Q1)

- Any $a \in F$,
  $e_1 \times a = (e_2 - e_2) \times a = a \times e_2 - a \times e_2$
  $= e_1$
  $(e_2 - e_2 = e_1$ and $(a \times e_2) + (-a \times e_2) = e_1)$

- Already Done
- For all $a \in F$, $e_1 \times a = e_1$.

Case One, $a \neq e_1$
$ab = 0 \Rightarrow a^{-1} \times (ab) = a^{-1} \times e_1$
$\Rightarrow (a^{-1} \times a) \times b = e_1$
$\Rightarrow e_2 \times b = e_1$
$\Rightarrow b = e_1$

Case Two, $b \neq e_1$
$ab = e_1 \Rightarrow b^{-1} (ab) \times b^{-1} = e_1 \times b^{-1}$
$a \times (b \times b^{-1}) = e_1 \times b^{-1}$
$a \times e_2 = e_1$
$a = e_1$

Case Three, $a = e_1 = b$,
$ab = e_1$: We are done!

- $a(-b) = ?$
  For all $a \in F$,
  $-a = -e_2 \times a$

$a + (-e_2 \times a)$

- $(-a) = -1 \times a$

$a + (-1 \times a) = a(1 + (-1)) = a \times 0 = 0$

Thus, $(-a) = -1 \times a$.

1. Now, $(a)(-b) = a \times (-1 \times b)$

$= a \times -1 \times b = (a \times -1) \times b = (-1 \times a) \times b$

$= (-a)(b)$

2. $(a)(-b) = a \times (-1 \times b) = -1 \times a \times b$

$= -1 \times (a \times b) = -1 \times (ab) = -(ab)$.

The additive inverse of an element is equal to negative one times the element.

Q2) Proof that 0^{-1} does not exist:

Assume that $x \in F$ such that:

1. $x \times e_1 = e_2 = e_1 \times x$
2. Note that $e_1^{-1} \neq e_1$ since $e_1 \times e_1 = e_1$.

Thus,

$x^{-1} \times (x \times e_1) = x^{-1} \times e_2$

$(x^{-1} \times x) \times e_1 = x^{-1} \times e_2$

$e_2 \times e_1 = x^{-1} \times e_2$

3. $e_1 = x^{-1} \times e_2$

Now since $x^{-1} \neq e_1$ and $e_2 \neq e_1$, $x^{-1} \times e_2 \neq e_1$. Thus, line 3 is a contradiction.

Also, $e_1 = x^{-1} \times e_2 \Rightarrow \boxed{e_1 = x^{-1}}$. Another contradiction.

Hence, $ab = 0 \Rightarrow a = 0$ or $b = 0$ implies that 0^{-1} does not exist.

Q3)

$\Rightarrow$ Forward conditions

We have to prove that if S is a finite field, then $ab = 0$ means that either $a = 0$ or $b = 0$.

I Case One: Assume that $a \neq 0$.

By axiom (M2), a^{-1} exists.

- $ab = 0$
- $a^{-1}(ab) = a^{-1} \times 0$
- $(a^{-1} \times a)b = a^{-1} \times 0$
- $1 \times b = 0$
- $b = 0$

II Case Two: Assume that $b \neq 0$.

By axiom (M2), b^{-1} exists

- $ab = 0$
- $(ab)b^{-1} = 0 \times b^{-1}$
- $a(b \times b^{-1}) = 0 \times b^{-1}$
- $a \times 1 = 0$
- $a = 0$

III Case Three: Assume that $a = 0$ and $b = 0$. Then we are done!

Q3)

Part 2 : Backward condition.

S is a set that satisfies all of the field axioms except for M2 and has a finite cardinality.

- Theorem: For all $s \in S$, there exist integers m and n such that $m \neq n$ and $s^m = s^n$.

  Proof: Consider the set G_1 such that $G_1 = [s, s^2, s^3, s^4 \cdots]$. Assume that for all $m \neq n$, we have that $s^m \neq s^n$. This would imply that there are infinitely elements in G_1. Since multiplication is closed, $s^n \in S$ for $n \in \mathbb{Z}^+$. This then means that there are infinitely many distinct elements in S, which is a contradiction. Thus, there exist integers $m > n$ and $s^m = s^n$. ∎

- Theorem: For all $s \in S$, there exists an integer n such that $s^n = e_2$ (e_2 = multiplicative identity).

