CHAPTER 2

# Introduction to Algebra

The purpose of this chapter is to provide the reader with an elementary knowledge of algebra that will aid in the understanding of the material in the following chapters. The treatment is basically descriptive, and no attempt is made to be mathematically rigorous. There are many good textbooks on algebra. The reader who is interested in more advance algebraic coding theory is referred to the textbooks listed at the end of the chapter.

## 2.1 GROUPS

Let $G$ be a set of elements. A *binary operation* $*$ on $G$ is a *rule* that assigns to each pair of elements $a$ and $b$ a uniquely defined third element $c = a * b$ in $G$. When such a binary operation $*$ is defined on $G$, we say that $G$ is *closed* under $*$. For example, let $G$ be the set of all integers and let the binary operation on $G$ be real addition $+$. We all know that, for any two integers $i$ and $j$ in $G$, $i + j$ is a uniquely defined integer in $G$. Hence, the set of integers is closed under real addition. A binary operation $*$ on $G$ is said to be *associative* if, for any $a$, $b$, and $c$ in $G$,

$$a * (b * c) = (a * b) * c.$$

Now, we introduce a useful algebraic system called a *group*.

DEFINITION 2.1 A set $G$ on which a binary operation $*$ is defined is called a *group* if the following conditions are satisfied:

i. The binary operation $*$ is associative.

ii. $G$ contains an element $e$ such that, for any $a$ in $G$,

$$a * e = e * a = a.$$

This element $e$ is called an *identity element* of $G$.

iii. For any element $a$ in $G$, there exists another element $a'$ in $G$ such that

$$a * a' = a' * a = e.$$

The element $a'$ is called an *inverse* of $a$ ($a$ is also an inverse of $a'$).

A group $G$ is said to be *commutative* if its binary operation $*$ also satisfies the following condition: For any $a$ and $b$ in $G$,

$$a * b = b * a.$$

THEOREM 2.1 The identity element in a group $G$ is unique.

*Proof.* Suppose that there exist two identity elements $e$ and $e'$ in $G$. Then $e' = e' * e = e$. This implies that $e$ and $e'$ are identical. Therefore, there is one and only one identity element. **Q.E.D.**

**THEOREM 2.2** The inverse of a group element is unique.

*Proof.* Suppose that there exist two inverses $a'$ and $a''$ for a group element $a$. Then

$$a' = a' * e = a' * (a * a'') = (a' * a) * a'' = e * a'' = a''.$$

This implies that $a'$ and $a''$ are identical and there is only one inverse for $a$. **Q.E.D.**

The set of all integers is a commutative group under real addition. In this case, the integer 0 is the identity element, and the integer $-i$ is the inverse of integer $i$. The set of all rational numbers excluding zero is a commutative group under real multiplication. The integer 1 is the identity element with respect to real multiplication, and the rational number $b/a$ is the multiplicative inverse of $a/b$. The groups just noted contain infinite numbers of elements. Groups with finite numbers of elements do exist, as we shall see in the next example.

---

**EXAMPLE 2.1**

Consider the set of two integers $G = \{0, 1\}$. Let us define a binary operation, denoted by $\oplus$, on $G$ as follows:

$$0 \oplus 0 = 0, \qquad 0 \oplus 1 = 1, \qquad 1 \oplus 0 = 1, \qquad 1 \oplus 1 = 0.$$

This binary operation is called *modulo-2* addition. The set $G = \{0, 1\}$ is a group under modulo-2 addition. It follows from the definition of modulo-2 addition $\oplus$ that $G$ is closed under $\oplus$, and $\oplus$ is commutative. We can easily check that $\oplus$ is associative. The element 0 is the identity element. The inverse of 0 is itself, and the inverse of 1 is also itself. Thus, $G$ together with $\oplus$ is a commutative group.

---

The number of elements in a group is called the *order* of the group. A group of finite order is called a *finite* group. For any positive integer $m$, it is possible to construct a group of order $m$ under a binary operation that is very similar to real addition, as is shown in the next example.

---

**EXAMPLE 2.2**

Let $m$ be a positive integer. Consider the set of integers $G = \{0, 1, 2, \cdots, m-1\}$. Let $+$ denote real addition. Define a binary operation $\boxplus$ on $G$ as follows: For any integers $i$ and $j$ in $G$,

$$i \boxplus j = r,$$

where $r$ is the *remainder* resulting from dividing $i + j$ by $m$. The remainder $r$ is an integer between 0 and $m - 1$ (Euclid's division algorithm) and is therefore in $G$. Hence, $G$ is closed under the binary operation $\boxplus$, which is called *modulo-m*

*addition*. The set $G = \{0, 1, \cdots, m-1\}$ is a group under modulo-$m$ addition. First, we see that 0 is the identity element. For $0 < i < m$, $i$ and $m - i$ are both in $G$. Since

$$i + (m - i) = (m - i) + i = m,$$

it follows from the definition of modulo-$m$ addition that

$$i \boxplus (m - i) = (m - i) \boxplus i = 0.$$

Therefore, $i$ and $m - i$ are inverses of each other with respect to $\boxplus$. It is also clear that the inverse of 0 is itself. Because real addition is commutative, it follows from the definition of modulo-$m$ addition that, for any $i$ and $j$ in $G$, $i \boxplus j = j \boxplus i$. Therefore, modulo-$m$ addition is commutative. Next, we show that modulo-$m$ addition is also associative. Let $i$, $j$, and $k$ be three integers in $G$. Since real addition is associative, we have

$$i + j + k = (i + j) + k = i + (j + k).$$

Dividing $i + j + k$ by $m$, we obtain

$$i + j + k = qm + r,$$

where $q$ and $r$ are the quotient and the remainder, respectively, and $0 \leq r < m$. Now, dividing $i + j$ by $m$, we have

$$i + j = q_1 m + r_1 \tag{2.1}$$

with $0 \leq r_1 < m$. Therefore, $i \boxplus j = r_1$. Dividing $r_1 + k$ by $m$, we obtain

$$r_1 + k = q_2 m + r_2 \tag{2.2}$$

with $0 \leq r_2 < m$. Hence, $r_1 \boxplus k = r_2$, and

$$(i \boxplus j) \boxplus k = r_2.$$

Combining (2.1) and (2.2), we have

$$i + j + k = (q_1 + q_2)m + r_2.$$

This implies that $r_2$ is also the remainder when $i + j + k$ is divided by $m$. Because the remainder resulting from dividing an integer by another integer is unique, we must have $r_2 = r$. As a result, we have

$$(i \boxplus j) \boxplus k = r.$$

Similarly, we can show that

$$i \boxplus (j \boxplus k) = r.$$

Therefore, $(i \boxplus j) \boxplus k = i \boxplus (j \boxplus k)$, and modulo-$m$ addition is associative. This concludes our proof that the set $G = \{0, 1, 2, \cdots, m-1\}$ is a group under modulo-$m$ addition. We shall call this group an *additive* group. For $m = 2$, we obtain the binary group given in Example 2.1.

TABLE 2.1: Modulo-5 addition.

| $\boxplus$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

The additive group under modulo-5 addition is given in Table 2.1.

Finite groups with a binary operation similar to real multiplication also can be constructed.

---

**EXAMPLE 2.3**

Let $p$ be a prime (e.g., $p = 2, 3, 5, 7, 11, \cdots$). Consider the set of integers, $G = \{1, 2, 3, \cdots, p-1\}$. Let $\cdot$ denote real multiplication. Define a binary operation $\boxdot$ on $G$ as follows: For $i$ and $j$ in $G$,

$$i \boxdot j = r,$$

where $r$ is the remainder resulting from dividing $i \cdot j$ by $p$. First, we note that $i \cdot j$ is not divisible by $p$. Hence, $0 < r < p$, and $r$ is an element in $G$. Therefore, the set $G$ is closed under the binary operation $\boxdot$, which is referred to as *modulo-p multiplication*. The set $G = \{1, 2, \cdots, p-1\}$ is a group under modulo-$p$ multiplication. We can easily check that modulo-$p$ multiplication is commutative and associative. The identity element is 1. The only thing left to be proved is that every element in $G$ has an inverse. Let $i$ be an element in $G$. Because $p$ is a prime, and $i < p$, $i$ and $p$ must be relatively prime (i.e., $i$ and $p$ do not have any common factor greater than 1). It is well known that there exist two integers $a$ and $b$ such that

$$a \cdot i + b \cdot p = 1 \tag{2.3}$$

and $a$ and $p$ are relatively prime (Euclid's theorem). Rearranging (2.3), we have

$$a \cdot i = -b \cdot p + 1. \tag{2.4}$$

This says that when $a \cdot i$ is divided by $p$, the remainder is 1. If $0 < a < p$, $a$ is in $G$, and it follows from (2.4) and the definition of modulo-$p$ multiplication that

$$a \boxdot i = i \boxdot a = 1.$$

Therefore, $a$ is the inverse of $i$. However, if $a$ is not in $G$, we divide $a$ by $p$,

$$a = q \cdot p + r. \tag{2.5}$$

Because $a$ and $p$ are relatively prime, the remainder $r$ cannot be 0, and $r$ must be between 1 and $p-1$. Therefore, $r$ is in $G$. Now, combining (2.4) and (2.5), we obtain

$$r \cdot i = -(b + qi)p + 1.$$

TABLE 2.2: Modulo-5 multiplication.

| $\boxdot$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

Therefore, $r \boxdot i = i \boxdot r = 1$ and $r$ is the inverse of $i$. Hence, any element $i$ in $G$ has an inverse with respect to modulo-$p$ multiplication. The group $G = \{1, 2, \cdots, p-1\}$ under modulo-$p$ multiplication is called a *multiplicative* group. For $p = 2$, we obtain a group $G = \{1\}$ with only one element under modulo-2 multiplication.

If $p$ is *not* a prime, the set $G = \{1, 2, \cdots, p-1\}$ is not a group under modulo-$p$ multiplication (see Problem 2.3). Table 2.2 illustrates the group $G = \{1, 2, 3, 4\}$ under modulo-5 multiplication.

---

Let $H$ be a nonempty subset of $G$. The subset $H$ is said to be a *subgroup* of $G$ if $H$ is closed under the group operation of $G$ and satisfies all the conditions of a group. For example, the set of all rational numbers is a group under real addition. The set of all integers is a subgroup of the group of rational numbers under real addition. A subgroup of $G$ that is not identical to $G$ is called a *proper subgroup* of $G$.

THEOREM 2.3 Let $G$ be a group under the binary operation $*$. Let $H$ be a nonempty subset of $G$. Then $H$ is a subgroup of $G$ if the following conditions hold:

i. $H$ is closed under the binary operation $*$.
iii. For any element $a$ in $H$, the inverse of $a$ is also in $H$.

*Proof.* Condition (ii) says that every element of $H$ has an inverse in $H$. Conditions (i) and (ii) ensure that the identity element of $G$ is also in $H$. Because the elements in $H$ are elements in $G$, the associative condition on $*$ holds automatically. Hence, $H$ satisfies all the conditions of a group and is a subgroup of $G$. Q.E.D.

DEFINITION 2.2 Let $H$ be a subgroup of a group $G$ with binary operation $*$. Let $a$ be an element of $G$. Then the set of elements $a * H \triangleq \{a * h : h \in H\}$ is called a *left coset* of $H$; the set of elements $H * a \triangleq \{h * a : h \in H\}$ is called a *right coset* of $H$.

It is clear that if the group $G$ is commutative, then every left coset $a * H$ is identical to every right coset $H * a$; that is, $a * H = H * a$ for any $a \in G$. In this text, we are primarily interested in commutative groups, so, we will make no further distinction between left and right cosets. We will simply refer to them as cosets.

**EXAMPLE 2.4**

Consider the additive group $G = \{0, 1, 2, \cdots, 15\}$ under modulo-16 addition. We can readily check that $H = \{0, 4, 8, 12\}$ forms a subgroup of $G$. The coset $3 \boxplus H$ is

$$\begin{aligned} 3 \boxplus H &= \{3 \boxplus 0, 3 \boxplus 4, 3 \boxplus 8, 3 \boxplus 12\} \\ &= \{3, 7, 11, 15\}. \end{aligned}$$

The coset $7 \boxplus H$ is

$$\begin{aligned} 7 \boxplus H &= \{7 \boxplus 0, 7 \boxplus 4, 7 \boxplus 8, 7 \boxplus 12\} \\ &= \{7, 11, 15, 3\}. \end{aligned}$$

We find that $3 \boxplus H = 7 \boxplus H$. There are only four distinct cosets of $H$. Besides $3 \boxplus H$, the other three distinct cosets are

$$\begin{aligned} 0 \boxplus H &= \{0, 4, 8, 12\}, \\ 1 \boxplus H &= \{1, 5, 9, 13\}, \\ 2 \boxplus H &= \{2, 6, 10, 14\}. \end{aligned}$$

The four distinct cosets of $H$ are disjoint, and their union forms the entire group $G$.

In the following theorems, we prove some important properties of cosets of a subgroup of a group.

**THEOREM 2.4** Let $H$ be a subgroup of a group $G$ with binary operation $*$. No two elements in a coset of $H$ are identical.

