分圆域 $Q(\zeta_{40})$的幂元整基

施 俊[1], 夏建国[2]

(1.江苏技术师范学院数理学院, 江苏 常州 213001
(2.南京师范大学数学科学学院, 江苏 南京 210097

[摘要] 讨论了分圆域 $Q(\zeta_{40})$的幂元整基问题. 证明了对于任何代数整数 $\alpha\in Z[\zeta_{40}]$, 当 $\alpha+\alpha\notin \mathbf{Z}$时, $Z[\alpha]=Z[\zeta_{40}]$当且仅当 α与 ζ_{40}等价.

[关键词] 幂元整基, 分圆域, 生成元, 单位
[中图分类号] O156.1 [文献标识码] A [文章编号] 1001-4616(2010)04-0028-05

Power Integral Bases of Cyclotomic Field $Q(\zeta_{40})$

Shi Jun[1], Xia Jianguo[2]

(1. School of Mathematics and Physics, Jiangsu Teachers University of Technology, Changzhou 213001, China
(2. School of Mathematical Sciences, Nanjing Normal University, Nanjing 210097, China

Abstract In this paper, we discuss the generators of power integral bases of the cyclotomic field $Q(\zeta_{40})$. We prove that for any algebraic integer $\alpha\in Z[\zeta_{40}]$, if $\alpha+\alpha\notin \mathbf{Z}$, then $Z[\alpha]=Z[\zeta_{40}]$ if and only if α is equivalent to ζ_{40}.

Key words power integral bases; cyclotomic field; generator; unit

对于一个数域 K, 其幂元整基不一定存在, Dedekind给出了不具有幂元整基的三次域的例子. 但对于分圆域 $Q(\zeta_n)$, 幂元整基总是存在的, 这里 ζ_n是一个 n次本原单位根, ζ_n就是幂元整基的一个生成元, 我们感兴趣的是找出它的所有幂元整基生成元.

对于一个伽罗华数域 K, 幂元整基生成元集在整数平移、伽罗华自同构、乘以 -1的情况下是不变的. 即若 α是 K的幂元整基生成元, 则 $\alpha'=n\pm\sigma(\alpha)$仍是 K的幂元整基生成元, 其中 $n\in\mathbf{Z}$, $\sigma\in Gal(K/Q)$, 我们称 α与 α'等价.

Bremner[1] 猜测分圆域 $Q(\zeta_p)$ (p为奇素数)的幂元整基生成元在等价意义下仅有 ζ_p与 $1/(1+\zeta_p)$两个, 并证明了 $p=7$时结论成立. Robertson L[2] 证明了 Bremner猜测在 $p\leqslant 23$且 $p\neq 17$时成立. Robertson[3] 找出了 2的幂次分圆域的所有幂元整基. 本文研究的是分圆域 $Q(\zeta_{40})$, 我们要证明的是: 当 $\alpha+\alpha\notin\mathbf{Z}$时, $Z[\alpha]=Z[\zeta_{40}]$当且仅当 α与 ζ_{40}等价. 以下我们用 ζ表示 ζ_{40}, G表示 $Gal(Q(\zeta)/Q)$.

1 主要结论研究

由参考文献[4], $G=\{\sigma_1,\sigma_3,\sigma_7,\sigma_9,\sigma_{11},\sigma_{13},\sigma_{17},\sigma_{19},\sigma_{21},\sigma_{23},\sigma_{27},\sigma_{29},\sigma_{31},\sigma_{33},\sigma_{37},\sigma_{39}\}$, 其中 $\sigma_i(\zeta)=\zeta^i$, 进而 $G=\langle\sigma_{-1}\rangle\times\langle\sigma_7\rangle\times\langle\sigma_{11}\rangle$.

引理 **1**[4] 设 ε是 $Z[\zeta]$的单位, 则 $\varepsilon/\bar{\varepsilon}$是 $Z[\zeta]$的单位根.

