第30卷第5期
2010年10月

河池学院学报
JOURNAL OF HECHI UNIVERSITY

Vol.30 No.5
Oct.2010

Selmer多项式不可约性的一个新证明

谭发龙，方 辉
（黄山学院 数学系，安徽 黄山 245021）

［摘 要］ 由n次多项式$f(x)$的全部根$\alpha_1,\alpha_2,\cdots,\alpha_n$，构造一个关于根的对称多项式$S(f)=\sum_{i=1}^{n}(\alpha_i-\frac{1}{\alpha_i})$，如果多项式$f(x)$在$\mathbb{Q}[x]$可以分解为多项式$g(x)h(x)$，利用恒等式$S(f)=S(g)+S(h)$，得出多项式$g(x)$的可能形式，并利用上述方法给出Selmer多项式不可约性的一个统一证明.

［关键词］ Selmer多项式；不可约性；多项式根

［中图分类号］ O151.1 ［文献标识码］ A ［文章编号］1672-9021(2010)05-0012-02

［作者简介］ 谭发龙(1984-)，男，湖南邵东人，黄山学院数学系助教，硕士，主要研究方向：代数与数论.

［基金项目］ 安徽省教育厅教研基金资助项目(2007jyxm113).

高次整系数多项式的不可约的判定常常很困难，关于这方面有许多研究工作，其中较为著名有Eisenstein判别法（利用系数素因子的条件）. 文献[1]中给出了Perron判别法及其各种推广形式（利用系数绝对值满足的不等式的条件），Brown和Graham判别法（利用多项式在整数集合$\mathbb{Z}$上的取值为1和素数的个数满足一个不等式的条件），Schur也给出许多有趣不可约多项式问题. 1956年，Selmer在文献[2]中给出下面的定理.

定理：（ⅰ）当$n\geq 2$时，多项式$f_n(x)=x^n-x-1$在$\mathbb{Q}[x]$上不可约；

（ⅱ）当$n>2$且$n\not\equiv 2(\mathrm{mod}3)$时，多项式$g_n(x)=x^n+x+1$在$\mathbb{Q}[x]$上不可约.

证明： 设$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in\mathbb{Z}[x]$，$\alpha_1,\alpha_2,\cdots,\alpha_n$是$f(x)$的$n$个根. 定义

$$S(f)=\sum_{i=1}^{n}(\alpha_i-\frac{1}{\alpha_i}) \tag{1}$$

易知$S(f)$为$f(x)$全部根的对称函数. 由多项式函数根与系数的关系知

$$S(f)=\sum_{i=1}^{n}(\alpha_i-\frac{1}{\alpha_i})=\sum_{i=1}^{n}\alpha_i-\frac{\sum_{i=1}^{n}\alpha_1\cdots\alpha_{i-1}\alpha_{i+1}\cdots\alpha_n}{\prod_{i=1}^{n}\alpha_i})=-a_{n-1}-\frac{(-1)^{n-1}a_1}{(-1)^na_0}=-a_{n-1}+\frac{a_1}{a_0} \tag{2}$$

则$S(f)\in\mathbb{Q}$，特别地，当$a_0=\pm1$时，$S(f)\in\mathbb{Z}$.

如果$f(x)$在$\mathbb{Q}[x]$上可约，则$f(x)$在$\mathbb{Z}[x]$上可约，存在$g(x),h(x)\in\mathbb{Z}[x]$，使得$f(x)=g(x)h(x)$，其中$\deg(g(x)),\deg(h(x))<n$. 根据(1)式的定义则有

$$S(f)=S(g)+S(h) \tag{3}$$

下面讨论Selmer多项式$f_n(x)=x^n-x-1$和$g_n(x)=x^n+x+1$.

根据(1)式的定义则：$S(f_n)=S(g_n)=1$，为了方便我们对$f_n(x)=x^n-x-1$来证明($g_n(x)=x^n+x+1$

的证明完全类似). 设 α_i 是 $f_n(x)$ 的任意一个根, $\bar{\alpha}_i$ 是它的共轭,则

$$\alpha_i + 1 = \alpha_i^n, \qquad \bar{\alpha}_i + 1 = (\bar{\alpha}_i)^n \tag{4}$$

故有 $$\alpha_i + 1 + \bar{\alpha}_i = \alpha_i^n(\bar{\alpha}_i)^n - \alpha_i\bar{\alpha}_i = \begin{cases} \geqslant 0 & |\alpha_i| \geqslant 1 \\ \leqslant 0 & |\alpha_i| \leqslant 1 \end{cases} \tag{5}$$

