Acta Mathematica Sinica, English Series
May, 2007, Vol. 23, No. 5, pp. 819–826
Published online: Sep. 21, 2006
DOI: 10.1007/s10114-005-0852-6
Http://www.ActaMath.com

Acta Mathematica Sinica, English Series

Some Elements of Finite Order in $K_2\mathbb{Q}$

Xiao Yun CHENG
Department of Mathematics, Nanjing University, Nanjing 210093, *P. R. China*
E-mail: xychengnt@yahoo.com.cn

Jian Guo XIA
Department of Mathematics, Nanjing Normal University, Nanjing 210097, *P. R. China*
E-mail: jgxia@njnu.edu.cn

Hou Rong QIN
Department of Mathematics, Nanjing University, Nanjing 210093, *P. R. China*
E-mail: hrqin@nju.edu.cn

Abstract Let K_2 be the Milnor functor and let $\Phi_n(x) \in \mathbb{Q}[x]$ be the n-th cyclotomic polynomial. Let $G_n(\mathbb{Q})$ denote a subset consisting of elements of the form $\{a, \Phi_n(a)\}$, where $a \in \mathbb{Q}^*$ and $\{,\}$ denotes the Steinberg symbol in $K_2\mathbb{Q}$. J. Browkin proved that $G_n(\mathbb{Q})$ is a subgroup of $K_2\mathbb{Q}$ if $n = 1, 2, 3, 4$ or 6 and conjectured that $G_n(\mathbb{Q})$ is not a group for any other values of n. This conjecture was confirmed for $n = 2^r3^s$ or $n = p^r$, where $p \geq 5$ is a prime number such that $h(\mathbb{Q}(\zeta_p))$ is not divisible by p. In this paper we confirm the conjecture for some n, where n is not of the above forms, more precisely, for $n = 15, 21, 33, 35, 60$ or 105.

Keywords $K_2\mathbb{Q}$, cyclotomic polynomial, Diophantine equation
MR(2000) Subject Classification 19C20

1 Introduction

Let $\mathbb{Q}$ be the field of rational numbers. Let $v_p(\cdot)$ denote the p-adic valuation on $\mathbb{Q}$. Denote by K_2 the Milnor functor and by $\Phi_n(x)$ the n-th cyclotomic polynomial. The following isomorphism ([1]), which is due to Tate, is well known: $K_2\mathbb{Q} \overset{\tau}{\cong} A_2 \oplus A_3 \oplus A_5 \oplus \cdots \oplus A_p \oplus \cdots$, where $A_2 = \{\pm 1\}$, and for any odd prime p, $A_p = (\mathbb{Z}/p\mathbb{Z})^*$. The isomorphism $\tau = (\tau_p)$ is defined as follows. For any odd prime p and any $x, y \in \mathbb{Q}^*$,

$$\tau_p\{x, y\} = (-1)^{v_p(x)v_p(y)} x^{v_p(y)} y^{-v_p(x)} \pmod{p}.$$

And τ_2 is defined as follows: If $x = (-1)^i 2^j 5^k u, y = (-1)^I 2^J 5^K w$, where $u, w \equiv 1 \pmod 8$, then $\tau_2\{x, y\} = (-1)^{iI+jK+kJ}$. Let $G_n(\mathbb{Q})$ denote a subset of $K_2\mathbb{Q}$ consisting of the Steinberg symbols $\{a, \Phi_n(a)\}$, where $a, \Phi_n(a) \in \mathbb{Q}^*$. For an abelian group H, and $n \in \mathbb{N}$, let $H_n = \{x \in H \mid x^n = 1\}$. Browkin ([2]) proved that $G_n(\mathbb{Q}) \subseteq (K_2\mathbb{Q})_n$ and $(K_2\mathbb{Q})_3 = G_3(\mathbb{Q})$. Moreover, he proved that $G_n(\mathbb{Q})$ is a group if $n = 1, 2, 3, 4$ or 6 and conjectured that $G_n(\mathbb{Q})$ is not a group otherwise. The last assertion was proved for an arbitrary field having at least three elements, and the conjecture was formulated for these fields. Browkin's result on $K_2\mathbb{Q}$ was extended in [3] and [4]. Browkin's conjecture was confirmed in many cases: $n = 5$ and 7 ([5]); $n = 2^r3^s$ ([6]); $n = p^r$ with the class number $h(\mathbb{Q}(\zeta_p))$ not divisible by p ([6–8]). For $n = 5$ see also [9].

In this paper, we confirm Browkin's conjecture for $n = 15, 21, 33, 35, 60$ and 105.

Received November 19, 2004, Accepted March 8, 2005
This work is supported by SRFDP, the 973 Grant, the National Natural Science Foundation of China 10471118 and the Jiangsu Natural Science Foundation Bk2002023

2 Preliminaries

In the following we shall need two lemmas on cyclotomic polynomial. From now on, we denote $\Phi_n(x,y)=y^{\phi(n)}\Phi_n(\frac{x}{y})$, where $\phi(\cdot)$ is the Euler function.

Lemma 2.1 *Let p be an odd prime. Suppose $x,y\in\mathbb{Z}$, with $(x,y)=1$. (1) If $x\not\equiv y \pmod p$, then $p\nmid\Phi_p(x,y)$; (2) If $x\equiv y \pmod p$, then $p\parallel\Phi_p(x,y)$; (3) $2\nmid\Phi_p(x,y)$.*

Proof See (1), (2) in [5]. (3) is obvious.

Lemma 2.2 *Let q be a prime with $q\equiv 1 \pmod n$, where $n\in\mathbb{N}$ and n has at least two distinct prime factors. If for some $a\in\mathbb{Z}$, $q^2\mid\Phi_n(a)$, then $q\parallel\Phi_n(a+q)$.*

Proof Let $n=p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}$ be the prime factorization. Since $q\equiv 1 \pmod n$, q splits completely in $\mathbb{Q}(\zeta_n)$. Write $\Phi_n(a)=\prod_{i=1,(i,n)=1}^{n}(a-\zeta_n^i)=\prod_{i=1,(i,p_j)=1}^{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}(a-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$. If $i\neq j$, $(a-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})-(a-\zeta^j_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})=\zeta^j_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}(1-\zeta^{i-j}_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$. Since n has at least two distinct prime factors, there are no common factors for ideals $(a-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$ and $(a-\zeta^j_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$ except $(1-\zeta_{p_1^{n_1}}),(1-\zeta_{p_2^{n_2}}),\ldots,$ and $(1-\zeta_{p_s^{n_s}})$. Since $q^2\mid\Phi_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}(a)$, there exists a prime factor $\Im$ of q such that $\Im^2\mid(a-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$. We also have $\Im\mid(a+q-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$. If $\Im^2\mid(a+q-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}})$, then $\Im^2\mid q$, which is impossible since q is unramified in $\mathbb{Q}(\zeta_n)$. So $\Im\parallel(a+q-\zeta^i_{p_1^{n_1}p_2^{n_2}\cdots p_sn_s})$ and then $q\parallel\Phi_n(a+q)$. This completes the proof.