***Proof.*** The proof is based on the fact that all the elements in the subgroup $H$ are distinct. Consider the coset $a * H = \{a * h : h \in H\}$ with $a \in G$. Suppose two elements, say $a * h$ and $a * h'$, in $a * H$ are identical, where $h$ and $h'$ are two distinct elements in $H$. Let $a^{-1}$ denote the inverse of $a$ with respect to the binary operation $*$. Then,

$$\begin{aligned} a^{-1} * (a * h) &= a^{-1} * (a * h'), \\ (a^{-1} * a) * h &= (a^{-1} * a) * h', \\ e * h &= e * h', \\ h &= h'. \end{aligned}$$

This result is a contradiction to the fact that all the elements of $H$ are distinct. Therefore, no two elements in a coset are identical. **Q.E.D.**

**THEOREM 2.5** No two elements in two different cosets of a subgroup $H$ of a group $G$ are identical.

*Proof.* Let $a * H$ and $b * H$ be two distinct cosets of $H$, with $a$ and $b$ in $G$. Let $a * h$ and $b * h'$ be two elements in $a * H$ and $b * H$, respectively. Suppose $a * h = b * h'$. Let $h^{-1}$ be the inverse of $h$. Then

$$\begin{aligned}(a * h) * h^{-1} &= (b * h') * h^{-1},\\ a * (h * h^{-1}) &= b * (h' * h^{-1}),\\ a * e &= b * h'',\\ a &= b * h'',\end{aligned}$$

where $h'' = h' * h^{-1}$ is an element in $H$. The equality $a = b * h''$ implies that

$$\begin{aligned}a * H &= (b * h'') * H,\\ &= \{(b * h'') * h : h \in H\},\\ &= \{b * (h'' * h) : h \in H\},\\ &= \{b * h''' : h''' \in H\},\\ &= b * H.\end{aligned}$$

This result says that $a * H$ and $b * H$ are identical, which is a contradiction to the given condition that $a * H$ and $b * H$ are two distinct cosets of $H$. Therefore, no two elements in two distinct cosets of $H$ are identical. Q.E.D.

From Theorems 2.4 and 2.5, we obtain the following properties of cosets of a subgroup $H$ of a group $G$:

i. Every element in $G$ appears in one and only one coset of $H$;
ii. All the distinct cosets of $H$ are disjoint; and
iii. The union of all the distinct cosets of $H$ forms the group $G$.

Based on the preceding structural properties of cosets, we say that all the distinct cosets of a subgroup $H$ of a group $G$ form a *partition* of $G$, denoted by $G/H$.

THEOREM 2.6 (LAGRANGE'S THEOREM) Let $G$ be a group of order $n$, and let $H$ be a subgroup of order $m$. Then $m$ divides $n$, and the partition $G/H$ consists of $n/m$ cosets of $H$.

*Proof.* It follows from Theorem 2.4 that every coset of $H$ consists of $m$ elements of $G$. Let $i$ be the number of distinct cosets of $H$. Then, it follows from the preceding structural properties of cosets that $n = i \cdot m$. Therefore, $m$ divides $n$, and $i = n/m$. Q.E.D.

## 2.2 FIELDS

Now, we use group concepts to introduce another algebraic system, called a *field*. Roughly speaking, a field is a set of elements in which we can perform addition, subtraction, multiplication, and division without leaving the set. Addition and multiplication must satisfy the commutative, associative, and distributive laws. A formal definition of a field is given next.

**Definition 2.3** Let $F$ be a set of elements on which two binary operations, called addition "+" and multiplication "·", are defined. The set $F$ together with the two binary operations + and · is a field if the following conditions are satisfied:

i. $F$ is a commutative group under addition +. The identity element with respect to addition is called the *zero element* or the *additive identity* of $F$ and is denoted by 0.

ii. The set of nonzero elements in $F$ is a commutative group under multiplication ·. The identity element with respect to multiplication is called the *unit element* or the *multiplicative identity* of $F$ and is denoted by 1.

iii. Multiplication is *distributive* over addition; that is, for any three elements $a$, $b$, and $c$ in $F$,

$$a \cdot (b + c) = a \cdot b + a \cdot c.$$

It follows from the definition that a field consists of at least two elements, the additive identity and the multiplicative identity. Later, we will show that a field of two elements does exist. The number of elements in a field is called the *order* of the field. A field with a finite number of elements is called a *finite field*. In a field, the additive inverse of an element $a$ is denoted by $-a$, and the multiplicative inverse of $a$ is denoted by $a^{-1}$, provided that $a \neq 0$. Subtracting a field element $b$ from another field element $a$ is defined as adding the additive inverse, $-b$, of $b$ to $a$ [i.e., $a - b \triangleq a + (-b)$]. If $b$ is a nonzero element, dividing $a$ by $b$ is defined as multiplying $a$ by the multiplicative inverse, $b^{-1}$, of $b$ [i.e., $a \div b \triangleq a \cdot b^{-1}$].

A number of basic properties of fields can be derived from the definition of a field.

***Property I*** For every element $a$ in a field, $a \cdot 0 = 0 \cdot a = 0$.

***Proof.*** First, we note that

$$a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0.$$

Adding $-a$ to both sides of the preceding equality, we have

$$\begin{aligned} -a + a &= -a + a + a \cdot 0 \\ 0 &= 0 + a \cdot 0 \\ 0 &= a \cdot 0. \end{aligned}$$

Similarly, we can show that $0 \cdot a = 0$. Therefore, we obtain $a \cdot 0 = 0 \cdot a = 0$. **Q.E.D.**

***Property II*** For any two nonzero elements $a$ and $b$ in a field, $a \cdot b \neq 0$.

***Proof.*** This is a direct consequence of the fact that the nonzero elements of a field are closed under multiplication. **Q.E.D.**

***Property III*** $a \cdot b = 0$ and $a \neq 0$ imply that $b = 0$.

*Proof.* This is a direct consequence of Property II. Q.E.D.

*Property IV* For any two elements $a$ and $b$ in a field,

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b).$$

*Proof.* $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. Therefore, $(-a) \cdot b$ must be the additive inverse of $a \cdot b$, and $-(a \cdot b) = (-a) \cdot b$. Similarly, we can prove that $-(a \cdot b) = a \cdot (-b)$. Q.E.D.

*Property V* For $a \neq 0$, $a \cdot b = a \cdot c$ implies that $b = c$.

*Proof.* Because $a$ is a nonzero element in the field, it has a multiplicative inverse, $a^{-1}$. Multiplying both sides of $a \cdot b = a \cdot c$ by $a^{-1}$, we obtain

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$

$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$$

$$1 \cdot b = 1 \cdot c.$$

Thus, $b = c$. Q.E.D.

We can readily verify that the set of real numbers is a field under real-number addition and multiplication. This field has an infinite number of elements. Fields with finite number of elements can be constructed and are illustrated in the next two examples and in Section 2.4.

---

EXAMPLE 2.5

Consider the set $\{0, 1\}$ together with modulo-2 addition and multiplication, defined in Tables 2.3 and 2.4. In Example 2.1 we showed that $\{0, 1\}$ is a commutative group under modulo-2 addition; and in Example 2.3, we showed that $\{1\}$ is a group under modulo-2 multiplication. We can easily check that modulo-2 multiplication is distributive over modulo-2 addition by simply computing $a \cdot (b + c)$ and $a \cdot b + a \cdot c$ for eight possible combinations of $a, b$ and $c$($a = 0$ or $1, b = 0$ or 1, and $c = 0$ or 1). Therefore, the set $\{0, 1\}$ is a field of two elements under modulo-2 addition and modulo-2 multiplication.

---

The field given in Example 2.5 is usually called a *binary field* and is denoted by $GF(2)$. The binary field $GF(2)$ plays an important role in coding theory and is widely used in digital computers and digital data transmission (or storage) systems.

TABLE 2.3: Modulo-2 addition.

| + | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

TABLE 2.4: Modulo-2 multiplication.

| · | 0 | 1 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 0 | 1 |

**EXAMPLE 2.6**

Let $p$ be a prime. We showed in Example 2.2 that the set of integers $\{0, 1, 2, \cdots, p-1\}$ is a commutative group under modulo-$p$ addition. We also showed in Example 2.3 that the nonzero elements $\{1, 2, \cdots, p-1\}$ form a commutative group under modulo-$p$ multiplication. Following the definitions of modulo-$p$ addition and multiplication and the fact that real-number multiplication is distributive over real-number addition, we can show that modulo-$p$ multiplication is distributive over modulo-$p$ addition. Therefore, the set $\{0, 1, 2, \cdots, p-1\}$ is a field of order $p$ under modulo-$p$ addition and multiplication. Because this field is constructed from a prime, $p$, it is called a *prime field* and is denoted by $GF(p)$. For $p = 2$, we obtain the binary field $GF(2)$.

Let $p = 7$. Modulo-7 addition and multiplication are given by Tables 2.5 and 2.6, respectively. The set of integers $\{0, 1, 2, 3, 4, 5, 6\}$ is a field of seven elements, denoted by $GF(7)$, under modulo-7 addition and multiplication. The addition table is also used for subtraction. For example, if we want to subtract 6 from 3, we first use the addition table to find the additive inverse of 6, which is 1. Then we add 1 to 3 to obtain the result [i.e., $3 - 6 = 3 + (-6) = 3 + 1 = 4$]. For division, we use the multiplication table. Suppose that we divide 3 by 2. We first find the multiplicative inverse of 2, which is 4, and then we multiply 3 by 4 to obtain the result [i.e., $3 \div 2 = 3 \cdot (2^{-1}) = 3 \cdot 4 = 5$]. Here we have demonstrated that in a finite field, addition, subtraction, multiplication, and division can be carried out much like ordinary arithmetic, with which we are quite familiar.

In Example 2.6, we showed that, for any prime $p$, there exists a finite field of $p$ elements. In fact, for any positive integer $m$, it is possible to extend the prime field $GF(p)$ to a field of $p^m$ elements, which is called an *extension field* of $GF(p)$ and is denoted by $GF(p^m)$. Furthermore, it has been proved that the order of any finite field is a power of a prime. Finite fields are also called *Galois* fields, in honor of their discoverer. A large portion of algebraic coding theory, code construction, and decoding is built around finite fields. In the rest of this section and in the next two sections we examine some basic structures of finite fields, their arithmetic, and the construction of extension fields from prime fields. Our presentation is mainly descriptive, and no attempt is made to be mathematically rigorous. Because finite-field arithmetic is very similar to ordinary arithmetic, most of the rules of ordinary

TABLE 2.5: Modulo-7 addition.

| + | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

TABLE 2.6: Modulo-7 multiplication.

| · | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

arithmetic apply to finite-field arithmetic. Therefore, it is possible to utilize most of the techniques of algebra in the computations over finite fields.

Consider a finite field of $q$ elements, $GF(q)$. Let us form the following sequence of sums of the unit element 1 in $GF(q)$:

$$\sum_{i=1}^{1} 1 = 1, \quad \sum_{i=1}^{2} 1 = 1 + 1, \quad \sum_{i=1}^{3} 1 = 1 + 1 + 1, \cdots,$$

$$\sum_{i=1}^{k} 1 = 1 + 1 + \cdots + 1 (k \text{ times}), \cdots$$

Because the field is closed under addition, these sums must be elements in the field; and because the field has finite number of elements, these sums cannot be all distinct. Therefore, at some point in the sequence of sums, there must be a repetition; that is, there must exist two positive integers $m$ and $n$ such that $m < n$ and

$$\sum_{i=1}^{m} 1 = \sum_{i=1}^{n} 1.$$

This equality implies that $\sum_{i=1}^{n-m} 1 = 0$. Therefore, there must exist a *smallest positive integer* $\lambda$ such that $\sum_{i=1}^{\lambda} 1 = 0$. This integer $\lambda$ is called the *characteristic* of the field $GF(q)$. The characteristic of the binary field $GF(2)$ is 2, since $1 + 1 = 0$. The characteristic of the prime field $GF(p)$ is $p$, since $\sum_{i=1}^{k} 1 = k \neq 0$ for $1 \leq k < p$ and $\sum_{i=1}^{p} 1 = 0$.

THEOREM 2.7 The characteristic $\lambda$ of a finite field is prime.

*Proof.* Suppose that $\lambda$ is not a prime and is equal to the product of two smaller integers $k$ and $m$ (i.e., $\lambda = km$). Because the field is closed under multiplication,

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i=1}^{m} 1\right)$$

is also a field element. It follows from the distributive law that

$$\left(\sum_{i=1}^{k} 1\right) \cdot \left(\sum_{i=1}^{m} 1\right) = \sum_{i=1}^{km} 1.$$

Because $\sum_{i=1}^{km} 1 = 0$, then either $\sum_{i=1}^{k} 1 = 0$ or $\sum_{i=1}^{m} 1 = 0$; however, this contradicts the definition that $\lambda$ is the smallest positive integer such that $\sum_{i=1}^{\lambda} 1 = 0$. Therefore, we conclude that $\lambda$ is prime. Q.E.D.

It follows from the definition of the characteristic of a finite field that for any two distinct positive integers $k$ and $m$ less than $\lambda$,

$$\sum_{i=1}^{k} 1 \neq \sum_{i=1}^{m} 1.$$

Suppose that $\sum_{i=1}^{k} 1 = \sum_{i=1}^{m} 1$. Then, we have

$$\sum_{i=1}^{m-k} 1 = 0$$

(assuming that $m > k$); however, this is impossible, since $m - k < \lambda$. Therefore, the sums

$$1 = \sum_{i=1}^{1} 1, \quad \sum_{i=1}^{2} 1, \quad \sum_{i=1}^{3} 1, \quad \cdots, \quad \sum_{i=1}^{\lambda-1} 1, \quad \sum_{i=1}^{\lambda} 1 = 0$$

are $\lambda$ distinct elements in $GF(q)$. In fact, this set of sums itself is a field of $\lambda$ elements, $GF(\lambda)$, under the addition and multiplication of $GF(q)$ (see Problem 2.7). Because $GF(\lambda)$ is a subset of $GF(q)$, $GF(\lambda)$ is called a *subfield* of $GF(q)$. Therefore, any finite field $GF(q)$ of characteristic $\lambda$ contains a subfield of $\lambda$ elements. It can be proved that if $q \neq \lambda$, then $q$ is a power of $\lambda$.

