分裂域和重复根式扩张*

张文华, 姜小龙
(中山大学数学系, 广东 广州 510275)

摘 要: 设 E 为系数在 F 上的多荐式 $f(x)$ 的分裂域, 若 $f(x)$ 在 F 上根式可解, 则 E 必含在 F 的一个重复根式扩张中, 而 E 不一定是 F 的重复根式扩张。本文继续探讨了这一问题, 当 $\mathrm{Char}F \nmid n = \deg(f(x))$ 时证明: (1) 若 Galois 群 $\mathrm{Gal}(E/F)$ 可解, E 包含 p_i 次本原单位根, 则 E 是 F 的重复根式扩张, 这里 p_i 是 $\deg(f(x))$ 的全部素因子; (2) 若 E 是 F 的重复根式塔, 则 E 包含 p_i 次本原单位根; 并讨论了 $n = 2^s p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, p_i 为 Fermat 素数的情形。

关键词: 分裂域; 重复根式扩张; 根式塔; 本原单位根
中图分类号: O153.4 文献标识码: A 文章编号: 05A001 (2005) S1-0119-03

1 概念和背景

首先给出几个基本概念。设 K 是域 F 的扩张。若存在 $\alpha \in K$ 和正整数 n 使得 $K = F(\alpha)$, $\alpha^n \in F$, 则 K 称 F 是的根式扩张。当 $[K:F] = n$ 时, 又称 K 是 F 的单根式塔 (simple radical tower)。一般地, 若存在子域链 $F = F_0 \subseteq F_1 \subseteq \cdots \subseteq F_r = K$, 使得 F_i 是 F_{i-1} 的根式扩张, $i = 1, 2, \cdots, r$, 则称 K 是 F 的重复根式扩张 (repeated radical extension)。当 F_i 是 F_{i-1} 的单根式塔时, $i = 1, 2, \cdots, r$, 又称 K 是 F 的根式塔 (radical tower)。设 $f(x)$ 是 F 上次数大于 0 的多项式, E 是 $f(x)$ 在 F 上的分裂域, 如果存在 F 的一个重复根式扩张 L, 使得 $E \subseteq L$, 则称方程 $f(x) = 0$ 在 F 上可用根式解。

显然, 若方程 $f(x) = 0$ 在 F 上可用根式解, 则 E 必含在 F 的一个重复根式扩张中。有时, E 还可以含在 F 的一个根式塔中 ([1], 第八章定理 11)。然而, E 不一定是 F 的重复根式扩张。例如, 取 $F = Q$, 其中 Q 表示有理数域, $f(x) = x^3 - 6x + 3 \in F[x]$, 此时 E 就不是 F 的重复根式扩张[2]。在文 [2] 中, Isaacs 证明了在某些条件下, E 是 F 的重复根式扩张。本文继续探讨了这一问题, 并给出了 E 是 F 的重复根式扩张 (或根式塔) 的一些充分条件和必要条件。在本文中, 若无特别声明, F 是域, $f(x)$ 是 F 上次数大于 0 的多项式, E 是 $f(x)$ 在 F 上的分裂域, $[E:F] = n > 1$。

2 一些引理

下面的引理 1 是文 [3] 中定理 22.8 的一种特殊情形。

引理 1 设 K 是 F 的扩域, 且 F 含有一个 p 次本原单位根, 其中 p 为素数, 则下列条件等价: ① K 在 F 上是 Galois 的, 且 $[K:F] = p$。② $K = F(\alpha)$, $\alpha \notin F$, $\alpha^p \in F$。

引理 2 (1) $p^s q^t$ 阶群是可解群, 其中 p 和 q 均为素数 ([4], 第二章定理 7.4)。

(2) 奇数阶群是可解群。[5]

下面的引理 3 是文 [6] 中定理 3.5.3 的一个推论。

引理 3 设 m 是正整数, $\mathrm{char}F \nmid m$, ξ 是 m 次本原单位根, 则 $\mathrm{Gal}(F(\xi)/F)$ 的阶是 $\varphi(m)$ 的一个因子, 其中 φ 是欧拉函数。

引理 4 ([7], 第三章第 3 节定理 5) 设 $p_1, p_2, \cdots, p_k$ 是不同的素数, φ 是欧拉函数, 则 $\varphi(p_1, p_2 \cdots p_k) = (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$。

引理 5 ([8], 第五章引理 9.3) 设 K 是 F 的重复根式扩张, 若 L 是 K 在 F 上的正规闭包, 则 L 也是 F 的重复根式扩张。

3 主要结论

定理 1 设 $\mathrm{char}F \nmid n$, 若, 1) $\mathrm{Gal}(E/F)$ 是可解群; 2) E 包含 p_i 次本原单位根, 其中 p_i 是 n 的

