Exam Problem 2021

$f(x) = (x^2-2)(x^2-5) \in \mathbb{Q}[x]$

4a Find the zeros of $f(x)$ in $\mathbb{C}$ and determine the splitting field K of $f(x)$ over $\mathbb{Q}$.

Show $[K:\mathbb{Q}] = 4$. (You may use w/o proof that $x^4 - 14x^2 + 9$ is irreducible / $\mathbb{Q}$)

$x^2 - 2 \Rightarrow x = \pm\sqrt{2}$

$x^2 - 5 \Rightarrow x = \pm\sqrt{5}$

$\mathbb{Q}(\sqrt{2}, \sqrt{5}) = K$

$[K:\mathbb{Q}] = 4$

Proof: $[K:\mathbb{Q}] = \underbrace{[K:\mathbb{Q}(\sqrt{2})]} \cdot \underbrace{[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]}_{2}$

Need to show that 0's of x^2-5 is not in $\mathbb{Q}(\sqrt{2})$ to conclude that

$\operatorname{irr}(\pm\sqrt{5}, \mathbb{Q}(\sqrt{2})) = x^2-5$

show $\nexists\, a_0, a_1 \in \mathbb{Q}$ s.t.

$a_1\sqrt{2} + a_0 = \sqrt{5}$?

so $[K:\mathbb{Q}(\sqrt{2})] = \deg \operatorname{irr}(\pm\sqrt{5}, \mathbb{Q}(\sqrt{2})) = 2$

$\Rightarrow [K:\mathbb{Q}] = 2 \cdot 2 = 4$ $\boxtimes$

4b) Determine the group $G(K/\mathbb{Q})$ and write down diagrams of subgroups H of $G(K/\mathbb{Q})$ and subfields E of K obtained as fixed fields of H.

Separable Extensions §51

Recall $E \geq F$

$[E:F]$ = dimension of E as a vector space over F "degree of E/F"

$\{E:F\}$ = # of field isomorphisms $\tau : E \to \tau[E] \leq \overline{F}$ extending $id : F \to F$ (fixing F) "index of E/F"

$G(E/F) = \{ \tau : E \to E \mid \tau \text{ automorphism fixing } F \}$

When $[E:F] < \infty$ "E finite ext'n over F"

$$|G(E/F)| \leq \{E:F\} \leq [E:F].$$

Def 51.7 A finite ext'n E of F is a separable extension of F if $\{E:F\} = [E:F]$

An element $\alpha \in \overline{F}$ is separable over F if $F(\alpha)$ is a separable ext'n over F.

An irred $f(x) \in F[x]$ is separable over F if $\forall$ zero of $f(x)$ is separable over F.

$4 = [K:\mathbb{Q}] \geq$

Example $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$ is separable over $\mathbb{Q}$.

$\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is a splitting field $\Rightarrow |G(\mathbb{Q}(\sqrt{2},\sqrt{5})/\mathbb{Q})| = \underbrace{\{\mathbb{Q}(\sqrt{2},\sqrt{5}):\mathbb{Q}\}}_{K}$

$G(K/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\circ\tau = \tau\circ\sigma\}$

where

$\sigma(\sqrt{2}) = -\sqrt{2}$ $\quad \tau(\sqrt{5}) = -\sqrt{5}$ $\quad \tau\circ\sigma = \sigma\circ\tau = \gamma$

$\sigma(\sqrt{5}) = \sqrt{5}$ $\quad \tau(\sqrt{2}) = \sqrt{2}$ $\quad \gamma(\sqrt{2}) = -\sqrt{2}$

σ fixes $\mathbb{Q}$ $\quad \tau$ fixes $\mathbb{Q}$. $\quad \gamma(\sqrt{5}) = -\sqrt{5}$.

fix $\mathbb{Q}$

$|G(K/\mathbb{Q})| = 4 = \{K:\mathbb{Q}\} = [K:\mathbb{Q}]$

4b) Determine the group $G(K/\mathbb{Q})$ and write down diagrams of subgroups H of $G(K/\mathbb{Q})$ and subfields E of K obtained as fixed fields of H.

see above example where we showed

$G(K/\mathbb{Q}) = \{ id, \sigma, \tau, \sigma \circ \tau = \gamma \}$

Notice σ, τ, γ have order 2. $\Rightarrow$

$G(K/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ aka Klein 4-group.

