# 方程的根式求解

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

$$T_F^K(u+v)=\sum_{i=1}^n\varphi_i(u+v)=\sum_{i=1}^n\varphi_i(u)+\sum_{i=1}^n\varphi_i(v)=T_F^K(u)+T_F^K(v)$$

$$T_F^K(au)=\sum_{i=1}^n\varphi_i(au)=a\sum_{i=1}^n\varphi_i(u)=aT_F^K(u)$$

$$N_F^K(uv)=\prod_{i=1}^n\varphi_i(uv)=N_F^K(u)N_F^K(v)$$

$$N_F^K(au)=a^nN_F^K(u)$$

$K/F$ 称为循环扩张(可解扩张) 若 $Gal(K/F)$ 是循环群(可解群)

定理1: (Speiser) 设 $K/F$ 为有限伽罗瓦扩张, $\eta: Gal(K/F)\to U(F)$ 为映射 s.t. $\varphi\to\eta_\varphi$

$$\eta_{\varphi_1\varphi_2}=\eta_{\varphi_1}\varphi_1(\eta_{\varphi_2})$$

则 $\exists\ 0\neq v\in K$ s.t. $\eta_\varphi=\dfrac{v}{\varphi(v)}$ $\forall\varphi\in Gal(K/F)$.

证: 设 $Gal(K/F)=\{\varphi_1,\cdots\varphi_n\}$. $\because\eta_{\varphi_i}\neq0$ $\forall 1\le i\le n$ 且 $\varphi_1,\cdots\varphi_n$ 在 $K$ 上线性无关.

$\therefore\exists\ w\in K$ s.t. $v=\sum_{i=1}^n\eta_{\varphi_i}\varphi_i(w)\neq0$

$\forall 1\le j\le n$

$$\varphi_j(v)=\sum_{i=1}^n\varphi_j(\eta_{\varphi_i})\varphi_j\varphi_i(w)=\sum_{i=1}^n\eta_{\varphi_j\varphi_i}\cdot\eta_{\varphi_j}^{-1}\varphi_j\varphi_i(w)$$

$$=\Big[\sum_{i=1}^n\eta_{\varphi_j\varphi_i}\varphi_j\varphi_i(w)\Big]\eta_{\varphi_j}^{-1}=v\eta_{\varphi_j}^{-1}$$

$\therefore\eta_{\varphi_j}=v/\varphi_j(v)$. □

定理2 (Hilbert 1897) 设 $K/F$ 为有限循环扩张, $Gal(K/F)=\langle\varphi\rangle$, $|Gal(K/F)|=n$

$u\in K$. 则 $N_F^K(u)=1\iff\exists\ 0\neq v\in K$ s.t. $u=\dfrac{v}{\varphi(v)}$

证: ($\Rightarrow$) 设 $\eta_{\varphi^i}:=\begin{cases}1 & i=0\\ u\varphi(u)\cdots\varphi^{i-1}(u) & 1\le i\le n\\ \eta_{\varphi^r},\ r\equiv i \bmod n,\ 0\le i<n & i>n\end{cases}$

$\forall 0\le i,j\le n-1$,

当 $i+j\le n$ 时 $\eta_{\varphi^{i+j}} = u\varphi(u)\cdots\varphi^{i-1}(u)\varphi^{i}(u)\cdots\varphi^{i+j-1}(u)$

$= u\varphi(u)\cdots\varphi^{i-1}(u)\varphi^{i}(u\varphi(u)\cdots\varphi^{j-1}(u))$

$= \eta_{\varphi^i}\varphi^i(\eta_{\varphi^j})$

当 $i+j>n$ 时，则 $i+j=n+r$，$0\le r<n$.

$\eta_{\varphi^{i+j}} = \eta_{\varphi^r} = u\varphi(u)\cdots\varphi^{r-1}(u)\varphi^{r}(u\varphi(u)\cdots\varphi^{n-1}(u))$

$= u\varphi(u)\cdots\varphi^{n+r-1}(u) = u\varphi(u)\cdots\varphi^{i-1}(u)\varphi^{i}(u\varphi(u)\cdots\varphi^{j-1}(u))$

$= \eta_{\varphi^i}\varphi^i(\eta_{\varphi^j})$

$\therefore \eta$ 满足定理1中条件 $\therefore \exists\, 0\neq v\in K$ s.t. $u=\eta_\varphi = \frac{v}{\varphi(v)}$

($\Leftarrow$) $u=\frac{v}{\varphi(v)} \Rightarrow N_F^K(u) = \prod_{i=0}^{n-1}\varphi^i(u) = \frac{v}{\varphi^n(v)} = 1$.

