ACTA ARITHMETICA
124.4 (2006)

Tame kernels of cubic cyclic fields

by

HAIYAN ZHOU (Nanjing)

1. Introduction. Let K/k be a Galois extension of number fields and G its Galois group. The tame kernel of K, $K_2\mathcal{O}_K$, is a G-module. This fact can often be used to investigate the structure of $K_2\mathcal{O}_K$. The tame kernels of number fields have been investigated by many authors (see the list of references). In particular, J. Browkin gave some explicit results for cubic cyclic fields with exactly one ramified prime in [Br1]. In this paper, we study cubic cyclic fields with only two ramified primes.

This paper is organized as follows. In Section 2, we study the 2-primary part of tame kernels of cubic cyclic fields F. Section 3 applies reflection theorems to study the ℓ-rank of $K_2\mathcal{O}_F$. In particular, we obtain a bound on the 3-rank of $K_2\mathcal{O}_F$. Finally, we use the G-module structure of $K_2\mathcal{O}_F$ to study the 3-primary and ℓ-primary parts of tame kernels of cubic cyclic fields F where $\ell \equiv 5 \pmod 6$. Moreover, we obtain some results about the 3^i-rank of $K_2\mathcal{O}_F$, $i > 1$. In particular, we compute the structure of the 3-primary part of $K_2\mathcal{O}_F$ in the cases left open in [Br1]. Moreover, we prove the following theorem for all cubic cyclic fields. In particular, Conjecture 4.6 in [Br1] is true.

THEOREM. *Let F be a cubic cyclic field and τ a generator of the Galois group* $\mathrm{Gal}(F/\mathbb{Q})$. *If $\ell \equiv 5 \pmod 6$ is a prime*, *then*

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

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

Let F be a cubic cyclic field with only two ramified primes. In Sects. 4–6 we investigate the tame kernel $K_2\mathcal{O}_F$, where $\mathcal{O}_F$ is the ring of integers of F. Using the well-known Birch–Tate conjecture, it is easy to compute the order

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

Key words and phrases: cubic fields, cyclic fields, tame kernel.

of $K_2\mathcal{O}_F$. We discuss its divisibility by small primes. To get information on the structure of the group $K_2\mathcal{O}_F$ we investigate its q-rank for $q = 2, 3, 7, 13$.

Acknowledgements. The author would like to thank Jerzy Browkin for useful advice and correspondence. She would also like to express her thanks to her supervisor, Hourong Qin, for useful discussions.

2. The 2-primary part of the tame kernel

2.1. *The 2-rank of $K_2\mathcal{O}_F$.* Let F be a cubic cyclic field.

LEMMA 2.1 ([Br1, (3.2)]). *We have*

$$\text{2-rank}\, K_2\mathcal{O}_F = \begin{cases} 3 + \text{2-rank}\,\mathrm{Cl}(\mathcal{O}_F[1/2]) & \text{if } 2 \text{ is inert in } F,\\ 5 + \text{2-rank}\,\mathrm{Cl}(\mathcal{O}_F[1/2]) & \text{if } 2 \text{ splits in } F. \end{cases}$$

LEMMA 2.2. *The* 2*-rank of* $\mathrm{Cl}(\mathcal{O}_F[1/2])$ *is even.*

Proof. Let $V = {}_2\mathrm{Cl}(\mathcal{O}_F[1/2])$ and $r = \text{2-rank}\,\mathrm{Cl}(\mathcal{O}_F[1/2])$, so V has 2^r elements. Let τ generate the Galois group $\mathrm{Gal}(F/\mathbb{Q})$. Then τ acts on V. Let $v \in V,\ v \neq 0$ and let $\tau(v) = v$. Therefore

$$v^3 = (1 + \tau + \tau^2)v = \mathrm{Norm}(v),$$

where the norm is induced by the norm from F to $\mathbb{Q}$. It is easy to see that $v^3 = 0$. But $v^2 = 0$, so $v = 0$, contradiction. It follows that the orbit of every $v \neq 0$ has three elements, so $2^r \equiv 1 \pmod 3$. Therefore $2 \mid r$. This completes the proof. ∎

LEMMA 2.3. *Let F be a cubic cyclic field with at least two ramified primes. For a prime number q, let A_q be the Sylow q-subgroup of the class group* $\mathrm{Cl}(\mathcal{O}_F)$ *of F. Then*

(i) *The class number of F is divisible by* 3.
(ii) 3-rank $\mathrm{Cl}(\mathcal{O}_F) = 1$ *if and only if* $3 \,\|\, \#\mathrm{Cl}(\mathcal{O}_F)$.
(iii) *If* $q \equiv 2 \pmod 3$, *then* $A_q = B_q \times \tau(B_q)$ *for some subgroup B_q of A_q.*

The same holds if we replace $\mathcal{O}_F$ by the ring $\mathcal{O}_{F,\ell} = \mathcal{O}_F[1/\ell]$ of integers of F localized at ℓ, where ℓ is a prime.

Proof. (i) follows from [CH, Theorem 9.3], (ii) follows from [CR, Corollary] and (iii) follows from [Wa, Theorem 10.8]. The last statement follows from Lemma 2.2. ∎

THEOREM 2.4. *The* 2*-rank of $K_2\mathcal{O}_F$ is odd.*

Proof. This follows from Lemmas 2.1 and 2.3. ∎

2.2. *Elements of order 2 in $K_2\mathcal{O}_F$.* Elements of order 2 in $K_2\mathcal{O}_F$ can be described explicitly. Let $\varepsilon_1, \varepsilon_2$ be fundamental units of F. Changing sign if necessary, we may assume that $N\varepsilon_1 = 1$, and $\varepsilon_2 = \tau(\varepsilon_1)$, where τ is a generator of the Galois group $T = \mathrm{Gal}(F/\mathbb{Q})$. In view of Lemma 2.3

we can take independent generators of the group ${}_2\mathrm{Cl}(\mathcal{O}_F[1/2])$ of the form $\mathrm{Cl}(\wp_j)$, $\mathrm{Cl}(\tau(\wp_j))$, $j = 1, \ldots, t$, where $2t = 2\text{-rank}\,\mathrm{Cl}(\mathcal{O}_F[1/2])$, and $\wp_j$ are prime ideals satisfying $\wp_j \nmid 2$. Then the ideals $\wp_j^2$ are principal, $\wp_j^2 = (\gamma_j)$ for $j = 1, \ldots, t$. We may assume that $N\gamma_j > 0$. If 2 splits in F, $(2) = \wp \cdot \tau(\wp) \cdot \tau^2(\wp)$, and the class $\mathrm{Cl}(\wp)$ in $\mathrm{Cl}(\mathcal{O}_F)$ has order r, then the ideal $\wp^r$ is principal, $\wp^r = (\gamma)$. From [Br1, 3.2], we have the following result:

THEOREM 2.5.

(i) *If* 2 *is inert in* F, *then the subgroup of elements of order* ≤ 2 *in* $K_2\mathcal{O}_F$ *is generated by*

$$\{-1,-1\}, \{-1,\varepsilon_1\}, \{-1,\tau(\varepsilon_1)\}, \{-1,\gamma_j\}, \{-1,\tau(\gamma_j)\},$$

where $j = 1, \ldots, t$.

(ii) *If* 2 *splits in* F, *then the subgroup of elements of order* ≤ 2 *in* $K_2\mathcal{O}_F$ *is generated by*

$\{-1,-1\}, \{-1,\varepsilon_1\}, \{-1,\tau(\varepsilon_1)\}, \{-1,\gamma\}, \{-1,\tau(\gamma)\},$
$\{-1,\gamma_j\}, \{-1,\tau(\gamma_j)\},$
where $j = 1, \ldots, t$.

THEOREM 2.6. *For* $r \geq 2$ *the* 2^r*-rank of* $K_2\mathcal{O}_F$ *is even and if there are* n *elements in the set* $\{\varepsilon_1, \gamma, \gamma_j : 1 \leq j \leq t\}$ *that are not totally positive, then*

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

Proof. If an element $\alpha \in F^*$ is not totally positive, then applying the three real Hilbert symbols of F to $\{-1,\alpha\}$ we see that $\{-1,\alpha\}$ is not a square in K_2F. In particular $\{-1,-1\}$ is not a square. Since $\{-1,\alpha\}$ is a power of some element of F^*, $\{-1,\tau(\alpha)\}$ is the same power of some element of F^*. It follows from Theorem 2.5 that the 2^r-rank of $K_2\mathcal{O}_F$ is even, where $r \geq 2$. The inequality follows from the fact that if α is not totally positive, then $\tau(\alpha)$ is not totally positive. ■

3. The ℓ-primary parts of tame kernels for an odd prime ℓ

3.1. *Notation.* In this paper, we use the same notation as in [Br1]. Let ℓ be an odd prime number, ζ_ℓ a primitive ℓth root of unity, and $G := \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$. Then

$$G = \{\sigma_a : 1 \leq a \leq \ell - 1\}$$

where $\sigma_a(\zeta_\ell) = \zeta_\ell^a$. For a fixed primitive root k modulo ℓ the automorphism $\sigma := \sigma_k$ generates G.

