记号: 设域扩张 E/F, 以 $\mathrm{Aut}_F E$ 表示 E/F 的 Galois 群.
设域 E,G 是 E 自同构群的子群, 以 E^G 表示 $\{a \in E \mid \sigma(a)=a, \forall\sigma \in G\}$. 它是 E 的子域.
设域扩张 E/F,$\alpha \in E$ 在 F 上代数, 以 $\mathrm{Irr}(\alpha, F, x)$ 表示 α 在 F 上的极小多项式,x 为未定元.
设 F 为域, 则 F 的代数闭包存在且在同构意义下唯一, 记为 F^{a}.
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{F}_q$ 分别记整数环, 有理数域, 实数域, 复数域,q 阶域, 其中 q 是某一素数的幂.
$\mathcal{S}_n, \mathcal{A}_n$ 分别记 n 次对称群,n 次交错群.
设 G, H 是群.$G=1$ 表示 G 只有一个元素,$G \simeq H$ 表示 G 同构于 H.
1 有时表示只有一个元素的群, 有时表示群的幺元.

正文没有完整证明, 只含简略的说明.

引理 0.1 *设代数扩张 E/k,$\sigma: k \to L$ 将 k 嵌入到一代数闭域 L. 则 σ 可延拓为嵌入 $E \to L$.*

证明 令集合 S 由 (F, τ) 组成, 其中 F 是 E/k 的中间域,τ 是嵌入 $F \to L$ 并且 $\tau|_k = \sigma$. 则 $(k, \sigma) \in S$, 从而 S 非空. 设 $(F, \tau), (F', \tau') \in S$, 记 $(F, \tau) \leq (F', \tau')$ 如果 $F \subset F'$ 且 $\tau'|_F = \tau$. 这在 S 上定义了偏序. 设链 $\{(F_i, \tau_i)\}_{i \in I} \subset S$, 令 $F = \bigcup_{i \in I} F_i$, 定义映射 $\tau\colon F \to L$, 若 $\alpha \in F_i$, 则 $\tau(\alpha) = \tau_i(\alpha)$. 易验证 F 是 E/k 的中间域,τ 是良定义的嵌入 $F \to L$. 从而是 $\{(F_i, \tau_i)\}$ 的上界. 用 Zorn 引理,S 有极大元.

令 (K, λ) 为 S 的一个极大元, 我们断言 $K = E$. 否则, 取 $\alpha \in E - K$, 则 λ 可延拓为 $K(\alpha) \to L$, 与 (K, λ) 是极大元矛盾! 这就证明 σ 可延拓为嵌入 $E \to L$.

1 有限域

定理 1.1 *设 F 是域,G 是 F 乘法群的有限子群, 则 G 是循环群.*

设 $|G| = n$, 取 $m \mid n$, 则方程 $x^m = 1$ 在 G 中的解至多有 m 个.

定理 1.2 *设有限群 G 的阶为 n. 若任意 $m \mid n$,G 中满足 $x^m = 1$ 的元至多 m 个. 则 G 是循环群.*

事实上, 设 $m \mid n$, 记 $d_m(G)$ 表示 G 中 m 阶元的个数. 必然有 $d_m(G) \le \varphi(m)$. 否则 G 有两个不同的 m 阶循环群, 导致 $x^m = 1$ 的解多于 m 个. 有

$$|G| = n = \sum_{m|n} d_m(G) \le \sum_{m|n} \varphi(m) = n.$$

于是 $d_m(G) = \varphi(m), \forall m \mid n$. 特别地,$G$ 有 n 阶元, 从而 G 是循环群.

由此, 设 F 是有限域, 则 F 的乘法群 $F^\times$ 是循环群.

设 F 是有限域, 则 F 的特征 $p > 0$, F 含 $\mathbf{F}_p$ 为子域, 是 $\mathbf{F}_p$ 上的线性空间. 记 $n = [F : \mathbf{F}_p]$, 得到 $|F| = p^n$. 由此, 有限域的阶是某一素数的幂. 记 $|F| = q$, 有 $|F^\times| = q - 1$, 从而任意 $\alpha \in F - \{0\}$, 有 $\alpha^{q-1} - 1 = 0$. 再考虑 0, 我们得到

$$x^q - x = 0, \forall x \in F.$$

记 $f(x) = x^q - x$, 则 $f(x)$ 在 F 上分裂 (分解为一次因式之积).F 的所有元素恰为 $f(x)$ 的所有根, 易见 F 是 $f(x) \in \mathbf{F}_p[x]$ 在 $\mathbf{F}_p$ 上的分裂域. 从而,q 阶域在同构意义下唯一.

