

1, 设 $E=Q(\sqrt{2}, \sqrt{3})$, 求 E 关于 Q 的伽罗瓦群

解: $E=Q(\sqrt{2}, \sqrt{3})=Q(\sqrt{2}+\sqrt{3})$,

且 $f(x)=x^4-10x^2+1$ 是 $\sqrt{2}+\sqrt{3}$ 在 Q 上的极小多项式

又因 $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$, $(\sqrt{2}, \sqrt{3})^3=11\sqrt{2}+9\sqrt{3}$

从而, $E=Q(\sqrt{2}, \sqrt{3})=\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6} \mid a, b, c, d \in Q\}$

则对属于 $\text{Aut}_Q(E)$ 的任意 φ , φ 由 $\varphi(\sqrt{2}), \varphi(\sqrt{3})$ 决定

因为 $\sqrt{2}$ 是 $g(x)=x^2-\sqrt{2}$ 的根, $\sqrt{3}$ 是 $h(x)=x^2-3$ 的根

所以 $\varphi(\sqrt{2}), \varphi(\sqrt{3})$ 分别是 $g(x), h(x)$ 的根, 因此 $\varphi(\sqrt{2})=\pm\sqrt{2}$, $\varphi(\sqrt{3})=\pm\sqrt{3}$

从而

$$\varphi_0=\text{id}$$

$$\varphi_1(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6}$$

$$\varphi_2(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6}$$

$$\varphi_3(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})=a+b\sqrt{2}-c\sqrt{3}-d\sqrt{6}$$

故 $\text{Aut}_Q(E)=\{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$

2, 设包含 F 的 E 是域的扩张, K, M 是中间域, H, J 是 $\text{Aut}_F(E)$ 的子群, 试证明

(1) 如果 K 包含于 M , 那么 M' 包含于 K' , 如果 H 包含于 J , 那么 J' 包含于 H'

(2) K 包含于 K'' , H 包含于 H''

(3) $K' = K''$, $H' = H''$ ($K''' = (K'')'$, $H''' = (H'')'$),

证明: (1) 因为 $M' = \text{Aut}_M(E) = \{\varphi \in \text{Aut}(E) | \varphi(a) = a, \forall a \in M\}$,

$K = \text{Aut}_F(E) = \{\varphi \in \text{Aut}(E) | \varphi(a) = a, \forall a \in K\}$,

由于 K 包含于 M , 从而对属于 M' 的任意 φ , 都有 $\varphi(a) = a$, 其中 a 属于 M ,

因此 $\varphi(a) = a$, a 属于 K , 即 φ 属于 K' , 于是 K' 包含 M'

因为 $H' = \{x \in E | \sigma(x) = x, \forall \sigma \in H\}$, $J' = \{x \in E | \sigma(x) = x, \forall \sigma \in J\}$, H 包含于 J ,

所以对属于 J' 的任意 x 都有 $\sigma(x) = x$, 任意 σ 属于 J ,

因此对属于 H 的任意 σ 也有 $\sigma(x) = x$, 即 x 属于 H' , 故 J' 包含于 H'

(2) $K'' = (K')' = \{x \in E | \sigma(x) = x, \forall \sigma \in K'\}$,

由于对属于 K 的任意 x , 对属于 K' 任意 σ 都有 $\sigma(x) = x$, 从而 x 属于 K''

故 K 包含于 K''

由于 H 为 $\text{Aut}_F(E)$ 的子群, $H' = \{x \in E | \sigma(x) = x, \forall \sigma \in H\}$,

因此 $H'' = (H')' = \{\varphi \in \text{Aut}_F(E) | \varphi(x) = x, \forall x \in H\}$,

于是对属于 H 的任意 σ , 对属于 H' 任意 x , 都有 $\sigma(x) = x$, 从而 σ 属于 H''

故 H 包含于 H''

(3) 由(2)知 K 包含于 K'' , 再由(1)知 K' 包含 $(K'')'$, 即 K' 包含 K'''

对 K' 应用(2)得 K' 包含于 $(K')'' = K'''$, 故 $K' = K'''$

由(2)知, H 包含于 H'' , 又由(1)知 $(H'')'$ 包含于 H' , 即 H''' 包含于 H'

