Lec 21 3/1/2021

Fundamental Thm of Galois Theory.

Let $F \subseteq K$ be a field extension.

Let $G = \mathrm{Gal}(K/F)$

$$\left\{\begin{array}{l}\text{intermediate fields } E \\ \text{w/ } F \subseteq E \subseteq K\end{array}\right\} \underset{\Phi = \mathrm{Fix}(-)}{\overset{\Gamma = \mathrm{Gal}(K/-)}{\rightleftarrows}} \left\{\begin{array}{l}\text{subgroups } H \\ \text{of } G\end{array}\right\}$$

$$\Gamma : E \longrightarrow \underbrace{\mathrm{Gal}(K/E)}_{\text{a subgroup of } G}$$

a subgroup of G.

$\mathrm{Fix}(H) = \{ a \in K \mid \sigma(a) = a \ \forall \sigma \in H \}$.

is a subfield of K containing F, so

$F \subseteq \mathrm{Fix}(H) \subseteq K$.

<u>Goal</u>: when $F \subseteq K$ is Galois ($[K:F] < \infty$) then Γ, Φ are inverse

bijections of sets.

<u>Ex.</u> K splitting field of x^3-2 over $\mathbb{Q}$

$K = \mathbb{Q}(\alpha = \sqrt[3]{2}, \varphi = e^{2\pi i/3})$

$f = x^3 - 2 = (x-\alpha)(x-\alpha\varphi)(x-\alpha\varphi^2)$ in $\mathbb{C}[x]$.

$K/\mathbb{Q}$ is Galois since it is the splitting field of f. $|\mathrm{Gal}(K/\mathbb{Q})| = [K:\mathbb{Q}] = 6$

Any $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ sends α to another root of x^3-2

and sends φ to another root of $x^2+x+1 = \mathrm{minpoly}_{\mathbb{Q}}(\varphi)$.

Also σ is determined by where it sends α, φ

So all choices occur.

$\sigma(\alpha) = \alpha\varphi \qquad \tau(\alpha) = \alpha$.

$\sigma(\varphi) = \varphi \qquad \sigma(\varphi) = \varphi^2$

Check that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

since σ, τ don't commute.

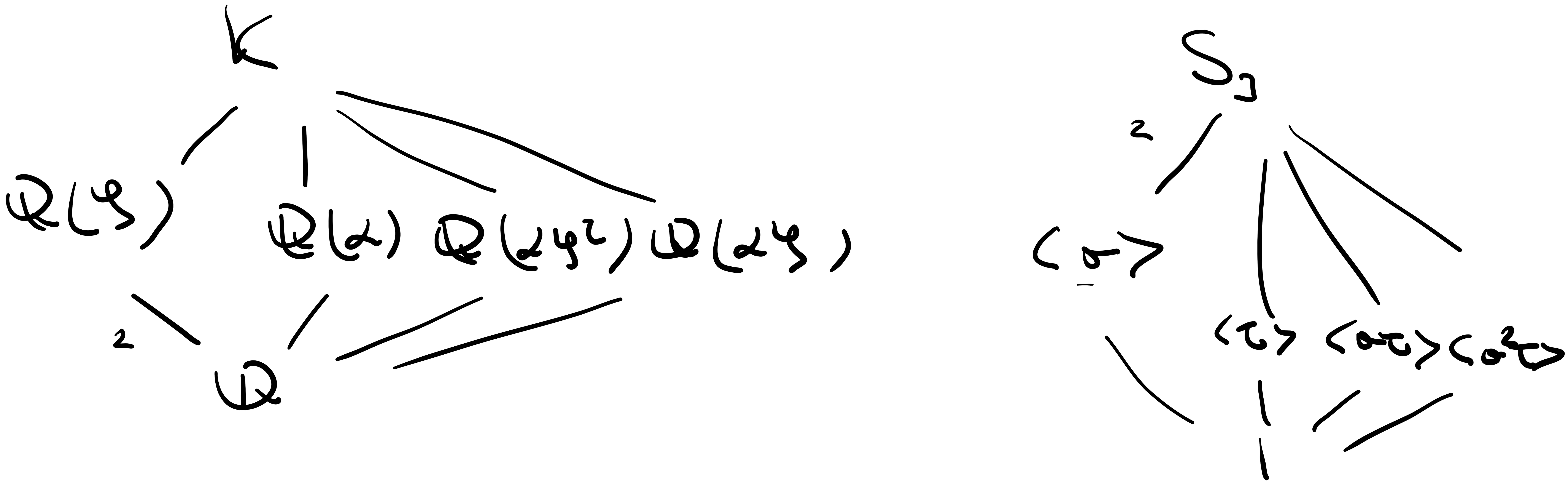
$o(\sigma) = 3$, $H = \langle \sigma \rangle$ $|H| = 3$.

Check $\mathrm{Fix}(H) = \mathbb{Q}(\varphi)$

$o(\tau) = 2 \quad \mathrm{Fix}(\langle \tau \rangle) = \mathbb{Q}(\alpha)$

$o(\sigma\tau) = 2 \quad \mathrm{Fix}(\langle \sigma\tau \rangle) = \mathbb{Q}(\alpha\varphi^2)$

$o(\sigma^2\tau) = 2 \quad \mathrm{Fix}(\langle \sigma^2\tau \rangle) = \mathbb{Q}(\alpha\varphi)$



Lemma. $F \subseteq K$ Galois, $[K:F] < \infty$.
if $F \subseteq E \subseteq K$, then K/E is Galois
and $\Phi\Gamma(E) = \mathrm{Fix}\,\mathrm{Gal}(K/E) = E$.