We also need a lemma on the group of units in some special cyclotomic fields.

Lemma 2.3 *In $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{11})$, the groups of units can be generated by $-1,1+\zeta_5^3,\zeta_5$, $-1,1+\zeta_7,1+\zeta_7^2,\zeta_7$, and $-1,1+\zeta_{11},1+\zeta_{11}^2,1+\zeta_{11}^3,1+\zeta_{11}^4,\zeta_{11}$, respectively.*

Proof See [5]. Since the class numbers of $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{11})$ are 1, the group of units can be generated by the cyclotomic units. By Lemma 8.1 [10], we see that the results follow.

Lemma 2.4 ([5]) *Let $n\geq 1$ and p be an odd prime. Suppose that q is a prime with $q=mp+1$. Then $\Phi_p(x)\equiv 0 \pmod q$ has $p-1$ distinct roots, say, $\alpha_1,\alpha_2,\ldots,\alpha_{p-1} \pmod q$, and we have the following isomorphism: $\mathbb{Z}/q\mathbb{Z}[x]/(\Phi_p(x))\overset{\alpha}{\cong}\bigoplus_{i=1}^{p-1}\mathbb{Z}/q\mathbb{Z}$, where α is defined as follows: For any $f(x)\in(\mathbb{Z}/q\mathbb{Z})[x]/(\Phi_p(x))$, $\alpha(f(x))=(f(\alpha_1),f(\alpha_2),\ldots,f(\alpha_{p-1}))$.*

Lemma 2.5 *Let a,b be two integers and p be a prime. If $a\not\equiv b \pmod p$, then $(a-b\zeta_p^i,a-b\zeta_p^j)=1(i\neq j)$. If $a\equiv b \pmod p$, then $1-\zeta_p^i\mid a-b\zeta_p^i$ and $(\frac{a-b\zeta_p^i}{1-\zeta_p^i},\frac{a-b\zeta_p^j}{1-\zeta_p^j})=1(i\neq j)$.*

Proof If $a\not\equiv b \pmod p$, then for any prime ideal with $\wp\mid(a-\zeta_p^ib)$ and $\wp\mid(a-\zeta_p^jb)$, where $i\neq j$, we have $\wp\mid(\zeta_p^ib-\zeta_p^jb)=(unit)(1-\zeta_p)b$. Therefore $\wp=(1-\zeta_p)$ or $\wp\mid b$. Similarly, $\wp\mid\zeta_p^j(a-\zeta_p^ib)-\zeta_p^i(a-\zeta_p^jb)=(unit)(1-\zeta_p)a$. So $\wp=(1-\zeta_p)$ or $\wp\mid a$. If $\wp\neq(1-\zeta_p)$ then $\wp\mid a$ and $\wp\mid b$, which is impossible since $(a,b)=1$. Therefore $\wp=(1-\zeta_p)$. But $a-\zeta_p^ib=(a-b)+b(1-\zeta_p^i)\equiv 0 \pmod\wp$. This implies that $a\equiv b \pmod\wp$, so we have $a\equiv b \pmod p$, since $a-b\in\mathbb{Z}$, a contradiction. If $a\equiv b \pmod p$, it's easy to see that $1-\zeta_p^i\mid a-b\zeta_p^i$ and $(\frac{a-b\zeta_p^i}{1-\zeta_p^i},\frac{a-b\zeta_p^j}{1-\zeta_p^j})=1$ since $a-\zeta_p^ib=(a-b)+b(1-\zeta_p^i)$.

3 Main Theorems

In this section, we will prove two theorems. In the first of them we determine $v_p(\Phi_n(a,b))$, where $p\mid n$, and in the second we prove that, if Browkin's conjecture is true, then the Diophantine equation $\Phi_n(a,b)=\varepsilon_n z^pq^p$, where p is the greatest prime divisor of n, $q\equiv 1(\mathrm{mod}\,n)$ and $\varepsilon_n=p$ or 1, has a solution $(a,b,z)\in\mathbb{Z}^3$ with z not divisible by any prime divisor of n.

Theorem 3.1 *For a natural number n not being a prime power, let p be the greatest prime factor of n. Then, for $a,b\in\mathbb{Z}$, $(a,b)=1$, we have*

(1) $v_r(\Phi_n(a,b)) = 0$ *if* $r \neq p$ *is a prime divisor of* n;

(2) $v_p(\Phi_n(a,b)) = 1$ *only if* $p-1$ *is divisible by every prime divisor different from* p *of* n; *and* $v_p(\Phi_n(a,b)) = 0$ *otherwise.*

Proof Let $n = p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}$ be the prime factorization, where $p_1 < p_2 < \cdots < p_s = p$. Since $\Phi_{p_1^{n_1}p_2^{n_2}\cdots p_s^{n_s}}(x) = \Phi_{p_1p_2\cdots p_s}(x^{p_1^{n_1-1}p_2^{n_2-1}\cdots p_s^{n_s-1}})$, we need to consider only the prime factors of $\Phi_n(a,b)$, where $n = p_1p_2\cdots p_s$. We have $\Phi_n(x) = \prod_{d|n}(x^d-1)^{\mu(\frac{n}{d})}$, where $\mu(\cdot)$ is the Möbius function. We see that, if s is odd, then

$$\Phi_{p_1p_2\cdots p_s}(x) = \frac{(x^{p_1p_2p_3\cdots p_s}-1)\cdot\prod_{1\le i<j\le s}(x^{\frac{n}{p_ip_j}}-1)\cdots\prod_{i=1}^{s}(x^{p_i}-1)}{\prod_{i=1}^{s}(x^{\frac{n}{p_i}}-1)\cdot\prod_{1\le i<j<k\le s}(x^{\frac{n}{p_ip_jp_k}}-1)\cdots(x-1)};$$

if s is even, then

$$\Phi_{p_1p_2\cdots p_s}(x) = \frac{(x^{p_1p_2p_3\cdots p_s}-1)\cdot\prod_{1\le i<j\le s}(x^{\frac{n}{p_ip_j}}-1)\cdots(x-1)}{\prod_{i=1}^{s}(x^{\frac{n}{p_i}}-1)\cdot\prod_{1\le i<j<k\le s}(x^{\frac{n}{p_ip_jp_k}}-1)\cdots\prod_{i=1}^{s}(x^{p_i}-1)}.$$