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

$$\varepsilon_j = \frac{1}{\ell-1}\sum_{a=1}^{\ell-1}\omega(a)^j\sigma_a^{-1} = \frac{1}{\ell-1}\sum_{i=0}^{\ell-2}\omega(k)^{ij}\sigma^{-i}, \qquad 0 \le j \le \ell-2. \tag{3.1}$$

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

For a $\mathbb{Z}_\ell[G]$-module M, we get a decomposition of M into a direct sum of $\mathbb{Z}_\ell[G]$-submodules:

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

The group μ_ℓ of ℓth roots of unity has the natural structure of a $\mathbb{Z}_\ell[G]$-module. We define the action of G on $\mu_\ell \otimes M$ by

$$(\zeta\otimes m)^\sigma = \zeta^\sigma \otimes m^\sigma, \qquad \text{where } \zeta\in\mu_\ell,\ m\in M,\ \sigma\in G.$$

Since $|G| = \ell-1$, we have

$$(\mu_\ell\otimes M)^G = \varepsilon_0(\mu_\ell\otimes M). \tag{3.2}$$

From [Br1],

$$\varepsilon_0(\mu_\ell\otimes M) = \mu_\ell\otimes\varepsilon_{\ell-2}M. \tag{3.3}$$

In the following we always assume that $E = F(\zeta_\ell)$, where F is a cubic cyclic field. Denote by $\lambda : \mathrm{Cl}(\mathcal{O}_E) \to \mathrm{Cl}(\mathcal{O}_E[1/\ell])$ the homomorphism of the class groups induced by the imbedding $\mathcal{O}_E \to \mathcal{O}_E[1/\ell]$, and let $A = A_E$ be the Sylow ℓ-subgroup of $\mathrm{Cl}(\mathcal{O}_E)$. Then $\lambda(A)$ is the Sylow ℓ-subgroup of $\mathrm{Cl}(\mathcal{O}_E[1/\ell])$ by the surjectivity of λ.

Since A is an ℓ-group on which $G = \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q}) = \mathrm{Gal}(E/F)$ acts, we have

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

LEMMA 3.1. *If ℓ does not ramify in F or $\ell = 3$, then for $j \ne 0$ the mapping $\lambda : \varepsilon_j A \to \varepsilon_j\lambda(A)$ is an isomorphism.*

Proof. If ℓ does not ramify in F, then the result follows from the same proof as [Br1, Lemma 4.1]. If 3 ramifies in F and $\ell = 3$, then 3 is totally ramified in $E = F(\zeta_3)$ since $(2,3) = 1$. Thus $\sigma(\mathfrak{p}) = \mathfrak{p}$ for every $\sigma \in G$, where $\mathfrak{p}$ is the prime ideal of E which divides 3. Therefore $\mathrm{Ker}(\lambda)\cap A \subset \varepsilon_0 A$. Consequently, $\mathrm{Ker}(\lambda)\cap\varepsilon_j A = 0$ for $j\ne 0$. This completes the proof. ∎

THEOREM 3.2. *Let F be a cubic cyclic field and $E = F(\zeta_\ell)$. If ℓ does not ramify in F or $\ell = 3$, then*

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

Proof. The result follows from the same proof as [Br1, Theorem 4.3] and Lemma 3.1. ∎

3.2. *The 3-primary part of the tame kernel of F.* If $\ell = 3$, then $E = F(\zeta_3)$, $G = \mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) = \langle\sigma\rangle$ where σ is the complex conjugation. So

$$\varepsilon_0 = \frac{1}{2}(1+\sigma), \quad \varepsilon_1 = \frac{1}{2}(1-\sigma).$$

By Theorem 3.2, 3-rank $K_2\mathcal{O}_F$ = 3-rank $\varepsilon_1 A_E$. According to [Br2, Lemma 2.1], $N_{E/F} : A_E \to A_F$ is surjective and $\mathrm{Ker}(N_{E/F}) = \varepsilon_1 A_E$. So we have the following important theorem:

THEOREM 3.3. 3-rank $K_2\mathcal{O}_F$ = 3-rank A_E − 3-rank A_F.

We apply reflection theorems to prove some estimates of the 3-rank $K_2\mathcal{O}_F$. Let $E/\mathbb{Q}$ be a Galois extension with $\zeta_\ell \in E$. Let L be the maximal unramified and elementary abelian ℓ-extension of E with the Galois group $H := \mathrm{Gal}(L/E)$. Then the Artin reciprocity map gives an isomorphism of $\mathrm{Gal}(E/\mathbb{Q})$-modules $A/\ell \to H$.

By Kummer theory, $L = E(B^{1/\ell})$, where B is a subgroup of E^* containing $E^{*\ell}$. Set $B_0 := B/E^{*\ell}$. Then every principal ideal (b), where $b \in B$, is the ℓth power of an ideal in E, since L/E is unramified. Moreover B_0 is isomorphic to the dual $\widehat{H}$ of H as a $\mathrm{Gal}(E/\mathbb{Q})$-module.

Define ${}_\ell A = \{a \in A : a^\ell = 1\}$. Then there is a homomorphism of $\mathrm{Gal}(E/\mathbb{Q})$-modules

$$\varphi : B_0 \to {}_\ell A$$

such that $\varphi(bE^{*\ell}) = \mathrm{Cl}(\mathfrak{a})$, where the ideal $\mathfrak{a}$ of $\mathcal{O}_E$ is defined by the condition $(b) = \mathfrak{a}^\ell$.

LEMMA 3.4.

(i) *If* 3 *is ramified in F, then* 3-rank $A_F - 1 \le$ 3-rank $\varepsilon_1 A_E$.
(ii) *If* 3 *does not ramify in F, then* 3-rank $A_F \le$ 3-rank $\varepsilon_1 A_E$.

Proof. It is obvious that F is the maximal real subfield of $E = F(\zeta_3)$. And we know that if 3 does not ramify in F, then $F(\zeta_9)/E$ is totally ramified. Thus the lemma follows from [Wa, Theorem 10.11]. ∎

PROPOSITION 3.5.

(i) *If* 3 *is ramified in F, then*

$$3\text{-rank}\, A_F - 1 \le 3\text{-rank}\, K_2\mathcal{O}_F \le 3\text{-rank}\, A_F + 2.$$

(ii) *If* 3 *does not ramify in* F, *then*

$$3\text{-rank}\, A_F \le 3\text{-rank}\, K_2\mathcal{O}_F \le 3\text{-rank}\, A_F + 2.$$

Proof. By the above arguments, we have $A = \varepsilon_0 A \oplus \varepsilon_1 A$. Note that $H \cong A/3$ as G-modules. So $\varepsilon_i H \cong \varepsilon_i(A/3)$ for $i = 0, 1$. Let $h \in \varepsilon_i H$. Then $\sigma_a h = h^{\omega^i(a)}$ for all $a \in (\mathbb{Z}/3)^*$, where $\sigma_1 = 1$, $\sigma_2 = \sigma$ and ω is the Teichmüller character of the group $(\mathbb{Z}/3)^*$. Let $b \in \varepsilon_k B_0$. Then

$$\langle h, b\rangle^{\omega(a)} = \langle h, b\rangle^{\sigma_a} = \langle h^{\omega^i(a)}, b^{\omega^k(a)}\rangle = \langle h, b\rangle^{\omega^{i+k}(a)}$$

for all a. If $i + k \not\equiv 1 \pmod 2$, then $\langle h, b\rangle = 1$. Since the pairing between $B = \varepsilon_0 B \oplus \varepsilon_1 B$ and $H = \varepsilon_0 H \oplus \varepsilon_1 H$ is nondegenerate, it follows easily that the induced pairing

$$\varepsilon_i H \times \varepsilon_j B \to \mu_3, \quad i = 0,\ j = 1 \text{ or } i = 1,\ j = 0$$

is nondegenerate. Hence we have

$$\varepsilon_0 B_0 \cong \varepsilon_1 H \cong \varepsilon_1(A/3) \quad \text{as abelian groups.}$$

Now the reflection map $\varphi : B_0 \to {}_3A$ is G-linear, so

$$\varphi : \varepsilon_0 B_0 \to \varepsilon_0({}_3A).$$

Therefore we have the exact sequence

$$0 \to \operatorname{Ker}(\varphi) \cap \varepsilon_0 B_0 \to \varepsilon_0 B_0 \to A_F.$$

We also have

$$\operatorname{Ker}(\varphi) \cap \varepsilon_0 B_0 \cong \text{subgroup of } \varepsilon_0(U_E/U_E^3).$$

Thus by Theorem 3.2 and Dirichlet's unit theorem, we have

$$\begin{aligned} 3\text{-rank}\, K_2\mathcal{O}_F &= 3\text{-rank}\, \varepsilon_1 A_E = 3\text{-rank}\, \varepsilon_0 B_0 \\ &\le 3\text{-rank}\, A_F + \operatorname{Ker}(\varphi) \cap \varepsilon_0 B_0 \\ &\le 3\text{-rank}\, A_F + 3\text{-rank}\, U_F/3 \\ &\le 3\text{-rank}\, A_F + 2. \end{aligned}$$

The proposition now follows from Lemma 3.4. ∎

THEOREM 3.6. *Let* F *be a cubic cyclic field with* r *ramified primes and* $r \ge 2$. *Then* $3\text{-rank}\, K_2\mathcal{O}_F \le 2r$. *Moreover*, *if* 3 *does not ramify in* F, *then* $1 \le 3\text{-rank}\, K_2\mathcal{O}_F \le 2r$.

