ACTA ARITHMETICA
136.3 (2009)

Tame kernels of cyclic extensions of number fields

by

HAIYAN ZHOU (Nanjing)

1. Introduction. Let F be an algebraic number field, $\mathcal{O}_F$ the ring of integers in F and K_2 the Milnor K-functor. For an odd prime p, results on the p-primary part of tame kernels of number fields can be found in [Br1], [Br2], [Gu], [Ke], [Ko], [Qi], [Wu], [Zh1] and [Zh2]. For $m \geq 1$, it is of interest to find the value of p^m- rank $K_2\mathcal{O}_F$. However, even for $m = 1$, we do not know this value in general. In this paper we investigate the p^m-rank of the tame kernel $K_2\mathcal{O}_E$ for a cyclic extension E/F of number fields of degree n with $p \nmid n$. As applications, for $E/\mathbb{Q}$ being a cyclic extension of odd prime order l, we obtain some results on the divisibility of p^m- rank $K_2\mathcal{O}_E$ that generalize results for $l = 3, 5$ proved in [Br1], [Zh1] and [Wu]. For a cyclotomic field $\mathbb{Q}(\zeta_l)$, we investigate the divisibility of the orders of $K_2\mathcal{O}_{\mathbb{Q}(\zeta_l)}$ for $l < 2000$ and $l \equiv 3 \pmod 4$.

We use the following notation, terminology and general facts. F_v denotes the completion of F with respect to the valuation v, and μ_v is the group of roots of unity in F_v. It is well-known that $K_2\mathcal{O}_F$ is the kernel of the homomorphism $\tau : K_2F \to \coprod \overline{F_v^*}$, v running through discrete valuations of F, where τ satisfies $\tau(\{\alpha, \beta\}) = ((\alpha, \beta)_v)_v$. Here $(\ ,\ )_v$ is the tame symbol, as defined in [Mi]. Let E/F be a number field extension. Denote by $\mathrm{tr}_{E/F}$ the transfer homomorphism $\mathrm{tr}_{E/F} : K_2(E) \to K_2(F)$, and by $j_{E/F}$ the natural homomorphism $j_{E/F} : K_2(F) \to K_2(E)$ induced by the inclusion $F \subseteq E$.

Let G be a finite group and A a finite abelian group which is a G-module. Let $x \in A$. The stabilizer of x is denoted by G_x and the G-orbit of x by Gx, that is,
$$G_x = \{\sigma \in G \mid \sigma x = x\}, \qquad Gx = \{\sigma x \in A \mid \sigma \in G\}.$$
For H a subgroup of G we set $N_H = \sum_{h\in H} h \in \mathbb{Z}[G]$. Let E/F be a Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then we write $N_G = N_{E/F}$. Therefore, we have $j_{E/F}\,\mathrm{tr}_{E/F} = N_G$ (see [Ke, (4.5)]). Since $j_{E/F} : K_2(F) \to$

2000 *Mathematics Subject Classification*: 11R70, 11R20, 19F99.
Key words and phrases: number fields, cyclic extension, tame kernels.

DOI: 10.4064/aa136-3-5

$K_2(E)$ and $\mathrm{tr}_{E/F}: K_2(E) \to K_2(F)$ can be restricted to the groups $K_2\mathcal{O}_E$ and $K_2\mathcal{O}_F$, the equality $j_{E/F}\,\mathrm{tr}_{E/F} = N_G$ holds for these groups as well.

Let p be a prime and $(A)_p$ the p-primary part of A. Suppose that A is a p-group and m is a positive integer. Then p^m-rank A is defined to be $\dim_{\mathbb{Z}/p\mathbb{Z}}(A^{p^{m-1}}/A^{p^m})$. Set $A(p^m) = \{a \in A \mid p^m a = 0\}$. Obviously, also p^m-rank $A = p$-rank $A(p^m)/A(p^{m-1})$. In this paper, we define

$$M_E = K_2\mathcal{O}_E(p^m)/K_2\mathcal{O}_E(p^{m-1}) \quad \text{and} \quad M_F = K_2\mathcal{O}_F(p^m)/K_2\mathcal{O}_F(p^{m-1}).$$

For an integer $n > 1$ prime to p, denote by $o(n,p)$ the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^*$, and by $c(n,p)$ the greatest common divisor of $o(l,p)$ for all prime factors l of n.