Pf. Since K/F is Galois, it is normal and separable. Then K/E is also normal and separable, so K/E is Galois.

Let $E' = \mathrm{Fix}\,\mathrm{Gal}(K/E) \supseteq E$.

K/E' is Galois, for the same reason.

Now

$[K:E] = |\mathrm{Gal}(K/E)| \quad |\mathrm{Gal}(K/E')| = [K:E']$

But $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/E')$ —

$\mathrm{Gal}(K/E') \subseteq \mathrm{Gal}(K/E)$. by def.

if $\sigma \in \mathrm{Gal}(K/E)$, then σ fixes E'

So $\mathrm{Gal}(K/E) \subseteq \mathrm{Gal}(K/E')$.

So $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/E')$.

So $[K:E] = [K:E'] \Rightarrow$

$[E':E] = 1$, so $E = E'$.

<u>Cor.</u> If $[K:F] < \infty$ with K/F separable. Then $K = F(\underline{\gamma})$ for some $\gamma \in K$.

<u>Pf.</u> Recall that the existence of γ is equivalent to there being finitely many fields E with $F \subseteq E \subseteq K$.

if K/F is Galois, any such $E = \mathrm{Fix}\,\mathrm{Gal}(K/E) = \mathrm{Fix}\,H$ for a subgroup H of $G = \mathrm{Gal}(K/F)$, and there are finitely many H.

if K/F is just separable, then there is $K \subseteq L$ s.t. L/F is Galois and $[F:L] < \infty$. If $K = F(\alpha_1, \dots, \alpha_m)$

Take L = splitting field over K of

$f = \prod_i \text{minpoly}_F(\alpha_i)$ and then L is also splitting field over K of g which is separable ($g = f$ with any repeats removed).

Since L/F has finitely many intermediate fields, so does K/F.

Lemma. K/F Galois, $[K:F] < \infty$.

$H \subseteq \text{Gal}(K/F)$ a subgroup s.t.

$\text{Fix}(H) = F$.

① For $\alpha \in K$, let

$O_\alpha = \{\sigma(\alpha) \mid \sigma \in H\}$.

Then $\text{minpoly}_F(\alpha) = \prod_{\beta \in O_\alpha} (x - \beta)$.

② $H = \text{Gal}(K/F)$.

Pf ① $f = \prod_{\beta \in O_\alpha} (x - \beta) \in K[x]$

We want $f \in F[x]$.

For $\sigma \in H$, we apply σ to f

$$\sigma(f) = \prod_{\beta \in \Theta_\alpha} (x - \sigma(\beta))$$

$$= \prod_{\beta \in \Theta_\alpha} (x - \beta)$$ since σ permutes Θ_α.

So coefficients of f are fixed by all $\sigma \in H$. So $f \in (\mathrm{Fix}\, H)[x]$
$= F[x]$

- check f is irreducible over F.
- $\underline{f}$ is separable.

(2) Since $F \subseteq K$ is Galois, $K = F(\gamma)$ some γ.

So $|\mathrm{Gal}(K/F)| = [K:F]$

$= [F(\gamma):F] = \deg \mathrm{minpoly}_F(\gamma)$

$\leq |H|$. So $|G| \leq |H|$

So $H = G = \mathrm{Gal}(K/F)$.

Thm (Fund Thm of Galois Theory)

$F \subseteq K$, $[K:F] < \infty$, K/F Galois.

① Γ, Φ defined above are inverse bijections

$$\left\{ \begin{array}{c} E \text{ s.t.} \\ F \subseteq E \subseteq K \end{array} \right\} \underset{\Phi = \mathrm{Fix}(-)}{\overset{\Gamma = \mathrm{Gal}(K/-)}{\rightleftarrows}} \left\{ \begin{array}{c} \text{subgroups } H \\ \text{of } \mathrm{Gal}(K/F) \end{array} \right\}$$

② $[K:E] = |\mathrm{Gal}(K/E)|$ and
$[E:F] = |G : \mathrm{Gal}(K/E)|$.

③ E/F is normal (and thus Galois)
iff $H = \mathrm{Gal}(K/E)$ is normal
in $G = \mathrm{Gal}(K/F)$.

Pf.

① $\Phi\Gamma = 1$ int. fields by an earlier lemma.

$$\Gamma\Phi(H) = \mathrm{Gal}\left(K/_{\mathrm{Fix}(H)}\right) \supseteq H.$$

Apply previous result to

$\text{Fix}(H) \subseteq K$.

$H \subseteq \text{Gal}(K/\text{Fix}(H))$ and

$\text{Fix}(H) = \text{Fix}(H)$

Lemma says $H = \text{Gal}(K/\text{Fix}(H))$.

$\Gamma \Phi = 1_{\text{subgroups}}$.

(2) K/E is also Galois so

$[K:E] = |\text{Gal}(K/E)|$

since $[K:F] = [E:F][K:E]$

so $[E:F] = \dfrac{|\text{Gal}(K/F)|}{|\text{Gal}(K/E)|}$

$= [G : \text{Gal}(K/E)]$

(3) prove it by looking at

$$\phi: \mathrm{Gal}(K/F) \longrightarrow \mathrm{Gal}(\underline{\underline{E}}/F)$$
$$\sigma \longmapsto \sigma|_{\underline{E}}$$

and prove this is a homomorphism when E/F is normal.

$\ker\phi = \mathrm{Gal}(K/\underline{E}) \triangleleft G.$