G_{81}(Q) Is not a Subgroup of K_2(Q)

Wu Jiandong, Xia Jianguo

(School of Mathematics and Computer Science, Nanjing Normal University, 210097, Nanjing, China)

Abstract: Let K_2 be the Milnor functor and let $\Phi_n(x)\in\mathbf{Q}[x]$ be the n-th cyclotomic polynomial. Denote by $G_n(\mathbf{Q})$ a subset consisting of elements of the form $\{a,\Phi_n(a)\}$, where $a\in\mathbf{Q}^*$. J. Browkin proved that $G_n(\mathbf{Q})$ is a subgroup of $K_2(\mathbf{Q})$ if $n=1,2,3,4$ or 6 and conjectured that $G_n(\mathbf{Q})$ is not a group for any other values of n. In the paper we conform the conjecture for $n=81$.

Key words: K_2 group, Diophantine equation, functor

CLC number 11R11, **Document code** A, **Article ID** 1001-4616(2005)02-0024-04

G_{81}(Q)不是 K_2(Q)的子群

吴建东,夏建国

(南京师范大学数学与计算机科学学院,210097,江苏,南京)

[摘要] 设 K_2 是 Milnor 函子,$\Phi_n(x)\in\mathbf{Q}[x]$ 是分圆多项式. $G_n(\mathbf{Q})$ 表示形如 $\{a,\Phi_n(a)\}$ 的元素组成的集合,其中 $a\in\mathbf{Q}^*$. J. Browkin 证明了 $G_n(\mathbf{Q})$ 在 $n=1,2,3,4$ 或 6 时是 $K_2\mathbf{Q}$ 的子群,并且猜测对任何其它的 n,$G_n(\mathbf{Q})$ 都不是群. 本文证明了 J. Browkin 猜测在 $n=81$ 时是对的.

[关键词] K_2 群,丢番图方程,函子

J. Tate proved in [3] that if a global field F contains a primitive n-th root of unity ζ_n, then every element of order n in K_2F is of the form $\{a,\zeta_n\}$ for some a in F^*. Let $\Phi_n(x)$ be the n-th cyclotomic polynomial and $G_n(F)=\{\{a,\Phi_n(a)\}\in K_2F\mid a,\Phi_n(a)\in F^*\}$, where F is any field. J. Browkin proved in [1]:

(1) For every global field F and $n=1,2,3,4$ or 6 if $\zeta_n\in F$, then every element $\{a,\zeta_n\}$ in K_2F can be written in the form $\{b,\Phi_n(b)\}$, where $b\in F^*$ satisfying $\Phi_n(b)\neq 0$.

(2) For every field $F\neq F_2$ and $n=1,2,3,4$ or 6, $G_n(F)$ is a subgroup of K_2F.

Browkin conjectured that for any fields, (1) and (2) do not hold for any other values of n.

Qin proved in [2] that neither $G_5(\mathbf{Q})$ nor $G_7(\mathbf{Q})$ is a subgroup of $K_2(\mathbf{Q})$. Xu proved in [5] that neither $G_9(\mathbf{Q})$ nor $G_{27}(\mathbf{Q})$ is a subgroup of $K_2(\mathbf{Q})$.

In this paper we will prove $G_{81}(\mathbf{Q})$ is not a subgroup of $K_2(\mathbf{Q})$.

1 Preliminaries

Lemma 1.1 Let $n\in\mathbf{Z}$, p be a prime and $\Phi_{p^n}(x,y)=y^{p^{n-1}(p-1)}\Phi_{p^n}\left(\frac{x}{y}\right)$. Suppose $x,y\in\mathbf{Z}$, $(x,y)=1$.

(1) If $x\not\equiv y\pmod p$, then $p\nmid\Phi_{p^n}(x,y)$;

Received date: 2004-08-28.

Foundation item: Supported by the National Natural Science Foundation of China (10471118) and the Jiangsu Natural Science Foundation (BK2002023).

Biography: Wu Jiandong, born in 1978, Master, Majored in Algebraic Number Theory. E-mail: nj_wjd@sohu.com

(2) If $x \equiv y \pmod p$, then $p \parallel \Phi_{p^n}(x, y)$.

