Problems on Finite Fields

1. The standard proof of the uniqueness of finite fields (up to isomorphism) uses the fact that a splitting field of a polynomial is unique up to isomorphism. The purpose of this problem is to establish this fact.
   Definition: Let E be an extension field of F, and $f(x) \in F[x]$. We say that $f(x)$ *splits* in E if $f(x)$ can be written as a product of linear factors in $E[x]$. We call E a splitting field of $f(x)$ over F if $f(x)$ splits in E but in no proper subfield of E.

   (a) Show that every non-constant polynomial has a splitting field.

   (b) Let F be a field and let $p(x) \in F[x]$ be irreducible over F. If α is a root of $p(x)$ in some extension E of F and β is a root of $p(x)$ in some extension E' of F, then show that $F(\alpha) \cong F(\beta)$

   (c) Let $p(x) \in F[x]$ be irreducible over F, where F is a field, and let α be a root of $p(x)$ in some extension of F. If ϕ is a field isomorphism from F to F', and β is a root of $\phi(p(x))$ in some extension of F', then show that there exists an isomorphism from $F(\alpha)$ to $F'(\beta)$ that agrees with ϕ on F and carries α to β.

   (d) Let ϕ be an isomorphism from a field F to a field F' let $f(x) \in F[x]$. If E is a splitting field for $f(x)$ over F and E' is a splitting field for $\phi(f(x))$ over F', then $\exists$ an isomorphism from E to E' that agrees with ϕ on F. [Hint: Use induction on $\deg(f(x))$]

   (e) Let F be a field and $f(x) \in F[x]$. Show that any two splitting fields of $f(x)$ over F are isomorphic.

2. Let F be a finite field different from $\mathbb{Z}_2$. Show that the sum of all elements of F is 0.

3. Let $a, b \in \mathbb{F}_{2^n}$, where n is odd. Show that $a^2 + ab + b^2 = 0$ implies that $a = b = 0$.

4. Let F be any field. If F^* is cyclic then show that F is finite.

5. Let α be a root of $x^2 - 2 \in \mathbb{Z}_5[x]$. Explain why $\mathbb{Z}_5(\alpha)$ must be the field $GF(25)$. List every element of $GF(25)$ as a linear combination of $\{1, \alpha\}$ over $\mathbb{Z}_5$. Is α a generator of the multiplicative group of $GF(25)^*$? If not, find one (such an element is called a primitive element) and call it β. Finally, for each $\gamma \in GF(25)$ of the form $a + b\alpha, a, b \in \mathbb{Z}_5$ (in your list above), determine the least $n \in \mathbb{N}$ such that $\gamma = \beta^n$. (The integer n with this property is called the **discrete logarithm** of γ to the base β, and denoted by $\log_\beta \gamma$)

6. Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial of degree m.

   (a) Show that $f(x)$ has a root α in $\mathbb{F}_{q^m}$. Also show that the roots are simple (not repeated) and given by $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$

   (b) Let $\alpha \in \mathbb{F}_{q^m}$. The elements $\alpha, \alpha^q, \ldots, \alpha^{q^{m-1}}$ are called the conjugates of α over $\mathbb{F}_q$ (or conjugates of α with respect to $\mathbb{F}_q$). Show that the conjugates of $\alpha \in \mathbb{F}_{q^m}^*$ with respect to $\mathbb{F}_q$ have the same order in $(\mathbb{F}_{q^m}^*, \cdot)$.

   (c) Let $f(x) = x^4 + x + 1 \in \mathbb{F}_2[x]$. Show that $f(x)$ is irreducible over $\mathbb{F}_2$. Let α be a root of $f(x)$. What is the smallest finite field that contains α? Let $\mathbb{F}_q$ be that finite field. Compute conjugates of α over $\mathbb{F}_2$ and also over $\mathbb{F}_4$. What is the order of α in $\mathbb{F}_q$? Is it a primitive element of $\mathbb{F}_q$?

7. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ of degree d dividing n (This is the same as Problem 13 in Section 33)

8. Let q be a prime power and let n be a positive integer such that $\gcd(n, q) = 1$.

   (a) Show that the polynomial $x^n - 1 \in \mathbb{F}_q[x]$ has distinct roots (no multiple roots)

   (b) What is the smallest extension of $\mathbb{F}_q$ that contains a primitive n-th root of unity?

   (c) Let $q = 3$ and $n = 11$. Find the smallest extension E of $\mathbb{F}_3$ that contains an 11-th root of unity, and identify a primitive 11-th root of unity in E.

   (d) Obtain the factorization $x^{11} - 1$ over E, and use this factorization to obtain the factorization of $x^{11} - 1$ over $\mathbb{F}_3$.