引理 **2**[5] 设 $\alpha\in Z[\zeta]$, $H=\{3,7,9,11,13,17,19,21,23,27,29,31,33,37,39\}$, 则下列几个结论是等价的:

(i) $Z[\alpha]=Z[\zeta]$.

收稿日期: 2009-12-16
基金项目: 国家自然科学基金(10771180)、江苏省自然科学基金(BK2007220).
通讯联系人: 夏建国, 博士, 教授, 研究方向: 代数数论. E-mail: xiajianguo@hotmail.com

(ii) $N_{Q(\zeta)/Q}(\alpha-\sigma_i(\alpha)) = \pm N_{Q(\zeta)/Q}(\zeta-\zeta^i)$, $\forall\, i\in H$.

(iii) $\dfrac{\alpha-\sigma_i(\alpha)}{\zeta-\zeta^i}$ 是 $Z[\zeta]$ 中的一个单位, $\forall\, i\in H$.

引理 **3**　设 α 是 $Q(\zeta)$ 的幂元整基生成元, $\gamma_7 = \dfrac{\alpha-\sigma_7(\alpha)}{\alpha-\alpha}$,

$$B_1 = \{l_1(-\zeta^4+\zeta^9)+l_2(-\zeta^3+\zeta^5+\zeta^7-\zeta^{11}+\zeta^{14})+l_3(-\zeta^5+\zeta^{15}) \mid l_1, l_2, l_3\in \mathbf{Z}\},$$

$$B_2 = \{l_1(\zeta-\zeta^5+\zeta^{11})+l_2(-\zeta^5+\zeta^{15})+l_3(-2\zeta^6+\zeta^{10}) \mid l_1, l_2, l_3\in \mathbf{Z}\},$$

$$B_3 = \{l_1(\zeta^3-\zeta^5-\zeta^7+\zeta^{11})+l_2(-\zeta^4+\zeta^{14})+l_3(-\zeta^5+\zeta^{15}) \mid l_1, l_2, l_3\in \mathbf{Z}\},$$

$$B_4 = \{l_1(\zeta^3-\zeta^5-\zeta^7-\zeta^9+\zeta^{11})+l_2\zeta^{14}+l_3(-\zeta^5+\zeta^{15}) \mid l_1, l_2, l_3\in \mathbf{Z}\}.$$

若 $\gamma_7\notin \mathbf{R}$, 则 α 与 $B_1\cup B_2\cup B_3\cup B_4$ 中的某一个元素等价.

证明　设 $\tau_7 = 1-\gamma_7$, $\pi_1 = 1-\zeta^8$, 由引理 2知 γ_7 和 $\dfrac{\tau_7}{\pi_1}$ 均为单位, 由引理 1知 $\dfrac{\overline{\gamma_7}}{\gamma_7}$ 为单位根, $\left(\dfrac{\overline{\tau_7}}{\pi_1}\right)\Big\backslash\dfrac{\tau_7}{\pi_1} = \dfrac{\overline{\tau_7}}{\tau_7}(-\zeta^8)$ 为单位根, $\dfrac{\overline{\tau_7}}{\tau_7}$ 也为单位根, 故存在 $s, r\in \mathbf{Z}$, 使得 $\overline{\gamma_7} = \zeta^s\gamma_7$, $\overline{\tau_7} = \zeta^r\tau_7$. 由 $\begin{cases}\gamma_7+\tau_7 = 1\\ \overline{\gamma_7}+\overline{\tau_7} = 1\end{cases}$ 解得

$$\begin{cases}\gamma_7 = \dfrac{\zeta^r-1}{\zeta^r-\zeta^s},\\ \tau_7 = \dfrac{1-\zeta^s}{\zeta^r-\zeta^s},\end{cases}\quad (1\leqslant r, s\leqslant 39).$$

因为 $\dfrac{\tau_7}{\pi_1} = \dfrac{1-\zeta^s}{\zeta^r-\zeta^s}\cdot\dfrac{1}{1-\zeta^8}$ 为单位, 所以 $s\equiv 0(\mathrm{mod}\ 8)$, 即 $s\in\{8, 16, 24, 32\}$. 又因为存在 $\sigma_i\in G$ 使 $\sigma_i(\gamma_7) = \dfrac{\zeta^r-1}{\zeta^r-\zeta^8}$, 故不妨设 $s = 8$, 即 $\gamma_7 = \dfrac{\zeta^r-1}{\zeta^r-\zeta^8}$.