Proof See that in [5]

Lemma 1.2 The group of units of $\mathbf{Q}(\zeta_9)$ can be generated by

$$-1,\ 1+\zeta_9,\ 1+\zeta_9^2,\ \zeta_9.$$

Proof The group of units of $Q(\zeta_9)$ can be generated by the cyclotomic units since the class number of $Q(\zeta_9)$ is 1. Hence, the proof can be completed by Lemma 8.1 in [4].

Lemma 1.3 Let $n \geqslant 1$ and p be an odd prime. Suppose that q is a prime with $q = mp^n + 1$, then $\Phi_{p^n}(x) \equiv 0 \pmod q$ has t distinct roots, say, $\alpha_1, \cdots, \alpha_t$, where $t = \Phi(p^n)$, and we have the following isomorphism:

$$(\mathbf{Z}/q\mathbf{Z})[x]/(\Phi_{p^n}(x)) \overset{\alpha}{\cong} \bigoplus_{i=1}^{t} \mathbf{Z}/q\mathbf{Z},$$

where α is defined as follows. For any $f(x) \in (\mathbf{Z}/q\mathbf{Z})[x]/(\Phi_{p^n}(x))$,

$$\alpha(f(x)) = (f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_t)).$$

Proof It is just a consequence of the Chinese Remainder Theorem.

2 Main Result

Theorem 2.1 $G_{81}(\mathbf{Q})$ is not a subgroup of $K_2(\mathbf{Q})$

Proof We have $\Phi_{81}(4, 1) = 3 \cdot 163 \cdot 2593 \cdot 71119 \cdot 135433 \cdot 97685839 \cdot 272010961$, Let

$$\beta = \{4, \Phi_{81}(4)\}^3,$$

then $\beta^{27} = 1$. If $G_{81}(\mathbf{Q})$ is a subgroup of $K_2(\mathbf{Q})$, then $\beta \in G_{81}(\mathbf{Q})$, so there exist $a, b \in \mathbf{Z}$, $(a, b) = 1$ such that

$$\beta = \left\{\frac{a}{b}, \Phi_{81}\left(\frac{a}{b}\right)\right\}. \tag{1}$$

We show that this is impossible.

Let $p = 163$. Since $3 \nmid v_p(\Phi_{81}(4)) = 1$, it is easy to see

$$\tau_p\{4, \Phi_{81}(4)\}^{27} \equiv 4^{27} \equiv 104 \not\equiv 1 \pmod p. \tag{2}$$

Let $q \neq 3$ be a prime with $r = v_q(\Phi_{81}(a, b)) > 0$. We claim that if $3 \nmid r$ then

$$\tau_q\left\{\frac{a}{b}, \Phi_{81}\left(\frac{a}{b}\right)\right\}^{27} \not\equiv 1 \pmod q.$$

Otherwise, from $(a, b) = 1$ and $q \mid \Phi_{81}(a, b)$, it follows that $q \nmid ab$. Consequently $v_q\left(\frac{a}{b}\right) = 0$. So we obtain

$$\tau_q\left\{\frac{a}{b}, \Phi_{81}\left(\frac{a}{b}\right)\right\}^{27} \equiv \left(\frac{a}{b}\right)^{27r} \equiv 1 \pmod q$$

On the other hand, since $r = v_q(\Phi_{81}(a,b)) > 0$, so $\left(\frac{a}{b}\right)^{81} - 1 = \Phi_{81}\left(\frac{a}{b}\right)\left(\left(\frac{a}{b}\right)^{27} - 1\right) \equiv 0 \pmod p$, and $(27r, 81) = 27$ since $3 \nmid r$. So we have $\left(\frac{a}{b}\right)^{27} \equiv 1 \pmod p$, or equivalently $a^{27} \equiv b^{27} \pmod q$.

Since

$$v_q(\Phi_{81}(a,b)) > 0, \quad \Phi_{81}(a,b) = a^{54} + a^{27}b^{27} + b^{54} \equiv 3a^{54} \equiv 0 \pmod q,$$

we obtain $a \equiv 0 \pmod q$. Consequently $b \equiv 0 \pmod q$. This contradicts to $(a,b) = 1$.