* 收稿日期: 2005-01-04
基金项目: 国家自然科学基金资助项目 (10271121)
作者简介: 张文华 (1973 年生), 男, 研究生; 通讯联系人: 姜小龙; E-mail: ytzwh@163.com

全部不同的素因子，$i=1, 2, \cdots, s$，则 E 是 F 的重复根式扩张。

证明 因为 E 是 $f(x)$ 在 F 上的分裂域，且 $\mathrm{char}F \nmid n$，所以 E 是 F 的有限 Galois 扩张。设 ε_i 是 p_i 次本原单位根，$i=1, 2, \cdots, s$，令 $\varepsilon=\varepsilon_1\varepsilon_2\cdots\varepsilon_s$，$m=p_1p_2\cdots p_s$，则 ε 是 m 次本原单位根。由于 E 包含 ε_i，故 E 也包含 ε。令 $K=F(\varepsilon)$，根据 Galois 理论基本定理，$\mathrm{Gal}(E/K)$ 是 $\mathrm{Gal}(E/F)$ 的子群。因为可解群的子群仍是可解群，所以 $G=\mathrm{Gal}(E/K)$ 是可解群。于是有合成群列 $1=G_0\triangleleft G_1\triangleleft\cdots G_{r-1}\triangleleft G_r=G$，使得 G_i/G_{i-1} 为素数 n_i 阶循环群，$i=1, 2, \cdots, r$。在 Galois 对应下得到子域链 $E=K_0\supseteq K_1\supseteq\cdots\supseteq K_{r-1}\supseteq K_r=K$，其中 K_i 与 G_i 对应，并且 K_{i-1} 在 K_i 上是 Galois 的，由 $[K_{i-1}:K_i]=n_i$，$i=1, 2\cdots, r$。由 $[K_{i-1}:K_i]\mid[E:F]$ 知，$n_i\mid n$。因为 n_i 为素数，所以 n_i 等于 p_1，p_2，$\cdots$，p_s 中的某一个。显然 K_i 包含 m 次本原单位根 ε，$i=1, 2, \cdots, r$，从而也包含 p_j 次本原单位根，$j=1, 2, \cdots, s$。这样 K_i 包含 n_i 次本原单位根。由引理 1 知，K_{i-1} 是 K_i 的单根式塔，因此 E 是 K 的根式塔。又因为 $K=F(\varepsilon)$，而 $\varepsilon^m=1\in F$，所以 K 是 F 的根式扩张，于是 E 是 F 的重复根式扩张。

推论 1 设 $\mathrm{char}F \nmid n$，令 m 是 n 的全部不同的素因子之积。若 F 包含 m 次本原单位根，则 E 是 F 的根式塔当且仅当 $\mathrm{Gal}(E/F)$ 是可解群。

推论 2 设 $\mathrm{char}F\neq 2$，若 n 为 2 的方幂，则 E 是 F 的根式塔。

注：从定理 1 的证明过程中容易看出，推论 2 的结论可以更强些，即若 $\mathrm{char}F\neq 2$，则 E 是 F 的重复二次扩张当且仅当 n 为 2 的方幂。因为特征不为 2 的域的二次扩张是单根式塔，所以重复二次扩张是根式塔。

定理 2 设 $\mathrm{char}F \nmid n$，若 E 是 F 的根式塔，则 E 包含 p_i 次本原单位根，其中 p_i 是 n 的全部不同的素因子，$i=1, 2, \cdots, s$。

证明 设 $F=F_1\subseteq F_2\subseteq\cdots\subseteq F_{r+1}=E$，其中 $[F_{i+1}: F_i]=n_i>1$，$F_{i+1}=F_i(\alpha_i)$，$\alpha_i^{n_i}=a_i\in F_i$，$i=1, 2, \cdots, r$。不妨设 n_i 为素数。由 $[F_{i+1}: F_i]=n_i$ 知，$f_i(x)=x^{n_i}-a_i$ 上不可约。因为 $\mathrm{char}F \nmid n$，而 $n_i\mid n$，所以 $\mathrm{char}F \nmid n_i$，从而 $f_i(x)$ 在 F_i 可分，这样 $f_i(x)$ 有 n_i 个不同的根 α_i，$\varepsilon_i\alpha_i$，$\cdots$，$\varepsilon_i^{n_i-1}\alpha_i$，其中 ε_i 为 n_i 次本原单位根。由于 E 在 F 上正规，所以 E 在 F_i 上也正规且包含 $f_i(x)$ 的一个根 α_i，因此 E 包含 $f_i(x)$ 的全部根，从而包含 ε_i。又因为 $n=[E:F]=[F_{r+1}:F_r]\cdots[F_2:F_1]=n_r\cdots n_1$，所以 n_1，n_2，$\cdots$，n_r 就是 n 的全部素因子（可能有相同的）。于是 E 包含 p_i 次本原单位根，$i=1, 2, \cdots, s$。

