Lecture 2:-

Example:- Let $f(x) = x^4 - 2 \in \mathbb{Q}[x]$.

It is irreducible by Eisenstein.

Let $\alpha = \sqrt[4]{2} \in \mathbb{R}$. The other roots are $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-i\sqrt[4]{2}$, where i is a root of x^2+1.

Consider $K = \mathbb{Q}(\sqrt[4]{2}, i) \subseteq \mathbb{C}$.

All the roots of f are contained in K!

$[K : \mathbb{Q}]$ $(4, 2, 8)$ then

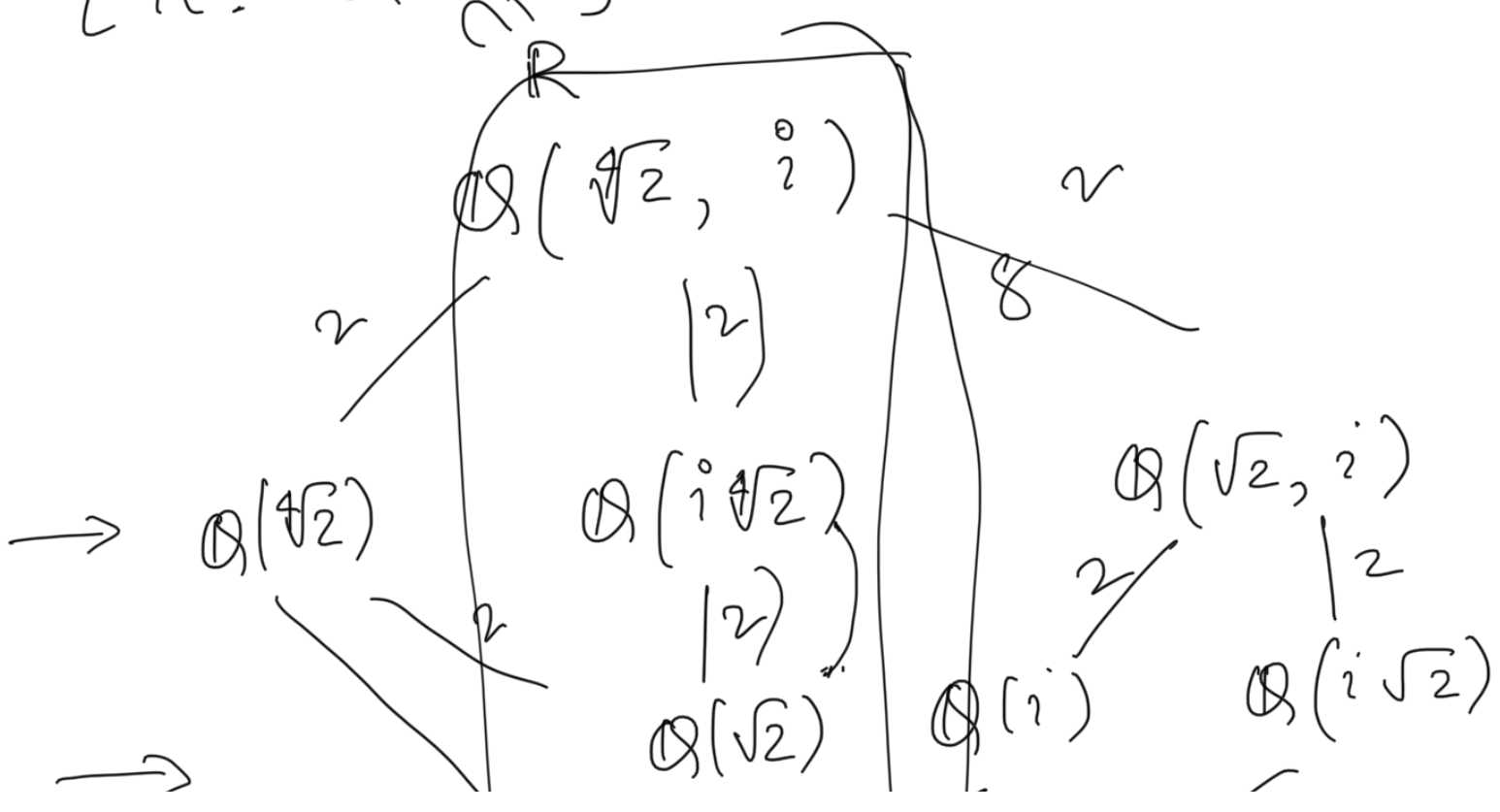
~~If α is a root of x^4-2~~

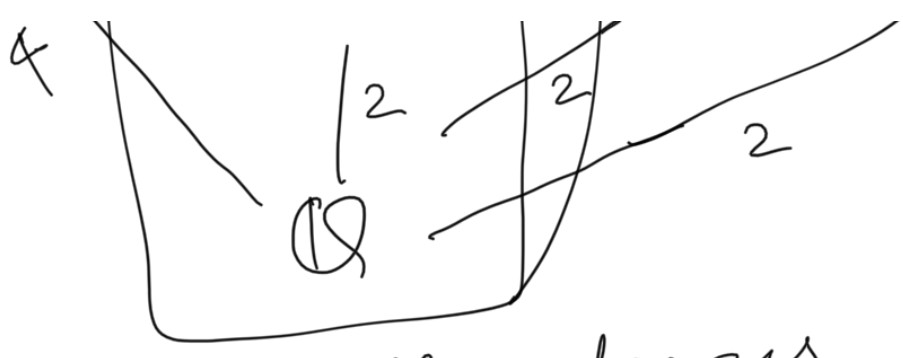
$\mathbb{Q}(\alpha) \simeq \dfrac{\mathbb{Q}[x]}{(f(x))}$ is of deg $= \deg f(x) = 4$.

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and $\mathbb{Q}(\alpha) \subseteq K$

$[K : \mathbb{Q}(\alpha)]$

$[K : \mathbb{Q}(\sqrt[4]{2})] = 2$ so $[K : \mathbb{Q}] = 8$





Ex: Check that the degrees are as labelled in the picture.

K contains all the roots of x^4-2.

If $L \subseteq K$ also contains all the roots of x^4-2, then $\sqrt[4]{2} \in L$,

$i\sqrt[4]{2} \in L$

$\Rightarrow i \in L$

$\Rightarrow \mathbb{Q}(\sqrt[4]{2}, i) \subseteq L$.

$\Rightarrow L = K$.

Such a field is called a splitting field of the polynomial f.

Splitting fields :-

So far, given a field F and an irr poly $f(x) \in F[x]$, we know that $\exists$ K/F finite that contains a root of f.

$\left(K = \frac{F[x]}{(f(x))} \right)$.

Defn :- Let $f(x) \in F[x]$. A field extn K/F is a splitting field of f

K/F

over F if

(a) f splits in K into linear factors

$$f = c\prod_{i=1}^{n}(x-\alpha_i) \quad \text{with } \alpha_i \in K$$

(b) $K = F(\alpha_1, \cdots \alpha_n)$.

(b) means that f does not split in any strict subfield of K.

Eg: (1) Consider $x^2 - 2 \in \mathbb{Q}[x]$. $\xrightarrow{\pm\sqrt{2}}$

$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$.

(2) $f(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$

