L24: $Gal(f)\cong S_p$, 例

lem: G is transitive permutation group on Ω, if G contains a transposition, $|\Omega|$ is a prime $=p$, then: $G\cong Sym(\Omega)=S_p$

- transitive: $\forall x_1 x_2\in\Omega$, $\exists g\in G$ s.t. $g(x_1)=x_2$; x_1和x_2在G作用下的轨道是相同的, 均为Ω

  x在G下的轨道 $x^G=\{g(x): g\in G\}$

  设 $g_0(x_1)=x_2$, then $\forall g(x_1)=(g\circ g_0^{-1})(x_2)$, $g(x_2)=(g\circ g_0)(x_1)$, $\therefore x_1 x_2$同轨 (原因: $g\in G$可逆

  性质: $\forall \sigma_1,\sigma_2\in G$, σ_1,σ_2有相同的置换阶; 即$\sigma^k=id$所用的最小次数

- transposition: 两个元素间的置换 $\sigma(a)=b$, $\sigma(b)=a$

  G contains transposition σ, 即G中有一个 2-cycle $(i\ j)$

proof: 轨道定理有 $|G|=|w^G|\times|G_w|$, $\forall w\in\Omega$,

G transitive $\therefore |w^G|=|\Omega|$ $\forall w$, $|G_w|=|G|\div p$

由Cauchy定理知: p is Prime, $p\,|\,|G|$, 一定存在 $g\in G$, $o(g)=p$

$\therefore$ 不妨设 $g=(1,2,\cdots p)$,

let $(i,j)\in G$; $\underbrace{\langle(i\,j)(1\,2\cdots p)\rangle}_{\text{所以生成所有 2-cycle}}=S_p$ $\therefore G\cong Sym(\Omega)=S_p$

Th: $f(x)\in\mathbb{F}[x]$, $\mathbb{F}=\mathbb{Q}$, $f(x)$ irreducible in $\mathbb{Q}[x]$, $deg(f)=p$ 素数, 若 $f(x)$恰有2个 complex root $\Rightarrow Gal(f)\cong S_p$

proof: $f(x)=0$, $x_1=a$, $x_2=\bar{a}$, $\cdots$ $a\in\mathbb{C}$,

$Gal(f)$ act on $\Omega=\{f(x)$的解集$\}$, $\sigma\in Gal(f)$, $\sigma(i)=\pm i$, 只有2个复根 $\therefore \sigma(a)=\bar{a}$, $\sigma(\bar{a})=a$

又$\because f$ irr in $\mathbb{Q}[x]$, f separable, 在$\mathbb{Q}$中无root,

then $Gal(f)$ act on Ω transitively, $\xRightarrow{\text{综上}}$ $Gal(f)\cong S_p$

Q: 为什么transitive, $\forall\sigma\in Gal(f)$, $\sigma(i)=\pm i$ $\therefore$ 对于复根, 只有 $\begin{cases}\sigma(a)=a, \sigma(\bar{a})=\bar{a}\\ \sigma(a)=\bar{a}, \sigma(\bar{a})=a\end{cases}$ 两种情况

那其它根$\beta\in\mathbb{R}$, 要$\sigma(\beta)=a$ or $\bar{a}$, 不可能 transitive

Dummit P562: def: $Aut(K/F)$是K的automorphism, 且fix F pointwise; let K/F finite (本科不学无限Galois)

K/F is Galois extension (finite) 若 $|Aut(K/F)|=[K:F]$; 此时$Aut(K/F)$记为$Gal(K/F)$

Rmk: 结合中文书定义, 此时E/F is finite Galois extension; 即normal, separable; E/F可分定义为$\forall a\in E$, $m_{a,F}\in F[x]$可分; 故而要验证这个$\Leftrightarrow$ E is splitting field of separable f over $\mathbb{F}$; 即定义不矛盾

Corollary 6. If K is the splitting field over F of a separable polynomial $f(x)$ then K/F is Galois.

finite normal + separable

We shall see in the next section that the converse is also true, which will completely characterize Galois extensions. E/F is splitting of $f(x)$; E/F可分$\Leftrightarrow f(x)$可分

proof not in final range (But used in Exercise section)

命题 4.4 设 E 为域扩张 K/F 的中间域，K/F 和 E/F 都是有限 Galois 扩张，则 $\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$.

命题 4.5 设 E/F 是代数扩张，K/F 是有限 Galois 扩张，E是中间域 $(K \cap E = F)$ 则 KE/E 是有限 Galois 扩张，并且

proof easy

$$\mathrm{Gal}(KE/E) \cong \mathrm{Gal}(K/F).$$

例: $\underbrace{(x^5-2)(x^5-3)}_{f}=0$ $\quad \mathrm{Gal}(f) = Z_5 : Z_5 : Z_5$ by 4.4.

