Galois例题整理

$x^{p^n}-x$ 和 x^n-1 都是这个 extension

例：证明 $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic, of order n

- $f(x)=x^{p^n}-x$ is separable ; $\mathbb{F}_{p^n}$ is splitting of $f(x)$ over $\mathbb{F}_p$

  $f(x)=(x-1)(x-2)^{p^n-1}$，f在$\mathbb{F}_p$中的解 $x_1=1, x_2=2$

  由于Frobenius map中生成(以q最后)，$\forall x\in\mathbb{F}_{p^n}$, $\phi^n(x)=x$, $x^{p^n}=x$, } 即 $\mathbb{F}_{p^n}\rightleftharpoons\{\phi^n(x)=x$ 的所有x}

  $g(x)=x^{p^n}-x$，在其splitting field中至多 p^n 个 roots

  即 $f(x)=0$ 的其它root均在$\mathbb{F}_{p^n}$中，$\mathbb{F}_{p^n}$刚好是 splitting of $g(x)$ (也记为$f(x)$) over $\mathbb{F}_p$

- $\langle\sigma\rangle=Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$, the galois group is cyclic

  $\sigma:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$, $\sigma(a)=a\ \forall a\in\mathbb{F}_p$

  所有fix $\mathbb{F}_p$ pointwise的 σ 均可用 ϕ^m，$\phi: x\mapsto x^p$ 表示，且 $\phi^m:\mathbb{F}_{p^n}\to\mathbb{F}_{p^n}$

correct! $(\phi)^n=id$ on $\mathbb{F}_{p^n}$ ∴ 即 $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)=\langle\sigma\rangle$，$\sigma=\phi$ is generator

Q：为什么 σ 一定具有 $\phi^m: x\mapsto x^{p^m}$ 形式，$m\in\mathbb{Z}$.

[ϕ^m 为什么是 $\mathbb{F}_{p^n}$ 的 automorphism，怎么证 surjective } ⇒ in the following part : "Finite Field" P2

- $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois extension

  ① by: $n=|Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)|=[\mathbb{F}_{p^n}:\mathbb{F}_p]$

  一般求 $[A:B]$，将 A 写成 $B(a_1,a_2\cdots a_n)$；记 $B_i=(a_1,a_2\cdots a_i)$

  $[A:B]=[A:B_{n-1}]\times[B_{n-1}:B_{n-2}]\times\cdots[B_1:B_0]$, 其中 $[B_i(a_{i+1}):B_i]=\deg(m_{a_{i+1},B_i})$

  这里不容易求上述过程，

  but: $\mathbb{F}_{p^n}$中，$\forall x\in\mathbb{F}_{p^n}$ 可以表示为 $\mathbb{F}_p$ 元素的线性生成；$\mathbb{F}_{p^n}=\mathbb{F}_p\times\mathbb{F}_p\times\cdots\mathbb{F}_p$ ∴ $[\mathbb{F}_{p^n}:\mathbb{F}_p]=n$

  ② by def: finite normal separable extension

  finite normal ⇌ splitting 已证

  在A/B splitting 前提下，A separable ⇌ A split 的函数 $f(x)\in B[x]$, $f(x)$ separable

  此处 $f(x)=x^{p^n}-x$，f若在 $x=a$ 处有重根，$f'(a)=0$

  $f'(x)=p^n\cdot x^{p^n-1}-1$，$\forall a\in\mathbb{F}_{p^n}$, $a^{p^n-1}=1$； $p^n-1\neq0$ 故而 $f(x)$ 可分

例：$f(x)=x^4-2$，$f(x)\in\mathbb{Q}[x]$

$f(x)=0$, $x=\pm\sqrt[4]{2}$, $x=\pm\sqrt[4]{2}i$

$[\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}]=\deg m_{a,\mathbb{Q}}=\deg(x^4-2)=4$

$\sigma\in Gal(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})$, $\sigma(\sqrt[4]{2})=\pm\sqrt[4]{2}$, since 设$(\mathbb{Q}(\sqrt[4]{2})$, then $Gal(\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q})=2$ } ⇒ $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ not Galois

或者：$\sqrt[4]{2}$ 的最小多项式 $m_{a,\mathbb{Q}}$, has other roots

∴ $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}$ not splitting，故而 not finite normal；(separable 满足)

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{Q}(\sqrt[4]{2})/\mathbb{Q}(\sqrt{2})$ both Galois

⇒ Galois extension of galois extension not necessarily Galois

例: $f(x)=x^p-a \in \mathbb{Q}[x]$, $f(x)$ irr in $\mathbb{Q}[x]$,

$p\neq 2$, $Gal(f) \cong \mathbb{Z}_p:\mathbb{Z}_{p-1} = Hol(\mathbb{Z}_p) \cong Aut(D_{2p})$ 对比下一个例子 $x^{p^n}-1=0$

解: $x^p-1=(x-1)(x^{p-1}+x^{p-2}+\cdots+1)$

$w=e^{2\pi i/p}$, $w, w^2, \cdots w^{p-1}$ 是 $x^{p-1}+x^{p-2}+\cdots+1$ 的 root

$\therefore \alpha=a^{\frac{1}{p}}$, $f(x)=0$ 的root是 $\alpha, \alpha w, \cdots \alpha w^{p-1}$,

$E=\mathbb{Q}(\alpha, \alpha w, \cdots \alpha w^{p-1})$ is splitting field thus finite normal

$f(x)=x^p-a$ 没有重根 since $w^i \neq w^j$, 对 $i \in \{1, \cdots p-1\}$ } $\Rightarrow E/\mathbb{Q}$ is Galois extension

Let $L=\mathbb{Q}(w)$, $E \supseteq L \supseteq \mathbb{Q}$

$g(x)=x^{p-1}$, root为 $w, w^2 \cdots w^{p-1}$, $1 \in \mathbb{Q}(w)$ $\therefore \mathbb{Q}(w)$ is splitting field; $g(x)$ separable $\Rightarrow L/\mathbb{Q}$ Galois

判断是否在splitting, 找 α 的 min. 其它root是否在 $\mathbb{Q}(\alpha)$ 中

$\Rightarrow$ 由于: $L/\mathbb{Q}$ is normal $\overset{HW12\#3}{\Leftrightarrow}$ L is fixed by $Gal(E/\mathbb{Q}) \Leftrightarrow Gal(E/L) \triangleleft Gal(E/\mathbb{Q})$

