ins. ext.

$\alpha \in K / F$

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

$$\begin{array}{l} K \\ | \\ F(\alpha) \\ | \\ F(\alpha^{p^k}) \\ | \\ F \end{array}$$

sep.

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

If $\alpha^{p^k} \in F$ then the min $g(x)$ is of deg 1.

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

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

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

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

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

$f(x) = g(x)\, g(x-i) \dots$

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

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

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

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.

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

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

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

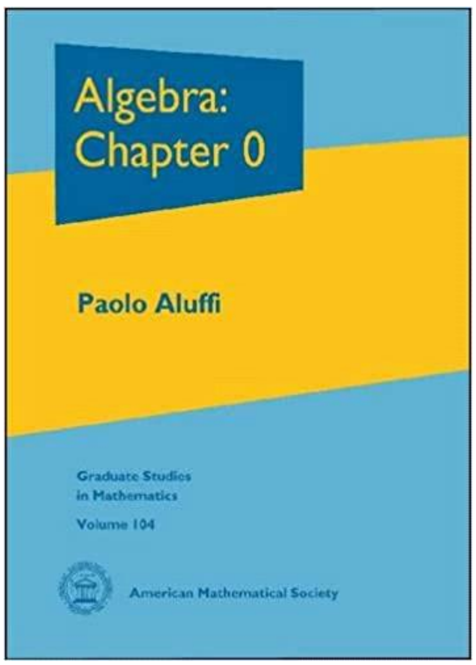
$$\begin{tikzcd}
 & & s(g) \arrow[d] & g \arrow[d] & \\
1 \arrow[r] & \mathrm{Gal}(K/F_1) \arrow[r] & \mathrm{Gal}(K/\mathbb{Q}) \arrow[r] & \mathrm{Gal}(F_1/\mathbb{Q}) \arrow[r] \arrow[l, bend left, "s"] & 1.
\end{tikzcd}$$

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

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

$\mathbb{F}_{16}$

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

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

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

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

deg k poly $f(x)$.

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

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

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

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

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

then G is cyclic.

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

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

trivial gp

$K = \mathbb{Q}(\alpha)$. $\left\{ g \in \mathrm{Gal}(K/\mathbb{Q}) . \; g\big|_{\mathbb{Q}(\alpha)} = id. \right\} = $ trivial.

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

$\neq id.$

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

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

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

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

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

$e_i = 0$ or .

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

$\parallel$

α.

$g(\alpha) = \alpha$

$K \xrightarrow{\iota} \mathbb{R}$

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

$=$ 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 $-\beta$ With this numbering we have a map
1   2   3   4.

$G \to S_4$. justify

(i). $G \cong K_4$ iff $\alpha\beta \in \mathbb{Q}$. (a different ordering results in a inner aut of S_4).

"$\Rightarrow$" 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 $\beta = \sigma_3 \alpha$. $\alpha\beta = \alpha \cdot \sigma_3\alpha$. $\Rightarrow$
$$\begin{aligned}\sigma_2(\alpha\beta) &= \sigma_2(\alpha)\cdot\sigma_2(\beta)\\ &= \sigma_2(\alpha)\cdot\sigma_4(\alpha)\\ &= -\alpha\cdot -\beta = \alpha\beta.\end{aligned}$$

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, ...

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

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

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

" $\Rightarrow$ " $\quad$ 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 $\mathbb{Q}(\alpha\beta) = \mathbb{Q}(\alpha^2)$.

" $\Leftarrow$ " $\quad$ Assume $\quad \mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha\beta)$, 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 $\quad \alpha\beta \in \mathbb{Q} \Rightarrow \mathbb{Q}(\alpha^2) = \mathbb{Q}(\alpha\beta) = \mathbb{Q}$. Absurd!

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.

$H', H \leq S_4$, $|H| = 8$.

H = Sylow 2-subgp.

H', H conj. $\Rightarrow H' \cong H$.

a b

$$H = \langle \overset{a}{(1234)}, \overset{b}{(24)} \rangle.$$

$\downarrow$ ord 4 $\qquad$ $\downarrow$ ord. 2

$$(24)(1234)(24) = (1432) = (1234)^3.$$

f has $\qquad K$

$$\text{"Gal"} \qquad \begin{tikzcd} \overset{\alpha}{K} \arrow[r] \arrow[d, dash] & \overset{\beta}{\bar{K}} \arrow[d, dash, "\text{normal}"] \\ F \arrow[r, dash] & F \end{tikzcd}$$

$x^3 - 2$ irrd. $/ \mathbb{Q}$.

