

(以下设  $F$  是域, 且  $\text{Char } F=0$ )

1, 设包含  $F$  的  $E$  是有限伽罗瓦扩张,

包含于  $M$  的  $K$  是包含  $F$  的  $E$  的中间域,  $M'$  是  $K'$  的正规子群,

试证明包含  $K$  的  $M$  是有限伽罗瓦扩张,

**证明:** 由[第四章推论 8.1]得有限伽罗瓦扩张等价于正规扩张,

由[第四章推论 4.2]得包含  $K$  的  $E$  是有限伽罗瓦扩张,

因为  $M'$  是  $K'$  的正规子群,

所以由[第四章定理 6.2(3)]得包含  $K$  的  $M$  是正规扩张, 从而是有限伽罗瓦扩张,

2, 设  $p$  是素数,  $a$  属于  $F$ ,

试证明多项式  $x^p-a$  或为  $F$  的不可约元, 或在  $F$  上有根

**证明:** 若  $\text{Char } F=p$ , 则  $x^p=x$ , 其中  $x$  属于  $F$ ,

从而  $a$  是  $x^p-a$  的根,  $x^p-a$  在  $F$  上有根

若  $\text{Char } F \neq p$ , 设  $b^p=a$ , 若  $b$  属于  $F$ , 则  $x^p-a$  在  $F$  上有根,

若不存在属于  $F$  的  $b$  满足  $b^p=a$ , 则  $f(x)$  在  $F$  上无根,

设  $f(x)=x^p-a$  在其分裂域上的分解式为  $f(x)=(x-b)(x-b\zeta)\cdots(x-b\zeta^{p-1})$ ,

其中  $\zeta$  为本原  $p$  次单位根,

若  $f(x)$  在  $F$  上可约, 则存在属于  $F[x]$  的  $g(x)$ , 使得  $g(x)|f(x)$ ,

那么  $g(x)$  的常数项为属于  $F$  的  $(-1)^r b^r \prod_{k=1}^r \zeta^{ik}$ ,  $r < p$ ,

令  $\eta = \prod_{k=1}^r \zeta^{ik}$ , 则  $\eta$  为  $p$  次单位根,  $b^r \eta$  属于  $F$ .

因为  $(r, p)=1$ , 故存在属于  $\mathbb{Z}$  的  $u, v$  使得  $ru+pv=1$ ,

故  $b\eta = (b\eta)^{ru+pv} = (b^r \eta)^u \eta^{ru-u} a^v$

从而  $b\eta^{1+u-ru} = (b^r \eta)^u a^v$  属于  $F$ ,  $\eta^{1+u-ru}$  为  $p$  次单位根, 故  $(b\eta^{1+u-ru})^p = a$ , 矛盾

3, 设  $p$  是素数, 域  $F$  包含所有  $p$  次单位根,

求属于  $F[x]$  的多项式  $x^p - a$  的伽罗瓦群

**证明:**  $x^p - a$  在其分裂域  $E$  上的分解式为  $x^p - a = (x - b)(x - b\zeta) \cdots (x - b\zeta^{p-1})$ ,

其中  $\zeta$  为本原  $p$  次单位根,  $E = F(b)$ ,  $b^p$  属于  $F$

因为属于  $\text{Aut}_F(E)$   $\sigma$  由  $\sigma(b)$  决定, 而  $\sigma(b)$  也是  $x^p - a$  的根,

所以, 若  $b$  属于  $F$ , 则  $\text{Aut}_F(E) = \{\text{id}\}$

若  $b$  不属于  $F$ , 则  $\text{Aut}_F(E) = \{\sigma_i | \sigma_i(b) = b\zeta^i\}$  是  $p$  阶循环群

4, 设  $p$  是素数, 域  $F$  包含所有  $p$  次单位根,  $E = F(\alpha)$ ,  $\alpha$  不属于  $F$ ,  $\alpha^p$  属于  $F$ ,

试证明属于  $F[x]$  的  $f(x) = x^p - \alpha^p$  是不可约元

**证明:**  $x^p - \alpha^p$  在其分裂域上的分解式为  $x^p - \alpha^p = (x - \alpha)(x - \alpha\zeta) \cdots (x - \alpha\zeta^{p-1})$ ,