下面分析 r. 因为 $\gamma_7 = \dfrac{\zeta^r-1}{\zeta^r-\zeta^8}\dfrac{\tau_7}{\pi_1} = \dfrac{1}{\zeta^r-\zeta^8}$ 均为单位, 故 $\zeta^r-\zeta^8 = \zeta^8(\zeta^{r-8}-1)$, ζ^r-1 也都是单位. 又易知 ζ^8-1, ζ^5-1 均不是单位, 所以 $5\nmid r$, $8\nmid r$, $5\nmid(r-8)$, 即 $r\in\{1, 2, 4, 6, 7, 9, 11, 12, 14, 17, 19, 21, 22, 26, 27, 29, 31, 34, 36, 37, 39\}$. 又因为 $r = 11, 21, 31$ 时, 存在 $\sigma_i\in G$, 使 $\sigma_i(\gamma_7) = \dfrac{\zeta-1}{\zeta-\zeta^8}$, 其中 i 分别取 11, 21, 31; $r = 22, 26$ 时, 存在 $\sigma_{11}\in G$, 分别使 $\sigma_{11}(\gamma_7) = \dfrac{\zeta^2-1}{\zeta^2-\zeta^8}$, $\sigma_{11}(\gamma_7) = \dfrac{\zeta^6-1}{\zeta^6-\zeta^8}$; $r = 17, 27, 37$ 时, 存在 $\sigma_i\in G$, 使 $\sigma_i(\gamma_7) = \dfrac{\zeta^7-1}{\zeta^7-\zeta^8}$, 其中 i 分别取 31, 21, 11; $r = 19, 29, 39$ 时, 存在 $\sigma_i\in G$, 使 $\sigma_i(\gamma_7) = \dfrac{\zeta^9-1}{\zeta^9-\zeta^8}$, 其中 i 分别取 11, 21, 31; $r = 34$ 时, 存在 $\sigma_{11}\in G$, 使 $\sigma_{11}(\gamma_7) = \dfrac{\zeta^{14}-1}{\zeta^{14}-\zeta^8}$; 故可设

$r\in\{1, 2, 4, 6, 7, 9, 12, 14, 36\}$.

设 $\alpha = \sum_{i=0}^{15} a_i\zeta^i$, $a_i\in \mathbf{Z}$, 将它代入方程

$$\frac{\alpha-\sigma_7(\alpha)}{\alpha-\alpha} = \frac{\zeta^r-1}{\zeta^r-\zeta^8}. \tag{1}$$

(i) 当 $r = 1$ 时, 方程 (1) 变为

$$\frac{\alpha-\sigma_7(\alpha)}{\alpha-\alpha} = \frac{\zeta-1}{\zeta-\zeta^8}, \tag{2}$$

由于 $g(x) = x^{16}-x^{12}+x^8-x^4+1$ 是 ζ 的极小多项式, 故

$$\zeta^{16}-\zeta^{12}+\zeta^8-\zeta^4+1 = 0. \tag{3}$$

联合 (2) 及 (3) 得到关于 $a_1, \cdots, a_{15}$ 的 16个方程组成的齐次线性方程组, 解得其基础解系为:

$$\xi_1 = (0, 0, 0, -1, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0),$$

$$\xi_2 = (0, 0, -1, 0, 1, 0, 1, 0, 0, 0, -1, 0, 0, 1, 0),$$
$$\xi_3 = (0, 0, 0, 0, -1, 0, 0, 0, 0, 0, 0, 0, 0, 1),$$

故 $\alpha = l_1(-\zeta^4 + \zeta^9) + l_2(-\zeta^3 + \zeta^5 + \zeta^7 - \zeta^{11} + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15}) \in B_1$.

