抽象代数学

回忆：一个群G作用在一个集合X上，即$G\times X\to X$.

这个作用是忠实的$\Longleftrightarrow$若$g.x=x$ $\forall x\in X$，则$g=e$

这个作用是可迁的$\Longleftrightarrow$ $\forall x,y\in X$，$\exists g\in G$ $g.x=y$.

记号：$\mathbb{F}\subseteq\mathbb{E}$ 域扩张.

$\mathrm{Aut}_{\mathbb{F}}\mathbb{E}=\{\sigma:\mathbb{E}\to\mathbb{E}$ 域同构 $|\ \sigma|_{\mathbb{F}}=id\}$

命题 设$\mathbb{F}$域，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$，$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域，$\mathbb{L}$，$\mathbb{L}'$是两个中间域，$\mathbb{F}\subseteq\mathbb{L}\subseteq\mathbb{E}$，$\mathbb{F}\subseteq\mathbb{L}'\subseteq\mathbb{E}$，$\sigma:\mathbb{L}\to\mathbb{L}'$域同构，满足$\sigma|_{\mathbb{F}}=id$ 则σ可扩充为一个域自同构$\tau\in\mathrm{Aut}_{\mathbb{F}}\mathbb{E}$.

这是上一讲最后定理特殊情形，$f(x)\in\mathbb{F}[x]\subseteq\mathbb{L}[x]$，$\mathbb{E}$是$f(x)$在$\mathbb{L}$上分裂域，也是$\sigma(f(x))$在$\mathbb{L}'$上分裂域.

$$\begin{tikzcd}
\mathbb{E} \arrow[r, dashed, "\tau"] & \mathbb{E} \\
\mathbb{L} \arrow[u, "\subseteq"] \arrow[r, "\sigma"] & \mathbb{L}' \arrow[u, "\subseteq"'] \\
\mathbb{F} \arrow[u, "\subseteq"] \arrow[r, equal] & \mathbb{F} \arrow[u, "\subseteq"']
\end{tikzcd}$$

命题 设 $K \subseteq \mathbb{L}$ 域扩张，$f(x) \in K[x]$.

(a) 若 $\sigma \in \mathrm{Aut}_K \mathbb{L}$，则 σ 给出 $f(x)$ 在 $\mathbb{L}$ 中的根的重排；

(b) 若 $\mathbb{L}$ 是 $f(x)$ 在 K 上分裂域，则 $\mathrm{Aut}_K(\mathbb{L})$ 在 $f(x)$ 的根的集合上作用是忠实的. 这个作用在 $f(x)$ 的不可约因子的根集上作用是可迁的.

证明：(a) 设 $\sigma \in \mathrm{Aut}_K \mathbb{L}$，$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$

设 $\alpha \in \mathbb{L}$，$f(\alpha) = 0$. 则 $f(\sigma(\alpha)) = a_0 + a_1 \sigma(\alpha) + \cdots + a_n \sigma(\alpha)^n$

$$= \sigma(f(\alpha)) = 0$$

即 $\sigma(\alpha) \in \mathbb{L}$ 也是 $f(x)$ 的根. 令 X 是 $f(x)$ 在 $\mathbb{L}$ 中全体互异根的集合. 则 $\mathrm{Aut}_K \mathbb{L}$ 作用在 X 上：

$\forall \alpha \in X$，$\sigma(\alpha) \in X$.

设 $X = \{\alpha_1, \alpha_2, \cdots, \alpha_k\}$ $\quad \sigma \longmapsto \begin{pmatrix} \alpha_1 & \alpha_2 & \cdots & \alpha_k \\ \sigma(\alpha_1) & \sigma(\alpha_2) & \cdots & \sigma(\alpha_k) \end{pmatrix}$

(b) 若 $\mathbb{L} = K(\alpha_1, \cdots, \alpha_k)$ $\quad X = \{\alpha_1, \cdots, \alpha_k\}$ 是 $f(x)$ 全部互异根集合. 若 $\sigma \in \mathrm{Aut}_K \mathbb{L}$，$\underset{i=1,\cdots,k}{\sigma(\alpha_i) = \alpha_i} \Rightarrow \sigma(x) = x \ \forall x \in \mathbb{L}$

$\Rightarrow \sigma = \mathrm{id}$. 设 $p(x) \mid f(x)$，$p(x)$ 不可约. α, β 是 $p(x)$ 的

两根，正如上一讲

$$\begin{tikzcd}
\mathbb{F} \arrow[r, equal] \arrow[d, hook] & \mathbb{F} \arrow[d, hook] \\
\mathbb{F}(\alpha) \arrow[r, "\sim"] \arrow[d] & \mathbb{F}(\beta) \arrow[d] \\
\mathbb{L} \arrow[r, "\exists\sigma", "\sim"'] & \mathbb{L}
\end{tikzcd}$$

$\sigma(\alpha)=\beta$. 证毕.