  Proof: From the previous theorem, we know that there exist positive integers $m > n$ such that $s^m = s^n$. Adding $(-s^n)$ on both sides, $s^m - s^n = e_1$, $a^n(a^{m-n} - e_2) = e_1$. Now, by the zero product property, either $a^n = e_1$ or $a^{m-n} = e_2$ (or both).

Case One: If $a^n = e_1$ then that implies that $a = e_1$ (using the zero product property).

Case Two: If $a^{m-n} = e_2$, then that implies that $a \neq e_1$.

Thus for all $a \in S$ st $a \neq e_1$, than we can find an integer such that $a^k = e_2$. Now,

$$a \cdot \underbrace{(a \cdot \cdots \cdot a)}_{k-1 \text{ times}} = e_2 = \underbrace{(a \cdot a \cdots a)}_{k-1 \text{ times}} \cdot a$$

Thus, $a \cdot a^{k-1} = e_2 = a^{k-1} \cdot a$ which means that $a^{-1} = a^{k-1}$.

Q6) F must contain 0 and 1. By A0, (F is closed under addition) we get that ~~F ⊆~~ $\mathbb{N} \subseteq F$ and by A2 (existance of additive inverses), $\mathbb{Z} \subseteq F$. Now, by M2. (existance of multiplicative) inversences, $\frac{1}{n} \in F$ for all $n \in \mathbb{Z}$ $(n \neq 0)$.

By M0 (F is closed under multiplication), $(\frac{1}{n} \times m) \in F$ (for all $m \in \mathbb{Z}$), and thus we get that $\frac{m}{n} \in F$ for all $m, n \in \mathbb{Z}$ and $n \neq 0$. By the definition of $\mathbb{Q}$, $\mathbb{Q} \subseteq F$. (Q.E.D.).

Q7) Let F be a field such that $\mathbb{R} \subsetneq F \subsetneq \mathbb{C}$. Since $\mathbb{R}$ is a proper subset of F, there must exist at least one non-zero real number b such that $(a + bi) \in F$. Now,

For any $c \in \mathbb{R}$, $\frac{c}{b} \in F$ $\left(\frac{c}{b} \in \mathbb{R}\right)$.

Since multiplication is closed in F, (MO)

$$\frac{c}{b} \times (a + bi) = \left(\frac{ac}{b} + ci\right) \in F.$$

Also, $-\frac{ac}{b} \in F$ and since addition is (AO) closed in F,

$$\left(-\frac{ac}{b}\right) + \left(\frac{ac}{b} + ci\right) = ci \in F.$$

Thus for all any real number c, $ci \in F$. Also for any real number a, we have that $a \in F$. Lastly, since addition is closed in F, (AO)

$((a) + (ci)) \in F \Rightarrow (a + bi) \in F$ and thus $\mathbb{C} \subseteq F$. We have shown that:

$\mathbb{R} \subsetneq F \subsetneq \mathbb{C}$ is immpossible since $\mathbb{R} \subsetneq F$ implies that $\mathbb{C} \subseteq F$.

Q9) Given a nonconstant polynomial $p(x)$, and that $p(x) = q(x)r(x)$ for (non-constant) polynomials $q(x)$ and $r(x)$, $\deg(q) < \deg(p)$ and $\deg(r) < \deg(p)$.

- Thus for x and $x+1$, polynomials of degree 1, if they can be writen as a product of two polynomials $q(x)$ and $r(x)$, they would be of 0-degree, meaning they are constant polynomials. This means (by definition 1.7) are ineducible polynomials, (both in $F_2[x]$ and $F_3[x]$).

- $x^2 + x + 1$ is reducible in $F_3[x]$. Note that:
$(x+2)(x+2) = x^2 + 4x + 4 = x^2 + x + 1$
$(4 = 3+1 \equiv 1 \pmod 3$ and $4 \equiv 1 \pmod 3)$.
Note that $(x+2) \in F_3[x]$.

