Chapter 2

2.3 Since m is not a prime, it can be factored as the product of two integers a and b,

$$m = a \cdot b$$

with $1 < a, b < m$. It is clear that both a and b are in the set $\{1, 2, \cdots, m-1\}$. It follows from the definition of modulo-m multiplication that

$$a \boxdot b = 0.$$

Since 0 is not an element in the set $\{1, 2, \cdots, m-1\}$, the set is not closed under the modulo-m multiplication and hence can not be a group.

2.5 It follows from Problem 2.3 that, if m is not a prime, the set $\{1, 2, \cdots, m-1\}$ can not be a group under the modulo-m multiplication. Consequently, the set $\{0, 1, 2, \cdots, m-1\}$ can not be a field under the modulo-m addition and multiplication.

2.7 First we note that the set of sums of unit element contains the zero element 0. For any $1 \leq \ell < \lambda$,

$$\sum_{i=1}^{\ell} 1 + \sum_{i=1}^{\lambda-\ell} 1 = \sum_{i=1}^{\lambda} 1 = 0.$$

Hence every sum has an inverse with respect to the addition operation of the field GF(q). Since the sums are elements in GF(q), they must satisfy the associative and commutative laws with respect to the addition operation of GF(q). Therefore, the sums form a commutative group under the addition of GF(q).

Next we note that the sums contain the unit element 1 of GF(q). For each nonzero sum

$$\sum_{i=1}^{\ell} 1$$

with $1 \leq \ell < \lambda$, we want to show it has a multiplicative inverse with respect to the multiplication operation of GF(q). Since λ is prime, ℓ and λ are relatively prime and there exist two integers a and b such that

$$a \cdot \ell + b \cdot \lambda = 1, \tag{1}$$

where a and λ are also relatively prime. Dividing a by λ, we obtain

$$a = k\lambda + r \quad with \quad 0 \leq r < \lambda. \tag{2}$$

Since a and λ are relatively prime, $r \neq 0$. Hence

$$1 \leq r < \lambda$$

Combining (1) and (2), we have

$$\ell \cdot r = -(b + k\ell) \cdot \lambda + 1$$

Consider

$$\begin{aligned} \sum_{i=1}^{\ell} 1 \cdot \sum_{i=1}^{r} 1 &= \sum_{i=1}^{\ell \cdot r} 1 = \sum_{i=1}^{-(b+k\ell)\cdot\lambda} +1 \\ &= (\sum_{i=1}^{\lambda} 1)(\sum_{i=1}^{-(b+k\ell)} 1) + 1 \\ &= 0 + 1 = 1. \end{aligned}$$

Hence, every nonzero sum has an inverse with respect to the multiplication operation of GF(q). Since the nonzero sums are elements of GF(q), they obey the associative and commutative laws with respect to the multiplication of GF(q). Also the sums satisfy the distributive law. As a result, the sums form a field, a subfield of GF(q).

2.8 Consider the finite field GF(q). Let n be the maximum order of the nonzero elements of GF(q) and let α be an element of order n. It follows from Theorem 2.9 that n divides $q - 1$, i.e.

$$q - 1 = k \cdot n.$$

Thus $n \leq q - 1$. Let β be any other nonzero element in GF(q) and let e be the order of β.

Suppose that e does not divide n. Let (n, e) be the greatest common factor of n and e. Then $e/(n, e)$ and n are relatively prime. Consider the element

$$\beta^{(n,e)}$$

This element has order $e/(n, e)$. The element

$$\alpha\beta^{(n,e)}$$

has order $ne/(n, e)$ which is greater than n. This contradicts the fact that n is the maximum order of nonzero elements in GF(q). Hence e must divide n. Therefore, the order of each nonzero element of GF(q) is a factor of n. This implies that each nonzero element of GF(q) is a root of the polynomial

$$X^n - 1.$$

Consequently, $q - 1 \leq n$. Since $n \leq q - 1$ (by Theorem 2.9), we must have

$$n = q - 1.$$

Thus the maximum order of nonzero elements in GF(q) is q-1. The elements of order $q - 1$ are then primitive elements.

2.11 (a) Suppose that $f(X)$ is irreducible but its reciprocal $f^*(X)$ is not. Then

$$f^*(X) = a(X) \cdot b(X)$$

where the degrees of $a(X)$ and $b(X)$ are nonzero. Let k and m be the degrees of $a(X)$ and $b(X)$ respectivly. Clearly, $k + m = n$. Since the reciprocal of $f^*(X)$ is $f(X)$,

$$f(X) = X^n f^*(\frac{1}{X}) = X^k a(\frac{1}{X}) \cdot X^m b(\frac{1}{X}).$$

This says that $f(X)$ is not irreducible and is a contradiction to the hypothesis. Hence $f^*(X)$ must be irreducible. Similarly, we can prove that if $f^*(X)$ is irreducible, $f(X)$ is also irreducible. Consequently, $f^*(X)$ is irreducible if and only if $f(X)$ is irreducible.

(b) Suppose that $f(X)$ is primitive but $f^*(X)$ is not. Then there exists a positive integer k less than $2^n - 1$ such that $f^*(X)$ divides $X^k + 1$. Let

$$X^k + 1 = f^*(X)q(X).$$

Taking the reciprocals of both sides of the above equality, we have

$$\begin{aligned} X^k + 1 &= X^k f^*(\frac{1}{X})q(\frac{1}{X}) \\ &= X^n f^*(\frac{1}{X}) \cdot X^{k-n} q(\frac{1}{X}) \\ &= f(X) \cdot X^{k-n} q(\frac{1}{X}). \end{aligned}$$

This implies that $f(X)$ divides $X^k + 1$ with $k < 2^n - 1$. This is a contradiction to the hypothesis that $f(X)$ is primitive. Hence$f^*(X)$ must be also primitive. Similarly, if $f^*(X)$ is primitive, $f(X)$ must also be primitive. Consequently $f^*(X)$ is primitive if and only if $f(X)$ is primitive.

