§2.7 Finite fields

We first prove that if F is a finite field then any polynomial of the form $f(x) = g(x^p)$ for some $g(x) \in F[x]$ is necessarily reducible.
This will show that every irreducible poly is also separable in the case of finite fields.
Let $\mathbb{F}$ be a field of char p.

Defn The map $\varphi : \mathbb{F} \to \mathbb{F}$, $a \mapsto a^p$ is called the

Frobenious homomorphism.

Lemma 2.30 φ is a monomorphism and if F is finite then it is an automorph.

Proof It follows easily that φ is a hom.

Since
$$\left.\begin{aligned}(a+b)^p &= a^p + b^p\\ (ab)^p &= a^p b^p\\ \varphi(1) &= 1\end{aligned}\right\} \Rightarrow \varphi \text{ is a homomorphism}$$

Since $\varphi(1) = 1$ and it is a homomorphism of fields, φ is injective.
If $\mathbb{F}$ is also finite it also has to be surjective

$\square$

Corollary 2.31 Suppose $\mathbb{F}$ is a finite field of char p. Then every element of $\mathbb{F}$ is a p-th power in $\mathbb{F}$.

Pf Follows from surjectivity of Frobenius hom. ◪

Prop 2.32 Every irreducible polynomial over a finite field $\mathbb{F}$ is separable.

Proof Let $f(x) \in \mathbb{F}[x]$ be irred. and separable

We've seen that

$f(x) \in \mathbb{F}(x]$ is insep. if and only if
$f(x) = g(x^p)$ for some $g(x) \in \mathbb{F}[x]$

where $g(x) = b_m x^m + \dots + b_0$

Since each $b_i \in \mathbb{F}$ is a pth power $b_i = c_i^p$ for some $c_i \in \mathbb{F}$, by the above corollary.

Then $f(x) = g(x^p) = c_m^p x^{mp} + c_{m-1}^p x^{(m-1)p} + \dots + c_0^p$

$$= (c_m x^m)^p + \qquad + c_0^p$$

$$= (c_m x^m + \dots + c_0)^p$$

Hence f is reducible ◪

<u>Goal</u>: To show that for every prime power $q = p^n$ there is (up to isom) unique field with q elements, $\mathbb{F}_q$, and it is the splitting field of the poly $x^q - x$ over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

<u>Thm 2.33</u> If $\mathbb{F}$ is a finite field, then $\mathbb{F}$ has characteristic $p > 0$ and the number of elts in $\mathbb{F}$ is p^n where $n = [\mathbb{F} : \mathbb{F}_p]$

<u>Proof</u>. For each comm. ring R, recall that there is a ring hom $\varphi : \mathbb{Z} \to R$
$$m \mapsto m.1_R$$
We apply this to $R = \mathbb{F}$ a finite field
The kernel of φ is non-zero, since $\mathbb{F}$ is finite and $\mathbb{Z}$ is infinite, say $\ker \varphi = m\mathbb{Z}$.
Since $\mathbb{Z}/m\mathbb{Z}$ is a subring of the field $\mathbb{F}$ it must ~~be~~ a domain. Hence $m = p$ a prime
Therefore there is an embedding $\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbb{F}$. Viewing $\mathbb{F}$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$, it is finite dim'l since $\mathbb{F}$ is finite. Let $n = \dim_{\mathbb{Z}/p\mathbb{Z}} \mathbb{F}$

Pick a basis $\{x_1, \dots, x_n\}$ of $\mathbb{F}$ over $\mathbb{Z}/p\mathbb{Z}$
~~Then~~ every elt of $\mathbb{F}$ has a unique repn as
from $c_1x_1 + \dots + c_nx_n$, $c_i \in \mathbb{Z}/p\mathbb{Z}$. Each coef c_i has p choices. Hence $|\mathbb{F}| = p^n$. ☒

Rmk ① Even though there are groups of any order, there are not fields of any order
e.g there is no field of order $2.3=6$.

② For groups, there can be non-isom gps of same order eg. $\mathbb{Z}_6$, S_3

But up to isom there is a unique field of order p^n. This is the content of

Thm 2.33 Let p be a prime, $q=p^n$ $n \in \mathbb{Z}_{>0}$
A field $\mathbb{F}$ has q elements if and only if it is a splitting field of $f(x)=x^q-x \in \mathbb{F}_p[x]$
Moreover since splitting fields exist and unique up to isom there is a unique field with $q=p^n$ elements.

Proof Suppose $\mathbb{F}$ is a finite field with $q=p^n$ elements.
The set $\mathbb{F}\setminus\{0\}$ is a group under multiplication of order $q-1$.
Hence if $x \in \mathbb{F}\setminus\{0\}$, then $x^{q-1}=1$
and $x^q=x$. Since $0^q=0$ trivially
Every elt of $\mathbb{F}$ is a zero of x^q-x

and $x^q - x$ splits in $\mathbb{F}$. Since the zeroes of f exhaust $\mathbb{F}$, they certainly generate $\mathbb{F}$, so $\mathbb{F}$ is a splitting field of $f = x^q - x$ over $\mathbb{F}_p$.