$\therefore Gal(E/L) \triangleleft Gal(E/\mathbb{Q})$ (下面这个商群才well-defined)

由于: $E \supseteq L \supseteq \mathbb{Q}$, $E/\mathbb{Q}$, $L/\mathbb{Q}$ both Galois $\Rightarrow Gal(L/\mathbb{Q}) \cong Gal(E/\mathbb{Q}) / Gal(E/L)$

此处也成立,

$\Rightarrow$ 要求 $Gal(E/\mathbb{Q})$. $E=\mathbb{Q}(\alpha, \alpha w, \cdots \alpha w^{p-1}) = \mathbb{Q}(\alpha, w)$

$\sigma \in Gal(E/\mathbb{Q})$ { $\sigma(\alpha) = \alpha w^i$, $i=0, \cdots p-1$, p种
$\sigma(w) = w^i$, $i=1, \cdots p-1$, since $\mathbb{Q}(w)/\mathbb{Q}$ splitting, σ fix $\mathbb{Q}(w)$; $p-1$种

$\therefore |Gal(E/\mathbb{Q})| = p \times (p-1)$

但是, 这里并不是 direct product 结构!

$\Rightarrow$ 原因是: $Gal(E/\mathbb{Q}) = Gal(f)$, f is irr in $\mathbb{Q}[x]$, E is splitting of $f(x)$ over $\mathbb{Q}$

irr $\Rightarrow Gal(E/\mathbb{Q})$ acts on $\Omega = \{f(x)=0$, roots in $E\}$ transitively

$\forall x \in \Omega$, 轨道 $x^{Gal(E/\mathbb{Q})} = \Omega$,

无法分成不相交的轨道, $Gal(f)$ not has non-trivial block thus primitive (没法分成 $A \times B$, A B 各自对 Ω 作用)

即 direct product 不行

$\Rightarrow$ then consider $Gal(L/\mathbb{Q}) \cong Gal(E/\mathbb{Q}) / Gal(E/L)$; (为semi直积)

设 $A \cong B/C$, $A \leq B$, $C \triangleleft B$ $A \cap C = \{e\}$, then $B = A \rtimes C$,

$\Rightarrow$ 此处 $Gal(L/\mathbb{Q})$, $Gal(E/L)$ 还不满足ws上条件, 去找能满足条件的 isomorphism

{ $\sigma \in Gal(L/\mathbb{Q})$: $\sigma: L=\mathbb{Q}(w) \to L$
$w \longmapsto w^i$, $i=1, 2, \cdots p-1$ 均可, $\therefore Gal(L/\mathbb{Q}) \cong \mathbb{Z}_{p-1}$

$\tau \in Gal(E/L)$: $\tau: \mathbb{Q}(\alpha, w) \to E$, τ fix L pointwise $\therefore \tau(w)=w$
$\alpha \longmapsto \alpha w^i$, $i=0, 1, \cdots p-1$ 均可 $\therefore Gal(E/L) \cong \mathbb{Z}_p$

$\therefore Gal(E/\mathbb{Q}) = Gal(L/\mathbb{Q}) \cdot Gal(E/L) = \langle \sigma \rangle \langle \tau \rangle \cong \mathbb{Z}_p \cdot \mathbb{Z}_{p-1}$

$|\mathbb{Z}_p| = p$ coprime with $|\mathbb{Z}_{p-1}| = p-1$ $\therefore$ 可以写成半直积 $Gal(E/\mathbb{Q}) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_{p-1}$

Remk: ① σ和τ的选择 never conflict,

因为: $Q(\alpha,w)$的基的生成元 α, w, $q_i \in Q$, 三者相互独立(independent); 加乘均无法相互表示

∴不会出现 $\sigma(\alpha)=\cdots$, $\sigma(w)=\cdots$, 与 $\sigma(q_i)=\sigma(a\alpha^i w^j + b\alpha^{i'}w^{j'}+\cdots)$ 矛盾的情况

= 这个不存在

② $A=\mathbb{Z}_p\cdot\mathbb{Z}_{p-1} \Rightarrow$ then $A=\mathbb{Z}_p\times\mathbb{Z}_{p-1}$ 改成 $\mathbb{Z}_p\cdot\mathbb{Z}_q$, $\gcd(p,q)=1$ 也可以

示意: $\mathbb{Z}_3^+$和$\mathbb{Z}_5^+$ intersection $=\{e\}^{=0}$, 不是 0, 1, 2,

$2\in\mathbb{Z}_3$ 并 $2\in\mathbb{Z}_5$; $o(2\in\mathbb{Z}_3)=3$ 而 $o(2\in\mathbb{Z}_5)=5$

$\mathbb{Z}_2$ 也不是 $\mathbb{Z}_4$ 的 subgroup; 因为并 $A\le B$, $o(a\in A)$和$o(a\in B)$一样, aA和aB完全是一个东西

对比上面一个例子, $f(x)=x^p-a(\forall a)$ $[k:\mathbb{Q}]=p-1$ 用公式 $\phi(n)$ 和这题一样, $Gal(k/\mathbb{Q})\cong\mathbb{Z}_p:\mathbb{Z}_{p-1}$

HW12.10 10. Let p be an odd prime number, K be the splitting field of $x^{p^n}-1$ over $\mathbb{Q}$.

(1). Prove $[K:\mathbb{Q}]=p^{n-1}(p-1)$;

(2). Prove $Gal(K/\mathbb{Q})$ is a cyclic group. 水, 5列一下就行

10): $f(x)=x^{p^n}-1=0$ over $\mathbb{Q}$

- first consider $g(x)=x^k-1=0$. root: $1, \alpha, \alpha^2, \cdots \alpha^{k-1}$, $\alpha=e^{2\pi i/k}$, k is Prime

splitting extension $=Q(\alpha)=\{a_0+a_1\alpha+\cdots a_{k-1}\alpha^{k-1}: a_i\in\mathbb{Q}\}$

$\deg Q(\alpha)=\deg(m_{\alpha\mathbb{Q}})=k-1$

$\frac{g(x)}{x-1}=\frac{g(y+1)}{y}=\frac{1}{y}\{y^k+C_k^1y^{k-1}+\cdots C_k^1y+1-1\}$ is irreducible by Eisenstein; } ...(*)