Now, let $a$ be a nonzero element in $GF(q)$. Since the set of nonzero elements of $GF(q)$ is closed under multiplication, the following powers of $a$,

$$a^1 = a, \quad a^2 = a \cdot a, \quad a^3 = a \cdot a \cdot a, \cdots$$

must also be nonzero elements in $GF(q)$. Because $GF(q)$ has only a finite number of elements, the powers of $a$ given cannot all be distinct. Therefore, at some point in the sequence of powers of $a$ there must be a repetition; that is, there must exist two positive integers $k$ and $m$ such that $m > k$ and $a^k = a^m$. Let $a^{-1}$ be the multiplicative inverse of $a$. Then $(a^{-1})^k = a^{-k}$ is the multiplicative inverse of $a^k$. Multiplying both sides of $a^k = a^m$ by $a^{-k}$, we obtain

$$1 = a^{m-k}.$$

This equality implies that there must exist a *smallest positive integer* $n$ such that $a^n = 1$. This integer $n$ is called the *order* of the field element $a$. Therefore, the sequence $a^1, a^2, a^3, \cdots$ repeats itself after $a^n = 1$. Also, the powers $a^1, a^2, \cdots, a^{n-1}, a^n = 1$ are all distinct. In fact, they form a group under the multiplication of $GF(q)$. First, we see that they contain the unit element 1. Consider $a^i \cdot a^j$. If $i + j \leq n$,

$$a^i \cdot a^j = a^{i+j}.$$

If $i + j > n$, we have $i + j = n + r$, where $0 < r \leq n$. Hence,

$$a^i \cdot a^j = a^{i+j} = a^n \cdot a^r = a^r.$$

Therefore, the powers $a^1, a^2, \cdots, a^{n-1}, a^n = 1$ are closed under the multiplication of $GF(q)$. For $1 \leq i < n$, $a^{n-i}$ is the multiplicative inverse of $a^i$. Because the powers of $a$ are nonzero elements in $GF(q)$, they satisfy the associative and commutative laws. Therefore, we conclude that $a^n = 1, a^1, a^2, \cdots, a^{n-1}$ form a commutative group under the multiplication of $GF(q)$. A group is said to be *cyclic* if there exists an element in the group whose powers constitute the whole group.

**Theorem 2.8** Let $a$ be a nonzero element of a finite field $GF(q)$. Then $a^{q-1} = 1$.

There are two polynomials over $GF(2)$ with degree 1: $X$ and $1 + X$. There are four polynomials over $GF(2)$ with degree 2: $X^2$, $1 + X^2$, $X + X^2$, and $1 + X + X^2$. In general, there are $2^n$ polynomials over $GF(2)$ with degree $n$.

Polynomials over $GF(2)$ can be added (or subtracted), multiplied, and divided in the usual way. Let

$$g(X) = g_0 + g_1 X + g_2 X^2 + \cdots + g_m X^m$$

be another polynomial over $GF(2)$. To add $f(X)$ and $g(X)$, we simply add the coefficients of the same power of $X$ in $f(X)$ and $g(X)$ as follows (assuming that $m \leq n$):

$$\begin{aligned} f(X) + g(X) = (f_0 + g_0) + (f_1 + g_1)X + \cdots \\ +(f_m + g_m)X^m + f_{m+1}X^{m+1} + \cdots + f_n X^n, \end{aligned}$$

where $f_i + g_i$ is carried out in modulo-2 addition. For example, adding $a(X) = 1 + X + X^3 + X^5$ and $b(X) = 1 + X^2 + X^3 + X^4 + X^7$, we obtain the following sum:

$$\begin{aligned} a(X) + b(X) &= (1 + 1) + X + X^2 + (1 + 1)X^3 + X^4 + X^5 + X^7 \\ &= X + X^2 + X^4 + X^5 + X^7. \end{aligned}$$

When we multiply $f(X)$ and $g(X)$, we obtain the following product:

$$f(X) \cdot g(X) = c_0 + c_1 X + c_2 X^2 + \cdots + c_{n+m} X^{n+m},$$

where

$$\begin{aligned} c_0 &= f_0 g_0, \\ c_1 &= f_0 g_1 + f_1 g_0, \\ c_2 &= f_0 g_2 + f_1 g_1 + f_2 g_0, \\ &\vdots \\ c_i &= f_0 g_i + f_1 g_{i-1} + f_2 g_{i-2} + \cdots + f_i g_0, \\ &\vdots \\ c_{n+m} &= f_n g_m. \end{aligned} \tag{2.6}$$

(Multiplication and addition of coefficients are modulo-2.) It is clear from (2.6) that if $g(X) = 0$, then

$$f(X) \cdot 0 = 0. \tag{2.7}$$

We can readily verify that the polynomials over $GF(2)$ satisfy the following conditions:

i. Commutative:

$$\begin{aligned} a(X) + b(X) &= b(X) + a(X), \\ a(X) \cdot b(X) &= b(X) \cdot a(X). \end{aligned}$$

iii. Associative:

$$a(X) + [b(X) + c(X)] = [a(X) + b(X)] + c(X),$$
$$a(X) \cdot [b(X) \cdot c(X)] = [a(X) \cdot b(X)] \cdot c(X).$$

iiii. Distributive:

$$a(X) \cdot [b(X) + c(X)] = [a(X) \cdot b(X)] + [a(X) \cdot c(X)]. \tag{2.8}$$

Suppose that the degree of $g(X)$ is *not* zero. When $f(X)$ is divided by $g(X)$, we obtain a unique pair of polynomials over $GF(2)$—$q(X)$, called the quotient, and $r(X)$, called the remainder—such that

$$f(X) = q(X)g(X) + r(X),$$

and the degree of $r(X)$ is less than that of $g(X)$. This expression is known as *Euclid's division algorithm.* As an example, we divide $f(X) = 1 + X + X^4 + X^5 + X^6$ by $g(X) = 1 + X + X^3$. Using the long-division technique, we have

$$\begin{array}{r|l} & X^3+X^2 \quad \text{(quotient)} \\ \hline X^3+X+1 & X^6+X^5+X^4 \qquad\qquad +X+1 \\ & \underline{X^6 \quad +X^4+X^3} \\ & \quad X^5 \quad +X^3 \qquad +X+1 \\ & \quad \underline{X^5 \quad +X^3 \; + \; X^2} \\ & \qquad\qquad\qquad X^2+X+1 \qquad \text{(remainder).} \end{array}$$

We can easily verify that

$$X^6 + X^5 + X^4 + X + 1 = (X^3 + X^2)(X^3 + X + 1) + X^2 + X + 1.$$

When $f(X)$ is divided by $g(X)$, if the remainder $r(X)$ is identical to zero $[r(X) = 0]$, we say that $f(X)$ is divisible by $g(X)$, and $g(X)$ is a factor of $f(X)$.

For real numbers, if $a$ is a *root* of a polynomial $f(X)$ [i.e., $f(a) = 0$], $f(X)$ is divisible by $X - a$. (This fact follows from Euclid's division algorithm.) This statement is still true for $f(X)$ over $GF(2)$. For example, let $f(X) = 1+X^2+X^3+X^4$. Substituting $X = 1$, we obtain

$$f(1) = 1 + 1^2 + 1^3 + 1^4 = 1 + 1 + 1 + 1 = 0.$$

Thus, $f(X)$ has 1 as a root, and it should be divisible by $X + 1$, as shown:

$$\begin{array}{r|l} & X^3+X+1 \\ \hline X+1 & X^4+X^3+X^2 \quad +1 \\ & \underline{X^4+X^3} \\ & \qquad\quad X^2 \quad +1 \\ & \qquad\quad \underline{X^2+X} \\ & \qquad\qquad\quad X+1 \\ & \qquad\qquad\quad \underline{X+1} \\ & \qquad\qquad\qquad\quad 0. \end{array}$$

For a polynomial $f(X)$ over $GF(2)$, if the polynomial has an even number of terms, it is divisible by $X + 1$. A polynomial $p(X)$ over $GF(2)$ of degree $m$ is said to be *irreducible* over $GF(2)$ if $p(X)$ is not divisible by any polynomial over $GF(2)$ of degree less than $m$ but greater than zero. Among the four polynomials of degree 2, $X^2$, $X^2 + 1$, and $X^2 + X$ are not irreducible, since they are either divisible by $X$ or $X + 1$; however, $X^2 + X + 1$ does not have either 0 or 1 as a root and so is not divisible by any polynomial of degree 1. Therefore, $X^2 + X + 1$ is an irreducible polynomial of degree 2. The polynomial $X^3 + X + 1$ is an irreducible polynomial of degree 3. First, we note that $X^3 + X + 1$ does not have either 0 or 1 as a root. Therefore, $X^3 + X + 1$ is not divisible by $X$ or $X + 1$. Because the polynomial is not divisible by any polynomial of degree 1, it cannot be divisible by a polynomial of degree 2. Consequently, $X^3 + X + 1$ is irreducible over $GF(2)$. We may verify that $X^4 + X + 1$ is an irreducible polynomial of degree 4. It has been proved that for any $m \geq 1$ there exists an irreducible polynomial of degree $m$. An important theorem regarding irreducible polynomials over $GF(2)$ is given next without a proof.

THEOREM 2.10 Any irreducible polynomial over $GF(2)$ of degree $m$ divides $X^{2^m-1} + 1$.

As an example of Theorem 2.10, we can check that $X^3 + X + 1$ divides $X^{2^3-1} + 1 = X^7 + 1$:

$$
\begin{array}{r|l}
 & X^4 + X^2 + X + 1 \\
X^3 + X + 1 & \overline{X^7 \qquad\qquad\qquad\qquad + 1} \\
 & X^7 + X^5 + X^4 \\
 & \overline{\qquad X^5 + X^4 \qquad\qquad + 1} \\
 & \qquad X^5 + X^3 + X^2 \\
 & \qquad\overline{\qquad X^4 + X^3 + X^2 + 1} \\
 & \qquad\qquad X^4 + X^2 + X \\
 & \qquad\qquad\overline{\qquad X^3 + X + 1} \\
 & \qquad\qquad\qquad X^3 + X + 1 \\
 & \qquad\qquad\qquad\overline{\qquad\qquad 0.}
\end{array}
$$

An irreducible polynomial $p(X)$ of degree $m$ is said to be *primitive* if the smallest positive integer $n$ for which $p(X)$ divides $X^n + 1$ is $n = 2^m - 1$. We may check that $p(X) = X^4 + X + 1$ divides $X^{15} + 1$ but does not divide any $X^n + 1$ for $1 \leq n < 15$. Hence, $X^4 + X + 1$ is a primitive polynomial. The polynomial $X^4 + X^3 + X^2 + X + 1$ is irreducible but it is not primitive, since it divides $X^5 + 1$. It is not easy to recognize a primitive polynomial; however, there are tables of irreducible polynomials in which primitive polynomials are indicated [6, 8]. For a given $m$, there may be more than one primitive polynomial of degree $m$. A list of primitive polynomials is given in Table 2.7. For each degree $m$, we list only a primitive polynomial with the smallest number of terms.

TABLE 2.7: List of primitive polynomials.

| $m$ | | $m$ | |
|---|---|---|---|
| 3 | $1+X+X^3$ | 14 | $1+X+X^6+X^{10}+X^{14}$ |
| 4 | $1+X+X^4$ | 15 | $1+X+X^{15}$ |
| 5 | $1+X^2+X^5$ | 16 | $1+X+X^3+X^{12}+X^{16}$ |
| 6 | $1+X+X^6$ | 17 | $1+X^3+X^{17}$ |
| 7 | $1+X^3+X^7$ | 18 | $1+X^7+X^{18}$ |
| 8 | $1+X^2+X^3+X^4+X^8$ | 19 | $1+X+X^2+X^5+X^{19}$ |
| 9 | $1+X^4+X^9$ | 20 | $1+X^3+X^{20}$ |
| 10 | $1+X^3+X^{10}$ | 21 | $1+X^2+X^{21}$ |
| 11 | $1+X^2+X^{11}$ | 22 | $1+X+X^{22}$ |
| 12 | $1+X+X^4+X^6+X^{12}$ | 23 | $1+X^5+X^{23}$ |
| 13 | $1+X+X^3+X^4+X^{13}$ | 24 | $1+X+X^2+X^7+X^{24}$ |

Before leaving this section, we derive another useful property of polynomials over $GF(2)$. Consider

$$\begin{aligned} f^2(X) &= (f_0 + f_1X + \cdots + f_nX^n)^2 \\ &= [f_0 + (f_1X + f_2X^2 + \cdots + f_nX^n)]^2 \\ &= f_0^2 + f_0 \cdot (f_1X + f_2X^2 + \cdots + f_nX^n) \\ &\quad + f_0 \cdot (f_1X + f_2X^2 + \cdots + f_nX^n) + (f_1X + f_2X^2 + \cdots + f_nX^n)^2 \\ &= f_0^2 + (f_1X + f_2X^2 + \cdots + f_nX^n)^2. \end{aligned}$$

Expanding the preceding equation repeatedly, we eventually obtain

$$f^2(X) = f_0^2 + (f_1X)^2 + (f_2X^2)^2 + \cdots + (f_nX^n)^2.$$

Since $f_i = 0$ or 1, $f_i^2 = f_i$. Hence, we have

$$\begin{aligned} f^2(X) &= f_0 + f_1X^2 + f_2(X^2)^2 + \cdots + f_n(X^2)^n \\ &= f(X^2). \end{aligned} \tag{2.9}$$

It follows from (2.9) that, for any $i \geq 0$,

$$[f(X)]^{2^i} = f(X^{2^i}). \tag{2.10}$$

## 2.4 CONSTRUCTION OF GALOIS FIELD $GF(2^m)$

In this section we present a method for constructing the Galois field of $2^m$ elements ($m > 1$) from the binary field $GF(2)$. We begin with the two elements 0 and 1 from

$GF(2)$ and a new symbol $\alpha$. Then, we define a multiplication "$\cdot$" to introduce a sequence of powers of $\alpha$ as follows:

$$\begin{aligned}
&0 \cdot 0 = 0,\\
&0 \cdot 1 = 1 \cdot 0 = 0,\\
&1 \cdot 1 = 1,\\
&0 \cdot \alpha = \alpha \cdot 0 = 0,\\
&1 \cdot \alpha = \alpha \cdot 1 = \alpha,\\
&\alpha^2 = \alpha \cdot \alpha,\\
&\alpha^3 = \alpha \cdot \alpha \cdot \alpha,\\
&\quad\vdots\\
&\alpha^j = \alpha \cdot \alpha \cdot \cdots \cdot \alpha \ (j \text{ times}),\\
&\quad\vdots
\end{aligned} \tag{2.11}$$

It follows from the preceding definition of multiplication that

$$\begin{aligned}
&0 \cdot \alpha^j = \alpha^j \cdot 0 = 0,\\
&1 \cdot \alpha^j = \alpha^j \cdot 1 = \alpha^j,\\
&\alpha^i \cdot \alpha^j = \alpha^j \cdot \alpha^i = \alpha^{i+j}.
\end{aligned} \tag{2.12}$$

Now, we have the following set of elements on which a multiplication operation "$\cdot$" is defined:

$$F = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^j, \cdots\}.$$

The element 1 is sometimes denoted by $\alpha^0$.