Conversly, let K be a splitting field of $f(x) = x^q - x$ over $\mathbb{F}_p$

$f'(x) = -1$, hence f' is relatively prime to f, and all zeroes of f in K are distinct and therefore f has exactly q zeroes in K.

Let α, β be zeroes of f. Since

$$\alpha^q = \alpha, \quad \beta^q = \beta, \quad (\alpha\beta)^q = \alpha^q\beta^q = \alpha\beta$$

hence $\alpha\beta$ is also a zero of f

Similarly $\left(1/\alpha\right)^q = 1/\alpha^q = 1/\alpha$. and $1/\alpha$ is also a root of $f(x)$.

Finally,

$$(\alpha \pm \beta)^q = \alpha^q \pm \beta^q = \alpha \pm \beta$$ This is because $\binom{p^n}{k}$ is divisible by p $1 \leq k \leq p^n - 1$ or

$$\alpha^q = \varphi^n(\alpha)$$, where $\varphi : K \to K$, $\alpha \to \alpha^p$, $\left(\varphi^n = \underbrace{\varphi \circ \cdots \circ \varphi}_{n \text{ times}}\right)$

and Since φ is additive so is φ^n.

Hence zeroes of f in K form a field which then must be the whole field of K. Hence $|K| = q = p^n$

Our next theorem about finite fields require some abelian group theory.

Defn The exponent $e(G)$ of a finite group G is the least common multiple of the orders of the elements of G.

Rmk: ① Clearly $e(G) \leq |G|$ and $e(G) \mid |G|$.
② Note $e(G)$ is the least positive integer k s.t $g^k = e \quad \forall g \in G$.

Recall the following thm from finite abelian group theory.

Thm Suppose $(G, +)$ is a finite abelian group. Then G is isomorphic to a product of cyclic groups

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$$

Furthermore the isomorphism can be chosen so that $d_j \mid d_k$ for $1 \leq j < k \leq s$

Cor Suppose G is a finite abelian group. Then $\exists\, g \in G$ s.t $\text{order}(g) = e(G)$.

Proof. $G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_s}$ with $d_j \mid d_k$
$1 \leq j < k \leq s$.

If $g \in G$ then $g^{d_s} = e$. Hence $e(G) \leq d_s$

On the other hand G has a s/gp isomorphic to $\mathbb{Z}_{d_s} = \langle h \rangle$ where h is a generator of this s/gp.

Hence $\text{order}(h) = d_s$.

Since $\text{order}(h) \leq e(G)$

we have $d_s \leq e(G)$

hence $d_s = e(G) = \text{ord}(h)$. $\boxtimes$

<u>Rmk.</u> In general G need not possess an element of order $e(G)$.

For example if $G = S_3$, then $e(G) = 6 = |S_3|$.

but G has no elt of order 6.

It has elts of order 1, 2, 3.

Their least common multiple is 6.

In S_6, the elements have order

1, 2, 3, 4, 5 or 6, $e(S_6) = 60$

$|S_6| = 720$.

We now apply these to the multiplicative group of a field

<u>Thm 2.34</u> Suppose that K is a field and $K^* = K \setminus \{0\}$ its non-zero elements.

If G is a finite subgroup of K^* then G is cyclic.

Proof: let $n = e(G)$. Then $\alpha^n = 1 \ \forall \alpha \in G$. Since $x^n - 1$ has at most n roots $|G| \leq n$. But $e(G) \leq |G|$. Hence $e(G) = |G|$. But then G has an elt of order $e(G) = |G|$ by the above cor. Hence G is cyclic

As a corollary we have

Thm 2.35 If $\mathbb{F}$ is a finite field then $\mathbb{F}^{\times}$ is cyclic.

and

Cor 2.36 If $L : K$ is an extension of finite fields, then $L : K$ is simple

Proof let α generate the multiplicative group $L^{\times}$. Then $L = K(\alpha)$.

Example (i) In $\mathbb{F}_{11}$, powers of 2 are

$$1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1$$

Hence 2 generates the multiplicative gp.

Whereas powers of 4 are $1, 4, 5, 9, 3, 1$ so 4 does not generate $\mathbb{F}_{11}^{\times}$

(2) $\mathbb{F}_{25}$: This can be constructed as a splitting field of $x^2-2 \in \mathbb{F}_5[x]$

Check x^2-2 is irreducible since it has no roots in $\mathbb{F}_5$.

$$\mathbb{F}_{25} \cong \mathbb{F}_5[x] / (x^2-2)$$

Let α be a root of x^2-2. Then

$$\mathbb{F}_{25} = \{ a + b\alpha \mid a, b \in \mathbb{F}_5 \}$$

By trial an error one can check that $2+\alpha$ has powers

$1,\ 2+\alpha,\ 1+4\alpha,\ 4\alpha,\ 3+3\alpha,\ 2+4\alpha,\ 2$
$4+2\alpha,\ 2+3\alpha,\ 3\alpha,\ 1+\alpha,\ 4+3\alpha,\ 4$
$3+4\alpha,\ 4+\alpha,\ \alpha,\ 2+2\alpha,\ 3+\alpha,\ 3$
$1+3\alpha,\ 3+2\alpha,\ 2\alpha,\ 4+4\alpha,\ 1+2\alpha,\ 1.$

Rmk In general there is no known procedure for finding a generator other than trial and error.
Fortunately, the existence of a generator is sufficient for most purposes.