定理3：设 $n>0$，$\mathrm{char}F\nmid n$ 且 $F$ 含有 $x^n-1$ 的所有根，则

1) 若 $K/F$ 为循环扩张且 $n=[K:F]$，则 $K=F(u)$，$u^n\in F$.

2) 若 $u\in K$ 满足 $u^n\in F$，则 $F(u)/F$ 为循环扩张且 $[F(u):F]\mid n$，$u^{[F(u):F]}\in F$.

证：1) $\because \mathrm{char}F\nmid n \therefore x^n-1$ 在 $F$ 中无重根，设 $\zeta\in F$ 满足 $\zeta^n=1$，$\zeta^i\neq 1\ 0<i<n$

设 $\mathrm{Gal}(K/F)=\langle\varphi\rangle$，则 $N_F^K(\zeta)=\zeta^n=1$. 由定理2，$\exists\, 0\neq v\in K$ s.t.

$\zeta=\frac{v}{\varphi(v)}$ 即 $\varphi(v)=\zeta^{-1}v \Rightarrow \varphi(v^n)=v^n \Rightarrow v^n=a\in F$

设 $f_v$ 为 $v$ 在 $F$ 上极小多项式，则 $f_v(\varphi^i(v))=f_v(\zeta^{-i}v)=0$. $\forall\, 0\le i\le n-1$

$\therefore f_v$ 在 $F$ 中有 $n$ 个根 $\Rightarrow f_v=x^n-a$.

$\therefore [F(v):F]=\deg f_v = n \Rightarrow F(v)=K$.

2) 设 $u^n=a\in F$，则 $\zeta^i u$，$0\le i\le n-1$ 为 $x^n-a$ 的所有根

$\therefore F(u)$ 为 $x^n-a$ 在 $F$ 上的分裂域 $\because x^n-a$ 可分

$\therefore F(u)/F$ 为伽罗瓦扩张且 $[F(u):F]\le n$.

设 $\varphi\in\mathrm{Gal}(F(u)/F)$ 则 $\varphi(u)=\zeta^{m_\varphi}u$ $0\le m_\varphi\le n-1$.

定义：$\psi:\mathrm{Gal}(F(u)/F)\longrightarrow\langle\zeta\rangle$，$\varphi\longrightarrow\zeta^{m_\varphi}$ 则 $\psi$ 为群的单同态

$\because \psi(\mathrm{Gal}(K/F))$ 为循环群且阶数为 $n$ 的因子

∴ $Gal(K/F)$ 为循环群且 $m=|Gal(K/F)|\,|n$.

设 $Gal(K/F)=\langle\varphi\rangle$. 则 $\varphi^m(u)=\xi^{m m_\varphi}u=u \Rightarrow n\mid m m_\varphi$

∴ $\varphi(u^m)=(\xi^{m_\varphi}u)^m=u^m \Rightarrow u^m\in F$.

下面假设 $\mathrm{char}F=0$.

定义：$K/F$ 称为根式扩张. 若 $\exists$

$$F=k_0\subset k_1\subset\cdots\subset k_{r-1}\subset k_r=K$$

其中 $k_i=k_{i-1}(u_i)$ $u_i^{n_i}\in k_{i-1}$, $\forall\ 1\le i\le r$, $n_i>0$.

$f\in F[X]$ 称为根式可解若 $\exists$ 根式扩张 $K/F$ s.t. $K$ 包含 $f$ 的所有根

引理1：

1) 若 $K/F$, $L/K$ 为根式扩张 则 $L/F$ 为根式扩张.

2) 设 $F\subseteq K_1\subseteq L$ 且 $F\subseteq K_2\subseteq L$ 为中间域. 若 $K_1/F$ 为根式扩张

则 $K_2(K_1)/K_2$ 为根式扩张.

进一步若 $K_2/F$ 也为根式扩张 则 $K_1(K_2)/F$ 为根式扩张.

证：1) 由定义

2) $\exists\ F=F_0\subseteq F_1\subseteq\cdots\subseteq F_r=K_1$, $F_i=F_{i-1}(u_i)$, $u_i^{n_i}\in F_{i-1}$.

