On the elements of prime power order in $K_2$ of a number field

by

KEJIAN XU (Qingdao)

1. Introduction. Let $F$ be a field and $K_2(F)$ be the Milnor $K_2$-group of $F$ (see [4]). It is an important problem to write down explicitly the elements of a given order in $K_2(F)$. Tate [8] proved that if $F$ is a global field containing $\zeta_n$, a primitive $n$th root of unity, then every element of order $n$ in $K_2(F)$ can be written in the form of $\{\zeta_n, a\}$, $a \in F^*$. Suslin [7] generalized Tate’s result to any field containing $\zeta_n$. It is natural to generalize this result further to a field possibly not containing $\zeta_n$. In [1], Browkin considered elements of small orders in $K_2(F)$. Let $\Phi_n(x)$ be the $n$th cyclotomic polynomial and

$$G_n(F) = \{\{a, \Phi_n(a)\} \in K_2(F) \mid a, \Phi_n(a) \in F^*\}.$$ 

Browkin proved in [1] that for any $a \in F^*$, $\{a, \Phi_n(a)\}^n = 1$ and that for every field $F \neq \mathbb{F}_2$ and $n = 1, 2, 3, 4$ or 6, $G_n(F)$ is a subgroup of $K_2(F)$. Then Browkin conjectured that for any integer $n \neq 1, 2, 3, 4, 6$ and any field $F$, $G_n(F)$ is not a subgroup of $K_2(F)$. In particular, he pointed out the case of $F = \mathbb{Q}$ (the rational number field) and $n = 5$.

From [6], $G_n(\mathbb{Q})$ is not a group if $n = 5, 7$, from [5], $G_{2n}(\mathbb{Q})$ is a group if and only if $n \leq 2$, and from [10], for $n \geq 2, G_{2n^2m}(\mathbb{Q})$ is a group if and only if $n = 2, m = 0$. Furthermore, similar results are also true for some special quadratic fields (see [11]). The idea behind the proofs is that the problem can be reduced to some diophantine equations which have no nontrivial solutions. But we think that this idea is too restricted. Actually, we found that the problem could be reduced simply to some equations which could have only finitely many solutions. Following this idea and using Faltings’ theorem on the Mordell conjecture, we proved in [12] that if $p \geq 5$ is a prime and $n \geq 2$ a positive integer, then $G_{pn}(\mathbb{Q})$ is not a subgroup of $K_2(\mathbb{Q})$.

2000 Mathematics Subject Classification: 11R70, 19F15.

This research is supported by National Natural Science Foundation of China (10371061).
In this paper, it is proved that for a number field $F$ and a prime number $p$, if $p \geq 3$ and $n \geq 2$, or $p = 2$ and $n \geq 4$, then $G_{p^n}(F)$ is not a subgroup of $K_2(F)$.

2. Main theorem

**Lemma 2.1** ([1]). If $F$ is a field and $a, \Phi_n(a) \in F^*$, then $\{a, \Phi_n(a)\}^n = 1$ in $K_2(F)$.

**Theorem 2.2.** Let $F$ be a number field and $p$ a prime number. If $p \geq 3$ and $n \geq 2$, or $p = 2$ and $n \geq 4$, then $G_{p^n}(F)$ is not a subgroup of $K_2(F)$.

**Proof.** By the definition, if $a, \Phi_n(a) \in F^*$, then $\{a, \Phi_n(a)\} \in G_{p^n}(F)$.

We shall find $a$ such that $\{a, \Phi_n(a)\}^p$ is not an element in $G_{p^n}(F)$.

The proof will be divided into several steps.

1) Let $S$ be a finite set of places of $F$ containing all archimedean ones, and all places above $p$ and above the primes ramified in $F$. Moreover, we assume that $S$ is sufficiently large, so that the ring $\mathcal{O}_{F,S}$ of $S$-integers is a unique factorization domain.

By the Dirichlet–Hasse–Chevalley theorem (see [9]), the group of $S$-units in $\mathcal{O}_{F,S}$ is finitely generated: There are fundamental $S$-units $\varepsilon_1, \ldots, \varepsilon_t$ such that every $S$-unit $u$ can be written uniquely in the form

$$u = \zeta^r \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t}, \quad \text{where } r, k_1, \ldots, k_t \in \mathbb{Z}.$$

Here $\zeta$ is a generator of the group of roots of unity in $F$ and $0 \leq r < \text{ord} \zeta$.

