ACTA ARITHMETICA
134.2 (2008)

Tame kernels of quintic cyclic fields

by

XIA WU (Nanjing)

1. Introduction. The structure of the tame kernels of algebraic number fields has been investigated by many authors, e.g., [1], [2], [4], [5], [7], [10], [11], [12] and [15]. In particular, J. Browkin gave some explicit results for cubic cyclic fields with only one ramified prime in [1], and H. Zhou investigated the structure of tame kernels of cubic cyclic fields with two ramified primes in [15].

In the present paper, we investigate quintic cyclic fields. Let F be a quintic cyclic number field, and G its Galois group. It is well-known that $K_2\mathcal{O}_F$ is the tame kernel of F. We know that $K_2\mathcal{O}_F$ is a G-module, and we often use this fact to study the structure of $K_2\mathcal{O}_F$.

The paper is organized as follows. In Section 2, we give some results about the structure of the class groups $\mathcal{C}l(\mathcal{O}_F)$ and $\mathcal{C}l(\mathcal{O}_{F,2})$. In Section 3, we use these results to investigate the 2-primary part of $K_2\mathcal{O}_F$. We determine the elements of order 2 in $K_2\mathcal{O}_F$ explicitly and we prove that 4 divides the 2^i-rank of $K_2\mathcal{O}_F$ for $i \geq 2$. In Section 4, we use the G-module structure of $K_2\mathcal{O}_F$ and apply reflection theorems to investigate the q-primary part of $K_2\mathcal{O}_F$ for odd q. In particular, we prove a theorem, similar to the main result in [15], which confirms Browkin's Conjecture 4.6 of [1]. Finally, we assume that in F there is only one ramified prime p, $p > 11$. It is easy to see that $p \equiv 1 \pmod{10}$ and F is the unique quintic subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. We use the well-known Birch–Tate conjecture to compute the order of $K_2\mathcal{O}_F$, and deduce that $5 \mid \#K_2\mathcal{O}_F$.

Acknowledgements. I would like to thank my supervisor, Hourong Qin, for useful advice, and also Xuejun Guo and Qingzhong Ji for useful discussions on the subject.

2000 *Mathematics Subject Classification*: Primary 11R70; Secondary 11R16, 11Y40, 19-04, 19C99.

Key words and phrases: quintic fields, cyclic fields, tame kernels.

Supported by NSFC.

2. Structure of the Sylow q-subgroup of the class group. Let F be a quintic cyclic field. Let A_q be the Sylow q-subgroup of the class group $\mathcal{C}l(\mathcal{O}_F)$ of F for a prime number q, and let τ be a generator of the Galois group $T := \mathrm{Gal}(F/\mathbb{Q})$. If B is a group, we denote its order by $|B|$. For any element $a \in A_q$, let $\langle a\rangle$ denote the cyclic group generated by a.

LEMMA 2.1. *Let $a \in A_q$ with $q \neq 5$. If $a \neq 1$, then a, τa, $\tau^2 a$, $\tau^3 a$, $\tau^4 a$ are all distinct.*

Proof. Let $\tau^0 a = a$. If $\tau^i a = \tau^j a$ with $0 \le i < j \le 4$, it is easy to see that $a = \tau a = \tau^2 a = \tau^3 a = \tau^4 a$. Hence

$$a^5 = a \cdot \tau a \cdot \tau^2 a \cdot \tau^3 a \cdot \tau^4 a = \mathrm{Norm}_{F/\mathbb{Q}}(a) = 1.$$

Since $q \nmid 5$, it follows that $a = 1$, a contradiction. ∎

Let B_1 be a subgroup of A_q, and $B_1 \simeq \mathbb{Z}/q^i\mathbb{Z},\ i \ge 1$.

LEMMA 2.2. *For $q \equiv 2$, 3 or $4 \pmod 5$, we have $B_1 \cap \tau(B_1) = 1$.*

Proof. (1) If $B_1 \simeq \mathbb{Z}/q\mathbb{Z}$, then any $a \in B_1$ with $a \neq 1$ is a generator of B_1. If $\tau(a) \in B_1$, then

$$\tau(a) = a^t \in B_1,\ \tau^2(a) = a^{t^2} \in B_1,\ \tau^3(a) = a^{t^3} \in B_1,\ \tau^4(a) = a^{t^4} \in B_1.$$

By Lemma 2.1 the orbit of every $a \neq 1$ has five elements in B_1. Therefore $q = |B_1| \equiv 1 \pmod 5$, a contradiction.

(2) When $B_1 \simeq \mathbb{Z}/q^i\mathbb{Z}$, and $i \ge 2$, consider an element a of B_1 with $a \neq 1$. If the order of a is q^j, $1 \le j \le i$, set $B_1' := \langle a^{q^{j-1}}\rangle \simeq \mathbb{Z}/q\mathbb{Z}$. If $\tau(a) \in B_1$, then $\tau(a) = a^s$, $0 < s \le q^j - 1$, $q \nmid s$. Hence $\tau(a^{q^{j-1}}) = a^{q^{j-1}s} \in B_1'$. This is a contradiction to (1), so $\tau(a) \notin B_1$. ∎

Since τ^i is also a generator of the Galois group for $i = 2, 3, 4$, we know that

$$B_1 \cap \tau^i(B_1) = 1, \qquad 1 \le i \le 4. \tag{2.1}$$

LEMMA 2.3. *Let $q \equiv 2$ or $3 \pmod 5$. By (2.1) we can set $B = B_1 \times \tau^2(B_1)$. Then $B \cap \tau(B_1) = 1$ and $B \cap \tau^3(B_1) = 1$.*

Proof. (1) When $B_1 \simeq \mathbb{Z}/q\mathbb{Z}$, consider an element a of B_1 with $a \neq 1$. If $\tau(a) \in B$, then $\tau(a) = a^s \cdot \tau^2(a)^t$. If s or t is zero, this contradicts (2.1). It follows that $0 < s, t \le q - 1$. Then

$$\begin{aligned}\tau^3(a) &= \tau^2(\tau(a)) = \tau^2(a^s \cdot \tau^2(a)^t) = \tau^2(a)^s \cdot \tau^4(a)^t \\ &= \tau^2(a)^s \cdot (a \cdot \tau(a) \cdot \tau^2(a) \cdot \tau^3(a))^{-t} \\ &= \tau^2(a)^s \cdot (a \cdot a^s \cdot \tau^2(a)^t \cdot \tau^2(a) \cdot \tau^3(a))^{-t},\end{aligned}$$

so

$$\tau^3(a)^{1+t} = a^{-t(1+s)} \cdot \tau^2(a)^{s-t(1+t)} \in B.$$

It is easy to see that if $1 + t \neq q$, then $\tau^3(a) \in B$.

If $1+t=q$, then $\tau^3(a)^{1+t}=1$. We obtain $q \mid t(1+s)$ and $q \mid s-t(1+t)$. But the two conditions cannot hold at the same time. Therefore $\tau^3(a)\in B$.

It follows that $\tau^4(a)=(a\cdot\tau(a)\cdot\tau^2(a)\cdot\tau^3(a))^{-1}\in B$.