Proof. Suppose $T = \operatorname{Gal}(F/\mathbb{Q})$ and $3\text{-rank}\, A_F^T = s$. By the well-known fact that $3\text{-rank}\, A_F^T$ is one less than the number of ramified primes, we have $s = r - 1$. From the proof of [CR, Proposition 5], we have the following cases:

Case 1. If A_F is an elementary 3-group, then

$$A_F \cong \bigoplus_{i=1}^{s} (\mathbb{Z}/3)^{a_i}, \quad \text{where } a_i \le 2.$$

Thus $3\text{-rank}\, A_F \le 2(r-1)$.

Case 2. If A_F contains an element of order 9, then

$$A_F/3 \cong (\mathbb{Z}/3)^2 \oplus \bigoplus_{i=2}^{s} (\mathbb{Z}/3)^{b_i}, \quad \text{where } b_i \le 2.$$

So, $3\text{-rank}\, A_F \le 2 + 2(r-2) = 2(r-1)$. Therefore the result follows from Lemma 2.3 and Proposition 3.5. ■

Corollary 3.7. *Let F be a cubic cyclic field with at least two ramified primes. If 3 does not ramify in F and $3 \,\|\, \#K_2\mathcal{O}_F$, then $3 \,\|\, \#A_F$.*

Theorem 3.8. *Let $\mathfrak{p} \mid 3$ be the prime ideal of E. If 3 is ramified in F, then*

$$3\text{-rank}\, K_2\mathcal{O}_F = \begin{cases} 3\text{-rank}\, K_2\mathcal{O}_E - 3\text{-rank}\, A_F & \text{if } \mathfrak{p} \text{ is principal},\\ 3\text{-rank}\, K_2\mathcal{O}_E - 3\text{-rank}\, A_F - 1 & \text{otherwise.}\end{cases}$$

Proof. Since 3 is ramified in F, it is totally ramified in E. By [Ke, Corollary 3.9], we have $3\text{-rank}\, K_2\mathcal{O}_E = 3\text{-rank}\, \mathrm{Cl}(\mathcal{O}_E[1/3])$. If $\mathfrak{p}$ is principal, then $A_E = \mathrm{Cl}(\mathcal{O}_E[1/3])$. Otherwise, $3\text{-rank}\, \mathrm{Cl}(\mathcal{O}_E[1/3]) = 3\text{-rank}\, A_E - 1$. Thus the assertion follows from Theorem 3.3. ■

Let F be a cubic cyclic field and $T = \mathrm{Gal}(F/\mathbb{Q})$. Denote by τ a generator of G. Let K/E be an extension of number fields. Denote by tr the transfer homomorphism $\mathrm{tr} : K_2K \to K_2E$. Let $j : K_2E \to K_2K$ be the homomorphism induced by the inclusion map $E \subset K$. Let M be a finite abelian group and p a prime number. Denote by $(M)_p$ the p-primary part of M.

Lemma 3.9. *If $K_2\mathcal{O}_F$ has an element of order 9, then*

$$3\text{-rank}\, K_2\mathcal{O}_F \ge 1 + 3\text{-rank}\, (K_2\mathcal{O}_F)^G.$$

Proof. It is well known that $K_2\mathbb{Z} \cong \mathbb{Z}/2$. Note that $j \cdot \mathrm{tr} = \sum_{g\in G} g$. The lemma follows from [CR, Proposition 5]. ■

Corollary 3.10. *The 3-primary part of $K_2\mathcal{O}_F$ is cyclic if and only if $3 \,\|\, \#K_2\mathcal{O}_F$.*

Proof. Since G is a 3-group, it is easy to see that $((K_2\mathcal{O}_F)_3)^G \ne 0$. So by Lemma 3.9, the presence of an element of order 9 implies 3-rank ≥ 2. This completes the proof. ■

From Propositions 6 and 7 of [CR], we have the following results:

Corollary 3.11. *The* 3*-primary part of* $K_2\mathcal{O}_F$ *cannot be the sum of three summands each cyclic of order divisible by* 9.

Corollary 3.12. *If* 3^i-rank $K_2\mathcal{O}_F \geq 2r+1$, *then* 3^{i-1}-rank $K_2\mathcal{O}_F \geq 2(r+1)$. *In particular*, *if* 3^i-rank $K_2\mathcal{O}_F \geq 1$, *then* 3^{i-1}-rank $K_2\mathcal{O}_F \geq 2$.

As an application of Corollary 3.12, we determine the structure of the 3-primary parts of those $K_2\mathcal{O}_F$ which are left open in [Br1], for $p = 1747,\ 2593,\ 3061,\ 3583,\ 4789$. Now, using the GP/PARI, we compute the 3-primary part of $\mathrm{Cl}(\mathcal{O}_E)$, and obtain the following table:

p	$(K_2\mathcal{O}_F)_3$	$(\mathrm{Cl}(\mathcal{O}_E))_3$
1747	$\mathbb{Z}/9 \times \mathbb{Z}/9$	$\mathbb{Z}/3 \times \mathbb{Z}/9$
2593	$\mathbb{Z}/27 \times \mathbb{Z}/27$	$\mathbb{Z}/3 \times \mathbb{Z}/9$
3061	$\mathbb{Z}/9 \times \mathbb{Z}/9$	$\mathbb{Z}/9 \times \mathbb{Z}/9$
3583	$\mathbb{Z}/9 \times \mathbb{Z}/9$	$\mathbb{Z}/3 \times \mathbb{Z}/9$
4789	$\mathbb{Z}/9 \times \mathbb{Z}/27$	$\mathbb{Z}/3 \times \mathbb{Z}/9$

where $E = F(\zeta_3)$.

3.3. *The* ℓ*-primary part of* $K_2\mathcal{O}_F$, *where* $\ell \equiv 5 \pmod 6$ *is a prime*

Theorem 3.13. *The* ℓ^i*-rank of* $K_2\mathcal{O}_F$ *is even*, *where* $i > 0$.

Proof. Let B be the Sylow ℓ-subgroup of $K_2\mathcal{O}_F$ and $V = B^{\ell^{i-1}}/B^{\ell^i}$. So $r_i := \ell^i\text{-rank}\, K_2\mathcal{O}_F = \dim V$ and V has ℓ^{r_i} elements. Suppose $v \in V,\ v \neq 0$ and $\tau(v) = v$. Then

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

where j is induced by the inclusion $\mathbb{Q} \subset F$ and tr is the transfer homomorphism of K_2. Note that $K_2\mathbb{Z} \cong \mathbb{Z}/2$. Therefore, $v^3 = 0$. But $\ell \nmid 3$, so $v = 0$, contradiction. It follows that $\tau(v) \neq v$, so $\ell^{r_i} \equiv 1 \pmod 3$. Therefore $2 \mid r_i$. This completes the proof. ■

Corollary 3.14. *Let* F *be a cubic cyclic field and* τ *a generator of the Galois group* $\mathrm{Gal}(F/\mathbb{Q})$. *If* $\ell \equiv 5 \pmod 6$ *is a prime*, *then*

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

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

Proof. The corollary follows easily from Theorem 3.13. ■

Remark. Conjecture 4.6 in [Br1] follows from Corollary 3.14.