(ii 当 $r = 2$时, 由方程(1)得

$$(\alpha - \sigma_7(\alpha))(\zeta^2 - \zeta^8) + (\alpha - \alpha)(\zeta^2 - 1) = 0 \tag{4}$$

联合(3)及(4)同理可得方程组并解得: $a_1 = a_2 = a_3 = a_4 = a_6 = a_7 = a_8 = a_9 = a_{10} = a_{11} = a_{12} = a_{13} = a_{14} = 0$, $a_{15} = -a_5$.

因此 $\alpha = a_5(\zeta^5 - \zeta^{15})$. 又因为 $\alpha = a_5(\zeta^5 - \zeta^{15}) \in \mathbf{R}$, 故 α不是分圆域 $Q(\zeta)$的幂元整基的一个生成元. 所以 $r \neq 2$ 同理可证 $r \neq 7, 9, 12, 14$

(iii 当 $r = 4$时, 同理可得

$$\alpha = l_1(\zeta - \zeta^5 + \zeta^{11}) + l_2(-\zeta^5 + \zeta^{15}) + l_3(-2\zeta^6 + \zeta^{10}) \in B_2.$$

(iv 当 $r = 6$时, 同理可得

$$\alpha = l_1(\zeta^3 - \zeta^5 - \zeta^7 + \zeta^{11}) + l_2(-\zeta^4 + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15}) \in B_3.$$

(v 当 $r = 36$时, 同理可得

$$\alpha = l_1(\zeta^3 - \zeta^5 - \zeta^7 - \zeta^9 + \zeta^{11}) + l_2\zeta^{14} + l_3(-\zeta^5 + \zeta^{15}) \in B_4.$$

综上, 我们证明了引理 3.

引理 4 设 α是 $Q(\zeta)$的幂元整基生成元, $\gamma_{11} = \dfrac{\alpha - \sigma_{11}(\alpha)}{\alpha - \alpha}$,

$$A = \{k_1\zeta^3 + k_2(-\zeta^4 + \zeta^6 + \zeta^{10}) + k_3(\zeta - \zeta^7 - \zeta^9 + \zeta^{11}) + k_4(-\zeta^8 + \zeta^{12}) + k_5(-\zeta + \zeta^5 - \zeta^7 - \zeta^9 + 2\zeta^{13}) + k_6(\zeta^2 + \zeta^4 - \zeta^8 + \zeta^{14}) + k_7(\zeta - \zeta^7 - \zeta^9 + \zeta^{15}),\ k_1, \cdots, k_7 \in \mathbf{Z}\},$$

若 $\gamma_{11} \notin \mathbf{R}$, 则 α与集合 A中某一元素等价.

证明 设 $\tau_{11} = 1 - \gamma_{11}$, $\pi_2 = 1 - \zeta^{10}$, 易知$\dfrac{\gamma_{11}}{\pi_2}$和 τ_{11}均为单位, 则存在 $m, n \in \mathbf{Z}$, 使 $\overline{\gamma_{11}} = \zeta^m\gamma_{11}$, $\overline{\tau_{11}} = \zeta^n\tau_{11}$. 由$\begin{cases}\gamma_{11} + \tau_{11} = 1\\ \overline{\gamma_{11}} + \overline{\tau_{11}} = 1\end{cases}$解得$\begin{cases}\gamma_{11} = \dfrac{1 - \zeta^n}{\zeta^m - \zeta^n}\\ \tau_{11} = \dfrac{\zeta^m - 1}{\zeta^m - \zeta^n}\end{cases}$, $(1 \leqslant m, n \leqslant 39)$. 因为$\dfrac{\gamma_{11}}{\pi_2}$和 τ_{11}均为单位, 故 $n \in \{10, 20, 30\}$. 而 $\sigma_3(\zeta^{30}) = \zeta^{10}$, 所以可设 $n \in \{10, 20\}$.