Let v be an element of B with $v\neq 1$. We know that $v=a^s\cdot\tau^2(a)^t$ with $0\le s,t\le q-1$. Then

$$\tau(v)=\tau(a)^s\cdot\tau^3(a)^t\in B,\qquad \tau^2(v)=\tau^2(a)^s\cdot\tau^4(a)^t\in B,$$
$$\tau^3(v)=\tau^3(a)^s\cdot a^t\in B,\qquad \tau^4(v)=\tau^4(a)^s\cdot\tau(a)^t\in B.$$

By Lemma 2.1 the orbit of v has five elements. Hence,

$$q^2=|B|\equiv 1 \pmod 5.$$

But the order of q mod 5 is 4, a contradiction. Therefore $\tau(a)\notin B$.

In a similar way, we can prove that $\tau^3(a)\notin B$.

(2) When $B_1\simeq\mathbb{Z}/q^i\mathbb{Z}$ and $i\ge 2$, consider an element a of B_1 with $a\neq 1$. If the order of a is $q^j,\ 1\le j\le i$, set

$$B_1':=\langle a^{q^{j-1}}\rangle\simeq\mathbb{Z}/q\mathbb{Z}\quad\text{and}\quad B'=B_1'\times\tau^2(B_1').$$

If $\tau(a)\in B$, then $\tau(a)=a^s\cdot\tau^2(a)^t$, $\tau(a^{q^{j-1}})=a^{q^{j-1}s}\cdot\tau^2(a)^{q^{j-1}t}\in B'$ and $0<s,t\le q^j-1$, $q\nmid s\cdot t$; by (1) this is a contradiction. We conclude that $\tau(a)\notin B$. In a similar way, we can prove that $\tau^3(a)\notin B$. ∎

Lemma 2.4. *Let $q\equiv 2$ or $3 \pmod 5$. By Lemma 2.3 we can set $B=B_1\times\tau(B_1)\times\tau^2(B_1)$. Then $B\cap\tau^3(B_1)=1$.*

Proof. (1) When $B_1\simeq\mathbb{Z}/q\mathbb{Z}$, consider an element a of B_1 with $a\neq 1$. If $\tau^3(a)\in B$, then

$$\tau^4(a)=(a\cdot\tau(a)\cdot\tau^2(a)\cdot\tau^3(a))^{-1}\in B.$$

For any element $v\in B$ with $v\neq 1$, we know that

$$v=a^s\cdot\tau(a)^t\cdot\tau^2(a)^k\quad\text{and}\quad 0\le s,t,k\le q-1.$$

It is easy to see that

$$\tau(v)\in B,\quad \tau^2(v)\in B,\quad \tau^3(v)\in B,\quad \tau^4(v)\in B.$$

The orbit of v has five elements. Therefore

$$q^3=|B|\equiv 1 \pmod 5.$$

But the order of q mod 5 is 4, a contradiction.

(2) When $B_1\simeq\mathbb{Z}/q^i\mathbb{Z}$, $i\ge 2$, for any $a\in B_1$, $a\neq 1$, if the order of a is q^j, $1\le j\le i$, set

$$B_1':=\langle a^{q^{j-1}}\rangle\simeq\mathbb{Z}/q\mathbb{Z}\quad\text{and}\quad B'=B_1'\times\tau(B_1')\times\tau^2(B_1').$$

If $\tau^3(a)\in B,\ \tau^3(a)=a^s\cdot\tau(a)^t\cdot\tau^2(a)^k$, then

$$\tau^3(a^{q^{i-1}})=a^{q^{j-1}s}\cdot\tau(a)^{q^{j-1}t}\cdot\tau^2(a)^{q^{j-1}k}\in B',\ 0<s,t,k\le q^j-1,\ q\nmid s\cdot t\cdot k.$$

By (1) this is a contradiction. Hence $\tau^3(a)\notin B$. ∎

Lemma 2.5. *A_q is the Sylow q-subgroup of the class group $\mathcal{C}l(\mathcal{O}_F)$, where F is a quintic cyclic field, and $q \neq 5$. We know that A_q is a finite abelian q-group, and*

$$A_q \simeq \bigoplus \mathbb{Z}/q^{a_i}\mathbb{Z}$$

for some integers a_i. Let f be the order of q mod 5 and let

$$n_a = \text{number of } i \text{ with } a_i = a,$$
$$r_a = \text{number of } i \text{ with } a_i \geq a.$$

Then

$$n_a \equiv r_a \equiv 0 \pmod{f}.$$

Proof. This follows from [13, Theorem 10.8]. ∎

From the above results, we can easily deduce the following.

Theorem 2.6. *Under the above notation, the following results hold:*

(1) *If $q \equiv 2$ or $3 \pmod 5$, then $A_q = B_q \times \tau(B_q) \times \tau^2(B_q) \times \tau^3(B_q)$ for some subgroup B_q of A_q.*
(2) *If $q \equiv 4 \pmod 5$, then $A_q = B_q \times \tau(B_q)$ for some subgroup B_q of A_q.*

The same results hold if we replace $\mathcal{O}_F$ by the ring $\mathcal{O}_{F,2} = \mathcal{O}_F[1/2]$ of integers of F localized at 2.

Proof. (1) It is sufficient to show that if

$$A_q \cong \mathbb{Z}/q^i\mathbb{Z} \times \mathbb{Z}/q^i\mathbb{Z} \times \cdots \times \mathbb{Z}/q^i\mathbb{Z} \tag{2.2}$$

for some $i \geq 1$, then

$$A_q = B_q \times \tau(B_q) \times \tau^2(B_q) \times \tau^3(B_q)$$

for some subgroup B_q of A_q.

When $q \equiv 2$ or $3 \pmod 5$, the order of q mod 5 is 4. Let n be the number of $\mathbb{Z}/q^i\mathbb{Z}$'s in (2.2). From Lemma 2.5 it follows that $n = 4t$ for some $t \geq 1$. Let B_1 be a subgroup of A_q with $B_1 \cong \mathbb{Z}/q^i\mathbb{Z}$. Then by Lemma 2.4,

$$A_q = B_1 \times \tau(B_1) \times \tau^2(B_1) \times \tau^3(B_1) \times A_{q1}$$

for some subgroup A_{q1} of A_q. It is easy to see that

$$A_{q1} \cong \mathbb{Z}/q^i\mathbb{Z} \times \mathbb{Z}/q^i\mathbb{Z} \times \cdots \times \mathbb{Z}/q^i\mathbb{Z}, \tag{2.3}$$

and the number of $\mathbb{Z}/q^i\mathbb{Z}$'s in (2.3) is $4(t-1)$.

Let B_2 be a subgroup of A_{q1} with $B_2 \cong \mathbb{Z}/q^i\mathbb{Z}$. Then from Lemma 2.4 we know that

$$A_{q1} = B_2 \times \tau(B_2) \times \tau^2(B_2) \times \tau^3(B_2) \times A_{q2}$$

for some subgroup A_{q2} of A_{q1}, etc. until

$$A_{q(t-1)} = B_t \times \tau(B_t) \times \tau^2(B_t) \times \tau^3(B_t),$$

where B_t is a subgroup of $A_{q(t-1)}$ with $B_t \cong \mathbb{Z}/q^i\mathbb{Z}$.