4. Orders of tame kernels

4.1. *Basic information on the field* F. In the following, let F be a cubic cyclic field with only two primes $p > 7$, $q > 7$ ramified in F. From [Co, Theorem 6.4.6], it follows that $p \equiv 1 \pmod 6$ and $q \equiv 1 \pmod 6$, and the discriminant of F is p^2q^2. We describe such a field in detail as follows. By the conductor-discriminant formula [Wa, Theorem 3.11], the conductor of F is pq. So F is a cubic subfield of the cyclotomic field $\mathbb{Q}(\zeta_{pq})$. We may assume that $g, h \in \mathbb{Z}$ satisfy:

- g is a primitive root modulo p, and $g \equiv 1 \pmod q$,
- h is a primitive root modulo q, and $h \equiv 1 \pmod p$.

For $a \in \mathbb{Z}$ with $(a, pq) = 1$ denote by σ_a the automorphism of the field $\mathbb{Q}(\zeta_{pq})$ satisfying $\sigma_a(\zeta_{pq}) = \zeta_{pq}^a$. Then the Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$ is generated by σ_g and σ_h; and there are four subgroups of index 3: $H_1 = \langle \sigma_g^3, \sigma_h \rangle$, $H_2 = \langle \sigma_g, \sigma_h^3 \rangle$, $H_3 = \langle \sigma_g^3, \sigma_g\sigma_h \rangle$, $H_4 = \langle \sigma_g^3, \sigma_g\sigma_h^{-1} \rangle$.

Denote by F_i the fixed field of H_i, $i = 1, 2, 3, 4$. It is obvious that $F_1 \subset \mathbb{Q}(\zeta_p)$ and $F_2 \subset \mathbb{Q}(\zeta_q)$. Then F is F_3 or F_4. In what follows we consider only the field $F = F_3$, the arguments for the field F_4 are similar. Define the Gauss sums:

$$\alpha_1 = \sum_{j_1=1}^{p-1} \sum_{\substack{j_2=1 \\ j_2 \equiv j_1 \ (\mathrm{mod}\ 3)}}^{q-1} \zeta_{pq}^{g^{j_1} h^{j_2}}, \tag{4.1}$$

$$\alpha_2 = \sigma_g(\alpha_1) = \sum_{j_1=1}^{p-1} \sum_{\substack{j_2=1 \\ j_2 \equiv j_1 \ (\mathrm{mod}\ 3)}}^{q-1} \zeta_{pq}^{g^{j_1+1} h^{j_2}}, \tag{4.2}$$

$$\alpha_3 = \sigma_g^2(\alpha_1) = \sum_{j_1=1}^{p-1} \sum_{\substack{j_2=1 \\ j_2 \equiv j_1 \ (\mathrm{mod}\ 3)}}^{q-1} \zeta_{pq}^{g^{j_1+2} h^{j_2}}. \tag{4.3}$$

Then $F = \mathbb{Q}(\alpha_j)$, $j = 1, 2, 3$, and $\alpha_1, \alpha_2, \alpha_3$ are conjugate in F. Moreover, by Section 1 of [Gr], the minimal polynomial for the Gauss sums is

$$f(X) = X^3 - X^2 - \frac{pq-1}{3} X + \frac{pq(A+3)-1}{27} \in \mathbb{Z}[X]$$

where $4pq = A^2 + 27B^2$, $A, B \in \mathbb{Z}$, $A \equiv 1 \pmod 3$, $B > 0$.

Remark. It is well known that there are only two pairs $A, B \in \mathbb{Z}$ such that $4pq = A^2 + 27B^2$, $A \equiv 1 \pmod 3$, $B > 0$. Thus F_3 and F_4 are the corresponding splitting fields of $f(x)$ according to the value of A.

Substituting $X \mapsto \frac{1}{3}(X+1)$ we get another polynomial with the same splitting field:

$$g(X) = X^3 - 3pqX + Apq. \tag{4.4}$$

Now we state some known facts on the class group of the field F. Let $T = \mathrm{Gal}(F/\mathbb{Q})$, and let τ be the restriction of σ_g to the subfield F.

4.2. *Orders of tame kernels.* By the Birch–Tate conjecture, we can actually compute the order of the group $K_2\mathcal{O}_F$. Recall that the conjecture states that whenever L is a totally real number field,

$$\#K_2\mathcal{O}_L = w_2(L)|\zeta_L(-1)|,$$

where ζ_L is the Dedekind zeta function of the field L and $w_2(L)$ is the maximal order of a root of unity belonging to the compositum of all quadratic extensions of L. The conjecture is known to be true when L is abelian over $\mathbb{Q}$ and is known to be true in general up to a power of 2. (See [Ko], [MW] and [Wi].)

Now, in our case, $w_2(F) = 24$.

Recall that 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 over the linear characters of the Galois group $\mathrm{Gal}(F/\mathbb{Q})$.

In our case there are two nontrivial cubic Dirichlet characters χ and $\overline{\chi}$, where

$$\chi(a) = \begin{cases} \zeta_3^k & \text{if } (a,pq)=1,\ \sigma_a \in \sigma_{g^k}H,\ k=0,1,2,\\ 0 & \text{if } p \mid a \text{ or } q \mid a,\end{cases}$$

and $\overline{\chi}$ is the complex conjugate character of χ. Hence

$$\zeta_F(s) = \zeta(s)L(s,\chi)L(s,\overline{\chi}).$$

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

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

where $B_{n,\chi}$ is the generalized Bernoulli number corresponding to a Dirichlet character χ of conductor f, since $\zeta(-1) = -1/12$ and $B_{n,\overline{\chi}} = \overline{B}_{n,\chi}$, we get

$$\zeta_F(-1) = \zeta(-1)\,\frac{B_{2,\chi}\cdot B_{2,\overline{\chi}}}{4} = -\frac{1}{48}\,|B_{2,\chi}|^2.$$

Hence

$$\#K_2\mathcal{O}_F = \frac{1}{2}\,|B_{2,\chi}|^2.$$

So it is necessary to compute $B_{2,\chi}$.

For $k=0,1,2$, we define $T_k := \{j : 1 \le j \le pq-1,\ \sigma_j \in \sigma_{g^k}H\}$ and

$$S_k := \frac{1}{pq}\sum_{j\in T_k} j^2.$$

Since $j \in T_k$ iff $j \equiv g^{3r+k+i}h^i \pmod{pq}$ for some r, $0 \le r < (p-1)/3$, and $i,\ 0 \le i < q-1$, we have

$$\begin{aligned}\sum_{j\in T_k} j^2 &\equiv g^{2k} \sum_{r=0}^{(p-4)/3} g^{6r} \sum_{i=0}^{q-2} (gh)^{2i}\\ &= g^{2k} \cdot \frac{g^{2(p-1)}-1}{g^6-1} \cdot \frac{(gh)^{2(q-1)}-1}{(gh)^2-1}\\ &\equiv 0 \pmod{pq},\end{aligned}$$

hence the S_k are integers. Moreover

$$\begin{aligned}S_0+S_1+S_2 &= \frac{1}{pq}\Big(\sum_{n=1}^{pq-1} n^2 - p^2\sum_{n=1}^{q-1} n^2 - q^2 \sum_{n=1}^{p-1} n^2\Big)\\ &= \tfrac{1}{6}((pq-1)(2pq-1) - p(q-1)(2q-1) - q(p-1)(2p-1))\\ &= \tfrac{1}{6}(p-1)(2pq+1)(q-1).\end{aligned}$$

By [Wa, Exercise 4.2(a)], it is easy to get

$$B_{2,\chi} = \frac{1}{pq}\sum_{j=1}^{pq-1} \chi(j)j^2 = S_0 - \frac{1}{2}(S_1+S_2) + \frac{\sqrt{3}}{2}\, i(S_1-S_2).$$

Consequently,

$$\begin{aligned}(4.5)\quad \#K_2\mathcal{O}_F &= \tfrac{1}{2}|B_{2,\chi}|^2\\ &= \tfrac{1}{4}((S_0-S_1)^2+(S_1-S_2)^2+(S_2-S_0)^2)\\ &= \tfrac{1}{2}((S_0+S_1+S_2)^2 - 3(S_0S_1+S_1S_2+S_2S_0))\\ &= \tfrac{1}{2}\Big(\big(\tfrac{1}{6}(p-1)\cdot(2pq+1)\cdot(q-1)\big)^2 - 3(S_0S_1+S_1S_2+S_2S_0)\Big).\end{aligned}$$

In the following, we use another method to compute $\#K_2\mathcal{O}_F$. We know that the Dedekind zeta function $\zeta_F(s)$ of the field F can be defined by the Euler product

$$\begin{aligned}\zeta_F(s) &= \left(1-\frac{1}{p^s}\right)^{-1}\left(1-\frac{1}{q^s}\right)^{-1}\\ &\quad\times \prod_{\ell \text{ splits}}\left(1-\frac{1}{\ell^s}\right)^{-3} \prod_{\ell \text{ is inert}}\left(1-\frac{1}{\ell^{3s}}\right)^{-1}.\end{aligned}$$