$(\sqrt[3]{2})^t \neq 1.$

$\sqrt[3]{2} \qquad \omega\sqrt[3]{2} \qquad \bar{\omega}\sqrt[3]{2}.$

$$K = \mathbb{Q}(\omega, \sqrt[3]{2}) / \mathbb{Q}.$$

$$\mathbb{Z}/2 \ltimes \mathbb{Z}/3 \cong S_3.$$

$$\mathbb{Q}(\sqrt[3]{2}, \omega)$$

$$|$$

$$\mathbb{Q}.$$

$\tau \to \quad \tau(\omega) = \overline{\omega}, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}$

$\sigma \to \quad \sigma(\omega) = \omega, \quad \sigma(\sqrt[3]{2}) = \omega \cdot \sqrt[3]{2}$

$$\tau\sigma \neq \sigma\tau$$

insep.

$$\overline{\mathbb{F}_p(x, y)}.$$

$$|$$

$$K(a,b) := \overline{\mathbb{F}_p}(x^p, y^p, (ax+by))$$

p

$$\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$$

$$|$$

$$?$$

$$\overline{\mathbb{F}_p} = \bigcup_n \mathbb{F}_{p^n}$$

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

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^n}$

$d \mid n.$

$(a_n, b_n) \in \mathbb{F}_{p^n}$

$$\alpha = \sum_{i=0}^{p-1} \zeta^{i^2}.$$

$$\begin{array}{c} K = \mathbb{Q}(\zeta). \\ | \\ F = \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array} \qquad \deg 2.$$

$$\mathrm{Gal}(K/F) = ?$$

$$= \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) \mid \sigma(\alpha) = \alpha\},$$

$$\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/p)^*.$$

$\sigma = \sigma_a \qquad \sigma_a(\zeta) = \zeta^a.$

$\sigma_a(\alpha) \overset{?}{=} \alpha$

$$\sigma_a(\alpha) \stackrel{?}{=} \alpha$$

$$\sigma_a\left(\sum \zeta^{i^2}\right) = \sum \zeta^{i^2}.$$

$$\sum \zeta^{a i^2} = \sum \zeta^{(xi)^2} = \sum \zeta^{i^2}.$$

$$\begin{cases} \sigma_a(\alpha) = \alpha & \text{if } a = \text{quadratic residue mod } p \\ \neq \alpha & \text{if } a \neq \text{quadratic residue mod } p \end{cases}$$

if $a \equiv x^2 \mod p$ then $\sigma_a(\alpha) = \alpha$.

if $a \not\equiv x^2 \mod p$

$$\boxed{\sigma_a(\alpha) + \alpha = 2\sum_{j=0}^{p-1} \zeta^j = 0.}$$

$$\alpha = \sum_{i=0}^{p-1} \zeta^{i^2} = 2 \sum_{t \equiv \text{quadratic residue}} \zeta^t$$

$$\zeta^{i^2} = \zeta^{(p-i)^2}$$

$i^2 \equiv (p-i)^2 \mod p$

$a \neq$ q.r. $\quad \sigma_a(\alpha) = 2 \cdot \sum_{s \neq \text{q.r.}} \zeta^s \Rightarrow \alpha + \sigma_a(\alpha)$

$$= 2 \cdot \sum_{s=0}^{p-1} \zeta^s = 0.$$

a q.r mod p if

a q.r. mod p if

$a \equiv x^2 \mod p$ for some x.

$\left(\frac{\cdot}{p}\right)$ $\mathbb{Z}/p^* \twoheadrightarrow \{\pm 1\}$ $\left(\frac{a}{p}\right) = 1$ if a = q.r

Ker = gp of q.r. -1 if $a \neq$ q.r.

$[\mathbb{Z}/p^* : \text{Ker}] = 2.$ Legendre symbol

$$\zeta = e^{\frac{2\pi i}{p}} = \cos\left(\frac{2\pi i}{p}\right) + i\sin\left(\frac{2\pi}{p}\right).$$

$\zeta^{-1} = \bar{\zeta}$ $\zeta + \zeta^{-1} = 2\mathrm{Re}(\zeta)$

ζ is a root of

$$(X - \zeta)(X - \zeta^{-1}) = X^2 - (\zeta + \zeta^{-1}) + 1$$

K/L is deg 2 ext.

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \underline{(\mathbb{Z}/p)^*}$$

$$\sigma \rightsquigarrow \hat{a} \leftarrow a$$

$$\sigma_a(\zeta) = \zeta^a$$

f irrd.

$f(\alpha) = 0$ So some $\alpha \in S$.