Now,

$$\tau_q\left\{\frac{a}{b}, \Phi_{81}\left(\frac{a}{b}\right)\right\}^{27} = \tau_q(\{4, \Phi_{81}(4)\}^3)^{27} \equiv 1 \pmod q.$$

From the above claim, for any prime $q \neq 3$ with $r = v_q(\Phi_{81}(a,b)) > 0$ we must have $3 \mid r$.

On the other hand, if $v_p\left(\frac{a}{b}\right) \neq 0$, it is easy to check that $\tau_p\left\{\frac{a}{b}, \Phi_n\left(\frac{a}{b}\right)\right\} \equiv 1 \pmod p$, so

$$\tau_p\{4, \Phi_{81}(4)\}^{27} \equiv \tau_p\left\{\frac{a}{b}, \Phi_{81}\left(\frac{a}{b}\right)\right\}^9 \equiv 1 \pmod p,$$

this contradicts to (2), so $v_p\left(\frac{a}{b}\right)=0$. Further, $v_p\left(\Phi_{81}\left(\frac{a}{b}\right)\right)>0$. If that is not the case,

$$\tau_p\{4,\Phi_{81}(4)\}^3=\tau_p\left\{\frac{a}{b},\Phi_{81}\left(\frac{a}{b}\right)\right\}=(-1)^{v_p\left(\frac{a}{b}\right)v_p\left(\Phi_{81}\left(\frac{a}{b}\right)\right)}\frac{\left(\frac{a}{b}\right)^{v_p\left(\Phi_{81}\left(\frac{a}{b}\right)\right)}}{\left(\Phi_{81}\left(\frac{a}{b}\right)\right)^{v_p\left(\frac{a}{b}\right)}}\equiv 1 \pmod p,$$

It also contradicts to (2) again. In a word, from the above argument and according to Lemma 1.1, if a,b satisfy (1), then they should satisfy at least one of the following Diophantine equations:

$$\Phi_{81}(a,b)=163^3c^3, \tag{3}$$

$$\Phi_{81}(a,b)=3\cdot 163^3c^3, \tag{4}$$

or equivalently

$$\Phi_3(a^{27},b^{27})=163^3c^3, \tag{5}$$

$$\Phi_9(a^9,b^9)=3\cdot 163^3c^3, \tag{6}$$

where $a,b,c\in\mathbf{Z}$ with $(a,b)=1$.

One can check that

$$S_1=\{z\in\mathbf{Z}/163\mathbf{Z}\mid\Phi_3(z)=0\}=\{58,-59\}$$

and

$S_2=(\mathbf{Z}/163\mathbf{Z})^3=\{0,\pm1,\pm5,\pm6,\pm8,\pm13,\pm17,\pm21,\pm22,\pm23,\pm25,\pm27,\pm28,\pm30,\pm31,\pm36,\pm37,\pm38,\pm40,\pm48,\pm53,\pm58,\pm59,\pm61,\pm64,\pm65,\pm77,\pm78\}$.

Factoring the left side of the equation (5) in $\mathbf{Z}[\zeta_3]$, noting that the units of $\mathbf{Z}[\zeta_3]$ is $\{\pm\zeta_3^j, j=0,1,2\}$. One may get

$$a^{27}-b^{27}\zeta_3=\zeta_3^j\alpha^3, j=0,1,2$$

where $\alpha\in\mathbf{Z}[\zeta_3]$.

So, if there exist a,b satisfy the equation (5), we have the following equation over $(\mathbf{Z}/163\mathbf{Z})[x]/\Phi_3(x)$

$$a^{27}-b^{27}x=x^j\alpha(x)^3. \tag{7}$$

If $b^9\not\equiv 0 \pmod{163}$, from (7), (5) and Lemma 1.3, then

(i) when $j=0$, we have

$$\alpha_1^3=z-58, \alpha_2^3=z+59, z\in S_1; \tag{8}$$

(ii) when $j=1$, we have

$$\alpha_1^3=104z-1, \alpha_2^3=58z-1, z\in S_1; \tag{9}$$

(iii) when $j=2$, we have

$$\alpha_1^3=58z+59, \alpha_2^3=59z+58, z\in S_1. \tag{10}$$

But, if z takes the values of S_1, none of the equations (8), (9) and (10) can hold; so $b^9\equiv 0 \pmod{163}$, that is $163\mid b$. From (5), we have $163\mid a$, which contradicts $(a,b)=1$. Hence the equation (5) has no integer solutions with $(a,b)=1$.

