§5: Finite fields

Theorem 5.1. $\forall$ prime p and $n \geq 1$; $\exists$ a finite field of order p^n denoted by $\mathbb{F}_{p^n}$; uniquely determined as a subfield of an algebraic closure $\mathbb{F}_p^a$.

It is the splitting field of the polynomial:

$$X^{p^n} - X$$

And its elements are the roots of this polynomial. Every finite field is isomorphic to exactly one field $\mathbb{F}_{p^n}$.

Proof:

Let F be a finite field w/ q elements. We have a homomorphism:

$$\varphi: \mathbb{Z} \longmapsto F$$
$$1 \longmapsto 1$$

Note that $\ker \varphi \neq 0$ since $\mathbb{Z}$ is infinite & F is finite; since F is a field then $\ker \varphi$ is a prime ideal so $\ker \varphi = p\mathbb{Z}$ for some prime p.

∴ $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Q}(\mathbb{Z})$ is a subfield of F. So F has characteristic p.

We identify $\mathbb{Z}/p\mathbb{Z}$ w/ $\mathbb{Q}(\mathbb{Z})$ and look at F as a vector space over $\mathbb{Z}/p\mathbb{Z}$.

Note since F is finite this v.s. has finite degree say, n.
Let $\{w_1, \dots, w_n\}$ be a basis of F over $\mathbb{Z}/p\mathbb{Z}$.

So $F = \{ a_1 w_1 + \cdots + a_n w_n \mid a_i \in \mathbb{Z}/p\mathbb{Z} \} \Rightarrow q = |F| = p^n$

The multiplicative group F^* of F has order $q-1$; so by Lagrange; every $\alpha \in F^*$ satisfies the equation:

$$X^{q-1} = 1.$$

∴ Every element of F satisfies:

$$f(X) = X^q - X = 0.$$

So f splits into factors of degree 1 in F:

$$f(X) = \prod_{\alpha \in F} (X - \alpha)$$

So F is the splitting field for f; splitting fields are unique up to isomorphisms; so if a finite field of order p^n exists, it is uniquely determined, up to isomorphism, as the splitting field of $X^{p^n} - X$ over $\mathbb{Z}/p\mathbb{Z}$.

Now we need to show that these field exists. Let us denote $\mathbb{Z}/p\mathbb{Z}$ as $\mathbb{F}_p$. Let $n \geq 1$ and consider the splitting field of:

$$f(X) = X^{p^n} - X$$

in an algebraic closure $\mathbb{F}_p^a$. We will show that the elements of this field are the roots of f and then that f has has p^n roots.

Let α, β be roots of $f(X)$. Then

- $(\alpha+\beta)^{p^n} - (\alpha+\beta) = (\alpha^{p^n} - \alpha) + (\beta^{p^n} - \beta) = 0$

  (freshman's dream)

- $(\alpha\beta)^{p^n} - \alpha\beta = \alpha^{p^n}\beta^{p^n} - \alpha\beta = \alpha\beta - \alpha\beta = 0$

  since $\alpha^{p^n} = \alpha$, $\beta^{p^n} = \beta$

- $(-\beta)^{p^n} - (-\beta) = (-1)^{p^n} \beta^{p^n} + \beta = \begin{cases} -\beta + \beta = 0 & \text{if } p \text{ is odd} \\ \beta + \beta = 0 & \text{if } p = 2 \end{cases}$

since $1 \in \mathbb{F}_2$ has char 2

If $\beta \neq 0$ then:

- $(\beta^{-1})^{p^n} - \beta^{-1} = (\underbrace{\beta^{p^n}}_{= \beta})^{-1} - \beta^{-1} = \beta^{-1} - \beta^{-1} = 0$

So $\alpha\beta$; $\alpha+\beta$; $-\beta$; β^{-1} are roots of f and $1 \neq 0$ are roots of f.

So: $\mathbb{F}_{p^n} = \{\alpha \in \mathbb{F}_p^a \mid f(\alpha) = 0\}$ is a subfield of $\mathbb{F}_p^a$, and it is clearly the splitting field of $f(X)$.

Finally:

$$f'(X) = p^n X^{p^n - 1} - 1 = -1 \quad (p^n X^{p^n-1} \to 0)$$

So $f(X)$ has no multiple roots so $|\mathbb{F}_{p^n}| = p^n$.