$\therefore x^{k-1}+x^{k-2}+\cdots+x+1=0$ 是 $m_{\alpha\mathbb{Q}}$

(*)在 $k=p^n$ 时是不成立的,

✓ $g(x)=x^k-1=0$. k is not prime

Consider $\alpha^m=e^{2\pi mi/k}$, $\gcd(m,k)=1$ 记这些根为 $\beta_1,\beta_2\cdots\beta_l$

$h(x)=(x-\beta_1)(x-\beta_2)\cdots(x-\beta_l)$ 其中 $\beta_1=\alpha=e^{2\pi i/k}$

- lem: E/F is Galois extension (finite normal + 可分); $\gamma_1,\gamma_2,\cdots\gamma_n$ 是 E/F 中的代数元

$P(\gamma_1,\gamma_2,\cdots\gamma_n)$ 是关于 $\gamma_1\gamma_2\cdots\gamma_n$ 的对称多项式(任意改变 γ_i 顺序, P 不变); then $P\in F[x]$

例如此: $P(\gamma_1,\gamma_2)=\gamma_1^2+\gamma_2^2=P(\gamma_2,\gamma_1)$

$P(\gamma_1,\gamma_2;x)=(x-\gamma_1)(x-\gamma_2)=P(\gamma_2,\gamma_1;x)$

$\Rightarrow$ 此处 $h(x)$ 的系数均在 $\mathbb{Q}$ 中, $h(x)\in\mathbb{Q}(x)$

- lem: $h(x)$ is cyclic polynomial, 循环多项式(一定对称)在 $\mathbb{Q}[x]$ irreducible

即: $h(x)=m_{\alpha\mathbb{Q}}$, $\deg(\mathbb{Q}(\alpha))=\deg h(x)=\varphi(k)=k\prod_{p|k}(1-\frac{1}{p})$ p 是所有质因数

即: $x^k-1=0$ 的分裂域 $[\mathbb{Q}(\alpha):\mathbb{Q}]=\varphi(k)$

在 Arbitary $f(x)=0$ 时, f 的 root 不一定线性无关, 如 $(x-\alpha-\beta)(x-\alpha)(x-\beta)$

考虑单扩张 $\mathbb{Q}(\alpha)$, f reducible (本题), $\exists\ \alpha^a=(\cdots)\alpha^b+(\cdots)\alpha^c$, $a,b,c\le k-1$ $\Rightarrow$ 若不则不会

即 $f=(x-\alpha_1)\cdots(x-\alpha_m)(x-\alpha_{m+1})\cdots(x-\alpha_n))$ 这组因式 $\in\mathbb{Q}[x]$, 代入任意一个 α_i 得线性组合

finite field

HW11.8: 求一个8个元素的field

Consider $GF(2)[x]$ $f(x)=x^3+x+1$ irreducible in $GF(2)[x]$

$GF(2)[x]$ is PID

$(f(x))$ is irr in PID $\therefore$ maximal $\Rightarrow$ $GF(2)[x]/(f(x))$ is field

$GF(2)[x]/(f(x)) \cong GF_2(\alpha)$, α is root of $f(x)$

$=\{a_0+a_1\alpha+a_2\alpha^2 : a_i \in GF(2)\}$. 阶数为3, since $m_{\alpha,F}=f(x)$

此处共有 $2\times2\times2=8$ 个元素

加,乘使用 $GF(2)$, $GF(2)[x]$ 中的. 如: $\theta^3=-\theta-1$

Rmk: WTS: $\{a_0+a_1\theta+\cdots a_n\theta^n : a_i \in F\}$, $\deg = |F|^{n+1}=8 \Rightarrow |F|=2, n+1=3$

直接找数太对多了,用扩域找

HW11.9: $f(x)=x^3+1$, $g(x)=x^2-x-1$, α,β 是 $f(x), g(x)$ 在 $GF(9)$ 中的 root, show isomorphism $GF(3)(\alpha) \to GF(3)(\beta)$

- 易知 splitting field of $f(x), g(x)$ over $GF(3)$ is $GF(9)$

since $f(x), g(x)$ 均可irr,

$x/(f(x))=\theta$. splitting of $f(x)$ over $GF(3)=\{a_0+a_1\theta : a_0,a_1 \in GF(3)\}$ $\deg=3\times3=9$

- $f(\alpha)=\alpha^3+1=0$

证: $g(\alpha+a)=\alpha^2+a^2+2a\alpha-\alpha-a-1=(\alpha^2+1)+(a^2+2a\alpha-\alpha-a-2)=0$

$\alpha(2a-1)+(a^2-a-2)=\alpha(2a+2)+(a^2-a-2)=0 \Rightarrow a=-1$

$\therefore g(\alpha-1)=g(\beta)=0$. $\therefore \varphi: \alpha \mapsto \beta$ 下一面写了

HW11.10: 1): $GF(p^m) \subseteq GF(p^n)$ 证 $m|n$ $GF(p) \xrightarrow{\text{次n-1}} GF(p^n)$ 参照HW11.8

- $f_1(x)=x^{p^n-1}$ root: $1, \alpha=e^{\frac{2\pi i}{p^n-1}}, \alpha^2, \cdots \alpha^{p^n-1}$

the splitting field of $f_1(x)$ over $GF(p)=\{a_0+a_1\alpha+\cdots a_{n-1}\alpha^{n-1} : a_i \in GF(p)\}=GF(p^n)$

同样的 $f_2(x)=x^{p^m-1}$, $GF(p^m)$ 也是 splitting field

- $GF(p^m)=\{a'_0+a'_1\beta+\cdots a'_{m-1}\beta^{m-1} : a'_i \in GF(p)\} \subseteq \{a_0+a_1\alpha+\cdots a_{n-1}\alpha^{n-1} : a_i \in GF(p)\}$

即 $GF(p^m)$ 的生成元 $1,\beta$ 可以用 $GF(p^n)$ 的生成元 $1,\alpha$ 表示

$\therefore \alpha^t=\beta$ for some t, $e^{2\pi i\frac{t}{p^n-1}}=e^{\frac{2\pi i}{p^m-1}} \Rightarrow m|n$

2): in $GF(p)[x]$, $x^{p^m}-x \mid x^{p^n}-x \Leftrightarrow m|n$

$f(x)=x^{p^m}-x=x(x^{p^m-1}-1)=x(x-1)^{p^m-1}$ root: $0,1,\alpha,\alpha^2\cdots\alpha^{k}$, $k=p^m-2$, $\alpha=e^{\frac{2\pi i}{p^n-1}}$