Next, we put a condition on the element $\alpha$ so that the set $F$ contains only $2^m$ elements and is closed under the multiplication "$\cdot$" defined by (2.11). Let $p(X)$ be a primitive polynomial of degree $m$ over $GF(2)$. We assume that $p(\alpha) = 0$ (i.e., $\alpha$ is a root of $p(X)$). Since $p(X)$ divides $X^{2^m-1} + 1$ (Theorem 2.10) we have

$$X^{2^m-1} + 1 = q(X)p(X). \tag{2.13}$$

If we replace $X$ with $\alpha$ in (2.13), we obtain

$$\alpha^{2^m-1} + 1 = q(\alpha)p(\alpha).$$

Because $p(\alpha) = 0$, we have

$$\alpha^{2^m-1} + 1 = q(\alpha) \cdot 0.$$

If we regard $q(\alpha)$ as a polynomial of $\alpha$ over $GF(2)$, it follows from (2.7) that $q(\alpha) \cdot 0 = 0$. As a result, we obtain the following equality:

$$\alpha^{2^m-1} + 1 = 0.$$

Adding 1 to both sides of $\alpha^{2^m-1} + 1 = 0$ (using modulo-2 addition), we obtain the following equality:

$$\alpha^{2^m-1} = 1. \tag{2.14}$$

Therefore, under the condition that $p(\alpha) = 0$, the set $F$ becomes finite and contains the following elements:

$$F^* = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}.$$

The nonzero elements of $F^*$ are closed under the multiplication operation "$\cdot$" defined by (2.11). To see this, let $i$ and $j$ be two integers such that $0 \leq i,\ j < 2^m - 1$. If $i + j < 2^m - 1$, then $\alpha^i \cdot \alpha^j = \alpha^{i+j}$, which is obviously a nonzero element in $F^*$. If $i + j \geq 2^m - 1$, we can express $i + j$ as follows: $i + j = (2^m - 1) + r$, where $0 \leq r < 2^m - 1$. Then,

$$\alpha^i \cdot \alpha^j = \alpha^{i+j} = \alpha^{(2^m-1)+r} = \alpha^{2^m-1} \cdot \alpha^r = \alpha^r,$$

which is also a nonzero element in $F^*$. Hence, we conclude that the nonzero elements of $F^*$ are closed under the multiplication "$\cdot$" defined by (2.11). In fact, these nonzero elements form a commutative group under "$\cdot$". First, we see that the element 1 is the unit element. From (2.11) and (2.12) we see readily that the multiplication operation "$\cdot$" is commutative and associative. For $0 < i < 2^m - 1$, $\alpha^{2^m-i-1}$ is the multiplicative inverse of $\alpha^i$, since

$$\alpha^{2^m-i-1} \cdot \alpha^i = \alpha^{2^m-1} = 1.$$

(Note that $\alpha^0 = \alpha^{2^m-1} = 1$.) It will be clear in the discussion that follows that $1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}$ represent $2^m - 1$ distinct elements. Therefore, the nonzero elements of $F^*$ form a commutative group of order $2^m - 1$ under the multiplication operation "$\cdot$" defined by (2.11).

Our next step is to define an addition operation "+" on $F^*$ so that $F^*$ forms a commutative group under "+". For $0 \leq i < 2^m - 1$, we divide the polynomial $X^i$ by $p(X)$ and obtain the following:

$$X^i = q_i(X)p(X) + a_i(X), \tag{2.15}$$

where $q_i(X)$ and $a_i(X)$ are the quotient and the remainder, respectively. The remainder $a_i(X)$ is a polynomial of degree $m - 1$ or less over $GF(2)$ and is of the following form:

$$a_i(X) = a_{i0} + a_{i1}X + a_{i2}X^2 + \cdots + a_{i,m-1}X^{m-1}.$$

Because $X$ and $p(X)$ are relatively prime (i.e., they do not have any common factor except 1), $X^i$ is not divisible by $p(X)$. Therefore, for any $i \geq 0$,

$$a_i(X) \neq 0. \tag{2.16}$$

For $0 \leq i, j < 2^m - 1$, and $i \neq j$, we can also show that

$$a_i(X) \neq a_j(X). \tag{2.17}$$

Suppose that $a_i(X) = a_j(X)$. Then, it follows from (2.15) that

$$\begin{aligned} X^i + X^j &= [q_i(X) + q_j(X)]p(X) + a_i(X) + a_j(X) \\ &= [q_i(X) + q_j(X)]p(X). \end{aligned}$$

This implies that $p(X)$ divides $X^i + X^j = X^i(1 + X^{j-i})$ (assuming that $j > i$). Because $X^i$ and $p(X)$ are relatively prime, $p(X)$ must divide $X^{j-i} + 1$; however, this is impossible, since $j - i < 2^m - 1$, and $p(X)$ is a primitive polynomial of degree $m$ that does not divide $X^n + 1$ for $n < 2^m - 1$. Therefore, our hypothesis that $a_i(X) = a_j(X)$ is invalid. As a result, for $0 \le i, j < 2^m - 1$, and $i \ne j$, we must have $a_i(X) \ne a_j(X)$. Hence, for $i = 0, 1, 2, \cdots, 2^m - 2$, we obtain $2^m - 1$ distinct nonzero polynomials $a_i(X)$ of degree $m - 1$ or less. Now, replacing $X$ with $\alpha$ in (2.15) and using the equality that $q_i(\alpha) \cdot 0 = 0$ [see (2.7)], we obtain the following polynomial expression for $\alpha^i$:

$$\alpha^i = a_i(\alpha) = a_{i0} + a_{i1}\alpha + a_{i2}\alpha^2 + \cdots + a_{i,m-1}\alpha^{m-1}. \tag{2.18}$$

From (2.16), (2.17), and (2.18), we see that the $2^m - 1$ nonzero elements, $\alpha^0, \alpha^1, \cdots, \alpha^{2^m-2}$ in $F^*$, are represented by $2^m - 1$ *distinct nonzero polynomials* of $\alpha$ over $GF(2)$ with degree $m - 1$ or less. The zero element 0 in $F^*$ may be represented by the *zero polynomial*. As a result, the $2^m$ elements in $F^*$ are represented by $2^m$ *distinct polynomials* of $\alpha$ over $GF(2)$ with degree $m - 1$ or less and are regarded as $2^m$ distinct elements.

Now, we define an addition "+" on $F^*$ as follows:

$$0 + 0 = 0 \tag{2.19a}$$

and, for $0 \le i, j < 2^m - 1$,

$$0 + \alpha^i = \alpha^i + 0 = \alpha^i, \tag{2.19b}$$

$$\begin{aligned} \alpha^i + \alpha^j &= (a_{i0} + a_{i1} + \cdots + a_{i,m-1}\alpha^{m-1}) + (a_{j0} + a_{j1}\alpha + \cdots + a_{j,m-1}\alpha^{m-1}) \\ &= (a_{i0} + a_{j0}) + (a_{i1} + a_{j1})\alpha + \cdots + (a_{i,m-1} + a_{j,m-1})\alpha^{m-1}, \end{aligned} \tag{2.19c}$$

where $a_{i,k} + a_{j,k}$ is carried out in modulo-2 addition for $0 \le k < m$. From (2.19c) we see that, for $i = j$,

$$\alpha^i + \alpha^i = 0 \tag{2.20}$$

and for $i \ne j$,

$$(a_{i0} + a_{j0}) + (a_{i1} + a_{j1})\alpha + \cdots + (a_{i,m-1} + a_{j,m-1})\alpha^{m-1}$$

is nonzero and must be the polynomial expression for some $\alpha^k$ in $F^*$. Hence, the set $F^*$ is closed under the addition "+" defined by (2.19). We can immediately verify that $F^*$ is a commutative group under "+". First, we see that 0 is the additive identity. Because modulo-2 addition is commutative and associative, the addition defined on $F^*$ is also commutative and associative. From (2.19a) and (2.20) we see that the additive inverse of any element in $F^*$ is itself.

Up to this point we have shown that the set $F^* = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$ is a commutative group under an addition operation "+", and the nonzero elements of

$F^*$ form a commutative group under a multiplication operation ".". Using the polynomial representation for the elements in $F^*$ and (2.8) (polynomial multiplication satisfies distributive law), we readily see that the multiplication on $F^*$ is distributive over the addition on $F^*$. Therefore, the set $F^* = \{0, 1, \alpha, \alpha^2, \cdots, \alpha^{2^m-2}\}$ is a Galois field of $2^m$ elements, $GF(2^m)$. We notice that the addition and multiplication defined on $F^* = GF(2^m)$ imply modulo-2 addition and multiplication. Hence, the subset $\{0, 1\}$ forms a subfield of $GF(2^m)$ [i.e., $GF(2)$ is a subfield of $GF(2^m)$]. The binary field $GF(2)$ is usually called the *ground* field of $GF(2^m)$. The characteristic of $GF(2^m)$ is 2.

In our process of constructing $GF(2^m)$ from $GF(2)$, we have developed two representations for the nonzero elements of $GF(2^m)$: the power representation and the polynomial representation. The power representation is convenient for multiplication, and the polynomial representation is convenient for addition.

---

**EXAMPLE 2.7**

Let $m = 4$. The polynomial $p(X) = 1 + X + X^4$ is a primitive polynomial over $GF(2)$. Set $p(\alpha) = 1 + \alpha + \alpha^4 = 0$. Then, $\alpha^4 = 1 + \alpha$. Using this relation, we can construct $GF(2^4)$. The elements of $GF(2^4)$ are given in Table 2.8. The identity $\alpha^4 = 1 + \alpha$ is used repeatedly to form the polynomial representations for the elements of $GF(2^4)$. For example,

$$\alpha^5 = \alpha \cdot \alpha^4 = \alpha(1 + \alpha) = \alpha + \alpha^2,$$
$$\alpha^6 = \alpha \cdot \alpha^5 = \alpha(\alpha + \alpha^2) = \alpha^2 + \alpha^3,$$
$$\alpha^7 = \alpha \cdot \alpha^6 = \alpha(\alpha^2 + \alpha^3) = \alpha^3 + \alpha^4 = \alpha^3 + 1 + \alpha = 1 + \alpha + \alpha^3.$$

To multiply two elements $\alpha^i$ and $\alpha^j$, we simply add their exponents and use the fact that $\alpha^{15} = 1$. For example, $\alpha^5 \cdot \alpha^7 = \alpha^{12}$, and $\alpha^{12} \cdot \alpha^7 = \alpha^{19} = \alpha^4$. Dividing $\alpha^j$ by $\alpha^i$, we simply multiply $\alpha^j$ by the multiplicative inverse $\alpha^{15-i}$ of $\alpha^i$. For example, $\alpha^4/\alpha^{12} = \alpha^4 \cdot \alpha^3 = \alpha^7$, and $\alpha^{12}/\alpha^5 = \alpha^{12} \cdot \alpha^{10} = \alpha^{22} = \alpha^7$. To add $\alpha^i$ and $\alpha^j$, we use their polynomial representations given in Table 2.8. Thus,

$$\alpha^5 + \alpha^7 = (\alpha + \alpha^2) + (1 + \alpha + \alpha^3) = 1 + \alpha^2 + \alpha^3 = \alpha^{13},$$
$$1 + \alpha^5 + \alpha^{10} = 1 + (\alpha + \alpha^2) + (1 + \alpha + \alpha^2) = 0.$$

