Lec 20 2/26/2021

Separable + normal extensions

Def. Let $F \subseteq K$ we define

$$\mathrm{Aut}(K) = \{\sigma : K \to K \mid \sigma \text{ is an aut. of } K \text{ (as ring)}\}$$

as a group under $\circ$.

$$\mathrm{Gal}(K/F) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(a) = a \ \forall a \in F\}$$

every $\sigma \in \mathrm{Gal}(K/F)$ fixes F.

"the Galois group of K over F".

(subgroup of $\mathrm{Aut}(K)$).

Suppose $f \in F[x]$, and $\sigma \in \mathrm{Gal}(K/F)$.

if $\alpha \in K$ is a root of f, then

$\sigma(\alpha)$ is a root of f. So σ permutes the roots of f in K.

$$f = \sum_{i=0}^{n} a_i x^i \qquad f(\alpha) = 0$$

$$0 = \sum_{i=0}^{n} a_i \alpha^i \qquad \text{apply } \sigma$$

$$0 = \sum_{i=0}^{n} \sigma(a_i)\,\sigma(\alpha)^i \qquad \sigma(a_i) = a_i \ \forall i$$

$$= \sum_{i=0}^{n} a_i\,\sigma(\alpha)^i$$

$$= f(\sigma(\alpha))$$

Def. A finite degree extension $F \subseteq K$ is **Galois** if $|\mathrm{Gal}(K/F)| = [K:F]$.

Ex. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{C}$.

$f = x^3 - 2 = \mathrm{minpoly}_{\mathbb{Q}}(\sqrt[3]{2})$

its roots in $\mathbb{C}$ are $\sqrt[3]{2}$, $\sqrt[3]{2}\psi$, $\sqrt[3]{2}\psi^2$

$\psi = e^{\frac{2\pi i}{3}}$ $\qquad \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$.

So $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in $\mathbb{Q}(\sqrt[3]{2})$

So if $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$

then $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$.

so $\sigma = 1_{\mathbb{Q}(\sqrt[3]{2})}$.

So $|\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| = 1 \neq [\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]$

Ex. $F = \mathbb{F}_2(y)$

$f = x^2 - y \in F(x)$

K = splitting field of f over F.

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

satisfies $\alpha^2 = y$. $((x-\alpha)^2 = x^2 - \alpha^2 = x^2 - y)$

So $K = F(\alpha)$.

if $\sigma \in \mathrm{Gal}(K/F)$ $\sigma(\alpha) = \alpha$.

So $\sigma = 1_K$

$|\mathrm{Gal}(K/F)| = 1 \neq [K:F] = 2$.

Def. $F \subseteq K$ alg. extension.

We say K/F is *separable* if for all $\alpha \in K$, $\min\text{poly}_F(\alpha)$ is separable.

Def. $F \subseteq K$ alg. extension

We say K/F is *normal* if for all $\alpha \in K$, $\min\text{poly}_F(\alpha)$ splits in $K[x]$.

Basic props –

if $F \subseteq E \subseteq K$

if K/F is separable, so are E/F and K/E.

if K/F is normal, so is K/E. (maybe not E/F).

Lemma. if $F \subseteq K$, $[K:F] < \infty$.
Then K/F is normal iff K is a splitting field over F for some $f \in F[x]$.

Pf. Let K be a splitting field of $f \in F(x)$ over F.

$$f = c(x-\alpha_1)\cdots(x-\alpha_m) \in K[x]$$

$$K = F(\alpha_1, \ldots, \alpha_m).$$

Take $g \in F[x]$ irreducible over F with a root $\beta_1 \in K$. $g(\beta_1) = 0$.
We need g splits over K.

Take a splitting field L for g over K. so in $L[x]$ $g = d(x-\beta_1)\cdots(x-\beta_n)$

$$L = K(\beta_1, \ldots, \beta_n).$$

look at $L = F(\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n)$.

Note that L is a splitting field over F of fg.

Now if β_1 is a root of g, there is an automorphism σ_i of L s.t. $\sigma_i(\beta_1) = \beta_i$ for all i. Also $\sigma_i \in \mathrm{Gal}(L/F)$

$\in K$, σ permutes the roots of f, so $\sigma(K) \subseteq K$ since K is generated by the α_i.

So $\beta_i \in K$ for all i.

Forces $K = L$ and so g already splits over K.

Converse skipped.

Ex. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \zeta) = K.$

$\zeta := e^{2\pi i/3}$

K = splitting field of $x^3 - 2$ over $\mathbb{Q}$.

So $K/\mathbb{Q}$ is normal.

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

Thm. $F \subseteq K$ $[K:F] < \infty$.

1. $|\mathrm{Gal}(K/F)| \leq [K:F]$.

2. TFAE.

(i) K/F is Galois.

(ii) K/F is normal + separable.

(iii) K is a splitting over F of a separable poly $f \in F[x]$.

pf. Idea. $[K:F] \geq 2$.

Pick $\alpha_1 \in K - F$ and

let $g = \text{minpoly}_F(\alpha_1) \in F(x)$.

g has roots $\{\alpha_1, \ldots, \alpha_m\}$ in K.

Suppose for some i there is

$\sigma_i \in \text{Gal}(K/F)$ $\sigma_i(\alpha_1) = \alpha_i$.

If $\tau \in \text{Gal}(K/F)$ then

$\tau(\alpha_1) = \alpha_i$ some i

then $(\sigma_i)^{-1}\tau(\alpha_1) = \alpha_1$.

So $(\sigma_i)^{-1}\tau \in \text{Gal}(K/F(\alpha_1))$

(iii) $\Rightarrow$ (i).

K is a splitting field of

a separable poly $f \in F(x)$.

Let g be an irreducible factor of f, $\deg g \geq 2$,

$$g = c(x-\alpha_1)\cdots(x-\alpha_m)$$

$\alpha_i \in K$ distinct

For each i, there is $\sigma_i \in \mathrm{Gal}(K/F)$

$\sigma_i(\alpha_1) = \alpha_i$;

Also, K is a splitting field of f over $F(\alpha_1)$.

By induction, $K/F(\alpha_1)$ is Galois. $|\mathrm{Gal}(K/F(\alpha_1))|$

$= [K : F(\alpha_1)]$.

$|\{\sigma_1, \ldots, \sigma_m\}| = m = [F(\alpha_1) : F]$

if $H = \mathrm{Gal}(K/F(\alpha_1))$

$\sigma_1 H, \ldots, \sigma_m H$ are disjoint.

$$|G| \geq m\,|H|$$

$$[F(\alpha_1):F][K:F(\alpha_1)]$$

$$= [K:F].$$

□.