Galois 理论初步

基本理论

定义1. 设 E/F 是一个域扩张，记 $Aut(E/F)$ 为 E 的所有满足 $\sigma(a) = a \quad \forall a \in F$ 的自同构，称为 E 在 F 上的自同构群。

容易验证 $Aut(E/F)$ 在复合运算下确实是一个群。

设 K 是 E/F 的一个中间域，则 $Aut(E/K)$ 是 $Aut(E/F)$ 的子群。这就给出从E/F 的全体中间域集合到Aut(E/F)的子群集合的一个映射

$$K \mapsto Aut(E/K).$$

另一方面，设 H 是 $Aut(E/F)$ 的一个子群。令

$$E^H = \{b \in E | \sigma(b) = b \text{ 对所有} \sigma \in H\}.$$

则 E^H 是 E/F 的一个中间域,叫做 H 的固定子域。这就给出从Aut(E/F)的子群集合到 E/F 的全体中间域集合的一个映射

$$H \mapsto E^H.$$

引理1. 1) 设 K_1, K_2 是 E/F 的中间域， $K_1 \subseteq K_2$. 则 $Aut(E/K_1) \supseteq Aut(E/K_2)$;

2) 设 H_1, H_2 是 $G(E/F)$ 的子群， $H_1 \subseteq H_2$. 则 $E^{H_1} \supseteq E^{H_2}$;

3) 对 E/F 的任意中间域 K 都有 $K \subseteq E^{Aut(E/K)}$;

4) 对 $Aut(E/F)$ 的任意子群 H 都有 $H \subseteq Aut(E/E^H)$;

证明：简单。□

定义2. 设 E/F 是一个扩张。L/F 为 F 的任意扩张。设 $\sigma : E \to L$ 是一个单同态，并且 $\sigma(a) = a$ 对所有 $a \in F$ 成立。则称 σ 为 E/F 到 L 中的一个**嵌入**(embedding)。

命题2. 设 E/F 是有限扩张。则 E/F 到 L 中的嵌入的总数不超过 $[E:F]$.

证明：先假定 E/F 是单扩张，即 $E=F[\alpha]$. 设 $f(x)$ 是 α 的极小多项式，则 $\deg(f)=n=[E:F]$. 设 $f(x)=0$ 在 L 中有 m 个两两不同的根，则 $m\leq n$.

假定有 $m+1$ 个从 E/F 到 L 的嵌入 $\sigma_1,\ldots,\sigma_{m+1}$. 则 $\sigma_1(\alpha),\ldots,\sigma_{m+1}(\alpha)$ 都是 $f(x)=0$ 的根。于是至少有两个相同，不妨设 $\sigma_1(\alpha)=\sigma_2(\alpha)$. 这表明 $\sigma_1=\sigma_2$. 矛盾。所以 E/F 到 L 中的嵌入的总数不超过 m.

对一般的情形对 $n=[E:F]$ 进行归纳。可以设 E/F 不是单扩张。于是存在中间域 K 满足

$$[E:K]>1,[K:F]>1.$$

于是

$$[E:K]<n,[K:F]<n.$$

设 $\sigma_1,\ldots,\sigma_m$ 是从 K/F 到 L 的全部嵌入。根据归纳假设，$m\leq[K:F]$. 令 $d=[E:K]$. 则

$$dm\leq[E:K][K:F]=[E:F]=n.$$

假定有 $n+1$ 个从 E/F 到 L 中的嵌入

$$\rho_1, \ldots, \rho_{n+1}.$$

由于 $n+1 > dm$, 根据抽屉原理，存在其中 $d+1$ 个嵌入在 K 上的限制相同。不妨设

$$\rho_1|_K = \cdots = \rho_{d+1}|_K.$$

则 $\rho_1(K) = \cdots = \rho_{d+1}(K) = K'$. 记 $E_1 = \rho_1(E)$, 则

$$\rho_1^{-1} : E_1 \to E$$

是同构映射。

$$\rho_1\rho_1^{-1}, \ldots, \rho_{d+1}\rho_1^{-1} \tag{1}$$

是从 E_1/K' 到 L 的嵌入。根据归纳假设，(1) 中至少有两个相同，即 $\rho_i\rho_1^{-1} = \rho_j\rho_1^{-1}$. 这表明 $\rho_i = \rho_j$, 产生矛盾。□

系3. 设 E/F 是一个有限扩张。则 $|Aut(E/F)| \leq [E:F]$.