其中  $\zeta$  为本原  $p$  次单位根,

因为  $\alpha$  不属于  $F$ ,  $\zeta$  属于  $F$ , 所以  $x^p - \alpha^p$  在  $F$  上无根,

若  $f(x)$  在  $F$  上可约, 则存在属于  $F[x]$  的  $g(x)$ , 使得  $g(x) | f(x)$ ,

那么  $g(x)$  的常数项为属于  $F$  的  $(-1)^r b^r \prod_{k=1}^r \zeta^{ik}$ ,  $r < p$ ,

令  $\eta = \prod_{k=1}^r \zeta^{ik}$ , 则  $\eta$  为  $p$  次单位根,  $\alpha^r \eta$  属于  $F$ .

因为  $(r, p) = 1$ , 故存在属于  $\mathbb{Z}$  的  $u, v$  使得  $ru + pv = 1$ ,

故  $\alpha\eta = (\alpha\eta)^{ru+pv} = (\alpha^r \eta)^u \eta^{ru-u} \alpha^{pv}$

从而  $\alpha\eta^{1+u-ru} = (\alpha^r \eta)^u \alpha^{pv}$  属于  $F$ ,  $\eta^{1+u-ru}$  为  $p$  次单位根, 故  $(\alpha\eta^{1+u-ru})^p = \alpha^p$ , 矛盾,

5, 令  $f(x) = x^3 + 2x + 1$  属于  $\mathbb{Q}[x]$ , 试求  $f(x)$  的伽罗瓦群,

**解:**  $f(x) = x^3 + 2x + 1$  在  $\mathbb{Q}$  上不可约,  $f(x)$  有两个复数根,

所以  $f(x)$  在  $\mathbb{Q}$  上的伽罗瓦群为  $S_3$

**习题 1** 设域  $F$  特征为零, 证明  $F$  上  $n$  ( $n=3, 4$ ) 次多项式  $f(x)$  可以用根式解

**证明:**  $f(x)$  的伽罗瓦群是  $S_n$  的子群,  $S_3, S_4$  是可解群, 其子群也是可解群,

于是  $f(x)$  在  $F$  上可以用根式解,

**习题 2** 试证明包含  $\mathbb{Q}$  的  $\mathbb{Q}(\sqrt[3]{2})$  不是伽罗瓦扩张，

**证明：** 因为不可约多项式  $x^3-2$  的一个根  $\sqrt[3]{2}$  在域  $\mathbb{Q}(\sqrt[3]{2})$  中，

另一个根  $\sqrt[3]{2} \frac{-1+i\sqrt{3}}{2}$  不在域  $\mathbb{Q}(\sqrt[3]{2})$  中，

所以包含  $\mathbb{Q}$  的  $\mathbb{Q}(\sqrt[3]{2})$  不是正规扩张，从而不是伽罗瓦扩张

**习题 3** 举例说明在扩张  $K \supseteq E \supseteq F$  中，

即使包含  $E$  的  $K$  和包含  $F$  的  $E$  都是伽罗瓦扩张，

包含  $F$  的  $K$  也不一定是伽罗瓦扩张，

**解：** 由于  $\mathbb{Q}(\sqrt{2})$  是多项式  $x^2-2$  在有理数域上的分裂域，

因此包含  $\mathbb{Q}$  的  $\mathbb{Q}(\sqrt{2})$  是正规扩张，从而是伽罗瓦扩张，

同理包含  $\mathbb{Q}(\sqrt{2})$  的  $\mathbb{Q}(\sqrt[4]{2})$  也是伽罗瓦扩张，

但是  $x^4-2=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-\sqrt[4]{2}i)(x+\sqrt[4]{2}i)$ ，