对 H' 应用(2)得 H' 包含于 $(H')'' = H'''$, 因此 $H' = H'''$

3, 设包含 F 的 E 是域的有限扩张,

试证明包含 F 的 E 的伽罗瓦群的子群都是闭群

证明: 设 H 是包含 F 的 E 的伽罗瓦群的子群,

根据[第四章引理 6.1] $|F' : E'| \leq |E : F|$, 从而 $|H : E'| \leq |E : F|$,

因为 E' 是闭群, 所以根据[第四章定理 6.1(2)]知 H 是闭群,

4, 设包含 F 的 E 是有限伽罗瓦扩张, 试证明 $|\text{Aut}_F(E)| = |E : F|$,

证明: 由[第四章引理 6.1]得 $|F' : E'| \leq |E : F|$,

由[第四章定理 6.1(2)]有 $|E'' : F''| = |F' : E'|$

因为包含 F 的 E 是伽罗瓦扩张, 所以 $F'' = F$, 因此 $|E : F| = |F' : E'| = |F'|$

5, 设包含 F 的 E 是有限伽罗瓦扩张, K 是包含 F 的 E 的中间域, 证明 K 是闭域

证明: 因为包含 F 的 E 是有限伽罗瓦扩张,

所以 F 是闭域, $|K : F| \leq |E : F|$, 根据[第四章定理 6.1(1)], K 为闭域

6, 设 a, b 是不含平方因数的整数,

试证明包含 Q 的 $Q(\sqrt{a}, \sqrt{b})$ 是伽罗瓦扩张, 并确定其对应的伽罗瓦群,

证明: $Q(\sqrt{a}, \sqrt{b}) = Q(\sqrt{a} + \sqrt{b})$,

且 $f(x) = x^4 + (2a^2 - 4a - 4ab + 2b^2)x^2 + (a - b)^2$ 是 $\sqrt{a} + \sqrt{b}$ 在 Q 上的极小多项式,

又因 $Q(\sqrt{a}, \sqrt{b}) = \{k_0 + k_1\sqrt{a} + k_2\sqrt{b} + k_3\sqrt{ab} \mid k_i \in Q, i = 0, 1, 2, 3\}$,

则任意 φ 属于 $\text{Aut}_Q(E)$, φ 由 $\varphi(\sqrt{a}), \varphi(\sqrt{b})$ 决定,

因为 $\sqrt{a}$ 是 $g(x) = x^2 - a$ 的根, $\sqrt{b}$ 是 $h(x) = x^2 - b$ 的根,

所以 $\varphi(\sqrt{a}), \varphi(\sqrt{b})$ 分别是 $g(x), h(x)$ 的根,

因此 $\varphi(\sqrt{a}) = \pm\sqrt{a}, \varphi(\sqrt{b}) = \pm\sqrt{b}$, 因此 $\text{Aut}_Q Q(\sqrt{a} + \sqrt{b}) = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$,

由固域定义可知包含 Q 的 $Q(\sqrt{a}, \sqrt{b})$ 是伽罗瓦扩张,

7, 设 $\text{Char } F=0$, E 是 $F[x]$ 中属于 $F[x]$ 的不可约元 $f(x)$ 在 F 上的分裂域, 试证明 E 是 F 的伽罗瓦扩张

证明: 因为包含 F 的 E 是有限扩张,

所以由[第四章推论 3.2]可知, 包含 F 的 E 是单代数扩张,

设 $E=F(\alpha)$, α 在 F 上的极小多项式为 $g(x)$,

则 $\text{Aut}_F(E)$ 中的任意元素 σ 由 $\sigma(\alpha)$ 决定, 且 $\sigma(\alpha)$ 是 $g(x)$ 的根,

由[第四章定理 4.3]可知, 包含 F 的 E 是正规扩张, 进而 $g(x)$ 的根都属于 E ,

因此, $|\text{Aut}_F(E)|$ 等于 $g(x)$ 的不同根的个数,

由[第三章定理 9.4]可知, $g(x)$ 没有重根, 所以, $|\text{Aut}_F(E)|=\deg g(x)=|E:F|$,

因为 F 包含于 F'' , 所以 E 是 $f(x)$ 在 F'' 上的分裂域, 因此, $|\text{Aut}_{F''}(E)|=|E:F''|$

再由 $\text{Aut}_{F''}(E)=\text{Aut}_F(E)$ 及 $|E:F|=|E:F''||F'':F|$ 可得 $|F'':F|=1$, 即 $F=F''$

从而, 包含 F 的 E 是伽罗瓦扩张

习题 1 设 F 是域, 证明 $E=\{a \in F | \sigma(a)=a, \forall \sigma \in \text{Aut}(F)\}$ 是域,

证明: 显然 $0, 1$ 属于 F , 若 a, b 属于 E , 则对属于 $\text{Aut}(F)$ 的任意 σ ,

有 $\sigma(a-b)=\sigma(a)-\sigma(b)=a-b$, $\sigma(ab^{-1})=\sigma(a)\sigma(b)^{-1}=ab^{-1}$