取 $\mathbf{F}_p$ 的代数闭包 $\mathbf{F}_p^{\mathrm{a}}$, 取 $\mathbf{F}_p^{\mathrm{a}}$ 的有限子域 $\mathbf{F}_q$, 设 $x \in \mathbf{F}_p^{\mathrm{a}}$, 则 $x \in \mathbf{F}_q \iff x^q - x = 0$.

设有限域 $\mathbf{F}_{p^n}$, 取其子域 $\mathbf{F}_{p^m}$, 则 $m \mid n$. 设

$$\phi : \mathbf{F}_{p^n} \to \mathbf{F}_{p^n}, x \mapsto x^{p^m}.$$

则 ϕ 是 $\mathbf{F}_{p^n}$ 的自同构, 且保持 $\mathbf{F}_{p^m}$. 可验证 $o(\phi) = \frac{n}{m}$ 和 $|\mathrm{Aut}_{\mathbf{F}_{p^m}} \mathbf{F}_{p^n}| \le [\mathbf{F}_{p^n} : \mathbf{F}_{p^m}] = \frac{n}{m}$, 从而

$$\mathrm{Aut}_{\mathbf{F}_{p^m}} \mathbf{F}_{p^n} = \langle \phi \rangle = \{\phi^k : x \mapsto x^{p^{km}}\}.$$

称

$$\varphi : \mathbf{F}_q \to \mathbf{F}_q, x \mapsto x^p$$

为 **Frobenius mapping**.

2 可分性

设 E/F 是代数扩张, 设 $\sigma\colon F\to L$ 将 F 嵌入到一代数闭域 L, 且 L 在 σF 上代数 (即 L 是 σF 的一个代数闭包).σ 可延拓为嵌入 $E\to L$, 记 σ 的所有这样的延拓为 S_σ, 定义

$$[E\colon F]_s=|S_\sigma|.$$

下面说明 $[E\colon F]_s$ 与 σ 的选取无关. 设 $\tau\colon F\to L'$ 是另一个满足上述条件的嵌入. 则存在同构 $\lambda\colon L\to L'$, 且 $\lambda|_{\sigma F}=\tau\sigma^{-1}$, 即

$$\begin{tikzcd} L \arrow[rr, "\lambda"] \arrow[d, dash] & & L' \arrow[d, dash] \\ \sigma F & F \arrow[l, "\sigma"'] \arrow[r, "\tau"'] & \tau F \end{tikzcd}$$

则验证 $\lambda S_\sigma=S_\tau$, 从而验证 $|S_\sigma|=|S_\tau|$. 选取 E 的代数闭包 E^{a}, 则 $[E:F]_s$ 就是 F-嵌入 $\sigma:E\to E^{\mathrm{a}}$ 的多少.

定理 2.1 *设域的代数扩张塔 $k\subset F\subset E$, 有*

$$[E:k]_s=[E:F]_s[F:k]_s.$$

设 $[E:k]$ 有限, 则 $[E:k]_s\mid[E:k]$.

选取 E 的代数闭包 E^{a}, 设 $\{\sigma_i:F\to E^{\mathrm{a}}\}_{i\in I}$ 是所有的 k-嵌入 $F\to E^{\mathrm{a}}$. 对每个 i, 将 σ_i 延拓为 $\{\tau_{ij}:E\to E^{\mathrm{a}}\}_{j\in J_i}$. 每个 σ_i 的延拓 $\{\tau_{ij}\}_{j\in J_i}$ 的基数恰为 $[E:F]_s$, 不同的 σ_i 给出的延拓必然不同. 从而 $|\{\tau_{ij}\}_{i,j}|=[E:F]_s[F:k]_s$. 再说明每个 k-嵌入 $E\to E^{\mathrm{a}}$ 必然等于某个 τ_{ij} 即可.

对第二个论断,E/k 是有限扩张, 从而存在扩张塔

$$k\subset k(\alpha_1)\subset k(\alpha_1,\alpha_2)\subset\cdots\subset k(\alpha_1,\cdots,\alpha_r)=E.$$

我们只证明, 每个单代数扩张 $k(\alpha)/k$, 有 $[k(\alpha):k]_s\mid[k(\alpha):k]$. 并且只考虑 $\operatorname{char}k=p>0$.

