Monday, March 8, 2021 6:05 PM

ins. ext.

$\alpha \in K / F$

$f(x) = g(x^{p^k})$ for some $g \to$ irrd. sep.

$$\begin{array}{c} K \\ | \\ F(\alpha) \\ | \\ F(\alpha^{p^k}) \\ | \\ F \end{array} \quad \text{sep.}$$

$\min(\alpha^{p^k}) = g(x)$.

If $\alpha^{p^k} \notin F$ $g(x)$ is of deg 1.

then the min

Otherwise $F(\alpha^{p^k}) / F$ is a nontrivial sep. ext.

$f(x) = x^p - x - 1$

$\min(\alpha) = g(x)$.

$\min(\alpha + i) = g(x - i)$.

$f(x) = g(x) \ldots$

$f(x) = g(x) \cdot g(x - i) \ldots$

Look at degrees $\quad p = \deg(g)$. # of factors

$\Downarrow$

$\deg(g) = \cancel{1}$. or p.

$K = \mathbb{Q}(\zeta_p, \sqrt[p]{2})$.

normal subgp

$$\begin{tikzcd}
 & K \arrow[dl, dash] \arrow[dr, dash] & \\
F_1 \quad \mathbb{Q}(\zeta_p) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[p]{2}) = F_2 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Galois.

$s : \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathrm{Gal}(F_2(\zeta_p)/F_2)$

$g \curvearrowright \mathrm{Gal}(K/F_1)$

$s(g)\, \mathrm{Gal}(K/F_1)\, s(g)^{-1}$.

$s(g)$. $\quad$ s $\quad$ g.

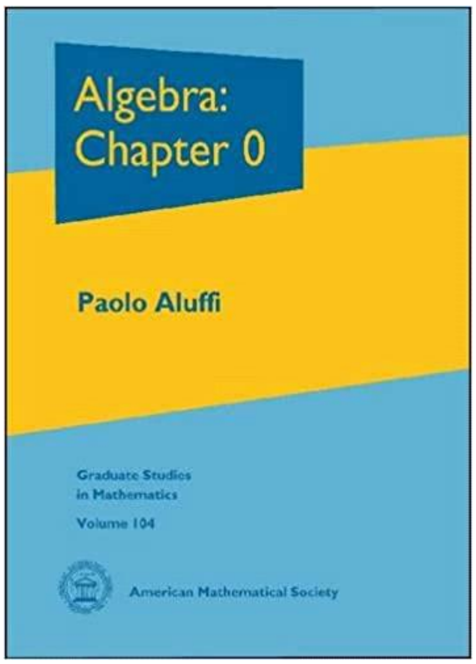
$$1 \to \mathrm{Gal}(K/F_1) \to \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Gal}(F_1/\mathbb{Q}) \to 1.$$

One sees:

$$\mathrm{Gal}(K/\mathbb{Q}(\sqrt[p]{2})) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}).$$

$\sigma(\zeta_p) = \zeta_p^a \qquad \tau(\zeta_p) = \zeta_p^a$.

Group theory: $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(F_1/\mathbb{Q}) \ltimes \mathrm{Gal}(K/F_1)$.



$h(x)$ = deg 4 poly. (S) $s \in S$. $h(s) = 0$,

$\mathbb{F}_{16} / \mathbb{F}_2$.

$\forall\ \alpha \in \mathbb{F}_{16}$ is a root of

$\Rightarrow h(x) \mid f(x)$.

$f(x) = x^{16} - x$ $\qquad f(s) = 0. \Rightarrow h(x) \mid f(x).$

factor $x^{16} - x$ & find deg 4 ird. factors.

$$(x^{16} - x) = x(x+1)(x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1) \cdot (x^8 + x^7 + \cdots + 1)$$

$\mathbb{F}_{2^n} / \mathbb{F}_2 \qquad s \qquad \mathbb{F}_{2^n}^*$

deg k poly $f(x)$.

