MAT401 April 2 2008

HW8 returned
HW9 due
HW10 on web by midnight Thu

TA office hour Thursday 5-7pm Bahen center 6th floor. It is his last office hour.

Ref Card Error : $Gal(E/K_1) > Gal(E/K_2)$

Review of the fundamental theorem of Galois theory

Take F such that char $F = 0$. If E/F is a splitting field. Then there is a bijection between $\{K : E/K/F\}$ and $H < Gal(E/F)$ with $K \to Gal(E/K)$ and $E_H \leftarrow H$.

Illustrative Diagram :

$$\begin{array}{ccl}
E & \longleftrightarrow & Gal(E/E) = \{e\} \\
| & & \\
K & \longleftrightarrow & Gal(E/K) = H \\
| & & \\
F & \longleftrightarrow & Gal(E/F) = G
\end{array}$$

$$[E:K] = \frac{|H|}{|\{e\}|} = [H:\{e\}]$$

$$[K:F] = \frac{|G|}{|H|} = [G:H].$$

If K is a splitting field, then H is normal and furthermore

$$Gal(K/F) = G/H = \frac{Gal(E/F)}{Gal(E/K)}$$

Theorem :

If E is a splitting field of $x^n - a = 0$ over F, where from now on we will take char $F = 0$ always, and also $a \in F$. Then $Gal(E/F)$ is solvable.

Definition:

A primitive root of unity of order n is an element $w \in E$ such that $w^n = 1$, and furthermore if $n^n = 1$ then $n = w^k$ for some k.

Examples:

$\{\pm 1, \pm i\}$ are the roots of $x^4 - 1 = 0$, and $\{i, -i\}$ are the primitive roots. In general, $w = e^{\pm i 2\pi/n}$ is primitive, and There may also be others.

Proof (Theorem):

Case ①:

F already contains a primitive root of unity w of order n.

let b be some root of $x^n - a = 0$.

Now if w is a primitive root of unity of order n, then the others are $\{w^0, w^1, w^2 \dots w^{n-1}\}$

Then $b, wb, w^2b \dots w^{n-1}b$ are all the roots of $x^n - a = 0$.

So $E = F(b, wb, w^2b \dots w^{n-1}b) = F(b) \quad \because b \in F$.

Now, recall that for $\sigma \in Gal(E/F)$, if b is a root of $f \in F[x]$ then $\sigma(b)$ is also a root of f. So $\sigma(b) = w^k b$. For some k and this determines σ entirely. Likewise for $\tau \in Gal(E/F)$ $\tau(b) = w^j b$

Now $\sigma \cdot \tau(b) = \sigma(w^j b) = \sigma(w^j)\sigma(b) = w^j \sigma(b) = w^{j+k} b$ because $w \in F$, so σ and $\tau \in Gal(E/F)$ both fix it.

Similary $\tau \cdot \sigma(b) = w^{k+j} b = \sigma \cdot \tau(b)$ and $\therefore$ σ, τ are completely determined by its action on b, and likewise for all other elements of $Gal(E/F)$, this means that Gal (E/F) is abelian and hence trivally solvable.

Case ② : $\omega \notin F$

For subfields of $\mathbb{C}$ it is obvious that there is an extension which contains a primitive root of unity. In general this is not so obvious, but for our purposes. it is sufficient.

$$\begin{array}{ccc} & E(\omega) & \\ (=)\diagup & & \diagdown \\ E & & F(\omega) \\ & \diagdown F \diagup & \end{array}$$

Let $b \in E$ be a root of $x^n - a = 0$. Then in $E(\omega)$ the roots of $x^n - a = 0$ are $\{b, \omega b, \omega^2 b \ldots \omega^{n-1} b\}$ But $E = S_F(x^n - a)$ so $\{b, \omega b, \omega^2 b, \ldots \omega^{n-1} b\} \in E$, meaning $(\omega b)(b^{-1}) = \omega \in E$ so $E(\omega) = E$.

$\Downarrow$

$$\begin{array}{c} E \\ | \\ F(\omega) \\ | \\ F \end{array}$$

$F(\omega)/F$ is abelian $\therefore$ it is the splitting field of x^{n-1}/F.