Set $B_q = B_1 \times \cdots \times B_t$. It is easy to see that

$$A_q = B_q \times \tau(B_q) \times \tau^2(B_q) \times \tau^3(B_q).$$

(2) When $q \equiv 4 \pmod 5$, the order of q mod 5 is 2, and the proof is similar to that of (1).

In a similar way, we can obtain the last statement. ∎

3. The 2-primary part of the tame kernel. For an arbitrary number field F, we have (see [12])

$$\text{2-rank}\, K_2\mathcal{O}_F = r_1 + g_2 - 1 + \text{2-rank}\, \mathcal{C}l(\mathcal{O}_{F,2}),$$

where r_1 (resp. g_2) is the number of real (resp. dyadic) places of F.

When F is a quintic cyclic field, we have

$$g_2 = \begin{cases} 1 & \text{if 2 is inert in } F, \\ 5 & \text{if 2 splits in } F. \end{cases}$$

In this case,

$$\text{(3.1)} \qquad \text{2-rank}\, K_2\mathcal{O}_F = \text{2-rank}\, \mathcal{C}l(\mathcal{O}_{F,2}) + \begin{cases} 5 & \text{if 2 is inert in } F, \\ 9 & \text{if 2 splits in } F. \end{cases}$$

Hence we have the following lemma:

LEMMA 3.1. *The* 2*-rank of* $K_2\mathcal{O}_F$ *is odd.*

Proof. From (3.1) and Theorem 2.6 we obtain 2-rank $K_2\mathcal{O}_F \equiv 1 \pmod 4$. The desired result is immediate. ∎

With the above results we can determine elements of order 2 in $K_2\mathcal{O}_F$ explicitly.

By [12, Theorem 6.3] the group $B = \{a \in F^* : \{-1, a\} = 1\}$ has the property that 2-rank$(B/F^{*2}) = 1$. Hence $B = F^{*2} \cup 2F^{*2}$.

By [3], there exists a Minkowski unit ε_1 in F such that ε_1, $\varepsilon_2 = \tau(\varepsilon_1)$, $\varepsilon_3 = \tau^2(\varepsilon_1)$, and $\varepsilon_4 = \tau^3(\varepsilon_1)$ are fundamental units of F, where τ is a generator of the Galois group $T = \mathrm{Gal}(F/\mathbb{Q})$. Changing sign if necessary, we may assume that $N\varepsilon_1 = 1$. Then

$$\{-1,-1\}, \{-1, \varepsilon_1\}, \{-1, \tau(\varepsilon_1)\}, \{-1, \tau^2(\varepsilon_1)\}, \{-1, \tau^3(\varepsilon_1)\} \in K_2\mathcal{O}_F.$$

By the last statement of Theorem 2.6, there are independent generators of the group ${}_2\mathcal{C}l(\mathcal{O}_{F,2})$ of the form $\mathcal{C}l(\mathfrak{p}_j)$, $\mathcal{C}l(\tau(\mathfrak{p}_j))$, $\mathcal{C}l(\tau^2(\mathfrak{p}_j))$, $\mathcal{C}l(\tau^3(\mathfrak{p}_j))$, $j = 1, \ldots, t$, where $4t = \text{2-rank}\, \mathcal{C}l(\mathcal{O}_{F,2})$, and $\mathfrak{p}_j$ are prime ideals satisfying $\mathfrak{p}_j \nmid 2$. It follows that $\mathfrak{p}_j^2 = (\gamma_j)$, for $j = 1, \ldots, t$. We may assume that $N\gamma_j > 0$. Then $N\gamma_j = N\mathfrak{p}_j^2 = (N\mathfrak{p}_j)^2 \in F^{*2} \in B$.

It follows that

$$\{-1, \gamma_j\}, \{-1, \tau(\gamma_j)\}, \{-1, \tau^2(\gamma_j)\}, \{-1, \tau^3(\gamma_j)\} \in K_2\mathcal{O}_F \quad \text{for } j = 1, \ldots, t.$$

If 2 splits in F, then $(2)=\mathfrak{p}\cdot\tau(\mathfrak{p})\cdot\tau^2(\mathfrak{p})\cdot\tau^3(\mathfrak{p})\cdot\tau^4(\mathfrak{p})$, and if the class $\mathcal{C}l(\mathfrak{p})$ in $\mathcal{C}l(\mathcal{O}_F)$ has order r, then $\mathfrak{p}^r$ is principal, $\mathfrak{p}^r=(\gamma)$ and $N\gamma=N(\mathfrak{p}^r)=2^r\in B$. It is easy to see that

$$\{-1,\gamma\},\{-1,\tau(\gamma)\},\{-1,\tau^2(\gamma)\},\{-1,\tau^3(\gamma)\}\in K_2\mathcal{O}_F.$$

If 2 is inert in F, consider the elements

$$\begin{aligned}&-1,\varepsilon_1,\tau(\varepsilon_1),\tau^2(\varepsilon_1),\tau^3(\varepsilon_1),\gamma_1,\tau(\gamma_1),\\&\tau^2(\gamma_1),\tau^3(\gamma_1),\dots,\gamma_t,\tau(\gamma_t),\tau^2(\gamma_t),\tau^3(\gamma_t).\end{aligned}\tag{3.2}$$

If 2 splits in F, consider the elements

$$\begin{aligned}&-1,\varepsilon_1,\tau(\varepsilon_1),\tau^2(\varepsilon_1),\tau^3(\varepsilon_1),\gamma_1,\tau(\gamma_1),\tau^2(\gamma_1),\tau^3(\gamma_1),\dots,\\&\gamma_t,\tau(\gamma_t),\tau^2(\gamma_t),\tau^3(\gamma_t),\gamma,\tau(\gamma),\tau^2(\gamma),\tau^3(\gamma).\end{aligned}\tag{3.3}$$

In both cases, the elements are multiplicatively independent modulo $B=F^{*2}\cup 2F^{*2}$, then by (3.1) we obtain the following result:

THEOREM 3.2.

(1) *If 2 is inert in F, then the elements* $\{-1,-1\},\{-1,\varepsilon_1\},\{-1,\tau(\varepsilon_1)\},\{-1,\tau^2(\varepsilon_1)\},\{-1,\tau^3(\varepsilon_1)\}$, $\{-1,\gamma_j\},\{-1,\tau(\gamma_j)\},\{-1,\tau^2(\gamma_j)\},\{-1,\tau^3(\gamma_j)\}$, *where $j=1,\dots,t$, are independent generators of the group ${}_2K_2\mathcal{O}_F$.*
(2) *If 2 splits in F, then the elements* $\{-1,-1\},\{-1,\varepsilon_1\},\{-1,\tau(\varepsilon_1)\},\{-1,\tau^2(\varepsilon_1)\},\{-1,\tau^3(\varepsilon_1)\}$, $\{-1,\gamma\},\{-1,\tau(\gamma)\},\{-1,\tau^2(\gamma)\},\{-1,\tau^3(\gamma)\},\{-1,\gamma_j\}$, $\{-1,\tau(\gamma_j)\},\{-1,\tau^2(\gamma_j)\},\{-1,\tau^3(\gamma_j)\}$, *where $j=1,\dots,t$, are independent generators of the group ${}_2K_2\mathcal{O}_F$.*

From the above we obtain

$$2\text{-rank}\,\mathcal{C}l(\mathcal{O}_F)=2\text{-rank}\,\mathcal{C}l(\mathcal{O}_{F,2})$$

when 2 is inert in F, and

$$2\text{-rank}\,\mathcal{C}l(\mathcal{O}_F)=2\text{-rank}\,\mathcal{C}l(\mathcal{O}_{F,2})+4$$

when 2 splits in F, since the class $\mathcal{C}l(\mathfrak{p})$ generates in $\mathcal{C}l(\mathcal{O}_F)$ a direct summand of an even order.