由命题，设$\mathbb{E}$是$f(x)$在$\mathbb{F}$上分裂域，$f(x)=p_1^{e_1}(x)\cdots p_s^{e_s}(x)$

$p_i(x)\in\mathbb{F}[x]$不可约，全部互异零点为$\alpha_{i1},\cdots,\alpha_{in_i}\in\mathbb{E}$.

$i=1,\cdots,s$

则$f(x)$的全部互异零点为$\{\alpha_{11},\cdots,\alpha_{1n_1},\alpha_{21},\cdots,\alpha_{2n_2},\cdots,\alpha_{s1},\cdots,\alpha_{sn_s}\}$

令$m=n_1+\cdots+n_s\leq \deg f(x)$

定义
$$\mathrm{Aut}_{\mathbb{F}}\mathbb{E}\xrightarrow{\Phi} S_m$$
$$\sigma\longmapsto\begin{pmatrix}\alpha_{11}\cdots\alpha_{1n_1} & \alpha_{21}\cdots\alpha_{2n_2} & \cdots & \alpha_{s1}\cdots\alpha_{sn_s}\\ \sigma(\alpha_{11})\cdots\sigma(\alpha_{1n_1}) & \cdots & \cdots & \sigma(\alpha_{s1})\cdots\sigma(\alpha_{sn_s})\end{pmatrix}$$

定理 Φ是一个单的群同态

例 $f(x)=(x^2-2)(x^2-3)\in\mathbb{Q}[x]$

$\mathbb{Q}\subseteq\mathbb{C}$，在$\mathbb{C}$中$f(x)$全部根$\alpha_1=\sqrt{2}$，$\alpha_2=-\sqrt{2}$，$\alpha_3=\sqrt{3}$，$\alpha_4=-\sqrt{3}$

$\mathbb{E}$是$f(x)$在$\mathbb{Q}$上分裂域，则$\mathbb{E}=\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3,\alpha_4)$

$= \mathbb{Q}(\sqrt{2},\sqrt{3})$

$$\mathrm{Aut}_{\mathbb{Q}}\mathbb{E} \xrightarrow{\Phi} S_4$$

$$\mathrm{Im}\,\Phi = \left\{ \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_3 & \alpha_4 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_1 & \alpha_2 & \alpha_4 & \alpha_3 \end{pmatrix}, \begin{pmatrix} \alpha_1 & \alpha_2 & \alpha_3 & \alpha_4 \\ \alpha_2 & \alpha_1 & \alpha_4 & \alpha_3 \end{pmatrix} \right\}$$

定理 若$\mathbb{F}$是一个域，$\mathrm{char}\,\mathbb{F}=0$，$f(x)\in\mathbb{F}[x]$，$\deg f(x)>0$．$\mathbb{E}$是一个分裂域（$f(x)$在$\mathbb{F}$上分裂域），则有

$$|\mathrm{Aut}_{\mathbb{F}}\mathbb{E}| = [\mathbb{E}:\mathbb{F}]$$

由前一定理，$|\mathrm{Aut}_{\mathbb{F}}\mathbb{E}|<\infty$，为了证明定理，先证明

Primitive element theorem.

定理 设$\mathbb{F}$是一个域，$\mathrm{char}\,\mathbb{F}=0$，则$\mathbb{F}$上有限维扩张是单代数扩张．

证明：设$\mathbb{E}$是$\mathbb{F}$的有限维扩张，则存在代数元$\alpha_1,\cdots,\alpha_l\in\mathbb{E}$，$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_l)$．设$\mathbb{L}=\mathbb{F}(a,b)$　$a=\alpha_1$，$b=\alpha_2$

a,b在$\mathbb{F}$上极小多项式为$p(x)$，$q(x)$．$p(x)$，$q(x)$的全部互异根为$a=a_1,a_2,\cdots,a_s$，$b=b_1,\cdots,b_t$（存在$\mathbb{F}$的扩域

K包含全部 a_i, b_j)，令 $\lambda \in \mathbb{F}$，满足

$$\lambda \neq \frac{a_i - a}{b - b_j} \quad \forall i = 1, \cdots, s,\ j = 2, \cdots, t$$

(因为 $\operatorname{char}\mathbb{F} = 0$，$\mathbb{F}$中有无穷个元，这样的$\lambda$存在)

令 $c = a + \lambda b \quad \mathbb{F}(c) \subseteq \mathbb{F}(a, b)$

考虑多项式 $q(x)$ 和 $r(x) = p(c - \lambda x)$，$q(x), r(x) \in \mathbb{F}(c)[x]$

因为 $q(b) = r(b) = 0$，设 b 在 $\mathbb{F}(c)$ 上极小多项式为 $d(x)$

则 $d(x) \in \mathbb{F}(c)[x]$，$d(x) \mid q(x)$，$d(x) \mid r(x)$.