So

$$\Phi_{p_1p_2\cdots p_s}(a,b) = \frac{\Phi_{p_i}(a^{p_1p_2\cdots p_{i-1}p_{i+1}\cdots p_s}, b^{p_1p_2\cdots p_{i-1}p_{i+1}\cdots p_s})\prod_{j,k}\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_jp_k}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_jp_k}})\cdots\Phi_{p_i}(a,b)}{\prod_j\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_j}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_j}})\prod_{j,k,l}\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_jp_kp_l}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_jp_kp_l}})\cdots\prod_j\Phi_{p_i}(a^{p_j}, b^{p_j})}$$

when s is odd, and

$$\Phi_{p_1p_2\cdots p_s}(a,b) = \frac{\Phi_{p_i}(a^{p_1p_2\cdots p_{i-1}p_{i+1}\cdots p_s}, b^{p_1p_2\cdots p_{i-1}p_{i+1}\cdots p_s})\prod_{j,k}\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_jp_k}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_jp_k}})\cdots\prod_j\Phi_{p_i}(a^{p_j}, b^{p_j})}{\prod_j\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_j}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_j}})\prod_{j,k,l}\Phi_{p_i}(a^{\frac{p_1p_2\cdots p_s}{p_ip_jp_kp_l}}, b^{\frac{p_1p_2\cdots p_s}{p_ip_jp_kp_l}})\cdots\Phi_{p_i}(a,b)}$$

when s is even.

We are going to compute $v_r(\Phi_n(a,b))$ for any prime divisor $r \mid n$. First we consider $r \neq p$, i.e., $r = p_i$ $(1 \le i \le s-1)$.

If $p_1 = 2$, then $2 \nmid \Phi_{p_1p_2\cdots p_s}(a,b)$. We need to consider only $p_i \nmid a$ and $p_i \nmid b$ because, if $p_i \mid a$ or $p_i \mid b$, then $a^n \not\equiv b^n \pmod{p_i}, \forall n \in \mathbb{N}$, since $(a,b) = 1$. By Lemma 2.1, we have $v_{p_i}(\Phi_{p_1p_2\cdots p_s}(a,b)) = 0$.

Case 1 $a \equiv b \pmod{p_i}$: It follows easily by Lemma 2.1.

Case 2 $a \not\equiv b \pmod{p_i}$, but $a^{p_j} \equiv b^{p_j} \pmod{p_i}(j \neq i)$: We need to consider only $j < i$ because $(p_j, p_i - 1) = 1$ when $j > i, p_j > p_i$. We can also consider only one prime p_j since if $a^{p_j} \equiv b^{p_j} \pmod{p_i}$ and $a^{p_k} \equiv b^{p_k} \pmod{p_i}$, for $j \neq k$, it follows that $a \equiv b \pmod{p_i}$, a contradiction. We have $(a^{p_j})^* \equiv (b^{p_j})^* \pmod{p_i}$, where $*$ denotes any positive integer. Since the form like $\Phi_{p_i}(a^{p_j*}, b^{p_j*})$ where $* \mid p_1p_2\cdots p_s$ but $* \nmid p_ip_j$ appears the same times $(C_{s-2}^0 + C_{s-2}^2 + \cdots = C_{s-2}^1 + C_{s-2}^3 + \cdots = 2^{s-3}$ times) on the numerator and the denominator of $\Phi_n(a,b)$, the result follows from Lemma 2.1.

Case 3 $a \not\equiv b \pmod{p_i}$ and $a^{p_j} \not\equiv b^{p_j} \pmod{p_i}$, $1 \le j \le s, j \neq i$, but $a^{p_jp_k} \equiv b^{p_jp_k} \pmod{p_i}$: We also need to consider only those $\Phi_{p_i}(a^*, b^*)$, where $p_jp_k \mid *$ because if $a^{p_jp_k} \equiv b^{p_jp_k} \pmod{p_i}$ and $a^{p_jp_l} \equiv b^{p_jp_l} \pmod{p_i}$, then $a^{p_j} \equiv b^{p_j} \pmod{p_i}$, which is just Case 2. Similarly, we may check that the form like $\Phi_{p_i}(a^{p_jp_k*}, b^{p_jp_k*})$, where $* \mid p_1p_2\cdots p_s$ but $* \nmid p_ip_jp_k$ appears the same times $(C_{s-3}^0 + C_{s-3}^2 + \cdots = C_{s-3}^1 + C_{s-3}^3 + \cdots = 2^{s-4}$ times) in the numerator and the denominator of $\Phi_n(a,b)$. By Lemma 2.1, we get $v_{p_i}(\Phi_{p_1p_2\cdots p_s}(a,b)) = 0$.

Continuing this procedure, we always have $v_{p_i}(\Phi_{p_1p_2\cdots p_s}(a,b)) = 0$.

Case $(s-1)$ $a \not\equiv b \pmod{p_i}$, $a^{p_j} \not\equiv b^{p_j} \pmod{p_i}(j \neq i), \ldots, a^{p_jp_k} \not\equiv b^{p_jp_k} \pmod{p_i}, \ldots,$ $a^{\frac{n}{p_ip_k}} \not\equiv b^{\frac{n}{p_ip_k}} \pmod{p_i}(1 \le j \neq k \le s)$ but $a^{\frac{n}{p_i}} \equiv b^{\frac{n}{p_i}} \pmod{p_i}$: Since $p_i < p_s, (p_s, p_i - 1) = 1$. Then $a^{\frac{n}{p_ip_s}} \equiv b^{\frac{n}{p_ip_s}} \pmod{p_i}$, it's just case $(s-2)$. The result follows from Lemma 2.1.

