Exam Problem 2019

a) Let K be the splitting field of x^3-2 over $\mathbb{Q}$. Find $[K:\mathbb{Q}]$ and the Galois group $\underline{G(K/\mathbb{Q})}$

$= 6$ $\cong S_3$

b) Let K be the splitting field over $\mathbb{Q}$ of $f(x) \in \mathbb{Q}[x]$ where $f(x)$ irreducible, $\deg f(x) = 3$. Let A_3 denote the alternating subgroup of S_3. Show $G(K/\mathbb{Q}) = A_3$ if and only if $K = \mathbb{Q}(\alpha)$ for α any root of $f(x)$. (Recall that $A_3 \leq S_3$ consisting of even permutations in particular $[S_3 : A_3] = 2$, $A_3 \trianglelefteq S_3$ normal)

If $K = \mathbb{Q}(\alpha)$ then $[K : \mathbb{Q}] = 3 = |G(K/\mathbb{Q})|$ since K is a finite normal extension

α has 3 conjugates $\alpha_1 = \alpha, \alpha_2, \alpha_3$ and any $\sigma \in G(K/\mathbb{Q})$ gives a permutation of them.

$G(K/\mathbb{Q}) \leq S_3$ The only subgp of order 3 of S_3 is $A_3 = \{ id, (1,2,3), (1,3,2)\}$.

If $G(K/\mathbb{Q}) = A_3$ $\quad 3 = |G(K/\mathbb{Q})| = [K : \mathbb{Q}]$

$\mathbb{Q} \leq \mathbb{Q}(\alpha) \leq K$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$

$\Rightarrow [K : \mathbb{Q}(\alpha)] = 1 \Rightarrow K = \mathbb{Q}(\alpha)$.

c) Conclude all roots of $f(x)$ from part b) must be in $\mathbb{R}$.

We must have at least one zero $\alpha \in \mathbb{R}$.

If $K = \mathbb{Q}(\alpha) = \{ a_0 + a_1\alpha + a_2\alpha^2 \mid a_i \in \mathbb{Q} \}$

If K is splitting field $\overset{\alpha}{\overset{\shortparallel}{\alpha_1}}, \alpha_2, \alpha_3 \in K$ but

$K \stackrel{*}{=} \mathbb{Q}(\alpha) \leq \mathbb{R}$ so all roots are real.

<u>Finite Fields</u> Let $|F| = p^r$ and $[K:F] = n$. p prime

then $|K| = p^{rn}$.

Recall F is perfect so K is separable.

Moreover

$K = \{ \alpha \mid \alpha \text{ zero of } x^{p^{rn}} - x \} \leq \overline{F}$

so K is a splitting field. K is a finite normal extension of F.

Recall $\sigma_{p^r} : K \to K$ $\quad \sigma_{p^r}(\alpha) = \alpha^{p^r}$ fixes F

so $\sigma_{p^r} \in G(K/F)$.

Thm 53.7 Let K be a finite extension of degree n of a finite field F $|F| = p^r$. Then
p prime.

$$G(K/F) = \langle \sigma_{p^r} \rangle$$

Proof $|G(K/F)| = [K : F] = n$.

What is the order of σ_{p^r}?

Suppose $\sigma_{p^r}^{\,i} = \sigma_{p^r} \circ \dots \circ \sigma_{p^r} = id \Rightarrow \forall\ \alpha \in K$

$\sigma_{p^r}^{\,i}(\alpha) = \alpha \iff \alpha^{p^{ri}} = \alpha \iff \alpha$ is a zero of $x^{p^{ri}} - x$