By the functional equation we have

$$\zeta_F(-1) = -\left(\frac{pq}{2\pi^2}\right)^3 \zeta_F(2).$$

Therefore,

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

From the above formula for $\zeta_F(s)$ it follows that $1 < \zeta_F(2) < \zeta(2)^3$, where $\zeta(s)$ is the Riemann zeta function. Consequently

$$\frac{3}{\pi^6}(pq)^3 < \# K_2\mathcal{O}_F < \frac{1}{72}(pq)^3. \tag{4.6}$$

THEOREM 4.1. *If we fix a prime number p, then*

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

Proof. This follows from (4.6). ∎

THEOREM 4.2. *Let $v_p(m)$ be the p-adic valuation of m. Then*

(i) *$v_2(\# K_2\mathcal{O}_F)$ is odd.*
(ii) *For every prime number $q \equiv -1 \pmod 6$, the number $v_q(\# K_2\mathcal{O}_F)$ is even. Moreover $q \mid \# K_2\mathcal{O}_F$ iff $S_0 \equiv S_1 \equiv S_2 \pmod q$.*
(iii) *$S_0 \equiv S_1 \equiv S_2 \pmod 2$.*
(iv) *$v_3(\# K_2\mathcal{O}_F) \geq 1$.*
(v) *$3 \parallel \# K_2\mathcal{O}_F$ iff S_1, S_2, S_3 are distinct modulo 3. In this case we have $\# K_2\mathcal{O}_F \equiv 6 \pmod 9$. Moreover,*

$$3^2 \mid \# K_2\mathcal{O}_F \quad \textit{iff} \quad S_0 \equiv S_1 \equiv S_2 \pmod 3.$$

Proof. Part (iv) follows from (4.5) since $9 \mid (p-1)\cdot(q-1)$.
Other parts can be proved analogously to [Br1, Theorem 2.4]. ∎

REMARK. (i) also follows from Theorem 2.3, and (iv) can be obtained from Theorem 3.6.

4.3. *The 2-rank of $K_2\mathcal{O}_F$*

LEMMA 4.3. *2 splits in F if and only if A is even.*

Proof. The polynomial defined by (4.4) satisfies $g(X) \equiv X^3 + X + A \pmod 2$. Hence by the Hensel lemma $g(X)$ splits in $\mathbb{Q}_2[X]$ iff A is even iff 2 splits in F. ∎

COROLLARY 4.4. *We have*

$$2\text{-rank}\, K_2\mathcal{O}_F = 2\text{-rank}\,\mathrm{Cl}(\mathcal{O}_{F,2}) + \begin{cases} 3 & \textit{if } A \textit{ is odd},\\ 5 & \textit{if } A \textit{ is even}.\end{cases}$$

Proof. By Lemmas 2.1 and 4.3. ∎

4.4. *The 3-rank of $K_2\mathcal{O}_F$*

PROPOSITION 4.5. $1 \leq 3\text{-rank}\, K_2\mathcal{O}_F \leq 4$.

PROPOSITION 4.6. $3\text{-rank}\, A_E \geq 2$. *Moreover*, $3\text{-rank}\, A_E = 2$ *if and only if* $3 \parallel \# K_2\mathcal{O}_F$.

Proof. This result easily follows from Theorem 3.3, Lemma 2.3, Corollary 3.7 and Proposition 4.5. ∎

4.5. *The case $\ell = p$ or q.* Suppose $\ell = p$. Let $E = F(\zeta_p)$, where F is the cubic cyclic field defined above.

LEMMA 4.7. *Let f be the order of p (mod q). If $3 \mid f$ and $q-1$ is not divisible by 9, then for $j \neq 0$, $\lambda : \varepsilon_j A \to \varepsilon_j \lambda(A)$ is an isomorphism.*

Proof. Since the inertia index of p in $\mathbb{Q}(\zeta_{pq})$ is f, we have $f \mid q-1$. If $3 \mid f$, then $f \nmid \frac{q-1}{3}$. As $[E : \mathbb{Q}(\zeta_p)] = 3$, the inertia index of p in E is 3. Thus prime divisors $\wp$ of p in F are not split in E. It follows that $\sigma\wp = \wp$ for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$.

Since λ commutes with the action of σ, we have $\lambda(\varepsilon_j A) = \varepsilon_j \lambda(A)$, i.e. λ is surjective. Moreover, the group $\mathrm{Ker}(\lambda)$ is generated by the classes containing prime ideals $\wp$ of E which divide p. Consequently, $\mathrm{Ker}(\lambda) \cap A \subset A^G = \varepsilon_0 A$. Therefore $\mathrm{Ker}(\lambda) \cap \varepsilon_j A = 0$ for $j \neq 0$, and the lemma follows. ∎

LEMMA 4.8. *Let f be the order of p (mod q). If $f = q-1$, then for $j \neq 0$, $\lambda : \varepsilon_j A \to \varepsilon_j \lambda(A)$ is an isomorphism.*

Proof. Since $f = q-1$ and p does not split in E, it follows that prime divisors $\wp$ of p in F do not split in E. Consequently, by the same proof of Lemma 4.7, the lemma follows. ∎

THEOREM 4.9. *Under the conditions of Lemma 4.7 or Lemma 4.8,*

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

Proof. Since there is an exact sequence

$$0 \to (\mu_p \otimes \mathrm{Cl}(\mathcal{O}_E[1/p]))^G \to K_2\mathcal{O}_F/p \to \bigoplus_{p \in S'} \mu_p \to 0$$

(see [Ke, Theorem 5.4], and [Ge]), the theorem follows from (3.2), (3.3), Lemma 4.7 or Lemma 4.8, and [Br1, Lemma 4.2]. ∎

5. Some estimates of the ℓ-rank of $K_2\mathcal{O}_F$. Let $E = F(\zeta_\ell)$. Let L be the maximal unramified and elementary abelian ℓ-extension of E with the Galois group $H := \mathrm{Gal}(L/E)$. Let $B_0 := B/(E^*)^\ell$. By the arguments in Section 3, for every $b \in E^*$ and $b_0 := b(E^*)^\ell$, we have $b_0 \in B_0$ iff b is singular primary, i.e. $(b) = \wp^\ell$ for some ideal $\wp$ of E and

$$x^\ell \equiv b \ (\mathrm{mod}\, \ell(1-\zeta_\ell)) \quad \text{for some } x \in E^* \tag{5.1}$$

(see [Wa, Exercise 9.3]).

Let U_E be the group of units of $\mathcal{O}_E$, and denote by U'_E its subgroup of units u satisfying (5.1). Such a u is called a *singular primary unit*. It is easy to see that $U_E^\ell \subseteq U'_E$ and $\mathrm{Ker}(\varphi) = U'_E/U_E^\ell$, where φ is defined in Section 3 (see [Br2, (3.1)]).

Theorem 5.1. *Let F be as above and let $E = F(\zeta_\ell)$. For $\ell \neq p, q$, we have*

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

Proof. See the proof of [Br1, Theorem 5.3]. ∎

Corollary 5.2. *Under the conditions of Theorem* 5.1, *if* ℓ-rank $A_E = 0$, *then* $\ell\text{-rank}\,K_2\mathcal{O}_F = \ell\text{-rank}\,\varepsilon_2(U'_E/U^\ell_E)$.

In Theorem 5.1, we give some estimates of the ℓ-rank of $K_2\mathcal{O}_F$ in terms of the ℓ-ranks of some subgroups of the class group and of the group of singular primary units (modulo ℓth powers) of the field $E = F(\zeta_\ell)$. Unfortunately, for large prime numbers ℓ, the degree $(E : \mathbb{Q}) = 3(\ell - 1)$ 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. By part 5 of [Br1], E can be replaced by its proper subfields.