From the above discussion, we deduce the following.

THEOREM 3.3. *Let $i\geq 2$, and denote by r the 2^i-rank of $K_2\mathcal{O}_F$. Then $4\,|\,r$.*

Proof. Let c be an element of order 2^i of $K_2\mathcal{O}_F$ with $i\geq 2$. Then $b:=c^{2^{i-1}}$ is an element of order 2. Hence $b=\{-1,a\}$, where a is the product of some elements in (3.2), respectively in (3.3),

$$(3.4)\qquad a = (-1)^{k_0} \cdot \varepsilon_1^{s_1} \cdot \tau(\varepsilon_1)^{s_2} \cdot \tau^2(\varepsilon_1)^{s_3} \cdot \tau^3(\varepsilon_1)^{s_4} \cdot \gamma^{t_1} \cdot \tau(\gamma)^{t_2} \cdot \tau^2(\gamma)^{t_3} \cdot \tau^3(\gamma)^{t_4} \cdot \prod_{j=1}^{t} \gamma_j^{u_{1j}} \cdot \tau(\gamma_j)^{u_{2j}} \cdot \tau^2(\gamma_j)^{u_{3j}} \cdot \tau^3(\gamma_j)^{u_{4j}},$$

and the exponents $k_0, s_1, s_2, s_3, s_4, t_1, t_2, t_3, t_4, u_{1j}, u_{2j}, u_{3j}, u_{4j}$ are 0 or 1.

It is easy to see that $\tau(c)$, $\tau^2(c)$, $\tau^3(c)$ also have order 2^i. It is sufficient to prove that b, $\tau(b)$, $\tau^2(b)$, $\tau^3(b)$ are all distinct, or equivalently, a, $\tau(a)$, $\tau^2(a)$, $\tau^3(a)$ are multiplicatively independent modulo B.

We have proved above that the norms $N\varepsilon_1, N\gamma, N\gamma_j$ belong to B. Hence $\tau^4(\xi) \equiv (\xi \cdot \tau(\xi) \cdot \tau^2(\xi) \cdot \tau^3(\xi))^{-1} \pmod{B}$, where $\xi = \varepsilon_1, \gamma, \gamma_j$. Hence from (3.4) we get

$$(3.5)\qquad \tau(a) \equiv (-1)^{k_0} \cdot \tau(\varepsilon_1)^{s_1} \cdot \tau^2(\varepsilon_1)^{s_2} \cdot \tau^3(\varepsilon_1)^{s_3} \cdot (\varepsilon_1\tau(\varepsilon_1)\tau^2(\varepsilon_1)\tau^3(\varepsilon_1))^{-s_4} \cdot \tau(\gamma)^{t_1} \cdot \tau^2(\gamma)^{t_2} \cdot \tau^3(\gamma)^{t_3} \cdot (\gamma\tau(\gamma)\tau^2(\gamma)\tau^3(\gamma))^{-t_4} \cdot \prod_{j=1}^{t} (\tau(\gamma_j)^{u_{1j}} \cdot \tau^2(\gamma_j)^{u_{2j}} \cdot \tau^3(\gamma_j)^{u_{3j}} \cdot (\gamma_j\tau(\gamma_j)\tau^2(\gamma_j)\tau^3(\gamma_j))^{-u_{4j}}) \pmod{B}.$$

If $\tau(a) \equiv a \pmod{B}$, then by the multiplicative independence of the elements modulo B, they must appear in (3.4) and (3.5) with exponents of the same parity. Therefore,

$$\begin{cases} s_1 \equiv -s_4 \pmod{2}, \\ s_2 \equiv s_1 - s_4 \pmod{2}, \\ s_3 \equiv s_2 - s_4 \pmod{2}, \\ s_4 \equiv s_3 - s_4 \pmod{2}. \end{cases}$$

From an easy computation we get

$$s_1 \equiv s_2 \equiv s_3 \equiv s_4 \equiv 0 \pmod{2}.$$

In the same way we get

$$t_1 \equiv t_2 \equiv t_3 \equiv t_4 \equiv 0 \pmod{2},$$
$$u_{1j} \equiv u_{2j} \equiv u_{3j} \equiv u_{4j} \equiv 0 \pmod{2}.$$

That is, $a \in B,\ b = 1$. Since b is an element of order 2, this is a contradiction. Hence $\tau(b) \neq b$.

In a similar way we can show that

$$b \neq \tau^2(b), \quad b \neq \tau^3(b), \quad \tau(b) \neq \tau^2 b, \quad \tau(b) \neq \tau^3 b, \quad \tau^2(b) \neq \tau^3 b.$$

It is easy to see that $c, \tau(c), \tau^2(c), \tau^3(c)$ are all distinct. This proves the desired result. ∎

THEOREM 3.4. *If there are k elements in the set $\{\varepsilon_1, \gamma, \gamma_j : 1 \le j \le t\}$ which are not totally positive*, *then*

$$4\text{-rank}\, K_2\mathcal{O}_F \le 2\text{-rank}\, K_2\mathcal{O}_F - (4k+1).$$

Proof. If an element $\beta \in F^*$ is not totally positive, then applying the five real Hilbert symbols of F to $\{-1,\beta\}$, we conclude that $\{-1,\beta\}$ is not a square in K_2F. In particular, $\{-1,-1\}$ is not a square. If β is not totally positive, then $\tau(\beta)$, $\tau^2(\beta)$ and $\tau^3(\beta)$ are also not totally positive. The desired result follows. ■

4. The q-primary parts of tame kernels for an odd prime q

4.1. *Notation.* In this section, we use the same notation as in [1]. Let q be an odd prime number, ζ_q a primitive qth root of unity, and $G := \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. Then

$$G = \{\sigma_a : 1 \le a \le q-1\},$$

where $\sigma_a(\zeta_q) = \zeta_q^a$. The mapping $(\mathbb{Z}/q)^* \to G$, $a \mapsto \sigma_a$, is an isomorphism. For a fixed primitive root h modulo q, the automorphism $\sigma := \sigma_h$ generates G.