引理 2.1 *设 F 是特征为 $p>0$ 的域. 设 $f(x)\in F[x]$ 是 F 上不可约多项式, 则 $f(x)$ 的每一根有相同的重数 $p^u.u\geq 0$. 存在 $h(x)\in F[x]$,$h(x)$ 无重根使 $f(x)=h(x^{p^u})$.*

推论 2.1 *设 α 在 F 上代数, 存在 $u\geq 0$, 使 α^{p^u} 在 F 上可分.*

设 $g(x)=\operatorname{Irr}(\alpha,k,x)$. 取 k 的代数闭包 k^{a}. 存在两两不同的元素 $\alpha=u_1,u_2,\cdots,u_m\in k^{\mathrm{a}}$, 整数 u, 使

$$g(x)=(x-u_1)^{p^u}(x-u_2)^{p^u}\cdots(x-u_m)^{p^u}.$$

易见 $[k(\alpha):k]_s=m$,$[k(\alpha):k]=\deg g=p^um$.

设 α 在 F 上代数, 称 α 在 F 上纯不可分, 如果存在 $u\geq 0$ 使得 $\alpha^{p^u}\in F$.

定理 2.2 *设 α 在 F 上代数, 下列条件等价:*
i) α 在 F 上纯不可分.
ii) α 在 F 上的极小多项式只有一根.
iii) α 在 F 上的极小多项式形如 $x^{p^u}-a$, $u\geq 0$, $a\in F$.

对 i) $\Longrightarrow$ ii), 多项式 $x^{p^u}-\alpha^{p^u}\in F[x]$ 零化 α, 从而 $\operatorname{Irr}(\alpha,F,x)$ 是 $x^{p^u}-\alpha^{p^u}=(x-\alpha)^{p^u}$ 的因子, 只有一根. 对 ii) $\Longrightarrow$ iii), 设 $g(x)=\operatorname{Irr}(\alpha,F,x)=(x-\alpha)^{p^km}$,$m,p$ 互素. 有

$$g(x)=(x^{p^k}-\alpha^{p^k})^m=x^{p^km}-m\alpha^{p^k}x^{(m-1)p^k}+\cdots+(-1)^m\alpha^{mp^k}\in F[x].$$

于是 $m\alpha^{p^k}\in F$,$m\neq 0$, 从而 $\alpha^{p^k}\in F$, 导致 $g(x)=(x-\alpha)^{p^k}$.iii) $\Longrightarrow$ i) 是显然的.

推论 2.2 *设 α 在 F 上代数,α 在 F 上同时可分和纯不可分当且仅当 $\alpha\in F$.*

称域扩张 E/F 为纯不可分 (resp. 可分) 扩张, 如果 E 的每一元在 F 上纯不可分 (resp. 可分).

定理 2.3 *设代数扩张 E/F, 以下条件等价:*
i) $[E:F]_s=1$.
ii) E/F 纯不可分.
iii) 存在 E 在 F 上的生成元 $\{\alpha_i\}_{i\in I}\subset E$, 满足每个 α_i 在 F 上纯不可分.

i) $\Longrightarrow$ ii). 设 $\alpha\in E$, 取 u 是 $\mathrm{Irr}(\alpha,F,x)$ 在代数闭包 E^{a} 的一根, 有 F-嵌入 $\sigma:F(\alpha)\to F(u)$, 满足 $u=\sigma(\alpha)$. 延拓为 $E\to E^{\mathrm{a}}$, 仍然记为 σ. 由 $[E:F]_s=1$, 只有 $\sigma=\mathrm{id}$, 从而 $u=\alpha$,$\mathrm{Irr}(\alpha,F,x)$ 只有一根.

ii) $\Longrightarrow$ iii). 取 $\{\alpha_i\}=E$.

iii) $\Longrightarrow$ i). 每个 α_i 在 F 上纯不可分, 从而在 F 上的极小多项式只有一根. 设 σ 是 F-嵌入 $E\to E^{\mathrm{a}}$, 只有 $\sigma(\alpha_i)=\alpha_i,\forall i\in I$, 从而 $\sigma=\mathrm{id}$.

E/F 是可分扩张, 等价于 E 存在可分的生成元. 当 E/F 有限时, 等价于 $[E:F]_s=[E:F]$.

