§5.4 伽罗瓦群的计算

伽罗瓦理论中心两个基本问题：

1) 正问题：给定可分 $f \in F[X] \setminus F$，如何计算 $Gal(f)$？

Kroneck (David Cox, Galois Theory 2004)

2) 反正问题：什么样的有限群同构于伽罗瓦群？

猜测：$\forall$ 有限群 G，$\exists f \in \mathbb{Q}[X]$ s.t. $Gal(f) \cong G$ (未解决)

设 K 为可分多项式 f 在 F 上的分裂域，$\alpha_1, \cdots \alpha_n$ 为 f 的所有互异根.

$\forall \varphi \in Gal(f)$, $\{\varphi(\alpha_1), \cdots \varphi(\alpha_n)\} = \{\alpha_1, \cdots \alpha_n\}$

$\therefore \exists! \sigma_\varphi \in S_n$ s.t. $\varphi(\alpha_i) = \alpha_{\sigma_\varphi(i)}$

$\sigma: Gal(f) \longrightarrow S_n$, $\varphi \longrightarrow \sigma_\varphi$ 易验证 σ 为群同态且为单的.

$(\varphi_1\varphi_2(\alpha_i) = \varphi_1(\alpha_{\sigma_{\varphi_2}(i)}) = \alpha_{\sigma_{\varphi_1}(\sigma_{\varphi_2}(i))} = \alpha_{\sigma_{\varphi_1}\sigma_{\varphi_2}(i)})$

下面将 $Gal(f)$ 看作 S_n 的子群.

问题：何时 $Gal(f) \subseteq A_n$？

定理：设 $\mathrm{char}F \neq 2$，K 为 $f \in F[X] \setminus F$ 在 F 上的分裂域，f 无重根，$\theta_1, \cdots, \theta_n$ 为 f 在 K 中

令 $\Delta(f) = \prod_{1 \le i < j \le n} (\theta_i - \theta_j)$. 则 $F(\Delta) = K^{Gal(f) \cap A_n}$.

证：设 $\tau = (kl)$, $k < l$.

$$\Delta(f) = (\theta_k - \theta_l) \prod_{k<j<l} (\theta_k - \theta_j)(\theta_j - \theta_l) \quad (=: \delta_1)$$

$$\left[\prod_{1 \le i < k} (\theta_i - \theta_k)(\theta_i - \theta_l) \cdot \prod_{l < j \le n} (\theta_k - \theta_j)(\theta_l - \theta_j) \cdot \prod_{\substack{1 \le i < j \le n \\ i,j \neq k,l}} (\theta_i - \theta_j) \quad (=: \delta_2) \right]$$

则 $\tau(\delta_i) = \delta_i$

$\tau(\theta_k - \theta_l) = -(\theta_k - \theta_l)$

$\Rightarrow \tau(\Delta(f)) = -\Delta(f)$

$\therefore \forall \tau \in S_n$ $\tau(\Delta(f)) = \pm\Delta(f)$ 且 $\because \mathrm{char}F \neq 2$

$\therefore \tau(\Delta(f)) = \Delta(f) \Leftrightarrow \sigma \in A_n$

$\therefore Gal(K/F(\Delta)) = Gal(f)\cap A_n \Rightarrow F(\Delta) = K^{Gal(K/F(\Delta))} = K^{Gal(f)\cap A_n}$ □

推论：F, f, θ_i 如定理1所设. 令 $D(f) = \Delta(f)^2$. 则

$Gal(f) \subseteq A_n \Leftrightarrow D(f) = c^2,\ c\in F$.

$D(f)$ 的计算：$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0$

$g = \frac{f'}{n} = x^{n-1} + \frac{n-1}{n}a_{n-1}x^{n-2} + \cdots + \frac{a_1}{n}$

$$D(f) = \begin{vmatrix} 1 & a_{n-1} & \cdots & a_0 & & & \\ & 1 & a_{n-1} & \cdots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & 1 & a_{n-1} & \cdots & a_0 \\ 1 & \frac{n-1}{n}a_{n-1} & \cdots & a_1 & & & \\ & 1 & \frac{n-1}{n}a_{n-1} & \cdots & a_1 & & \\ & & \ddots & & \ddots & \ddots & \\ & & & 1 & \frac{n-1}{n}a_{n-1} & \cdots & a_1 \end{vmatrix} \begin{matrix} \\ \\ \\ \\ \} n-1 \\ \\ \\ \\ \} n \end{matrix}$$

称为 f 与 g 的结式.

