Finite Fields

Prop Let F be a finite field. Then

(a) $\exists!$ prime p s.t. F contains a subfield isomorphic to $\mathbb{F}_p$

(b) F is a finite extn of $\mathbb{F}_p$, and $|F| = p^n$ for $n = [F:\mathbb{F}_p]$.

Pf There is a unique ring hom $\mathbb{Z} \xrightarrow{f} F$ taking $1 \mapsto 1$. Since F is finite, the hom is not inj hence has kernel $m\mathbb{Z}$ for some $m > 1$, whence $\mathbb{Z}/m\mathbb{Z} \xrightarrow{\cong} \text{im}(f)$. But $\text{im}(f)$ has no 0 divisors, so in fact $m = p$ prime, and $\mathbb{Z}/p\mathbb{Z} \subseteq F$ by this map. ($\mathbb{Z}/p\mathbb{Z} \cong \mathbb{F}_p$)

This makes F an $\mathbb{F}_p$-vs, and finiteness of $F \Rightarrow [F:\mathbb{F}_p] = n < \infty$. But then $F \cong \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vs, so $|F| = p^n$. □

Thm Let F be a finite field with $q = p^n$ elements. Then

(a) $\alpha^q = \alpha \quad \forall \alpha \in F$

(b) $x^q - x = \prod_{\alpha \in F} (x - \alpha)$

(c) F is a splitting field over $\mathbb{F}_p$ of $x^q - x \in \mathbb{F}_p[x]$.

Thus any two fields with q elts are isomorphic.

Pf $F^\times \leq \mathbb{Z}_{q-1}$ is a group with $q-1$ elts, so $\alpha^{q-1} = 1 \ \forall \alpha \in F^\times$.

So $\alpha^q = \alpha \ \forall \alpha \in F$. □

Thm Given any prime p and any positive integer n, $\exists$ finite field with p^n elements.

Pf Let $q = p^n$ and let L be the splitting field of $x^q - x$ over $\mathbb{F}_p$. Then $x^q - x$ is separable, so $F = \{\alpha \in L \mid \alpha^q = \alpha\}$ is a subset of L containing q elts. F is a subfield (check) so is the desired field.

Prop If $f \in \mathbb{F}_p[x]$ is nonconstant and $n \geq 1$, then the number of roots of f in $\mathbb{F}_{p^n}$ is the degree of the polynomial $\gcd(f, x^{p^n} - x)$.

Pf Let $g = \gcd =$ product of the $x - \alpha_i$ dividing f (for $\mathbb{F}_{p^n} = \{\alpha_1, \ldots, \alpha_{p^n}\}$). But $x - \alpha_i$ divides f iff $f(\alpha_i) = 0$ so $g = \prod_{f(\alpha_i)=0} (x - \alpha_i)$. □

Thm If $q = p^n$, then

(a) $\mathbb{F}_q / \mathbb{F}_p$ is a Galois extension of degree n.

(b) The map $\mathrm{Frob}_p : \mathbb{F}_q \to \mathbb{F}_q$, $\alpha \mapsto \alpha^p \in \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p)$.

(c) $\langle \mathrm{Frob}_p \rangle = \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p) \cong C_n$

Pf $\mathbb{F}_q$ is the splitting field of the separable polynomial $x^q - x$.

$\mathrm{Frob}_p \in \mathrm{Gal}(\mathbb{F}_q / \mathbb{F}_p)$ is obvious since $\mathbb{F}_q$ has char p and $a^p = a$ for $a \in \mathbb{F}_p$.

Know that the order of Frob_p divides n. Suppose $\mathrm{Frob}_p^r = \mathrm{id}$. Then $\alpha^{p^r} = \alpha \ \forall \alpha \in \mathbb{F}_q \Rightarrow x^{p^r} - x$ has q roots in $\mathbb{F}_q \Rightarrow p^r = q$, so Frob_p has order n. □

Cor For finite fields $\mathbb{F}_{p^m}$, $\mathbb{F}_{p^n}$, have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ iff $m \mid n$.

Pf Suppose $\mathbb{F}_{p^n}$ Then $m \mid n$ by the tower thm.

n | $\mathbb{F}_{p^n}$ | $\mathbb{F}_{p^m}$ | m | $\mathbb{F}_p$

Conversely, suppose $m \mid n$. Since $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p) \cong C_n$, it has a subgp H of order $\frac{n}{m}$. Then $\mathbb{F}_{p^n}^H \cong \mathbb{F}_{p^m}$. □

Thm For $m \mid n$, $\mathrm{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_{p^m}) \cong C_{n/m}$.

$H = \langle \mathrm{Frob}_p^m \rangle$ □