---

There is another useful representation for the field elements in $GF(2^m)$. Let $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{m-1}\alpha^{m-1}$ be the polynomial representation of a field element $\beta$. Then, we can represent $\beta$ by an ordered sequence of $m$ components called an *m-tuple*, as follows:

$$(a_0, a_1, a_2, \cdots, a_{m-1}),$$

where the $m$ components are simply the $m$ coefficients of the polynomial representation of $\beta$. Clearly, we see that there is one-to-one correspondence between this $m$-tuple and the polynomial representation of $\beta$. The zero element 0 of $GF(2^m)$ is represented by the zero $m$-tuple $(0, 0, \cdots, 0)$. Let $(b_0, b_1, \cdots, b_{m-1})$ be the $m$-tuple

TABLE 2.8: Three representations for the elements of $GF(2^4)$ generated by $p(X) = 1 + X + X^4$.

| Power representation | Polynomial representation | 4-Tuple representation |
|---|---|---|
| 0 | 0 | (0 0 0 0) |
| 1 | 1 | (1 0 0 0) |
| $\alpha$ | $\alpha$ | (0 1 0 0) |
| $\alpha^2$ | $\alpha^2$ | (0 0 1 0) |
| $\alpha^3$ | $\alpha^3$ | (0 0 0 1) |
| $\alpha^4$ | $1+\alpha$ | (1 1 0 0) |
| $\alpha^5$ | $\alpha+\alpha^2$ | (0 1 1 0) |
| $\alpha^6$ | $\alpha^2+\alpha^3$ | (0 0 1 1) |
| $\alpha^7$ | $1+\alpha+\alpha^3$ | (1 1 0 1) |
| $\alpha^8$ | $1+\alpha^2$ | (1 0 1 0) |
| $\alpha^9$ | $\alpha+\alpha^3$ | (0 1 0 1) |
| $\alpha^{10}$ | $1+\alpha+\alpha^2$ | (1 1 1 0) |
| $\alpha^{11}$ | $\alpha+\alpha^2+\alpha^3$ | (0 1 1 1) |
| $\alpha^{12}$ | $1+\alpha+\alpha^2+\alpha^3$ | (1 1 1 1) |
| $\alpha^{13}$ | $1+\alpha^2+\alpha^3$ | (1 0 1 1) |
| $\alpha^{14}$ | $1+\alpha^3$ | (1 0 0 1) |

representation of $\gamma$ in $GF(2^m)$. Adding $\beta$ and $\gamma$, we simply add the corresponding components of their $m$-tuple representations as follows:

$$(a_0 + b_0, a_1 + b_1, \cdots, a_{m-1} + b_{m-1}),$$

where $a_i + b_i$ is carried out in modulo-2 addition. Obviously, the components of the resultant $m$-tuple are the coefficients of the polynomial representation for $\beta + \gamma$. All three representations for the elements of $GF(2^4)$ are given in Table 2.8.

Galois fields of $2^m$ elements with $m = 3$ to 10 are given in Appendix A.

## 2.5 BASIC PROPERTIES OF A GALOIS FIELD $GF(2^m)$

In ordinary algebra we often see that a polynomial with real coefficients has roots not from the field of real numbers but from the field of complex numbers that contains the field of real numbers as a subfield. For example, the polynomial $X^2+6X+25$ does not have roots from the field of real numbers but has two complex-conjugate roots, $-3 + 4i$ and $-3 - 4i$, where $i = \sqrt{-1}$. This situation is also true for polynomials with coefficients from $GF(2)$. In this case, a polynomial with coefficients from $GF(2)$ may not have roots from $GF(2)$ but has roots from an extension field of $GF(2)$. For example, $X^4 + X^3 + 1$ is irreducible over $GF(2)$ and therefore it does not have roots from $GF(2)$; however, it has four roots from the field $GF(2^4)$. If we substitute the elements of $GF(2^4)$ given by Table 2.8 into $X^4 + X^3 + 1$, we find that $\alpha^7$, $\alpha^{11}$, $\alpha^{13}$, and $\alpha^{14}$ are the roots of $X^4 + X^3 + 1$. We may verify this result as follows:

$$(\alpha^7)^4 + (\alpha^7)^3 + 1 = \alpha^{28} + \alpha^{21} + 1 = (1 + \alpha^2 + \alpha^3) + (\alpha^2 + \alpha^3) + 1 = 0.$$

Indeed, $\alpha^7$ is a root for $X^4 + X^3 + 1$. Similarly, we may verify that $\alpha^{11}$, $\alpha^{13}$, and $\alpha^{14}$ are the other three roots. Since $\alpha^7, \alpha^{11}, \alpha^{13}$, and $\alpha^{14}$ are all roots of $X^4 + X^3 + 1$, then $(X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14})$ must be equal to $X^4 + X^3 + 1$. To see this, we multiply out the preceding product using Table 2.8:

$$\begin{aligned}
&(X+\alpha^7)(X+\alpha^{11})(X+\alpha^{13})(X+\alpha^{14}) \\
&\quad = [X^2 + (\alpha^7 + \alpha^{11})X + \alpha^{18}][X^2 + (\alpha^{13} + \alpha^{14})X + \alpha^{27}] \\
&\quad = (X^2 + \alpha^8 X + \alpha^3)(X^2 + \alpha^2 X + \alpha^{12}) \\
&\quad = X^4 + (\alpha^8 + \alpha^2)X^3 + (\alpha^{12} + \alpha^{10} + \alpha^3)X^2 + (\alpha^{20} + \alpha^5)X + \alpha^{15} \\
&\quad = X^4 + X^3 + 1.
\end{aligned}$$

Let $f(X)$ be a polynomial with coefficients from $GF(2)$. If $\beta$, an element in $GF(2^m)$, is a root of $f(X)$, the polynomial $f(X)$ may have other roots from $GF(2^m)$. Then, what are these roots? This question is answered by the following theorem.

**Theorem 2.11** Let $f(X)$ be a polynomial with coefficients from $GF(2)$. Let $\beta$ be an element in an extension field of $GF(2)$. If $\beta$ is a root of $f(X)$, then for any $l \geq 0$, $\beta^{2^l}$ is also a root of $f(X)$.

***Proof.*** From (2.10), we have

$$[f(X)]^{2^l} = f(X^{2^l}).$$

Substituting $\beta$ into the preceding equation, we obtain

$$[f(\beta)]^{2^l} = f(\beta^{2^l}).$$

Since $f(\beta) = 0$, $f(\beta^{2^l}) = 0$. Therefore, $\beta^{2^l}$ is also a root of $f(X)$. **Q.E.D.**

The element $\beta^{2^l}$ is called a *conjugate* of $\beta$. Theorem 2.11 says that if $\beta$, an element in $GF(2^m)$, is a root of a polynomial $f(X)$ over $GF(2)$, then all the distinct conjugates of $\beta$, also elements in $GF(2^m)$, are roots of $f(X)$. For example, the polynomial $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ has $\alpha^4$, an element in $GF(2^4)$ given by Table 2.8, as a root. To verify this, we use Table 2.8 and the fact that $\alpha^{15} = 1$:

$$\begin{aligned}
f(\alpha^4) &= 1 + \alpha^{12} + \alpha^{16} + \alpha^{20} + \alpha^{24} = 1 + \alpha^{12} + \alpha + \alpha^5 + \alpha^9 \\
&= 1 + (1 + \alpha + \alpha^2 + \alpha^3) + \alpha + (\alpha + \alpha^2) + (\alpha + \alpha^3) = 0.
\end{aligned}$$

The conjugates of $\alpha^4$ are

$$(\alpha^4)^2 = \alpha^8, \quad (\alpha^4)^{2^2} = \alpha^{16} = \alpha, \quad (\alpha^4)^{2^3} = \alpha^{32} = \alpha^2.$$

[Note that $(\alpha^4)^{2^4} = \alpha^{64} = \alpha^4$.] It follows from Theorem 2.11 that $\alpha^8, \alpha$, and $\alpha^2$ must also be roots of $f(X) = 1 + X^3 + X^4 + X^5 + X^6$. We can check that $\alpha^5$ and its conjugate, $\alpha^{10}$, are roots of $f(X) = 1 + X^3 + X^4 + X^5 + X^6$. Therefore, $f(X) = 1 + X^3 + X^4 + X^5 + X^6$ has six distinct roots in $GF(2^4)$.

Let $\beta$ be a nonzero element in the field $GF(2^m)$. It follows from Theorem 2.8 that

$$\beta^{2^m-1} = 1.$$

Adding 1 to both sides of $\beta^{2^m-1} = 1$, we obtain

$$\beta^{2^m-1} + 1 = 0.$$

This says that $\beta$ is a root of the polynomial $X^{2^m-1} + 1$. Hence, every nonzero element of $GF(2^m)$ is a root of $X^{2^m-1} + 1$. Because the degree of $X^{2^m-1} + 1$ is $2^m - 1$, the $2^m - 1$ nonzero elements of $GF(2^m)$ form all the roots of $X^{2^m-1} + 1$. Summarizing the preceding result, we obtain Theorem 2.12.

THEOREM 2.12 The $2^m - 1$ nonzero elements of $GF(2^m)$ form all the roots of $X^{2^m-1} + 1$.

Since the zero element 0 of $GF(2^m)$ is the root of $X$, Theorem 2.12 has the following corollary:

COROLLARY 2.12.1 The elements of $GF(2^m)$ form all the roots of $X^{2^m} + X$.

Because any element $\beta$ in $GF(2^m)$ is a root of the polynomial $X^{2^m} + X$, $\beta$ may be a root of a polynomial over $GF(2)$ with a degree less than $2^m$. Let $\phi(X)$ be the polynomial of *smallest degree* over $GF(2)$ such that $\phi(\beta) = 0$. [We can easily prove that $\phi(X)$ is unique.] This polynomial $\phi(X)$ is called the *minimal polynomial of* $\beta$. For example, the minimal polynomial of the zero element 0 of $GF(2^m)$ is $X$, and the minimal polynomial of the unit element 1 is $X + 1$. Next, we derive a number of properties of minimal polynomials.

THEOREM 2.13 The minimal polynomial $\phi(X)$ of a field element $\beta$ is irreducible.

*Proof.* Suppose that $\phi(X)$ is not irreducible and that $\phi(X) = \phi_1(X)\phi_2(X)$, where both $\phi_1(X)$ and $\phi_2(X)$ have degrees greater than 0 and less than the degree of $\phi(X)$. Since $\phi(\beta) = \phi_1(\beta)\phi_2(\beta) = 0$, either $\phi_1(\beta) = 0$ or $\phi_2(\beta) = 0$. This result contradicts the hypothesis that $\phi(X)$ is a polynomial of smallest degree such that $\phi(\beta) = 0$. Therefore, $\phi(X)$ must be irreducible. Q.E.D.

THEOREM 2.14 Let $f(X)$ be a polynomial over $GF(2)$. Let $\phi(X)$ be the minimal polynomial of a field element $\beta$. If $\beta$ is a root of $f(X)$, then $f(X)$ is divisible by $\phi(X)$.

*Proof.* Dividing $f(X)$ by $\phi(X)$, we obtain

$$f(X) = a(X)\phi(X) + r(X),$$

where the degree of the remainder $r(X)$ is less than the degree of $\phi(X)$. Substituting $\beta$ into the preceding equation and using the fact that $f(\beta) = \phi(\beta) = 0$, we have $r(\beta) = 0$. If $r(X) \neq 0$, $r(X)$ would be a polynomial of lower degree than $\phi(X)$, which has $\beta$ as a root. This is a contradiction to the fact that $\phi(X)$ is the minimal polynomial of $\beta$. Hence, $r(X)$ must be identical to 0 and $\phi(X)$ divides $f(X)$. Q.E.D.

The following result follows from Corollary 2.12.1 and Theorem 2.14.

**Theorem 2.15** The minimal polynomial $\phi(X)$ of an element $\beta$ in $GF(2^m)$ divides $X^{2^m} + X$.

Theorem 2.15 says that all the roots of $\phi(X)$ are from $GF(2^m)$. Then, what are the roots of $\phi(X)$? This question is answered by the next two theorems.

**Theorem 2.16** Let $f(X)$ be an irreducible polynomial over $GF(2)$. Let $\beta$ be an element in $GF(2^m)$. Let $\phi(X)$ be the minimal polynomial of $\beta$. If $f(\beta) = 0$, then $\phi(X) = f(X)$.

***Proof.*** It follows from Theorem 2.14 that $\phi(X)$ divides $f(X)$. Since $\phi(X) \neq 1$ and $f(X)$ is irreducible, we must have $\phi(X) = f(X)$. **Q.E.D.**

Theorem 2.16 says that if an irreducible polynomial has $\beta$ as a root, it is the minimal polynomial $\phi(X)$ of $\beta$. It follows from Theorem 2.11 that $\beta$ and its conjugates $\beta^2, \beta^{2^2}, \cdots, \beta^{2^l}, \cdots$ are roots of $\phi(X)$. Let $e$ be the smallest integer such that $\beta^{2^e} = \beta$. Then, $\beta^2, \beta^{2^2}, \cdots, \beta^{2^{e-1}}$ are all the distinct conjugates of $\beta$ (see Problem 2.15). Since $\beta^{2^m} = \beta$, $e \leq m$ (in fact $e$ divides $m$).

**Theorem 2.17** Let $\beta$ be an element in $GF(2^m)$, and let $e$ be the smallest nonnegative integer such that $\beta^{2^e} = \beta$. Then,

$$f(X) = \prod_{i=0}^{e-1} (X + \beta^{2^i})$$

is an irreducible polynomial over $GF(2)$.