例：$F=\mathbb{Q}$, $f = x^3 + ax + b \in \mathbb{Q}[x]$. 则 $D(f) = -4a^3 - 27b^2$

设 f 不可约 则 $3 \mid |Gal(f)| \mid 6 \Rightarrow |Gal(f)| = 3$, 或 6.

$$\therefore Gal(f) = \begin{cases} A_3 & -4a^3-27b^2 = c^2,\ c\in\mathbb{Q} \\ S_3 & \text{其它} \end{cases}$$

定理2：设 $f\in F[x]$ 无重根，$\theta_1, \cdots \theta_n$ 为其所有根. 则 f 在 F 上不可约

$\Leftrightarrow Gal(f)$ 在 $\{\theta_1, \cdots \theta_n\}$ 作用是可迁的.

证：$\forall \varphi \in Gal(f)$. $f(\varphi(\theta_1)) = 0 \Rightarrow \{\varphi(\theta_1) \mid \varphi\in Gal(f)\} \subseteq \{\theta_1, \cdots \theta_n\}$

令 $g = \prod_{\varphi\in Gal(f)} (X - \varphi(\theta_1))$. 则 $\forall \psi \in Gal(f)$, $\psi(g) = \prod_{\varphi\in Gal(f)} (X - \psi\varphi(\theta_1)) = g$

$\therefore g \in F[x]$.

($\Rightarrow$) f 不可约且 $f(\theta_1) = 0 \Rightarrow f \mid g \Rightarrow \{\theta_1, \cdots \theta_n\} = \{\varphi(\theta_1) \mid \forall \varphi \in Gal(f)\}$.

($\Leftarrow$) 设 $f = f_1 f_2$, $f_1, f_2 \in F[x]$. 且 $f_1(\theta_1) = 0$. 则 $\forall \varphi \in Gal(f)$, $f_1(\varphi(\theta_1)) = 0$.

$\because Gal(f)$ 在 $\{\theta_1, \cdots \theta_n\}$ 上作用是可迁的. $\therefore \forall \theta_i, \exists \varphi_i \in Gal(f)$ s.t. $\theta_i = \varphi_i(\theta_1)$.

从而 $\forall 1\le i\le n,\ f_1(\theta_i)=0 \Rightarrow f=\lambda f_1,\ \lambda_1\in F \Rightarrow f$ 不可约. □

命题1：设 $G\le S_n$ 为可迁的，且 G 含有对换及一个长度为 $n-1$ 的置换，则 $G=S_n$.

证：经适当排序，设 $\sigma=(12\cdots n-1)\in G$，$(ij)\in G$.

$\because G$ 可迁 $\therefore (kn)\in G,\ k<n$.

$\sigma(kn)\sigma^{-1}=(k+1,n)\in G$，重复下去有 $(in)\in G,\ \forall 1\le i\le n-1$

$\therefore G=S_n$.

命题2：设 p 为素数，$G\le S_p$ 为子群，若 G 含 p 阶元与对换，则 $G=S_p$.

证：经适当排序，设 $(12)\in G$. $\because p$ 为素数 $\therefore G$ 中 p 阶元有形式 $(1i_2\cdots i_p)$.

则 $\exists s>0$ s.t. $\tau=\sigma^s=(12j_3\cdots j_p)\in G$.

则 $\tau(12)\tau^{-1}=(2j_3)$，$\tau(2j_3)\tau^{-1}=(j_3j_4)\cdots\ \tau(j_{p-2}j_{p-1})\tau^{-1}=(j_{p-1}j_p)\in G$

$\therefore G=S_p$. □

定理3：设 $f\in\mathbb{Q}[X]$ 为素数次不可约，若 f 在 $\mathbb{C}$ 中恰有两个非实根，则 $Gal(f)=S_p$.