Let ω be the q-adic Teichmüller character of the group $(\mathbb{Z}/q)^*$. Then, for $1 \le a \le q-1$, the value $\omega(a) \in \mathbb{Z}_q^*$ is uniquely determined by the conditions $\omega(a)^{q-1} = 1$ and $\omega(a) \equiv a \pmod{q}$. It is well known that, for $0 \le j \le q-2$, ω^j are all irreducible characters of $G = (\mathbb{Z}/q)^*$. The corresponding primitive idempotents of the group ring $\mathbb{Z}_q[G]$ are

$$\varepsilon_j = \frac{1}{q-1}\sum_{a=1}^{q-1} \omega(a)^j \sigma_a^{-1} = \frac{1}{q-1}\sum_{k=0}^{q-2} \omega(h)^{kj}\sigma^{-k}, \qquad 0 \le j \le q-2. \tag{4.1}$$

In particular, $\varepsilon_0 = \frac{1}{q-1}N$, where $N = 1 + \sigma + \sigma^2 + \dots + \sigma^{q-2} = N_{\mathbb{Q}(\zeta_q)/\mathbb{Q}}$ is the norm element in the group ring $\mathbb{Z}_q[G]$.

For a $\mathbb{Z}_q[G]$-module M we have

$$\varepsilon_j M = \{m \in M : \sigma_a(m) = \omega(a)^j m\},$$

and we obtain a decomposition of M into a direct sum of $\mathbb{Z}_q[G]$-submodules:

$$M = \bigoplus_{j=0}^{q-2} \varepsilon_j M = NM \oplus \bigoplus_{j=1}^{q-2} \varepsilon_j M.$$

The group μ_p of qth roots of unity has the natural structure of a $\mathbb{Z}_q[G]$-module. We define the action of G on $\mu_q \otimes M$ by

$$(\zeta \otimes m)^\tau = \zeta^\tau \otimes m^\tau, \quad \text{where } \zeta \in \mu_q,\ m \in M,\ \tau \in G.$$

Obviously,

$$(\mu_q \otimes M)^G = \varepsilon_0(\mu_q \otimes M). \tag{4.2}$$

By [1] we have

$$\varepsilon_0(\mu_q \otimes M) = \mu_q \otimes \varepsilon_{q-2} M. \tag{4.3}$$

4.2. *The q-rank of $K_2\mathcal{O}_F$.* In the following we always assume that $E = F(\zeta_q)$, and q does not ramify in F, where F is a quintic cyclic field. Denote by $\lambda : \mathcal{C}l(\mathcal{O}_E) \to \mathcal{C}l(\mathcal{O}_E[1/q])$ the homomorphism induced by the imbedding $\mathcal{O}_E \to \mathcal{O}_E[1/q]$, and let $A = A_E$ be the Sylow q-subgroup of $\mathcal{C}l(\mathcal{O}_E)$. Then, by the surjectivity of λ, $\lambda(A)$ is the Sylow q-subgroup of $\mathcal{C}l(\mathcal{O}_E[1/q])$.

Since A is a q-group on which $G = \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q}) = \mathrm{Gal}(E/F)$ acts, we have

$$A = \bigoplus_{j=0}^{q-2} \varepsilon_j A.$$

LEMMA 4.1. *For $j \neq 0$ the mapping $\lambda : \varepsilon_j A \to \varepsilon_j \lambda(A)$ is an isomorphism.*

Proof. See the proof of [1, Lemma 4.1]. ■

LEMMA 4.2. *Let S' be the set of ideals of F which divide q and which split completely in $E = F(\zeta_q)$. Then S' is empty.*

Proof. Since the extension $F/\mathbb{Q}$ is of odd degree, the result follows from [1, Lemma 4.2]. ■

THEOREM 4.3. *Let $E = F(\zeta_q)$. Then*

$$q\text{-rank}\, K_2\mathcal{O}_F = q\text{-rank}\, \varepsilon_{q-2} A_E.$$

Proof. There is an exact sequence

$$0 \to (\mu_q \otimes \mathcal{C}l(\mathcal{O}_E[1/q]))^G \to K_2\mathcal{O}_F/q \to \mu_q^{S'} \to 0$$

(see [7, Theorem 5.4] and [4]). By (4.2), (4.3) and Lemma 4.1 we conclude that

$$(\mu_q \otimes \mathcal{C}l(\mathcal{O}_E[1/q]))^G = \mu_q \otimes \varepsilon_{q-2} A.$$

The proof is completed by applying Lemma 4.2. ■

THEOREM 4.4. *Let F be a quintic cyclic field and let τ be a generator of the Galois group* $\mathrm{Gal}(F/\mathbb{Q})$. *Then the following results hold.*

(1) *If* $q \equiv 7 \pmod{10}$ *or* $q \equiv 3 \pmod 5$,

$$4 \mid q^i\text{-rank}\, K_2\mathcal{O}_F, \qquad i > 0.$$

(2) *If* $q \equiv 4 \pmod 5$, *then*

$$2 \mid q^i\text{-rank}\, K_2\mathcal{O}_F, \qquad i > 0.$$

Proof. (1) It is easy to see that the order of q mod 5 is 4. Let B be the Sylow q-subgroup of $K_2\mathcal{O}_F$ and set $V = B^{l^{i-1}}/B^{l^i}$. Define $r_i = q^i\text{-rank}\, K_2\mathcal{O}_F$.

Then $r_i = \dim_{\mathbb{Z}/q\mathbb{Z}} V$ and V has q^{r_i} elements. Let v be any element of V with $v \neq 1$. If $\tau(v) = v$, then

$$v^5 = v\tau(v)\tau^2(v)\tau^3(v)\tau^4(v) = j(\mathrm{tr}(v)),$$

where j is induced by the inclusion $\mathbb{Q} \subset F$ and tr is the transfer homomorphism of K_2. It is well known that $K_2\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z}$. Therefore, $v^5 = 1$. But $q \nmid 5$, hence $v = 1$, a contradiction. It follows that the orbit of every $v \neq 1$ has five elements, hence $q^{r_i} \equiv 1 \pmod 5$. Therefore $4 \mid r_i$.

(2) In this case, the order of q mod 5 is 2, and the result follows from the proof of (1). ■

THEOREM 4.5. *Under the same assumption as in Theorem* 4.4, *the following results hold.*

(1) *If* $q \equiv 7 \pmod{10}$ *or* $q \equiv 3 \pmod 5$, *then*

$$\mathrm{Syl}_q(K_2\mathcal{O}_F) = A' \times \tau(A') \times \tau^2(A') \times \tau^3(A')$$

for some subgroup A' *of the Sylow* q*-subgroup of* $K_2\mathcal{O}_F$.

(2) *If* $q \equiv 4 \pmod 5$, *then*

$$\mathrm{Syl}_q(K_2\mathcal{O}_F) = A' \times \tau(A')$$

for some subgroup A' *of the Sylow* q*-subgroup of* $K_2\mathcal{O}_F$.

Proof. The result follows easily from the proofs of Theorem 4.4, and of Lemmas 2.2–2.4. ■

Let $E' = \mathbb{Q}(\zeta_q)$, and denote by A' the Sylow q-subgroup of $\mathcal{C}l(\mathcal{O}_{E'}) = \mathcal{C}l(\mathbb{Z}[\zeta_q])$. By the theorems of Herbrand and Ribet (see [6, Chapter 15, §3]), we know that $\varepsilon_{q-2}A' = 1$ for every odd prime number q.

THEOREM 4.6.