令 $\widetilde{F}_0=K_2$, $\widetilde{F}_1=\widetilde{F}_0(u_1)$, $\cdots$ $\widetilde{F}_r=\widetilde{F}_{r-1}(u_r)$

则 $K_1\subseteq\widetilde{F}_r \Rightarrow K_2(K_1)\subseteq\widetilde{F}_r$ $\because u_r\in K_1$ $\therefore \widetilde{F}_r\subseteq K_2(K_1)$

$\therefore \widetilde{F}_r=K_2(K_1)$ 易知：$u_i^{n_i}\in F_{i-1}\subseteq\widetilde{F}_{i-1}$

$\therefore K_2(K_1)/K_2$ 为根式扩张.

若 $K_2/F$ 为根式扩张 由1)有 $K_2(K_1)/F$ 为根式扩张. □

引理2：设 $K/F$ 为根式扩张. 则 $\exists\ L/K$ s.t. $L/F$ 为根式伽罗瓦扩张.

证：$\because K/F$ 为有限可分 $\therefore \exists\ \alpha\in K$ s.t. $K=F(\alpha)$

令 $f_\alpha$ 为 $\alpha$ 在 $F$ 上的极小多项式，$L$ 为 $f_\alpha$ 在 $F$ 上的分裂域

则 $L/F$ 为伽罗瓦扩张. 下证 $L/F$ 为根式扩张.

设 $\alpha_1=\alpha,\cdots\alpha_m$ 为 $f_\alpha$ 在 $L$ 中的所有根 则 $L=F(\alpha_1,\cdots\alpha_m)$

$\because F(\alpha)/F$ 为根式扩张.

∴ 存 $F=F_0\subset F_1\subset F_2\subset\cdots\subset F_r=F(\alpha)$

$F_i=F_{i-1}(u_i)$, $u_i^{n_i}\in F_{i-1}$

$\forall\ \alpha_j$ 由BA三 P190 定理2，存 $\varphi_j\in Gal(K/F)$ s.t. $\alpha_j=\varphi_j(\alpha)$

则 $F=F_0\subset\varphi_j(F_1)\subset\varphi_j(F_2)\subset\cdots\subset\varphi_j(F_r)=F(\alpha_j)$

$\forall\ u_i$, $u_i^{n_i}\in F_{i-1}\Rightarrow\varphi_j(u_i)^{n_i}\in\varphi_j(F_{i-1})$

并且 $\varphi_j(F_i)=\varphi_j(F_{i-1}(u_i))=\varphi_j(F_{i-1})(\varphi_j(u_i))$

∴ $F(\alpha_j)/F$ 为根式扩张.

由引理1知：$K(\alpha_1,\cdots\alpha_m)/F$ 为根式扩张. □

定理4：设 $K/F$ 为根式伽罗瓦扩张. 则 $Gal(K/F)$ 可解.

证：设 $F=K_0\subset K_1\subset\cdots\subset K_r=K$ $K_i=K_{i-1}(u_i)$, $u_i^{n_i}\in K_{i-1}$.

设 $\xi$ 为 $\prod_{i=1}^{r}n_i$ 次本原根. 考虑

$$F=K_0\subset K_0(\xi)\subset K_1(\xi)\subset\cdots\subset K_r(\xi)=K(\xi)$$

设 $K$ 为 $f$ 在 $F$ 上的分裂域 则 $K(\xi)$ 为 $(x^n-1)f$ 在 $F$ 上的分裂域

∴ $K(\xi)/F$ 为伽罗瓦扩张.

$\forall\ 1\le i\le r$, $K_i(\xi)$ 为 $x^{n_i}-u_i^{n_i}$ 在 $K_{i-1}(\xi)$ 上的分裂域

∴ $K_i(\xi)/K_{i-1}(\xi)$ 为伽罗瓦扩张.

记 $G_i=Gal(K(\xi)/K_i(\xi))$ $i=0,\cdots r$.

则由BA三 P185 定理2 有：$G_{i+1}$ 为 $G_i$ 的正规子群且 $Gal(K_i(\xi)/K_{i-1}(\xi))\cong G_{i-1}/G_i$

∴ $G_0\trianglerighteq G_1\trianglerighteq G_2\trianglerighteq\cdots\trianglerighteq G_{r-1}\trianglerighteq G_r=\{1\}$.

且由定理3，$G_{i-1}/G_i$ 为循环群

∴ $G_0$ 可解. 又∵ $K_0(\xi)/K_0$ 为伽罗瓦扩张且 $Gal(K_0(\xi)/K_0)$ 为交换群.

