CHAPTER 2

Introduction to Algebra

GROUPS

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.

THEOREM 2.2 The inverse of a group element is unique.

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:

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

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*.

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

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*.

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

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 $*$.

ii. 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

$$0 \boxplus H = \{0, 4, 8, 12\},$$

$$1 \boxplus H = \{1, 5, 9, 13\},$$

$$2 \boxplus H = \{2, 6, 10, 14\}.$$

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

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.

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

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.

FIELDS

DEFINITION 2.3 Let F be a set of elements on which two binary operations, called addition "$+$" and multiplication "$\cdot$", are defined. The set F together with the two binary operations $+$ and $\cdot$ 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 $\cdot$. 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, $a \cdot 0 = 0 \cdot a = 0$.

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

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

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.

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 $GF(2)$.

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

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.

Characteristic of a field

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

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

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

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

This equality implies that $\sum_{i=1}^{n-m} 1 = 0$. Therefore, there must exist a *smallest positive integer* λ such that $\sum_{i=1}^{\lambda} 1 = 0$. This integer λ 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 λ of a finite field is prime.

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 λ distinct elements in $GF(q)$. In fact, this set of sums itself is a field of λ 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 λ contains a subfield of λ elements. It can be proved that if $q \neq \lambda$, then q is a power of λ.

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 $GF(q)$.

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 $a^{q-1} = 1$.

THEOREM 2.9 Let a be a nonzero element in a finite field $GF(q)$. Let n be the order of a. Then n divides $q - 1$.

In a finite field $GF(q)$, a nonzero element a is said to be *primitive* if the order of a is $q-1$. Therefore, the powers of a primitive element generate all the nonzero elements of $GF(q)$. Every finite field has a primitive element (see Problem 2.8).

Consider the prime field $GF(7)$ illustrated by Tables 2.5 and 2.6. The characteristic of this field is 7. If we take the powers of the integer 3 in $GF(7)$ using the multiplication table, we obtain

$$3^1 = 3, \quad 3^2 = 3 \cdot 3 = 2, \quad 3^3 = 3 \cdot 3^2 = 6,$$

$$3^4 = 3 \cdot 3^3 = 4, \quad 3^5 = 3 \cdot 3^4 = 5, \quad 3^6 = 3 \cdot 3^5 = 1.$$

Therefore, the order of the integer 3 is 6, and the integer 3 is a primitive element of $GF(7)$. The powers of the integer 4 in $GF(7)$ are

$$4^1 = 4, \quad 4^2 = 4 \cdot 4 = 2, \quad 4^3 = 4 \cdot 4^2 = 1.$$

Clearly, the order of the integer 4 is 3, which is a factor of 6.

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 v in V, $0 \cdot \mathrm{v} = \mathbb{0}$.

Property II For any scalar c in F, $c \cdot \mathbb{0} = \mathbb{0}$. (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 $\mathbb{u} = (u_0, u_1, \cdots, u_{n-1})$ and $\mathbb{v} = (v_0, v_1, \cdots, v_{n-1})$ in V_n,

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

where $u_i + v_i$ is carried out in modulo-2 addition. Clearly, $\mathbb{u} + \mathbb{v}$ 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 $\mathbb{0} = (0, 0, \cdots, 0)$ is the additive identity. For any $\mathbb{v}$ in V_n,

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

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

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

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

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:

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

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

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

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

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.

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 $(0\,0\,1\,1\,1)$ and $(1\,1\,1\,0\,1)$ are

$$0 \cdot (0\,0\,1\,1\,1) + 0 \cdot (1\,1\,1\,0\,1) = (0\,0\,0\,0\,0),$$

$$0 \cdot (0\,0\,1\,1\,1) + 1 \cdot (1\,1\,1\,0\,1) = (1\,1\,1\,0\,1),$$

$$1 \cdot (0\,0\,1\,1\,1) + 0 \cdot (1\,1\,1\,0\,1) = (0\,0\,1\,1\,1),$$

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

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

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

A set of vectors $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ is said to be *linearly independent* if it is not linearly dependent. That is, if $\mathbb{v}_1, \mathbb{v}_2, \cdots, \mathbb{v}_k$ are linearly independent, then

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

unless $a_1 = a_2 = \cdots = a_k = 0$.

