MAT 347
Finite fields
March 24, 2020

Finite fields

Recall what we already know. Let K be a finite field. Then we know its characteristic is a prime p. Moreover, the field with p elements $\mathbb{F}_p$ is the prime subfield of K, so that $\mathbb{F}_p \subseteq K$. Hence K is a (finite dimensional) vector space over $\mathbb{F}_p$ so that $|K| = p^n$, where the integer n is the dimension of K as $\mathbb{F}_p$-vector space.

We also defined the *Frobenius homomorphism* $\sigma_p : K \to K$ by $\sigma_p(a) = a^p$ for all $a \in K$. Notice that $\sigma_p \in \mathrm{Gal}(K/\mathbb{F}_p)$.

Our first goal is to show that for each $n \geq 1$ there is a unique field K with $|K| = p^n$, up to isomorphism.

1. Let K be a field of size p^n. Then K is a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. (*Hint:* recall that the group $K^\times$ is cyclic!)
2. Conversely, fix any integer $n \geq 1$ and let K be a splitting field of the polynomial $X^{p^n} - X$ over $\mathbb{F}_p$. Prove that $|K| = p^n$. (*Hint:* let Σ be the set of roots of $X^{p^n} - X$ in K. Show that Σ is a field so $\Sigma = K$. Also show that $X^{p^n} - X$ is separable.)
3. Deduce that for any $n \geq 1$ there exists a unique field of order p^n up to isomorphism. We will denote it by $\mathbb{F}_{p^n}$.
4. Deduce that for any $n \geq 1$ there exists an irreducible polynomial in $\mathbb{F}_p[X]$ of degree n. (*Hint:* use that $\mathbb{F}_{p^n}/\mathbb{F}_p$ is simple.)
5. Show that the extension $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois.
6. Prove that the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic of order n, generated by the Frobenius automorphism σ_p.
7. Classify the intermediate fields of $\mathbb{F}_{p^n}/\mathbb{F}_p$: what sizes do they have and how many are there of each size?
8. Let $F = \mathbb{F}_2$. Let $K = F[X]/(X^4 + X + 1)$. Describe $\mathrm{Gal}(K/F)$ and draw the lattice of subextensions of K/F. For each subfield $F \subseteq M \subseteq K$ find $\alpha \in M$ such that $M = F(\alpha)$ and find the minimal polynomial of α over K.

9. Continuing with the previous question, how does the polynomial $X^4 + X + 1$ factor over K? (*Hint:* if β denotes the obvious root in K, how do you obtain new roots from β?)

Further problems

10. Repeat Question 8 with $K = F[X]/(X^6 + X + 1)$. You may assume that this polynomial is irreducible.

11. Suppose that F is a finite field of characteristic p and that K/F is an extension of degree n. Show that K/F is Galois and that $\mathrm{Gal}(K/F)$ is cyclic, generated by $\sigma_p^{[F:\mathbb{F}_p]}$ (i.e., the automorphism $x \mapsto x^{|F|}$).