By Lagrange any $H \leq G(K/\mathbb{Q})$ subgroup must have $|H|$ divides $|G(K/\mathbb{Q})| = 4$

If $|H| = 1$ $\quad H = \{id\}$

if $|H| = 2$ $\quad H = \{id, \overset{\langle \sigma \rangle}{\overset{\shortparallel}{\sigma}}\}$ or $\{id, \tau\}$ or $\{id, \gamma\}$.

if $|H| = 4$ $\quad H = G(K/\mathbb{Q})$.

Recall $K_H = \left\{ a \in K \;\middle|\; \begin{array}{l} \psi(a) = a \\ \forall \psi \in H \end{array} \right\}$

The subgroup diagram is:

$K_{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{5}) \leq K$.

$K_{\langle\tau\rangle} = \mathbb{Q}(\sqrt{2}) \leq K$

$K \neq K_{\langle\gamma\rangle} \geqslant \mathbb{Q}(\sqrt{10})$

since $\gamma(\sqrt{10}) = \gamma(\sqrt{2})\gamma(\sqrt{5}) = (-1)(-1)\sqrt{10} = \sqrt{10}$.

$$\begin{tikzcd}
 & G(K/\mathbb{Q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle\sigma\rangle \arrow[dr, dash] & \langle\tau\rangle \arrow[d, dash] & \langle\gamma\rangle \arrow[dl, dash] \\
 & \{id\} &
\end{tikzcd}$$

$$\text{deg } 4 \left[\begin{array}{c} K \\ | \neq \\ K_{\langle\gamma\rangle} \\ \shortparallel \\ \mathbb{Q}(\sqrt{10}) \\ | \\ \mathbb{Q} \end{array} \right. \quad \left. \begin{array}{c} \mathbb{Q}(\sqrt{10}) \\ \mathbb{Q} \end{array} \right] \text{deg } 2$$

to see $K_{\langle\gamma\rangle} = \mathbb{Q}(\sqrt{10})$ notice

implies $[K : \mathbb{Q}(\sqrt{10})] = 2$

so $[K_{\langle\gamma\rangle} : \mathbb{Q}(\sqrt{10})] = 1, 2$ but $\neq 2$ since $K \neq K_{\langle\gamma\rangle}$.

$id : K \to K$

$id(a) = a$

so $\quad K_{\langle \gamma \rangle} = \mathbb{Q}(\sqrt{10})$

$$K_{id} = K$$

$$K_{G(K/\mathbb{Q})} = \mathbb{Q}.$$

$$\begin{tikzcd}
 & G(K/\mathbb{Q}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\langle \sigma \rangle \arrow[dr, dash] & \langle \tau \rangle \arrow[d, dash] & \langle \gamma \rangle \arrow[dl, dash] \\
 & \{id\} &
\end{tikzcd}
\qquad
\begin{tikzcd}
 & \mathbb{Q} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{5}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(\sqrt{10}) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

This is the first example of a Galois correspondence

Thm 51.9 $F \leq E \leq K$ and $[K:E], [E:F] < \infty$.

K is separable over F if and only if K is separable over E and E is separable over F.

Proof For any fields $F \leq E$ $\{E:F\} \leq [E:F]$. and

$$\{K:F\} = \{K:E\}\{E:F\}$$
$$[K:F] = [K:E][E:F].$$

Corollary 51.10 $F \leq E$ $[E:F] < \infty$ then E is separable if and only if $\forall$ $\alpha \in E$ is separable over F.

Proof $E = F(\alpha_1, \dots, \alpha_k)$ when $[E:F] < \infty$. recursively use Thm 51.9

Example

$$\begin{array}{ccl} \mathbb{Q}(\sqrt{2}, \sqrt{5}) & = & K \\ | & & \\ \mathbb{Q}(\sqrt{2}) & = & E \\ | & & \\ \mathbb{Q}. & = & F \end{array}$$

separable over $\mathbb{Q}(\sqrt{2})$

separable over $\mathbb{Q}$

by Thm 51.9 K separable over $\mathbb{Q}$.