***Proof.*** Consider

$$[f(X)]^2 = \left[\prod_{i=0}^{e-1} (X + \beta^{2^i})\right]^2 = \prod_{i=0}^{e-1} (X + \beta^{2^i})^2.$$

Since $(X + \beta^{2^i})^2 = X^2 + (\beta^{2^i} + \beta^{2^i})X + \beta^{2^{i+1}} = X^2 + \beta^{2^{i+1}}$,

$$[f(X)]^2 = \prod_{i=0}^{e-1} (X^2 + \beta^{2^{i+1}}) = \prod_{i=1}^{e} (X^2 + \beta^{2^i})$$

$$= \left[\prod_{i=1}^{e-1} (X^2 + \beta^{2^i})\right] (X^2 + \beta^{2^e}).$$

Since $\beta^{2^e} = \beta$, then

$$[f(X)]^2 = \prod_{i=0}^{e-1} (X^2 + \beta^{2^i}) = f(X^2). \tag{2.21}$$

Let $f(X) = f_0 + f_1 X + \cdots + f_e X^e$, where $f_e = 1$. Expand

$$[f(X)]^2 = (f_0 + f_1 X + \cdots + f_e X^e)^2$$

$$= \sum_{i=0}^{e} f_i^2 X^{2i} + (1+1) \sum_{\substack{i=0 \\ i \neq j}}^{e} \sum_{j=0}^{e} f_i f_j X^{i+j} = \sum_{i=0}^{e} f_i^2 X^{2i}. \tag{2.22}$$

From (2.21) and (2.22), we obtain

$$\sum_{i=0}^{e} f_i X^{2i} = \sum_{i=0}^{e} f_i^2 X^{2i}.$$

Then, for $0 \leq i \leq e$, we must have

$$f_i = f_i^2.$$

This result holds only when $f_i = 0$ or 1. Therefore, $f(X)$ has coefficients from $GF(2)$.

Now, suppose that $f(X)$ is not irreducible over $GF(2)$, and $f(X) = a(X)b(X)$. Since $f(\beta) = 0$, either $a(\beta) = 0$ or $b(\beta) = 0$. If $a(\beta) = 0$, $a(X)$ has $\beta, \beta^2, \cdots, \beta^{2^{e-1}}$ as roots, so $a(X)$ has degree $e$, and $a(X) = f(X)$. Similarly, if $b(\beta) = 0$, $b(X) = f(X)$. Therefore, $f(X)$ must be irreducible. Q.E.D.

A direct consequence of Theorems 2.16 and 2.17 is Theorem 2.18.

THEOREM 2.18 Let $\phi(X)$ be the minimal polynomial of an element $\beta$ in $GF(2^m)$. Let $e$ be the smallest integer such that $\beta^{2^e} = \beta$. Then

$$\phi(X) = \prod_{i=0}^{e-1} (X + \beta^{2^i}). \tag{2.23}$$

---

EXAMPLE 2.8

Consider the Galois field $GF(2^4)$ given by Table 2.8. Let $\beta = \alpha^3$. The conjugates of $\beta$ are

$$\beta^2 = \alpha^6, \quad \beta^{2^2} = \alpha^{12}, \quad \beta^{2^3} = \alpha^{24} = \alpha^9.$$

The minimal polynomial of $\beta = \alpha^3$ is then

$$\phi(X) = (X + \alpha^3)(X + \alpha^6)(X + \alpha^{12})(X + \alpha^9).$$

Multiplying out the right-hand side of the preceding equation with the aid of Table 2.8, we obtain

$$\phi(X) = [X^2 + (\alpha^3 + \alpha^6)X + \alpha^9][X^2 + (\alpha^{12} + \alpha^9)X + \alpha^{21}]$$

$$= (X^2 + \alpha^2 X + \alpha^9)(X^2 + \alpha^8 X + \alpha^6)$$

$$= X^4 + (\alpha^2 + \alpha^8)X^3 + (\alpha^6 + \alpha^{10} + \alpha^9)X^2 + (\alpha^{17} + \alpha^8)X + \alpha^{15}$$

$$= X^4 + X^3 + X^2 + X + 1.$$

---

There is another way of finding the minimal polynomial of a field element, which is illustrated by the following example.

**EXAMPLE 2.9**

Suppose that we want to determine the minimal polynomial $\phi(X)$ of $\gamma = \alpha^7$ in $GF(2^4)$. The distinct conjugates of $\gamma$ are

$$\gamma^2 = \alpha^{14}, \quad \gamma^{2^2} = \alpha^{28} = \alpha^{13}, \quad \gamma^{2^3} = \alpha^{56} = \alpha^{11}.$$

Hence, $\phi(X)$ has degree 4 and must be of the following form:

$$\phi(X) = a_0 + a_1 X + a_2 X^2 + a_3 X^3 + X^4.$$

Substituting $\gamma$ into $\phi(X)$, we have

$$\phi(\gamma) = a_0 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3 + \gamma^4 = 0.$$

Using the polynomial representations for $\gamma$, $\gamma^2$, $\gamma^3$, and $\gamma^4$ in the preceding equation, we obtain the following:

$$a_0 + a_1(1 + \alpha + \alpha^3) + a_2(1 + \alpha^3) + a_3(\alpha^2 + \alpha^3) + (1 + \alpha^2 + \alpha^3) = 0$$
$$(a_0 + a_1 + a_2 + 1) + a_1\alpha + (a_3 + 1)\alpha^2 + (a_1 + a_2 + a_3 + 1)\alpha^3 = 0.$$

For the preceding equality to be true, the coefficients must equal zero:

$$\begin{aligned} a_0 + a_1 + a_2 \quad &+ 1 = 0, \\ a_1 \quad &= 0, \\ a_3 &+ 1 = 0, \\ a_1 + a_2 + a_3 &+ 1 = 0. \end{aligned}$$

Solving the preceding linear equations, we obtain $a_0 = 1$, $a_1 = a_2 = 0$, and $a_3 = 1$. Therefore, the minimal polynomial of $\gamma = \alpha^7$ is $\phi(X) = 1 + X^3 + X^4$. All the minimal polynomials of the elements in $GF(2^4)$ are given by Table 2.9.

TABLE 2.9: Minimal polynomials of the elements in $GF(2^4)$ generated by $p(X) = X^4 + X + 1$.

| Conjugate roots | Minimal polynomials |
|---|---|
| 0 | $X$ |
| 1 | $X + 1$ |
| $\alpha, \alpha^2, \alpha^4, \alpha^8$ | $X^4 + X + 1$ |
| $\alpha^3, \alpha^6, \alpha^9, \alpha^{12}$ | $X^4 + X^3 + X^2 + X + 1$ |
| $\alpha^5, \alpha^{10}$ | $X^2 + X + 1$ |
| $\alpha^7, \alpha^{11}, \alpha^{13}, \alpha^{14}$ | $X^4 + X^3 + 1$ |

A direct consequence of Theorem 2.18 is Theorem 2.19.

THEOREM 2.19 Let $\phi(X)$ be the minimal polynomial of an element $\beta$ in $GF(2^m)$. Let $e$ be the degree of $\phi(X)$. Then $e$ is the smallest integer such that $\beta^{2^e} = \beta$. Moreover, $e \leq m$.

In particular, the degree of the minimal polynomial of any element in $GF(2^m)$ divides $m$. The proof of this property is omitted here. Table 2.9 shows that the degree of the minimal polynomial of each element in $GF(2^4)$ divides by 4. Minimal polynomials of the elements in $GF(2^m)$ for $m = 2$ to 10 are given in Appendix B.

In the construction of the Galois field $GF(2^m)$ we use a primitive polynomial $p(X)$ of degree $m$ and require that the element $\alpha$ be a root of $p(X)$. Because the powers of $\alpha$ generate all the nonzero elements of $GF(2^m)$, $\alpha$ is a primitive element. In fact, all the conjugates of $\alpha$ are primitive elements of $GF(2^m)$. To see this, let $n$ be the order of $\alpha^{2^l}$ for $l > 0$. Then

$$(\alpha^{2^l})^n = \alpha^{n2^l} = 1.$$

Also, it follows from Theorem 2.9 that $n$ divides $2^m - 1$:

$$2^m - 1 = k \cdot n. \tag{2.24}$$

Because $\alpha$ is a primitive element of $GF(2^m)$, its order is $2^m - 1$. For $\alpha^{n2^l} = 1$, $n2^l$ must be a multiple of $2^m - 1$. Since $2^l$ and $2^m - 1$ are relatively prime, $n$ must be divisible by $2^m - 1$, say

$$n = q \cdot (2^m - 1). \tag{2.25}$$

From (2.24) and (2.25) we conclude that $n = 2^m - 1$. Consequently, $\alpha^{2^l}$ is also a primitive element of $GF(2^m)$. In general, we have the following theorem.

THEOREM 2.20 If $\beta$ is a primitive element of $GF(2^m)$, all its conjugates $\beta^2, \beta^{2^2}, \cdots$ are also primitive elements of $GF(2^m)$.

---

EXAMPLE 2.10

Consider the field $GF(2^4)$ given by Table 2.8. The powers of $\beta = \alpha^7$ are

$$\beta^0 = 1,\ \beta^1 = \alpha^7,\ \beta^2 = \alpha^{14},\ \beta^3 = \alpha^{21} = \alpha^6,\ \beta^4 = \alpha^{28} = \alpha^{13},$$
$$\beta^5 = \alpha^{35} = \alpha^5,\ \beta^6 = \alpha^{42} = \alpha^{12},\ \beta^7 = \alpha^{49} = \alpha^4,\ \beta^8 = \alpha^{56} = \alpha^{11},$$
$$\beta^9 = \alpha^{63} = \alpha^3,\ \beta^{10} = \alpha^{70} = \alpha^{10},\ \beta^{11} = \alpha^{77} = \alpha^2,\ \beta^{12} = \alpha^{84} = \alpha^9,$$
$$\beta^{13} = \alpha^{91} = \alpha,\ \beta^{14} = \alpha^{98} = \alpha^8,\ \beta^{15} = \alpha^{105} = 1.$$

Clearly, the powers of $\beta = \alpha^7$ generate all the nonzero elements of $GF(2^4)$, so $\beta = \alpha^7$ is a primitive element of $GF(2^7)$. The conjugates of $\beta = \alpha^7$ are

$$\beta^2 = \alpha^{14}, \quad \beta^{2^2} = \alpha^{13}, \quad \beta^{2^3} = \alpha^{11}.$$

We may readily check that they are all primitive elements of $GF(2^m)$.

---

A more general form of Theorem 2.20 is Theorem 2.21.

**THEOREM 2.21** If $\beta$ is an element of order $n$ in $GF(2^m)$, all its conjugates have the same order $n$. (The proof is left as an exercise.)

---

**EXAMPLE 2.11**

Consider the element $\alpha^5$ in $GF(2^4)$ given by Table 2.8. Since $(\alpha^5)^{2^2} = \alpha^{20} = \alpha^5$, the only conjugate of $\alpha^5$ is $\alpha^{10}$. Both $\alpha^5$ and $\alpha^{10}$ have order $n = 3$. The minimal polynomial of $\alpha^5$ and $\alpha^{10}$ is $X^2 + X + 1$, whose degree is a factor of $m = 4$. The conjugates of $\alpha^3$ are $\alpha^6$, $\alpha^9$, and $\alpha^{12}$. They all have order $n = 5$.

---

## 2.6 COMPUTATIONS USING GALOIS FIELD $GF(2^m)$ ARITHMETIC

Here we perform some example computations using arithmetic over $GF(2^m)$. Consider the following linear equations over $GF(2^4)$ (see Table 2.8):

$$\begin{aligned} X + \alpha^7 Y &= \alpha^2, \\ \alpha^{12} X + \alpha^8 Y &= \alpha^4. \end{aligned} \tag{2.26}$$

Multiplying the second equation by $\alpha^3$ gives

$$\begin{aligned} X + \alpha^7 Y &= \alpha^2, \\ X + \alpha^{11} Y &= \alpha^7. \end{aligned}$$

By adding the two preceding equations, we get

$$\begin{aligned} (\alpha^7 + \alpha^{11}) Y &= \alpha^2 + \alpha^7, \\ \alpha^8 Y &= \alpha^{12}, \\ Y &= \alpha^4. \end{aligned}$$

Substituting $Y = \alpha^4$ into the first equation of (2.26), we obtain $X = \alpha^9$. Thus, the solution for the equations of (2.26) is $X = \alpha^9$ and $Y = \alpha^4$.

Alternatively, the equations of (2.26) could be solved by using Cramer's rule:

$$X = \frac{\begin{vmatrix} \alpha^2 & \alpha^7 \\ \alpha^4 & \alpha^8 \end{vmatrix}}{\begin{vmatrix} 1 & \alpha^7 \\ \alpha^{12} & \alpha^8 \end{vmatrix}} = \frac{\alpha^{10} + \alpha^{11}}{\alpha^8 + \alpha^{19}} = \frac{1 + \alpha^3}{\alpha + \alpha^2} = \frac{\alpha^{14}}{\alpha^5} = \alpha^9,$$

$$Y = \frac{\begin{vmatrix} 1 & \alpha^2 \\ \alpha^{12} & \alpha^4 \end{vmatrix}}{\begin{vmatrix} 1 & \alpha^7 \\ \alpha^{12} & \alpha^8 \end{vmatrix}} = \frac{\alpha^4 + \alpha^{14}}{\alpha^8 + \alpha^{19}} = \frac{\alpha + \alpha^3}{\alpha + \alpha^2} = \frac{\alpha^9}{\alpha^5} = \alpha^4.$$

As one more example, suppose that we want to solve the equation

$$f(X) = X^2 + \alpha^7 X + \alpha = 0$$

over $GF(2^4)$. The quadratic formula will not work because it requires dividing by 2, and in this field, $2 = 0$. If $f(X) = 0$ has any solutions in $GF(2^4)$, the solutions can be found simply by substituting all the elements of Table 2.8 for $X$. By doing so, we would find that $f(\alpha^6) = 0$ and $f(\alpha^{10}) = 0$, since

$$f(\alpha^6) = (\alpha^6)^2 + \alpha^7 \cdot \alpha^6 + \alpha = \alpha^{12} + \alpha^{13} + \alpha = 0,$$
$$f(\alpha^{10}) = (\alpha^{10})^2 + \alpha^7 \cdot \alpha^{10} + \alpha = \alpha^5 + \alpha^2 + \alpha = 0.$$

Thus, $\alpha^6$ and $\alpha^{10}$ are the roots of $f(X)$, and $f(X) = (X + \alpha^6)(X + \alpha^{10})$.