即 $a-b, ab^{-1}$ 属于 $\text{Aut}(F)$, 因此 E 是域, 称为 F 的固定域

习题 2 设 α 是 x^3-2 的一个根, 求 $Q(\alpha)$ 的自同构群,

解: 设 φ 是 $Q(\alpha)$ 的自同构, 则对整数 m , 有 $\varphi(m)=m\varphi(1)=m$,

从而 φ 是 Q 的恒等映射,

由 α 是 x^3-2 的一个根可得 $\varphi(\alpha)$ 是 x^3-2 的一个根, 于是 $\varphi(\alpha)=\alpha$

由于 x^3-2 是有理数域上的不可约多项式, 故 $Q(\alpha)$ 的元素形式为 $a_0+a_1\alpha+a_2\alpha^2$

因此 φ 是恒等映射, $Q(\alpha)$ 的自同构群只有一个元素

习题 3 设 F 是特征不等于 2 的域, α 是 F 上不可约多项式 x^2-a 的一个根, 求 $\text{Aut}_F(F(\alpha))$,

解: 设 φ 属于 $\text{Aut}_F(F(\alpha))$,

由 α 是 x^2-a 的一个根可得 $\varphi(\alpha)$ 是 x^2-a 的一个根, 于是 $\varphi(\alpha)=\pm\alpha$,

由于 x^2-a 是不可约多项式, 故 $F(\alpha)$ 的元素形式为 $c+d\alpha$, 其中 c, d 属于 F ,

因此 $\varphi(c+d\alpha)=c+d\alpha$ 或 $\varphi(c+d\alpha)=c-d\alpha$,

习题 4 设 α 是域 F 上的代数元, $f(x)$ 是 α 在域 F 上的极小多项式,

试证明 $|\text{Aut}_F(F(\alpha))|$ 等于 $F(\alpha)$ 中 $f(x)$ 的互异根的个数,

特别地, 当且仅当 $f(x)$ 无重根时,

$|\text{Aut}_F(F(\alpha))| \leq |F(\alpha) : F| = \deg f(x)$, 且等号成立, 且 $f(x)$ 的所有根均在 $F(\alpha)$ 中,

证明: 若 σ 属于 $\text{Aut}_F(F(\alpha))$,

则由 α 是 $f(x)$ 的根知, 属于 $F(\alpha)$ 的 $\sigma(\alpha)$ 是 $f(x)$ 的一个根

反之, 若属于 $F(\alpha)$ 的 β 是 $f(x)$ 的一个根, 则 $F(\beta)$ 包含于 $F(\alpha)$,

再由 $|F(\beta) : F| = \deg f(x) = |F(\alpha) : F|$ 知 $F(\beta) = F(\alpha)$,

从而存在域同构 $\sigma : F(\alpha) \rightarrow F(\beta)$, 使得 $\sigma(\alpha) = \beta, \sigma|_F = \text{id}$

故 σ 属于 $\text{Aut}_F(F(\alpha))$

习题 5 设 F 是域, 属于 $F[x]$ 的 $f(x)$ 在 F 上的分裂域为 E , 且在 E 上 $f(x)$ 无重根,

试证明属于 $\text{Aut}_F(E)$ 的 σ 是 $f(x)$ 的所有根构成集合上的一个置换,

证明: 只需证明 $f(x)$ 的根在 σ 下的像是 $f(x)$ 的根,

若 α 是 $f(x)$ 的根, 由 $\sigma(f(\alpha)) = f(\sigma(\alpha))$ 知 $\sigma(\alpha)$ 是 $f(x)$ 的一个根,

习题 6 设 $K \supseteq E \supseteq F$, E 是 F 的正规扩张, σ 是 K 的 F -自同构, 则 $\sigma(E) = E$,

证明: 设 α 属于 E , $f(x)$ 为 α 在 F 上的极小多项式, 于是 $0 = \sigma(f(\alpha)) = f(\sigma(\alpha))$,

由于 E 是 F 的正规扩张, 故 $\sigma(\alpha)$ 属于 E , 因此 $\sigma(E)$ 包含于 E ,

于是 $E = \sigma(\sigma^{-1}(E)) \subseteq \sigma(E) \subseteq E$, 因此 $\sigma(E) = E$,

习题 7 设 K 包含 F , $f(x)$ 属于 $F[x]$, $f(x)$ 在 F 上的分裂域为 E ,
在 K 上的分裂域为 L , 试证明 $\text{Aut}_K(L)$ 同构于 $\text{Aut}_F(E)$ 的一个子群

证明: $f(x)$ 在 L 和 E 中都可以分解为一次因式的乘积

而由在包含 L 和 E 的域中 $f(x)$ 的分解式是唯一的

可设 $f(x)$ 在 L 和 E 中分解为 $f(x)=a(x-a_1)\cdots(x-a_n)$,

则 $E=F(a_1, \dots, a_n)\subseteq K(a_1, \dots, a_n)=L$

若 σ 属于 $\text{Aut}_K(L)$, 由上题知 $\sigma(E)=E$,

从而可以定义映射 $\varphi: \text{Aut}_K(L)\rightarrow\text{Aut}_F(E), \sigma\rightarrow\sigma|_E$