Corollary 5.2. Let $\mathbb{F}_q$ be a finite field. Let $n \in \mathbb{N}^*$. In a given algebraic closure $\mathbb{F}_q^a$, there exists a unique extension of $\mathbb{F}_q$ of degree n, and this extension is $\mathbb{F}_{q^n}$.

Proof: Let $q = p^m$, the splitting field of $X^{p^{mn}} - X$ is $\mathbb{F}_{p^{mn}} = \mathbb{F}_{q^n}$; it has degree mn over $\mathbb{F}_p$.

$$\Rightarrow [\mathbb{F}_{q^n} : \mathbb{F}_q] = \frac{[\mathbb{F}_{q^n} : \mathbb{F}_p]}{[\mathbb{F}_q : \mathbb{F}_p]} = \frac{mn}{m}$$

Conversely any extension of degree n over $\mathbb{F}_q$ has degree mn over $\mathbb{F}_p$ so it must be $\mathbb{F}_{p^{mn}}$

Definition 5.0.

Let $q = p^n$, we consider the Frobenius mapping

$$\varphi : \mathbb{F}_q \longrightarrow \mathbb{F}_q$$
$$x \longmapsto x^p$$

Then ℓ is a homomorph by the freshman's dream. and it's kernel is 0 - so this is an injective and since $\mathbb{F}_q$ is finite this is an isomorphism.

Theorem 5.4

The group of automorphisms of $\mathbb{F}_q$ is cyclic of degree n, generated by φ.

Proof: Let $G = \langle \varphi \rangle = \{ \varphi^k : k \in \mathbb{N} \}$.

Note $\varphi^n = id$ since $\varphi^n(x) = x^{p^n} = x \quad \forall x \in \mathbb{F}_q$ - so $|G| \leq n$.

Let d be the period of φ, so $\varphi^d(x) = x^{p^d} = x \quad \forall x \in \mathbb{F}_q$

$\Rightarrow$ Each $x \in \mathbb{F}_q$ is a root of:

$$X^{p^d} - X = 0.$$

$\therefore d \geq n \Rightarrow d = n$.

Now we need to show that G is the group of all automorphisms of $\mathbb{F}_q$.

Any automorphism of $\mathbb{F}_q$ leaves $\mathbb{F}_p$ fixed (since $\mathbb{F}_p$ is additively generated by 1).

So any automorphism of $\mathbb{F}_q$ is over $\mathbb{F}_p$. By th 4.1 the number of such automorphism is $\leq n$.

Since $G \leq Aut(\mathbb{F}_q) \Rightarrow G = Aut(\mathbb{F}_q)$

□

Theorem 5.5

Let $m, n \in \mathbb{N}^*$. Then in any alg closure of $\mathbb{F}_p$, the subfield $\mathbb{F}_{p^n}$ is contained in $\mathbb{F}_{p^m}$ iff $n \mid m$.

If this is the case then if $q = p^n$ and $m = nd$, then $\mathbb{F}_{p^m}$ is normal and seperable over $\mathbb{F}_q$; and the group of automorphisms of $\mathbb{F}_{p^m}$ over $\mathbb{F}_q$ is cyclic our d, generated by φ^n.

Proof: Let $\mathbb{F}_{p^n}$ de-contained in $\mathbb{F}_{p^m}$.

If we let $[\mathbb{F}_{p^m} : \mathbb{F}_{p^n}] = d$ we see that:

$$[F_{p^m} : \mathbb{F}_p] = [\mathbb{F}_{p^m} : \mathbb{F}_{p^n}][\mathbb{F}_{p^r} : \mathbb{F}_p]$$

$$\Rightarrow \quad m = dn$$

$\therefore \quad n \mid m.$

On the other hand if $m = dn$; then by cor. 5.2. there is an extension of $\mathbb{F}_{p^r}$ of degree d and this field is $\mathbb{F}_{p^d} = \mathbb{F}_{p^m}$.

- $\mathbb{F}_{p^m}$ is normal over $\mathbb{F}_q$ since it's the splitting field of $X^{p^m} - X$. Furthermore looking at the tower:

$$\mathbb{F}_p \subseteq \mathbb{F}_q \subseteq \mathbb{F}_{p^m}$$

$\mathbb{F}_{q^m}$ is separable over $\mathbb{F}_p$ by Th 5.9 so by Th 4.5:
$\mathbb{F}_{p^m}$ is separable over $\mathbb{F}_q$.

• The proof of the last statement is analogous to the proof of Th. 5.9. w/

$$G = \langle \varphi^n \rangle .$$