因此 $(\alpha_i + 1 + \bar{\alpha}_i)(1 - \frac{1}{\alpha_i\bar{\alpha}_i}) \geqslant 0$,可得

$$\alpha_i - \frac{1}{\alpha_i} + \bar{\alpha}_i - \frac{1}{\bar{\alpha}_i} = (\alpha_i + \bar{\alpha}_i)(1 - \frac{1}{\alpha_i\bar{\alpha}_i}) \geqslant \frac{1}{\alpha_i\bar{\alpha}_i} - 1 \tag{6}$$

对 $f_n(x)$ 的任意首1整系数因式 $g(x)$,则 $g(x)$ 常数项为1或 -1 ,设 $\deg(g(x)) = l < n$,且 $S(g) \in \mathbb{Z}$. 记 β_j 为 $g(x)$ 的任意一个根,由(6)式可知

$$S(g) = \sum_{j=1}^{l}(\beta_j - \frac{1}{\beta_j}) \geqslant \frac{1}{2}\sum_{j=1}^{l}(\frac{1}{|\beta_j|^2} - 1) \tag{7}$$

再根据 $g(x)$ 常数项为1或 -1 ,则 $\prod_{j=1}^{l}\frac{1}{|\beta_j|^2} = 1$,

$$\sum_{j=1}^{l}\frac{1}{|\beta_j|^2} \geqslant l(\prod_{j=1}^{l}\frac{1}{|\beta_j|^2})^{\frac{1}{l}} = l \Rightarrow \sum_{j=1}^{l}(\frac{1}{|\beta_j|^2} - 1) \geqslant 0 \tag{8}$$

当且仅当 $|\beta_j| = 1 (j = 1,2,\cdots,l)$ 时,取等号. 所以有 $S(g) \geqslant 0$.

假设 f_n 在 $\mathbb{Q}[x]$ 上可约,则 $f_n(x)$ 在 $\mathbb{Z}[x]$ 上可约,存在 $g(x),h(x) \in \mathbb{Z}[x]$,使得 $f_n(x) = g(x)h(x)$,其中 $\deg(g(x)),\deg(h(x)) < n$. 由(3)式和 $S(g) \geqslant 0, S(h) \geqslant 0$ 知: $S(g) = 0$ 或 $S(h) = 0$,故 $1 = |\beta_j| = |1 + \beta_j| = |\beta_j|^n$,可得 $\beta_j = e^{\pm\frac{2\pi i}{3}}$,即 $f_n(x)$ 的因式 $g(x) = x^2 + x + 1$ 或 $\frac{f_n(x)}{g(x)} = x^2 + x + 1$,很显然 $(x^2 + x + 1) \nmid f_n(x)$,所以 $f_n(x) = x^n - x - 1$ 在 $\mathbb{Q}[x]$ 上不可约.

注意到 $(x^2 + x + 1) | g_n(x) = x^n - x^2 + (x^2 + x + 1)$,可得 $(x^2 + x + 1) | x^2(x^{n-2} - 1)$

又因为 $(x^2 + x + 1) | (x^3 - 1)$, $(x^2 + x + 1, x^2) = (x^2 + x + 1, x - 1) = 1$,从而有 $n - 2 \equiv 0 (\mathrm{mod}3)$. 故当 $n > 2$ 且 $n \not\equiv 2(\mathrm{mod}3)$ 时,多项式 $g_n(x) = x^n + x + 1$ 在 $\mathbb{Q}[x]$ 上不可约.

参考文献:

[1] 柯召,孙琦. 数论讲义[M]. 北京:高等教育出版社,1987.

[2] Ernst S Selmer. On the Irreducibility of Certain Trinomials [J]. Math. Scand, 1956, (4):287-302.

New Proof of Irreducibility of Selmer Polynomial

TAN Fa-long, FANG Hui

(Department of Mathematics, Huangshan University, Huangshan, Anhui 245041, China)

[Abstract] From the polynomial $f(x)$ of degree, we construct a symmetric polynomial $S(f) = \sum_{i=1}^{n}(\alpha_i - \frac{1}{\alpha_i})$ where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all the roots of $f(x)$. If $f(x)$ can be written as a product of two polynomials $g(x)$, $h(x)$ in $\mathbb{Q}[x]$, we can get all the results of $g(x)$ by using the identity $S(f) = S(g) + S(h)$. Then a new proof of the irreducibility of Selmer polynomial is given by using the method above.

[Key words] Selmer polynomial; irreducible; the root of the polynomial

收稿日期 2010-09-07

[责任编辑 刘景平]