Finally we consider $v_p(\Phi_{p_1p_2\cdots p_s}(a,b))$. The same discussion goes on as in the foregoing part, except case $(s-1)$. If $a \not\equiv b \pmod{p_s}$, $a^{p_j} \not\equiv b^{p_j} \pmod{p_s}(j \neq s)$, $a^{p_jp_k} \not\equiv b^{p_jp_k} \pmod{p_s}(j,k \neq s), \ldots, a^{\frac{n}{p_jp_k}} \not\equiv b^{\frac{n}{p_jp_k}} \pmod{p_s}$ and $a^{p_1p_2\cdots p_{s-1}} \not\equiv b^{p_1p_2\cdots p_{s-1}} \pmod{p_s}$, by Lemma 2.1, then $v_{p_s}(\Phi_{p_1p_2\cdots p_s}(a,b)) = 0$. On the other hand, we see that $v_{p_s}(\Phi_{p_1p_2\cdots p_s}(a,b)) = 1$ happens only if $p_s \equiv 1 \pmod{p_1p_2\cdots p_{s-1}}$ together with $a^{p_1p_2\cdots p_{s-1}} \equiv b^{p_1p_2\cdots p_{s-1}} \pmod{p_s}$. Our theorem is proved.

Theorem 3.2 *Let p be the greatest prime divisor of n. Given $q \equiv 1 \pmod{n}$, if $G_n(\mathbb{Q})$ is a subgroup of $K_2\mathbb{Q}$,* then we have:

(1) *The Diophantine equation $\Phi_n(a,b) = \varepsilon_n z^p q^p$ has a solution $(a,b,z) \in \mathbb{Z}^3$ with $(a,b) = 1$ and z is not divisible by any prime divisor r of n,* where $\varepsilon_n = p$ only if $p-1$ is divisible by every prime divisor r, $r \neq p$ of n and $\varepsilon_n = 1$ otherwise,

(2) *For any prime divisor $r \mid n$, $r \neq p$, the Diophantine equation $\Phi_n(a,b) = \varepsilon_n z^r q^r$ has solutions $(a,b,z) \in \mathbb{Z}^3$ with $(a,b) = 1$ and z is not divisible by every prime divisor r of n, where ε_n is the same as above.*

Proof Since $q \equiv 1 \pmod{n}$, by Proposition 2.10 [10], there exists $a_0 \in \mathbb{Z}$ such that $q \mid \Phi_n(a_0)$. By Lemma 2.2, we may suppose $q \parallel \Phi_n(a_0)$. Let $\beta = \{a_0, \Phi_n(a_0)\}^p$. If $G_n(\mathbb{Q})$ is a subgroup of $K_2\mathbb{Q}$, then there exist $a,b \in \mathbb{Z}$ with $(a,b) = 1$ such that $\beta = \{\frac{a}{b}, \Phi_n(\frac{a}{b})\}$. Choosing a prime l other than any prime divisor of n, we prove that $p \mid j = v_l(\Phi_n(a,b)) > 0$. It is obvious that $l \nmid ab$. We claim that, for $p \neq j$,

$$\tau_l\left\{\frac{a}{b}, \Phi_n\left(\frac{a}{b}\right)\right\}^{\frac{n}{p^{v_p(n)}}} \not\equiv 1 \pmod{l}. \qquad (*)$$

In fact, if $(*)$ does not hold, then

$$\tau_l\left\{\frac{a}{b}, \Phi_n\left(\frac{a}{b}\right)\right\}^{\frac{n}{p^{v_p(n)}}} = \left(\frac{a}{b}\right)^{j\cdot(\frac{n}{p^{v_p(n)}})} \equiv 1 \pmod{l}.$$

On the other hand, $\{\frac{a}{b}, \Phi_n(\frac{a}{b})\}^n = 1$, so $(\frac{a}{b})^n \equiv 1 \pmod{l}$. Since $(j,p) = 1$, $(\frac{a}{b})^{\frac{n}{p^{v_p(n)}}} \equiv 1 \pmod{l}$. Since $l \mid \Phi_n(a,b)$, we have $l \mid$ (numerator of $\Phi_n(a,b)$). By the expression of $\Phi_n(a,b)$ in the proof of the former theorem, l must divide such a form $\Phi_p(a^t,b^t)$, where $t \mid n$ and $(t,p) = 1$. Then $a^{p\cdot t} \equiv b^{p\cdot t} \pmod{l}$. Hence, $a^t \equiv b^t \pmod{l}$, which contradicts the fact that $l \mid \Phi_p(a^t,b^t)$ and $(a,b) = 1$. We obtain $p \mid v_l(\Phi_n(a,b))$.

Finally we will prove $p \mid v_q(\Phi_n(a,b))$. First we have $v_q(\frac{a}{b}) = 0$. If not, then an easy calculation shows that $\tau_q\{\frac{a}{b}, \Phi_n(\frac{a}{b})\} \equiv 1 \pmod{q}$, by the previous assumption, $\tau_q\{a_0, \Phi(a_0)\}^p \equiv 1 \pmod{q}$, i.e., $a_0^p \equiv 1 \pmod{q}$, which contradicts Lemma 2.9 [10]. Next we have $v_q(\Phi_n(a,b)) > 0$. If not, then

$$\tau_q\{a_0, \Phi(a_0)\}^p = \tau_q\left\{\frac{a}{b}, \Phi_n\left(\frac{a}{b}\right)\right\} = (-1)^{v_q(\frac{a}{b})v_q(\Phi_n(\frac{a}{b}))}\frac{(\frac{a}{b})^{v_q(\Phi_n(\frac{a}{b}))}}{(\Phi_n(\frac{a}{b}))^{v_q(\frac{a}{b})}} \equiv 1 \pmod{q}.$$

i.e., $a_0^p \equiv 1 \pmod{q}$, which is also a contradiction. Then, by the same argument of the foregoing part of the proof, we can get $p \mid v_q(\Phi_n(a,b))$. Hence, if $G_n(\mathbb{Q})$ is a group, then, by Theorem 3.1, we get (1). If we replace p by some other prime factor of n in the proof, then we will obtain (2).

4 Some Examples

In this section, we will verify that $G_n(\mathbb{Q})$ are not groups for $n = 15, 21, 33, 35, 60$ and 105. In all the cases we proceed in the same way:

1 We first find a prime $q \equiv 1 \pmod{n}$ such that we need to prove only that $\Phi_n(a,b) = \varepsilon_n z^p q^p$ has no integral solutions.

2 We factor $\Phi_n(a,b)$ in $\mathbb{Z}(\zeta_p)$ and get a polynomial about ζ_p.

3 Finally we consider a polynomial over $\mathbb{Z}/q\mathbb{Z}[x]/(\Phi_p(x))$. By Lemma 2.4, we are working over $\mathbb{Z}/q\mathbb{Z}$. By computation, if the polynomial has no solution over the finite field then we get what we want.