Recall that σ, τ are generators of $G := \mathrm{Gal}(\mathbb{Q}(\zeta_\ell)/\mathbb{Q})$ and $T := \mathrm{Gal}(F/\mathbb{Q})$, respectively, where $\ell \equiv 1 \pmod 6$. For every subfield L of E we define U'_L to be the group of singular primary units in L, i.e.

$$U'_L = U'_E \cap L.$$

Theorem 5.3. *Let $t = (\ell - 1)/2$, $r = (\ell - 1)/6$, and let E_j be the subfield of E fixed by the group $T_j = \langle \sigma^t, \sigma^{rj}\tau^{-1}\rangle$, where $j = 0, 1, 2$. If $\ell \neq p, q$, then*

$$\max_{0\le j\le 2} \ell\text{-rank}\,\varepsilon_2(U'_{E_j}/U^\ell_{E_j}) \le \ell\text{-rank}\,K_2\mathcal{O}_F \le \sum_{j=0}^{2} \ell\text{-rank}\,\varepsilon_2 A_{E_j} + \sum_{j=0}^{2} \ell\text{-rank}\,\varepsilon_2(U'_{E_j}/U^\ell_{E_j}).$$

Moreover, if the class number of the field $\mathbb{Q}(\zeta_\ell)$ is not divisible by ℓ, and in the field $L_0 := E_1 \cap E_2$ we have $U'_{L_0}/U^\ell_{L_0} = 1$, then

$$\sum_{j=0}^{2} \ell\text{-rank}\,\varepsilon_2(U'_{E_j}/U^\ell_{E_j}) \le \ell\text{-rank}\,K_2\mathcal{O}_F \le \sum_{j=0}^{2} \ell\text{-rank}\,\varepsilon_2 A_{E_j} + \sum_{j=0}^{2} \ell\text{-rank}\,\varepsilon_2(U'_{E_j}/U^\ell_{E_j}).$$

6. Application. Using PARI-GP, we apply the above results and the following two lemmas (see [Br1, Lemmas 6.1 and 7.1]) to determine the structure of $K_2\mathcal{O}_F$, where F is a cubic cyclic field with two ramified primes p, q, $7 \le p, q \le 100$.

6.1. *Important lemmas*

LEMMA 6.1. *Let a cyclic group $G = \langle\sigma\rangle$ of order* 6 *act on an elementary abelian* 7*-group A, and let $a \in A$.*

(i) *If*

$$(1 + \sigma + \sigma^2)a = 1 \tag{6.1}$$

then $\varepsilon_j a = 1$ for $j = 0, 1, 3, 5$.

(ii) *Moreover*,

$$\sigma(a) = a^2 \quad \textit{iff} \quad (\varepsilon_2 a = a \textit{ and } (6.1) \textit{ holds}),$$
$$\sigma(a) = a^4 \quad \textit{iff} \quad (\varepsilon_4 a = a \textit{ and } (6.1) \textit{ holds}).$$

LEMMA 6.2. *Let a cyclic group $G = \langle\sigma\rangle$ of order* 12 *act on an elementary abelian* 13*-group A, and let $a \in A$.*

(i) *If*

$$(1 + \sigma^2 + \sigma^4)a = 1 \quad \textit{and} \quad (1 + \sigma^3)a = 1, \tag{6.2}$$

then $\varepsilon_j a = 1$ for $0 \le j \le 11$, $j \ne 2, 10$.

(ii) *Moreover*,

$$\sigma(a) = a^4 \quad \textit{iff} \quad (\varepsilon_2 a = a \textit{ and } (6.2) \textit{ holds}),$$
$$\sigma(a) = a^{10} \quad \textit{iff} \quad (\varepsilon_{10} a = a \textit{ and } (6.2) \textit{ holds}).$$

6.2. *Computation of the 2-rank and 3-rank of $K_2\mathcal{O}_F$.* The structure of the 2-primary part of $K_2\mathcal{O}_F$ can be determined by Corollary 4.4, except for the following four cases: $p = 19$, $q = 61$, $A = -44$; $p = 37$, $q = 61$, $A = 46$; $p = 7$, $q = 97$, $A = 4$; $p = 13$, $q = 73$, $A = 58$. However, for the above four fields, 2-rank $\mathrm{Cl}(\mathcal{O}_{F,2}) = 0$ and the fundamental unit ε_1 is not totally positive by GP. Thus we can apply the inequality of Theorem 2.6.

To determine the structure of the 3-primary part of $K_2\mathcal{O}_F$ we use Theorem 3.3. For $p = 7$, $q = 79$, $A = -5$ and $p = 43$, $q = 79$, $A = -95$, we obtain 9-rank $(K_2\mathcal{O}_F) = 2$ by Corollary 3.12.

6.3. *Computation of the 7-rank of $K_2\mathcal{O}_F$.* We compute the 7-rank of $K_2\mathcal{O}_F$ via the 7-ranks of other groups appearing in Theorem 5.3. The arguments are similar to those in Section 6 of [Br1], so we omit some details.

For fixed primitive roots g modulo p, and h modulo q, where $p, q \equiv 1 \pmod 6$ are primes, we have defined the Gauss sums

$$\alpha_1 = \sum_{j\in H} \zeta^j, \quad \alpha_2 = \sum_{j\in aH} \zeta^j, \quad \alpha_3 = \sum_{j\in a^2H} \zeta^j.$$

If we replace g by g^{-1} and h by h^{-1} then α_2 and α_3 permute, hence the number $(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$ changes sign.

We shall assume henceforth that primitive roots g modulo p and h modulo q are chosen in such a way that

$$(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)>0.$$

In particular, for the prime 7, we choose the primitive root 3. Then the Gauss periods are

$$\gamma_1=\zeta_7+\zeta_7^{-1}=1.24,\quad \gamma_2=\zeta_7^3+\zeta_7^{-3}=-1.80,\quad \gamma_3=\zeta_7^2+\zeta_7^{-2}=-0.44,$$

hence $(\gamma_1-\gamma_2)(\gamma_2-\gamma_3)(\gamma_3-\gamma_1)>0$, and $\gamma_1,\gamma_2,\gamma_3$ are the roots of the polynomial $f(X)=X^3+X^2-2X-1$.

We denote by σ the automorphism of the field $\mathbb{Q}(\zeta_7)$ satisfying $\sigma(\zeta_7)=\zeta_7^3$. Then $\sigma(\gamma_i)=\gamma_{i+1}$, where the indices are taken modulo 3.

We recall that the field F is generated by any root β_i of the polynomial

$$g(X)=X^3-3pqX+Apq.$$

From our assumption on primitive roots it follows that

$$(\beta_1-\beta_2)(\beta_2-\beta_3)(\beta_3-\beta_1)=27(\alpha_1-\alpha_2)(\alpha_2-\alpha_3)(\alpha_3-\alpha_1)>0.$$

Moreover, the automorphism $\tau\in\mathrm{Gal}(\mathbb{Q}(\zeta_{pq})/\mathbb{Q})$ given by $\tau(\zeta_{pq})=\zeta_{pq}^a$ satisfies $\tau(\beta_i)=\beta_{i+1}$, where the indices are taken modulo 3.

It then follows from [Br1, 6.1] that $E_0=\mathbb{Q}(\zeta_7)^+=\mathbb{Q}(\gamma_i)$, $E_1=\mathbb{Q}(\varrho_1)$, $E_2=\mathbb{Q}(\varrho_2)$, where

$$\varrho_1=\gamma_1\beta_1+\gamma_2\beta_3+\gamma_3\beta_2,\qquad \varrho_2=\gamma_1\beta_1+\gamma_2\beta_2+\gamma_3\beta_3.$$

Applying the Viète formulas one can verify that the minimal polynomials for ϱ_1 and ϱ_2 are, respectively,

$$g_1(X)=X^3-21pqX+7pq\,\frac{A-27B}{2},$$
$$g_2(X)=X^3-21pqX+7pq\,\frac{A+27B}{2}.$$

If $p,q\neq 7$, then $A^2-B^2\equiv A^2+27B^2=4pq\not\equiv 0 \pmod 7$. So $A\not\equiv\pm B \pmod 7$. Hence, $g_j(X)$ is an Eisenstein polynomial with respect to 7. Consequently, every unit $u=a_0+a_1x+a_2x^2\in U_{E_j}$ is a singular primary unit iff $u\equiv 1 \pmod{7x}$ or equivalently,

$$a_0\equiv 1 \pmod{49},\qquad a_1\equiv a_2\equiv 0 \pmod 7$$

where $x:=\varrho_j$ (see [Br1, 6.4]). Finally, we can determine the 7-rank of $K_2\mathcal{O}_F$ in terms of Theorem 5.3 and Lemma 6.1, except for $p=7$, $q=73$, $A=-44$ and $p=7$, $q=97$, $A=4$. The results of the computations are given in Table 3, where we used the following shorthand notation, for $j=1,2$:

$$v_7:=v_7(\#K_2\mathcal{O}_F),\qquad d_j:=7\text{-rank}\,\varepsilon_2(U'_{E_j}/U^7_{E_j}),\qquad h_j:=7\text{-rank}\,\varepsilon_2A_{E_j},$$

and $(K_2\mathcal{O}_F)_7$ is the 7-primary part of $K_2\mathcal{O}_F$.

6.4. *Computation of the 13-rank of $K_2\mathcal{O}_F$.* The arguments are similar to those in Section 7 of [Br1], so we omit some details.