Claim Gal $(F(\omega)/F)$ is abelian

To prove this consider:
$\sigma, \tau \in Gal(F(\omega)/F)$, meaning $\sigma(\omega) = \omega^j$ and $\tau(\omega) = \omega^k$.
$\sigma \cdot \tau(\omega) = \sigma(\omega^k) = (\sigma(\omega))^k = \omega^{jk} = \tau \circ \sigma(\omega)$ so we have proved this claim ∎

Thm: Let $f \in F[x]$. If f splits over some field.

$F(\underbrace{a_1, a_2, \ldots, a_i}_{n_j} \ldots a_k)$ s.t $a_j \in F(a_1 \ldots a_{j-1})$

$\exists n_j \quad a_1 \in F$

Then $Gal(E/F)$ is solvable.
where E is a splitting field for f over F.

Proof: let $E_0 = F$.

$F(a_1) \subset E_1$ a splitting field of $x^{n_1} - a_1^{n_1}$ over E_0
$F(a_1, a_2) \subset E_2$ a splitting field of $x^{n_2} - a_2^{n_2}$ over E_1

$$\begin{array}{c}
F(a_1, a_n) \subset E_n \\
| \\
F(a_1, a_2) \subset E_2 \\
| \\
F(a_1) \subset E_1 \\
| \\
E_0 = F
\end{array}
\qquad E = S_F(F) \xrightarrow{\text{Galois}} \qquad
\begin{array}{c}
\{e\} \\
\text{Solvable } \{ \; | \\
Gal\, E_n(E_{n-1}) \\
\text{Solvable } \{ \; | \\
Gal\,(E_n / E_{n-2}) \\
| \\
Gal\,(E_n / F)
\end{array}$$

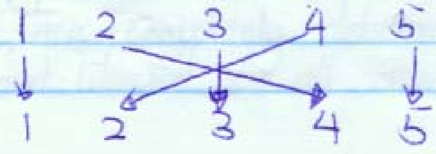
Solvable
$Gal(E_n/E)$
$= Gal(E_n/F)$
$\overline{\text{Solvable}}$
$Gal(E_n/E)$

Debt.
A splitting extension of a splitting extension is a splitting extension.

$E_2 = SE_2(F_2) = S_F(g)$
$E1 = S_p(F_1)$
$|$
F

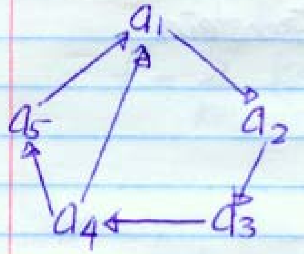
$Gal(E/F)$

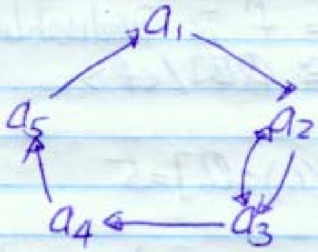
claim: Suppose $H < S_5$ contains a 5 cycle.
$1 \to 4 \to 3 \to 5 \to 2 \to 1$ & a 2 cycle:



In that case: $H = S_5$

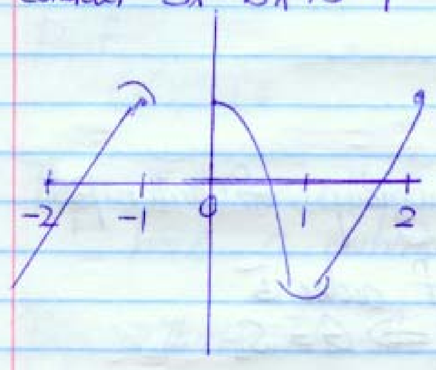
Proof: This a baby Rubik's cube exercise!





$\{a_1 \dots a_5\} = \{1 \dots 5\}$ can flip any non-arbitrary pair

Consider $3x^5 - 15x + 5 - f$.

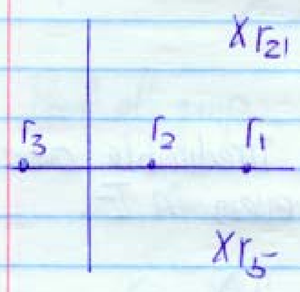


F has exactly 3 roots in $\mathbb{R}$

$f/(x-r_1)(x-r_2)(x-r_3)$

= quadratic

↳ 2 further complex roots. $\frac{-b \pm \sqrt{b^2-4ac}}{2a}$ $z, \bar{z}$.