2.15 We only need to show that $\beta, \beta^2, \cdots, \beta^{2^{e-1}}$ are distinct. Suppose that

$$\beta^{2^i} = \beta^{2^j}$$

for $0 \leq i, j < e$ and $i < j$. Then,

$$(\beta^{2^{j-i}-1})^{2^i} = 1.$$

Since the order β is a factor of $2^m - 1$, it must be odd. For $(\beta^{2^{j-i}-1})^{2^i} = 1$, we must have

$$\beta^{2^{j-i}-1} = 1.$$

Since both i and j are less than e, $j - i < e$. This is contradiction to the fact that the e is the smallest nonnegative integer such that

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

Hence $\beta^{2^i} \neq \beta^{2^j}$ for $0 \leq i, j < e$.

2.16 Let n' be the order of β^{2^i}. Then

$$(\beta^{2^i})^{n'} = 1$$

Hence

$$(\beta^{n'})^{2^i} = 1. \quad (1)$$

Since the order n of β is odd, n and 2^i are relatively prime. From(1), we see that n divides n' and

$$n' = kn. \quad (2)$$

Now consider

$$(\beta^{2^i})^n = (\beta^n)^{2^i} = 1$$

This implies that n' (the order of β^{2^i}) divides n. Hence

$$n = \ell n' \quad (3)$$

From (2) and (3), we conclude that

$$n' = n.$$

2.20 Note that $c \cdot \mathbf{v} = c \cdot (\mathbf{0} + \mathbf{v}) = c \cdot \mathbf{0} + c \cdot \mathbf{v}$. Adding $-(c \cdot \mathbf{v})$ to both sides of the above equality, we have

$$\begin{aligned} c \cdot \mathbf{v} + [-(c \cdot \mathbf{v})] &= c \cdot \mathbf{0} + c \cdot \mathbf{v} + [-(c \cdot \mathbf{v})] \\ \mathbf{0} &= c \cdot \mathbf{0} + \mathbf{0}. \end{aligned}$$

Since $\mathbf{0}$ is the additive identity of the vector space, we then have

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

2.21 Note that $0 \cdot \mathbf{v} = \mathbf{0}$. Then for any c in F,

$$(-c + c) \cdot \mathbf{v} = \mathbf{0}$$

$$(-c) \cdot \mathbf{v} + c \cdot \mathbf{v} = \mathbf{0}.$$

Hence $(-c) \cdot \mathbf{v}$ is the additive inverse of $c \cdot \mathbf{v}$, i.e.

$$-(c \cdot \mathbf{v}) = (-c) \cdot \mathbf{v} \quad (1)$$

Since $c \cdot \mathbf{0} = \mathbf{0}$ (problem 2.20),

$$c \cdot (-\mathbf{v} + \mathbf{v}) = \mathbf{0}$$

$$c \cdot (-\mathbf{v}) + c \cdot \mathbf{v} = \mathbf{0}.$$

Hence $c \cdot (-\mathbf{v})$ is the additive inverse of $c \cdot \mathbf{v}$, i.e.

$$-(c \cdot \mathbf{v}) = c \cdot (-\mathbf{v}) \quad (2)$$

From (1) and (2), we obtain

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

2.22 By Theorem 2.22, S is a subspace if (i) for any $\mathbf{u}$ and $\mathbf{v}$ in S, $\mathbf{u} + \mathbf{v}$ is in S and (ii) for any c in F and $\mathbf{u}$ in S, $c \cdot \mathbf{u}$ is in S. The first condition is now given, we only have to show that the second condition is implied by the first condition for $F = GF(2)$. Let $\mathbf{u}$ be any element in S. It follows from the given condition that

$$\mathbf{u} + \mathbf{u} = \mathbf{0}$$

is also in S. Let c be an element in GF(2). Then, for any $\mathbf{u}$ in S,

$$c \cdot \mathbf{u} = \begin{cases} \mathbf{0} & for \quad c = 0 \\ \mathbf{u} & for \quad c = 1 \end{cases}$$

Clearly $c \cdot \mathbf{u}$ is also in S. Hence S is a subspace.

2.24 If the elements of GF(2^m) are represented by m-tuples over GF(2), the proof that GF(2^m) is a vector space over GF(2) is then straight-forward.

2.27 Let $\mathbf{u}$ and $\mathbf{v}$ be any two elements in $S_1 \cap S_2$. It is clear the $\mathbf{u}$ and $\mathbf{v}$ are elements in S_1, and $\mathbf{u}$ and $\mathbf{v}$ are elements in S_2. Since S_1 and S_2 are subspaces,

$$\mathbf{u} + \mathbf{v} \in S_1$$

and

$$\mathbf{u} + \mathbf{v} \in S_2.$$

Hence,$\mathbf{u} + \mathbf{v}$ is in $S_1 \cap S_2$. Now let $\mathbf{x}$ be any vector in $S_1 \cap S_2$. Then $\mathbf{x} \in S_1$, and $\mathbf{x} \in S_2$. Again, since S_1 and S_2 are subspaces, for any c in the field F, $c \cdot \mathbf{x}$ is in S_1 and also in S_2. Hence $c \cdot \mathbf{v}$ is in the intersection, $S_1 \cap S_2$. It follows from Theorem 2.22 that $S_1 \cap S_2$ is a subspace.