2. p^m-Rank of the tame kernel

LEMMA 1. *Let G be a finite cyclic group, and A and B be finite G-modules with $(|A|,|G|) = 1$. If $0 \to A \to B$ is an exact sequence of G-modules, then $(B/A)^G = B^G/A^G$.*

Proof. Clearly, $0 \to A \to B \to B/A \to 0$ is an exact sequence of G-modules. Then by [Ne, Chapter I, Proposition 3.1] we have the exact sequence

$$0 \to A^G \to B^G \to (B/A)^G \to H^1(G,A).$$

From [Ne, Chapter I, Propositions 4.3 and 4.4], it is easy to obtain $|H^1(G,A)| = |H^0(G,A)|$. We have $|H^0(G,A)| = 1$ since $(|A|,|G|) = 1$. So

$$0 \to A^G \to B^G \to (B/A)^G \to 0$$

is an exact sequence. Obviously, $B^G/A^G \subset (B/A)^G$. This proves the result.

LEMMA 2 ([Zh2, Lemma 4]). *Let E/F be a Galois extension with Galois group G of order n and $p \nmid n$. For any intermediate field K, the homomorphism $j: (K_2\mathcal{O}_K)_p \to (K_2\mathcal{O}_E)_p$ is injective. We identify $(K_2\mathcal{O}_K)_p$ with its image in $(K_2\mathcal{O}_E)_p$. Let $H \subseteq G$ be a subgroup. Then $(K_2\mathcal{O}_E)_p^H = (K_2\mathcal{O}_{E^H})_p$.*

PROPOSITION 1. *Let E/F be a cyclic extension of degree n prime to p and $G = \mathrm{Gal}(E/F)$. Then $N_G M_E = j_{E/F} M_F$ and $M_E = j_{E/F} M_F \oplus \mathrm{Ker}\, N_G$.*

Proof. Note the inclusion map $0 \to K_2\mathcal{O}_E(p^{m-1}) \to K_2\mathcal{O}_E(p^m)$ and $N_G: M_E \to M_E$. Since $(n,p) = 1$, we have $N_G M_E = M_E^G$. The first equality follows from Lemmas 1 and 2. It follows from the assumption that there exists an $a \in \mathbb{Z}$ such that $an \equiv 1 \pmod{|M_F|}$. Let $x \in j_{E/F} M_F \cap \mathrm{Ker}\, N_G$. Then $x = anx = aN_G x = 0$. This shows that $j_{E/F} M_F \cap \mathrm{Ker}\, N_G = 0$. Comparing the orders, we obtain $M_E = j_{E/F} M_F \oplus \mathrm{Ker}\, N_G$.

THEOREM 1. *Let E/F be a cyclic extension of degree n prime to p. Then*

$$p^m\text{-rank}\, K_2\mathcal{O}_E \equiv p^m\text{-rank}\, K_2\mathcal{O}_F \pmod{c(n,p)}.$$

Proof. Since G is cyclic, G has the composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_t = 1$$

such that every factor group $H_i = G_{i-1}/G_i$ has prime order. Note that $M_E^{G_i}$ is an H_i-module and further $(M_E^{G_i})^{H_i} = M_E^{G_{i-1}}$. Therefore, by Proposition 1, we have $p\text{-rank}\, M_E^{G_i} - p\text{-rank}\, M_E^{G_{i-1}} = p\text{-rank}\,\mathrm{Ker}\, N_{H_i}$ since H_i is cyclic, where $N_{H_i} : M_E^{G_i} \to M_E^{G_i}$.

