Presentation Problems on Finite Fields

---

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

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

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

4. 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 $\log_\beta \gamma$)

5. 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 $\mathbb{F}_q$?

6. 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)

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

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

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

   (c) Let $q = 3$ and $n = 11$. Construct 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 $\mathbb{F}_3$.