Theorem 4.1 *$G_{15}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We have $31 \parallel \Phi_{15}(-3) = 31 \cdot 271$. We let $q = 31$. Since $5 \not\equiv 1 \pmod 3$, by Theorem 3.2, we need to prove only the Diophantine equation $\Phi_{15}(a, b) = z^5 31^5$ has no solution $(a, b, z) \in \mathbb{Z}^3$. We see that the equation can be written as

$$\Phi_5(a^3, b^3) = \Phi_5(a, b) z^5 31^5, \tag{4.1}$$

i.e., $\prod_{i=1}^{4}(a^3 - b^3\zeta_5^i) = \prod_{j=1}^{4}(a - b\zeta_5^j) z^5 31^5$. We have

$$a^3 - b^3\zeta_5 = a^3 - b^3\zeta_5^6 = (a - b\zeta_5^2)(a^2 + ab\zeta_5 + b^2\zeta_5^4),$$

$$a^3 - b^3\zeta_5^2 = a^3 - b^3\zeta_5^{12} = (a - b\zeta_5^4)(a^2 + ab\zeta_5^4 + b^2\zeta_5^3),$$

$$a^3 - b^3\zeta_5^3 = (a - b\zeta_5)(a^2 + ab\zeta_5 + b^2\zeta_5^2),$$

$$a^3 - b^3\zeta_5^4 = a^3 - b^3\zeta_5^9 = (a - b\zeta_5^3)(a^2 + ab\zeta_5^3 + b^2\zeta_5).$$

If $a \not\equiv b \pmod 5$, then $a^3 \not\equiv b^3 \pmod 5$. By Lemma 2.5, $(a - b\zeta_5^i, a - b\zeta_5^j) = 1, (a^3 - b^3\zeta_5^i, a^3 - b^3\zeta_5^j) = 1 (1 \le i \ne j \le 4)$. If $a \equiv b \pmod 5$, then $1 - \zeta_5^i \mid a - b\zeta_5^i$ and $(\frac{a - b\zeta_5^i}{1 - \zeta_5^i}, \frac{a - b\zeta_5^j}{1 - \zeta_5^j}) = 1$. We can also see that $1 - \zeta_5^i \mid a^3 - b^3\zeta_5^i$ and $(\frac{a^3 - b^3\zeta_5^i}{1 - \zeta_5^i}, \frac{a^3 - b^3\zeta_5^j}{1 - \zeta_5^j}) = 1 (1 \le i, j \le 4, i \ne j)$. It is known that $\frac{1 - \zeta_5^i}{1 - \zeta_5^j}$ is a unit in $\mathbb{Z}[\zeta_5]$. From the above, we conclude that, if (4.1) is solvable in $\mathbb{Z}$, then $a^3 - b^3\zeta_5 = (a - b\zeta_5^2)\varepsilon\alpha^5$, where $\alpha \in \mathbb{Z}[\zeta_5]$ and ε is a unit of $\mathbb{Q}(\zeta_5)$.

By Lemma 2.3, we may assume that $\varepsilon = \zeta_5^i(1 + \zeta_5^3)^j (0 \le i, j \le 4)$. Hence

$$a^3 - b^3\zeta_5 = (a - b\zeta_5^2)\zeta_5^i(1 + \zeta_5)^j\alpha^5.$$

We have $\alpha^5 \equiv \rho \pmod 5$, where $\rho \in \mathbb{Z}$. For any $a, b \in \mathbb{Z}/5\mathbb{Z}$, consider

$$a^3 - b^3 x = (a - bx^2)x^i(1 + x^3)^j\rho \tag{4.2}$$

over $\mathbb{Z}/5\mathbb{Z}[x]/(\Phi_5(x))$.

One can check that only if i, j take the following values:

i	j
0	0
3	1
4	0

there are $a, b \in \mathbb{Z}/5\mathbb{Z}$ such that (4.2) holds.

Now let $a, b \in \mathbb{Z}/31\mathbb{Z}$, consider

$$(a^3 - b^3 x)(a - bx^2)^4 x^{5-i}(1 + x^3)^{5-j} = \alpha^5 \tag{4.3}$$

over $\mathbb{Z}/31\mathbb{Z}[x]/(\Phi_5(x))$.

Let

$$S_1 = \{x \in \mathbb{Z}/31\mathbb{Z} \mid \Phi_5(x) = 0\} = \{2, 4, 6, 8\},$$

$$S_2 = \{x \in \mathbb{Z}/31\mathbb{Z} \mid \Phi_{15}(x) = 0\} = \{7, 9, 10, 14, 18, 19, 20, 28\},$$

$$(\mathbb{Z}/31\mathbb{Z})^5 = \{0, \pm 1, \pm 5, \pm 6\}.$$

By Lemma 2.4, we see that (4.3) holds if and only if $x \in S_1$. Let i, j take the values as in the above and $\frac{a}{b} \pmod{31} \in S_2$. One can verify that, for any nonzero integers a, b, there exists no $\alpha \in \mathbb{Z}/31\mathbb{Z}[x]/(\Phi_5(x))$ satisfying (4.3). Hence $\Phi_{15}(a, b) = z^5 31^5$ has no solution $(a, b, z) \in \mathbb{Z}^3$ satisfying $(a, b) = 1$. Our theorem is proved.

Theorem 4.2 *$G_{21}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We see that $43 \parallel \Phi_{21}(-3) = 7 \cdot 43 \cdot 2269$. We choose $q = 43$. Since $7 \equiv 1 \pmod 3$, and we have to consider two Diophantine equations:

$$\Phi_7(a^3, b^3) = \Phi_7(a, b) 43^7 z^7, \tag{4.4}$$

$$\Phi_7(a^3, b^3) = 7\Phi_7(a, b) 43^7 z^7. \tag{4.5}$$

We have $a^3-b^3\zeta_7=a^3-b^3\zeta_7^{15}=(a-b\zeta_7^5)(a^2+ab\zeta_7^5+b^2\zeta_7^3)$. If (4.4) is solvable in $\mathbb{Z}$, as in the proof of Theorem 4.1, we must have $a^3-b^3\zeta_7=(a-b\zeta_7^5)\varepsilon\alpha^7$, where ε is a unit in $\mathbb{Z}[\zeta_7]$, and $\alpha\in\mathbb{Z}[\zeta_7]$.