证明：这是因为 $Aut(E/F)$ 恰好由 E/F 到 E 的全部嵌入所组成。□

定义3. 设 E/F 是一个有限扩张。若 $[E:F] = |Aut(E/F)|$ 则称 E/F 为**Galois 扩张**。这时群 $Aut(E/F)$ 称为 E/F 的 Galois 群，记作 $Gal(E/F)$ 或 $G(E/F)$.

例1. 假定域 F 的特征不等于 2。则 F 的任何一个二次扩张都是 Galois 扩张。

例2. 三次扩张 $\mathbb{Q}[\sqrt[3]{2}]/\mathbb{Q}$ 不是 Galois 扩张。

例3. 设 $\zeta = (-1+\sqrt{-3})/2,\ F = \mathbb{Q}[\zeta]$. 则三次扩张 $F[\sqrt[3]{2}]/F$ 是 Galois 扩张。

例4. 有限域的任何一个有限扩张是 Galois 扩张。

设 $F = \mathbb{F}_q$ 是含 q 个元素的有限域。 E 是 F 的一个 n 次有限扩张，则 $E \cong \mathbb{F}_{q^n}$. 令

$$\phi : E \to E, a \mapsto a^q.$$

则 $\phi \in Aut(E/F)$ 且 ϕ 生成 $Aut(E/F)$ 的 n 阶循环子群。因此 $|Aut(E/F)| = n = [E:F]$, 即 E/F 是 Galois 扩张，并且 $G(E/F)$ 是一个 n 阶循环群。

命题4. 设 E/F 是一个有限 Galois 扩张，K 是一个中间域。则 E/K 是 Galois 扩张。

证明：令 A 为由 K/F 到 E 中的全体嵌入所构成的集合。对任何 $g \in G(E/F)$, 记 $g|_K$ 为 g 在 K 上的限制，则 $g \mapsto g|_K$ 给出了一个映射

$$f : G(E/F) \to A.$$

对于任何 $h \in A$, 有两种情形可能发生：

1）$f^{-1}(h)$ 是空集；

2）$f^{-1}(h)$ 不是空集。

在第二种情形下设 $f(u) = h$, 也就是说 $u|_K = h$. 容易验证 $f^{-1}(h) = uAut(E/K)$, 即 $f^{-1}(h)$ 是 $G(E/F)$ 的子群 $Aut(E/K)$ 的一个左陪集。

综上所述，任何 $h \in A$ 的原象至多含 $|Aut(E/K)|$ 个元素。又根据命题2 集合 A 中的元素个数不超过 $[K : F]$. 于是 $|G(E/F)| \leq [K : F]|Aut(E/K)|$. 由于 E/F 是 Galois 扩张，$|G(E/F)| = [E : F]$. 因此 $[E : F] \leq [K : F]|Aut(E/K)|$, 即

$$|Aut(E/K)| \geq [E : F]/[K : F] = [E : K].$$

根据系3 $|Aut(E/K)| \leq [E : K]$. 因此 $|Aut(E/K)| = [E : K]$. 所以 E/K 是 Galois 扩张。 □

引理5. 设 E 是一个域，G 是 $Aut(E)$ 的一个有限子群，$F = E^G$. 则 E/F 是 Galois 扩张，并且 $G = G(E/F)$。

证明：设 $g_1, g_2, \ldots, g_n$ 是 G 的全部元素。假定 E 中有 $n+1$ 个元素 $u_1, \ldots, u_{n+1}$ 在 F 上线性无关。域 E 上齐次线性方程组