Suppose l_i is the order of $|H_i|$. Then $(l_i, p) = 1$. Let $x\ (\neq 0) \in \mathrm{Ker}\, N_{H_i}$. If $(H_i)_x = H_i$, then $0 = N_{H_i} x = l_i x$, which yields $x = 0$ since $(l_i, p) = 1$. This is a contradiction. Thus $(H_i)_x = 1$ since l_i is a prime. So $\#\,\mathrm{Ker}\, N_{H_i} \equiv 1 \pmod{l_i}$. It is easy to obtain $p\text{-rank}\,\mathrm{Ker}\, N_{H_i} \equiv 0 \pmod{o(l_i, p)}$.

In view of the sequence

$$M_F = M_E^G = M_E^{G_0} \subseteq M_E^{G_1} \subseteq \cdots \subseteq M_E^{G_t} = M_E,$$

we have

$$\begin{aligned} p\text{-rank}\, M_E - p\text{-rank}\, M_F &= \sum_{i=1}^{t} (p\text{-rank}\, M_E^{G_i} - p\text{-rank}\, M_E^{G_{i-1}}) \\ &= \sum_{i=1}^{t} p\text{-rank}\,\mathrm{Ker}\, N_{H_i}. \end{aligned}$$

Therefore $p\text{-rank}\, M_E \equiv p\text{-rank}\, M_F \pmod{c(n, p)}$. This proves our assertion.

Corollary 1. *Let E/F be a cyclic extension of prime degree $l \neq p$. Then*

$$p^m\text{-rank}\, K_2\mathcal{O}_E \equiv p^m\text{-rank}\, K_2\mathcal{O}_F \pmod{o(l, p)}.$$

Corollary 2. *Let E/F be a cyclic extension of degree n. If $(n, p) = 1$ and $c(n, p) \nmid p^m\text{-rank}\, K_2\mathcal{O}_F$, then $p^m\text{-rank}\, K_2\mathcal{O}_E \geq 1$ and*

$$p^m\text{-rank}\, K_2\mathcal{O}_E \equiv p^m\text{-rank}\, K_2\mathcal{O}_F \pmod{c(n, p)}.$$

Next, for a finite Galois extension E/F, we define a subgroup $B(E/F)$ of $K_2\mathcal{O}_E$ by

$$B(E/F) = \bigcap_K \mathrm{Ker}(\mathrm{tr}_{E/K} : K_2\mathcal{O}_E \to K_2\mathcal{O}_K),$$

where K runs through all the fields such that $F \subseteq K \subset E$ and E/K is cyclic of prime degree. Then we have

Theorem 2. *Let E/F be a cyclic extension of degree n prime to p. Then*

$$p^m\text{-rank}\, B(E/F) \equiv 0 \pmod{o(n, p)}.$$

Proof. Note $j_{E/F}\,\mathrm{tr}_{E/F} = N_G$. By Lemma 2, $j_{E/K}$ is injective. So $B(E/F) = \bigcap_K \mathrm{Ker}\, N_{G_K}$, where $G_K = \mathrm{Gal}(E/K)$.

Let $C = B(E/F)(p^m)/B(E/F)(p^{m-1})$ and $x\ (\neq 0) \in C$. Suppose that there exists $\sigma\ (\neq 1) \in G_x$. Let s be the order of σ. It follows from $x \in C \subseteq \operatorname{Ker} N_{\langle\sigma\rangle}$ that $sx = N_{\langle\sigma\rangle}x = 0$. Thus $x = 0$ by assumption. This is a contradiction. Therefore, $G_x = 1$. Furthermore, it is obvious that $|C| \equiv 1 \pmod{n}$. Hence $p\text{-rank}\, C \equiv 0 \pmod{o(n,p)}$, that is, $p^m\text{-rank}\, B(E/F) \equiv 0 \pmod{o(n,p)}$. This completes the proof.