This poly. has at most p^{ri} distinct zeros but $|K| = p^{rn}$ so

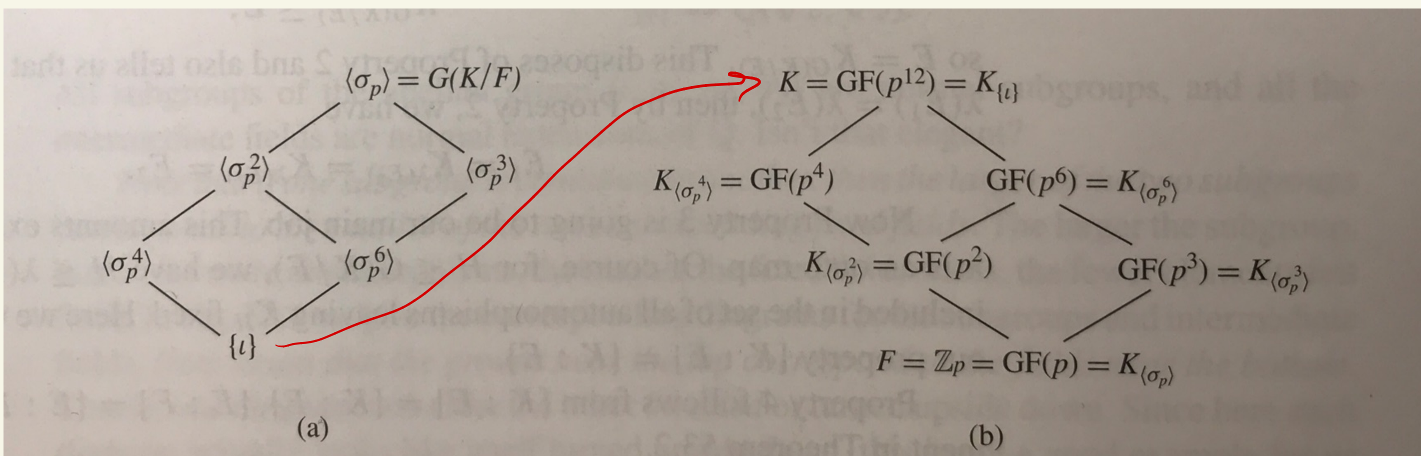
$$n \leq |\operatorname{ord}(\sigma_{p^r})| = |\langle \sigma_{p^r} \rangle| \leq |G(K/F)| = n$$

$\Rightarrow \langle \sigma_{p^r} \rangle = G(K/F)$. Hence the Galois group is cyclic $\square$.

Example $F = \mathbb{Z}_p$ $K = GF(p^{12})$ $[K:F] = 12$. $\boxed{n=12}$

$G(K/F) = \langle \sigma_p \rangle \cong \langle \mathbb{Z}_{12}, + \rangle$

distinct subgps are $\langle \mathrm{Id} \rangle$, $\langle \sigma_p^2 \rangle$, $\langle \sigma_p^3 \rangle$, $\langle \sigma_p^4 \rangle$, $\langle \sigma_p^6 \rangle$, $\langle \sigma_p \rangle$



(a) (b)

Galois Theorem (restated)

Let K be a finite normal extension of F with Galois group $G(K/F)$

(text points 1, 2, 3, 5)

1) There is an inclusion-reversing bijection

$$\lambda : \left\{ \begin{matrix} \text{intermediate} \\ \text{fields } F \leq K \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{subgroups of} \\ G(K/F) \end{matrix} \right\}, \quad \lambda(E) = G(K/E)$$

satisfying $[K:E] = |G(K/E)|$ and $[E:F] = (G(K/F) : G(K/E))$.

2) Let $F \leq E \leq K$ then E is a normal extension of F if and only if $G(K/E)$ is a normal subgroup of $G(K/F)$

When $G(K/E) \leq G(K/F)$ is normal then $G(E/F) \cong G(K/F)/G(K/E)$.

(text pt 4)

Proof <u>Claim</u>: $\lambda^{-1} : \left\{ \begin{matrix} \text{subgroups of} \\ G(K/F) \end{matrix} \right\} \longrightarrow \left\{ \begin{matrix} \text{intermediate} \\ \text{fields } F \leq K \end{matrix} \right\}$ $\lambda^{-1}(H) = K_H$

Recall $K_H = \{ \alpha \in K \mid \sigma(\alpha) = \alpha \ \ \forall \ \sigma \in H \leq G(K/F) \}$ "fixed field of H"

<u>First show $\lambda^{-1}\lambda = \text{id}$</u> ie. want to show $\lambda^{-1}\lambda(E) = K_{G(K/E)} = E$

We have $E \leq K_{G(K/E)}$. Now suppose $\alpha \in K$ $\alpha \notin E$ then $\psi_{\alpha,\alpha'}$ conjugation iso extends to $\tau : K \to K$ fixing E so
$\alpha \neq \alpha'$
$\tau \in G(K/E)$ $\tau(\alpha) = \alpha' \neq \alpha$ $\alpha \notin K_{G(K/E)} \Rightarrow K_{G(K/E)} \leq E$