证：设 $f=\prod_{i=1}^{p}(X-\theta_i)$，$\theta_1,\theta_2\notin\mathbb{R}$，$\theta_3,\cdots\theta_p\in\mathbb{R}$. 设 $K=\mathbb{Q}(\theta_1,\cdots\theta_p)$.

$\because f\in\mathbb{Q}[X]$ $\therefore \theta_1=\overline{\theta_2}$ 令 $\varphi:\mathbb{C}\to\mathbb{C},\ z\to\overline{z}$ 则 $\varphi(K)=K$ 且 $\varphi|_{\mathbb{Q}}=id$

$\therefore \varphi\in Gal(f)$ 且 $\varphi(\theta_1)=\theta_2$，$\varphi(\theta_2)=\theta_1$，$\varphi(\theta_i)=\theta_i$ $i\ge3$.

$\therefore \varphi$ 为一个对换.

另外，$[\mathbb{Q}(\theta_1):\mathbb{Q}]=\deg f=p \Rightarrow p\mid[K:F]=|Gal(f)|$.

由西罗定理，$Gal(f)$ 含 p 阶元，由命题2，$Gal(f)=S_p$. □

定理4 (Brauer) 对 $\forall$ 素数 p，$\exists$ 任意多个 p 次不可约多项式其伽罗瓦群为 S_p.

证：$p=2$ 时 令 $f=X^2-(2k+1)$，$k\in\mathbb{Z}\setminus\{0\}$. 则 $Gal(f)=S_2$.

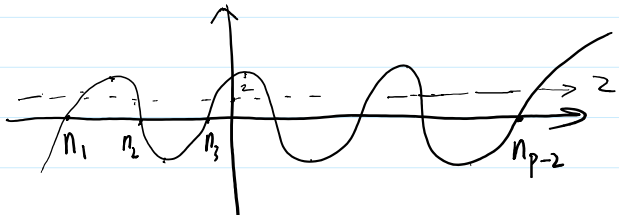
$p=3$ 时 令 $f=X^3+q(X+1)$ q 为素数，则 $Gal(f)=S_3$

设 $p>3$，$m,n_1,\cdots n_{p-2}$ 为偶数且 $m>0$，$n_1<n_2<\cdots<n_{p-2}$.

令 $g(X)=(X^2+m)(X-n_1)\cdots(X-n_{p-2})$ 则 $\deg g=p$.

g 有 $\frac{p-3}{2}$ 个局部极大值.

$\forall$ 实数 h 有 $|g(h)|>2$. $\because (n_i,n_{i+1})$ 存在实数



$\forall$ 奇数 h 有 $|g(h)|>2$. $\because (n_i, n_{i+1})$ 存在奇数 

$\therefore$ 局部极大值均 >2.

令 $f=g-2$. 则 f 在 (n_1, n_{p-2}) 中至少有 $p-3$ 个实根.

又 $\because$ 当 $a\to+\infty$ 时 $f(a)\to+\infty$ 且 $f(n_{p-2})=-2<0$.

$\therefore$ f 在 $(n_{p-2}, +\infty)$ 中至少有一个实根 $\Rightarrow$ f 至少有 $p-2$ 个实根

令 $f=\prod_{i=1}^{p}(X-\theta_i)=(X^2+m)(X-n_1)\cdots(X-n_{p-2})-2$.

比较系数有 $\sum_{i=1}^{p}\theta_i=\sum_{i=1}^{p-2}n_i$ $\sum_{1\le i<j\le p}\theta_i\theta_j=\sum_{1\le i<j\le p-2}n_in_j+m$

$$\therefore \sum_{i=1}^{p}\theta_i^2=\left(\sum_{i=1}^{p}\theta_i\right)^2-2\sum_{1\le i<j\le p}\theta_i\theta_j=\left(\sum_{i=1}^{p-2}n_i\right)^2-2\left(\sum_{1\le i<j\le p-2}n_in_j+m\right)$$
$$=\sum_{i=1}^{p-2}n_i^2-2m$$

当 m 充分大时有 $\sum_{i=1}^{p}\theta_i^2<0$ $\therefore$ f 有非实根 从而 f 恰有两个非实根.