设 $\alpha = \sum_{i=0}^{15} a_i\zeta^i$, $a_i \in \mathbf{Z}$,

情形 **1** $n = 20$,

$\dfrac{\gamma_{11}}{\pi_2} = \dfrac{1 - \zeta^{20}}{(\zeta^m - \zeta^{20})(1 - \zeta^{10})} = \dfrac{1 + \zeta^{10}}{1 + \zeta^m}$. 要使$\dfrac{\gamma_{11}}{\pi_2}$为单位, 须 $m = 10, 30$

当 $m = 10$时 $\gamma_{11} = 1 - \zeta^{10}$. 由 $\gamma_{11} = \dfrac{\alpha - \sigma_{11}(\alpha)}{\alpha - \alpha}$及(3)式得方程组并解得其基础解系为:

$$\xi_1 = (0, 0, 0, 0, 0, 0, 0, -1, 0, 0, 0, 1, 0, 0, 0),$$
$$\xi_2 = (1, 0, 1, 0, -1, 0, 1, 0, 1, 0, 0, 0, -2, 0, 0),$$
$$\xi_3 = (-1, 0, -1, 0, 0, 0, 1, 0, 1, 0, -2, 0, 0, 0, 1),$$

故 $\alpha = k_1(-\zeta^8 + \zeta^{12}) + k_2(\zeta + \zeta^3 - \zeta^5 + \zeta^7 + \zeta^9 - 2\zeta^{13}) + k_3(-\zeta - \zeta^3 + \zeta^7 + \zeta^9 - 2\zeta^{11} + \zeta^{15})$.

但 $\alpha = \alpha$, 即 $\alpha \in \mathbf{R}$, 故 α不是分圆域 $Q(\zeta)$的幂元整基的一个生成元. 所以 $m \neq 10$

同理可得 $m \neq 30$, 故 $n \neq 20$

情形 **2** $n = 10$,

$\dfrac{\gamma_{11}}{\pi_2} = \dfrac{1 - \zeta^{10}}{(\zeta^m - \zeta^{10})(1 - \zeta^{10})} = \dfrac{1}{\zeta^{10}(\zeta^{m-10} - 1)}$为单位, $\tau_{11} = \dfrac{\zeta^m - 1}{\zeta^{10}(\zeta^{m-10} - 1)}$为单位, 那么 $\zeta^{m-10} - 1$, $\zeta^m - 1$均为单位. 而 $1 - \zeta^5$, $1 - \zeta^8$均不是单位, 因此, $5 \nmid m$, $8 \nmid m$, $8 \nmid (m - 10)$. 从而 $m \in \{1, 3, 4, 6, 7, 9, 11, 12,$

13, 14, 17, 19, 21, 22, 23, 27, 28, 29, 31, 33, 36, 37, 38, 39}. 又因为 $m \in \{1, 9, 13, 17, 21, 29, 33, 37\}$ 时, 存在 $\sigma_i \in G$ 使 $\sigma_i(\gamma_{11}) = \frac{\zeta^{10}-1}{\zeta^{10}-\zeta}$; 同理 $m \in \{3, 7, 11, 19, 23, 27, 31, 39\}$ 时, 存在 $\sigma_i \in G$ 使 $\sigma_i(\zeta_{11}) = \frac{\zeta^{10}-1}{\zeta^{10}-\zeta^3}$; $m \in \{4, 12, 28, 36\}$ 时, 存在 $\sigma_i \in G$ 使 $\sigma_i(\gamma_{11}) = \frac{\zeta^{10}-1}{\zeta^{10}-\zeta^4}$; $m \in \{6, 14, 22, 38\}$ 时, 存在 $\sigma_i \in G$ 使 $\sigma_i(\zeta_{11}) = \frac{\zeta^{10}-1}{\zeta^{10}-\zeta^6}$, 所以不妨设 $m \in \{1, 3, 4, 6\}$.