① $f(s) = 0$ for some (all) $s \in S$.

② $s^{2^n} = s$ $\quad s$ is a rt of $x^{2^n} - x$.

$f(x) \mid x^{2^n} - x$. $\quad$ b/c. $f(x)$ is ird.

Lemma. If $\forall\ d \mid |G|$.

$$\left| S_d = \{ \quad x^d = 1 \quad \} \right| \leq d$$

then. G is cyclic.

$\alpha = \sum \sqrt{p_i}$

$$\begin{array}{c} K \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

trivial gp

$$K = \mathbb{Q}(\alpha). \ \{ g \in \mathrm{Gal}(K/\mathbb{Q}) \quad g|_{\mathbb{Q}(\alpha)} = id. \} = \text{trivial}.$$

$$g|_{\mathbb{Q}(\alpha)} \neq id.$$

$\neq id.$

$$\forall \ g \in \mathrm{Gal}(K/\mathbb{Q}), \quad g(\alpha) \neq \alpha.$$

$\forall\ g \in \mathrm{Gal}(K/\mathbb{Q}), \quad g(\alpha) \neq \alpha.$

$\sigma_i(\sqrt{p_i}) = -\sqrt{p_i}$

$\sigma_i(\sqrt{p_j}) = \sqrt{p_j}$.

$$g = \left((\sigma_1)^{e_i}, \ldots (\sigma_n)^{e_i} \right)$$

$e_i = 0$ or

$$g(\alpha) = \sum (-1)^{e_i} \cdot \sqrt{p_i}$$

$\parallel$

α.

$g(\alpha) = \alpha$

$K \overset{\iota}{\hookrightarrow} \mathbb{R}$

$\iota(g(\alpha)) \leq \alpha$

$=$ iff g is trivial.

HW8 Problem 1 part b. (Hints).

We will always number the roots in the following way:

prove: this is injective.

α	$-\alpha$	β	$-\beta$
1	2	3	4.

With this numbering we have a map $G \to S_4$.

justify → (a different ordering results in a inner aut of S_4).

(i). $G \cong K_4$ iff $\alpha\beta \in \mathbb{Q}$.

"$\Rightarrow$" There are two kinds of subgroups iso to K_4 in S_4.

- $\{\underset{\sigma_1}{()}, \underset{\sigma_2}{(12)(34)}, \underset{\sigma_3}{(13)(24)}, \underset{\sigma_4}{(14)(23)}\}$. which is normal.
- $\{(), (12), (34), (12)(34)\}$ and its conjugates.

As G acts transitively on the set of roots, G must be the first one.

Then $\beta = \sigma_3 \alpha$. $\alpha\beta = \alpha \cdot \sigma_3 \alpha$. $\Rightarrow$

$$\sigma_2(\alpha\beta) = \sigma_2(\alpha) \cdot \sigma_2(\beta) = \sigma_2(\alpha) \cdot \sigma_4(\alpha) = -\alpha \cdot -\beta = \alpha\beta.$$

Similarly $\sigma_3(\alpha\beta) = \sigma_4(\alpha\beta) = \alpha\beta$.

Thus $\sigma\alpha\beta = \alpha\beta \quad \forall \sigma \in G. \Rightarrow \alpha\beta \in \mathbb{Q}$.

"$\Leftarrow$" If $\alpha\beta \in \mathbb{Q}$ then one sees $K = \mathbb{Q}(\alpha)$, so $|G| = 4$. If $G \not\cong K_4$ then $G \cong \mathbb{Z}/4$,

Note $\pi(\alpha) = -\alpha$ gives $\pi \in G$ of ord $= 2$, so the element σ sending α to β has ord $= 4$.

On the other hand, $\alpha \cdot \beta = \alpha \cdot \sigma(\alpha)$.