设 $f=X^p+\sum_{i=0}^{p-1}a_iX^i$ 则 $2|a_i$ 且 $a_0=-mn_1\cdots n_{p-2}-2$ 不被 4 整除.

$\therefore$ f 不可约. 由定理 3 有 $Gal(f)=S_p$ □

K/F 为有限伽罗瓦扩张 $u_1,\cdots u_n$ 为 K 的一组 F-基, $\varphi\in Gal(K/F)$.

则 $\varphi: K\to K$ 为 F-线性映射 $\exists g_\varphi\in GL_n(F)$ s.t.

$$\begin{pmatrix}\varphi(u_1)\\ \vdots\\ \varphi(u_n)\end{pmatrix}=g_\varphi\begin{pmatrix}u_1\\ \vdots\\ u_n\end{pmatrix}$$

一般而言 g_φ 不是置换矩阵

另一方面 $\exists\alpha\in K$ s.t. $K=F(\alpha)$. f_α 为极小多项式 $/F$, $\alpha_i=\varphi_i(\alpha)$ $i=1,\cdots n$ 为 f_α 的所有根. 且 $\forall\varphi\in Gal(K/F)$, $\varphi(\alpha_1),\cdots\varphi(\alpha_n)$ 为 $\alpha_1,\cdots\alpha_n$ 的一个置换.

但 $\alpha_1,\cdots\alpha_n$ 不一定是 K 的一组 F-基.

例: $F=\mathbb{Q}$, $K=\mathbb{Q}(\sqrt2+\sqrt3)=\mathbb{Q}(\sqrt2,\sqrt3)$, $f=X^4-10X^2+1$,

$\{\pm\sqrt2\pm\sqrt3\}$ 为 f 的所有根 但它们不是一组基.

定义: K/F 为有限伽罗瓦扩张, $u\in K$. 若 $\{\varphi(u)\mid\varphi\in Gal(K/F)\}$ 为 K 的一组 F-基. 则称 $\{\varphi(u)\mid\varphi\in Gal(K/F)\}$ 为 K/F 的正规基.

H 为幺半群 F 为域

称半群同态 $\chi: H \to U(F)$ 为 H 到 F 的特征标:

$$(\chi(h_1h_2)=\chi(h_1)\chi(h_2),\ \chi(1)=1)$$

引理1 (Dedekind-Artin) H 到 F 的不同特征标 $\chi_1, \cdots \chi_n$ 在 F 上线性无关, 即

对于 $a_1, \cdots a_n \in F$, 若 $\sum_{i=1}^{n} a_i\chi_i(h)=0\ \forall h\in H$ 则 $a_i=0\ \forall 1\le i\le n$.

证: (归纳法) $n=1$ 时 $a_1\chi_1(1)=0 \Rightarrow a_1=0$.

设引理1对于 $n-1$ 成立. 设 $a_1, \cdots a_n \in F$ s.t. $\sum_{i=1}^{n} a_i\chi_i(h)=0\ \forall\ h\in H$ ①

$\chi_1 \neq \chi_2 \Rightarrow \exists\, h'\in H$ s.t. $\chi_1(h')\neq\chi_2(h')$

$\sum_{i=1}^{n} a_i\chi_i(h'h)=0\ \forall h\in H \Rightarrow \sum_{i=1}^{n} a_i\chi_i(h')\chi_i(h)=0\ \forall\ h\in H$ ②

$\chi_1(h')\times$① − ② 有 $\sum_{i=2}^{n} a_i(\chi_1(h')-\chi_i(h'))\chi_i(h)=0\ \forall h\in H$.

由归纳假设 $a_2(\chi_1(h')-\chi_2(h'))=0 \Rightarrow a_2=0$. ($\because \chi_1(h')-\chi_2(h')\neq 0$)

$\therefore\ a_1\chi_1(h)+\sum_{i=3}^{n} a_i\chi_i(h)=0\ \forall h\in H$.