定理 3 设 $\mathrm{char}F \nmid n$。

1）若 $n=2^sp^t$，其中 s 为非负整数，t 为正整数，p 为 Fermat 素数，则 E 是 F 的根式塔当且仅当 E 包含 p 次本原单位根。

2）若 $n=p_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$，其中 p_1，p_2，$\cdots$，p_k 是不同的 Fermat 素数，t_1，t_2，$\cdots$，t_k，k 均为正整数，则 E 是 F 的根式塔当且仅当 E 包含 p_i 次本原单位根，$i=1, 2, \cdots, k$。

证明 1）必要性 由定理 2 可知。

下证充分性。依题意，E 是 F 的有限 Galois 扩张，所以 $|\mathrm{Gal}(E/F)|=n=2^sp^t$。由引理 2 知，$\mathrm{Gal}(E/F)$ 是可解群，因此 E 和 F 满足定理 1 的条件。从定理 1 的证明过程中可知，E 是 $F(\varepsilon)$ 的根式塔，其中 ε 是 $2p$ 次本原单位根。由 $\mathrm{char}F \nmid n$ 知，$\mathrm{char}F\nmid 2p$。故 $x^{2p}-1$ 在 F 上可分。显然 $F(\varepsilon)$ 是 $x^{2p}-1$ 在 F 上的分裂域，从而 $F(\varepsilon)$ 是 F 的有限 Galois 扩张，于是 $[F(\varepsilon):F]=|\mathrm{Gal}(F(\varepsilon)/F|$。根据引理 3，$[F(\varepsilon):F]\mid\varphi(2p)$。因为 p 是 Fermat 素数，由引理 4 知，$\varphi(2p)=\varphi(2)\varphi(p)=(2-1)(p-1)=p-1$ 为 2 的方幂。再根据推论 2，$F(\varepsilon)$ 是 F 的根式塔，于是 E 是 F 的根式塔。

2）同理可证。

注：目前已知的 Fermat 素数有 3，5，17，257，65537。

定理 4 假设 $f(x)$ 在 F 上不可约，且有一个根含在 F 的扩张 K 中，而 $K\subseteq E$。

1）若 K 是 F 的重复根式扩张，则 E 也是 F 的重复根式扩张。

2）设 $n=2^sp_1^{t_1}p_2^{t_2}\cdots p_k^{t_k}$，其中 p_i 为 Fermat 素数，s 和 t_i 为非负整数，k 为正整数，$i=1, 2, \cdots, k$，$\mathrm{char}F \nmid N$。若 K 是 F 的根式塔，则 E 也是 F 的根式塔。

证明 1）依题意，E 是 K 在 F 上的正规闭包，由引理 5 即得。

2）设 $F=F_0\subseteq F_1\subseteq\cdots F_r=K$，其中，$F_i=F_{i-1}(\alpha_i)$，$\alpha_i^{n_i}=a_i\in F_{i-1}$，$n_i=[F_i:F_{i-1}]$，不妨设 n_i 为素数，$i=1, 2, \cdots, r$。类似于定理 2 的证明，可以证明 E 包含 n_i 次本原单位根 ε_i，$i=1, 2, \cdots, r$，不妨设 n_1，n_2，$\cdots$，n_t 是 $[K:F]$ 的全部不同的素因子，$1\leqslant t\leqslant r$。令 $m=n_1n_2\cdots n_t$，$\varepsilon=\varepsilon_1\varepsilon_2\cdots\varepsilon_t$，则 ε 是 m 次本原单位根且 $m\mid n$。令 $K_0=F(\varepsilon)$。易知 K_0 包含 n_i 次本原单位根 ε_i，$i=$