定理 2.4 *i) 设域的代数扩张塔 $k\subset F\subset E$, 则 E/k 是纯不可分 (resp. 可分) 扩张当且仅当 E/F, F/k 是纯不可分 (resp. 可分) 扩张.*
ii) 设 E/k 是纯不可分 (resp. 可分) 扩张,F/k 是任意域扩张,E,F 在某一共同的域中, 则 EF/F 是纯不可分 (resp. 可分) 扩张.
iii) 设 E/k,F/k 是纯不可分 (resp. 可分) 扩张,E,F 在某一共同域中, 则 EF/k 是纯不可分 (resp. 可分) 扩张.

iii) 可以由 i),ii) 推出. 用图表表示则是

$$
\begin{tikzcd}[arrows=dash]
E \arrow[d] \\
F \arrow[d] \\
k
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & EF \arrow[dl] \arrow[r] & F \arrow[dl] \\
E \arrow[r] & k &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & EF \arrow[dl] \arrow[dr] & \\
F \arrow[dr] & & E \arrow[dl] \\
 & k &
\end{tikzcd}
$$

设代数扩张 K/k, 则 K 中所有在 k 上可分的元素组成的集合 K_0 构成域.

定理 2.5 *K_0/k 是可分扩张,K/K_0 是纯不可分扩张.*

事实上, 设 $\alpha\in K$, 存在 p^u 使 α^{p^u} 在 k 上可分. 于是 $\alpha^{p^u}\in K_0$, 导致 α 在 K_0 上纯不可分.

我们有 $[K:k]_s=[K:K_0]_s[K_0:k]_s=[K_0:k]$. 定义 $[K:k]_i=[K:K_0]$, 则 $[K:k]_s[K:k]_i=[K:k]$.

定理 2.6 *设 E,F 是 k 的有限扩张, 且 E/k 可分,F/k 纯不可分. 设 E,F 在某个共同的域之中, 有*

$$[EF:F]=[E:k]=[EF:k]_s,$$
$$[EF:E]=[F:k]=[EF:k]_i.$$

画图 (s 表示可分扩张,i 表示纯不可分扩张)

$$\begin{tikzcd}[arrows=dash] & EF \arrow[dl, "i"'] \arrow[dr, "s"] & \\ E \arrow[dr, "s"'] & & F \arrow[dl, "i"] \\ & k & \end{tikzcd}$$

定理 2.7 设 K/k 是正规扩张,$G=\mathrm{Aut}_kK$, 则 K^G/k 是纯不可分扩张,K/K^G 是可分扩张. 且 $K^GK_0=K$,$K_0\cap K^G=k$.

图表如下 (s 表示可分扩张,i 表示纯不可分扩张).

$$\begin{tikzcd}[arrows=dash] & K \arrow[d] & \\ & K_0K^G \arrow[dl, "i"'] \arrow[dr, "s"] & \\ K_0 \arrow[dr, "s"'] & & K^G \arrow[dl, "i"] \\ & k & \end{tikzcd}$$

设 $\alpha\in K^G$, 设 k-嵌入 $\sigma: k(\alpha)\to K^{\mathrm{a}}$, 延拓为 $\sigma^*: K\to K^{\mathrm{a}}$.$K/k$ 正规, 从而 $\sigma^*\in\mathrm{Aut}_kK$, 于是 $\sigma(\alpha)=\alpha$, 从而 $\sigma=\mathrm{id}$. 从而 $[k(\alpha):k]_s=1$,α 在 k 上纯不可分.

设 $\alpha\in K$, 记 $G=\mathrm{Aut}_kK$. 令 $G\alpha=\{\alpha_1,\cdots,\alpha_r\}$(这当然是有限集). 记 $g(x)=(x-\alpha_1)\cdots(x-\alpha_r)$. 易见 $g(x)\in K^G[x]$ 是可分多项式,α 是 $g(x)$ 的根.

由 K^G/k 纯不可分知 K_0K^G/K_0 纯不可分. 再由 K/K_0 纯不可分知 K/K_0K^G 可分. 类似推出 K/K_0K^G 可分, 从而 $K=K_0K^G$.

由 K_0/k 可分和 K^G/k 纯不可分知 $K_0\cap K^G/k$ 同时是可分和纯不可分的, 从而 $K_0\cap K^G=k$.

注记: 当 K/k 同时是可分扩张和正规扩张, 即伽罗瓦扩张时,$K^G=k$, 且 $[K:k]=[K:k]_s=|G|$.