$$g_1(u_1)x_1 + \cdots + g_1(u_{n+1})x_{n+1} = 0,$$

$$\cdots$$

$$g_n(u_1)x_1 + \cdots + g_n(u_{n+1})x_{n+1} = 0$$

变量个数大于方程个数，因而有非零解

$$x_1 = a_1, \ldots, x_{n+1} = a_{n+1}.$$

我们选取一组解中非零元素的个数达到最小。不失一般性可设 $a_1 = 1$. 若所有 a_i 都在 F 中，则

$$g_1(a_1u_1 + \cdots + a_{n+1}u_{n+1}) = 0,$$

从而

$$a_1u_1 + \cdots + a_{n+1}u_{n+1} = 0,$$

与 $u_1, \ldots, u_{n+1}$ 的线性无关矛盾。因此至少有一个 a_i 不在 F 中，不妨设 $a_2 \notin F$.

于是存在 $g \in G$ 使 $g(a_2) \neq a_2$. 这样就有

$$gg_1(u_1)g(a_1) + \cdots + gg_1(u_{n+1})g(a_{n+1}) = 0,$$

$$\cdots$$

$$gg_n(u_1)g(a_1) + \cdots + gg_n(u_{n+1})g(a_{n+1}) = 0.$$

由于 $gg_1, gg_2, \ldots, gg_n$ 仍然是 G 的全体元素，所以上面的方程组只不过是下面方程组的置换：

$$g_1(u_1)g(a_1) + \cdots + g_1(u_{n+1})g(a_{n+1}) = 0,$$

$$\cdots$$

$$g_n(u_1)g(a_1) + \cdots + g_n(u_{n+1})g(a_{n+1}) = 0.$$

与方程组

$$g_1(u_1)a_1 + \cdots + g_1(u_{n+1})a_{n+1} = 0,$$

$$\cdots$$

$$g_n(u_1)a_1 + \cdots + g_n(u_{n+1})a_{n+1} = 0$$

逐个相减得

$$g_1(u_1)(g(a_1) - a_1) + g_1(u_2)(g(a_2) - a_2) + \cdots = 0,$$

$$\cdots$$

$$g_n(u_1)(g(a_1) - a_1) + g_n(u_2)(g(a_2) - a_2) + \cdots = 0.$$

这就得到一组新的不全为零的解，但其中非零元素的个数却减少了，产生矛盾。因此 $[E : F] \leq n$.

根据系3

$$Aut(E/F) \leq [E : F] \leq n.$$

因为 $G \subseteq Aut(E/F)$ 并且 $|G| = n$, 所以 $[E : F] = n$ 并且 $G = Aut(E/F)$. $\square$

定理6 (有限Galois 扩张的基本定理)**.** 设 E/F 是一个有限 Galois 扩张，$n = [E : F]$. 则

1) 映射

$$\phi : K \mapsto Aut(E/K)$$

和

$$\psi : H \mapsto E^H$$

给出 E/F 的 Galois 中间域集合和 $G(E/F)$ 的子群集合间的一一对应。

2) 对任意中间域 K, 都有 $[K : F] = (G(E/F) : G(E/K))$.

3) K/F 是 Galois 扩张当且仅当 $G(E/K) \triangleleft G(E/F)$. 此时，$G(K/F) \cong G(E/F)/G(E/K)$.