$\forall b$, $[e^{2\pi i\frac{1}{(p^n-1)}}]^a=[e^{2\pi i\frac{1}{(p^m-1)}}]^b$, some a

$b=1$ 满足即可 $\therefore 2\pi i\frac{1}{p^m-1}=2\pi i\frac{a}{p^n-1}$ 即: $p^n-1=a(p^m-1)$ 只有p的指数才可以! ~~$(p+1)^n=a(p+1)^m$~~

由1)知 $p^m-1 \mid p^n-1 \Leftrightarrow m|n$

☆ 1. F_{p^n} 并不是 $F_p[x]$ 的 $x^n-1=0$ 的 splitting

$x^n-1=0$ 根 $1, \alpha, \alpha^2, \cdots \alpha^{n-1}$ $F_p(\alpha)=\{a_0+a_1\alpha+\cdots a_{n-1}\alpha^{n-1} : a_i \in F_p\}$

但由于 $\alpha, \alpha^2, \cdots \alpha^{n-1}$ 并不是 independent 的 (考虑 $x^n-1=0$ $[Q(\alpha):Q]=\varphi(n)=n\cdot\prod_{p|n}(1-\frac{1}{p})$)

实际上 here: $[F(\alpha):F]=p^{\varphi(n)}$; 只有在 n is prime 时, 才是 p^n R, Q 不可以 Fp 不可以

2. F_{p^n} 是 $F_p[x]$ 中 $x^{p^n}-x$ 的 splitting field

考虑 $\phi: x \mapsto x^p$; $f(x)=x^{p^n}-x=\phi^n(x)-x$

在 F_{p^n} 上 $f(x)=0$, $\forall x$, 刚好有 p^n 个零点, $\Rightarrow F_{p^n}$ 恰好为 splitting of $f(x)=\phi^n(x)-x$ over $\mathbb{F}_p$

prop: fix F_p pt-wise 的只有 ϕ^m, $\phi: x \mapsto x^p$, $Gal(F_{p^n}/F_p)=\langle\phi\rangle$

引理: $Aut(A/B) \le [A:B]$, $\Rightarrow$ Galois 扩张时取等

F_{p^n}/F_p 一定是 Galois

$\therefore |Gal(F_{p^n}/F_p)|=[F_{p^n}:F_p]=n$ ... ①

$\phi: x \mapsto x^p$, $order(\phi)=n$

$\phi \in Gal(F_{p^n}/F_p)$ $\therefore \langle\phi\rangle \le Gal(F_{p^n}/F_p)$ ... ②

$\Rightarrow Gal(F_{p^n}/F_p)=\langle\phi\rangle$

若 $\exists \psi \neq \phi$, ψ fix F_p pointwise ;

把 ψ extend to ψ' s.t. $\psi' \in Aut(F_{p^n})$; 由上知 $\psi'=(\phi)^m$ some m

$\Rightarrow$ fix F_p pt-wise 的只有 $\phi: x \mapsto x^p$

HW12 9. Give all subgroups of $Gal(GF(p^n)/GF(p))$ and their fixed field.

考点是有限域的 Frobenius

$GF(p^n)$ is the splitting field of ~~$x^n-1=0$~~ over $GF(p)$, $GF(p^n)=GF(p)(\alpha)$, α 为 x^n-1 下的 primitive root $=e^{2\pi i/n}$

$\sigma \in Gal(GF(p^n)/GF(p))$, σ fix $GF(p)$

$\sigma(\alpha)=\alpha^k$, $gcd(n,k)=1$, 共 $\varphi(n)$ 种选法 $\Rightarrow$ 和 order 两回事!

在到 1 证过 $Gal(F_{p^n}/F_p)$ cyclic,

且 $\sigma \in Gal(F_{p^n}/F_p)$. σ fix F_p 则必有 ϕ^m 形式, $\phi: x \mapsto x^p$; ... ①

$\because \phi^n=id$ on $\mathbb{F}_{p^n}$

$\therefore |Gal(F_{p^n}/F_p)|=n$ 即 $Gal(F_{p^n}/F_p) \cong \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$

子群: $\langle\phi^m, \phi: x \mapsto x^p\rangle$, fix F_{p^m}, $m \le n$

$\langle\phi^{m_1}, \phi^{m_2}\rangle$ fix F_{p^m}, $m=\max(m_1,m_2)$ 不行 ... ②

Semi-direct product & (subnormal chain)

例1: semi-product of $(\mathbb{Z}_4,+)$ by $\mathbb{Z}_2$. 即: $\mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_2 = G$

step1: · find homomorphism $\phi: \mathbb{Z}_2 \to Aut(\mathbb{Z}_4)$

只有一种: $\begin{cases} e \mapsto \sigma_1 = id \\ b \mapsto \sigma_2 \end{cases}$

· $\mathbb{Z}_4 = \{e, a, a^2, a^3\}$ $\mathbb{Z}_2 = \{e, b\}$

consider generators a^1, a^3;

$Aut(\mathbb{Z}_4) = \{\sigma_1, \sigma_2\}$ $\begin{cases} \sigma_1: a_1 \to a_1 \\ \sigma_2: a_1 \to a^3 \end{cases}$, $\sigma_2^2 = \sigma_1$

$\therefore (a^i, b^j)\cdot(a^{i'}, b^{j'}) = (a^i \times \phi(b^j)(a^{i'}),\ b^j b^{j'})$

$= (a^{i+3i'}, b^{j+j'})$

这个运算方式确定了, $\mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_4$ 这个群也确定了, 本题中 ϕ 只有1种, $\therefore \mathbb{Z}_4 \rtimes \mathbb{Z}_2$ is unique

step2: (这个半直积群有时候可以写出来的, 写成 V.S.A. 这些学过的)

$\mathbb{Z}_4 \triangleleft (\mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_2)$, $b^{-1}ab = a^m$ some m

$\therefore \phi(b) = \tilde{b} \in Aut(\mathbb{Z}_4)$.