(1) *If* $q \equiv 7 \pmod{10}$ *or* $q \equiv 3 \pmod 5$, *and* $\varepsilon_j A' = 1$ *for some* j *with* $0 \le j \le q-2$, *then*

$$4 \mid q^i\text{-rank}\, \varepsilon_j A, \quad i > 0.$$

In particular, 4 *divides the* q^i-rank *of* $\varepsilon_{q-2}A$.

(2) *If* $q \equiv 4 \pmod 5$, *and* $\varepsilon_j A' = 1$ *for some* j *with* $0 \le j \le q-2$, *then*

$$2 \mid q^i\text{-rank}\, \varepsilon_j A, \quad i > 0.$$

In particular, 2 *divides the* q^i-rank $\varepsilon_{q-2}A$.

Proof. (1) Let τ be a generator of the Galois group $T := \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}(\zeta_q))$. Since $q \neq p$, it follows that σ and τ commute, and consequently T acts on the group $\varepsilon_j A$ for all j with $0 \le j \le q-2$. Since the order of q mod 5 is 4, and $N_{E/\mathbb{Q}(\zeta_p)}(\varepsilon_j A) \subseteq \varepsilon_j A' = 1$, by the proof of [13, Theorem 10.8] the result is immediate. The last assertion follows from $\varepsilon_{q-2}A' = 1$; then by Theorem 4.3 we also conclude that 4 divides the q-rank of $K_2\mathcal{O}_F$.

(2) The proof is similar to that of (1). By the last statement and Theorem 4.3, we also find that 2 divides q-rank $K_2\mathcal{O}_F$. ∎

4.3. *Reflection theorems.* In this section we apply reflection theorems to prove some estimates of q-rank $K_2\mathcal{O}_F$. We extend the above notation as follows.

Let L be the maximal unramified and elementary abelian q-extension of E with the Galois group $H := \mathrm{Gal}(L/E)$. Then the Artin reciprocity map gives an isomorphism of G-modules $A/q \to H$.

By Kummer theory, $L = E(B^{1/q})$, where B is a subgroup of E^* containing E^{*q}. Set $B_0 := B/E^{*q}$. Let $b \in B_0$ (or more accurately $b \bmod E^{*q} \in B_0$). Since $E(b^{1/q})/E$ is unramified, $(b) = \mathfrak{a}^q$ for some ideal $\mathfrak{a}$ of $\mathcal{O}_E$ ([13, Exercise 9.1]). Changing b by adding an element of E^{*q} leaves the ideal class of $\mathfrak{a}$ unchanged. Moreover, B_0 is isomorphic to the dual $\widehat{H}$ of H as a G-module. Therefore we have a homomorphism of G-modules

$$\varphi : B_0 \to {}_qA = \{a \in A : a^q = 1\},$$

such that $\varphi(bE^{*q}) = \mathcal{C}l(\mathfrak{a})$.

THEOREM 4.7 (see [2, Theorem 3.1]).

$$q\text{-rank}\,\varepsilon_j A = q\text{-rank}\,\varepsilon_{q-j} B_0.$$

Let U_E be the group of units of $\mathcal{O}_E$, and denote by U'_E its subgroup of units u satisfying

$$u \equiv x^q \pmod{q(1-\zeta_q)}$$

for some $x \in \mathcal{O}_E$. Such an element u is called a *singular primary unit*. It is easy to see that $U_E^q \subseteq U'_E$, and by [2, (3.1)] we know that $\ker\varphi = U'_E/U_E^q$.

THEOREM 4.8. *We have*

$$q\text{-rank}\,\varepsilon_2(U'_E/U_E^q) \le q\text{-rank}\,K_2\mathcal{O}_F \le q\text{-rank}\,\varepsilon_2 A_E + q\text{-rank}\,\varepsilon_2(U'_E/U_E^q).$$

Proof. See the proof of [1, Theorem 5.3]. ∎

Theorem 4.8 gives some estimates of the q-rank of $K_2\mathcal{O}_F$ in terms of the q-rank of some subgroups of the class group and of the group of singular primary units (modulo qth powers) of the field $E = F(\zeta_q)$. Unfortunately, for large prime numbers q, the degree of $E/\mathbb{Q}$, equal to $5(q-1)$, is large, and it is difficult to determine its class group and the group of units, and the action of the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ on them. We are going to show that in certain cases E can be replaced by its proper subfields.

For a fixed primitive root h modulo q set $\omega(h) = \zeta_{q-1} \in \mathbb{Z}_q^*$, and $t = (q-1)/2$. Then σ^t is the complex conjugation on E and $N_{E/E^+} = 1 + \sigma^t$, where E^+ is the maximal real subfield of E.

Lemma 4.9 (see [1, Lemma 5.4]). *Under the above notation we have*

$$\varepsilon_2 = \varrho \cdot N_{E/E^+} \quad \text{for some } \varrho \in \mathbb{Z}_q[G].$$

Suppose that $q \equiv 1 \pmod{10}$, and let

$$\eta_j := \frac{1}{5}\sum_{l=0}^{4} \zeta_5^{lj}\tau^{-l} \quad \text{for } j = 0,1,2,3,4,$$

where τ is a generator of $T = \mathrm{Gal}(F/\mathbb{Q}) = \mathrm{Gal}(E/\mathbb{Q}(\zeta_q))$. Then η_0, η_1, η_2, η_3, η_4 are primitive idempotents of the group ring $\mathbb{Z}_q[T]$. Hence

$$\varepsilon_2 = \sum_{j=0}^{4} \varepsilon_2\eta_j \tag{4.4}$$

in the group ring $\mathbb{Z}_q[G \times T]$. Set $r = (q-1)/10$. For $j = 0,1,2,3,4$, let T_j be the subgroup of $G \times T$ generated by σ_t and $\sigma^{rj}\tau^{-1}$, and denote by E_j the subfield of E which is fixed by T_j. Then $\#T_j = 10$, $E_j \subseteq E^+$, and $(E_j : \mathbb{Q}) = (q-1)/2 = t$. In particular, $E_0 = E^{\langle\sigma^t,\tau^{-1}\rangle} = \mathbb{Q}(\zeta_q)^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_q)$.

Lemma 4.10. *Under the above notation we have*

$$\varepsilon_2\eta_j = \varrho_j \cdot N_{E/E_j}$$

for $j = 0,1,2,3,4$ *and some* $\varrho_j \in \mathbb{Z}_q[G \times T]$.