We can say more about finite fields, some of which are in the exercises.

Namely we have that

Thm 2.37 Every finite field $\mathbb{F}$ is isomorphic to $\mathbb{F}_p[x]/(f(x))$ for some prime p and some irreducible monic poly $f(x) \in \mathbb{F}_p[x]$.

Pf Exercise: let α be a generator of $\mathbb{F}^\times$ and consider the evaluation hom
$$E_\alpha : \mathbb{F}_p[x] \to \mathbb{F}, \quad g(x) \longmapsto g(\alpha).$$

Thm 2.38 Every irreducible poly $f(x) \in \mathbb{F}_p[x]$ of degree n divides $x^{p^n} - x$ and is separable

Pf: Exercise

Thm 2.39 A subfield of $\mathbb{F}_{p^n}$ has order p^d where $d|n$ and $\exists$ one such subfield for each $d|n$.

Pf Exercise

§ 3. Basic definitions of Galois theory

Idea of Galois theory:

let $f(x) = x^m + a_{m-1}x^{m-1} + \dots + a_0 \in K[x]$

We are interested in the eqn $f(x)=0$.

How can we distinguish polynomials that can be solved by a "formula" involving the coefs of f and field operations as well as taking nth roots. (radical expressions).

We can consider the splitting field K of f - we've already seen that $L:K$ has a vector space structure
Galois's main idea was to look at symmetries of the roots of the poly $f(x)$

He associated to the extension $L:K$ a group of permutations, now called the Galois group of L/K, $Gal(L:K) =: G$ and showed that the Galois group G reflects the finer structure of $L:K$.
We'll see that under extra hypothesis there is a one-to-one correspondence

between ① Subgroups of the Galois group $G = Gal(L:K)$

② Subfields M of L such that $K \subseteq M \subseteq L$

This correspondence reverses inclusions

We start with the definition of K-autom of L

<u>Defn</u> Let K be a subfield of L.
An automorphism $\sigma \in Aut(L) := \{\sigma : L \to L \mid \sigma$ is an isom$\}$
is called a <u>K-automorphism of L</u> if
$\sigma(k) = k \quad \forall k \in K$, i.e. $\sigma|_K = id_K$.

Let $\boxed{Aut_K L := \{\sigma : L \to L \mid \sigma \text{ isom}, \sigma|_K = id_K\}}$.
$\sigma \in Aut_K L$ is an autom. of the extension.
A simple but pivotal result to the whole Galois theory is

<u>Thm 3.1</u> If $L:K$ is a field extension
Then the set of all K-autom of L
form a group under composition of maps.

Proof If $\sigma, \gamma \in Aut_K(L)$ then clearly

$\sigma \circ \gamma \in Aut(L)$ and if $k \in K$

$(\sigma \circ \gamma)(k) = \sigma(\gamma(k)) = \sigma(k) = k$. Hence
$\sigma \circ \gamma \in Aut_K(L)$

$1d : L \to L$ is clearly in $Aut_K(L)$

Finally $\sigma^{-1} \in Aut(L)$ and

$k = (\sigma^{-1} \circ \sigma)(k) = \sigma^{-1}(k)$, Hence $\sigma^{-1} \in Aut_K L$

$\boxtimes$

Defn The group of all K-autom of L is called the Galois group of the extension $L:K$.
It will be denoted by $Gal(L:K)$ or $\Gamma(L:K)$ (instead of $Aut_K L$ or $Aut(L/K)$)

Let $f \in K[x]$. If L is a splitting field of f then the Galois group $Gal(L:K)$ is called the Galois group of f.

Rmk. Note that every $\sigma \in Gal(L/K)$ is an invertible K-linear map of L.

Example. ① $\mathbb{C}:\mathbb{R}$.

let $\sigma \in Gal(\mathbb{C}:\mathbb{R})$

let $j := \sigma(i)$ then

$$j^2 = (\sigma(i))^2 \underset{\substack{\downarrow \\ \sigma \text{ is} \\ \text{a hom}}}{=} \sigma(i^2) = \sigma(-1) \underset{\substack{\downarrow \\ \sigma \in Gal(\mathbb{C}/\mathbb{R}) \\ \text{and } -1 \in \mathbb{R}}}{=} -1$$

Therefore $j^2 = -1$ and hence $j = i$ or $-i$

For any $r, s \in \mathbb{R}$, $\sigma(r+si) = \sigma(r) + \sigma(s)\sigma(i)$
$= r + s\,\sigma(i)$

Hence there are 2 possibilities for σ

Either $\sigma(i) = i$ then $\sigma(r+si) = r+si$
and hence σ = identity map

or $\sigma(i) = -i$ then $\sigma(r+si) = r-si$
ie σ is the complex conjugation map

And then $\sigma^2 = id$

so $Gal(\mathbb{C}/\mathbb{R}) = \{id, \text{complex conj}\} \cong \mathbb{Z}_2$