将 $\alpha = \sum_{i=0}^{15} a_i \zeta^i$, $a_i \in \mathbf{Z}$, 代入方程

$$\frac{\alpha - \sigma_{11}(\alpha)}{\alpha - \alpha} = \frac{1-\zeta^{10}}{\zeta^m - \zeta^{10}}. \tag{5}$$

(i) 当 $m = 1$时, 解由方程 (5) 及 (3) 组成的方程组得

$$\alpha = k_1(-\zeta^8 + \zeta^{12}) + k_2(\zeta + \zeta^3 - \zeta^5 + \zeta^7 + \zeta^9 - 2\zeta^{13}) + k_3(-\zeta - \zeta^3 + \zeta^7 + \zeta^9 - 2\zeta^{11} + \zeta^{15}).$$

但 $\alpha = \alpha$, 即 $\alpha \in \mathbf{R}$ 故 α 不是分圆域 $Q(\zeta)$ 的幂元整基的一个生成元, 所以 $m \neq 1$.

同理 $m \neq 3, 6$.

(ii) 当 $m = 4$时, 解由方程 (5) 及 (3) 组成的方程组得

$$\alpha = k_1\zeta^3 + k_2(-\zeta^4 + \zeta^6 + \zeta^{10}) + k_3(\zeta - \zeta^7 - \zeta^9 + \zeta^{11}) + k_4(-\zeta^8 + \zeta^{12}) + k_5(-\zeta + \zeta^5 - \zeta^7 - \zeta^9 + 2\zeta^{13}) + k_6(\zeta^2 + \zeta^4 - \zeta^8 + \zeta^{14}) + k_7(\zeta - \zeta^7 - \zeta^9 + \zeta^{15}),$$

此时 $\alpha \in A$.

综上, 我们证明了引理 4.

定理 1　设 α 是 $Q(\zeta)$ 的幂元整基生成元, 且 $\alpha + \alpha \notin \mathbf{Z}$, 则 α 与 ζ 等价.

证明　由于 $\alpha + \alpha \notin \mathbf{Z}$, 故 $\alpha + \alpha$ 不被 G 固定. 因为 $G = \langle\sigma_{-1}\rangle \times \langle\sigma_7\rangle \times \langle\sigma_{11}\rangle$, 所以 $\alpha + \alpha \neq \sigma_7(\alpha + \alpha)$ 或 $\alpha + \alpha \neq \sigma_{11}(\alpha + \alpha)$.

若 $\alpha + \alpha \neq \sigma_7(\alpha + \alpha)$, 则 $\gamma_7 = \frac{\alpha - \sigma_7(\alpha)}{\alpha - \alpha} \notin \mathbf{R}$ 若 $\alpha + \alpha \neq \sigma_{11}(\alpha + \alpha)$, 则 $\gamma_{11} = \frac{\alpha - \sigma_{11}(\alpha)}{\alpha - \alpha} \notin \mathbf{R}$.

下面我们分三种情形来证明.

情形 1　$\gamma_7 \notin \mathbf{R}$, $\gamma_{11} \notin \mathbf{R}$

由引理 3与引理 4知, α 与集合 $B_1 \cup B_2 \cup B_3 \cup B_4$ 中的某一个元素等价, α 又与集合 A 中某一元素等价, 故集合 A 中存在某一幂元整基生成元与集合 $B_1 \cup B_2 \cup B_3 \cup B_4$ 中的某一个元素等价.

注意到若 $\beta \in A$, 则 $-\beta \in A$, 故存在 $\beta \in A$, $\gamma \in B_1 \cup B_2 \cup B_3 \cup B_4$ 及 $\sigma_i \in G$ 使得

$$\gamma = \sigma_i(\beta) + n. \tag{6}$$

注意到 $\sigma_{20+i}(\beta)$ 与 $\sigma_i(\beta)$ 之间的关系, 等式 (6) 中我们只需考虑 $i = 1, 3, 7, 9, 11, 13, 17, 19$的情形.

