

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

$$x^2 - 2 \Rightarrow x = \pm\sqrt{2} \quad x^4 - 14x^2 + 9 \text{ is irreducible over } \mathbb{Q}.)$$

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

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

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

$$\text{Proof: } [K: \mathbb{Q}] = \underbrace{[K: \mathbb{Q}(\sqrt{2})]} \cdot \underbrace{[\mathbb{Q}(\sqrt{2}): \mathbb{Q}]}_2$$

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

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

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

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

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

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

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

$$E \supseteq F$$

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

$\{E:F\}$  = # of <sup>field</sup> isomorphisms  $\gamma: E \rightarrow \gamma(E) \subseteq \bar{F}$  extending  $\text{id}: F \rightarrow F$  (fixing  $F$ ) "index of  $E/F$ "

$G(E/F) = \{ \gamma: E \rightarrow E \mid \begin{array}{l} \text{automorphism} \\ \text{fixing } F \end{array} \}$

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  $\alpha \in \bar{F}$  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  $F$ .

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

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

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

where

$$\begin{aligned} \sigma(\sqrt{2}) &= -\sqrt{2} \\ \sigma(\sqrt{5}) &= \sqrt{5} \\ \sigma \text{ fixes } \mathbb{Q} \end{aligned}$$

$$\begin{aligned} \tau(\sqrt{5}) &= -\sqrt{5} \\ \tau(\sqrt{2}) &= \sqrt{2} \\ \tau \text{ fixes } \mathbb{Q} \end{aligned}$$

$$\begin{aligned} \sigma \circ \tau &= \tau \circ \sigma = \gamma \\ \gamma(\sqrt{2}) &= -\sqrt{2} \\ \gamma(\sqrt{5}) &= -\sqrt{5} \\ \gamma \text{ fixes } \mathbb{Q} \end{aligned}$$

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

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

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

Notice  $\sigma, \tau, \sigma\tau$  have order 2.  $\Rightarrow$

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

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

$$|H| \text{ divides } |G(K/\mathbb{Q})| = 4$$

if  $|H| = 1$   $H = \{id\}$   $\langle 6 \rangle$

if  $|H| = 2$   $H = \{id, \sigma\}$  or  $\{id, \tau\}$  or  $\{id, \gamma\}$ .

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

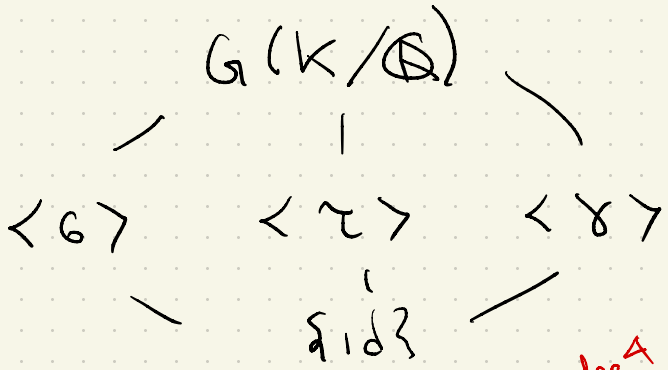
Recall  $K_H = \{a \in K \mid \psi(a) = a \forall \psi \in H\}$

The subgroup diagram is:

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

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

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



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

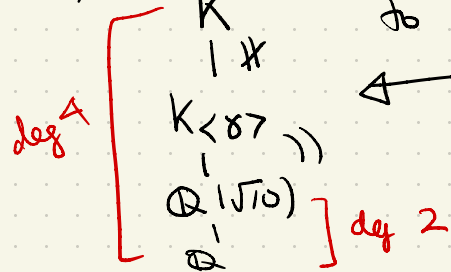
to see  $K_{\langle \gamma \rangle} = \mathbb{Q}(\sqrt{10})$  notice

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

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

$\neq 2$  since  $K \neq K_{\langle \gamma \rangle}$ .