Proof. From the computation used in [1, Lemma 5.5] we easily obtain

$$\varepsilon_2\eta_j = \frac{1}{5(q-1)}\Big(\sum_{m=0}^{r-1} \zeta_{5r}^{m}\sigma^{-m}\Big)\Big(\sum_{j=0}^{4} \zeta_5^{j}\sigma^{-rj}\Big) \cdot N_{E/E_j}. \ \blacksquare$$

For every subfield L of E we define U'_L to be the group of singular primary units in L. Then

$$U'_L = U'_E \cap L \quad \text{and} \quad N_{E/L}U'_E \subseteq U'_L.$$

By the proof of Lemma 5.6 in [1], the natural inclusion $U'_L \to U'_E$ induces an injection

$$U'_L/U^q_L \to U'_E/U^q_E \quad \text{for } q > 5.$$

From the above we get inclusions of elementary abelian q-groups

$$N_{E/L}(U'_E/U^q_E) \subseteq U'_L/U^q_L \subseteq U'_E/U^q_E,$$

hence, acting by ε_2, we obtain

$$q\text{-rank}\,\varepsilon_2 N_{E/L}(U'_E/U^q_E) \le q\text{-rank}\,\varepsilon_2(U'_L/U^q_L) \le q\text{-rank}\,\varepsilon_2(U'_E/U^q_E). \tag{4.5}$$

Lemma 4.11. *Let* L_1, L_2, L_3, L_4 *be subfields of* E, *and set* $L_0 = L_2L_3L_4 \cap L_1$. *Suppose that* L_1, L_2, L_3, L_4 *are proper subfields of* $L_1L_2L_3L_4$, *and that*

$$U'_{L_{i_1}L_{i_2}L_{i_3}\cap L_{i_4}}/U^q_{L_{i_1}L_{i_2}L_{i_3}\cap L_{i_4}} = 1 \quad \text{for } \{i_1,i_2,i_3,i_4\} = \{1,2,3,4\}.$$

Then the mapping

$$U'_{L_1}/U^q_{L_1} \times U'_{L_2}/U^q_{L_2} \times U'_{L_3}/U^q_{L_3} \times U'_{L_4}/U^q_{L_4} \to U'_{L_1L_2L_3L_4}/U^q_{L_1L_2L_3L_4}$$

given by $(u_1, u_2, u_3, u_4) \mapsto u_1u_2u_3u_4$ *is injective.*

Proof. Suppose that $u_1 \in U'_{L_1}$, $u_2 \in U'_{L_2}$, $u_3 \in U'_{L_3}$, $u_4 \in U'_{L_4}$ satisfy

$$(4.6) \qquad u_1u_2u_3u_4 = u^q \quad \text{for some } u \in U_{L_1L_2L_3L_4}.$$

Let $r = (L_1L_2L_3L_4 : L_1) \mid (E : \mathbb{Q}) = 5(q-1)$. We have

$$\begin{aligned}
&N_{L_1L_2L_3L_4/L_1}(u_1) = u_1^r,\\
&N_{L_1L_2L_3L_4/L_1}(u_2) = N_{L_2L_3L_4/L_0}(u_2) \in U'_{L_0} = U^q_{L_0} \subseteq U^q_{L_1},\\
&N_{L_1L_2L_3L_4/L_1}(u_3) = N_{L_2L_3L_4/L_0}(u_3) \in U'_{L_0} = U^q_{L_0} \subseteq U^q_{L_1},\\
&N_{L_1L_2L_3L_4/L_1}(u_4) = N_{L_2L_3L_4/L_0}(u_4) \in U'_{L_0} = U^q_{L_0} \subseteq U^q_{L_1},\\
&N_{L_1L_2L_3L_4/L_1}(u^q) = (N_{L_1L_2L_3L_4/L_1}(u))^q \subseteq U^q_{L_1}.
\end{aligned}$$

Consequently, from (4.6), we know that $u_1^r \in U^q_{L_1}$, so $u_1 \in U^q_{L_1}$, since $q \nmid r$. In a similar way we get $u_2 \in U^q_{L_2}$, $u_3 \in U^q_{L_3}$, $u_4 \in U^q_{L_4}$. Hence the mapping under consideration is injective. ∎

By Lemma 4.11 the restricted mapping

$$\varepsilon_2(U'_{L_1}/U^q_{L_1}) \times \varepsilon_2(U'_{L_2}/U^q_{L_2}) \times \varepsilon_2(U'_{L_3}/U^q_{L_3}) \times \varepsilon_2(U'_{L_4}/U^q_{L_4}) \to \varepsilon_2(U'_{L_1L_2L_3L_4}/U^q_{L_1L_2L_3L_4})$$

is injective. Hence, under the assumption of Lemma 4.11, we have

$$(4.7) \qquad \sum_{j=1}^{4} q\text{-rank}\, \varepsilon_2(U'_{L_j}/U^q_{L_j}) \le q\text{-rank}\, \varepsilon_2(U'_{L_1L_2L_3L_4}/U^q_{L_1L_2L_3L_4}) \le q\text{-rank}\, \varepsilon_2(U'_E/U^q_E).$$

Combining (4.4), (4.5), (4.7), Theorem 4.8, Lemma 4.10 and the proof of [1, Theorem 5.8], we obtain the following result.

THEOREM 4.12. *Let E_j be the subfield of E fixed by the group*

$$T_j = \langle \sigma^{rj}\tau^{-1}, \sigma^t \rangle, \quad j = 0, 1, 2, 3, 4.$$

Then

$$\max_{0\le j\le 4} q\text{-rank}\, \varepsilon_2(U'_{E_j}/U^q_{E_j}) \le q\text{-rank}\, K_2\mathcal{O}_F \le \sum_{j=0}^{4} q\text{-rank}\, \varepsilon_2 A_{E_j} + \sum_{j=0}^{4} q\text{-rank}\, \varepsilon_2(U'_{E_j}/U^q_{E_j}).$$

Moreover, if $U'_{E_{i_1}E_{i_2}E_{i_3}\cap E_{i_4}}/U^q_{E_{i_1}E_{i_2}E_{i_3}\cap E_{i_4}} = 1$ *for* $\{i_1, i_2, i_3, i_4\} = \{1, 2, 3, 4\}$, *and the class number of the field* $\mathbb{Q}(\zeta_q)$ *is not divisible by* q, *then*

$$\sum_{j=1}^{4} q\text{-rank}\,\varepsilon_2(U'_{E_j}/U^q_{E_j}) \le q\text{-rank}\,K_2\mathcal{O}_F \le \sum_{j=1}^{4} q\text{-rank}\,\varepsilon_2 A_{E_j} + \sum_{j=1}^{4} q\text{-rank}\,\varepsilon_2(U'_{E_j}/U^q_{E_j}).$$

5. Orders of tame kernels. In this section, we assume that in F there is only one ramified prime p, $p \equiv 1 \pmod{10}$. We know that F is the unique quintic subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$.

By the Birch–Tate conjecture, we can compute $\#K_2\mathcal{O}_F$. The conjecture states that whenever M is a totally real number field,

$$\#K_2\mathcal{O}_M = \omega_2(M)|\zeta_M(-1)|, \tag{5.1}$$

where ζ_M is the Dedekind zeta function of the field M, and

$$\omega_2(M) = 2\prod_{l\,\text{prime}} l^{n_l},$$

where n_l is the largest integer n such that M contains $Q(\zeta_{l^n} + \zeta_{l^n}^{-1})$, the maximal real subfield of $Q(\zeta_{l^n})$. The conjecture is known to be true when M is abelian over $\mathbb{Q}$ and is known to be true in general up to a power of 2. (See [8], [9] and [14].)

Let M^+ denote the maximal real subfield of a number field M. For every quintic cyclic field F, we have $\omega_2(F) = 24$, with one exception:

$$\omega_2(F) = 5\cdot 24 \quad \text{for } F = \mathbb{Q}(\zeta_{11})^+.$$

Now, we return to quintic cyclic fields F with only one ramified prime $p > 11$. In the following, we use two methods to compute $|\zeta_F(-1)|$.

