PS7 - finite fields

Math146 - George McNinch

2025-03-23

In these exercises, $p > 0$ denotes a prime number, and $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ the finite field of p elements. More generally, if $q = p^m$ then $\mathbf{F}_q = \mathbf{F}_{p^m}$ denotes the finite field of q elements.

1. Show that if $g(T) \in \mathbf{F}_p[T]$ is irreducible and if $g \mid T^{p^m} - T$, then $\deg g(T)$ is a divisor of m.
2. If E and F are subfields of $\mathbf{F}_{p^n}$ with p^e and p^f elements respectively, how many elements does $E \cap F$ contain? Prove your claim.
3. For $a \in \mathbf{F}_p$ let $f_a = T^p - T + a \in \mathbf{F}_p[T]$.

    a. If α is a root of f_a in some extension field of $\mathbf{F}_p$, show that $\alpha + 1$ is also a root of f_a.
    b. Let α be a root of f_a in some extension field. Prove that $E = \mathbf{F}_p(\alpha)$ is a splitting field for f_a. (*Hint:* use the result established in a.)
    c. Show that the mapping $x \mapsto x^p$ defines an automorphism $\sigma : E \to E$ which is the identity on $\mathbf{F}_p$ and satisfies $\sigma(\alpha) = \alpha + r$ for some $r \in \mathbf{F}_p$ with $r \neq 0$. *Hint:* Show that $\sigma(\alpha)$ must be a root of f_a.
    d. Show that f_a is irreducible over $\mathbf{F}_p$ – i.e. that f_p is irreducible in $\mathbf{F}_p[T]$.
    Hint: if $q \in \mathbf{F}_p[T]$ is an irreducible factor of f_a explain why $\sigma(q) = q$. If α is a root of q, show that $\alpha + i$ is a root of q for each $i \in \mathbf{F}_p$ and deduce that $f_a = q$.
    e. Let $a \neq b \in \mathbf{F}_p$ and let α, β be roots $f_a(T)$ and $f_b(T)$ respectively. Explain why $\mathbf{F}_p(\alpha) \simeq \mathbf{F}_p(\beta)$.

4. Let $p > 2$ be a prime and let $n \in \mathbf{Z}_{>0}$.

    a. Let S be the set of squares in $\mathbf{F}_{p^n}$; i.e.
    $$S = \{x^2 \mid x \in \mathbf{F}_{p^n}\}$$
    Show that S contains exactly $(p^n + 1)/2$ elements.
    Hint: Note that $x \mapsto x^2$ defines a group homomorphism $\phi : \mathbf{F}_{p^n}^\times \to \mathbf{F}_{p^n}^\times$. What is $\ker \phi$? What is the image of ϕ?
    b. Given $a \in \mathbf{F}_{p^n}$ let $T = \{a - x \mid x \in S\}$. Show that $T \cap S \neq \emptyset$.
    c. Show that every element of $\mathbf{F}_{p^m}$ may be written as a sum of two squares.