$d(x)$ 在 K 中的零点是 $q(x), r(x)$ 公共零点的一部分

设 $q(b_j) = r(b_j) = 0$ 则 $c - \lambda b_j = a_i \quad \exists i \in \{1, \cdots, s\}$

即 $\lambda = \dfrac{a_i - a}{b - b_j}$ 当 $j \neq 1$ 或 $(b - b_j)\lambda = a_i - a$

由λ的选择，$q(x), r(x)$ 只有公共零点 $b = b_1$

即 $d(x)$ 在 K 中只有零点 $x = b$，在 $K[x]$ 中，$d(x) = (x - b)^l$

在 $\mathbb{F}(c)[x]$ 中，$d(x)$ 不可约. 若 $l > 1$.

$d(x) = (x - b)^l = x^l + \cdots + b^l$，$d'(x) = l(x - b)^{l-1} \in \mathbb{F}(c)[x]$

在 $K[x]$ 中，$d(x), d'(x)$ 不互素 (若 $l > 1$)，则在 $\mathbb{F}(c)[x]$ 中

也不互素，与 $d(x)$ 不可约矛盾 $\Rightarrow x - b \in \mathbb{F}(c)[x] \Rightarrow b \in \mathbb{F}(c)$.

现在证明上一定理，即$|\mathrm{Aut}_{\mathbb{F}}\mathbb{E}|=[\mathbb{E}:\mathbb{F}]$

证明：因为$\mathbb{E}$是$\mathbb{F}$的分裂扩张，则$\mathbb{E}$是$\mathbb{F}$上有限维扩张，则存在$\theta\in\mathbb{E}$，$\mathbb{E}=\mathbb{F}(\theta)$，设$\theta$在$\mathbb{F}$上极小多项式为$p(x)$，$\theta_1\neq\theta$是$p(x)$的另一根（在$p(x)$在$\mathbb{F}$上的分裂域中）.

$$\mathbb{E}=\mathbb{F}(\theta)\xrightarrow{\varphi}\mathbb{F}(\theta_1)\simeq\frac{\mathbb{F}[x]}{(p(x))}\qquad \varphi(\theta)=\theta_1$$

设$f(x)$的全部互异根为$\alpha_1,\cdots,\alpha_k$，则$\mathbb{E}=\mathbb{F}(\alpha_1,\cdots,\alpha_k)$

$\varphi(\alpha_1),\cdots,\varphi(\alpha_k)$是$f(x)$的根的重排，即$\alpha_1,\cdots,\alpha_k\in\mathbb{F}(\theta_1)$

$\Rightarrow\mathbb{E}\subseteq\mathbb{F}(\theta_1)$ 但是φ是域同构，$\dim_{\mathbb{F}}\mathbb{E}=\dim_{\mathbb{F}}\mathbb{F}(\theta_1)$

$\Rightarrow\mathbb{E}=\mathbb{F}(\theta)=\mathbb{F}(\theta_1)$，即$\mathbb{E}$是$p(x)$的分裂域（在$\mathbb{F}$上）

设$\theta_1,\cdots,\theta_n$是$p(x)$的全部根，$\theta_i\neq\theta_j$（因为$p(x)$不可约，$\mathrm{char}\,\mathbb{F}=0$），则$\deg p(x)=n$.

若$\varphi\in\mathrm{Aut}_{\mathbb{F}}\mathbb{E}$，则$\varphi(\theta_1)$也满足$p(x)\in\mathbb{F}[x]$. $\varphi(\theta_1)=\theta_j$，$\exists j$

$$\Rightarrow\varphi=\varphi_j:\ \mathbb{F}(\theta_1)=\mathbb{E}\longrightarrow\mathbb{F}(\theta_j)=\mathbb{E}$$
$$f(\theta_1)\longmapsto f(\theta_j)$$

$\Rightarrow\mathrm{Aut}_{\mathbb{F}}\mathbb{E}=\{\varphi_1,\varphi_2,\cdots,\varphi_n\}=n=[\mathbb{E}:\mathbb{F}]$