1) The Dedekind zeta function $\zeta_F(s)$ of the field F is defined by the Euler product

$$\zeta_F(s) = \left(1-\frac{1}{p^s}\right)^{-1}\prod_{q\,\text{splits}}\left(1-\frac{1}{q^s}\right)^{-5}\prod_{q\,\text{is inert}}\left(1-\frac{1}{q^{5s}}\right)^{-1}. \tag{5.2}$$

From simple computations, it can be seen that $|d(F)| = p^4$ and $\Gamma(-1/2) = -2\sqrt{\pi}$. By the functional equation we obtain

$$|\zeta_F(-1)| = \left|-\frac{p^6}{32\pi^{10}}\,\zeta_F(2)\right|.$$

Consequently,

$$\#K_2\mathcal{O}_F = \frac{3p^6}{4\pi^{10}}\,\zeta_F(2).$$

From (5.2) we know that $1 < \zeta_F(2) < \zeta(2)^5$, where $\zeta(s)$ is the Riemann zeta function. Hence

$$\frac{3}{4\pi^{10}}\, p^6 < \#K_2\mathcal{O}_F < \frac{1}{2^7 \cdot 3^4}\, p^6. \tag{5.3}$$

2) The Dedekind zeta function of an abelian number field F is the product of L-series:

$$\zeta_F(s) = \prod_{\chi} L(s,\chi),$$

where χ runs through the linear characters of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$.

Let g be a primitive root modulo p. Then the subgroup $H = \langle g^5\rangle$ of the group $(\mathbb{Z}/p)^* = \langle g\rangle$ has index 5, and there are four nontrivial cosets g^jH for $j = 1, 2, 3, 4$.

In our case, there are four nontrivial Dirichlet characters χ_j, where

$$\chi_j(a) = \begin{cases} \zeta_5^{jk} & \text{if } a \pmod{p} \in g^kH,\ k = 0,1,2,3,4,\\ 0 & \text{if } p \mid a. \end{cases}$$

Hence,

$$\zeta_F(s) = \zeta(s)\prod_{j=1}^{4} L(s,\chi_j).$$

The generalized Bernoulli number $B_{2,\chi}$ corresponding to a Dirichlet character χ of conductor f is defined by

$$B_{n,\chi} = f^{n-1}\sum_{j=1}^{f}\chi(j)B_n\left(\frac{j}{f}\right),$$

where $B_n(X)$ is the nth Bernoulli polynomial.

Applying the formula (see [13, Theorem 4.2])

$$L(-1,\chi) = -B_{2,\chi}/2,$$

and $\zeta(-1) = -1/12$, we get

$$\zeta_F(-1) = -\frac{1}{192}\prod_{j=1}^{4} B_{2,\chi_j}.$$

Hence

$$\#K_2\mathcal{O}_F = \frac{1}{8}\prod_{j=1}^{4} B_{2,\chi_j}.$$

It is easy to compute B_{2,χ_j} (see [13, Exercise 4.2(a)]):

$$B_{2,\chi_j} = \frac{1}{p}\sum_{i=1}^{p}\chi_j(i)i^2.$$

For $k = 0,1,2,3,4$, we define $T_k := \{i : 1 \le i \le p-1,\ i \pmod p \in g^k H\}$ and

$$S_k := \frac{1}{p}\sum_{i\in T_k} i^2.$$

Since $i \in T_k$ iff $i \equiv g^{5r+k} \pmod p$ for some r with $0 \le r \le (p-6)/5$, it follows that

$$\sum_{i\in T_k} i^2 = g^{2k}\sum_{r=0}^{(p-6)/5} g^{10r} = g^{2k}\,\frac{1-g^{2(p-1)}}{1-g^{10}} \equiv 0 \pmod p,$$

since $g^{p-1} \equiv 1 \pmod p$. Thus the S_k are integers, and in the ring $\mathbb{Z}[\zeta_5]$ we have the congruence

$$B_{2,\chi_j} \equiv S_0+S_1+S_2+S_3+S_4 \pmod{(1-\zeta_5)}.$$

Consequently,

$$8\#K_2\mathcal{O}_F = \prod_{j=1}^{4} B_{2,\chi_j} \equiv (S_0+S_1+S_2+S_3+S_4)^4 \pmod{(1-\zeta_5)}.$$

Since both sides of the congruence are integers, we get

$$\begin{aligned} 8\#K_2\mathcal{O}_F &\equiv (S_0+S_1+S_2+S_3+S_4)^4 \pmod 5 \\ &\equiv \left(\frac{p-1}{6}(2p-1)\right)^4 \pmod 5. \end{aligned} \tag{5.4}$$

THEOREM 5.1. *If* $p \equiv 1 \pmod{10}$, *then* $5 \mid \#K_2\mathcal{O}_F$.

Proof. When $p = 11$, since $\omega_2(F) = 5\cdot 24$, from (5.1) we know that $5 \mid \#K_2\mathcal{O}_F$.

When $p > 11$, since $p \equiv 1 \pmod{10}$, from (5.4) we see that $5 \mid \#K_2\mathcal{O}_F$. ∎

THEOREM 5.2.

$$\lim_{p\to\infty} \#K_2\mathcal{O}_F = \infty.$$

Proof. This follows from (5.3). ∎

References

[1] J. Browkin, *Tame kernels of cubic cyclic fields*, Math. Comp. 74 (2005), 967–999.

[2] —, *On the p-rank of the tame kernel of algebraic number fields*, J. Reine Angew. Math. 432 (1992), 135–149.

[3] A. Brumer, *On the group of units of an absolutely cyclic number field of prime degree*, J. Math. Soc. Japan 21 (1969), 357–358.

[4] M. Geijsberts, *The tame kernel, computational aspects*, Ph.D. thesis, Catholic Univ. of Nijmegen, 1991.

[5] X. Guo and H. Qin, *The 3-adic regulators and wild kernels*, J. Algebra 312 (2007), 418–425.

[6] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, 1982.
[7] F. Keune, *On the structure of the K_2 of the ring of integers in a number field*, K-Theory 2 (1989), 625–645.
[8] M. Kolster, *A relation between the 2-primary parts of the main conjecture and the Birch–Tate conjecture*, Canad. Math. Bull. 32 (1989), 248–251.
[9] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.
[10] H. Qin, *Reflection theorems and the p-Sylow subgroup of $K_2\mathcal{O}_F$ for a number field F*, preprint.
[11] H. Qin and H. Zhou, *The 3-Sylow subgroup of the tame kernel of real number fields*, J. Pure Appl. Algebra 209 (2007), 245–253.
[12] J. Tate, *Relations between K_2 and Galois cohomology*, Invent. Math. 36 (1976), 257–274.
[13] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1982.
[14] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. (2) 131 (1990), 493–540.
[15] H. Y. Zhou, *Tame kernels of cubic cyclic fields*, Acta Arith. 124 (2006), 293–313.

Department of Mathematics
Nanjing University
Nanjing 210093, China
E-mail: xiaxia80@gmail.com

Received on 2.2.2008
and in revised form on 28.3.2008 (5628)