当 $\sigma|_E$ 是恒等映射时, σ 是恒等映射, 即 $\sigma\rightarrow\sigma|_E$ 是单射,

且保持运算, 从而是单同态,

故 $\text{Aut}_K(L)$ 同构于 $\text{Aut}_F(E)$ 的一个子群

习题 8 求 x^8-1 在 Q 上的分裂域 E , 计算 $|E:Q|$, 并确定伽罗瓦群 $\text{Aut}_Q(E)$,

解: 令 $\alpha_k=\cos \frac{k\pi}{4} +i\sin \frac{k\pi}{4}$, $k=0, 1, \dots, 7$,

则 x^8-1 在 Q 上的分裂域 E 为 $Q(i, \sqrt{2})$, 得 $|E:Q|=|Q(i, \sqrt{2}):Q(i)||Q(i):Q|=4$

若 σ 属于 $\text{Aut}_Q(E)$, 则 $\sigma(\sqrt{2})=\pm\sqrt{2}$, $\sigma(i)=\pm i$,

习题 9 令 $E=Q(\sqrt{2}, \sqrt{3})$, 确定包含 Q 的 E 的所有子域及 $\text{Aut}_Q(E)$ 的所有子群,

解: $E=Q(\sqrt{2}, \sqrt{3})$ 是 Q 上不可约多项式 $f(x)=x^4-10x^2+1$ 的分裂域,

因此包含 Q 的 E 是伽罗瓦扩张,

$\text{Aut}_Q(E)=\{\varphi_0, \varphi_1, \varphi_2, \varphi_3\}$,

其中 $\varphi_0=1$, $\varphi_1(\sqrt{2})=-\sqrt{2}$, $\varphi_1(\sqrt{3})=\sqrt{3}$, $\varphi_2(\sqrt{2})=-\sqrt{2}$, $\varphi_2(\sqrt{3})=-\sqrt{3}$, $\varphi_3=\varphi_1\varphi_2$

$\text{Aut}_Q(E)$ 有 5 个子群 $\langle 1 \rangle, \langle \varphi_1 \rangle, \langle \varphi_2 \rangle, \langle \varphi_3 \rangle$ 和 $\text{Aut}_Q(E)$,

$\{1\}$ 的固定域为 E , $\langle \varphi_1 \rangle$ 的固定域为 $Q(\sqrt{3})$, $\langle \varphi_2 \rangle$ 的固定域为 $Q(\sqrt{6})$,

$\langle \varphi_3 \rangle$ 的固定域为 $Q(\sqrt{2})$, $\text{Aut}_Q(E)$ 的固定域为 Q ,

因为 $\text{Aut}_Q(E)$ 的子群都是正规子群,

所以包含 F 的 E 的中间域对 Q 的扩张都是正规扩张,

习题 10 令 θ 是本原 n 次单位根，证明 $|\text{Aut}_Q Q(\theta)|$ 是 $\varphi(n)$ (欧拉函数) 的因数

证明: σ 属于 $\text{Aut}_Q Q(\theta)$ ，则 $\sigma(\theta)$ 也是本原 n 次单位根，

即存在唯一 $k(\sigma)$ 使得 $\sigma(\theta) = \theta^{k(\sigma)}$ ，其中 $1 \leq k(\sigma) \leq n$ 且 $(k(\sigma), n) = 1$ ，

令 $G = \{\bar{k} \mid (k, n) = 1\}$ ，易证 G 关于 $\mathbb{Z}_n$ 的乘法运算是群，

定义映射 $\varphi : \text{Aut}_Q Q(\theta) \rightarrow G, \sigma \rightarrow \overline{k(\sigma)}$

若 τ 属于 $\text{Aut}_Q Q(\theta)$ 且 $\tau(\theta) = \theta^{k(\tau)}$ ，则 $\theta^{k(\tau\sigma)} = (\tau\sigma)(\theta) = \tau(\sigma(\theta)) = \tau(\theta^{k(\sigma)}) = \theta^{k(\tau)k(\sigma)}$

即 $n \mid k(\tau\sigma) - k(\tau)k(\sigma)$ ，

于是 $\varphi(\tau\sigma) = \varphi(\tau)\varphi(\sigma)$ ， φ 是群同态，

若 $\overline{k(\sigma)} = \bar{1}$ ，则 $\sigma = 1$ ，即 φ 是群单同态，

于是 $\text{Aut}_Q Q(\theta)$ 可视为 G 的子群， $|G| = \varphi(n)$