$1, 2, \cdots, t$。设 $\mathrm{Gal}(E/F)=\{\sigma_1, \sigma_2, \cdots, \sigma_l\}$。令 $K_1=K_0(\alpha_1, \sigma_1(\alpha_1), \cdots, \sigma_i(\alpha_1))$。显然，对任意 $\tau \in \mathrm{Gal}(E/F)$，都有 $\tau(K_1) \subseteq K_1$，故 K_1 在 F 上正规。从 K_0 到 K_1 有一个扩张链 $K_0 \subseteq K_0(\alpha_1) \subseteq K_0(\alpha_1, \sigma_1(\alpha_1)) \subseteq \cdots \subseteq K_1$。因为 $\alpha_1^{n_1}=\alpha_1 \in F \subseteq K_0$，$\sigma_i(\alpha_1)^{n_1}=\sigma_i(\alpha_1^{n_1})=\sigma_i(\alpha_1)=\alpha_1 \in K_0$，$i=1, 2, \cdots, l$，所以根据引理 1，在上述扩张链中，后一项是前一项的单根式塔（后一项有可能等于前一项）。于是 K_1 是 K_0 的根式塔。令 $K_2=K_1(\alpha_2, \sigma_1(\alpha_2), \cdots, \sigma_l(\alpha_2))$，同理可证 K_2 在 F 上正规，并且 K_i 是 K_1 的根式塔。如此继续下去，得到一个扩张链 $F \subseteq K_0 \subseteq K_1 \subseteq \cdots \subseteq K_r$，其中 K_i 在 F 上正规，并且 K_i 是 K_{i-1} 的根式塔，$i=1, 2, \cdots, r$。显然 K_r 是 K_0 的根式塔且 K_r 包含 $\alpha_1, \alpha_2, \cdots, \alpha_r$，因此 $K \subseteq K_r$。又由于 $K_r \subseteq E$，而 E 是 K 在 F 上的正规闭包，所以 $K_r=E$。于是 E 是 K_0 的根式塔。由 $\mathrm{char}F \nmid n$ 知，$\mathrm{char}F \nmid m$。根据引理 3，$[F(\varepsilon):F]$ 整除 $\varphi(m)$。由于 $n_i \mid n$，而 n_i 为素数，所以 n_i 等于 2 或 $p_1, \cdots, p_k$ 中的某一个。因为 p_i 为 Fermat 素数，$i=1, 2, \cdots, k$，所以根据引理 4，$\varphi(m)=\varphi(n_1)\varphi(n_2)\cdots\varphi(n_t)=(n_1-1)(n_2-1)\cdots(n_t-1)$ 为 2 的方幂。由推论 2 知，$K_0=F(\varepsilon)$ 是 F 的根式塔，于是 E 是 F 的根式塔。

推论 3　假设 $\mathrm{char}F=0$，且 $f(x)$ 在 F 上不可约，α 是 $f(x)$ 的任一个根。

1）若 $F(\alpha)$ 是 F 的重复根式扩张，则 E 也是 F 的重复根式扩张。

2）若 $F(\alpha)$ 是 F 的根式塔，且 $\deg f \leqslant 6$，则 E 也是 F 的根式塔。

证明　1）显然成立。下证 2）。设 $\deg f=m \leqslant 6$，$G=\mathrm{Gal}(E/F)$，因为 $f(x)$ 是 F 上的不可约可分多项式，所以 G 同构于 S_m 的一个子群，因此 $|G|$ 整除 $|S_m|$。由 $m \leqslant 6$ 知，$|S_m|$ 整除 $|S_6|$。由于 E 是 F 的有限 Galois 扩张，故 $n=[E:F]=|G|$。由以上知，n 是 $|S_6|$ 的因子。因为 $|S_6|=2^4 \cdot 3^2 \cdot 5$，所以 n 的素因子最多只有 2，3，5。根据定理 4，结论 2）成立。

参考文献：

[1] 聂灵沼，丁石孙. 数学引论[M]. 第二版. 北京：高等教育出版社，2000.

[2] ISAACS I M, MOULTON D P. Real fields and repeated radical extensions [J]. J Algebra, 1998, 201(2): 429－455.

[3] ISAACS I M. Algebra: A Graduate Course [M]. Beijing: China Machine Press, 2003.

[4] 冯克勤，章璞，李尚志. 群与代数表示引论[M]. 合肥：中国科学技术大学出版社，2003.

[5] FEIT W, THOMPSON J Solvability of group of odd order [J]. Pac Jour Math, 1963, 13: 775－1029.

[6] 郝炳新. 域论基础[M]. 北京：北京师范大学出版社，1988.

[7] 闵嗣鹤，严士健. 初等数论[M]. 第 3 版. 北京：高等教育出版社，2003.

[8] HUNGERFORD T W. Algebra [M]. New York: Springer－Verlag, 1974.

Splitting Fields and Repeated Radical Extensions

ZHANG Wen-hua, JIANG Xiao-long

(Department of Mathematics, Sun Yat-sen University, Guangzhou 510275, China)

Abstract: Let $f(x)$ be non-constant polynomial over a field F with E its splitting field. If $f(x)=0$ can be solved radically over F, E is contained in a repeated radical extension, while it not necessarily a repeated radical extension itself. When $\mathrm{Char}F \nmid n=\deg(f(x))$, this paper continues the discussion and proves that: (1) If the Galois group $\mathrm{Gal}(E/F)$ is solvable and E contains the p_i-th primitive roots of unity, then E is a repeated radical extension, where, p_i is the prime factor of n; (2) If E is a repeated radical tower, then E contains the p_i-th primitive roots of unity; Cases like $n=2^s p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$, p_i is a Fermat prime, are also discussed.

Key words: splitting field; repeated radical extension; radical tower; primitive root of unity