$\therefore \phi(b)(a) = b^{-1}ab = a$ or $a^3 = a^{-1}$ (generators)

$\begin{cases} m=1: ab=ba, \mathbb{Z}_4 \cdot \mathbb{Z}_2 \text{ 在 } \mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_2 \text{ 中 commutative (needed in direct product)} \therefore G = \mathbb{Z}_4 \times \mathbb{Z}_2 \\ m=3: b^{-1}ab = a^{-1}; \text{又 } b^2=1, a^4=1 \Rightarrow G = D_8 = \mathbb{Z}_4 \rtimes_\phi \mathbb{Z}_2 \text{; 此处 } \phi \text{ 就是 step1 写的那种} \end{cases}$

Rmk: $\begin{cases} \phi(b) = \tilde{b} \in Aut(\mathbb{Z}_4) \text{ 在所有所有半直积题目中都会用, 最常见于 } G = D_{2n} \text{ 的;} \\ D_{2n} = \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2, \text{ but } \mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2 \text{ may not unique} \end{cases}$

例2: lem1: $Inn(G) \cong G/Z(G)$

对任意 G 成立, $Inn(G) = \{\tilde{g} : g \in G\}$ 内自同构群

$\varphi: G \to Inn(G) \leq Aut(G)$

$g \mapsto \varphi(g) = \tilde{g}: G \to G$

$x \mapsto g^{-1}xg$

lem2: $Z(S_n) = e, \forall n \geq 3$; $Z(A_n) = e, \forall n \geq 4$

A_3 is cyclic $\therefore Z(A_3) = A_3$. ; A_4 的 normal group: A_4, e, V_4

A_n is simple $(n \geq 5)$, $Z(A_n) \triangleleft A_n$

A_n not Abel $\Rightarrow Z(A_n) = e$

lem3: $Aut(A_4) = Aut(S_4) = S_4$

$\begin{cases} Inn(A_4) \cong A_4/Z(A_4) = A_4 \\ Inn(S_4) \cong S_4/Z(S_4) = S_4 \end{cases}$

$A_4 \cong Inn(A_4) \leq Inn(S_4) \cong S_4 = Aut(S_4)$ 不会

$\therefore A_4 \cong Inn(A_4) \leq Aut(A_4) \cong S_4$

$|A_4| = \frac{1}{2}|S_4| \therefore Aut(A_4) = S_4$ 或 A_4 $Aut(A_4) = S_4$ 不会?

例2: find semi-direct product of A_4 by $\mathbb{Z}_2$, 即 $G = A_4 \rtimes_\phi \mathbb{Z}_2$

- 先证明 $A_4 \rtimes_\phi \mathbb{Z}_2 = S_4$ some ϕ

$S_4 = \{(12), (13), (14), (24), (34), (23), 1, (13) = (123)(12), (13)(14), \cdots, (13)(12)(14), \cdots\}$

$A_4 \trianglelefteq S_4$; $\mathbb{Z}_2 \leq S_4$ (S_4 中 $\mathbb{Z}_2$ 形式可以为 $\{(12), 1\}$)

$A_4 = \{(13)(12), (13)(14), \cdots, 1\}$ 所有 2-cycles, 1 $\therefore A_4 \cap \mathbb{Z}_2 = 1$ } 存在 ϕ s.t. $A_4 \rtimes_\phi \mathbb{Z}_2 = S_4$

- 是否还有其它可能的 G, ϕ

$\phi: \mathbb{Z}_2 \to Aut(A_4) \cong S_4$; 由引理知 $A_4 \cong Inn(A_4) \leq Aut(A_4) = Aut(S_4) = Inn(S_4) = S_4$

$\begin{cases} e \mapsto 1 \\ x \mapsto 2\text{-cycle} \end{cases}$

$\therefore \tau \in Aut(A_4) = Inn(A_4)$, $\tau = \tilde{a}$ for some $a \in S_4$

要求 $\tau^2 = id$ $\Rightarrow$ find group $H = \{a \in S_4 : \tilde{a}^2 = id\}$,

$H^2 = \{a^2 : a^2 y a^2 = y\} = \{b : by = ya \ \forall y \in S_4\} = Z(S_4) = 1$

$\therefore H = \{2\text{-cycles}\}$

唯一的, 因为 $A_4 \leq S_4$ embedding inj

例4: $G = \mathbb{Z}_3 \times \mathbb{Z}_5$ $\tau \in Aut(G)$, $a^\tau = a^{-1}$, $b^\tau = b$ $\mathbb{Z}_3 \times \mathbb{Z}_5 = \langle \tau \rangle = D_6 \times \mathbb{Z}_5$

$\begin{cases} a^\tau = a^{-1}, b^\tau = b^{-1} \end{cases}$ $\mathbb{Z}_3 \times \mathbb{Z}_5 : \langle \tau \rangle = D_{30}$

(1): $\tau^{-1} b \tau = b$ $\Rightarrow$ $\mathbb{Z}_5$ commutes with $\langle \tau \rangle$, and $\mathbb{Z}_3$

$\therefore \mathbb{Z}_3 \times \mathbb{Z}_5 : \langle \tau \rangle = \mathbb{Z}_3 : \langle \tau \rangle \times \mathbb{Z}_5 \cdots (*)$ } $\Rightarrow D_6 \times \mathbb{Z}_5$

$\tau^{-1} a \tau = a^{-1}$, $\tau^2 = a^3 = e$ } $\Rightarrow \mathbb{Z}_3 : \langle \tau \rangle \cong D_6$

(Rmk: $\mathbb{Z}_5$ commute with $\mathbb{Z}_3, \langle \tau \rangle$, thus $\mathbb{Z}_5 \leq Z(H)$, center "(符号)中心群" 顺序是任意的)

(2): $\tau^{-1} b \tau = b^{-1}$, $\tau^{-1} a \tau = a^{-1}$ 均不可交换

$\mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$ 必然 (1)中也是对的, 但 $\mathbb{Z}_{15} : \langle \tau \rangle$ 不要求, $\mathbb{Z}_3 \times \mathbb{Z}_5 : \langle \tau \rangle$ 好求一点; 而且条件是按 $\mathbb{Z}_3 \times \mathbb{Z}_5$ 结构的本质就是 $\mathbb{Z}_{15} = \mathbb{Z}_2$,

$\tau^{-1} b \tau = b^{-1}$, $\tau^{-1} a \tau = a^{-1}$ $\Rightarrow$ $\forall x \in \mathbb{Z}_3 \times \mathbb{Z}_5$, $x = ab$ some a, b (1直 bijective)

$\therefore \tau^{-1} x \tau = x$, $\tau^2 = 1$, $x^{15} = 1$

$\Rightarrow \mathbb{Z}_3 \times \mathbb{Z}_5 : \langle \tau \rangle = D_{30}$

注意: 我一开始觉得 τ, ab 形式不一样, $\tau \in Aut\langle a \rangle \times \langle b \rangle$, "$\tau^{-1} a \tau$" = "$\tau^{-1} b \tau$" 是不能"乘"的.