By Lemma 2.3, $\varepsilon=\zeta_7^i(1+\zeta_7)^j(1+\zeta_7^2)^k(0\le i,j,k\le 6)$, so

$$a^3-b^3\zeta_7=(a-b\zeta_7^5)\zeta_7^i(1+\zeta_7)^j(1+\zeta_7^2)^k\alpha^7.$$

Letting $a,b\in\mathbb{Z}/43\mathbb{Z}$, we consider

$$(a^3-b^3x)(a-bx^5)^6x^{7-i}(1+x)^{7-j}(1+x^2)^{7-k}=\alpha^7 \tag{4.6}$$

over $\mathbb{Z}/43\mathbb{Z}[x]/(\Phi_7(x))$.

If $b\not\equiv 0 \pmod{43}$, then (4.6) can be written as $(\frac{a}{b})^3-x(\frac{a}{b}-x^5)^6x^{7-i}(1+x)^{7-j}(1+x^2)^{7-k}b^5=\alpha^7$. Let $f(c,a,x)=(a^3-x)(a-x^5)^6c$, $c\in(\mathbb{Z}/43\mathbb{Z})^*$. We have

$$S_1=\{x\in\mathbb{Z}/43\mathbb{Z}\mid\Phi_7(x)=0\}=\{4,11,16,21,35,41\},$$

$$S_2=\{x\in\mathbb{Z}/43\mathbb{Z}\mid\Phi_{21}(x)=0\}=\{9,10,13,14,15,17,23,24,25,31,38,40\},$$

$$(\mathbb{Z}/43\mathbb{Z})^7=\{0,\pm1,\pm6,\pm7\}.$$

By Lemma 2.4, one can see that (4.6) holds if and only if $x\in S_1$. Let x be taken from S_1, a from S_2, and let c range from 1 to 42. One can verify that no non-integers x,a,c exist to make $f(c,a,x)\in(\mathbb{Z}/43\mathbb{Z})^7$. Thus $b\equiv 0 \pmod{43}$, and $a\equiv 0 \pmod{43}$, which contradicts the fact $(a,b)=1$.

Considering (4.5), we know that $a^3\equiv b^3 \pmod 7$ and $a\not\equiv b \pmod 7$, and so if $i\ne j$, then $(\frac{a^3-b^3\zeta_7^i}{1-\zeta_7^i},\frac{a^3-b^3\zeta_7^j}{1-\zeta_7^j})=1$ and $(a-b\zeta_7^i,a-b\zeta_7^j)=1$. Note that $7=\Pi_{i=1}^6(1-\zeta_7^i)$. So if (4.5) is solvable in $\mathbb{Z}$, we must have $a^3-b^3\zeta_7=(1-\zeta_7)(a-b\zeta_7^5)\zeta_7^i(1+\zeta_7)^j(1+\zeta_7^2)^k$, $0\le i,j,k\le 6$. Consider

$$(a^3-b^3x)(a-bx^5)^6x^{7-i}(1+x)^{7-j}(1+x^2)^{7-k}(1-x)^6=\alpha^7. \tag{4.7}$$

Write $f(c,a,x)=(a^3-x)(a-x^5)^6c$, $c\in(\mathbb{Z}/43\mathbb{Z})^*$. Discussing as in (4.4), we see that there exist no nonzero integers a and b with $(a,b)=1$ satisfying $f(c,a,x)\in(\mathbb{Z}/43\mathbb{Z})^7$. This completes our proof.

Theorem 4.3 *$G_{33}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We have $67\parallel\Phi_{33}(-2)=67\cdot 20857$ and $11\not\equiv 1 \pmod 3$. By Theorem 3.2, we need to prove only that

$$\Phi_{33}(a,b)=67^{11}z^{11}, \tag{4.8}$$

i.e., $\Phi_{11}(a^3,b^3)=\Phi_{11}(a,b)67^{11}z^{11}$ has no solution $(a,b,z)\in\mathbb{Z}^3$ with $(a,b)=1$. We have

$$a^3-b^3\zeta_{11}=a^3-b^3\zeta_{11}^{12}=(a-b\zeta_{11}^4)(a^2+ab\zeta_{11}^4+b^2\zeta_{11}^8).$$

If (4.8) is solvable, discussing as in the foregoing theorem, we see that $a^3-b^3\zeta_{11}=(a-b\zeta_{11}^4)\varepsilon\alpha^{11}$, where ε is a unit in $\mathbb{Z}[\zeta_{11}]$, and $\alpha\in\mathbb{Z}[\zeta_{11}]$. If $b\not\equiv 0 \pmod{67}$, let $f(c,a,x)=(a^3-x)(a-x^4)^{10}c$, $c\in(\mathbb{Z}/67\mathbb{Z})^*$. We have

$$S_1=\{x\in\mathbb{Z}/67\mathbb{Z}\mid\Phi_{11}(x)=0\}=\{9,14,15,22,24,25,40,59,62,64\},$$

$$S_2=\{x\in\mathbb{Z}/67\mathbb{Z}\mid\Phi_{33}(x)=0\}$$

$$=\{4,6,10,16,17,19,21,23,26,33,35,36,39,47,49,54,55,56,60,65\},$$

$$(\mathbb{Z}/67\mathbb{Z})^{11}=\{0,\pm1,\pm29,\pm30\}.$$

Similarly to the previous proof, letting x be taken from S_1, a from S_2, and c range from 1 to 66, one can verify that there do not exist x,a,c to make $f(c,a,x)\in(\mathbb{Z}/67\mathbb{Z})^{11}$. Thus $b\equiv 0 \pmod{67}$, and $a\equiv 0 \pmod{67}$, which contradicts the fact $(a,b)=1$. Our theorem is proved.

Theorem 4.4 *$G_{35}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We have that $71\parallel\Phi_{35}(2)=71\cdot 122921$ and $7\not\equiv 1 \pmod 5$. Similarly to the foregoing examples, we need to show only that

$$\Phi_5(a^7,b^7)=\Phi_5(a,b)71^5z^5 \tag{4.9}$$

has no solution $(a,b,z)\in\mathbb{Z}^3$ with $(a,b)=1$. We have

$$a^7-b^7\zeta_5=a^7-b^7\zeta_5^{21}=(a-b\zeta_5^3)(a^6+a^5b\zeta_5^3+a^4b^2\zeta_5+a^3b^3\zeta_5^4+a^2b^4\zeta_5^2+ab^5+b^6\zeta_5^3).$$