- Since $x^2 + x + 1$ is polynomial of degree 2, if it is reducible polynomial it can be writen as $q(x) = (\alpha_1 x + \beta_1)$ and $r(x) = (\alpha_2 x + \beta_2)$.

$(\alpha_1 x + \beta_1)(\alpha_2 x + \beta_2) = \alpha_1\alpha_2 x^2 + \alpha_1\beta_2 x + \alpha_2\beta_1 x + \beta_1\beta_2$

$\alpha_1\alpha_2 x^2 + x(\alpha_1\beta_2 + \alpha_2\beta_1) + \beta_1\beta_2$

Thus, $\alpha_1\alpha_2 \equiv 1 \pmod 2$

$\alpha_1\beta_2 + \alpha_2\beta_1 \equiv 1 \pmod 2$

$\beta_1\beta_2 \equiv 1 \pmod 2$

$\alpha_1\alpha_2 \equiv 1 \pmod 2 \Rightarrow \alpha_1 \equiv 1 \pmod 2,\ \alpha_2 \equiv 1 \pmod 2$

$\beta_1\beta_2 \equiv 1 \pmod 2 \Rightarrow \beta_1 \equiv 1 \pmod 2,\ \beta_2 \equiv 1 \pmod 2$

$\alpha_1\beta_2 \equiv \alpha_1 \times \beta_2 \equiv 1 \pmod 2$

$\alpha_2\beta_1 \equiv \alpha_2 \times \beta_1 \equiv 1 \pmod 2$

$(\alpha_1\beta_2 + \alpha_2\beta_1) \equiv 1 + 1 \pmod 2$

$(\alpha_1\beta_2 + \alpha_2\beta_1) \equiv 0 \pmod 2$.

Thus, it is impossible to find $\alpha_1, \alpha_2, \beta_1$ and β_2 that satisfy the 3 congruences.

Since $x^2 + x + 1$ cannot be expressed as a product of linear factors, it is irreducible in $F_2[x]$.

Q8) Addition Axioms

- Given $p_1 \in F_p$ and $p_2 \in F_p$, we have: $(p_1 + p_2) \bmod p \in F_p$. (This is because, the remainder after division p can be one of $0, 1, \cdots, p$ which is the set F_p).
- $0 \in F_p$ such that $p_1 + 0 = p_1 = 0 + p_1$ $\Leftrightarrow (p_1 + 0) \bmod p = p_1 \bmod p = (0 + p_1) \bmod p$.
- For $p_1 \in F_p$, define $p_1^{-1,+} = p - p_1$.
  $(p_1^{-1,+} + p_1) = (p - p_1) + p_1 = p$
  $p_1 \equiv 0 \pmod p \Rightarrow p_1^{-1,+} + p_1 = 0$.

Since addition is commutative, it follows that $p_1 + p_1^{-1,+} = 0 \Rightarrow (p_1 + p_1^{-1,+}) \equiv 0 \pmod{p}$.

- Addition is associative
- Multiplication is commutative

II Multiplication Axioms

- Same reason as addition: The remainder when any no is divided by p, it is one of $0, 1, \cdots, p-1$.
- For all $p \geq 2$, $1 \in F_p$.
- For any $q \in F_p$, we have that $\gcd(p, q) = 1$ [Because $q < p$ and p is prime. Thus $p \nmid q$]. Hence, by bezouts theorem, we have integers q' and p' such that $qq' + pp' = 1$. Now, $pp' = 1 - qq' \Rightarrow p \mid 1 - qq' \Rightarrow qq' \equiv 1 \pmod{p}$

Note that,

- Multiplication is commutative and associative.

Note that multiplication is defined by the remainder left after multiplying a and b.
$ab \equiv n \pmod{p}$, where $n \in Z_p$.

Q10) A ternary operation ($\cdot$) on a set A is a function: $\cdot : A \times A \times A \to A$.
Here $A \times A \times A = [(x, y, z) : x, y, z \in A]$.