设 $\beta = k_1\zeta^3 + k_2(-\zeta^4 + \zeta^6 + \zeta^{10}) + k_3(\zeta - \zeta^7 - \zeta^9 + \zeta^{11}) + k_4(-\zeta^8 + \zeta^{12}) + k_5(-\zeta + \zeta^5 - \zeta^7 - \zeta^9 + 2\zeta^{13}) + k_6(\zeta^2 + \zeta^4 - \zeta^8 + \zeta^{14}) + k_7(\zeta - \zeta^7 - \zeta^9 + \zeta^{15}) \in A$.

若 $\gamma \in B_1$, 则可设

$$\gamma = l_1(-\zeta^4 + \zeta^9) + l_2(-\zeta^3 + \zeta^5 + \zeta^7 - \zeta^{11} + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15}), \text{其中 } l_1, l_2, l_3 \in \mathbf{Z}$$

当 $i = 1$时, 由 (6) 式可得关于 $k_1, \cdots, k_7, l_1, l_2, l_3$的齐次线性方程组, 此方程组仅有零解. 所以 $\beta = 0$, 这与 β是幂元整基生成元矛盾, 故 $i \neq 1$.

同理可证 $i \neq 3, 7, 9, 11, 13, 17, 19$, 故 $\gamma \notin B_1$. 同理可证 $\gamma \notin B_2 \cup B_4$.

若 $\gamma \in B_3$, 则可设

$$\gamma = l_1(\zeta^3 - \zeta^5 - \zeta^7 + \zeta^{11}) + l_2(-\zeta^4 + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15}), \text{其中 } l_1, l_2, l_3 \in \mathbf{Z}.$$

当 $i = 1$时, 由 (6) 式可得关于 $k_1, \cdots, k_7, l_1, l_2, l_3$的齐次线性方程组, 此方程组仅有零解. 所以 $\beta = 0$, 这与 β是幂元整基生成元矛盾, 故 $i \neq 1$.

同理可证 $i \neq 3, 7, 9, 11, 17, 19$.

当 $i = 13$时, 由 (6) 式可得关于 $k_1, \cdots, k_7, l_1, l_2, l_3$的齐次线性方程组并解得: $k_2 = k_3 = k_4 = k_5 = k_6$

$= k_7 = 0$, $l_1 = k_1$, $l_2 = 0$, $l_3 = -k_1$, 故 $\beta = k_1\zeta^3$. 由 β为幂元整基生成元, 易知 $k_1 = \pm 1$, 所以 α与 $\pm\zeta^3$等价, 从而 α与 ζ等价.

情形 **2**　$\gamma_7 \notin \mathbf{R}$, $\gamma_{11} \in \mathbf{R}$

由引理 3, α等价于 $B_1 \cup B_2 \cup B_3 \cup B_4$ 中的某一个元素. 不妨设 $\alpha \in B_1 \cup B_2 \cup B_3 \cup B_4$.

(i 若 $\alpha \in B_1$, 可设 $\alpha = l_1(-\zeta^4 + \zeta^9) + l_2(-\zeta^3 + \zeta^5 + \zeta^7 - \zeta^{11} + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15})$, 由 $\gamma_{11} \in \mathbf{R}$ 可得 $\alpha + \alpha - \sigma_{11}(\alpha + \alpha) = 0$, 由此可推得 $\alpha = 0$, 矛盾.