这说明, 当 K/k 是正规扩张时,K 由一个在 k 上可分的域和一个在 k 上纯不可分的域合成.

定理 2.8 设 K/k 是正规扩张, 则 K_0/k 是正规扩张.

设 $\sigma: K_0\to K^{\mathrm{a}}$ 是 k-嵌入, 延拓为嵌入 $K\to K^{\mathrm{a}}$, 仍然记为 σ.K/k 正规, 从而 $\sigma: K\to K$ 是 K 的 k-自同构.$\sigma K_0\subset K$ 在 k 上可分, 从而 $\sigma K_0\subset K_0$. 只有 $\sigma K_0=K_0$.

域 k 被称为完美域, 如果 $k^p=k$, 其中 p 是 k 的特征. 每个特征零的域都是完美的. 每个有限域也都是完美的.

定理 2.9 k 是完美域当且仅当 k 的每个代数扩张是可分的.

这里设 $\mathrm{char}\,k=p>0$.

设 k 是完美域, 记 $p=\mathrm{char}\,k$. 首先说明 k 的纯不可分扩张只有本身. 设 F/k 纯不可分, 设 $\alpha\in F$, 则 $\mathrm{Irr}(\alpha,k,x)$ 形如 $x^{p^u}-a$,$a\in k$. 由 k 完美知 $x^{p^u}-a$ 的根在 k 上, 从而 $\alpha\in k$.

设 α 在 k 上代数 (α 在某一扩域中), 取 $k(\alpha)$ 的正规闭包 K(在一选定的代数闭包中). 则 K 由一个在 k 上可分的域和一个在 k 上纯不可分的域合成. 然而在 k 上纯不可分的代数扩张只有 k 本身, 得到 K/k 可分, 从而 α 在 k 上可分.

反之, 设 k 的每个代数扩张可分. 设 $\alpha\in k$. 取 $\beta\in k^{\mathrm{a}}$ 是多项式 $x^p-\alpha$ 的一根, 则 β 在 k 上纯不可分, 从而 $k(\beta)$ 在 k 上纯不可分. 由假设, 只有 $k(\beta)=k$, 从而 $\beta\in k$. 这导致 $k^p=k$.

定理 2.10 (Primitive Element Theorem) *设 E/k 是有限扩张，则存在 $\alpha \in E$，使 $E = k(\alpha)$ 等价于 E/k 的中间域只有有限个. 若 E/k 是有限可分扩张，则满足上述条件的 α 存在.*

只需考虑 k 是无限域，设 E/k 中间域只有有限个. 只需证明 $E = k(\alpha, \beta)$ 时的情况然后归纳. 由 E/k 的中间域只有有限个知存在 $c_1 \neq c_2 \in k$ 使得

$$k(\alpha + c_1\beta) = k(\alpha + c_2\beta).$$

记为 F，有 $\alpha+c_1\beta, \alpha+c_2\beta \in F$，从而 $(c_1-c_2)\beta \in F$，从而 $\beta \in F$. 再推出 $\alpha \in F$. 于是 $E = k(\alpha, \beta) = F$.

反之，设 $E = k(\alpha)$. 设 $\Gamma = \{F \mid k \subset F \subset E\}$ 是 E/k 所有中间域的集合,$f(x) = \mathrm{Irr}(\alpha, k, x)$，设 $\Sigma = \{$首一 $g(x) \in E[x] \mid g(x) \mid f(x)\}$. 则 Σ 是有限集. 设 $F \in \Gamma$，记 $g_F(x) = \mathrm{Irr}(\alpha, F, x)$. 得到映射

$$\Gamma \to \Sigma, F \mapsto g_F(x).$$

再证它是单射，从而证明定理. 设 $g_F(x)$ 的系数在 k 上生成域 F_0，有 $F_0 \subset F.g_F(x)$ 在 F 上不可约，从而在 F_0 上不可约，从而 α 在 F_0 上的极小多项式也为 $g_F(x)$，有 $[k(\alpha) : F_0] = [k(\alpha) : F]$，从而 $F = F_0$. 这说明 F 由 $g_F(x)$ 的系数唯一确定，从而 $F \mapsto g_F(x)$ 是单射.