Since $\alpha\beta \in \mathbb{Q}$, $\sigma(\alpha\beta) = \alpha\beta = \alpha \cdot \sigma(\alpha)$

On the other hand, $\alpha \cdot \beta = \alpha \cdot \sigma(\alpha)$.

Since $\alpha\beta \in \mathbb{Q}$ $\quad \sigma(\alpha\beta) = \alpha\beta = \alpha \cdot \sigma(\alpha)$.

$$\sigma(\alpha\beta) = \sigma(\alpha) \cdot \sigma(\beta)$$

Thus $\alpha = \sigma(\beta) \Rightarrow \beta = \sigma(\alpha) = \sigma^2(\beta)$

Note $K = \mathbb{Q}(\beta)$ $\quad \beta = \sigma^2(\beta) \Rightarrow \sigma^2 = id$. Contradiction

(ii). $G \cong \mathbb{Z}/4$ iff $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

" $\Rightarrow$ " If $G \cong \mathbb{Z}/4$, we have also $\mathbb{Q}(\alpha) = K$.

Note that $\alpha^2\beta^2 = b \in \mathbb{Q}$ so $\mathbb{Q}(\alpha\beta)/\mathbb{Q}$ has deg 1 or 2.

The deg cannot be 1 due to (i). So

$\mathbb{Q}(\alpha\beta)/\mathbb{Q}$ has deg 2. Note: so does $\mathbb{Q}(\alpha^2)/\mathbb{Q}$.

By the fundamental thm of Galois theory,

there is only one intermediate subfield of deg 2, b/c.

$\mathbb{Z}/4$ has only 1 subgp of index 2.

Thus $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

" $\Leftarrow$ " Assume $\mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha\beta)$, then $\beta \in \mathbb{Q}(\alpha)$,

and $K = \mathbb{Q}(\alpha)$ is of deg 4.

$|G| = 4 \Rightarrow G \cong \mathbb{Z}/4$ or $G \cong K_4$.

If $G = K_4$ then $\alpha\beta \in \mathbb{Q} \Rightarrow \mathbb{Q}(\alpha^2)$ $\mathbb{Q}(\alpha\beta)$

If $G = K_4$ then $\alpha\beta \in \mathbb{Q} \Rightarrow \mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha\beta) = \mathbb{Q}$. Absurd!

(iii). $G \cong D_8$ iff $\alpha\beta \notin \mathbb{Q}(\alpha^2)$.

"$\Rightarrow$" follows from part (ii).

"$\Leftarrow$" First, $\beta \notin \mathbb{Q}(\alpha)$, otherwise $K = \mathbb{Q}(\alpha) \Rightarrow |G| = 4$

$\Downarrow$

$\alpha\beta \in \mathbb{Q}$ or $\mathbb{Q}(\alpha^2)$,

which is impossible

Then $\mathbb{Q}(\alpha, \beta) / \mathbb{Q}$ has degree 8 (justify).

Any subgroup $H \leq S_4$ with $|H| = 8$ is isomorphic to D_8.

This settles the problem.

prove this! Hint:

$H \leq S_4$ is a Sylow 2-subgp.

$$\hat{p} \in \left(\mathbb{Z}/(p^n - 1) \right)^*$$

$$\operatorname{ord}(\hat{p}) = n.$$

$$n \mid \left| \mathbb{Z}/(p^n-1)^* \right| = \varphi(p^n - 1).$$

$$\left| \operatorname{Aut}(\mathbb{Z}/(p^n-1)) \right| = \varphi(p^n - 1).$$

$$\operatorname{Gal}(\mathbb{F}_{p^n} / \mathbb{F}_p) \cong \mathbb{Z}/n.$$

$$= \operatorname{Aut}(\mathbb{F}_{p^n})$$

$$\varphi$$

$$\varphi|_{\mathbb{F}_{p^n} \setminus \{0\}} \longrightarrow \operatorname{Aut}(\mathbb{Z}/(p^n-1))$$

K/F finite deg.

$$G = \operatorname{Aut}_F(K).$$

If $F = K^G$, then

K/F is Galois ✓.

