Lecture 3:-

Separable, normal and Galois extns:-

Let F be a field and $f(x) \in F[x]$. Over a splitting field, K, we have

$$f(x) = C\,(x-\alpha_1)^{n_1}(x-\alpha_2)^{n_2}\cdots(x-\alpha_k)^{n_k}$$

where $\alpha_1, \ldots, \alpha_k$ are distinct elements of K and $n_i \geq 1$.

Defn:- α_i is multiple if $n_i > 1$
α_i is simple if $n_i = 1$.

Defn:- A polynomial f is separable if it has no multiple roots ie all its roots are distinct.

Criterion:-

Given $f(x) = a_0 + a_1 x + \cdots a_n x^n$, let

$$f'(x) := a_n n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \cdots 2a_2 x + a_1 \in F[x].$$

Note:- $(f+g)' = f' + g'$
$(fg)' = f'g + fg'$.

Prop:- A polynomial f has α as a multiple root iff α is also a root of f'. ie min poly of α divides both f and f'. will hold in a splitting field.

Pf :- ($\Rightarrow$) $\quad f(x) = (x-\alpha)^n g(x)$, $n > 1$ (over a splitting field)

Then $f'(x) = \boxed{n}(x-\alpha)^{n-1} g(x) + (x-\alpha)^n g'(x)$

$f'(\alpha) = 0$.

$\Rightarrow \alpha$ is a root of f'

($\Leftarrow$) Suppose α is a root of both f and f'

Then $f(x) = (x-\alpha)h(x)$

$f'(x) = h(x) + (x-\alpha)h'(x)$

But $f'(\alpha) = 0 \Rightarrow h(\alpha) = 0$

$\Rightarrow h(x) = (x-\alpha)h_1(x)$

$\Rightarrow f(x) = (x-\alpha)^2 h_1(x)$ in $K[x]$

Eg (1) Consider $f(x) = x^{p^n} - x \in \mathbb{F}_p[x]$.

$f'(x) = -1$ has no roots at all

$\Rightarrow f$ is separable over $\mathbb{F}_p$.

(2) $f(x) = x^n - 1 \in F[x]$.

$f'(x) = nx^{n-1}$.

When char$(F) \nmid n$, f is separable.

Otherwise if it is not, $f' \equiv 0$.

t is indeterminate.

(3) $F = \mathbb{F}_p(t)$

(3) ...

Consider $x^p - t$. Go to a splitting field which contains $\alpha \ni \alpha^p = t$ and then $x^p - t = (x-\alpha)^p$ in a splitting field.

Consequence:-
Every irr poly over a field of char 0 is separable. A poly. over such a field is separable $\iff$ if is a product of distinct irr. polynomials.

Pf:- $f(x)$ is irr. say of deg n.
What is deg $f'(x)$?
$n-1 < n$

$\Rightarrow f$ and f' are relatively prime.

Groups of auto. of fields:-
Suppose K/F is a finite extn.
$\text{Aut}(K/F) = \{\sigma : K \to K \mid \sigma$ is an automorphism and $\sigma(x) = x \ \forall x \in F\}$.

Fact:- Let K/F be a finite extn. Let $\alpha \in K$ and let $f(x) \in F[x]$. be $\ni f(\alpha) = 0$
$\forall \sigma \in \text{Aut}(K/F)$.

Then $\boxed{f(\sigma(\alpha)) = 0}$

Note: $\sigma(f) = f$.

$\Rightarrow$ $a_0 + a_1\alpha + \cdots a_n\alpha^n = 0$.

Then $\sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots \sigma(a_n)\sigma(\alpha)^n = 0$

$\Rightarrow$ $a_0 + a_1\sigma(\alpha) + \cdots a_n\sigma(\alpha)^n = 0$

Eg: $\mathrm{Aut}\left(\boxed{\mathbb{Q}(\sqrt{2})}/\mathbb{Q}\right) = \mathrm{Aut}(\mathbb{Q}(\sqrt{2}))$ $\boxed{x^2 - 2}$

$\boxed{\sqrt{2}} \to \sqrt{2}$

$\sqrt{2} \to -\sqrt{2}$.

$\{1, \sqrt{2}\}$ $\quad \sigma$

$\subseteq \mathbb{R}$ $\quad x^3 - 2$

$\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}\right)$ $\quad \sqrt[3]{2},\ \underline{\xi_3\sqrt[3]{2},\ \xi_3^2\sqrt[3]{2}}$

$\sqrt[3]{2} \xrightarrow{?} \text{any other root of } x^3-2 \text{ in } \mathbb{Q}(\sqrt[3]{2})$

$\| $

1.

$= \sqrt[3]{2}$

Exercise: $\boxed{\mathrm{Aut}\left(\mathbb{Q}(\sqrt[3]{2}, \xi_3)/\mathbb{Q}\right) = S_3}$.

$[\mathbb{Q}(\sqrt[3]{2}, \xi_3) : \mathbb{Q}] = 6$

Counting field hom:

(1) Suppose $K = \boxed{F(\alpha)}$ is a primitive

... min poly f ...

outm with be a field hom.

Let $\sigma : F \to L$

The set of F-hom $\tilde{\sigma} : K \to L$ whose restriction to F is σ is in bijection with the set of roots of $\sigma(f)$ in L.

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

<u>Why is this true?</u>

If $\tilde{\sigma}$ is such a hom

Then $\tilde{\sigma}(\alpha)$ should be a root of $\sigma(f)$.

$K = F(\alpha)$

$f(\alpha) = 0$.