Corollary 3. *Let E/F be a cyclic extension of prime degree $l \neq p$. Assume that there is a subfield k of F such that E/k is cyclic of degree l^t. Then*

$$p^m\text{-rank}\, K_2\mathcal{O}_E \equiv p^m\text{-rank}\, K_2\mathcal{O}_F \pmod{o(l^t,p)}.$$

Proof. From the assumption we have the identity $B(E/k) = \operatorname{Ker} N_G$. Consider the norm map $N_G : (K_2\mathcal{O}_E)_p \to (K_2\mathcal{O}_F)_p$. By the proof of Proposition 1, we have $(K_2\mathcal{O}_E)_p = (K_2\mathcal{O}_F)_p \oplus \operatorname{Ker} N_G$. Therefore, $p^m\text{-rank}\operatorname{Ker} N_G = p^m\text{-rank}\, K_2\mathcal{O}_E - p^m\text{-rank}\, K_2\mathcal{O}_F$. The result now follows from Theorem 2.

Remark. Corollary 3 generalizes Corollary 1.

Corollary 4. *Let F_∞/F be a $\mathbb{Z}_l$ extension for a prime number $l \neq p$, and F_n its nth layer, that is, $[F_n : F] = l^n$. Then*

$$p^m\text{-rank}\, K_2\mathcal{O}_{F_n} \equiv p^m\text{-rank}\, K_2\mathcal{O}_{F_{n-1}} \pmod{o(l^n,p)}$$

for $n \geq 1$.

Corollary 5. *Let E/F be a cyclic extension of degree n prime to p. Assume that p-rank $K_2\mathcal{O}_K = p$-rank $K_2\mathcal{O}_F$ for any intermediate fields $F \subseteq K \subset E$ such that E/K is cyclic of prime degree. Then*

$$p\text{-rank}\, K_2\mathcal{O}_E \equiv p\text{-rank}\, K_2\mathcal{O}_F \pmod{o(n,p)}.$$

Proof. For an intermediate field K of E/F, we consider the norm map $N_{G_K} : K_2\mathcal{O}_E(p) \to K_2\mathcal{O}_K(p)$, where $G_K = \operatorname{Gal}(E/K)$. By the proof of Proposition 1, we have $K_2\mathcal{O}_E(p) = K_2\mathcal{O}_K(p) \oplus \operatorname{Ker} N_{G_K}$. Therefore, $p\text{-rank}\operatorname{Ker} N_{G_K} = p\text{-rank}\, K_2\mathcal{O}_E - p\text{-rank}\, K_2\mathcal{O}_K$. If E/K is cyclic of prime degree, then $p\text{-rank}\operatorname{Ker} N_{G_K} = p\text{-rank}\operatorname{Ker} N_G$ by our assumption, and thus $\operatorname{Ker} N_{G_K} = \operatorname{Ker} N_G$. Hence $B(E/F)(p) = \operatorname{Ker} N_G$. The desired congruence follows from this and Theorem 2.

3. Some cyclic extensions of $\mathbb{Q}$. Let $E/\mathbb{Q}$ be a cyclic extension of odd prime order l. As applications, in this section, we obtain some results on the divisibility of $p^m\text{-rank}\, K_2\mathcal{O}_E$; they generalize results for $l = 3, 5$, proved in [Br1], [Zh1] and [Wu]. Using Proposition 4 below and results of [Br3], we investigate the divisibility of the orders of $K_2\mathcal{O}_{\mathbb{Q}(\zeta_l)}$ for $l < 2000$ and $l \equiv 3 \pmod{4}$.

Proposition 2. *Let $E/\mathbb{Q}$ be a cyclic extension of prime degree $l \neq p$. If $p \neq 2$ or $m \geq 2$, then*

$$o(l,p) \mid p^m\text{-rank}\, K_2\mathcal{O}_E.$$

Moreover, $o(l,2) \mid 2\text{-rank}\, K_2\mathcal{O}_E - 1$.