$M = K^H$.

K/M is Galois, then

K/F is Galois ✓.

$F = K^p$

K/F. $\quad\quad \alpha \in K \setminus F$.

$\min_F(\alpha) \overset{?}{=} (X^p - \alpha^p) = (X - \alpha)^p$.

So if $f(x)$ is the minimal poly.

Then $(X^p - \alpha^p) = g_1(x) \cdot g_2(x) \cdots g_k(x)$ over $F[x]$

g_i irrd. $\quad\quad g_i(x) = $ minimal poly of α

$g_i \mid (X^p - \alpha^p)$ $\quad\quad \| $

$\quad\quad\quad\quad f(x)$,

$g_i \mid (X-\alpha)^p \quad\quad (X^p - \alpha^p) = (f(x))^k \Rightarrow p = k \cdot \deg(f)$.

$X - \alpha \mid g_i$ in $K[x]$.

$K = \mathbb{F}_p(X, Y)$

$$\mathbb{F}_p(x,y)\,/\,\mathbb{F}_p(x^p,y^p).$$

$$\begin{array}{c}\mathbb{F}_p(x,y)\\ |\\ \mathbb{F}_p(x^p,y)\\ |\\ \mathbb{F}_p(x^p,y^p).\end{array}$$

\begin{tikzcd}
 & K = \mathbb{Q}(\zeta_p, \sqrt[p]{2}) \arrow[dl, dash, "H"'] \arrow[dr, dash, "N"] & \\
F_1 = \mathbb{Q}(\sqrt[p]{2}) \arrow[dr, dash] & & F_2 = \mathbb{Q}(\zeta_p) \arrow[dl, dash, "H'"] \\
 & \mathbb{Q} &
\end{tikzcd}

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

$H \curvearrowright N \lhd G$.

$(\mathbb{Z}/p)^* \simeq \mathbb{Z}/p$.

$F_2/\mathbb{Q}$ is Galois.

$g \curvearrowright$ as conjugation.

$$1 \to \mathrm{Gal}(K/F_2) \xrightarrow{\varphi} \mathrm{Gal}(K/\mathbb{Q}) \xrightarrow{\psi} \mathrm{Gal}(F_2/\mathbb{Q}) \to 1.$$

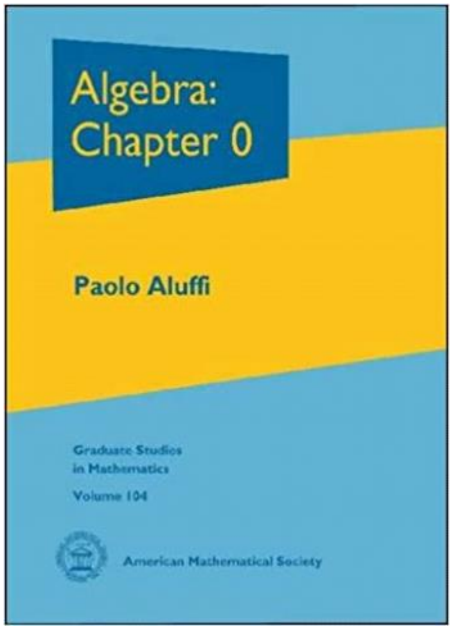
s

$\psi \circ s = id$

then:

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{Gal}(F_2/\mathbb{Q}) \ltimes_s \mathrm{Gal}(K/F_2).$$

$(\mathbb{Z}/p)^* \curvearrowright (\mathbb{Z}/p)$



Chapter 4/5.

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r] & H \arrow[r] \arrow[l, bend left] & 1. \end{tikzcd}$$

$$G \cong H \ltimes N.$$

$$(\mathbb{Z}/p)^* \to \mathrm{Aut}(\mathbb{Z}/p)$$