$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{C}$

(3) $f(x) = x^3 - 2 \in \mathbb{Q}[x]$

$\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field

$\mathbb{Q}(\sqrt[3]{2}, \xi_3)$ is a splitting field of x^3-2. $\xrightarrow{}$ primitive 3rd root of unity.

Thm:- (1) Given a field F and an $f(x) \in F[x]$, $\xrightarrow{\deg n}$ a splitting field K of f over F. Further $[K:F] \leq n!$.

Let $f(x) \in F[x]$ and let K be

(2) Let $f(x) \in F[x]$ and let K be a splitting field of f over F. Let L be any field and let $\sigma : F \to L$ be a field hom with $\sigma(f)$ splitting in $L[x]$. Then σ extends to a hom $\tilde{\sigma} : K \to L$

$$\begin{array}{ccc} K & \xrightarrow{\tilde{\sigma}} & L \\ \cup & \nearrow_{\sigma} & \\ F & & \end{array}$$

Pf :- For (1) write $f = l_1 \cdots l_a f'$ where l_i are linear and $f' \in F[x]$ has no linear factors. If f is not trivial, let g be an irr. factor of f'. Let $K_1 = \frac{F[x]}{(g(x))}$ $x \bmod g(x)$ $[K_1 : F] = \deg g$

Then K_1 contains a root of g and hence also a root of f. So over K_1, $f = l_1 \cdots l_b f''$ with $\deg f'' < \deg f'$. By induction, f'' over K_1 a splitting field K i.e. say $\alpha_1 \equiv x \bmod g$ say $f = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$

and $K = K_1(\alpha_1, \dots, \alpha_n)$

$= \cancel{K}(\alpha_1, \dots, \alpha_n)$.

$\Rightarrow$ K is also a splitting field of f over $\mathcal{F}$.

Further $[K : \mathcal{F}] \leq n!$.

For (2), let us by induction on $[K : \mathcal{F}]$.

Suppose K is a splitting field of f over $\mathcal{F}$ with roots $\alpha_1, \dots \alpha_n \in K$

WLOG assume $\alpha_1 \notin \mathcal{F}$. Let $p(x)$ be the min poly of α_1 over $\mathcal{F}$

Then $K_1 \cong \dfrac{\mathcal{F}[x]}{(p(x))}$, $[K_1 : \mathcal{F}] = \deg p > 1$.