Proof. It is well known that $K_2\mathbb{Z} = \mathbb{Z}/2\mathbb{Z}$. The desired results follow from Theorem 1.

Proposition 3. *Let $E/\mathbb{Q}$ be a cyclic extension of prime degree $l \neq p$. If p is an odd prime, then $v_p(|K_2\mathcal{O}_E|) \equiv 0 \pmod{o(l,p)}$, where $v_p(|K_2\mathcal{O}_E|)$ is the p-adic valuation of $|K_2\mathcal{O}_E|$.*

Proof. The result follows from Proposition 1 and the formula

$$v_p(|K_2\mathcal{O}_E|) = \sum_{m=1}^{\infty} p^m\text{-rank}\, K_2\mathcal{O}_E.$$

Remark. 1. If E is a cubic cyclic number field and $p \equiv 2 \pmod 3$, then $2 \mid p^m\text{-rank}\, K_2\mathcal{O}_E$ if $p \neq 2$ or $m \geq 2$. Moreover, $2 \mid 2\text{-rank}\, K_2\mathcal{O}_E - 1$. These results were proved in [Zh1] and [Br1].

2. If E is a quintic cyclic number field, then:

(i) $2 \mid 2\text{-rank}\, K_2\mathcal{O}_E - 1$ and $4 \mid 2^m\text{-rank}\, K_2\mathcal{O}_E$;
(ii) $4 \mid p^m\text{-rank}\, K_2\mathcal{O}_E$ for $p \equiv 2, 3 \pmod 5$;
(iii) $2 \mid p^m\text{-rank}\, K_2\mathcal{O}_E$ for $p \equiv 4 \pmod 5$.

This generalizes [Wu, Theorems 3.4 and 4.4].

Proposition 4. *Let l be an odd prime and $(p,(l-1)/2) = 1$. Let*

$$F = \begin{cases} \mathbb{Q}(\sqrt{l}) & \text{if } l \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{-l}) & \text{if } l \equiv 3 \pmod 4. \end{cases}$$

Then

$$p^m\text{-rank}\, K_2\mathcal{O}_{\mathbb{Q}(\zeta_l)} \equiv p^m\text{-rank}\, K_2\mathcal{O}_F \pmod{c((l-1)/2,p)}.$$

Proof. It is well known that E has a quadratic subfield $\mathbb{Q}(\sqrt{l})$ if $l \equiv 1 \pmod 4$ or $\mathbb{Q}(\sqrt{-l})$ if $l \equiv 3 \pmod 4$. The result then follows from Theorem 1.

Proposition 5. *Let $l \neq p$ be an odd prime. If $o(l,p) \nmid p^m\text{-rank}\, K_2\mathcal{O}_{\mathbb{Q}(\zeta_l)}$, then $p^m\text{-rank}\, K_2\mathcal{O}_{\mathbb{Q}(\zeta_{l^n})} \geq 1$ and*

$$p^m\text{-rank}\, K_2\mathcal{O}_{\mathbb{Q}(\zeta_{l^n})} \equiv p^m\text{-rank}\, K_2\mathcal{O}_{\mathbb{Q}(\zeta_l)} \pmod{o(l,p)}$$

for all integers $n \geq 2$.

Proof. Since $\mathbb{Q}(\zeta_{l^n})/\mathbb{Q}(\zeta_l)$ is a cyclic extension of degree l^{n-1}, the result follows from Theorem 1.

Example. In the following, by the conjectural results of [Br3] and Proposition 4, we get the divisibility of the odd parts of the tame kernels of $E = \mathbb{Q}(\zeta_l)$ for prime numbers $l < 2000$ and $l \equiv 3 \pmod 4$.