$\tilde{\sigma}(f(\alpha)) = 0$

$\tilde{\sigma}(f)(\tilde{\sigma}(\alpha)) = 0$

$\sigma(f)(\tilde{\sigma}(\alpha)) = 0$

On the other hand, if β is a root of $\sigma(f)$ in L then

$$K = F(\alpha) \cong \frac{F[x]}{(f(x))} \xrightarrow{\sigma} \frac{F'[x]}{(\sigma(f))} \xrightarrow{\sim} F'(\beta) \subseteq L$$

(Here $F' = \sigma(F)$)

If $\sigma(f)$ has distinct roots in L

then $\# \tilde{\sigma} = \deg f = [K : F]$, $K = F(\alpha)$

More generally:

<u>Thm</u>: Consider the diagram

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

with $K/\mathcal{F}$ a finite extn and $\sigma : \mathcal{F} \to L$ a field hom.

$$\{\# \tilde{\sigma} : K \to L \mid \tilde{\sigma}|_{\mathcal{F}} = \sigma\} \leq [K : \mathcal{F}]$$

and equality holds $\iff$

(1) $K/\mathcal{F}$ is separable extn.

(2) If $f(x) \in \mathcal{F}[x]$ is the min poly of some $\alpha \in K$, then $\sigma(f)$ splits in $L[x]$.

$\forall\, \alpha \in K$, the min poly of α, say f_α is $\ni$ $\sigma(f_\alpha)$ splits into distinct linear factors in L.

Remark:- An element $\alpha \in K$ is separable over $\mathcal{F}$ if its min poly is separable. An extn $K/\mathcal{F}$ is separable if every element of K is separable over $\mathcal{F}$.

Sketch of Pf:-

When $K_1 = \mathcal{F}(\alpha)$, we just proved this.

To count $\# \tilde{\sigma} : K \to L$ whose $\ldots\ \mathcal{F}$ is σ, we could restriction to " whose

(a) Count # $\sigma_1 : K_1 \to L$ whose restriction to $\mathcal{F}$ is σ

(b) Count # $\tilde{\sigma} : K \to L$ whose restriction to K_1 is σ_1.

We have done (a) and for (b), set up an induction argument.

Corollary :- If K is the splitting field over $\mathcal{F}$ of a polynomial $f(x) \in \mathcal{F}[x]$. Then
$$|\mathrm{Aut}(K/\mathcal{F})| \le [K:\mathcal{F}]$$
and equality holds if $K/\mathcal{F}$ is separable.

Defn :- Let $K/\mathcal{F}$ be a finite extn. Then $K/\mathcal{F}$ is Galois if $|\mathrm{Aut}(K/\mathcal{F})| = [K:\mathcal{F}]$.

In this case, $\mathrm{Aut}(K/\mathcal{F}) = \mathrm{Gal}(K/\mathcal{F})$.

Normal extns :-

An extn $K/\mathcal{F}$ is normal if for every irr $f(x) \in \mathcal{F}[x]$ that has one root in K, splits into factors in K.

linear ... but not

Eg: (1) $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is sep. normal.

(2) $\mathbb{F}_p(t) \subseteq \underline{\mathbb{F}_p(\alpha)}$ with $\alpha^p = t$ $\quad x^p - t$

α is a root of $x^p - t$;

In $\mathbb{F}_p(\alpha)$, $x^p - t = (x-\alpha)^p$.

(Work out the details here).

(3) $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ is not normal.

(An extn K/F is Galois if it is finite, normal and separable)

is not Galois

$$\underbrace{\mathbb{Q}(\sqrt[4]{2}) \supseteq \mathbb{Q}(\sqrt{2})}_{\text{Galois}} \xrightarrow{x^2-\sqrt{2}} \underbrace{\mathbb{Q}(\sqrt{2}) \supseteq \mathbb{Q}}_{\text{Galois}}$$

(4)
$$\begin{tikzcd}
\mathbb{Q}(\sqrt[3]{2}, \boxed{\zeta_3}) \arrow[d, "2"] \arrow[dd, bend right, "\text{Galois}"'] \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[d] \\
\mathbb{Q}
\end{tikzcd}$$

Galois $\quad \zeta_3 \to \zeta_3^2$, $\downarrow$ $\mathbb{Q}(\sqrt[3]{2})$

not Galois

In general, if $F \subseteq K \subseteq L$ and L/F is Galois, then L/K is Galois.

is necessarily Galois.

But K/F need not be Galois

In fact K/F is Galois

$\iff$ $\mathrm{Aut}(L/K) \trianglelefteq \mathrm{Aut}(L/F)$

Consider $\mathbb{F}_{p^n}/\mathbb{F}_p$ constructed last time as ~~the~~ a splitting field $x^{p^n} - x$.

$$\sigma : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$$
$$x \longrightarrow x^p .$$

This map is injective, so it is also surjective

Does it fix $\mathbb{F}_p$? It fixes $\mathbb{F}_p$.

$\sigma \in \mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) \leq n$

What is the order of σ?

For $\alpha \in \mathbb{F}_{p^n}$, $\sigma(\alpha) = \alpha^p$

$\sigma^2(\alpha) = \alpha^{p^2}$

$\vdots$

$\sigma^n(\alpha) = \alpha^{p^n} = \alpha$

Order of $\sigma \mid n$. ... has

Check that σ is of order n.

So $\left|\underbrace{\mathrm{Aut}\left(\mathbb{F}_{p^n}/\mathbb{F}_p\right)}_{\langle\sigma\rangle}\right| = n.$

Frobenius automorphism