证明：为证明1) 我们来验证 $\psi \circ \phi$ 和 $\phi \circ \psi$ 都是恒等映射。

首先引理5 正好意味着 $\phi \circ \psi$ 是恒等映射。

根据命题4 对任意中间域 K, E/K 是 Galois 扩张，因此

$$|Aut(E/K)| = [E : K].$$

令 $B = E^{Aut(E/K)}$. 则 $B \supseteq K$. 根据引理5 E/B 是 Galois 扩张，从而

$$[E : B] = |Aut(E/K)| = [E : K].$$

所以 $B = K$. 这证明了 $\psi \circ \phi$是恒等映射。

2) 由于 E/F 和 E/K 都是 Galois 扩张，因此

$$[E:F] = |G(E/F)|, [E:K] = |G(E/F)|.$$

从而 $[K:F] = [E:F]/[E:K] = (G(E/F) : G(E/K))$.

3) 设 $H \triangleleft G(E/F)$. 令 $K = E^H$. 任取对任意 $g \in G(E/F)$. 我们来证明 $g(b) \in K$ 对任意 $b \in K$ 成立。不然的话就存在 $b \in K$ 而 $g(b) \notin K$. 于是存在 $h \in H$ 使 $h(g(b)) \neq g(b)$. 由 $g^{-1}hg \in H$ 推得 $g^{-1}hg(b) = b$, 即 $hg(b) = g(b)$, 产生矛盾。

这样可以定义映射

$$\phi : G(E/F) \to Aut(K/F), g \mapsto g|_K.$$

显然 $Ker(\phi) = G(E/K)$. 根据同态基本定理

$$|Im\phi| = (G(E/F) : G(E/K)) = [E : F]/[E : K] = [K : F].$$

由

$$[K : F] = |Im\phi| \leq |Aut(K/F)| \leq [K : F]$$

推得 ϕ 是满射并且 $|Aut(K/F)| = [K : F]$. 这说明了 K/F 是 Galois 扩张并且

$$G(K/F) \cong G(E/F)/G(E/K).$$

反之，设 K/F 是 Galois 扩张，则 $|G(K/F)| = [K : F]$. 由于 K/F 到 E 中最多只有 $[K : F]$ 个嵌入，所以 $G(K/F)$ 包含了 K/F 到 E 中的全部嵌入。对任意 $\sigma \in G(E/F), \sigma|_K$ 是 K/F 到 E 中的嵌入，因此 $\sigma \in G(K/F)$. 这样就得到群同态

$$G(E/F) \to G(K/F), \sigma \mapsto \sigma|_K,$$

其核恰好是 $G(E/K)$. 因此 $G(E/K) \triangleleft G(E/F)$. $\square$

定理7. 有限扩张 E/F 是 Galois 扩张当且仅当存在 $\alpha \in E$ 满足下面条件：

1）$E = F[\alpha]$;

2）α 的极小多项式 $f(x) \in F[x]$ 在 E 中分解为

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

其中 $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ 是 E 中两两互异的元素。

证明：当 F 是有限域时结论是清楚的。以下可设 F 是无限域。

必要性：设 E/F 是 n 次 Galois 扩张。对任意 $u \in E$ 令

$$H_u = \{g \in G(E/F) | g(u) = u\}.$$

则 H_u 是 $G(E/F)$ 的一个子群。

对任意 $u, v \in E$ 我们来证明存在 $w \in E$ 使 $H_w = H_u \cap H_v$. 由于 $G(E/F)$ 只有有限多个子群而 F 中有无限多个元素，存在 $c_1, c_2 \in F, c_1 \neq c_2$ 使 $H_{u+c_1v} = H_{u+c_2v}$. 令 $w = u + c_1v$. 显然有 $H_u \cap H_v \subseteq H_w$. 设 $g \in H_w$. 则

$$g(u + c_1v) = u + c_1v, g(u + c_2v) = u + c_2v.$$

于是 $(c_1 - c_2)g(v) = (c_1 - c_2)v$, 从而 $g(v) = v$, 同时有 $g(u) = u$, 即得 $g \in H_u \cap H_v$. 这就证明了 $H_w = H_u \cap H_v$.