设 E/k 是可分扩张. 只对 $E = k(\alpha, \beta)$ 时证明. 令 $\sigma_1, \cdots, \sigma_n$ 为两两不同的 k-嵌入 $E \to k^{\mathrm{a}}$. 令

$$P(x) = \prod_{i \neq j}(\sigma_i\alpha + x\sigma_i\beta - \sigma_j\alpha - x\sigma_j\beta).$$

验证 $P(x)$ 不是零多项式，从而存在 $c \in k$，使 $P(c) \neq 0$. 于是 $\sigma_i(\alpha + c\beta)$ 两两不同 $(i = 1, 2, \cdots, n)$，于是 $[k(\alpha + c\beta) : k] \geq n$(在 k^{a} 中它有不少于 n 个共轭的元素). 但是 $n = [k(\alpha, \beta) : k]$，只有 $k(\alpha, \beta) = k(\alpha + c\beta)$.

3 多项式的伽罗瓦群

3.1 定义与基本性质

设 F 是域,$f(x) \in F[x]$,E 为 $f(x)$ 在 F 上的分裂域. 将 $\mathrm{Aut}_F E$ 称为多项式 $f(x)$ 在 F 上的伽罗瓦群.

以下记 $f(x)$ 的根集为 $\{u_1.u_2, \cdots, u_n\} = X$,$\mathrm{Aut}_F E = G$. 令 G 作用于 X 上,$\sigma \in G$ 在 X 上的作用唯一决定 σ, 给出单同态 $G \to \mathcal{S}_n$. 我们视 G 为 $\mathcal{S}_n$ 的子群.

回忆: 对称群 $\mathcal{S}_n$ 的子群 G 被称为 $\mathcal{S}_n$ 的可迁子群, 或者说, 集合 $\Lambda = \{1, 2, \cdots, n\}$ 上的可迁置换群, 如果 G 在 Λ 上的作用传递.

定理 3.1 *i) G 同构于对称群 $\mathcal{S}_n$ 的某一子群.*
ii) 设 f 无重根, 则 $f(x)$ 在 F 上不可约 $\Longleftrightarrow G$ 是 $\mathcal{S}_n$ 的可迁子群.

i) 已经说明, 对 ii), 设 $f(x)$ 在 F 上不可约. 任取 $u_1, u_2 \in X$,u_1, u_2 在 F 上的极小多项式恰为 f, 从而存在 F-同构 $\sigma : F(u_1) \to F(u_2)$, 使得 $\sigma(u_1) = u_2$. 将 σ 延拓为 E 的自同构, 仍然记 σ, 有 $\sigma \in G$, 说明 G 在 X 上作用传递. 反之, 设 G 在 X 上作用传递, 取 $u \in X$, 记 $g(x) = \mathrm{Irr}(u, F, x)$.$G$ 在 X 上的作用传递, 从而 $f(x)$ 的所有根都是 $g(x)$ 的根, 又 $f(x)$ 无重根,$g(x)$ 不可约, 只有 $f(x) = g(x)$ 在 F 上不可约.

定理 3.2 *设 $\sigma \in \mathcal{S}_n$. 则 $\sigma \in G$ 当且仅当 σ 保持 f 的根之间的所有代数关系, 即设 $g(x_1, x_2, \cdots, x_n) \in F[x_1, x_2, \cdots, x_n]$, 则 $g(u_1, u_2, \cdots, u_n) = 0 \Longrightarrow g(\sigma(u_1), \cdots \sigma(u_n)) = 0$.*

设 $\sigma \in \mathcal{S}_n$(即 X 的对称群), 且 σ 保持代数关系. 设 $a \in E$, 存在 $\psi \in F[x_1, \cdots, x_n]$ 使 $a = \psi(u_1, \cdots, u_n)$. 定义

$$\hat{\sigma} : E \to E, a = \psi(u_1, \cdots, u_n) \mapsto \psi(\sigma(u_1), \cdots, \sigma(u_n)).$$

验证这是良定义的, 且 $\hat{\sigma} \in \mathrm{Aut}_F E$.

从而,G 等价于保持 $f(x)$ 所有根之间的代数关系的 $\{u_1, u_2, \cdots, u_n\}$ 上的所有置换构成的群.G 反映的即是 $f(x)$ 根之间的对称.

3.2 判别式

依然沿用上文记号, 下设 F 的特征不为 2, $f(x)$ 无重根, 从而 E/F 是 (有限) 伽罗瓦扩张. 本节解决以下问题: 在伽罗瓦对应下,$G \cap \mathcal{A}_n$ 对应的中间域是什么.