Let us consider the $S$-units of the form

$$c = \zeta^r \varepsilon_1^{k_1} \cdots \varepsilon_t^{k_t}, \quad \text{where } 0 \leq r < p, 0 \leq k_j < p \text{ for } 1 \leq j \leq t.$$

The set of the $S$-units (1) is finite.

The equations

$$\Phi_p(x) = cy^p \quad \text{for } p > 3, \quad \Phi_3^2(x) = cy^3, \quad \Phi_{24}(x) = cy^2,$$

where $c$ is of the form (1), define curves of genera $> 1$, by a formula of Hurwitz ([3]). It follows from Faltings’ theorem ([2]) that each of the equations (2) has only a finite number of solutions $x, y \in F$.

From the identity

$$\Phi_{p^n}(x) = \Phi_{p^k}(x^{p^{n-k}}) \quad \text{for } n \geq k,$$

it follows that for every $c$ given in (1), also the equation

$$\Phi_{p^n}(x) = cy^p$$

has only a finite number of solutions $x, y \in F$, where $n \geq 1$ for $p > 3$, $n \geq 2$ for $p = 3$ and $n \geq 4$ for $p = 2$.

2) We state below some properties of cyclotomic polynomials $\Phi_k(x)$, $k > 1$, used in what follows.
Elements of prime power order in $K_2$  

Since $\Phi_k(0) = 1$, we have $\Phi_k(u) \equiv 1 \pmod{u}$ for every positive integer $u$. In particular, $\Phi_k(u!) \equiv 1 \pmod{u!}$, so every prime divisor of $\Phi_k(u!)$ is greater than $u$.

Since $\Phi_k(x)$ does not have multiple roots, we have $(\Phi_k(x), \Phi'_k(x)) = 1$. Hence

\begin{equation}
(4) \quad f(x)\Phi_k(x) + g(x)\Phi'_k(x) = D_k
\end{equation}

for some $f, g \in \mathbb{Z}[x]$ and $D_k \in \mathbb{N}$. It follows that if a prime $q > D_k$ divides $\Phi_k(u)$ for some $u \in \mathbb{Z}$, then $q \nmid \Phi'_k(u)$. Hence from

$$\Phi_k(u + q) \equiv \Phi_k(u) + q\Phi'_k(x) \pmod{q^2}$$

we deduce that

\begin{equation}
(5) \quad q \parallel \Phi_k(u) \quad \text{or} \quad q \parallel \Phi_k(u + q)
\end{equation}

for every prime $q > D_k$ and $u \in \mathbb{Z}$ such that $q \mid \Phi_k(u)$.

3) Let $m_1 > \max(p, D_{p^n})$, where $D_k$ is defined in (4). We assume moreover that $m_1$ is greater than every prime number which has a divisor in $S$, in particular, $m_1$ is greater than every prime number ramified in $F$.

Let $p_1$ be a prime divisor of $\Phi_{p^n}(m_1!)$. Then $p_1 > m_1$, and, by (5),

\begin{equation}
(6) \quad p_1 \parallel \Phi_{p^n}(a_1), \quad \text{where } a_1 = m_1! \text{ or } a_1 = m_1! + p_1.
\end{equation}

4) We claim that $\{a_1, \Phi_{p^n}(a_1)\}^p \neq 1$, where $a_1$ is defined in (6).

Since $p_1$ does not ramify in $F$, we have $v_{p_1}(r) = v_{p_1}(r)$ for every prime ideal $p_1$ of $F$ dividing $p_1$ and every $r \in \mathbb{Q}$. Therefore the corresponding tame symbol $\tau_{p_1}$ satisfies

$$\tau_{p_1}\{a_1, \Phi_{p^n}(a_1)\}^p \equiv a_1^p \equiv (m_1!)^p \pmod{p_1}.$$ 

If $(m_1!)^p \equiv 1 \pmod{p_1}$, then

$$\Phi_{p^n}(a_1) \equiv \Phi_{p^n}(m_1!) \equiv \Phi_{p^n}(1) = p \pmod{p_1}.$$ 

This is impossible, since $p_1 \mid p_1, p_1 \mid \Phi_{p^n}(a_1)$ and $p < p_1$.

5) Next we proceed inductively. Fix $m_2 > \Phi_{p^n}(a_1)$; then $m_2 > p_1$ and $m_2 > a_1 > m_1$.