由此推得，存在 $\alpha \in E$ 使 $H_\alpha \subseteq H_u$ 对任何 $u \in E$ 成立，也就是说对任何 $g \in H_\alpha$ 和任何 $u \in E$ 都有 $g(u) = u$. 根据 Galois 理论的基本定理 $H_\alpha = \{1\}$.

令 $f(x)$ 为 α 的极小多项式。则 $\deg(f) \leq n$. 若 $\deg(f) < n$, 由于 $f(g(\alpha)) = 0$ 对任意 $g \in G(E/F)$ 成立，由抽屉原理推得存在 $G(E/F)$ 中两个不同的元素 g_1, g_2 使 $g_1(\alpha) = g_2(\alpha)$, 于是 $g_1^{-1}g_2 \in H_\alpha$, 故 $g_1^{-1}g_2 = 1$. 这和 $g_1 \neq g_2$ 的假设矛盾。所以 $\deg(f) = n$. 也就是说 $E = F[\alpha]$.

设 $1 = g_1, g_2, \ldots, g_n$ 是 $G(E/F)$ 的全体元素。令 $\alpha_i = g_i(\alpha), 1 \leq i \leq n$. 则 $\alpha_1, \ldots, \alpha_n \in E$ 两两不同，且都是 $f(x)$ 的零点，因此

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n).$$

充分性：对每个 α_i 作满同态

$$f_i : F[x] \to E, h(x) \mapsto h(\alpha_i).$$

则 $Ker(f_i) = (f(x))$. 根据同态基本定理 f_i 诱导出同构

$$\phi_i : F[x]/(f(x)) \to E.$$

记 $g_i = \phi_i \circ \phi_1^{-1}, (1 \leq i \leq n)$. 则 $g_1, \ldots, g_n$ 是 $Aut(E/F)$ 中 n 个两两不同的元素。因此 $|Aut(E/F)| \geq n$. 但是我们知道 $|Aut(E/F)| \leq [E : F] = n$ 对任何有限扩张 E/F 成立。因此 $|Aut(E/F)| = [E : F]$, 即 E/F 是 Galois 扩张。 □

定义4. 设 F 是一个域，$f(x) \in F[x]$. 设 $\alpha_1, \ldots, \alpha_n$ 是 $f(x)$ 在 F 的代数闭包 $\bar{F}$ 中的全部零点。则 $F[\alpha_1, \ldots, \alpha_n]$ 称为 $f(x)$ 的**分裂域**(splitting field)。

引理8. 设 F 是特征等于零的域，$f(x) \in F[x]$. 则 $f(x)$ 的分裂域是 F 的有限 Galois 扩张。

证明：设 $E = F[\alpha_1, \ldots, \alpha_n]$, 其中 $\alpha_1, \ldots, \alpha_n$ 是 $f(x)$ 在 F 的代数闭包 $\bar{F}$ 中的全部零点。设 $\beta \in E \backslash F, p(x)$ 是 β 的极小多项式。由于 F 的特征为零，$p'(x) \neq 0$. 因此 $p'(x)$ 和 $p(x)$ 互素。因此 $p(x) = 0$ 在 $\bar{E}$ 中没有重根，故 $p(x) = 0$ 在 $\bar{E}$ 中有两个不同的根 β, β'. 于是存在 E/F 到 $\bar{E}$ 的嵌入 σ 使 $\sigma(\beta) = \beta'$. 对每个 α_i, 其在 σ 下的像仍然是 $f(x) = 0$ 的根。因此 σ 诱导出 $\alpha_1, \ldots, \alpha_n$ 的一个置换。因此 $\sigma(E) = E$. 这表明 $\sigma \in Aut(E/F)$.

这就证明了对任意 $\beta \in E \backslash F$, 都存在 $\sigma \in Aut(E/F)$ 使 $\sigma(\beta) \neq \beta$. 因此 E/F 是 Galois 扩张。□

可解扩张和高次方程求根公式：见英文版。