所以包含  $\mathbb{Q}$  的  $\mathbb{Q}(\sqrt[4]{2})$  不是正规扩张，从而不是伽罗瓦扩张

**习题 4** 设域  $F$  上多项式  $f(x)$  在  $F$  中有一个根  $\alpha$ ，

试证明  $f(x)$  的伽罗瓦群与  $\frac{f(x)}{x-\alpha}$  的伽罗瓦群相同，

**证明：** 因为  $\alpha$  属于  $F$ ，所以  $f(x)$  和  $\frac{f(x)}{x-\alpha}$  在  $F$  上的分裂域相同，从而伽罗瓦群相同

**习题 5** 求  $\mathbb{Q}[x]$  中多项式  $x^5-1$  的分裂域及其分裂域的  $\mathbb{Q}$ -自同构的个数

**解：** 所求分裂域为  $\mathbb{Q}(\alpha)$ ，其中  $\alpha = \cos \frac{2\pi}{5} + \sqrt{-1} \sin \frac{2\pi}{5}$

$f(x)=x^4+x^3+x^2+x+1$  是  $\alpha$  在有理数域上的极小多项式，因此  $|\mathbb{Q}(\alpha) : \mathbb{Q}|=4$ ，

因为包含  $\mathbb{Q}$  的  $\mathbb{Q}(\alpha)$  是正规扩张，进而是伽罗瓦扩张，

所以  $\mathbb{Q}(\alpha)$  的  $\mathbb{Q}$ -自同构的个数为 4

**习题 6** 求属于  $Q[x]$  的多项式  $f(x)=x^3-2$  的伽罗瓦群，

**解:**  $f(x)$  在  $Q$  上的分裂域为  $E=Q(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})=Q(\sqrt[3]{2}, 3)$

由  $|E:Q|=6$  知  $|\text{Aut}_Q(E)|=6$ ,

令  $\tau, \varphi$  属于  $\text{Aut}_Q(E)$ , 其中  $\tau(\sqrt[3]{2})=\sqrt[3]{2}, \tau(\omega)=\omega^2, \varphi(\sqrt[3]{2})=\omega\sqrt[3]{2}, \varphi(\omega)=\omega$ ,

验证可知  $\tau$  是 2 阶元素,  $\varphi$  是 3 阶元素,

因为  $f(x)$  无重根, 其伽罗瓦群是  $S_3$  的子群,

于是群  $\langle \tau, \varphi \rangle$  的阶为 6, 即  $\text{Aut}_Q(E)=S_3$

**习题 7** 设  $F$  是特征为零的域,  $\theta$  是本原  $n$  次单位根,  $E=F(\theta)$ ,

试证明包含  $F$  的  $E$  是伽罗瓦扩张, 其伽罗瓦群是交换群,

**证明:** 因为多项式  $x^n-1$  的每个根都可以表示为  $\theta$  幂的形式,

所以  $x^n-1$  在  $F$  上的分裂域为  $E=F(\theta)$ , 故包含  $F$  的  $E$  是伽罗瓦扩张,

设  $\sigma, \tau$  属于  $\text{Aut}_F(E)$ ,

因为  $\sigma, \tau$ , 将  $x^n-1$  的根映为  $x^n-1$  的根, 所以存在  $s, t$  使得  $\sigma(\theta)=\theta^s, \tau(\theta)=\theta^t$

故  $\tau\sigma(\theta)=\tau(\theta^s)=\theta^{st}=\sigma\tau(\theta)$ , 即  $\sigma\tau=\tau\sigma$ ,  $\text{Aut}_F(E)$  是交换群,

**习题 8** 设  $F$  是域, 且包含所有  $n$  次单位根,  $\alpha$  是属于  $F[x]$  的  $x^n-a$  的根,  $E=F(\alpha)$ ,

试证明当  $\text{Char } F=0$  或  $\text{Char } F=p \neq 0$  且  $(p, n)=1$ ,

则  $E$  关于  $F$  的伽罗瓦群是循环群

**证明:** 若  $\alpha=0$ , 结论显然成立, 下设  $\alpha \neq 0$ ,

对属于  $\text{Aut}_F(E)$  的任意  $\sigma$ ,  $\sigma(\alpha)$  也是属于  $F[x]$  的  $x^n-a$  的根,

且  $(\sigma(\alpha))\alpha^{-1}$  是  $n$  次单位根, 设为  $\theta_\sigma$  (不必是本原  $n$  次单位根, 但与  $\sigma$  有关),

从而  $\sigma(\alpha)=\theta_\sigma\alpha$ ,

定义  $\text{Aut}_F(E)$  到  $n$  次单位根构成的  $n$  阶循环群的映射:  $\sigma \rightarrow \theta_\sigma$

