CIMPA research school on
Group Actions in Arithmetic and Geometry

Exercises on Finite fields

February 20, 2020

1. Determine $(\alpha^2+\alpha+3)^{-1} \in (\mathbb{F}_5(\alpha), \alpha^3+\alpha^2+3\alpha+4=0)$.
2. Suppose that F_1 and F_2 are finite fields of characteristic p and that $\Psi : F_1 \longrightarrow F_2$ is a field isomorphism.
   (a) Show that if $\alpha \in F_1$ and $f \in \mathbb{F}_p[X]$ is such that $f(\alpha)=0$, then $f(\Psi(\alpha))=0$;
   (b) deduce that $f(\alpha^{p^k})=0$ for all $k \in \mathbb{N}$ (*hint: apply the above with* $\Psi=\Phi$ *the Frobenius automorphism*);
   (c) if furthermore f is irreducible of degree n, show that all the roots of f are $\alpha, \alpha^p \cdots, \alpha^{p^{n-1}}$.
3. Construct explicitly isomorphisms between:
   (a) $(\mathbb{F}_3(\alpha), \alpha^2=2)$ and $(\mathbb{F}_3(\beta), \beta^2=\beta+1)$;
   (b) $(\mathbb{F}_2(\rho), \rho^3=\rho+1)$ and $(\mathbb{F}_2(\gamma), \gamma^3=\gamma^2+1)$;
   (c) $(\mathbb{F}_5(\xi), \xi^2=2)$ and $(\mathbb{F}_5(\zeta), \zeta^2=\zeta-1)$.
4. List all *irreducible* and *primitive* polynomials of degree n in $\mathbb{F}_p[X]$ for $n \leq 5$ and $p \leq 5$.
5. An element α of a finite field $\mathbb{F}_{p^n}$ is said to be *normal* if $\alpha, \alpha^p \cdots, \alpha^{p^{n-1}}$ form an $\mathbb{F}_p$–basis of $\mathbb{F}_{p^n}$. The "*Normal Basis Theorem*" postulates the existence of a normal element in every finite field. The minimal polynomials of a normal element is called *Normal Polynomial*. Determine all normal polynomials of degree n in $\mathbb{F}_p[X]$ for $n \leq 3$ and $p \leq 3$.
6. Determine the number of elements of the *splitting field* of the following polynomials:
   (a) $\displaystyle\prod_{d \leq 10} X^{p^d} - X \in \mathbb{F}_p[X]$ (b) $(X^2+2)(X^2-X-1)(X^4+X+1)(X^{80}-1) \in \mathbb{F}_3[X]$.
7. Determine the number of irreducible factors of the polynomials above.
8. Determine the multiplicative order and the minimal polynomial over $\mathbb{F}_p$ of all the elements in the following fields: $(\mathbb{F}_3(\alpha), \alpha^2=2)$, $(\mathbb{F}_2(\rho), \rho^3=\rho+1)$, $(\mathbb{F}_5(\xi), \xi^2=2)$, $\mathbb{F}_7$ and $\mathbb{F}_{11}$.
9. Write down a `Pseudo Code` to test if a given polynomial in $\mathbb{F}_p[X]$ of degree n is or not irreducible.