但: 要在 $H = \mathbb{Z}_3 \times \mathbb{Z}_5 : \langle \tau \rangle$ 中, a, b, τ 均为 H 中元素 "," 当然是合理的!

例3：

为什么 $\mathbb{Z}_3 \rtimes D_8$ 有2个：

recall: $\varphi: A \times B \longrightarrow G$ （此处 $A \times B$ 为群未积不涉及结构）

$(a,b) \longmapsto ab$

不管是直积、半直积都存在 bijective $\varphi: A \times B \to G$ "值"对应关系

$$\begin{cases} \varphi(a_1,b_1)\cdot\varphi(a_2,b_2) = a_1b_1a_2b_2 \\ \varphi((a_1,b_1)\otimes(a_2,b_2)) = \varphi(a_1\phi(b_1)(a_2), b_1b_2) = a_1\phi(b_1)(a_2)b_1b_2, \ \phi \text{ 为 homomorphism} \end{cases}$$

? ① … 希望：$\varphi(a_1,b_1)\cdot\varphi(a_2,b_2) = \varphi((a_1,b_1)\otimes(a_2,b_2))$

$a_1b_1a_2b_2 = a_1\phi(b_1)(a_2)b_1b_2 \Rightarrow \phi(b_1)(a_2) = \tilde{b}_1(a_2) = b_1^{-1}a_2b_1$

$$\begin{cases} A \trianglelefteq G, B \trianglelefteq G,\ A \cap B = \{e\}, & a\in A\ b\in B \text{ commutative}; \text{即 } \varphi \text{ isomorphic}, \phi = e \\ \phi(b_1) = \tilde{b}_1 \end{cases}$$

? ② … 在半直积结构下，仍希望 $a_1\phi(b_1)(a_2)b_1b_2$ 保持 $(a_1\phi(b_1)(a_2))\cdot(b_1b_2)$（$a_1\phi(b_1)(a_2) \in A$，$b_1b_2 \in B$）

$$\begin{cases} \therefore b_1^{-1}a_2b_1 \in A\ \forall b_1, a_2, \text{故要求 } A \trianglelefteq G \\ \phi \text{只能是 conjugation} \end{cases}$$

例3：$\mathbb{Z}_3 \rtimes D_8$

$\mathbb{Z}_3 = \{e, x, x^2\}$ $D_8 = \langle a,b : a^4 = b^2 = e,\ b^{-1}ab = a^{-1}\rangle = \mathbb{Z}_4 \rtimes \mathbb{Z}_2$（$a \in \mathbb{Z}_4$，$b \in \mathbb{Z}_2$）

考虑 $\phi(a,b) = (\tilde{a}, \tilde{b})$ 的取值可能：

$$\begin{cases} a^{-1}xa = e, x, x^2 & \forall x \\ b^{-1}xb = e, x, x^2 \end{cases}$$

~~①~~ $(x^a, x^b) = (x,x) \Rightarrow$ commutative for element in $\mathbb{Z}_3, D_8 \Rightarrow$ direct product $\mathbb{Z}_3 \rtimes D_8 = \mathbb{Z}_3 \times D_8$

~~②~~ $x^a = e$ (or $x^b = e$) bbv can't

③ $a^{-1}xa = x$. $b^{-1}xb = x^2 = x^{-1}$, ✓

④ x^2 x

⑤ x^2 x^2 ✓

代入 $b^{-1}ab = a^{-1}$

$b^{-1}ab \overset{a^{-1}xa}{\overset{\parallel}{x}} b^{-1}a^{-1}b = b^{-1}ax^{-1}a^{-1}b = b^{-1}\underline{x^{-1}}b = x$ ③✓

$= b^{-1}a\underline{x}a^{-1}b = b^{-1}\underline{x^2}b = x^2$ ④✓

✗ ⑤✗

$\Rightarrow \mathbb{Z}_3 \rtimes D_8 = \langle a,b,x : a^{-1}xa = x,\ b^{-1}xb = x^2,\ a^4 = b^2 = x^3 = e,\ b^{-1}ab = a^{-1}\rangle$

$\langle a,b,x : a^{-1}xa = x^2,\ b^{-1}xb = x^2,\ a^4 = b^2 = x^3 = e,\ b^{-1}ab = a^{-1}\rangle$

Rmk: ③④⑤的检验是所行的过程即：考虑 $\phi: D_8 = \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ 可能性

✓ 这么到其实比较难，D_8 元素不好描述，

∴先 $\mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3)$，$\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$，由形成 D_8 的条件 $b^{-1}ab = a^{-1}$ 检验

group classification

例1: $|G|=24$. 群分类 (finite Abel + Sylow + semi-direct)

1. Abelian: finite Abel定理, 可以写成 $G_1\times G_2\times\cdots G_n$ $|G_i|=p_i^{r_i}$, $|G_i|=\langle a_1\rangle\langle a_2\rangle\cdots$
(obv nilpotent) $\therefore G\cong\langle a_{11}\rangle\times\langle a_{12}\rangle\cdots\langle a_{21}\rangle\times\langle a_{22}\rangle\times\cdots\langle a_{t1}\rangle\times\langle a_{t2}\rangle\times\cdots\langle\cdots\rangle$, a_{ij}是G_i中阶第j大的

(recall: G is finite Abel, $p\mid|G|$, p素数, 必有$g\in G$, $o(g)=p$)

$\therefore G\cong G_1\times G_2$ $|G_1|=3$, $|G_2|=8$

分类依据是G_2中最高阶、次高阶元素是多少 $\therefore Z_3\times Z_8$, $Z_3\times Z_4\times Z_2$, $Z_3\times Z_2\times Z_2$ 3种

2. Non-Abelian: 由Sylow Th知, 3 $|G_1|=8$、$|G_2|=3$ $G_2=Z_3$

nilpotent group: $G=P_1\times P_2\times\cdots P_n$ P_i是G的sylow-a_i子群 $\Leftrightarrow$ 所有sylow子群 normal to G
$\Leftrightarrow$ 任意极大子群 is normal

2.1 G nilpotent, $G=G_3\times G_8$, $G_8=Q_8$. D_8. $Z_2\times Z_4=Z_2\times Z_4$(舍), $Z_2\times Z_2\times Z_2=D_8$(重复) $=V_4\times Z_2$

$\therefore Z_3\times D_8$. $Z_3\times Q_8$ 2种

2.2 G not nilpotent

2.2.1 $G_3\triangleleft G$. $G_8\not\triangleleft G$

$Z_3\times Q_8$ (2个), $Z_3\times D_8$. $(Z_3\times Z_4)\times Z_2$, $(Z_3\times Z_2)\times Z_2\times Z_2$, $Z_3\times Z_8$ (舍) 5种

(因为8阶群只有 Z_8, $Z_4\times Z_2$, $Z_2\times Z_2\times Z_2$, D_8. Q_8.)