The preceding computations are typical of those required for decoding codes such as BCH and Reed–Solomon codes, and they can be programmed quite easily on a general-purpose computer. It is also a simple matter to build a computer that can do this kind of arithmetic.

## 2.7 VECTOR SPACES

Let $V$ be a set of elements on which a binary operation called addition, $+$, is defined. Let $F$ be a field. A multiplication operation, denoted by $\cdot$, between the elements in $F$ and elements in $V$ is also defined. The set $V$ is called a *vector space* over the field $F$ if it satisfies the following conditions:

i. $V$ is a commutative group under addition.

ii. For any element $a$ in $F$ and any element $\mathbb{v}$ in $V$, $a \cdot \mathbb{v}$ is an element in $V$.

iii. (Distributive Laws) For any elements $\mathbb{u}$ and $\mathbb{v}$ in $V$ and any elements $a$ and $b$ in $F$,

$$a \cdot (\mathbb{u} + \mathbb{v}) = a \cdot \mathbb{u} + a \cdot \mathbb{v},$$
$$(a + b) \cdot \mathbb{v} = a \cdot \mathbb{v} + b \cdot \mathbb{v}.$$

iv. (Associative Law) For any $\mathbb{v}$ in $V$ and any $a$ and $b$ in $F$,

$$(a \cdot b) \cdot \mathbb{v} = a \cdot (b \cdot \mathbb{v}).$$

v. Let 1 be the unit element of $F$. Then, for any $\mathbb{v}$ in $V$, $1 \cdot \mathbb{v} = \mathbb{v}$.

The elements of $V$ are called *vectors*, and the elements of the field $F$ are called *scalars*. The addition on $V$ is called a *vector addition*, and the multiplication that combines a scalar in $F$ and a vector in $V$ into a vector in $V$ is referred to as *scalar multiplication* (or *product*). The additive identity of $V$ is denoted by $\mathbb{0}$.

Some basic properties of a vector space $V$ over a field $F$ can be derived from the preceding definition.

*Property I* Let 0 be the zero element of the field $F$. For any vector $\mathbb{v}$ in $V$, $0 \cdot \mathbb{v} = \mathbb{0}$.

*Proof.* Because $1 + 0 = 1$ in $F$, we have $1 \cdot \mathbb{v} = (1 + 0) \cdot \mathbb{v} = 1 \cdot \mathbb{v} + 0 \cdot \mathbb{v}$. Using condition (v) of the preceding definition of a vector space, we obtain

$\mathbf{v} = \mathbf{v} + 0 \cdot \mathbf{v}$. Let $-\mathbf{v}$ be the additive inverse of $\mathbf{v}$. Adding $-\mathbf{v}$ to both sides of $\mathbf{v} = \mathbf{v} + 0 \cdot \mathbf{v}$, we have

$$\mathbf{0} = \mathbf{0} + 0 \cdot \mathbf{v}$$

$$\mathbf{0} = 0 \cdot \mathbf{v}.$$

***Property II*** For any scalar $c$ in $F$, $c \cdot \mathbf{0} = \mathbf{0}$. (The proof is left as an exercise.)

***Property III*** For any scalar $c$ in $F$ and any vector $\mathbf{v}$ in $V$,

$$(-c) \cdot \mathbf{v} = c \cdot (-\mathbf{v}) = -(c \cdot \mathbf{v})$$

That is, $(-c) \cdot \mathbf{v}$ or $c \cdot (-\mathbf{v})$ is the additive inverse of the vector $c \cdot \mathbf{v}$. (The proof is left as an exercise.)

Next, we present a very useful vector space over $GF(2)$ that plays a central role in coding theory. Consider an ordered sequence of $n$ components,

$$(a_0, a_1, \cdots a_{n-1}),$$

where each component $a_i$ is an element from the binary field $GF(2)$ (i.e., $a_i = 0$ or 1). This sequence is generally called an $n$-tuple over $GF(2)$. Because there are two choices for each $a_i$, we can construct $2^n$ distinct $n$-tuples. Let $V_n$ denote this set of $2^n$ distinct $n$-tuples over $GF(2)$. Now, we define an addition, $+$, on $V_n$ as the following: For any $\mathbf{u} = (u_0, u_1, \cdots, u_{n-1})$ and $\mathbf{v} = (v_0, v_1, \cdots, v_{n-1})$ in $V_n$,

$$\mathbf{u} + \mathbf{v} = (u_0 + v_0, u_1 + v_1, \cdots, u_{n-1} + v_{n-1}), \tag{2.27}$$

where $u_i + v_i$ is carried out in modulo-2 addition. Clearly, $\mathbf{u} + \mathbf{v}$ is also an $n$-tuple over $GF(2)$. Hence, $V_n$ is closed under the addition defined by (2.27). We can readily verify that $V_n$ is a commutative group under the addition defined by (2.27). First, we note that the all-zero $n$-tuple $\mathbf{0} = (0, 0, \cdots, 0)$ is the additive identity. For any $\mathbf{v}$ in $V_n$,

$$\begin{aligned}\mathbf{v} + \mathbf{v} &= (v_0 + v_0, v_1 + v_1, \cdots, v_{n-1} + v_{n-1}) \\ &= (0, 0, \cdots, 0) = \mathbf{0}.\end{aligned}$$

Hence, the additive inverse of each $n$-tuple in $V_n$ is itself. Because modulo-2 addition is commutative and associative, we can easily check that the addition defined by (2.27) is also commutative and associative. Therefore, $V_n$ is a commutative group under the addition defined by (2.27).

Next, we define scalar multiplication of an $n$-tuple $\mathbf{v}$ in $V_n$ by an element $a$ from $GF(2)$ as follows:

$$a \cdot (v_0, v_1, \cdots, v_{n-1}) = (a \cdot v_0, a \cdot v_1, \cdots, a \cdot v_{n-1}), \tag{2.28}$$

where $a \cdot v_i$ is carried out in modulo-2 multiplication. Clearly, $a \cdot (v_0, v_1, \cdots, v_{n-1})$ is also an $n$-tuple in $V_n$. If $a = 1$,

$$\begin{aligned}1 \cdot (v_0, v_1, \cdots, v_{n-1}) &= (1 \cdot v_0, 1 \cdot v_1, \cdots, 1 \cdot v_{n-1}) \\ &= (v_0, v_1, \cdots, v_{n-1}).\end{aligned}$$

We can easily show that the vector addition and scalar multiplication defined by (2.27) and (2.28), respectively, satisfy the distributive and associative laws. Therefore, the set $V_n$ of all $n$-tuples over $GF(2)$ forms a vector space over $GF(2)$.

---

EXAMPLE 2.12

Let $n = 5$. The vector space $V_5$ of all 5-tuples over $GF(2)$ consists of the following 32 vectors:

$$\begin{array}{cccc}
(00000), & (00001), & (00010), & (00011), \\
(00100), & (00101), & (00110), & (00111), \\
(01000), & (01001), & (01010), & (01011), \\
(01100), & (01101), & (01110), & (01111), \\
(10000), & (10001), & (10010), & (10011), \\
(10100), & (10101), & (10110), & (10111), \\
(11000), & (11001), & (11010), & (11011), \\
(11100), & (11101), & (11110), & (11111).
\end{array}$$

The vector sum of (10111) and (11001) is

$$(10111) + (11001) = (1+1, 0+1, 1+0, 1+0, 1+1) = (01110).$$

Using the rule of scalar multiplication defined by (2.28), we obtain

$$0 \cdot (11010) = (0 \cdot 1, 0 \cdot 1, 0 \cdot 0, 0 \cdot 1, 0 \cdot 0) = (00000),$$
$$1 \cdot (11010) = (1 \cdot 1, 1 \cdot 1, 1 \cdot 0, 1 \cdot 1, 1 \cdot 0) = (11010).$$

---

The vector space of all $n$-tuples over any field $F$ can be constructed in a similar manner; however, in this text we are mostly concerned with the vector space of all $n$-tuples over $GF(2)$ or over an extension field of $GF(2)$ [e.g., $GF(2^m)$].

Because $V$ is a vector space over a field $F$, it may happen that a subset $S$ of $V$ is also a vector space over $F$. Such a subset is called a *subspace* of $V$.

THEOREM 2.22 Let $S$ be a nonempty subset of a vector space $V$ over a field $F$. Then, $S$ is a subspace of $V$ if the following conditions are satisfied:

i. For any two vectors $\mathbb{u}$ and $\mathbb{v}$ in $S$, $\mathbb{u} + \mathbb{v}$ is also a vector in $S$.
ii. For any element $a$ in $F$ and any vector $\mathbb{u}$ in $S$, $a \cdot \mathbb{u}$ is also in $S$.

*Proof.* Conditions (i) and (ii) simply say that $S$ is closed under vector addition and scalar multiplication of $V$. Condition (ii) ensures that for any vector $\mathbb{v}$ in $S$ its additive inverse $(-1) \cdot \mathbb{v}$ is also in $S$. Then, $\mathbb{v} + (-1) \cdot \mathbb{v} = \mathbb{0}$ is also in $S$. Therefore, $S$ is a subgroup of $V$. Because the vectors of $S$ are also vectors of $V$, the associative and distributive laws must hold for $S$. Hence, $S$ is a vector space over $F$ and is a subspace of $V$. Q.E.D.

**EXAMPLE 2.13**

Consider the vector space $V_5$ of all 5-tuples over $GF(2)$ given in Example 2.12. The set

$$\{(00000), (00111), (11010), (11101)\}$$

satisfies both conditions of Theorem 2.22, so it is a subspace of $V_5$.

Let $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ be $k$ vectors in a vector space $V$ over a field $F$. Let $a_1, a_2, \cdots, a_k$ be $k$ scalars from $F$. The sum

$$a_1\mathbb{v}_1 + a_2\mathbb{v}_2 + \cdots + a_k\mathbb{v}_k$$

is called a *linear combination* of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$. Clearly, the sum of two linear combinations of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$,

$$\begin{aligned}(a_1\mathbb{v}_1 + a_2\mathbb{v}_2 + \cdots + a_k\mathbb{v}_k) + (b_1\mathbb{v}_1 + b_2\mathbb{v}_2 + \cdots + b_k\mathbb{v}_k)\\ = (a_1 + b_1)\mathbb{v}_1 + (a_1 + b_2)\mathbb{v}_2 + \cdots + (a_k + b_k)\mathbb{v}_k,\end{aligned}$$

is also a linear combination of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$, and the product of a scalar $c$ in $F$ and a linear combination of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$,

$$c \cdot (a_1\mathbb{v}_1 + a_2\mathbb{v}_2 + \cdots + a_k\mathbb{v}_k) = (c \cdot a_1)\mathbb{v}_1 + (c \cdot a_2)\mathbb{v}_2 + \cdots + (c \cdot a_k)\mathbb{v}_k,$$

is also a linear combination of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$. It follows from Theorem 2.22 that we have the following result.

THEOREM 2.23 Let $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ be $k$ vectors in a vector space $V$ over a field $F$. The set of all linear combinations of $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ forms a subspace of $V$.

**EXAMPLE 2.14**

Consider the vector space $V_5$ of all 5-tuples over $GF(2)$ given by Example 2.12. The linear combinations of (00111) and (11101) are

$$\begin{aligned}0 \cdot (00111) + 0 \cdot (11101) &= (00000),\\ 0 \cdot (00111) + 1 \cdot (11101) &= (11101),\\ 1 \cdot (00111) + 0 \cdot (11101) &= (00111),\\ 1 \cdot (00111) + 1 \cdot (11101) &= (11010).\end{aligned}$$

These four vectors form the same subspace given by Example 2.13.

A set of vectors $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ in a vector space $V$ over a field $F$ is said to be *linearly dependent* if and only if there exist $k$ scalars $a_1, a_2, \cdots, a_k$ from $F$, *not all zero*, such that

$$a_1\mathbb{v}_1 + a_2\mathbb{v}_2 + \cdots + a_k\mathbb{v}_k = \mathbb{0}.$$

The null space $S_d$ of $S$ consists of the following four vectors:

$$(00000), \quad (10101), \quad (01110), \quad (11011).$$

$S_d$ is spanned by (10101) and (01110), which are linearly independent. Thus, the dimension of $S_d$ is 2.

---

All the results presented in this section can be generalized in a straightforward manner to the vector space of all $n$-tuples over $GF(q)$, where $q$ is a power of prime (see Section 7.1).