再由归纳假设有 $a_1=a_3=\cdots=a_n=0$. □

命题3: 设 K/F 为有限伽罗瓦扩张, $n=[K:F]$, $Gal(K/F)=\{\varphi_1, \cdots \varphi_n\}$.

则 $\{u_1, \cdots u_n\}\subseteq K$ 为 F-组基 $\Leftrightarrow \det(M)\neq 0$

这里 $M=\begin{pmatrix} \varphi_1(u_1), & \varphi_1(u_2), & \cdots & \varphi_1(u_n) \\ \varphi_2(u_1), & \varphi_2(u_2), & \cdots & \varphi_2(u_n) \\ \vdots & & & \\ \varphi_n(u_1), & \varphi_n(u_2), & \cdots & \varphi_n(u_n) \end{pmatrix}$.

证: ($\Rightarrow$) 设 $\det(M)=0$. 则 $\exists\, a_1, \cdots a_n \in K$ 不全为0 s.t.

$$(a_1, \cdots a_n)M=0 \quad \text{i.e.} \quad \sum_{i=1}^{n}\varphi_j(u_j)a_i=0\ \ \forall 1\le j\le n.$$

$\forall \alpha\in K$, 记 $\alpha=\sum_{j=1}^{n} c_{j,\alpha}u_j$, $c_{j,\alpha}\in F$. 则

$$\sum_{i=1}^{n} a_i\varphi_i(\alpha)=\sum_{i=1}^{n} a_i\varphi_i\left(\sum_{j=1}^{n} c_{j,\alpha}u_j\right)=\sum_{j=1}^{n} c_{j,\alpha}\sum_{i=1}^{n} a_i\varphi_i(u_j)=0$$

易知: $\varphi_1, \cdots \varphi_n$ 为 $U(K)$ 到 $K^\times$ 的不同特征标 由引理1, $a_1=\cdots=a_n=0$ 矛盾.

$\therefore \det(M)\neq 0$.

($\Leftarrow$) 设 $\sum_{i=1}^{n} c_i u_i = 0$, $c_i \in F$. 则 $\sum_{i=1}^{n} c_i \varphi_j(u_i) = 0$.

$\therefore M(c_1, \cdots c_n)^t = 0$ $\because \det(M) \neq 0$ $\therefore c_1 = \cdots = c_n = 0$

$\therefore u_1, \cdots u_n$ 为一组 F-基. □

$\varphi \in Gal(K/F)$, φ 为 $U(K)$ 到 K 上的特征.

定义：称 $\varphi_1, \cdots \varphi_n \in Gal(K/F)$ 在 K 上代数无关. 若 $f \in K[X_1, \cdots X_n]$

$f(\varphi_1(a), \cdots \varphi_n(a)) = 0$ $\forall a \in K$ 则 $f = 0$.

命题4：设 $|F| = +\infty$. $Gal(K/F) = \{\varphi_1, \cdots \varphi_n\}$. 则 $\varphi_1, \cdots \varphi_n$ 在 K 上代数无关.

证：设 $f \in K[X_1, \cdots X_n]$. $f(\varphi_1(a), \cdots \varphi_n(a)) = 0$ $\forall a \in K$.

设 $u_1, \cdots u_n$ 为 K 的一组 F-基. 则 $a = \sum_{j=1}^{n} c_j u_j$, $c_i \in F$.

$\therefore 0 = f(\varphi_1(\sum_{j=1}^{n} c_j u_j), \cdots, \varphi_n(\sum_{j=1}^{n} c_j u_j)) = f(\sum_{j=1}^{n} c_j \varphi_1(u_j), \cdots, \sum_{j=1}^{n} c_j \varphi_n(u_j))$, $\forall c_1 \cdots c_n \in F$.

令 $g = f(\sum_{j=1}^{n} \varphi_1(u_j) X_j, \cdots, \sum_{j=1}^{n} \varphi_n(u_j) X_j) \in K[X_1, \cdots X_n]$

$= \sum_{j=1}^{n} g_j(X_1, \cdots X_n) u_j$ 其中 $g_j(X_1, \cdots X_n) \in F[X_1, \cdots X_n]$

$\because g(c_1, \cdots c_n) = 0$, $\forall c_1, \cdots c_n \in F$. $\Rightarrow \forall 1 \leq j \leq n$, $g_j(c_1, \cdots c_n) = 0$ $\forall c_1, \cdots c_n \in F$.