Hence $E = K_{G(K/E)}$ so $\lambda^{-1}\lambda = \text{id}$ and λ is injective

$\underline{\text{Second show: } \lambda\lambda^{-1} = \mathrm{id}}$ i.e. $\lambda\lambda^{-1}(H) = G(K/K_H) = H$

We have $H \leq G(K/K_H)$. Suppose $H < G(K/K_H)$

By primitive elt theorem $\exists\ \alpha \in K$ st $K = K_H(\alpha)$

So $|G(K/K_H)| = [K : K_H] = \deg \operatorname{irr}(\alpha, K_H)$.

Define $f(x) = \prod_{i=1}^{|H|} (x - \sigma_i(\alpha))$ $\quad H = \{\sigma_1, \dots, \sigma_{|H|}\}$

$\sigma_i : K \to K$

- $f(\alpha) = 0$ since some $\sigma_i = \mathrm{id}$
- $f(x) \in K_H[x]$ $\quad f(x) = \sum_{j=0}^{|H|} a_j x^j$ $\quad a_{|H|} = 1$, $a_{|H|-1} = -\sum_{i=1}^{|H|} \sigma_i(\alpha)$, $a_{|H|-2} = \sum_{i \neq j} \sigma_i(\alpha)\sigma_j(\alpha)$

$a_k = (-1)^k \cdot \sum \sigma_{i_1}(\alpha) \cdots \sigma_{i_k}(\alpha)$

claim: $\sigma \in H$ then $\sigma(a_k) = a_k \Rightarrow a_k \in K_H$.

eg. $\sigma(a_{|H|-1}) = \sigma\left(-\sum_{i=1}^{|H|} \sigma_i(\alpha)\right) = -\left(\sum_{i=1}^{|H|} \sigma\sigma_i(\alpha)\right) \overset{(*)}{=} -\sum_{i=1}^{|H|} \sigma_i(\alpha)$

$= a_{|H|-1}$.

$H = \{\sigma_1, \dots, \sigma_{|H|}\}$ $\quad \sigma \in H$

$A = \{\sigma\sigma_1, \sigma\sigma_2, \dots, \sigma\sigma_{|H|}\} \subseteq \{\sigma_1, \dots, \sigma_{|H|}\} = H$.

suppose $\sigma\sigma_i = \sigma\sigma_j$ then $\sigma^{-1} \in H$ and so

$\sigma^{-1}\sigma\sigma_i = \sigma^{-1}\sigma\sigma_j \Rightarrow \sigma_i = \sigma_j$

So the set A is in fact all of H.

with these two claims we see

$$|G(K/K_H)| = [K : K_H] = [K_H(\alpha) : K] = \deg \operatorname{irr}(\alpha, K_H) \leq \deg f = |H|$$

$\Rightarrow$ $H = G(K/K_H)$. this proves λ is surjective.

This proves λ is a bijection.

Index = order Since K is ~~separable~~ splitting field over F K is also ~~separable~~ splitting field over E.

moreover, $[K : E] = \{K : E\} = |G(K/E)|$

$$[E : F] = \frac{[K : F]}{[K : E]} = \frac{|G(K/F)|}{|G(K/E)|} =: (G(K/F) : G(K/E)).$$

λ inclusion reversing $\quad E_1 \leq E_2 \quad \lambda(E_i) = G(K/E_i)$

$\sigma \in G(K/E_2)$ σ fixes E_2 hence fixes E_1 so

$\sigma \in G(K/E_1)$

Exercise show analogous statement for λ^{-1}.

This completes proof of statement 1).

normal $\Leftrightarrow$ normal $\quad E$ is normal over F iff E is a splitting field over F.

Next time!

Aside to recall even permutations.

$\sigma \in S_n$ then $\sigma = \tau_{i_1 j_1} \tau_{i_2 j_2} \cdots \tau_{i_k j_k}$ for some transpositions

but expression is not unique but the parity of # of transpositions multiplying to σ is constant.

Say σ is even if the k above is even

is odd otherwise.

e.g. $(1,2,3) = (1,2)(2,3)$ so $(1,2,3)$ is even

$A_n = \{\text{even permutations in } S_n\} \leq S_n$

subgroup