$\alpha^{p^n} = \alpha \Rightarrow \alpha$ is rt of $x^{p^n} - x$

$f \mid (x^{p^n} - x) \Longrightarrow$ factor $x^{p^n} - x$ & look for deg n factors.

$$x^4 + x^3 + 1$$

$$\underline{x^{2^n} - x}$$

$$x^4 + x + 1 \qquad = x(x+1)(x^2+x+1)$$

$$(x^4+x^3+x^2+x+1)(x^8+x^7+\dots+1)$$

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

$\mathbb{F}_2[x]/$ deg 4 poly

$\mathbb{F}_q^* \cong \mathbb{Z}/_{q-1}$

$S \subseteq \mathbb{F}_{16}^* \cong \mathbb{Z}/_{15}$

$\mathbb{F}_2[x]/$ [illegible]

$$S \subseteq (\mathbb{F}_{16}^*) \cong \mathbb{Z}/15$$

$$\operatorname{ord}(\alpha) = 15.$$

$\mathbb{F}_{p^k}$

$|$

$\mathbb{F}_p$

$\hat{g}$

g $\quad \deg(g) < 4.$

$\mathbb{F}_{p^k}$ = the splitting field of $x^{p^k} - x$.

$$\varphi(p^n - 1).$$

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

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

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

$$\begin{tikzcd}
\alpha & \beta \\
K \arrow[r] & K \\
F \arrow[u, hook] \arrow[r] & F \arrow[u, hook]
\end{tikzcd}$$

$$\alpha \to \beta$$

$\alpha^2 \quad \underline{\alpha+\beta} \quad \underline{\alpha-\beta} \notin \mathbb{Q}.$

$\Rightarrow f$ irrd.

$$f(x) = (x-\alpha)(x+\alpha)(x-\beta)(x+\beta)$$
$$= (x^2-\alpha^2)(x^2-\beta^2).$$

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

* $\underline{\text{Legendre}}$ symbol. $\Rightarrow$ subgp of index 2.

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

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

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

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

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

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

$$\varphi$$

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

K/F finite deg.

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

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. $\qquad \alpha \in K \setminus F$.

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

So if $\underbrace{f(x) \text{ is the minimal poly}}$.

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

g_i irrd. $\qquad g_i(x) = $ minimal $\underline{\text{poly of}}$ α

$$g_i(x) = f(x)$$

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

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

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

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

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

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

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

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

$H \curvearrowright N \lhd G.$

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

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

$g \curvearrowright$ as conjugation.

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

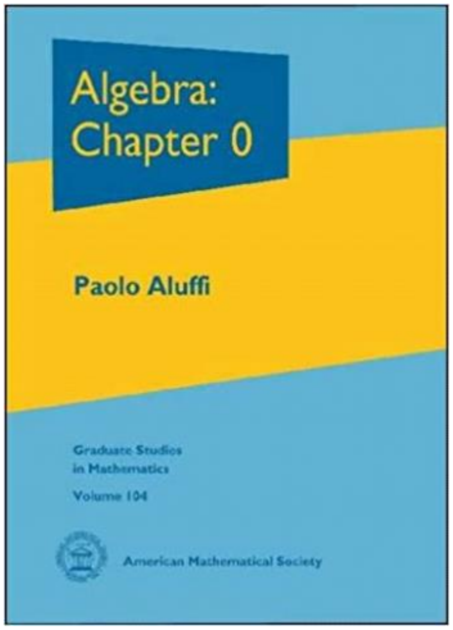
$s: \mathrm{Gal}(F_2/\mathbb{Q}) \to \mathrm{Gal}(K/\mathbb{Q})$

$\pi \circ s = id$

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.

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

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

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

R is a comm. alg over F

$\varphi_a : \quad R \to R \qquad x \to x \cdot a.$

$f(x) = \text{char poly } (\varphi_a).$ over F.

$\Downarrow$

$f(a) = 0.$ minimal poly of a over F.

$$g(x) = c_0 + c_1 x + \cdots + c_t x^t \qquad c_0 \neq 0,$$

$$g(a) = 0 \Rightarrow c_0 + c_1 a + \cdots + c_t a^t = 0$$

$$a \left[\frac{(c_1 + \cdots + c_t a^{t-1})}{-c_0} \right] = 1.$$

$$G = Gal(\mathbb{F}_{p^n} / \mathbb{F}_p) \simeq \mathbb{Z}/n.$$

α is $\in S$.

α is a rt of f, show that.

$\underline{\sigma(\alpha)} \in S$. $\sigma \in G$.

$\sigma(\alpha) \notin S$.

$$\mathrm{ord}(\sigma(\alpha)) = t < p^n - 1 = |\mathbb{F}_{p^n}^*|.$$

$$(\sigma(\alpha))^t = 1 \iff \sigma(\alpha^t) = 1$$

$$\iff \alpha^t = 1$$

$$\iff \mathrm{ord}(\alpha) = t < p^n - 1. \quad \alpha \notin S.$$

f splits in $\mathbb{F}_{p^n}$.

$Gal(\mathbb{F}_{p^n}) \curvearrowright$ transitively on rts of f