这个映射为群同态, 且当  $\theta_\sigma=1$  时,  $\sigma$  是恒等映射,

因此上述映射为群单同态映射, 于是  $\text{Aut}_F(E)$  是  $n$  次单位根群的子群,

从而是循环群,

**习题 9** 令  $E$  是多项式  $f(x)=x^4-2$  在有理数域上的分裂域，

试确定包含  $Q$  的  $E$  的所有子域及  $\text{Aut}_Q(E)$  的所有子群

**解:** 由  $f(x)=(x-\sqrt[4]{2})(x+\sqrt[4]{2})(x-i\sqrt[4]{2})(x+i\sqrt[4]{2})$  得分裂域  $E=Q(\sqrt[4]{2}, i)$ ,

从而扩张次数为  $|E:Q|=|Q(\sqrt[4]{2}, i):Q(\sqrt[4]{2})||Q(\sqrt[4]{2}):Q|=8$ ,  $|\text{Aut}_Q(E)|=8$ ,

易知  $\varphi, \sigma$  属于  $\text{Aut}_Q(E)$ , 其中  $\varphi(i)=i$ ,  $\varphi(\sqrt[4]{2})=i\sqrt[4]{2}$ ,  $\tau(i)=-i$ ,  $\tau(\sqrt[4]{2})=\sqrt[4]{2}$

验证可知  $\langle \varphi, \tau \rangle$  是  $\text{Aut}_Q(E)$  的 8 阶子群, 从而  $\text{Aut}_Q(E)=\langle \varphi, \tau \rangle$ ,

$\text{Aut}_Q(E)$  的一阶子群为  $\{1\}$ , 固定域为  $E$ ,

二阶子群为  $\langle \varphi^2 \rangle, \langle \tau \rangle, \langle \tau\varphi \rangle, \langle \tau\varphi^2 \rangle, \langle \tau\varphi^3 \rangle$

四阶子群为  $\langle \varphi \rangle, \langle \tau\varphi^2 \rangle, \langle \tau\varphi, \varphi^2 \rangle$

八阶子群为  $\text{Aut}_Q(E)$ , 固定域为  $Q$ ,

下面求  $\langle \tau, \varphi^2 \rangle$  的固定域,

设  $E$  的任意元素  $a=a_0+a_1\sqrt[4]{2}+a_2(\sqrt[4]{2})^2+a_3(\sqrt[4]{2})^3+b_0i+b_1i\sqrt[4]{2}+b_2i(\sqrt[4]{2})^2+b_3i(\sqrt[4]{2})^3$

则  $\tau(a)=a_0+a_1\sqrt[4]{2}+a_2(\sqrt[4]{2})^2+a_3(\sqrt[4]{2})^3-b_0i-b_1i\sqrt[4]{2}-b_2i(\sqrt[4]{2})^2-b_3i(\sqrt[4]{2})^3$

$\varphi^2(a)=a_0-a_1\sqrt[4]{2}+a_2(\sqrt[4]{2})^2-a_3(\sqrt[4]{2})^3+b_0i-b_1i\sqrt[4]{2}+b_2i(\sqrt[4]{2})^2-b_3i(\sqrt[4]{2})^3$

若  $\tau(a)=a=\varphi^2(a)$ , 则  $a=a_0+a_2(\sqrt[4]{2})^2$ , 即  $\langle \tau, \varphi^2 \rangle$  的固定域为  $Q(\sqrt{2})$

类似地, 二阶子群为  $\langle \varphi^2 \rangle, \langle \tau \rangle, \langle \tau\varphi \rangle, \langle \tau\varphi^2 \rangle, \langle \tau\varphi^3 \rangle$  的固定域依次为

$Q(i, \sqrt{2}), Q(\sqrt[4]{2}), Q((1+i)\sqrt[4]{2}), Q(i\sqrt[4]{2}), Q((1-i)\sqrt[4]{2})$ ,

四阶子群  $\langle \varphi \rangle, \langle \tau\varphi, \varphi^2 \rangle$  的固定域为  $Q(i), Q(i\sqrt{2})$ ,