Let $\gamma_j = \zeta_{13}^{2^j} + \zeta_{13}^{-2^j}$, $1 \le j \le 6$. Then $E_0 = \mathbb{Q}(\gamma_j)$. Define

$$\varrho_1 = \gamma_1\beta_1 + \gamma_5\beta_2 + \gamma_3\beta_3, \qquad \varrho_2 = \gamma_1\beta_1 + \gamma_3\beta_2 + \gamma_5\beta_3.$$

Then $E_j = \mathbb{Q}(\varrho_j)$ for $j = 1, 2$. Assume

$$\lambda_1 = (\gamma_1 + \gamma_4)\beta_1 + (\gamma_2 + \gamma_5)\beta_2 + (\gamma_3 + \gamma_6)\beta_3,$$
$$\lambda_2 = (\gamma_1 + \gamma_4)\beta_1 + (\gamma_3 + \gamma_6)\beta_2 + (\gamma_2 + \gamma_5)\beta_3.$$

Then $F_j := \mathbb{Q}(\lambda_j)$ is a cubic subfield of E_j, $j = 1, 2$.

There are three fields F corresponding to primes $7 \le p,\ q < 100$ such that $13^2 \mid \#K_2\mathcal{O}_F$. Namely,

$$p = 31, \quad q = 43, \quad A = -38,$$
$$p = 31, \quad q = 61, \quad A = -83,$$
$$p = 37, \quad q = 43, \quad A = -71.$$

In the above list, there are no nontrivial singular primary units in F_j. Similarly, we can determine the 13-rank of $K_2\mathcal{O}_F$ in terms of Theorem 5.3 and Lemma 6.2. The results of the computations are given in Table 4, where we used the following shorthand notation, for $j = 1, 2$:

$$v_{13} := v_{13}(\#K_2\mathcal{O}_F), \quad u_j := 13\text{-rank}\,\varepsilon_2(U'_{E_j}/U_{E_j}^{13}), \quad w_j := 13\text{-rank}\,\varepsilon_2 A_{E_j},$$

and $(K_2\mathcal{O}_F)_{13}$ is the 13-primary part of $K_2\mathcal{O}_F$.

6.5. *Description of the tables.* The field F in Table 1 is the fixed field of H_3, and F in Table 2 is the fixed field of H_4, where H_3, H_4 are defined in Section 4. The first and second columns of Tables 1 and 2 list all primes $p, q \equiv 1 \pmod 6$, $7 \le p, q < 100$, and the third the corresponding values of A. The fourth and fifth columns give the orders of $K_2\mathcal{O}_F$; moreover the fifth column provides information about the structure of the group $K_2\mathcal{O}_F$. We use the same convention as in [Br1]. That is, if the order of a group is written in the form $(n_1)^{k_1}(n_2)^{k_2}\ldots$, it means that the group is isomorphic to the product of k_1 copies of $\mathbb{Z}/n_1$, k_2 copies of $\mathbb{Z}/n_2$, etc. However, if a factor $(n_j^{k_j})$ is written in **bold** type, it means that there is a direct summand of order $n_j^{k_j}$, but its structure is unknown. Thus $(2)^2$ means $\mathbb{Z}/2 \times \mathbb{Z}/2$, and (2^2) means $\mathbb{Z}/4$, but $(\mathbf{31^2})$ means a group of order 31^2, i.e. one of the groups $\mathbb{Z}/31 \times \mathbb{Z}/31$ and $\mathbb{Z}/31^2$.

The sixth column of Tables 1 and 2 gives the class group of $E = F(\zeta_3)$, and the seventh column the class group of F. We use the same convention here, e.g. $(2)^2$ means $\mathbb{Z}/2 \times \mathbb{Z}/2$.

Table 1

p	q	A	$\#K_2\mathcal{O}_F$	$K_2\mathcal{O}_F$	$\mathrm{Cl}(\mathcal{O}_E)$	$\mathrm{Cl}(\mathcal{O}_F)$
7	13	−11	3624	$(2)^3(3)(151)$	(6)(6)	(3)
7	19	−17	11112	$(2)^3(3)(463)$	(6)(6)	(3)
7	31	25	54168	$(2)^3(3)(37)(61)$	(6)(6)	(3)
7	37	19	65544	$(2)^3(3)(2731)$	(21)(3)	(3)
7	43	31	127032	$(2)^3(3)(67)(79)$	(12)(12)	(3)
7	61	−41	256200	$(2)^3(3)(5)^2(7)(61)$	(57)(3)	(3)
7	67	43	339768	$(2)^3(3)(9)(11)^2(13)$	(21)(3)(3)	(3)
7	73	−44	1048992	$(2)^5(3)(\mathbf{7^2})(223)$	(21)(3)	(3)
7	79	−5	898776	$(2)^3(3^2)^2(19)(73)$	(6)(6)(3)	(3)
7	97	−23	1462344	$(2)^3(3)(13)(43)(109)$	(42)(6)	(3)
13	19	4	161376	$(2)^5(3)(41)^2$	(6)(6)	(3)
13	31	37	299544	$(2)^3(3)(7)(1783)$	(12)(12)	(3)
13	37	−14	897504	$(2)^5(3)(9349)$	(39)(3)	(3)
13	43	7	864024	$(2)^3(3)(7)(37)(139)$	(42)(6)	(3)
13	61	−38	3805344	$(2)^5(3)^2(73)(181)$	(9)(3)(3)	(3)
13	67	28	5986944	$(2)^3(4)^2(3)^2(5197)$	(9)(3)(3)	(3)
13	73	−23	2859192	$(2)^3(3)(9)(7)(31)(61)$	(9)(9)(3)	(3)
13	79	−56	12362784	$(2)^5(3)(7)(18397)$	(42)(6)	(3)
13	97	34	21712608	$(2)^5(3)^2(75391)$	(42)(6)(3)	(21)
19	31	13	958488	$(2)^3(3)(39937)$	(42)(6)	(3)
19	37	52	2743200	$(2)^5(3)^3(5)^2(127)$	(3)(3)(3)(3)	(3)
19	43	55	2931864	$(2)^3(3)(13)(9397)$	(12)(12)	(3)
19	61	−44	13558272	$(2)^3(8)^2(3)(7)(13)(97)$	(21)(3)	(3)
19	67	58	15608544	$(2)^5(3)(7)(23227)$	(39)(3)	(3)
19	73	−65	10502424	$(2)^3(3)^2(199)(733)$	(57)(3)(3)	(3)
19	79	46	36295296	$(2)^3(4)^2(3)(31)(3049)$	(12)(12)	(3)
19	97	−80	75614112	$(2)^5(3)^2(37507)$	(6)(6)(3)	(3)
31	37	−5	5670168	$(2)^3(3)(7)(33751)$	(57)(3)	(3)
31	43	−38	25812384	$(2)^5(3)(13^2)(37)(43)$	(42)(6)	(3)
31	61	−83	23147592	$(2)^3(3)(13^3)(439)$	(309)(3)	(3)
31	67	−71	29962728	$(2)^3(3)^2(416149)$	(63)(3)(3)	(3)
31	73	67	37733928	$(2)^3(3)(1572247)$	(33)(33)	(3)
31	79	61	77666904	$(2)^3(3)(9)(7)(31)(1657)$	(12)(12)(3)	(3)
31	97	−11	135219048	$(2)^3(3)(\mathbf{19^2})(15607)$	(222)(6)	(3)
37	43	−71	14313624	$(2)^3(3)(13^2)(3529)$	(291)(3)	(3)
37	61	46	88948224	$(2)^3(8)^2(3)^2(97)(199)$	(21)(3)(3)	(3)
37	67	−68	122215776	$(2)^5(3)(151)(8431)$	(111)(3)	(3)
37	73	79	64652472	$(2)^3(3)^3(299317)$	(57)(3)(3)(3)	(3)
37	79	−80	225283488	$(2)^5(3)(1303)(1801)$	(777)(3)	(21)
37	97	118	344603616	$(2)^5(3)(7)(512803)$	(111)(3)	(3)
43	61	85	67778232	$(2)^3(3)(307)(9199)$	(93)(3)	(3)
43	67	−101	82812192	$(2)^5(3)(862627)$	(222)(6)(2)(2)	(6)(2)
43	73	109	114663192	$(2)^3(3)(7)(682519)$	(219)(3)	(3)
43	79	−41	190302936	$(2)^3(3)(19)(417331)$	(294)(6)	(3)

Table 1 (cont.)

