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

group condition: ① closure ② associativity ③ identity ④ invertibility

proof: If m is not a prime, suggest m is a product of a and b

$$m = a \cdot b \qquad 1 < a, b < m$$

and a, b are in set $\{1, 2, \ldots, m-1\}$

However, since

$$a \cdot b = m \equiv 0 \pmod m$$

and 0 is not in set $\{1, 2, \ldots, m-1\}$,

the set is not closed in modulo-2 multiplication

$\therefore$ This set can not be a group

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

proof: If m is not a prime, suggest m is a product of a and b

$$m = a \cdot b \qquad 1 < a, b < m$$

and a, b are in set $\{1, 2, \ldots, m-1\}$

However, since

$$a \cdot b = m \equiv 0 \pmod m$$

which is contradicted to the field property II

$$\Rightarrow a \cdot b \neq 0 \text{ if } a \neq 0 \text{ and } b \neq 0$$

$\therefore$ This set can not be a field. (not closed)

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

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

form a subfield of $GF(q)$.

proof: If λ is the characteristic of $GF(q)$, λ is the smallest positive integer that makes $\sum_{i=1}^{\lambda} 1 = 0$

Suppose $1 < k < m < \lambda$, and $\sum_{i=1}^{k} 1 = \sum_{i=1}^{m} 1$

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

However, this contradicts to the definition of characteristic

Therefore the sums $1, \sum_{i=1}^{2} 1, \sum_{i=1}^{3} 1, \ldots, \sum_{i=1}^{\lambda-1}, \sum_{i=1}^{\lambda} = 0$ are λ distinct elements in $GF(q)$ under 2 operation $(+, \times)$

$\because$ $GF(\lambda)$ is a subset of $GF(q)$

$\therefore$ $GF(\lambda)$ is a subfield of $GF(q)$