为什么是$(Z_3\times Z_4)\times Z_2$ 而不是 $Z_3\times(Z_4\times Z_2)$

2.2.2 $G_3\not\triangleleft G$. $G_8\triangleleft G$

$Q_8\times Z_3$. $D_8\times Z_3$, $(Z_2\times Z_2\times Z_2)\times Z_3$, $Z_8\times Z_3$. $(Z_4\times Z_2)\times Z_3$ 4种
(舍)

2.2.3. $G_3\not\triangleleft G$. $G_8\not\triangleleft G$:

S_4. 1种

$\therefore$ 一共15种 Q: $Z_3\times D_8$ 为什么2个 ✓ (详见半直积例题3)
$(Z_3\times Z_4)\times Z_2=(Z_3\times Z_2)\times Z_4=Z_3\times(Z_2\times Z_4)$ 吗?

① 找出所有Z_3. G_8, $G_3=Z_3$

$G_8=Z_2\times Z_4$. $Z_2:Z_4=Z_2\times Z_4$, $Z_4:Z_2=D_8$. Q_8. Z_8. $Z_2\times Z_2\times Z_2$. $Z_2:Z_2\times Z_2=V_4\times Z_2=D_8$

② 按normal讨论,

如果$G_3\triangleleft G$. $G_8\not\triangleleft G$. $G\cong G_3\times G_8$,

$Z_3\times Z_8$. $Z_3\times Z_2\times Z_4$. $Z_3\times D_8$. $Z_3\times Q_8$ $Z_3\times Z_2\times Z_2\times Z_2$, 先列出来,排除重复的

$Z_3\times Z_8$(舍)

ED·norm (欧几里得)

作业1: HW9 T7&T8

7. Let K be a algebraic number field. We call $\alpha \in K$ an algebraic integer if α is a root of a monoic polynomial with integer coefficients. Let d be integer with no square factors. i.e. $\sqrt{d}$ is not a integer. Let $K = \mathbb{Q}(\sqrt{d})$.

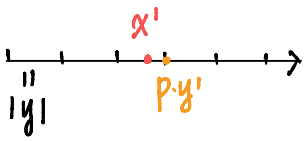
(1). If $d \equiv 2, 3 \pmod 4$, prove that all algebraic integer in K is a set:

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

Similarly, we want norm s.t. $p \times y'$ on the grid point

(2). If $d \equiv 1 \pmod 4$, prove that all algebraic integer in K is a set:

T8(2).(3)



$$\{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\}$$

Therefore all algebraic integers in K form a ring, called the algebraic integer ring of K.

8. (1). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{-3})$ is a ED.
(2). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{2})$ is a ED.
(3). Prove the algebraic integer ring of $\mathbb{Q}(\sqrt{5})$ is a ED.

T8(1): $-3 \equiv 1 \pmod 4$

algebraic integer ring: $R = \{a + b\frac{1+\sqrt{3}}{2} : a, b \in \mathbb{Z}\}$

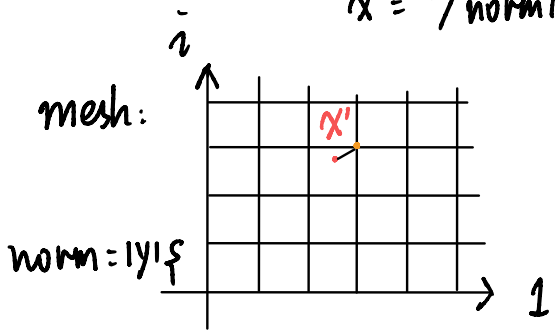
given any $x, y \in R$, we want: $\exists p, q \in R$, $x = p \cdot y + q$ $\text{norm}(q) < \text{norm}(y)$

⇓

1. Normalization: $x, y \longmapsto x', y'$

$x' = x/\text{norm}(y)$, $y' = y/\text{norm}(y)$, $x' = p' \times y + q'$

2. mesh:



Let $p' \times y$ be the nearest point to x'

the line from x' to $p' \times y$ represent q'

✅ we want: $y \cdot R \times |y|$ on the grid point

⇒ in R, $a, b \in \mathbb{Z}$, want → $z \in R$, $\text{norm}(z) \in \mathbb{Z}^+$

∴ $y \times z \times |y| \in \mathbb{Z}^+$, $y \times z$ 在边长为 $|y|$ 的格点上

∴ define: $|a + b\frac{1+\sqrt{3}}{2}| = |a + \frac{1}{2}b)^2 + (b\frac{\sqrt{3}}{2})^2 = a^2 + ab + b^2$ (not unique) ✓

group action

group action定义 $G \curvearrowright \Omega$. $\varphi: G \to Sym(\Omega)$

$g \to \varphi(g)$

① $\varphi(g)$为bijective (故为permutation) 不是Aut!

② $w \in \Omega$, $w^1 = w$;

③ $(w^g)^h = w^{gh}$ 结合律 ($g := \varphi(g)$, $h := \varphi(h)$)

1. Let G be a finite group, $H < G$ and $[G : H] = n > 1$. Prove G contains a non-trivial normal subgroup K where $[G : K] \mid n!$ or G is isomorphic to a subgroup of S_n. (Hint: consider the group action $G \curvearrowright X$ where X is the set of all H-cosets in G). (HW6.T1)

和$[G:H]$相关

故考虑 $G \curvearrowright$ Coset, G作

即: $\varphi: G \to Sym(X)$

$g \mapsto \varphi(g) = \hat{g}: X \to X$

$Hg_i \mapsto (Hg_i)g$

$\varphi(g_1g_2)(x \in X) = x^{\varphi(g_1g_2)} = (x^{\varphi(g_1)})^{\varphi(g_2)}$ 由定义③知, 此时φ是合法的 group action, 自然有 $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$

(所有 well-defined φ, φ is homomorphism)

