Finite fields

Please refer to literatures about finite fields for more details.

Definition 0.1. *field* $(F, +, \cdot)$

Lemma 0.2. *All non-zero elements have the same additional order of prime* p*.*

Proof. $F^\times \curvearrowright F^+ \backslash \{0\}$ by multiplication as group automorphism (distributive law) transitively. $\square$

Definition 0.3. *The* p *above is the* ***characteristic*** *of* F*.* $F_0 := \langle 1 \rangle_+$ *is the* ***prime subfield*** *of* F*.*

Lemma 0.4. $|F| = p^d$

Proof. F is a vector space over F_0. $\square$

Lemma 0.5. $F^\times = \langle \sigma \rangle \cong \mathbb{Z}_{p^d-1}$*, where* σ *is called a* ***Singer cycle****.*

Proof. By Vandermonde's lemma, polynomial of degree n on F has at most n solutions in F. $e := \exp(F^\times) < |F^\times| \implies x^e - 1 = 0$ has $|F^\times| > e$ solutions. $\square$

Proposition 0.6. *For any prime power* $q = p^d$*,* $\exists_1 F$ *of order* q *up to field isomorphism, says* $\mathbb{F}_q$*.*

Proof. Existance: $\mathbb{Z}/p\mathbb{Z}[x]/(f(x))$ for any irreducible polynomial $f(x)$ of degree d.

Uniqueness: If $|F| = p^d$, then $F_0 \cong \mathbb{F}_p$, F is the splitting field of $x^{p^d} - x$ over F_0, $F^\times = \langle x \rangle$. $\square$

Lemma 0.7. $\mathrm{Aut}(\mathbb{F}_q) = \langle \phi \rangle \cong \mathbb{Z}_d$*, where* $\phi : x \mapsto x^p$ *is called the* ***Frobenius automorphism****.*

Remark 0.8. ϕ *may not be a linear transformation on* $\mathbb{F}_q^n$ *since it may not preserve scalar multiplication.*

Definition 0.9. $\Gamma\mathrm{L}_n(q) := \mathrm{GL}_n(q) \rtimes \langle \phi \rangle$ *and* $\Sigma\mathrm{L}_n(q) := \mathrm{SL}_n(q) \rtimes \langle \phi \rangle$

Lemma 0.10. $x^n = 1$ *has* $(n, q-1)$ *solutions in* $\mathbb{F}_q$*.*