## 2.8 MATRICES

A $k \times n$ matrix over $GF(2)$ (or over any other field) is a rectangular array with $k$ rows and $n$ columns,

$$\mathbb{G} = \begin{bmatrix} g_{00} & g_{01} & g_{02} & \cdots & g_{0,n-1} \\ g_{10} & g_{11} & g_{12} & \cdots & g_{1,n-1} \\ \vdots & & & & \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix}, \tag{2.30}$$

where each entry $g_{ij}$ with $0 \leq i < k$ and $0 \leq j < n$ is an element from the binary field $GF(2)$. Observe that the first index, $i$, indicates the row containing $g_{ij}$, and the second index, $j$, tells which column $g_{ij}$ is in. We shall sometimes abbreviate the matrix of (2.30) by the notation $[g_{ij}]$. We also observe that each row of $\mathbb{G}$ is an $n$-tuple over $GF(2)$, and each column is a $k$-tuple over $GF(2)$. The matrix $\mathbb{G}$ can also be represented by its $k$ rows $\mathbb{g}_0, \mathbb{g}_1, \cdots, \mathbb{g}_{k-1}$ as follows:

$$\mathbb{G} = \begin{bmatrix} \mathbb{g}_0 \\ \mathbb{g}_1 \\ \vdots \\ \mathbb{g}_{k-1} \end{bmatrix}.$$

If the $k (k \leq n)$ rows of $\mathbb{G}$ are linearly independent, then the $2^k$ linear combinations of these rows form a $k$-dimensional subspace of the vector space $V_n$ of all the $n$-tuples over $GF(2)$. This subspace is called the *row space* of $\mathbb{G}$. We may interchange any two rows of $\mathbb{G}$ or add one row to another. These are called *elementary row operations*. Performing elementary row operations on $\mathbb{G}$, we obtain another matrix $\mathbb{G}'$ over $GF(2)$; however, both $\mathbb{G}$ and $\mathbb{G}'$ give the same row space.

---

### EXAMPLE 2.17

Consider a $3 \times 6$ matrix $\mathbb{G}$ over $GF(2)$,

$$\mathbb{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

Adding the third row to the first row and interchanging the second and third rows, we obtain the following matrix:

$$\mathbb{G}' = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{bmatrix}.$$

Both $\mathbb{G}$ and $\mathbb{G}'$ give the following row space:

$$(000000), \quad (100101), \quad (010011), \quad (001110),$$
$$(110110), \quad (101011), \quad (011101), \quad (111000).$$

This is a three-dimensional subspace of the vector space $V_6$ of all the 6-tuples over $GF(2)$.

---

Let $S$ be the row space of a $k \times n$ matrix $\mathbb{G}$ over $GF(2)$ whose $k$ rows $\mathbb{g}_0, \mathbb{g}_1, \cdots, \mathbb{g}_{k-1}$ are linearly independent. Let $S_d$ be the null space of $S$. Then, the dimension of $S_d$ is $n-k$. Let $\mathbb{h}_0, \mathbb{h}_1, \cdots, \mathbb{h}_{n-k-1}$ be $n-k$ linearly independent vectors in $S_d$. Clearly, these vectors span $S_d$. We may form an $(n-k) \times n$ matrix $\mathbb{H}$ using $\mathbb{h}_0, \mathbb{h}_1, \cdots, \mathbb{h}_{n-k-1}$ as rows:

$$\mathbb{H} = \begin{bmatrix} \mathbb{h}_0 \\ \mathbb{h}_1 \\ \vdots \\ \mathbb{h}_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{00} & h_{01} & \cdots & h_{0,n-1} \\ h_{10} & h_{11} & \cdots & h_{1,n-1} \\ \vdots & \vdots & & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix}.$$

The row space of $\mathbb{H}$ is $S_d$. Because each row $\mathbb{g}_i$ of $\mathbb{G}$ is a vector in $S$, and each row $\mathbb{h}_j$ of $\mathbb{H}$ is a vector of $S_d$, the inner product of $\mathbb{g}_i$ and $\mathbb{h}_j$ must be zero (i.e., $\mathbb{g}_i \cdot \mathbb{h}_j = 0$). Because the row space $S$ of $\mathbb{G}$ is the null space of the row space $S_d$ of $\mathbb{H}$, we call $S$ the null (or dual) space of $\mathbb{H}$. Summarizing the preceding results, we have Theorem 2.25.

**THEOREM 2.25** For any $k \times n$ matrix $\mathbb{G}$ over $GF(2)$ with $k$ linearly independent rows, there exists an $(n-k) \times n$ matrix $\mathbb{H}$ over $GF(2)$ with $n-k$ linearly independent rows such that for any row $\mathbb{g}_i$ in $\mathbb{G}$ and any $\mathbb{h}_j$ in $\mathbb{H}$, $\mathbb{g}_i \cdot \mathbb{h}_j = 0$. The row space of $\mathbb{G}$ is the null space of $\mathbb{H}$, and vice versa.

---

**EXAMPLE 2.18**

Consider the following $3 \times 6$ matrix over $GF(2)$:

$$\mathbb{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \end{bmatrix}.$$

The row space of this matrix is the null space

$$\mathbb{H} = \begin{bmatrix} 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

We can easily check that each row of $\mathbb{G}$ is orthogonal to each row of $\mathbb{H}$.

---

Two matrices can be added if they have the same number of rows and the same number of columns. To add two $k \times n$ matrices $\mathbb{A} = [a_{ij}]$ and $\mathbb{B} = [b_{ij}]$, we simply add their corresponding entries $a_{ij}$ and $b_{ij}$ as follows:

$$[a_{ij}] + [b_{ij}] = [a_{ij} + b_{ij}].$$

Hence, the resultant matrix is also a $k \times n$ matrix. Two matrices can be multiplied provided that the number of columns in the first matrix is equal to the number of rows in the second matrix. Multiplying a $k \times n$ matrix $\mathbb{A} = [a_{ij}]$ by an $n \times l$ matrix $\mathbb{B} = [b_{ij}]$, we obtain the product

$$\mathbb{C} = \mathbb{A} \times \mathbb{B} = [c_{ij}].$$

In the resultant $k \times l$ matrix the entry $c_{ij}$ is equal to the inner product of the $i$th row $\mathbb{a}_i$ in $\mathbb{A}$ and the $j$th column $\mathbb{b}_j$ in $\mathbb{B}$; that is,

$$c_{ij} = \mathbb{a}_i \cdot \mathbb{b}_j = \sum_{t=0}^{n-1} a_{it} b_{tj}.$$

Let $\mathbb{G}$ be a $k \times n$ matrix over $GF(2)$. The *transpose* of $\mathbb{G}$, denoted by $\mathbb{G}^T$, is an $n \times k$ matrix whose rows are columns of $\mathbb{G}$ and whose columns are rows of $\mathbb{G}$. A $k \times k$ matrix is called an *identity* matrix if it has 1's on the main diagonal and 0's elsewhere. This matrix is usually denoted by $\mathbb{I}_k$. A *submatrix* of a matrix $\mathbb{G}$ is a matrix that is obtained by striking out given rows or columns of $\mathbb{G}$.

It is straightforward to generalize the concepts and results presented in this section to matrices with entries from $GF(q)$ with $q$ as a power of a prime.

## PROBLEMS

2.1 Construct the group under modulo-6 addition.

2.2 Construct the group under modulo-3 multiplication.

2.3 Let $m$ be a positive integer. If $m$ is not a prime, prove that the set $\{1, 2, \cdots, m-1\}$ is not a group under modulo-$m$ multiplication.

2.4 Construct the prime field $GF(11)$ with modulo-11 addition and multiplication. Find all the primitive elements, and determine the orders of other elements.

2.5 Let $m$ be a positive integer. If $m$ is not prime, prove that the set $\{0, 1, 2, \cdots, m-1\}$ is not a field under modulo-$m$ addition and multiplication.

2.6 Consider the integer group $G = \{0, 1, 2, \cdots, 31\}$ under modulo-32 addition. Show that $H = \{0, 4, 8, 12, 16, 20, 24, 28\}$ forms a subgroup of $G$. Decompose $G$ into cosets with respect to $H$ (or modulo $H$).

2.7 Let $\lambda$ be the characteristic of a Galois field $GF(q)$. Let 1 be the unit element of $GF(q)$. Show that the sums

$$1, \sum_{i=1}^{2} 1, \sum_{i=1}^{3} 1, \cdots, \sum_{i=1}^{\lambda-1} 1, \sum_{i=1}^{\lambda} 1 = 0$$

form a subfield of $GF(q)$.

2.8 Prove that every finite field has a primitive element.

**2.9** Solve the following simultaneous equations of $X, Y, Z$, and $W$ with modulo-2 arithmetic:

$$\begin{aligned} X + Y \quad\quad + W &= 1, \\ X \quad + Z + W &= 0, \\ X + Y + Z + W &= 1, \\ Y + Z + W &= 0. \end{aligned}$$

**2.10** Show that $X^5 + X^3 + 1$ is irreducible over $GF(2)$.

**2.11** Let $f(X)$ be a polynomial of degree $n$ over $GF(2)$. The reciprocal of $f(X)$ is defined as

$$f^*(X) = X^n f\left(\frac{1}{X}\right).$$

**a.** Prove that $f^*(X)$ is irreducible over $GF(2)$ if and only if $f(X)$ is irreducible over $GF(2)$.

**b.** Prove that $f^*(X)$ is primitive if and only if $f(X)$ is primitive.

**2.12** Find all the irreducible polynomials of degree 5 over $GF(2)$.

**2.13** Construct a table for $GF(2^3)$ based on the primitive polynomial $p(X) = 1 + X + X^3$. Display the power, polynomial, and vector representations of each element. Determine the order of each element.

**2.14** Construct a table for $GF(2^5)$ based on the primitive polynomial $p(X) = 1 + X^2 + X^5$. Let $\alpha$ be a primitive element of $GF(2^5)$. Find the minimal polynomials of $\alpha^3$ and $\alpha^7$.

**2.15** Let $\beta$ be an element in $GF(2^m)$. Let $e$ be the smallest nonnegative integer such that $\beta^{2^e} = \beta$. Prove that $\beta^2, \beta^{2^2}, \cdots, \beta^{2^{e-1}}$, are all the distinct conjugates of $\beta$.

**2.16** Prove Theorem 2.21.

**2.17** Let $\alpha$ be a primitive element in $GF(2^4)$. Use Table 2.8 to find the roots of $f(X) = X^3 + \alpha^6 X^2 + \alpha^9 X + \alpha^9$.

**2.18** Let $\alpha$ be a primitive element in $GF(2^4)$. Divide the polynomial $f(X) = \alpha^3 X^7 + \alpha X^6 + \alpha^7 X^4 + \alpha^2 X^2 + \alpha^{11} X + 1$ over $GF(2^4)$ by the polynomial $g(X) = X^4 + \alpha^3 X^2 + \alpha^5 X + 1$ over $GF(2^4)$. Find the quotient and the remainder (use Table 2.8).

**2.19** Let $\alpha$ be a primitive element in $GF(2^4)$. Use Table 2.8 to solve the following simultaneous equations for $X, Y$, and $Z$:

$$\begin{aligned} X \quad + \alpha^5 Y + \quad Z \quad &= \alpha^7, \\ X \quad + \alpha Y \quad + \alpha^7 Z &= \alpha^9, \\ \alpha^2 X + \quad Y \quad + \alpha^6 Z &= \alpha. \end{aligned}$$

**2.20** Let $V$ be a vector space over a field $F$. For any element $c$ in $F$, prove that $c \cdot \mathbf{0} = \mathbf{0}$.

**2.21** Let $V$ be a vector space over a field $F$. Prove that, for any $c$ in $F$ and any $\mathbf{v}$ in $V$, $(-c) \cdot \mathbf{v} = c \cdot (-\mathbf{v}) = -(c \cdot \mathbf{v})$.

**2.22** Let $S$ be a subset of the vector space $V_n$ of all $n$-tuples over $GF(2)$. Prove that $S$ is a subspace of $V_n$ if for any $\mathbf{u}$ and $\mathbf{v}$ in $S$, $\mathbf{u} + \mathbf{v}$ is in $S$.

**2.23** Prove that the set of polynomials over $GF(2)$ with degree $n - 1$ or less forms a vector space $GF(2)$ with dimension $n$.

**2.24** Prove that $GF(2^m)$ is a vector space over $GF(2)$.

**2.25** Construct the vector space $V_5$ of all 5-tuples over $GF(2)$. Find a three-dimensional subspace and determine its null space.

2.26 Given the matrices

$$\mathbb{G} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}, \quad \mathbb{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix},$$

show that the row space of $\mathbb{G}$ is the null space of $\mathbb{H}$, and vice versa.

2.27 Let $S_1$ and $S_2$ be two subspaces of a vector $V$. Show that the intersection of $S_1$ and $S_2$ is also a subspace in $V$.

2.28 Construct the vector space of all 3-tuples over $GF(3)$. Form a two-dimensional subspace and its dual space.

## BIBLIOGRAPHY


1. G. Birkhoff and S. Maclane, *A Survey of Modern Algebra*, Macmillan, New York, 1953.

2. R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Ginn & Co., Boston, 1937.

3. A. Clark, *Elements of Abstract Algebra*, Dover, New York, 1984.

4. R. A. Dean, *Classical Abstract Algebra*, Harper & Row, New York, 1990.

5. T. W. Hungerford, *Abstract Algebra: An Introduction*, 2d ed., Saunders College Publishing, New York, 1997.

6. R. W. Marsh, *Table of Irreducible Polynomials over* GF*(2) through Degree 19*, NSA, Washington, D.C., 1957.

7. J. E. Maxfield and M. W. Maxfield, *Abstract Algebra and Solution by Radicals*, Dover, New York, 1992.

8. W. W. Peterson, *Error-Correcting Codes*, MIT Press, Cambridge, 1961.

9. B. L. Van der Waerden, *Modern Algebra*, Vols. 1 and 2, Ungar, New York, 1949.