EXAMPLE 2.15

The vectors (1 0 1 1 0), (0 1 0 0 1), and (1 1 1 1 1) are linearly dependent, since

$$1 \cdot (1\,0\,1\,1\,0) + 1 \cdot (0\,1\,0\,0\,1) + 1 \cdot (1\,1\,1\,1\,1) = (0\,0\,0\,0\,0);$$

however, (1 0 1 1 0), (0 1 0 0 1), and (1 1 0 1 1) are linearly independent. All eight linear combinations of these three vectors are given here:

$$0 \cdot (1\,0\,1\,1\,0) + 0 \cdot (0\,1\,0\,0\,1) + 0 \cdot (1\,1\,0\,1\,1) = (0\,0\,0\,0\,0),$$

$$0 \cdot (1\,0\,1\,1\,0) + 0 \cdot (0\,1\,0\,0\,1) + 1 \cdot (1\,1\,0\,1\,1) = (1\,1\,0\,1\,1),$$

$$0 \cdot (1\,0\,1\,1\,0) + 1 \cdot (0\,1\,0\,0\,1) + 0 \cdot (1\,1\,0\,1\,1) = (0\,1\,0\,0\,1),$$

$$0 \cdot (1\,0\,1\,1\,0) + 1 \cdot (0\,1\,0\,0\,1) + 1 \cdot (1\,1\,0\,1\,1) = (1\,0\,0\,1\,0),$$

$$1 \cdot (1\,0\,1\,1\,0) + 0 \cdot (0\,1\,0\,0\,1) + 0 \cdot (1\,1\,0\,1\,1) = (1\,0\,1\,1\,0),$$

$$1 \cdot (1\,0\,1\,1\,0) + 0 \cdot (0\,1\,0\,0\,1) + 1 \cdot (1\,1\,0\,1\,1) = (0\,1\,1\,0\,1),$$

$$1 \cdot (1\,0\,1\,1\,0) + 1 \cdot (0\,1\,0\,0\,1) + 0 \cdot (1\,1\,0\,1\,1) = (1\,1\,1\,1\,1),$$

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

A set of vectors is said to *span* a vector space V if every vector in V is a linear combination of the vectors in the set. In any vector space or subspace there exists at least one set B of linearly independent vectors that span the space. This set is called a *basis* (or *base*) of the vector space. The number of vectors in a basis of a vector space is called the *dimension* of the vector space. (Note that the number of vectors in any two bases are the same.)

Consider the vector space V_n of all n-tuples over $GF(2)$. Let us form the following n n-tuples:

$$\begin{aligned}
\mathbb{e}_0 &= (1,\ 0,\ 0,\ 0,\ \cdots,\ 0,\ 0),\\
\mathbb{e}_1 &= (0,\ 1,\ 0,\ 0,\ \cdots,\ 0,\ 0),\\
&\vdots\\
\mathbb{e}_{n-1} &= (0,\ 0,\ 0,\ 0,\ \cdots,\ 0,\ 1),
\end{aligned}$$

where the n-tuple $\mathbb{e}_i$ has only one nonzero component at the ith position. Then, every n-tuple $(a_0, a_1, a_2, \cdots, a_{n-1})$ in V_n can be expressed as a linear combination of $\mathbb{e}_0, \mathbb{e}_1, \cdots, \mathbb{e}_{n-1}$ as follows:

$$(a_0, a_1, a_2, \cdots, a_{n-1}) = a_0\mathbb{e}_0 + a_1\mathbb{e}_1 + a_2\mathbb{e}_2 + \cdots + a_{n-1}\mathbb{e}_{n-1}.$$

From the preceding equation we also see that $\mathbf{e}_0, \mathbf{e}_1, \cdots, \mathbf{e}_{n-1}$ are linearly independent. Hence, they form a basis for V_n, and the dimension of V_n is n. If $k < n$ and $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ are k linearly independent vectors in V_n, then all the linear combinations of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$ of the form

$$\mathbf{u} = c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_k\mathbf{v}_k$$

form a k-dimensional subspace S of V_n. Because each c_i has two possible values, 0 or 1, there are 2^k possible distinct linear combinations of $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$. Thus, S consists of 2^k vectors and is a k-dimensional subspace of V_n.