If (4.9) is solvable in $\mathbb{Z}$, then we have $a^7-b^7\zeta_5=(a-b\zeta_5^3)\varepsilon\alpha^5$, where $\alpha\in\mathbb{Z}[\zeta_5]$ and ε is a unit of $\mathbb{Q}(\zeta_5)$. By Lemma 2.3, we may assume that $\varepsilon=\zeta_5^i(1+\zeta_5^3)^j(0\le i,j\le 4)$. Hence,

$$a^7-b^7\zeta_5=(a-b\zeta_5^3)\zeta_5^i(1+\zeta_5^3)^j\alpha^5.$$

Consider $a^7-b^7x=(a-bx^3)x^i(1+x^3)^j\alpha^5$ over $\mathbb{Z}/71\mathbb{Z}[x]/(\Phi_5(x))$. Change it into

$$(a^7-b^7x)(a-bx^3)^4x^{5-i}(1+x^3)^{5-j}=\alpha^5. \tag{4.10}$$

Let

$$S_1=\{x\in\mathbb{Z}/71\mathbb{Z}\mid\Phi_5(x)=0\}=\{5,24,54,57\},$$

$$S_2=\{x\in\mathbb{Z}/71\mathbb{Z}\mid\Phi_{35}(x)=0\}$$

$$=\{2,3,4,6,8,9,10,12,15,16,18,19,24,27,29,36,38,40,43,49,50,58,60,64\},$$

$$(\mathbb{Z}/71\mathbb{Z})^5=\{0,\pm1,\pm20,\pm23,\pm26,\pm30,\pm32,\pm34\}.$$

If $b\not\equiv 0$, let $f(c,a,x)=(a^7-b^7x)(a-bx^3)^4\cdot c$. Again, similarly to the previous proof, letting x be taken from S_1, a from S_2 and c range from 1 to 70, one can verify that no nonzero integers a,x,c exist satisfying $f(c,a,x)\in(\mathbb{Z}/71\mathbb{Z})^5$. Then $b\equiv 0 \pmod{71}$, hence $a\equiv 0 \pmod{71}$, a contradiction. Hence $\Phi_{35}(a,b)=71^5z^5$ has no solution $(a,b,z)\in\mathbb{Z}^3$ satisfying $(a,b)=1$. Our theorem is proved.

Theorem 4.5 *$G_{60}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We have $60=2^2\cdot3\cdot5$ and $181\parallel\Phi_{60}(6)$. Furthermore, $5\not\equiv 1 \pmod{2\cdot3}$. By Theorem 3.2, if the Diophantine equation

$$\Phi_{60}(a,b)=181^5z^5 \tag{4.11}$$

has no solution $a,b,z\in\mathbb{Z}$ with $(a,b)=1$, then $G_{60}(\mathbb{Q})$ is not a group. We have

$$\Phi_{60}(a,b)=\frac{\Phi_5(a^{12},b^{12})\Phi_5(a^2,b^2)}{\Phi_5(a^6,b^6)\Phi_5(a^4,b^4)}=\prod_{i=1}^{4}(a^4-a^2b^2\zeta_5^i+b^4\zeta_5^{2i}),$$

where $a^4-a^2b^2\zeta_5^i+b^4\zeta_5^{2i}=\frac{(a^{12}-b^{12}\zeta_5^i)(a^2-b^2\zeta_5^i)}{(a^6-b^6\zeta_5^{3i})(a^4-b^4\zeta_5^{2i})}$.

Assume $a\equiv b \pmod 5$. If $a\ne b$, then $(\frac{a-b\zeta_5^i}{1-\zeta_5^i},\frac{a-b\zeta_5^j}{1-\zeta_5^j})=1$, $(\frac{a^2-b^2\zeta_5^i}{1-\zeta_5^i},\frac{a^2-b^2\zeta_5^j}{1-\zeta_5^j})=1$, $(\frac{a^6-b^6\zeta_5^i}{1-\zeta_5^i},\frac{a^6-b^6\zeta_5^j}{1-\zeta_5^j})=1$ and $(\frac{a^{12}-b^{12}\zeta_5^i}{1-\zeta_5^i},\frac{a^{12}-b^{12}\zeta_5^j}{1-\zeta_5^j})=1$. It's known that $\frac{1-\zeta_5^i}{1-\zeta_5^j}$ is a unit of $\mathbb{Z}[\zeta_5]$. Thus $(a^4-a^2b^2\zeta_5^i+b^4\zeta_5^{2i},a^4-a^2b^2\zeta_5^j+b^4\zeta_5^{2j})=1$.

Similarly, when $a\not\equiv b \pmod 5$, but $a^2\equiv b^2 \pmod 5$, or $a\not\equiv b \pmod 5$, but $a^3\equiv b^3 \pmod 5$, or $a\not\equiv b \pmod 5$, but $a^4\equiv b^4 \pmod 5$, we may also obtain $(a^4-a^2b^2\zeta_5^i+b^4\zeta_5^{2i},a^4-a^2b^2\zeta_5^j+b^4\zeta_5^{2j})=1$.

Hence if (4.11) is solvable in $\mathbb{Z}$, then $a^4-a^2b^2\zeta_5+b^4\zeta_5^2=\varepsilon\alpha^5$, where $\alpha\in\mathbb{Z}[\zeta_5]$ and ε is a unit of $\mathbb{Q}(\zeta_5)$. We will prove that it is impossible.

By Lemma 2.3, we may assume that $\varepsilon=\zeta_5^i(1+\zeta_5^3)^j(0\le i,j\le 4)$. Then $a^4-a^2b^2\zeta_5+b^4\zeta_5^2=\zeta_5^i(1+\zeta_5^3)^j\alpha^5$. Consider

$$(a^4-a^2b^2x+b^4x^2)x^{5-i}(1+x^3)^{5-j}=\alpha^5 \tag{4.12}$$

over $\mathbb{Z}/181\mathbb{Z}[x]/(\Phi_5(x))$.

If $b\not\equiv 0 \pmod{181}$, then let $f(c,a,x)=(a^4-a^2x+x^2)\cdot c$. Let

$$S_1=\{x\in\mathbb{Z}/181\mathbb{Z}\mid\Phi_{60}(x)=0\}$$

$$=\{6,8,30,40,51,68,71,86,95,110,113,130,141,151,173,175\},$$

$$S_2=\{x\in\mathbb{Z}/181\mathbb{Z}\mid\Phi_5(x)=0\}=\{42,59,125,135\},$$

$$(\mathbb{Z}/181\mathbb{Z})^5=\{0,\pm1,\pm7,\pm17,\pm19,\pm26,\pm32,\pm39,\pm43,\pm48,$$

$$\pm49,\pm61,\pm62,\pm65,\pm72,\pm73,\pm80,\pm88,\pm89\}.$$

By Lemma 2.4, (4.12) holds if and only if $x \in S_2$ and $\alpha_i = (a^4 - a^2x_i + x_i^2) \cdot c$. Let $a \in S_1$ and c range from 1 to 180. We can check that α_i will not be in $(\mathbb{Z}/181\mathbb{Z})^5$ simultaneously. Then we have $b \equiv 0 \pmod{181}$, therefore $a \equiv 0 \pmod{181}$, which is a contradiction. Our theorem is proved.