Since $p \mid f$ and $\sigma(f)$ splits in L, $\sigma(p)$ has a root, say β_1, in L.

and $\sigma : \mathcal{F} \longrightarrow L$. Let $\mathcal{F}' = \sigma(\mathcal{F})$

Then $\sigma : \mathcal{F} \xrightarrow{\sim} \mathcal{F}'$.

$\mathcal{F}(\alpha_1) \cong \dfrac{\mathcal{F}[x]}{(p(x))} \xrightarrow{\sigma} \dfrac{\mathcal{F}'[x]}{(\sigma(p)(x))} \cong \mathcal{F}'(\beta_1) \subseteq L$

Now we have $\sigma_1 : K_1 \longrightarrow L$

and $[K : K_1] < [K : \mathcal{F}]$ (from law).

Now the extn $K_1 \subseteq K$ and $\sigma_1 : K_1 \to L$ satisfy the assumptions in (2) with $[K : K_1] < [K : \mathcal{F}]$.

In fact K is the splitting field of f over K_1 and σ_1 is a hom $\mathcal{F} \to L$ s.t. $\sigma_1(f) = \sigma(f)$ splits in L

By induction σ_1 extends $\tilde{\sigma} : K \to L$ and $\tilde{\sigma}|_{K_1} = \sigma_1 \Rightarrow \tilde{\sigma}|_{\mathcal{F}} = \sigma$.

Corollary:- Given two splitting fields K_1 and K_2 of f over $\mathcal{F}$, they are isomorphic.

Pf:- let σ in the previous thm be the identity map. So (2) $\tilde{\sigma} : K_1 \to K_2$? $\tilde{\sigma}$ is necessarily injective. check it is also surjective

($[K_1 : \mathcal{F}] \leq [K_2 : \mathcal{F}]$
By symmetry $[K_2 : \mathcal{F}] \leq [K_1 : \mathcal{F}]$)

Finite fields:- An example of a finite field is $\mathbb{Z}/p\mathbb{Z}$, p is a field with finitely many elements. prime.

$\mathcal{F}$ a finite field has p^r elements

• A finite field for some prime p and $r \geq 1$.

What is its prime subfield?

Note:- The char of a finite field is a prime p. So $\mathbb{F}_p$ is its prime subfield.

Since $\mathbb{F}$ is finite, $[\mathbb{F} : \mathbb{F}_p] < \infty$

So $\mathbb{F} \cong (\mathbb{F}_p)^r$ for some r (as v-s).

$\Rightarrow$ $\mathbb{F}$ has p^r elements.

Consider the field $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z} = \{0, 1\}$

Let $f(x) = x^3 + x^2 + 1 \in \mathbb{F}_2[x]$.

If f is reducible over $\mathbb{F}_2$, then it has a root in $\mathbb{F}_2$.

But $f(0) = 1$

$f(1) = 1$

So f has no root in $\mathbb{F}_2$.

$\Rightarrow$ f is irr. over $\mathbb{F}_2$. $\deg = \deg f = 3$.

Consider $K = \mathbb{F}_2[x]/(f(x))$.

Now K is a field of $\mathbb{F}_2$.

deg 5 ...

So K has 8 elements.

(Existence and uniqueness of finite fields :-

- Let $n > 0$ be any +ve integer and consider K a splitting field of the polynomial $x^q - x \in \mathbb{F}_p[x]$ where $q = p^n$.

We will prove next time that this poly is separable, so if has distinct roots.

- Let α, β be roots of $x^q - x$ in K.

ie $\alpha^q = \alpha$ $\beta^q = \beta$

$(\alpha+\beta)^q = \alpha^q + \beta^q = \alpha + \beta$

(All the other terms in the expansion are divisible by p and hence 0 in K)

$(\alpha\beta)^q = \alpha^q \beta^q$, $(\alpha^{-1})^q = \alpha^{-1}$

$= \alpha\beta$

$\Rightarrow$ { roots of $x^q - x$ } in K is

a subfield of K.

$\Rightarrow$ K has q elements.

$\Rightarrow$ $[K : \mathbb{F}_p] = n$.

$\Rightarrow$ K = finite fields of deg n over $\mathbb{F}_p$ $\forall\, n > 0$.

Conversely, let F be field of order q. Then $|F^\times| = q-1$.

$\Rightarrow$ $\alpha^{q-1} = 1$ $\forall\, \alpha \in F^\times$.

$\Rightarrow$ $\alpha^q = \alpha$ $\forall\, \alpha \in F$.

$\Rightarrow$ $F \subseteq$ splitting field of $x^q - x$.

has q elements by what we discussed before

$\Rightarrow$ F is a splitting field of $x^q - x$.