Example 5. $f(x) = x^p - a \in \mathbb{Q}[x]$. *Where* $\sqrt[p]{a} \notin \mathbb{Q}$. $Gal(f) \simeq Z_p : Z_{p-1} = \mathrm{Hol}(Z_P) \simeq \mathrm{Aut}(D_{2p})$ *(when* $p \neq 2$*).*

Let $\omega = e^{\frac{2\pi i}{p}}$, *root of* $x^{p-1} + \cdots + x + 1$, $\alpha = a^{\frac{1}{p}} \notin \mathbb{Q}$. *Then* $\alpha, \alpha\omega, \ldots, \alpha\omega^{p-1}$ *are the* p *roots of* $x^p - a$.
Let $E = \mathbb{Q}(\alpha, \alpha\omega, \ldots, \alpha\omega^{p-1})$. *Then* E *is a splitting field of* $x^p - a$. *Thus a normal extension of* $\mathbb{Q}$.
Let $L = \mathbb{Q}(\omega) \subset E$, *then* $\mathbb{Q} \subset L \subset E$. *And* L *is a normal extension of* $\mathbb{Q}$, *since it is a splitting field of* $x^p - 1$ *over* $\mathbb{Q}$.
Thus $\mathrm{Gal}(E/L) \lhd \mathrm{Gal}(E/\mathbb{Q})$, *and* $\mathrm{Gal}(E/\mathbb{Q})/\mathrm{Gal}(E/L) \simeq \mathrm{Gal}(L/\mathbb{Q})$.
Consider $\mathrm{Gal}(E/L)$ *and* $\mathrm{Gal}(L/\mathbb{Q})$.
Notice that if f *is irreducible,* $\mathrm{Gal}(f)$ *acts transitively on the roots of* f. *Furthermore, since* $f(x) = x^p - a$ *consider that* $\mathrm{Gal}(f)$, *you can check the action of* $\mathrm{Gal}(f)$ *has no non-trivial blocks, i.e. this action is primitive.*

Now $\mathrm{Gal}(L/\mathbb{Q})$ *is a splitting field of irreducible polynomial* $x^{p-1} + \ldots x + 1$, *so* $\mathrm{Gal}(L/\mathbb{Q})$ *is transitive on the* $p - 1$ *roots:* $\omega, \omega^2, \ldots, \omega^{p-1}$. $\sigma: \omega \mapsto \{\text{root set}\}$ $\therefore \langle\sigma\rangle \cong Z_{p-1}$
The group $\mathrm{Gal}(E/L)$, *where* $E = L(\alpha)$, *contains an element* $\rho : \alpha \to \alpha\omega \to \cdots \to \alpha\omega^{p-1}$. *And* $< \rho > \simeq Z_p$.
Claim: $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) = Z_p : Z_{p-1}$.

证明. 1. Claim $\mathrm{Gal}(E/L) =< \rho >$.
Otherwise, $\exists \tau \in \mathrm{Gal}(E/L)$ s.t. $\alpha^\tau = \alpha$, $(\alpha\omega^i)^\tau = \alpha\omega^j$ with $i \neq j$. $\tau : \omega^i \mapsto \omega^j$. But $\tau \in \mathrm{Gal}(E/L)$ i.e. τ fixes L pointwise, contradiction.
2. Claim $\mathrm{Gal}(L/\mathbb{Q}) =< \sigma >$, where $\sigma : \omega \mapsto \omega^r$ with r is a primitive root of p. i.e. $\mathrm{Ord}_p(r) = p - 1$.
Now $Z_{p-1} \simeq < \sigma > \leqslant \mathrm{Gal}(L/\mathbb{Q}) = G$. As $< \sigma >$ is a transitive subgroup of G we can write $G =< \sigma > G_\omega$. And it's obvious $G_\omega = e$.
Therefore, $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) =< \rho > \cdot < \sigma > \simeq Z_p \cdot Z_{p-1}$. Since $|Z_p|$ and $|Z_{p-1}|$ coprime, this is a splitting extension of groups. so $\mathrm{Gal}(E/\mathbb{Q}) = \mathrm{Gal}(E/L) \cdot \mathrm{Gal}(L/\mathbb{Q}) =< \rho > \cdot < \sigma > \simeq Z_p : Z_{p-1}$. ":" by extending def, $A = B \cdot C$, $B \cap C = e$ $C \leq A$. $B \lhd A \Rightarrow A = B : C$
Actually, this splitting extension is faithful. i.e. this group is exact $\mathrm{AGL}(1, p)$.

Th: f $G = N : H$, where N is abelian and regular. Let $C_G(N) = \{g \in G \mid [g, N] = 1\}$. Then $N \leqslant C$. And a trnasitive abelian group is regular (prove it !). So $N = C$. $gn = ng \ \forall n$ $\stackrel{\Delta}{=} C$

□