Theorem 4.6 *$G_{105}(\mathbb{Q})$ is not a subgroup of $K_2\mathbb{Q}$.*

Proof We have $105 = 3 \cdot 5 \cdot 7$ and $211 \parallel \Phi_{105}(-2), 7 \not\equiv 1 \pmod{3 \cdot 5}$. Consider the Diophantine equation

$$\Phi_{105}(a, b) = 211^7 z^7. \tag{4.13}$$

We have

$$\Phi_{105}(a,b) = \frac{\Phi_7(a^{15},b^{15})\Phi_7(a,b)}{\Phi_7(a^5,b^5)\Phi_7(a^3,b^3)} = \prod_{i=1}^{6}(a^8 - a^7b\zeta_7^i + a^5b^3\zeta_7^{3i} - a^4b^4\zeta_7^{4i} + a^3b^5\zeta_7^{5i} - ab^7 + b^8\zeta_7^i).$$

In fact, $a^8 - a^7b\zeta_7 + a^5b^3\zeta_7^3 - a^4b^4\zeta_7^4 + a^3b^5\zeta_7^5 - ab^7 + b^8\zeta_7 = \frac{(a^{15}-b^{15}\zeta_7)(a-b\zeta_7)}{(a^5-b^5\zeta_7^5)(a^3-b^3\zeta_7^3)}$.

Similarly to the proof of Theorem 4.5,

$$(a^8 - a^7b\zeta_7^i + a^5b^3\zeta_7^{3i} - a^4b^4\zeta_7^{4i} + a^3b^5\zeta_7^{5i} - ab^7 + b^8\zeta_7^i, a^8 - a^7b\zeta_7^j + a^5b^3\zeta_7^{3j} - a^4b^4\zeta_7^{4j} + a^3b^5\zeta_7^{5j} - ab^7 + b^8\zeta_7^j) = 1,$$

if $i \neq j$.

Hence if (4.13) is solvable in $\mathbb{Z}$, then $a^8 - a^7b\zeta_7 + a^5b^3\zeta_7^3 - a^4b^4\zeta_7^4 + a^3b^5\zeta_7^5 - ab^7 + b^8\zeta_7 = \varepsilon\alpha^7$, where $\alpha \in \mathbb{Z}[\zeta_7]$ and ε is a unit of $\mathbb{Z}[\zeta_7]$. Similarly to the proof of Theorem 4.5, let

$$S_1 = \{x \in \mathbb{Z}/211\mathbb{Z} \mid \Phi_{105}(x) = 0\} = \{4, 6, 9, 16, 20, 24, 30, 36, 37, 44, 45,$$
$$46, 47, 49, 51, 52, 53, 56, 59, 62, 66, 69, 70, 78, 80, 81, 84, 93, 95, 99, 103, 105,$$
$$119, 120, 126, 136, 139, 154, 163, 170, 172, 176, 182, 189, 194, 204, 208, 209\},$$

$$S_2 = \{x \in \mathbb{Z}/211\mathbb{Z} \mid \Phi_7(x) = 0\} = \{58, 123, 144, 148, 171, 199\},$$

$$(\mathbb{Z}/211\mathbb{Z})^7 = \{0, \pm1, \pm10, \pm14, \pm15, \pm19, \pm21, \pm23,$$
$$\pm55, \pm61, \pm71, \pm74, \pm77, \pm83, \pm100, \pm104\}.$$

If $b \not\equiv 0 \pmod{211}$, let $f(c, a, x) = (a^8 - a^7x + a^5x^3 - a^4x^4 + a^3x^5 - a + x) \cdot c$.

By Lemma 2.4, (4.14) is solvable if and only if $x \in S_2$, and $\alpha_i = f(c, a, x_i), x_i \in S_2$. We can check that, if $a \in S_1, x_i \in S_2$ and c ranges from 1 to 210, all $f(c, a, x_i) \notin (\mathbb{Z}/211\mathbb{Z})^7$. This is a contradiction. Hence $b \equiv 0 \pmod{211}$, so $a \equiv 0 \pmod{211}$. This contradicts the fact $(a, b) = 1$. Hence (4.14) has no solution $(a, b, z) \in \mathbb{Z}^3$ with $(a, b) = 1$. Our theorem is completed.

References

[1] Milnor, J.: Introduction to Algebraic K-theory, Annals of Math., Studies 72, Princeton Univ. Press, 1971

[2] Browkin, J.: Elements of small order in K_2F, Algebraic K-Theory, Lecture Notes in Math., 966, 1–6, Springer-Verlag, Berlin-Heidelberg-New York, 1982

[3] Qin, H. R.: Elements of finite order in K_2F of fields. *Chinese Science Bulletin*, **39**, 449–451 (1994)

[4] Urbanowicz, J.: On elements of given orders in K_2F. *J. Pure Appl. Alg.*, **50**, 295–307 (1988)

[5] Qin, H. R.: The subgroup of finite order in $K_2\mathbb{Q}$, Algebraic K-theory and Its Applications (H. Bass, A. O. Kuku, C. Pedrini, Ed.), World Scientific, Singapore, 2000

[6] Xu, K. J., Qin, H. R.: Some elements of finite order in $K_2\mathbb{Q}$. *Annals of Chin. Math.*, **22**, 563–570 (2001)

[7] Xu, K. J.: Neither $G_9(\mathbb{Q})$ nor $G_{11}(\mathbb{Q})$ is a subgroup of $K_2\mathbb{Q}$. *Northeast Math. J.*, **18**, 59–62 (2002)

[8] Zhu, Q. S.: Elements of prime power order of $K_2\mathbb{Q}$. *J. Number Theory*, to appear

[9] Zantema, H.: Integer valued polynomials in algebraic number theory, Ph. D Thesis, Universiteit van Amsterdam, 1982

[10] Washington, L. C.: Introduction to Cyclotomic Fields, GTM83, Springer-Verlag, Berlin-Heidelberg-New York, 1982