Example Let $E = F(\alpha)$

$\{F(\alpha) : F\} =$ # conjugats of α over F $=$ # distinct roots of $\text{irr}(\alpha, F)$. $\leq \deg \text{irr}(\alpha, F)$

$$[F(\alpha) : F] = \deg \text{irr}(\alpha, F)$$

Hence $F(\alpha)$ is separable if and only if all zeros of $\text{irr}(\alpha, F)$ have mult $= 1$.

Def 51.12 A field is <u>perfect</u> if every finite extension is a separable extension.

Thm 51.13 Every field of characteristic 0 is perfect

(ie: every E finite ext'n of F has $\{E:F\} = [E:F]$ when $\operatorname{char} F = 0$)

Thm 51.14 Every finite field is perfect.

Proof idea: Both thms reduce to showing that $F(\alpha)$ is separable over F for all $\alpha \in \overline{F}$ by Cor 51.10.

$$\begin{array}{c} E = F(\alpha_1, \dots, \alpha_k) \\ | \\ F(\alpha_1, \dots, \alpha_{k-1}) \\ | \\ \vdots \\ F(\alpha_1) \\ | \\ F \end{array}$$

$F(\alpha)$ is separable over F if and only if $\operatorname{irr}(\alpha, F) = f(x) \in F[x]$ has all zeros having multiplicity 1. i.e.

$$f(x) = \prod (x - \alpha_i) \quad \text{for } \alpha_i \in \overline{F}$$

where $\alpha_i \neq \alpha_j$ for $i \neq j$.

Example $E = \mathbb{Z}_p(y)$ $\quad$ char $E = p$ but $|E| = \infty$.

Let $t = y^p$. Then y is a zero of $f(x) = x^p - t \in F[x]$.

$$\operatorname{irr}(y, F) = x^p - t \quad (\text{Ex } 51.10).$$

(see that y is a zero of $x^p - t$)

$$\begin{array}{c} E = \mathbb{Z}_p(y) \\ | \\ F = \mathbb{Z}_p(t) \\ | \\ F' = \mathbb{Z}_p \end{array} \qquad [E : F'] = \infty$$

$$x^p - t = x^p - y^p = (x - y)^p$$

Freshman's dream

y is a zero of multiplicity p of $\operatorname{irr}(\alpha, \underbrace{\mathbb{Z}_p(t)}_{F})$.

$\{E : F\} = 1$ not separable.

$[E : F] = p$

Goal: Show $f(x) \in F[x]$ irreducible has zeros of mult 1 for $|F| = \infty$ or $\mathrm{char}(F) = 0$.

Thm 51.2 Let $f(x) \in F[x]$ be irreducible. Then all zeros of $f(x)$ have the same multiplicity.

Proof Let α, β be zeros. $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ conj. iso.

Corollary / Thm 51.6 $F \leq E$ and $[E:F] < \infty$ then $\{E:F\}$ divides $[E:F]$.

Lemma 51.11 let $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in F(x]$

If $(f(x))^m \in F[x]$ and $m \cdot 1 \neq 0$ in F then

$f(x) \in F[x]$ ie $a_i \in F$ for all i,

Proof By indication on r show $a_{n-r} \in F$.

$r=1$ $(f(x))^m = x^{mn} + (m \cdot 1) a_{n-1} x^{mn-1} + \dots$

Thm 51.13 Every field of characteristic 0 is perfect

Proof Suffices to show $\forall\ \alpha \in \overline{F}$ $\operatorname{irr}(\alpha, F)$ has distinct zeros. Let $f(x)$ be irreducible.

Thm 51.14 Every finite field is perfect.

Proof Again suffices to show zeros of irred poly's have mult 1. Suppose $f(x) \in F[x]$ is irred

let $g(x) = \prod(x - \alpha_i^{p^t})$ ← separable over F.
and has distinct zeros