$\Longrightarrow \forall 1 \leq j \leq n$, $g_j(X_1, \cdots X_n) = 0$

$\because |F| = +\infty$

$\therefore g = 0$.

由命题3, $M = (\varphi_i(u_j))$ 为可逆矩阵.

ψ: $K[X_1, \cdots X_n] \longrightarrow K[X_1, \cdots X_n]$ 为环同构

$h(X_1, \cdots X_n) \longrightarrow h(\sum_{j=1}^{n} \varphi_1(u_j) X_j, \cdots, \sum_{j=1}^{n} \varphi_n(u_j) X_j)$

$\therefore g = 0 \Rightarrow f = 0$ □

引理：设 $|F| = +\infty$, $f \in F[X_1, \cdots X_n]$. 若 $f(c_1, \cdots c_n) = 0$ $\forall c_1, \cdots c_n \in F$. 则 $f = 0$.

证：(归纳法) $n = 1$ 时 若 $f \neq 0$. 则 $|\{c \in F \mid f(c) = 0\}| \leq \deg f < +\infty$

但 $F = \{c \in F \mid f(c) = 0\}$ 为无穷集 矛盾.

设引理对于 $n-1$ 时成立.

设 $f = \sum_{i=0}^{m} f_i X_n^i$, $m \geq 0$, $f_i \in F[X_1, \cdots X_{n-1}]$.

若 $f\neq 0$ 则 $\exists i_0$ s.t. $f_{i_0}\neq 0$ 由归纳假设 $\exists (\bar{c}_1,\cdots\bar{c}_{n-1})\in F^{n-1}$ s.t.

$$f_{i_0}(\bar{c}_1,\cdots\bar{c}_{n-1})\neq 0.$$

$\therefore f(\bar{c}_1,\cdots\bar{c}_{n-1},X_n)\neq 0$. 再由归纳假设 $\exists \bar{c}_n\in F$ s.t. $f(\bar{c}_1,\cdots\bar{c}_n)\neq 0$. 矛盾.

命题5：设 F 为有限域，K/F 为有限伽罗瓦扩张，则 K/F 有正规基.

证：由 BA II P175 定理2，$Gal(K/F)=\langle\sigma\rangle=\{1,\sigma,\cdots\sigma^{n-1}\}$ $n=[K:F]$.

将 K 看作 n 维 F-向量空间，则 σ 为 F 上 K 个可逆线性变换.

设 $\sum_{i=0}^{n-1}c_i\sigma^i=0$, $c_i\in F$. 即 $\sum_{i=0}^{n-1}c_i\sigma^i(a)=0\ \forall a\in K$.

由引理1知：$c_0=c_1=\cdots=c_{n-1}=0$, $\therefore 1,\sigma,\cdots\sigma^{n-1}$, F-线无关.

由 BA II P67 习题4知，$\exists u\in K$, s.t. $u,\sigma(u),\cdots,\sigma^{n-1}(u)$ 为 K 个一组 F-基. □

定理II：设 K/F 为有限伽罗瓦扩张，则 K/F 有正规基.

证：由命题5，仅需对 $|F|=+\infty$ 时证明定理.

设 $Gal(K/F)=\{\varphi_1,\cdots\varphi_n\}$, X_{φ_i} 为未定元，记 $X_i=X_{\varphi_i}$, $i=1,\cdots n$.

令 $f=\det\left((X_{\varphi_i^{-1}\varphi_j})\right)\in F[X_1,\cdots X_n]$. $(\because \varphi_i^{-1}\varphi_j\in\{\varphi_1,\cdots\varphi_n\})$

定义赋值同态 $\psi: F[X_1,\cdots X_n]\longrightarrow F$

$$X_i\longrightarrow \psi(X_i)=\psi(X_{\varphi_i}):=\begin{cases}1 & \varphi_i=id\\ 0 & \varphi_i\neq id\end{cases}.$$

则 $\psi(f)=\det\left(\begin{pmatrix}1&&\\&\ddots&\\&&1\end{pmatrix}\right)=1$ $\therefore f\neq 0$.