令 $\Delta = \prod_{1 \le i < j \le n} (u_i - u_j)$, 对 $\sigma \in G$, 有

$$\sigma(\Delta^2) = \sigma(\Delta)^2 = (\pm\Delta)^2 = \Delta^2.$$

由此,$\Delta^2 \in E^G = F$. 称 Δ^2 为 f 的判别式. 看出 $\sigma(\Delta) = \Delta \Longleftrightarrow \sigma \in \mathcal{A}_n \cap G$, 从而 $F(\Delta) = E^{G \cap \mathcal{A}_n}$.

定理 3.3 *i) $\mathrm{Aut}_{F(\Delta)} E = G \cap \mathcal{A}_n$, $E^{G \cap \mathcal{A}_n} = F(\Delta)$.*
ii) $G \subset \mathcal{A}_n \Longleftrightarrow \Delta \in F$.

3.3 三次方程

沿用上节记号和条件, 设 $f(x)$ 是 F 上的 3 次无重根不可约多项式.$\mathcal{S}_3$ 的可迁子群只有 $\mathcal{S}_3$ 和 $\mathcal{A}_3$, 故

$$G = \begin{cases} \mathcal{A}_3 & \text{若 } \Delta \in F, \\ \mathcal{S}_3 & \text{否则}. \end{cases}$$

3.4 四次方程

$\mathcal{S}_4$ 的全部可迁子群是
i) $\mathcal{S}_4$,
ii) $\mathcal{A}_4$,
iii) $V=\{(1),(12)(34),(13)(24),(14)(23)\}$,
iv) $C_4=\langle(1234)\rangle$ 以及其共轭子群,
v) 3 个 2-Sylow 子群:$D_4=V\cup\{(1234),(1432),(24),(13)\}$ 和其共轭.

设 $f(x)=x^4-p_1x^3+p_2x^2-p_3x+p_4\in F[x]$ 是无重根不可约多项式,E 是 $f(x)$ 在 F 上的分裂域,r_1,r_2,r_3,r_4 是 $f(x)$ 的根. 令

$$\alpha=r_1r_2+r_3r_4,\beta=r_1r_3+r_2r_4,\gamma=r_1r_4+r_2r_3.$$

则 V 保持 α,β,γ. 从而 $F(\alpha,\beta,\gamma)\subset E^{G\cap V}$. 另一方面, 可以验证 $G-G\cap V$ 中的元都变动 α,β,γ 之一, 从而 $E^{G\cap V}=F(\alpha,\beta,\gamma)$.($V$ 所有陪集的代表元分别为 $1,(123),(132),(12),(23),(13)$)

令 $r(x)=(x-\alpha)(x-\beta)(x-\gamma)=x^3-p_2x^2+(p_1p_3-4p_4)x+4p_2p_4-p_1^2p_4-p_3^2\in F[x]$.

则 $F(\alpha,\beta,\gamma)$ 恰是 $r(x)$ 在 F 上的分裂域. 易验证 α,β,γ 两两不同. 令 $m=[F(\alpha,\beta,\gamma):F]$, 则 $m\mid 6=|\mathcal{S}_3|$.

定理 3.4 设 F 特征不为 2, 其他记号同上, 有
i) $G=\mathcal{S}_4\iff r(x)$ 在 F 上不可约且 f 的判别式不属于 $F^2\iff m=6$.
ii) $G=\mathcal{A}_4\iff r(x)$ 在 F 上不可约且 f 的判别式属于 $F\iff m=3$.
iii) $G=V\iff m=1$.
iv) $G\simeq C_4\iff m=2$ 且 f 在 $F(\alpha,\beta,\gamma)$ 上可约.
v) $G\simeq D_4\iff m=2$ 且 f 在 $F(\alpha,\beta,\gamma)$ 上不可约.

记 $L=F(\alpha,\beta,\gamma)$, 有 $m=[L\colon F]=[G\colon G\cap V]$.

当 $G=\mathcal{S}_4$ 时 $m=[L\colon F]=[G\colon G\cap V]=6$. 此时 $r(x)$ 在 F 上不可约, 判别式不属于 F^2.$G=\mathcal{A}_4$ 时也有类似推理.

反之设 $r(x)$ 在 F 上不可约, 则 $3\mid|G|$. 但 G 是 $\mathcal{S}_4$ 的可迁子群, 只有 $G=\mathcal{S}_4$ 或 $\mathcal{A}_4$. 再由 f 的判别式决定 G. 也可知 $|G|=[E\colon L][L\colon F]=4m$. 所以当 $m=6$ 时 $|G|=24$, 当 $m=3$ 时 $G=12$.