Let $p_2$ be a prime divisor of $\Phi_{p^n}(m_2!)$. Hence $p_2 > m_2$ and, by (5),

$$p_2 \parallel \Phi_{p^n}(a_2), \quad \text{where } a_2 = m_2! \text{ or } a_2 = m_2! + p_2.$$ 

Similarly to the previous considerations we prove that

$$\tau_{p_2}\{a_2, \Phi_{p^n}(a_2)\}^p \neq 1, \quad \text{where } p_2 \mid p_2.$$ 

Moreover

$$\tau_{p_2}\{a_1, \Phi_{p^n}(a_1)\}^p = 1, \quad \text{since } p_2 > m_2 > \max(a_1, \Phi_{p^n}(a_1)).$$ 

Hence $\{a_1, \Phi_{p^n}(a_1)\}^p \neq \{a_2, \Phi_{p^n}(a_2)\}^p$. 

By induction, we get an infinite sequence $a_1 < a_2 < \cdots$ of positive integers such that the elements
\[
\{a_k, \Phi_{p^n}(a_k)\}^p \in K_2(F), \quad k = 1, 2, \ldots,
\]
are nontrivial and distinct.

6) Assume that for every $a_k$ defined above we have
\[
(7) \quad \{a_k, \Phi_{p^n}(a_k)\}^p = \{b_k, \Phi_{p^n}(b_k)\}
\]
for some $b_k \in F^*$. Since for $k = 1, 2, \ldots$ the left hand sides of (7) are distinct, and $\Phi_{p^n}(x)$ takes every value only a finite number of times, it follows that there are infinitely many distinct elements $\Phi_{p^n}(b_k)$. Therefore, by (3), there is $b = b_{k_0}$ such that $\Phi_{p^n}(b) \neq cy^p$ for every $c$ of the form (1) and every $y \in F$. Then, by (7), for $a = a_{k_0}$ we get
\[
(8) \quad \{a, \Phi_{p^n}(a)\}^p = \{b, \Phi_{p^n}(b)\}.
\]
Since $\mathcal{O}_{F,S}$ is a unique factorization domain, from $\Phi_{p^n}(b) \neq cy^p$ it follows that there is a prime ideal $q$ of $\mathcal{O}_{F,S}$ such that
\[
(9) \quad p \nmid v_q(\Phi_{p^n}(b)).
\]
If $v_q(b) < 0$, then $v_q(\Phi_{p^n}(b)) = \deg \Phi_{p^n} \cdot v_q(b) = (p - 1)p^{n-1}v_q(b)$, where $n \geq 2$, hence $p | v_q(\Phi_{p^n}(b))$, which contradicts (9); if $v_q(b) > 0$, then $\Phi_{p^n}(b) \equiv \Phi_{p^n}(0) = 1 \pmod{q}$, hence $v_q(\Phi_{p^n}(b)) = 0$, which contradicts (9). Therefore $v_q(b) = 0$ and $v_q(\Phi_{p^n}(b)) = r > 0$, where $p \nmid r$. Hence $q | \Phi_{p^n}(b)$.

Consider the element $\xi := \{b, \Phi_{p^n}(b)\}^{p^{n-1}}$. By (8), we have
\[
\xi = \{a, \Phi_{p^n}(a)\}^{p^n} = 1,
\]
in view of Lemma 2.1. Then taking the corresponding tame symbol $\tau_q$ we get
\[
1 = \tau_q\{b, \Phi_{p^n}(b)\}^{p^{n-1}} \equiv b^{p^{n-1}} \pmod{q}.
\]
Since $q | \Phi_{p^n}(b)$ and $\Phi_{p^n}(x) \mid x^{p^n} - 1$, we get $b^{p^n} \equiv 1 \pmod{q}$. Hence the order of $b$ (mod $q$) is a power of $p$. Consequently, from $b^{p^{n-1}} \equiv 1 \pmod{q}$ and $p \nmid r$ we conclude that $b^{p^{n-1}} \equiv 1 \pmod{q}$. Hence
\[
\Phi_{p^n}(b) = \Phi_p(b^{p^{n-1}}) \equiv \Phi_p(1) = p \pmod{q}.
\]
This is impossible, since $q | \Phi_{p^n}(b)$ and $p$ is an $S$-unit. This contradiction proves the theorem.

**Remark 2.3.** For a number field $F$, whether or not $G_S(F)$ is a subgroup of $K_2(F)$ is unknown.

**Acknowledgments.** The author should like to thank the referee who modified the proof of Theorem 2.2, in particular, the assumption on the class number in the original version of this paper is removed following the referee’s report. The author should also like to thank Prof. Wenting Tong, Prof. Kezheng Li and Prof. Hourong Qin for their help.
References


Department of Mathematics
Qingdao University
Qingdao, 266071, P.R. China
E-mail: kejianxu@amss.ac.cn

Received on 26.9.2006
and in revised form on 30.11.2006