p	q	A	$\#K_2\mathcal{O}_F$	$K_2\mathcal{O}_F$	$\mathrm{Cl}(\mathcal{O}_E)$	$\mathrm{Cl}(\mathcal{O}_F)$
43	97	103	378152664	$(2)^3(3)(43)(61)(6007)$	(114)(6)	(3)
61	67	124	741179616	$(2)^5(3)(7720621)$	(78)(6)	(3)
61	73	−125	458621016	$(2)^3(3)(7)(2729887)$	(84)(12)	(3)
61	79	−32	864177792	$(2)^3(4)^2(3)(67)(33589)$	(219)(3)	(3)
61	97	−50	1908361824	$(2)^5(3)(19)(283)(3697)$	(201)(3)	(3)
67	73	139	538985976	$(2)^3(3)(22457749)$	(156)(12)	(3)
67	79	−2	1235010912	$(2)^5(3)(43)(299179)$	(291)(3)	(3)
67	97	88	2137877664	$(2)^5(3)(13)(1713043)$	(291)(3)	(3)
73	79	19	628182888	$(2)^3(3)(67)(241)(1621)$	(651)(3)	(3)
73	97	−107	1284024696	$(2)^3(3)(97)(551557)$	(489)(3)	(3)
79	97	148	5012047584	$(2)^5(3)(9)(5800981)$	(42)(6)(3)(3)	(3)(3)

Table 2

p	q	A	$\#K_2\mathcal{O}_F$	$K_2\mathcal{O}_F$	$\mathrm{Cl}(\mathcal{O}_E)$	$\mathrm{Cl}(\mathcal{O}_F)$
7	13	16	5856	$(2)^5(3)(61)$	(3)(3)	(3)
7	19	10	20256	$(2)^5(3)(211)$	(3)(3)	(3)
7	31	−29	34632	$(2)^3(3)^2(13)(37)$	(9)(3)(3)	(3)
7	37	−8	188448	$(2)^5(3)(13)(151)$	(6)(6)	(3)
7	43	−23	103128	$(2)^3(3)(4297)$	(21)(3)	(3)
7	61	40	677664	$(2)^5(3)^2(13)(181)$	(3)(3)(3)	(3)
7	67	−38	818592	$(2)^5(3)(8527)$	(21)(3)	(3)
7	73	37	498408	$(2)^3(3)(19)(1093)$	(39)(3)	(3)
7	79	22	1326048	$(2)^5(3)(19)(727)$	(21)(3)	(3)
7	97	4	2784768	$(2)^3(8)^2(3)(\mathbf{7^2})(37)$	(6)(6)(2)(2)	(6)(2)
13	19	31	49704	$(2)^3(3)(13)(109)$	(21)(3)	(3)
13	31	−17	234312	$(2)^3(3)(13)(751)$	(57)(3)	(3)
13	37	−41	516264	$(2)^3(3)(7)^2(439)$	(12)(12)	(3)
13	43	−47	566568	$(2)^3(3)(9)(43)(61)$	(21)(3)(3)	(3)
13	61	43	1709016	$(2)^3(3)(71209)$	(129)(3)	(3)
13	67	−53	2515416	$(2)^3(3)(163)(643)$	(39)(3)	(3)
13	73	58	6418944	$(2)^3(8)^2(3)^2(7)(199)$	(6)(6)(6)(2)	(6)(2)
13	79	−29	3594264	$(2)^3(3)(31)(4831)$	(15)(15)	(3)
13	97	61	7078344	$(2)^3(3)(7^2)(13)(463)$	(147)(3)	(21)
19	31	−41	739176	$(2)^3(3)(19)(1621)$	(39)(3)	(3)
19	37	25	1839744	$(2)^3(4)^2(3)^2(1597)$	(12)(12)(3)	(6)(2)
19	43	1	1819608	$(2)^3(3)(7)(10831)$	(57)(3)	(3)
19	61	37	5262936	$(2)^3(3)(7)(31327)$	(129)(3)	(3)
19	67	−23	6756504	$(2)^3(3)(43)(6547)$	(147)(3)	(3)
19	73	16	21341088	$(2)^5(3)^2(74101)$	(21)(3)(3)	(3)
19	79	73	12409944	$(2)^3(3)(517081)$	(129)(3)	(3)
19	97	−53	20646792	$(2)^3(3)(9)(61)(1567)$	(63)(3)(3)	(3)

Table 2 (cont.)

p	q	A	$\#K_2\mathcal{O}_F$	$K_2\mathcal{O}_F$	$\mathrm{Cl}(\mathcal{O}_E)$	$\mathrm{Cl}(\mathcal{O}_F)$
31	37	49	7427616	$(2)^5(3)(7^2)(1579)$	(156)(12)	(6)(2)
31	43	70	21462912	$(2)^3(4)^2(3)^2(31)(601)$	(6)(6)(6)(2)	(6)(2)
31	61	79	25413864	$(2)^3(3)(7)(151273)$	(129)(3)	(3)
31	67	91	30947424	$(2)^5(3)(31)(10399)$	(258)(6)(2)(2)	(6)(2)
31	73	−95	43262232	$(2)^3(3)(13)(138661)$	(903)(3)	(21)
31	79	7	51167256	$(2)^3(3)(7)(151)(2017)$	(687)(3)	(3)
31	97	−65	101213592	$(2)^3(3)(4217233)$	(183)(3)	(3)
37	43	−17	21571224	$(2)^3(3)(193)(4567)$	(42)(6)	(3)
37	61	−35	46722312	$(2)^3(3)(9)(7)(13)(2377)$	(63)(3)(3)	(3)
37	67	13	49912152	$(2)^3(3)(61)(103)(331)$	(471)(3)	(3)
37	73	−2	166536288	$(2)^5(3)^2(578251)$	(21)(3)(3)	(3)
37	79	−107	115300248	$(2)^3(3)(7)(61)(11251)$	(186)(6)	(21)
37	97	91	259724472	$(2)^3(3)(7)(43)(157)(229)$	(84)(12)	(3)
43	61	−77	64650600	$(2)^3(3)^2(5)^2(7^2)(733)$	(63)(9)(3)	(3)
43	67	61	78701064	$(2)^3(3)(13)(31)(79)(103)$	(399)(3)	(3)
43	73	−53	99880008	$(2)^3(3)(4161667)$	(453)(3)	(3)
43	79	−95	146562696	$(2)^3(3^2)^2(7)(79)(409)$	(93)(3)(3)	(3)
43	97	49	253136184	$(2)^3(3)(7)(43)(67)(523)$	(813)(3)	(3)
61	67	−119	335806632	$(2)^3(3)^2(7)(31)(21493)$	(126)(6)(3)	(3)
61	73	118	952235808	$(2)^5(3)(97)(102259)$	(114)(6)	(3)
61	79	49	429057312	$(2)^5(3)(4469347)$	(222)(6)(2)(2)	(6)(2)
61	97	31	664492968	$(2)^3(3)^2(9229069)$	(219)(3)(3)	(3)
67	73	−104	1305878496	$(2)^5(3)(13)(103)(10159)$	(24)(24)	(3)
67	79	−83	479092632	$(2)^3(3)(19962193)$	(579)(3)	(3)
67	97	7	953343384	$(2)^3(3)(7)(5674663)$	(741)(3)	(3)
73	79	100	1710388608	$(2)^3(4)^2(3)(283)(15739)$	(84)(12)	(6)(2)
73	97	−26	2789750688	$(2)^5(3)(571)(50893)$	(201)(3)	(3)
79	97	175	1737265608	$(2)^3(3)^2(13)(19)(97687)$	(1953)(3)(3)(3)	(21)(3)

Table 3

p	q	A	v_7	d_1	d_2	h_1	h_2	7-rank $K_2\mathcal{O}_F$	$(K_2\mathcal{O}_F)_7$
13	37	−41	2	1	1	0	0	2	$(7)^2$
13	97	61	2	0	1	0	0	1	(7^2)
31	37	49	2	0	1	0	0	1	(7^2)
43	61	−77	2	1	0	0	0	1	(7^2)

Table 4

p	q	A	v_{13}	u_1	u_2	w_1	w_2	13-rank $K_2\mathcal{O}_F$	$(K_2\mathcal{O}_F)_{13}$
31	43	−38	2	0	1	0	0	1	(13^2)
31	61	−83	3	1	0	0	0	1	(13^3)
37	43	−71	2	0	1	0	0	1	(13^2)

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.

[Co] H. Cohen, *A Course in Computational Algebraic Number Theory*, Springer, 1996.

[CH] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, World Sci., 1988.

[CR] G. Cornell and M. Rosen, *Group-theoretic constraints on the structure of the class group*, J. Number Theory 13 (1981), 1–11.

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

[Gr] M. N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de* $\mathbb{Q}$, J. Reine Angew. Math. 277 (1975), 89–116.

[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, *A relation between the* 2*-primary parts of the main conjecture and the Birch–Tate conjecture*, Canad. Math. Bull. 32 (1989), 248–251.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbb{Q}$, Invent. Math. 76 (1984), 179–330.

[Wa] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1982.

[Wi] A. Wiles, *The Iwasawa conjecture for totally real fields*, Ann. of Math. 131 (1990), 493–540.

Department of Mathematics
Nanjing Normal University
Nanjing 210097, P.R. China
E-mail: haiyanxiaodong@gmail.com

Received on 23.1.2006 (5130)