1. (a) Define the characteristic of a ring $R$. \[2\]
(b) Prove that a ring $R \neq \{0\}$ of positive characteristic with an identity and no zero divisors must have prime characteristic. \[3\]
(c) Let $F$ be a field. Define what it means for a polynomial $p \in F[x]$ to be irreducible over $F$. \[1\]
(d) Find all irreducible polynomials over $\mathbb{F}_2$ of degree 4. \[3\]
(e) State (giving justification) whether the following are fields:
   (i) $\mathbb{F}_2[x]/(x^4 + x + 1)$;
   (ii) $\mathbb{F}_5[x]/(x^4 + x + 1)$. \[3\]
(f) Calculate the multiplicative order of $x + (x^4 + x^3 + x^2 + x + 1)$ in the field $\mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$. \[3\]

2. (a) Define (i) a prime field; (ii) the prime subfield of a field $F$. \[2\]
(b) Prove that the prime subfield of a field $F$ is a prime field. \[2\]
(c) Let \( F, K \) be fields. Let \( \alpha \in F \) be algebraic over \( K \) and let \( g \) be the minimal polynomial of \( \alpha \) over \( K \). Prove that \( K(\alpha) \) is isomorphic to \( K[x]/(g) \). [4]

(d) Consider the irreducible polynomials \( f(x) = x^2 + 1 \) and \( g(x) = x^2 - x - 1 \) in \( \mathbb{F}_3[x] \).

(i) Let \( L = \mathbb{F}_3[x]/(f) \). Show that \( L \) is the splitting field for \( f \) over \( \mathbb{F}_3 \).

(ii) Let \( \alpha \in L \) be a root of \( f \). By considering \( \alpha - 1 \) (or otherwise) show that \( L \) is also a splitting field for \( g \) over \( \mathbb{F}_3 \). [5]

(e) State in full (without proof) the theorem asserting the ‘Existence and Uniqueness of Finite Fields’. [2]

3. (a) Define a **primitive element** of a finite field \( \mathbb{F}_q \). [1]

(b) (i) How many primitive elements does \( \mathbb{F}_4 \) contain?

(ii) Expressing \( \mathbb{F}_4 \) as \( \mathbb{F}_2(\theta) \) for a suitable \( \theta \), list the primitive element(s) of \( \mathbb{F}_4 \). [2]

Let \( K \) be a field of characteristic \( p \), and \( n \in \mathbb{N} \) with \( p \nmid n \).

(c) Define the **\( n \)th cyclotomic field** \( K^{(n)} \) and a **\( n \)th root of unity** over \( K \). [2]

As usual, let

\[
Q_n(x) = \prod_{s=1 \atop (s,n)=1}^{n} (x - \zeta^s)
\]

where \( \zeta \) is a primitive \( n \)th root of unity over \( K \).

(d) Prove

(i) \( x^n - 1 = \prod_{d|n} Q_d(x) \);

(ii) \( Q_n(x) = \prod_{d|n} (x^d - 1)^{\mu(n/d)} \), where \( \mu \) is the Moebius function.

(You may assert, without proof, the Moebius Inversion Formula). [4]

(e) Using the fact that \( \mathbb{F}_8 \) is the 7th cyclotomic field over \( \mathbb{F}_2 \), find a primitive element of \( \mathbb{F}_8 \) and express \( \mathbb{F}_8 \) in terms of this primitive element. [4]

(f) If \( d|n \) with \( 1 \leq d \leq n \), prove that \( Q_n(x) \) divides \( \frac{x^n - 1}{x^d - 1} \) whenever \( Q_n(x) \) is defined. [2]

4. (a) Prove that if \( F \) is a finite field containing a subfield \( K \) with \( q \) elements, then \( F \) has \( q^m \) elements where \( m = [F : K] \). [3]

(b) Define the **conjugates** of \( \alpha \in \mathbb{F}_{q^m} \) with respect to \( \mathbb{F}_q \). [1]
(c) Let \( \alpha \in \mathbb{F}_{16} \) be a root of \( f(x) = x^4 + x + 1 \in \mathbb{F}_2[x] \). Calculate the conjugates of \( \alpha \) with respect to (i) \( \mathbb{F}_2 \) (ii) \( \mathbb{F}_4 \). [3]

(d) Let \( F \) be a finite extension of a finite field \( K \), and \( \alpha \in F \). Define the trace \( \text{Tr}_{F/K}(\alpha) \) and the norm \( N_{F/K}(\alpha) \) of \( \alpha \) over \( K \). [2]

(e) Let \( F = \mathbb{F}_{q^m} \) be a finite extension of \( K = \mathbb{F}_q \).

(i) Suppose \( \text{Tr}_{F/K}(\alpha) = 0 \) for some \( \alpha \in F \), and let \( \beta \) be a root of \( x^q - x - \alpha \) in an extension field of \( F \). Prove that, in fact, \( \beta \in F \).

(ii) Hence prove that (for \( \alpha \in F \) ) \( \text{Tr}_{F/K}(\alpha) = 0 \) if and only if \( \alpha = \beta^q - \beta \) for some \( \beta \in F \). [5]

(f) State the Primitive Normal Basis Theorem. [1]