$\ker\varphi = \{g : Hg_i = Hg_ig, \forall g_i\} = \bigcap_{g \in G} g^{-1}Hg$

$K := \ker\varphi$, $G/\ker\varphi \leq Sym(X) \Rightarrow$: $\ker\varphi = \{1\}$ then $G \leq Sym(X)$

$\ker\varphi \neq \{1\}$, $|K| \mid n!$

含义为 $G \leq Sym(X)$

$= G/\ker\varphi \leq Sym(X)$, $\ker\varphi = \{1\}$

"$\{Hg : g \in G\}| = X$

例2: L20的笔记: if Gal(E|F) fix 中间域 L

lem: field $F \subseteq L \subseteq E$, L is a field fixed by $Gal(E|F) \rightleftharpoons Gal(E|L) \triangleleft Gal(E|F)$

"$\Rightarrow$" $\sigma \in Gal(E|F)$ $\sigma: E \to E$ $\sigma(a) = a$ $\forall a \in F$

$\sigma(L) = L$, $\therefore \sigma$ induces an automorphism of L;

Gal(E|F) act on L naturally, 且 the kernel of this action is Gal(E|L)

$\therefore Gal(E|L) \triangleleft Gal(E|F)$

recall: group action: G act on H, 右乘 $\Rightarrow$ 此处类比写成:

$\varphi: G \to \hat{G}$

$g \to \hat{g}: H \to H$

$h \to hg$

解释一下这个 action "Gal(E|F) act on L"

$\varphi: Gal(E|F) \to Gal(E|F) \leq Sym(L)$

$\sigma \to \varphi(\sigma) = \sigma|_L: L \to L$

$l \mapsto \varphi(\sigma)(l) \in L$ 是 set-wise fixed

φ只要是map就可以, φ: group → 某个 group action, 一定 homo

$\ker\varphi = \{\sigma \in Gal(E|F) : \varphi(\sigma) = \sigma|_L = id\} \triangleleft Gal(E|F)$ 才成立的

σ fix L: $\varphi: Gal \to Sym(L)$

$\sigma \mapsto \sigma|_L: L \to L$

$\ker\varphi \triangleleft Gal$

induce (限制性算子) 和 lifting (或说 extension) 一定可以是 group action!

Field automorphism lifting

(last page of Lig / Dumit Psu1)

3. Let K/F be a finite normal extension, E is a intermediate field. Prove that E/F is a normal extension iff E is stable of K/F. i.e. For any F-automorphism σ of K, $\sigma(E) = E$. recite this theorem!

HW123 K/F finite normal extension, $k \supseteq E \supseteq F$; E/F is normal extension $\Leftrightarrow$ $\forall$ F-automorphism σ of K $\sigma(E)=E$, 即 E stable of K/F

$\Rightarrow$: K/F finite normal

∴ K/F 是 f(x)∈F[x] 的 splitting field. 不妨设 f(x) 在 F[x] 中没有 root, $f(x) = a(x-\alpha_1)^{r_1}\cdots(x-\alpha_n)^{r_n}$ in $K[x]$

E/F finite normal ($E \subseteq K$ ∴必 finite)

∴ $E = F(\beta_1, \beta_2, \cdots \beta_m)$, β_i 是 $g \in F[x]$ 的 root, 不妨设 $\beta_i \notin F$; $\beta_i \in \{\alpha_1, \cdots \alpha_n\}$ since $E \subseteq K$ ···(*)

$\sigma: K \to K$, $\sigma(f) = f$ $\forall f \in F$

证明 $\sigma(E) = E$, 还需 $\sigma(\beta_i) \in E$

分类 ① f(x) irreducible, ② if not, 在 F 中 f(x) 可以分解为 two f₁(x)f₂(x)···fₖ(x);

def: normal extension E/F 中, 若有 irr polynomial h(x)∈F[x] 的一个 root, 必然包含全部 root

①: by (*), f 的 root 在 E 中 ∴ f 所有 root 均在 E 中 $\Rightarrow E = F(\alpha_1, \alpha_2 \cdots \alpha_n) = K$

②: ···, fᵢ 的 root 在 E 中, Some i

不是从 K → E 的, E is finite normal ∴ E is splitting of g(x) over F, $g \in F[x]$

$g(x) = a_0 + a_1 x + a_2 x^2 + \cdots a_n x^n$, $a_i \in F$ 根为 $\gamma_1 \gamma_2 \cdots \gamma_n$

∴ $\sigma(g(x)) = g(x)$ 所以 permute $\{\gamma_1, \gamma_2 \cdots \gamma_n\}$ 前半是不变的

$\sigma(E) = \sigma(F(\gamma_1 \gamma_2 \cdots \gamma_n))$, $\sigma(a) = a$ $\forall a \in F$

$\sigma\{\gamma_1 \cdots \gamma_n\} = \{\gamma_1 \cdots \gamma_n\}$ $\sigma(\gamma_i) \mapsto \gamma_j$ 存在一个 bijective $\Rightarrow \forall f(x) \in F[x]$ σ permute f root

$\Leftarrow$: 反证: $\sigma(E) = E$, E/F not normal

即 $\exists$ irr $f(x) \in F[x]$, 2 β 是 f(x) 的 root ($\exists \beta \notin F$); $\exists \alpha \in E$, $\beta \notin E$

知识点: Lift automorphism

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & F \\ \downarrow & & \downarrow \\ F(\alpha) & \xrightarrow{\psi} & F(\beta) \\ \downarrow & & \downarrow \\ K & \xrightarrow{\phi} & K \end{array}$$

由 Lift auto 可知: $F \xrightarrow{\sigma} E$, $f \downarrow$, $\downarrow \sigma(f)$, $F' \xrightarrow{\psi} E'$

E 视 to F, $f \in F[x]$ 视 to $\sigma(f) \in E[x]$

对应的 splitting field of $f(\sigma f)$ over $F(E)$ 也

↑ 代数单射就 $F(\alpha) \cong E(\beta)$ 成立

∴ here $\sigma = id$, $F(\alpha) \xrightarrow{\psi} F(\beta)$ 且 $\psi|_F = \sigma = id$

然后将 $F(\alpha)$, $F(\beta)$ 均对到 K, $\phi|_{F(\alpha)} = \psi$; 且由题意 $\phi(E) = E$

but: $\phi(F(\alpha)) = \psi(F(\alpha)) = F(\beta)$; $F(\alpha) \subseteq E$, $F(\beta) \not\subseteq E$ $\Rightarrow \phi(E) \neq E$ 矛盾