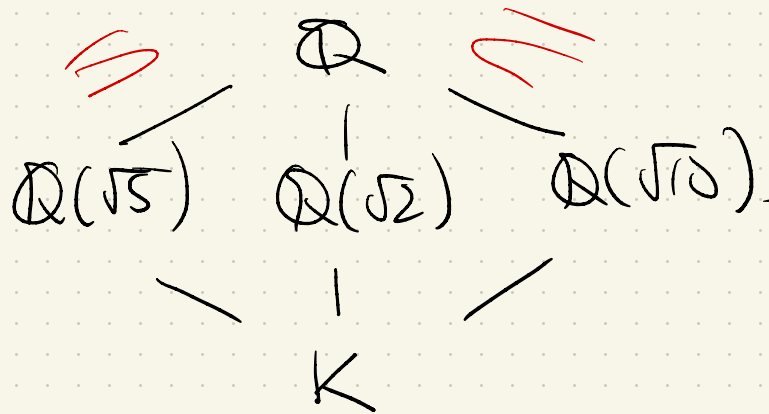
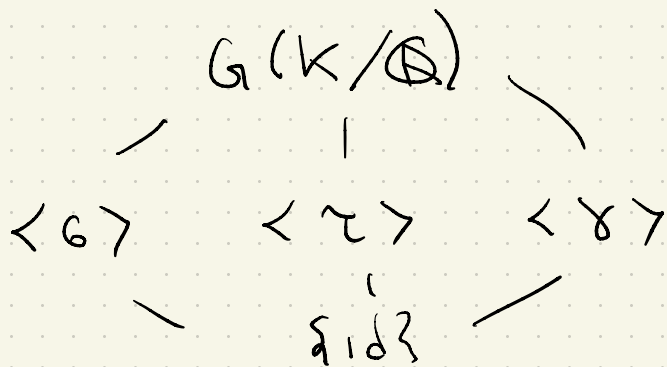
$id : K \rightarrow K$   
 $id(a) = a$



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

$K_{\text{id}} = K$

$K_G(K/\mathbb{Q}) = \mathbb{Q}$



This is the first example of a Galois correspondence



Thm 51.9  $F \subseteq E \subseteq K$  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  $F \subseteq E$   $\{E:F\} \leq [E:F]$  and

$$\{K:F\} = \{K:E\}\{E:F\}$$

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

Corollary 51.10  $F \subseteq E$   $[E:F] < \infty$  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

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

$$\downarrow$$
$$\mathbb{Q}(\sqrt{2}) = E$$

$$\downarrow$$
$$\mathbb{Q} = F$$

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

by Thm  
51.9

$K$  separable  
over  $\mathbb{Q}$ .

separable  
over  $\mathbb{Q}$

Example

Let  $E = F(\alpha)$

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

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

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 perfect 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  $\text{char } F = 0$ )

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  
 $\text{irr}(\alpha, F) = f(x) \in F[x]$  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  $E = \mathbb{Z}_p(y)$   $\text{char } E = p$  but  $|E| = \infty$

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

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

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

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

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

Freshman's dream

$y$  is a zero of multiplicity  $p$   
of  $\text{irr}(y, \mathbb{Z}_p(t))$ .

$$\{E:F\} = 1$$

$$[E:F] = p$$

not separable.

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

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

Proof Let  $\alpha, \beta$  be zeros  $\Psi_{\alpha, \beta}: F(\alpha) \rightarrow F(\beta)$  conj.  
iso.

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

Lemma 51.11 Let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{F}[x]$

is  $(f(x))^m \in \mathbb{F}[x]$  and  $m-1 \neq 0$  in  $\mathbb{F}$ . Then

$f(x) \in \mathbb{F}[x]$  is  $a_i \in \mathbb{F}$  for all  $i$ .

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

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



Thm 51.13 Every field of characteristic 0 is perfect

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

Thm 51.14 Every finite field is perfect.

Proof Again sufficient to show cases 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

