## 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:

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

**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 $f(X) = \alpha^3X^7 + \alpha X^6 + \alpha^7X^4 + \alpha^2X^2 + \alpha^{11}X + 1$ over $GF(2^4)$ by the polynomial $g(X) = X^4 + \alpha^3X^2 + \alpha^5X + 1$ 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 $Z$:

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

**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-dimensiona subspace and determine its null space.

**2.26** Given the matrices

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

show that the row space of $\mathbf{G}$ is the null space of $\mathbf{H}$, 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.