对 iii), 若 $G=V$, 则 $G\cap V=G$, 从而 $m=1$. 反之由 $m=1$ 可推出 $G=V$.

我们有 $E=L(r_1)$, 因为 $\mathcal{S}_4$ 中只有恒等映射才能保持 $L(r_1)$ 每个元不动. 设 $m=2$, 则 $f(x)$ 在 L 上不可约当且仅当 $[E\colon L]=4$, 当且仅当 $[E\colon F]=8$, 当且仅当 $G\simeq D_4$.

3.5 素数次对称群

设 p 是素数,$f(x)\in\mathbf{Q}[x]$ 是 $\mathbf{Q}$ 上的 p 次不可约多项式, 若 $f(x)$ 恰有两个非实的复根, 则 $f(x)$ 的伽罗瓦群同构于 $\mathcal{S}_p$.

$f(x)$ 无重根,$f(x)$ 的伽罗瓦群是 $\mathcal{S}_p$ 的可迁子群, 从而含有 p-轮换. 令 τ 是复数域的复共轭在 $f(x)$ 的分裂域 E 上的限制, 验证 τ 是对换. 对换和 p-轮换生成 $\mathcal{S}_p$.

3.5.1 布饶尔的构造

1. 设 m 是正偶数,$k\geq 5$ 是奇数,$n_1<n_2<\cdots<n_{k-1}$ 均为偶数, 令

$$g(x)=(x^2+m)(x-n_1)\cdots(x-n_{k-2})\in\mathbf{Z}[x].$$

分析 $g(x)$ 在开区间 (n_i, n_{i+1}) 的取值的正负, 知道 $y=g(x)$ 至少有 $\frac{k-3}{2}$ 个极大值, 在 (n_1, n_{k-2}) 中. 而任意奇数 h, 有 $|g(h)|>2$, 从而上述极大值都大于 2.

2. 令 $f(x)=g(x)-2$, 则 $f(x)$ 在开区间 (n_1, n_{k-2}) 至少有 $k-3$ 个实根. 然而 $f(n_{k-2})=-2, f(\infty)=\infty$, 因此 $f(x)$ 必有实根大于 n_{k-2}. 由此 $f(x)$ 至少有 $k-2$ 个两两不同的实根. 设 $r_1, r_2, \cdots, r_k$ 是 $f(x)$ 的全部复根, 则
$$\begin{cases} \sum\limits_{1\le i\le k} r_i = \sum\limits_{1\le i\le k-2} n_i, \\ \sum\limits_{1\le i<j<k} r_i r_j = m + \sum\limits_{1\le i<j\le k-2} n_i n_j. \end{cases}$$
从而 $\sum r_i^2 = \sum n_i^2 - 2m$. 当 $m > \frac{1}{2}\sum n_i^2$ 时两式小于 0, 这意味至少有一个 r_i 不是实数. 从而 $f(x)$ 有两个非实的复根.

3. 用 Eisenstein 判别法说明 $f(x)$ 在 $\mathbf{Q}$ 上不可约.

3.5.2 素数次对称群可解的可迁子群

1. 设 G 是 $\mathcal{S}_n$ 的可迁子群,H 是 G 的正规子群. 则 $\{1,2,\cdots,n\}$ 的每一个 H-轨道有相同的长度. 由此证明: 若 $n=p$ 是素数且 $H\neq 1$, 则 H 是 $\mathcal{S}_n$ 的可迁子群, 从而 $p \mid |H|$, 进而,H 含 p-轮换.

2. 设 G 是 $\mathcal{S}_p$ 的可迁子群,p 是素数.H 是 G 所有 p 阶元生成的子群, 则

   i) H 是单群.

   ii) G/H 是循环群, 且阶是 $p-1$ 的因子.

3. 设 $\langle(123\cdots p)\rangle = C \subset \mathcal{S}_p$, 令 $L=\left\{\begin{pmatrix} a & b \\ 0 & 1\end{pmatrix} \mid a,b\in\mathbf{F}_p, a\neq 0\right\}$. 则 $N_{\mathcal{S}_p}(C)\simeq L$.

4. 设 G 是 $\mathcal{S}_p$ 可解的可迁子群. 则 G 同构于 L 的子群.