由命题4知：$\exists\ u\in K$ s.t. $f(\varphi_1(u),\cdots\varphi_n(u))\neq 0$.

注意到 $\forall a\in K$, 若 $X_l=X_{\varphi_l}=\varphi_l(a)$, $l=1,\cdots n$. 则 $X_{\varphi_i^{-1}\varphi_j}=\varphi_i^{-1}\varphi_j(u)$

从而 $0\neq f(\varphi_1(u),\cdots\varphi_n(u))=\begin{vmatrix} u & \varphi_1^{-1}\varphi_2(u) & \cdots & \varphi_1^{-1}\varphi_n(u)\\ \varphi_2^{-1}\varphi_1(u) & u & \cdots & \varphi_2^{-1}\varphi_n(u)\\ \vdots & & & \vdots\\ \varphi_n^{-1}\varphi_1(u) & \varphi_n^{-1}\varphi_2(u) & \cdots & u\end{vmatrix}$

$\because\{\varphi_1^{-1},\cdots\varphi_n^{-1}\}=\{\varphi_1,\cdots\varphi_n\}$. 由命题3知：$\varphi_1(u),\cdots\varphi_n(u)$ 为 K 个一组 F-基 □.

K/F 为有限伽罗瓦扩张 $Gal(K/F)=\{\varphi_1,\cdots\varphi_n\}$, $\alpha\in K$.

$Tr_F^K(\alpha):=\sum_{i=1}^{n}\varphi_i(\alpha)$ 称为 α 在 K/F 中的迹.

$N_F^K(\alpha) := \prod_{i=1}^{n} \varphi_i(\alpha)$ 称为 α 在 K/F 中的范数.

$L_\alpha : \begin{matrix} K \longrightarrow K \\ \beta \longrightarrow \beta\alpha \end{matrix}$ 为 F-线性映射, $u_1, \cdots u_n$ 为 K 的一组 F-基.

则 $\exists M_\alpha \in M_n(F)$ s.t. $\begin{pmatrix} \alpha u_1 \\ \vdots \\ \alpha u_n \end{pmatrix} = M_\alpha \begin{pmatrix} u_1 \\ \vdots \\ u_n \end{pmatrix}$.

此时有 $T_F^K(\alpha) = Tr(M_\alpha)$, $N_F^K(\alpha) = \det(M_\alpha)$.

命题6: K/F 为有限伽罗瓦扩张. $\{\varphi(u) \mid \varphi \in Gal(K/F)\}$ 为 K/F 的正规基.

则 $\forall H \leq Gal(K/F)$ 子群, 有 $K^H = F(\alpha_H)$, 其中 $\alpha_H = T_{K^H}^K(\alpha)$.

证: $\forall \tilde{\varphi} \in H$, $\tilde{\varphi}(\alpha_H) = \tilde{\varphi}\left(\sum_{\varphi \in H} \varphi(\alpha)\right) = \sum_{\varphi \in H} \tilde{\varphi}\varphi(\alpha) = \alpha_H$

$\therefore \alpha_H \in K^H \Rightarrow F(\alpha_H) \subseteq K^H$

设 $\psi \in Gal(K/F)$, $\psi(\alpha_H) = \alpha_H$ 则 $0 = \sum_{\varphi \in H} \psi\varphi(\alpha) - \sum_{\varphi \in H} \varphi(\alpha)$

$\because \{\varphi(\alpha) \mid \varphi \in Gal(K/F)\}$ 为正规基 $\therefore \{\psi\varphi \mid \varphi \in H\} \cap H \neq \phi$.

i.e $\exists \varphi' \in H$ s.t. $\psi\varphi' \in H \Rightarrow \psi \in H$.

$\therefore Gal(K/F(\alpha_H)) \subseteq H \Rightarrow F(\alpha_H) = K^{Gal(K/F(\alpha_H))} \supseteq K^H \supseteq F(\alpha_H)$

$\therefore F(\alpha_H) = K^H$. □