Consider $G = Gal(S_{\mathbb{Q}}(f)/\mathbb{Q})$

any $\sigma \in G$ permutes $r_1 \dots r_5$:
σ is determined by this permutation

$S_{\mathbb{Q}}(f) = \mathbb{Q}(r_1, \dots, r_5)$
$\Rightarrow G < S_5$ $\Longrightarrow$ G contains a 2cycle.

$u \mapsto \bar{u}$

$r_1 \to r_1 \qquad r_4 \to r_5$
$r_2 \to r_2$
$r_3 \to r_3$

$\mathbb{Q}(r_1) =$ f is irreducible by Eisenstein
$\cong \mathbb{Q}[x]/\langle f \rangle$

so $[\mathbb{Q}(r_1) : \mathbb{Q}] = 5$

$$\begin{array}{ll} E = \mathbb{Q}(r_1, \ldots, r_5) & 5 \mid [E:\mathbb{Q}] \\ \mid ? & \quad \parallel \\ \mathbb{Q}(r_1) & \Rightarrow 5 \mid |Gal(E/\mathbb{Q})| = |G| \\ \mid 5 & \\ \mathbb{Q} & \end{array}$$

Sylow's theory:
$p \mid |G| \Rightarrow G$ has a subgroup of order p.

G has a subgroup of order 5
$G > \mathbb{Z}/5 \qquad \Rightarrow G = S_5$
$\Rightarrow G$ has a 5-cycle.

Thm
let E/F, $f \in F[x]$ if f is irreducible over $F[x]$.
then it has no multiple roots even in E.

$\left\{ \begin{array}{l} a \text{ is a root } (x-a) \mid F \\ a \text{ is a multi root} \Leftrightarrow (x-a)^2 \mid f \end{array} \right\}$.

Def: If $f \in F[x]$

$$f = \sum_{k=0}^{\deg f} a_k x^k .$$

define

$$f' = \sum_{k=1}^{\deg f} k a_k x^{k-1}$$

claim:

1. $a' = 0$
2. $(af + bg)' = af' + bg'$
3. $(fg)' = f'g + f \cdot g'$

Proof

$(x^n x^m)' = \ldots$

Prop: f has multiple roots (in some E/F) iff f & f' have a common factor of $\deg > 0$

Prop $\Rightarrow$ Thm: If f is irred, then f & f' have no common factors, QED.

Proof of prop:

$\Rightarrow$ Assume f has a multiple root a.

$(x-a)^2 | f \Rightarrow f = (x-a)^2 g$ for some g.

$$f' = 2(x-a)g + (x-a)^2 g'$$
$$= (x-a)(2g + (x-a)g').$$
$$\Rightarrow (x-a) | f'$$

Assume f & f' have no common factor of deg > 0 in $F[x]$.

$\langle f, f' \rangle = \langle p \rangle$ for some $p \in F[x]$

$\Rightarrow p | f$, $p | P'$. $\Rightarrow$ deg $P = 0$

$\Rightarrow \langle f, f' \rangle = \langle 1 \rangle \Rightarrow \exists \alpha, \beta \in F[x]$.

s.t $\alpha f + \beta f' = 1 \Rightarrow$ since $x-a | f$ & $x-a | f'$ $x-a | 1$ $\Rightarrow \Leftarrow$

$\Leftarrow$ Suppose $p | f$ & $p | f'$

W.L.O.G. p is irreducible,

let E be an extension of F in which P has a root, $(E = F[x]/\langle p \rangle)$ call this root a.

$\Rightarrow f(a) = 0$, $f'(a) = 0$

$\Rightarrow (x-a) | f$, $(x-a) | f'$ in $E[x]$

$f = (x-a) \cdot g$

$f' = g + (x-a) g'$

$\Rightarrow g = \underbrace{f'}_{x-a | f'} - (x-a) g'$

$\Rightarrow (x-a) | g$

$\Rightarrow g = (x-a) h$

$\Rightarrow f = (x-a) g = (x-a)(x-a) h = (x-a)^2 h$ $\square$