(1) 3-rank $K_2\mathcal{O}_E \equiv 1 \pmod{52}$ when $l = 107$, 3-rank $K_2\mathcal{O}_E \equiv 1 \pmod{125}$ when $l = 503$, 3-rank $K_2\mathcal{O}_E \equiv 1 \pmod{43}$ when $l = 863$, 3-rank $K_2\mathcal{O}_E \equiv 1 \pmod{329}$ when $l = 1319$, 3-rank $K_2\mathcal{O}_E \equiv 1 \pmod{808}$ when $l = 1619$;
(2) 27-rank $K_2\mathcal{O}_E \equiv 1 \pmod 2$ when $l = 1583$;
(3) 5-rank $K_2\mathcal{O}_E \equiv 1 \pmod{442}$ when $l = 887$, 5-rank $K_2\mathcal{O}_E \equiv 1 \pmod{64}$ when $l = 1283$, 5-rank $K_2\mathcal{O}_E \equiv 1 \pmod{742}$ when $l = 1487$;
(4) 7-rank $K_2\mathcal{O}_E \equiv 1 \pmod{238}$ when $l = 479$, 7-rank $K_2\mathcal{O}_E \equiv 1 \pmod{760}$ when $l = 1523$, 7-rank $K_2\mathcal{O}_E \equiv 1 \pmod 4$ when $l = 1571$;
(5) 13-rank $K_2\mathcal{O}_E \equiv 1 \pmod 2$ when $l = 491$;
(6) 83-rank $K_2\mathcal{O}_E \equiv 1 \pmod 2$ when $l = 1667$;
(7) 23-rank $K_2\mathcal{O}_E \equiv 1 \pmod 2$ when $l = 1847$.

Acknowledgments. I would like to thank the referee for his valuable comments. This paper was supported by the NSFC 10801076 and the Natural Science Foundation of the Jiangsu Higher Education Institutions of China (Grant No. 08KJB110006).

References

[Br1] J. Browkin, *Tame kernels of cubic cyclic fields*, Math. Comp. 74 (2005), 967–999.
[Br2] —, *On the p-rank of the tame kernel of algebraic number fields*, J. Reine Angew. Math. 432 (1992), 135–149.
[Br3] J. Browkin and H. Gangl, *Tame and wild kernels of quadratic imaginary number fields*, Math. Comp. 68 (1999), 291–305.
[Gu] X. Guo and H. Qin, *The 3-adic regulators and wild kernels*, J. Algebra 312 (2007), 418–425.
[Ke] F. Keune, *On the structure of the K_2 of the ring of integers in a number field*, K-Theory 2 (1989), 625–645.
[Ko] M. Kolster, *Odd torsion in the tame kernel of totally real number fields*, in: Algebraic K-Theory: Connections with Geometry and Topology, J. F. Jardine and V. P. Snaith (eds.), Springer, 1989, 177–188.
[Mi] J. Milnor, *Introduction to Algebraic K-Theory*, Ann. of Math. Stud. 72, Princeton Univ. Press, Princeton, 1971.
[Ne] J. Neukirch, *Class Field Theory*, Grundlehren Math. Wiss. 280, Springer, Berlin, 1986.
[Qi] H. R. Qin and H. Y. Zhou, *The 3-Sylow subgroup of the tame kernel of real number fields*, J. Pure Appl. Algebra 209 (2007), 245–253.
[Wu] X. Wu, *Tame kernels of quintic cyclic fields*, Acta Arith. 134 (2008), 183–199.
[Zh1] H. Y. Zhou, *Tame kernels of cubic cyclic fields*, ibid. 124 (2006), 293–313.

[Zh2] H. Y. Zhou, *The tame kernel of multiquadratic number fields*, Comm. Algebra, to appear.

Department of Mathematics
Nanjing Normal University
Nanjing 210093, P.R. China
E-mail: haiyanxiaodong@gmail.com

Received on 14.6.2008
and in revised form on 27.7.2008 (5738)