(ii 若 $\alpha \in B_2$, 可设 $\alpha = l_1(\zeta - \zeta^5 + \zeta^{11}) + l_2(-\zeta^5 + \zeta^{15}) + l_3(-2\zeta^6 + \zeta^{10})$, 由 $\gamma_{11} \in \mathbf{R}$可得 $\alpha + \alpha - \sigma_{11}(\alpha + \alpha) = 0$, 由此可推得 $\alpha = l_2(\zeta^{15} - 2\zeta^{11} + \zeta^5 - 2\zeta)$, 但此时有 $\alpha = \sigma_{11}(\alpha)$, $d(\alpha) = 0$, 故 α不是分圆域 $Q(\zeta)$ 的幂元整基的一个生成元, 矛盾.

(iii 若 $\alpha \in B_3$, 可设 $\alpha = l_1(\zeta^3 - \zeta^5 - \zeta^7 + \zeta^{11}) + l_2(-\zeta^4 + \zeta^{14}) + l_3(-\zeta^5 + \zeta^{15})$, 由 $\gamma_{11} \in \mathbf{R}$可得 $\alpha + \alpha - \sigma_{11}(\alpha + \alpha) = 0$, 由此可推得 $\alpha = 0$, 矛盾.

(iv 若 $\alpha \in B_4$, 可设 $\alpha = l_1(\zeta^3 - \zeta^5 - \zeta^7 - \zeta^9 + \zeta^{11}) + l_2\zeta^{14} + l_3(-\zeta^5 + \zeta^{15})$, 由 $\gamma_{11} \in \mathbf{R}$可得 $\alpha + \alpha - \sigma_{11}(\alpha + \alpha) = 0$, 由此可推得 $\alpha = -l_3(\zeta^{15} - \zeta^{11} + \zeta^9 + \zeta^7 - \zeta^3)$, 但 $\alpha = \sigma_{11}(\alpha)$, $d(\alpha) = 0$, 故 α不是分圆域 $Q(\zeta)$ 的幂元整基的一个生成元, 矛盾.

故 $\gamma_7 \notin \mathbf{R}$, $\gamma_{11} \in \mathbf{R}$不成立.

情形 **3**　$\gamma_7 \in \mathbf{R}$, $\gamma_{11} \notin \mathbf{R}$

由引理 4, α等价于集合 A 中的某一个元素. 不妨设 $\alpha \in A$, 设

$$\alpha = k_1\zeta^3 + k_2(-\zeta^4 + \zeta^6 + \zeta^{10}) + k_3(\zeta - \zeta^7 - \zeta^9 + \zeta^{11}) + k_4(-\zeta^8 + \zeta^{12}) +$$
$$k_5(-\zeta + \zeta^5 - \zeta^7 - \zeta^9 + 2\zeta^{13}) + k_6(\zeta^2 + \zeta^4 - \zeta^8 + \zeta^{14}) + k_7(\zeta - \zeta^7 - \zeta^9 + \zeta^{15}),$$

由 $\gamma_7 \in \mathbf{R}$可得 $\alpha + \alpha - \sigma_7(\alpha + \alpha) = 0$, 由此可得 $\alpha = k_5(-3\zeta^{15} + 2\zeta^{13} + 2\zeta^{11} + \zeta^5 + 2\zeta^3 - 2\zeta)$. 但由于 $d(\alpha) = 2^{392} \cdot 5^{12} \cdot 11^8 \cdot 101^4 \cdot 401 \cdot k_5^{240}$, $d(\zeta) = 2^{32} \cdot 5^{12}$, $d(\alpha) \neq d(\zeta)$. 矛盾.

综上, 我们证明了定理.

[参考文献]

[1] Bremner A. On power bases in cyclotomic number fields[J]. J Number Theory, 1988, 28: 288-298.

[2] Robertson L. Power bases for cyclotomic integer rings[J]. J Number Theory, 1998, 69: 98-118.

[3] Robertson L. Power bases for 2-power cyclotomic fields[J]. J Number Theory, 2001, 88: 196-209.

[4] 冯克勤. 代数数论[M]. 北京: 科学出版社, 2001.

[5] Washington L J. Introduction to cyclotomic Fields[J]. 2nd ed. New York: Springer-Verlag, 1997.

[责任编辑: 丁　蓉]