($\varphi,\psi\in Gal(K_0(\xi)/K_0)$, 则 $\varphi(\xi)=\xi^{m_\varphi}$, $\psi(\xi)=\xi^{m_\psi}\Rightarrow\varphi\psi(\xi)=\xi^{m_\varphi m_\psi}=\psi\varphi(\xi)$)

∴ $G_0\trianglelefteq Gal(K(\xi)/F)$ 且 $Gal(K(\xi)/F)/G_0$ 为交换群.

∵ $G_0 \trianglelefteq Gal(K(\zeta)/F)$ 且 $Gal(K(\zeta)/F)/G_0$ 为交换群.

由 BA III $P_{37}$ 定理1, $Gal(K(\zeta)/F)$ 可解 □

引理3: 设 $F \subset K \subset L$ 为域扩张, $E \subset L$ 为子域且 $K/F$, $K(E)/E$ 为有限伽罗瓦扩张.

则 $Gal(K(E)/F(E))$ 到 $Gal(K/F)$ 存在单同态.

证: $\forall \varphi \in Gal(K(E)/F(E))$, $\varphi(K)=K$. $\Rightarrow \varphi|_K \in Gal(K/F)$

定义 $\psi$: $Gal(K(E)/F(E)) \longrightarrow Gal(K/F)$

$\varphi \longrightarrow \varphi|_K$

易验证 $\psi$ 为群同态.

设 $\varphi \in \ker\psi$. 则 $\varphi|_K = id_K$. 又∵ $\varphi|_E = id_E$ ∴ $\varphi = id_{K(E)}$ ∴ $\psi$ 为单射. □

定理5: $f \in F[x]\setminus F$ 根式可解 $\Leftrightarrow$ $Gal(f)$ 可解.

证: ($\Rightarrow$) 由引理2, $\exists$ $K/F$ 为根式伽罗瓦扩张 s.t. $f$ 的所有根 $\alpha_1, \cdots \alpha_n$ 在 $K$ 中.

则 $F(\alpha_1, \cdots \alpha_n) \subset K$ 为伽罗瓦扩张.

由伽罗瓦对应, $Gal(f) = Gal(F(\alpha_1,\cdots\alpha_n)/F) \cong Gal(K/F)/Gal(K/F(\alpha_1\cdots\alpha_n))$

由定理4, $Gal(K/F)$ 可解 ∴ $Gal(f)$ 可解.

($\Leftarrow$) 设 $K$ 为 $f$ 在 $F$ 上的分裂域且 $G = Gal(K/F)$ 可解.

令 $L$ 为 $X^{|G|}-1$ 在 $K$ 上的分裂域. 则 $L = K(\zeta)$ 其中 $\zeta$ 为 $|G|$ 次本原根.

则 $L$ 为 $(X^{|G|}-1)f$ 在 $F$ 上的分裂域 ∴ $L/F$ 为有限伽罗瓦扩张.

由引理3, $\widetilde{G} = Gal(L/F(\zeta))$ 可看作 $Gal(K/F)$ 的子群.

∴ $\widetilde{G}$ 可解且 $|\widetilde{G}| \mid |G|$.

令 $\widetilde{G} = \widetilde{G}_0 \trianglerighteq \widetilde{G}_1 \trianglerighteq \widetilde{G}_2 \trianglerighteq \cdots \trianglerighteq \widetilde{G}_m = \{1\}$ 为合成列.

由 BA III P41 习题1, 可假设 $\widetilde{G}_i/\widetilde{G}_{i+1}$ 为素数阶循环群, 记 $p_i = |\widetilde{G}_i/\widetilde{G}_{i+1}|$.

由伽罗瓦对应: $F(\zeta) = L_0 \subset L_1 \subset \cdots \subset L_m = L$

其中 $L_{i+1}/L_i$ 为伽罗瓦扩张且 $Gal(L_{i+1}/L_i) \cong \widetilde{G}_i/\widetilde{G}_{i+1}$, $0 \le i \le m-1$

∵ $p_i \mid n$ ∴ $\zeta^{\frac{n}{p_i}} \in L_i$ 为 $p_i$ 次本原根

由定理3, $L_{i+1} = L_i(u_{i+1})$, $u_{i+1}^{p_i} \in L_i$

$\therefore$ $\forall F(x)$ 为相对打张. $\because$ $F(x)$ 作为相对打张 $\therefore$ $\forall F$ 为相对打张.

由于 $K \subseteq L$ $\therefore$ $\mathcal{F}$ 相对可解 □