Q14) As an example, consider $1 + x + x^2 + x^3 \in \mathbb{Q}[x]$.
$1 + x + x^2 + x^3$ is reducible in $\mathbb{Q}[x]$ because $(x^2 + 1)(x + 1) = 1 + x + x^2 + x^3$ and $(x + 1) \in \mathbb{Q}[x]$ and $(x^2 + 1) \in \mathbb{Q}[x]$. The roots of the polynomial are $\pm i$ and -1.
$\mathbb{Q}(\pm i, -1) = \mathbb{Q}(i) = \mathbb{Q}$ field adjoin i which is not equal to $\mathbb{Q}$. Note that $\mathbb{Q}(i) = [a + bi \mid a, b \in \mathbb{Q}]$.

However, this process will not result in a new field if one considers elements of $C[x]$ (C field adjoin x).
This is because of two facts,

1. All the roots of a polynomial in $C[x]$ are in C.
2. Any polynomial in $C[x]$ can be written as $a(x-r_1)(x-r_2)\cdots(x-r_n)$ where $r_1, r_2, \cdots r_n$ are the roots of the polynomial and a is the leading coefficient. By 1 we know that $r_i \in C$, and thus $(x-r_i) \in C[x]$. Hence that means all elements of $C[x]$ are reducible over C, this process will never result in a new field.

Also note that this process will never result in a new field when we consider quadratics over any field.

Consider a polynomial $P(x) = ax^2 + bx + c$ in $F[x]$. We know that $P(x)$ can be written as $(ax - ar_1)(x - r_2)$ or $(x - r_1)(ax - ar_2)$ and in general as $P(x) = a(x - r_1)(x - r_2)$, where r_1 and r_2 are the roots of P.

If $P(x)$ is reducible in F, $(x - r_1)$ and $(x - r_2)$ are in $F[x]$, meaning that $-r_1 \in F$ and $-r_2 \in F$, and by A2, $r_1 \in F$ and $r_2 \in F$. Thus $F(r_1, r_2) = F(r_1) = F(r_2) = F$.

(Scratch work)

Q15) The identity element for this group is 1.

$a \equiv c \pmod{n}$, where $c \in \mathbb{Z}/n\mathbb{Z}$.
$a' \equiv c' \pmod{n}$, where $c' \in \mathbb{Z}/n\mathbb{Z}$.

$aa' \equiv cc' \pmod{n}$

$cc' \equiv 1 \pmod{n}$

- Thus, given that $a \in \mathbb{Z}/n\mathbb{Z}$, we have to find $a' \in \mathbb{Z}/n\mathbb{Z}$ such that $aa' \equiv 1 \pmod{n}$
- Let $\gcd(a, n) = k$, there exist integers a_1 and n_1 such that $aa_1 + nn_1 = k$.

- Let a be such that $\gcd(a, n) = 1$. Then we have integers a_1 and n_1, $aa_1 + nn_1 = 1 \Rightarrow aa_1 = 1 - nn_1 \Rightarrow a_1 \mid 1 - nn_1$ $\Rightarrow n \mid 1 - aa_1 \Rightarrow 1 \equiv aa_1 \pmod{n}$. Thus $a_1 = a'$.

Conjecture: G_1 has $\varphi(n)$ elements. Since $\varphi(n) = n$ when n is prime,

Q16) A dihedral group can be represented by matrices:

- Rotations: $\begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} - (O_\alpha)$

- Reflections: $\begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} - (E_\alpha)$

Here $\alpha = \frac{2\pi k}{n}$, where $0 \leq k \leq n$.

- Consider, $O_\alpha E_\alpha = \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix}$

$$= \begin{bmatrix} \cos^2(\alpha) - \sin^2(\alpha) & 2\cos(\alpha)\sin(\alpha) \\ 2\cos(\alpha)\sin(\alpha) & \cos^2(\alpha) - \sin^2(\alpha) \end{bmatrix}$$

- Consider, $E_\alpha O_\alpha = \begin{bmatrix} \cos(\alpha) & \sin(\alpha) \\ \sin(\alpha) & -\cos(\alpha) \end{bmatrix} \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix}$

$$= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Hence, we can find α such that $O_\alpha E_\alpha \neq E_\alpha O_\alpha$.

This shows that D_n is not abelian.