.9** Suppose $D = \mathbb{Z}_3[x]$, and let $B = (f(x))$ for the irreducible polynomial $f(x) = x^2 + x + 2 \in \mathbb{Z}_3[x]$. (Note: We could very easily verify that $f(x)$ is irreducible in $\mathbb{Z}_3[x]$ by showing that $f(a) \neq 0$ for all $a \in \mathbb{Z}_3$.) Then the field $D/B$ will contain the $3^2 = 9$ polynomials of degree less than 2 in $\mathbb{Z}_3[x]$. That is, $D/B = \{0, 1, 2, x, x+1, x+2, 2x, 2x+1, 2x+2\}$. To add elements in $D/B$, we simply reduce the coefficients in $\mathbb{Z}_3$. For example, $(2x+1)+(2x+2) = 4x+3 = x$. To multiply elements in $D/B$, we can use several methods. One method is to divide the product by $f(x)$ and take the remainder. For example, to multiply $2x + 1$ and $2x + 2$ in $D/B$, we could form $(2x+1)(2x+2) = 4x^2+6x+2 = x^2+2$. Dividing $x^2+2$ by $f(x)$ yields a quotient of 1 and a remainder of $-x = 2x$. Thus, $(2x + 1)(2x + 2) = 2x$ in $D/B$. Another method for multiplying elements in $D/B$ uses the fact that $x^2 + x + 2 = 0$ in $D/B$. Thus, $x^2 = -x - 2 = 2x + 1$ in $D/B$, an identity that can be used to reduce powers of $x$ in $D/B$. For example, we can also compute the product of $2x + 1$ and $2x + 2$ in $D/B$ by forming $(2x + 1)(2x + 2) = 4x^2 + 6x + 2 = x^2 + 2 = (2x + 1) + 2 = 2x$. We will describe a third method for multiplying elements in $D/B$ next, and then illustrate this method in Example 1.10. ■

A fundamental fact regarding finite fields is that the nonzero elements in every finite field form a cyclic group under multiplication (see Theorem 1.15). Suppose $D = \mathbb{Z}_p[x]$ for some prime $p$, and let $B = (f(x))$ for some irreducible polynomial $f(x) \in D$. For the field $F = D/B$, if $x$ is a cyclic generator for the nonzero elements $F^*$ in $F$, then $f(x)$ is said to be product of $2x$ and $x+2$ in $D/B$ as follows.

$$(2x)(x+2) = x^5x^6 = x^{11} = x^8x^3 = 1x^3 = 2x+2$$

Other products of nonzero elements in $D/B$ can be computed similarly. ■

**Example 1.11** Suppose $D = \mathbb{Z}_3[x]$, and let $B = (f(x))$ for the irreducible polynomial $f(x) = x^2+1 \in \mathbb{Z}_3[x]$. Since $f(x)$ is irreducible of degree 2 in $\mathbb{Z}_3[x]$, then $D/B$ is a field of order $3^2 = 9$, with the exact same elements as the field in Example 1.9. However, note that $x^2 = -1 = 2$ in $D/B$, and so $x^4 = 4 = 1$ in $D/B$. Thus, it follows that computing powers of $x$ will not generate all 8 nonzero elements in $D/B$. Therefore, $f(x) = x^2+1$ is not primitive in $\mathbb{Z}_3[x]$, and we cannot compute all possible products of nonzero elements in $D/B$ using the method illustrated in Example 1.10. However, we can still compute all possible products in $D/B$ using either of the two methods illustrated in Example 1.9. ■

We close this section by proving a pair of fundamental results we have mentioned regarding finite fields.

**Theorem 1.14** *Suppose $F$ is a finite field. Then $|F| = p^n$ for some prime $p$ and positive integer $n$.*

**Proof.** Let $H$ be the additive subgroup of $F$ generated by 1. Suppose that $|H| = mn$ for some positive integers $m, n$ with $m \neq 1$ and $n \neq 1$. Then $0 = (mn)1 = (m1)(n1)$. However, since $m1 \neq 0$ and $n1 \neq 0$, this contradicts the fact that $F$ is a field. Thus, $|H| = p$ for some prime $p$. That is, $H = \mathbb{Z}_p$ for some prime $p$. The field $F$ can be viewed as a vector space over $H$ with scalar multiplication given by the field multiplication, and so $F$ has a basis with a finite number of elements, say $n$. The order of $F$ is then the number $p^n$ of linear combinations of these basis elements over $\mathbb{Z}_p$. ■

**Theorem 1.15** *Suppose $F$ is a finite field. Then the nonzero elements $F^*$ in $F$ form a cyclic multiplicative group.*

**Proof.** Clearly, $F^*$ is an abelian multiplicative group. To show that $F^*$ is cyclic, we use the first of the well-known Sylow Theorems, which states that for any finite group $G$ of order $n$, if $p^k$ divides $n$ for some prime $p$ and positive integer $k$, then $G$ contains a subgroup of order $p^k$. Suppose $|F^*|$ has prime factorization $p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$, and let $S_i$ be subgroups of order $p_i^{n_i}$ in $F^*$ for each $i = 1, 2, \ldots, t$. Also, let $k_i = p_i^{n_i-1}$ for each $i = 1, 2, \ldots, t$. Then if $S_i$ is not cyclic for some $i$, it follows that $a^{k_i} = 1$ for all $a \in S_i$. Thus, $f(x) = x^{k_i} - 1$ has $p_i^{n_i}$ roots in $F$, a contradiction. Therefore, each $S_i$ must have a cyclic generator $a_i$. Let $b = a_1a_2\cdots a_t$. Since $b$ has order $|F^*|$, then $b$ is a cyclic generator for $F^*$. ■