We define the *inner product* (or *dot product*) of $\mathbf{u}$ and $\mathbf{v}$ as

$$\mathbf{u} \cdot \mathbf{v} = u_0 \cdot v_0 + u_1 \cdot v_1 + \cdots + u_{n-1} \cdot v_{n-1}, \tag{2.29}$$

where $u_i \cdot v_i$ and $u_i \cdot v_i + u_{i+1} \cdot v_{i+1}$ are carried out in modulo-2 multiplication and addition. Hence, the inner product $\mathbf{u} \cdot \mathbf{v}$ is a scalar in $GF(2)$. If $\mathbf{u} \cdot \mathbf{v} = 0$, $\mathbf{u}$ and $\mathbf{v}$ are said to be *orthogonal* to each other. The inner product has the following properties:

i. $\mathbf{u} \cdot \mathbf{v} = \mathbf{v} \cdot \mathbf{u}$.

ii. $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w}$.

iii. $(a\mathbf{u}) \cdot \mathbf{v} = a(\mathbf{u} \cdot \mathbf{v})$.

(The concept of inner product can be generalized to any Galois field.)

Let S be a k-dimensional subspace of V_n and let S_d be the set of vectors in V_n such that for any $\mathbf{u}$ in S and $\mathbf{v}$ in S_d, $\mathbf{u} \cdot \mathbf{v} = 0$. The set S_d contains at least the all-zero n-tuple $\mathbf{0} = (0, 0, \cdots, 0)$, since for any $\mathbf{u}$ in S, $\mathbf{0} \cdot \mathbf{u} = 0$. Thus, S_d is nonempty. For any element a in $GF(2)$ and any $\mathbf{v}$ in S_d,

$$a \cdot \mathbf{v} = \begin{cases} \mathbf{0} & \text{if } a = 0, \\ \mathbf{v} & \text{if } a = 1. \end{cases}$$

Therefore, $a \cdot \mathbf{v}$ is also in S_d. Let $\mathbf{v}$ and $\mathbf{w}$ be any two vectors in S_d. For any vector $\mathbf{u}$ in S, $\mathbf{u} \cdot (\mathbf{v} + \mathbf{w}) = \mathbf{u} \cdot \mathbf{v} + \mathbf{u} \cdot \mathbf{w} = 0 + 0 = 0$. This says that if $\mathbf{v}$ and $\mathbf{w}$ are orthogonal to $\mathbf{u}$, the vector sum $\mathbf{v} + \mathbf{w}$ is also orthogonal to $\mathbf{u}$. Consequently, $\mathbf{v} + \mathbf{w}$ is a vector in S_d. It follows from Theorem 2.22 that S_d is also a subspace of V_n. This subspace S_d is called the *null* (or *dual*) *space* of S. Conversely, S is also the null space of S_d. The dimension of S_d is given by Theorem 2.24, whose proof is omitted here [1].

THEOREM 2.24 Let S be a k-dimensional subspace of the vector space V_n of all n-tuples over $GF(2)$. The dimension of its null space S_d is $n - k$. In other words, $\dim(S) + \dim(S_d) = n$.

EXAMPLE 2.16

Consider the vector space V_5 of all 5-tuples over $GF(2)$ given by Example 2.12. The following eight vectors form a three-dimensional subspace S of V_5:

$$(00000), \quad (11100), \quad (01010), \quad (10001),$$
$$(10110), \quad (01101), \quad (11011), \quad (00111).$$

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

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 $GF(2)$.

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

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 3×6 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 $\mathbf{g}_i$ in $\mathbb{G}$ and any $\mathbf{h}_j$ in $\mathbb{H}$, $\mathbf{g}_i \cdot \mathbf{h}_j = 0$. The row space of $\mathbb{G}$ is the null space of $\mathbb{H}$, and vice versa.

EXAMPLE 2.18

Consider the following 3×6 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 ith row $\mathbb{a}_i$ in $\mathbb{A}$ and the jth 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.