Now, consider the equation (6). We can check

$$S_3=\{z\in\mathbf{Z}/163\mathbf{Z}\mid\Phi_9(z)=0\}=\{38,40,53,85,133,140\}.$$

In $\mathbf{Z}[\zeta_9]$, $3=(1-\zeta_9^3)^2(1+\zeta_9^3)$. From the equation (4), we have $(a^{27}-b^{27})\Phi_{81}(a,b)=a^{81}-b^{81}\equiv a-b\equiv 0 \pmod 3$. Therefore, $(1-\zeta_9)^2\mid(a-b)$. Since $a^9-b^9\zeta_9=(a^9-b^9)+b^9(1-\zeta_9)$, we get $(1-\zeta_9)\parallel(a^9-b^9\zeta_9)$. Now we factor the left side of equation (6) in $\mathbf{Z}[\zeta_9]$, we obtain

$$a^9-b^9\zeta_9=(1-\zeta_9)(1+\zeta_9)^r(1+\zeta_9^2)^s\zeta_9^t\alpha^3, \tag{11}$$

where $\alpha\in\mathbf{Z}[\zeta_9]$ and $\leqslant r,s,t\leqslant 2$. In $(\mathbf{Z}/3\mathbf{Z})[x]/\Phi_9(x)$, (11) can be changed into

$$\rho(a^9-b^9x)=(1-x)(1+x)^r(1+x^2)^sx^t, \tag{12}$$

where $0 \leqslant r, s, t \leqslant 2$ and $\rho \in \mathbf{Z}/3\mathbf{Z}$. It can be checked that (12) holds possibly only when $r = s = t = 0$. When $r = s = t = 0$, (11) can be changed into

$$(a^9 - b^9 x)(1 - x)^2 = \alpha^3 \tag{13}$$

over $(\mathbf{Z}/163\mathbf{Z})[x]/\Phi_9(x)$.

If $b^3 \not\equiv 0 \pmod{163}$, according to lemma 1.3 and (13), we have

$$\begin{cases} \alpha_1^3 = 65z + 138 & \pmod{163} \\ \alpha_2^3 = 54z + 122 & \pmod{163} \\ \alpha_3^3 = 96z + 128 & \pmod{163} \\ \alpha_4^3 = 47z + 80 & \pmod{163} \\ \alpha_5^3 = 146z + 142 & \pmod{163} \\ \alpha_6^3 = 87z + 45 & \pmod{163} \end{cases} \tag{14}$$

where $\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6 \in \mathbf{Z}/163\mathbf{Z}$ and $z \in S_3$.

But, if z takes the values of S_3, (14) cann't hold, so $b^3 \equiv 0 \pmod{163}$, that is $163 \mid b$, consequently $163 \mid a$. That is a contradiction as $(a, b) = 1$. Hence the equation (6) has no integer solutions with $(a, b) = 1$. Therefore, $G_{81}(\mathbf{Q})$ is not a subgroup of $K_2(\mathbf{Q})$.

[References]

[1] Browkin J. Elements of small order in K_2F, Algebraic K-Theory[M]. Berlin-Heidelerg, New York: Springer-Verlag, 1982. 1—6.

[2] Qin H R. The subgroup of finite order in $K_2(\mathbf{Q})$, Algebraic K-Theory and Its Application[M]. Singapore-New Jersey-London-Hong Kong: World Scintific, 1999. 600—607.

[3] Tate J. Relations between K_2 and Galois cohomology[J]. Invent Math, 1976, 36: 257—274.

[4] Washington L L. Introduction to cyclotomic fields[M]. GTM 83, New York, Berlin-Heidelerg: Springer-Verlag, 1982.

[5] Xu K J. On Browkin conjecture[D]. Ph D Thesis, Nanjing University, 2001.

[责任编辑: 陆炳新]