Tôhoku Math. J.
44 (1992), 557–565

THE 2-CLASS GROUPS OF CUBIC FIELDS AND 2-DESCENTS ON ELLIPTIC CURVES

MAYUMI KAWACHI AND SHIN NAKANO*

(Received November 5, 1991, revised January 27, 1992)

Abstract. We investigate the relationship between the 2-class groups of cubic fields and the Mordell-Weil groups of elliptic curves defined over $\boldsymbol{Q}$. There is an exact sequence which connects those two groups together for a certain kind of cyclic cubic fields. Using the twists of elliptic curves, we give a more precise result for the simplest cubic fields.

Introduction. In [8], Washington proved a theorem giving a relationship between the 2-class groups (i.e. the 2-Sylow subgroups of the ideal class groups) of cyclic cubic fields and the Mordell-Weil groups of elliptic curves defined over $\boldsymbol{Q}$. The fields that he treated are called the simplest cubic fields which have been studied in detail by Shanks [5], and besides him, Cohn [2], Uchida [7] and Nakano [4]. In fact, these fields and the associated elliptic curves are defined by cubic polynomials in a special form (see §2), and Washington's proof depends on properties peculiar to that form.

In the present paper, we first discuss the relationship between 2-class groups and elliptic curves from a general viewpoint, and try to extend Washington's result to some other kinds of cubic polynomials. We then regard the cubic fields as the 2-division fields of elliptic curves defined over $\boldsymbol{Q}$ with no rational point of order two. One cubic field may be attached to several elliptic curves which are not isomorphic to one another over $\boldsymbol{Q}$, as twisted curves. In the last section, we deal simultaneously with the elliptic curve and its twist which are related to one simplest cubic field, and utilize this technique to improve the result of Washington.

The authors wish to thank Professors Shôkichi Iyanaga and Norio Adachi for their valuable suggestion and warm encouragement.

NATATION. For an abelian group A and its element a, let $[a]$ denote the coset represented by a of the factor group $A/2A$ (or A/A^2 if the group law is written multiplicatively). If V is a vector space over $\boldsymbol{Z}/2\boldsymbol{Z}$, we denote its dimension by $\mathrm{rk}_2(V)$. For any elliptic curve, we always denote the identity of the group law by O. Let E be an elliptic curve defined over a number field k. The Mordell-Weil group, denoted by $E(k)$, is the group of k-rational points of E. We denote its rank over $\boldsymbol{Z}$ by $\mathrm{rank}\, E(k)$.

1991 *Mathematics Subject Classification.* Primary 11R16; Secondary 11G05, 11R29.

* Partly supported by the Grants-in-Aid for Encouragement of Young Scientists, The Ministry of Education, Science and Culture, Japan.

1. Preliminaries. Let K be a cubic field and $C_2(K)$ the 2-torsion subgroup of the ideal class group of K. We denote by $H_2(K)$ the subgroup of $K^\times/K^{\times 2}$ consisting of those cosets represented by α in $K^\times$ for which the principal ideal (α) is the square of an ideal of K and $N\alpha>0$, where N is the norm map from K to $\boldsymbol{Q}$. Let $\alpha\in K^\times$ with $[\alpha]\in H_2(K)$ and $\mathfrak{a}$ the ideal of K satisfying $\mathfrak{a}^2=(\alpha)$. Then the ideal class of $\mathfrak{a}$ is in $C_2(K)$ and depends only on the coset $[\alpha]$. Hence we have a homomorphism $H_2(K)\to C_2(K)$ defined by $[\alpha]\mapsto$ "the class of $\mathfrak{a}$". We denote its kernel by $V_2(K)$ and obtain an exact sequence

$$1\to V_2(K)\to H_2(K)\to C_2(K)\to 1\,. \tag{1}$$

The kernel $V_2(K)$ is the subgroup of $K^\times/K^{\times 2}$ whose elements can be represented by units with norm 1.

We now consider cubic fields related to elliptic curves. For the following argument, refer to [1] or [6, Chaps. 8, 10]. Let E be an elliptic curve defined over $\boldsymbol{Q}$. Assume that E has no rational point of order two. Then E is given in the form $y^2=f(x)$, where $f(x)$ is an irreducible monic polynomial in $\boldsymbol{Z}[x]$ of degree three. Let ρ_1, ρ_2 and ρ_3 be the roots of $f(x)$. The non-trivial 2-torsion points on E are $(\rho_1, 0)$, $(\rho_2, 0)$ and $(\rho_3, 0)$. Letting ρ represent any one of these roots, we suppose that $K=\boldsymbol{Q}(\rho)$. Then there is a homomorphism

$$\lambda\colon E(\boldsymbol{Q})\to K^\times/K^{\times 2}$$

defined by $(x, y)\mapsto[x-\rho]$ and $O\mapsto 1$, which induces an injective homomorphism

$$E(\boldsymbol{Q})/2E(\boldsymbol{Q})\to K^\times/K^{\times 2}\,.$$

In the following we will identify K with the $\boldsymbol{Q}$-algebra $\boldsymbol{Q}[T]/(f(T))$ by the correspondence $\rho\leftrightarrow T \bmod f(T)$.

Next we shall define the local homomorphisms in a similar way. Let p be a finite or infinite prime of $\boldsymbol{Q}$ and $\boldsymbol{Q}_p$ the completion of $\boldsymbol{Q}$ at p, that is, the field of p-adic or real numbers. We consider the $\boldsymbol{Q}_p$-algebra

$$K_p=\boldsymbol{Q}_p[T]/(f(T))\,,$$

instead of K in the global case. This is isomorphic to the direct sum of the completions $K_\mathfrak{p}$ of K at the primes $\mathfrak{p}$ lying above p; $K_p\simeq\bigoplus_{\mathfrak{p}|p}K_\mathfrak{p}$, and the group of the invertible elements in K_p is written as $K_p^\times\simeq\bigoplus_{\mathfrak{p}|p}K_\mathfrak{p}^\times$. If p is finite, we define a subgroup U_p of $K_p^\times$ as $U_p=\bigoplus_{\mathfrak{p}|p}U_\mathfrak{p}$, where $U_\mathfrak{p}$ is the unit group of $K_\mathfrak{p}$. Note that $\sum_{\mathfrak{p}|p}[K_\mathfrak{p}:\boldsymbol{Q}_p]=3$, therefore K_p is three-dimensional over $\boldsymbol{Q}_p$. As in the global case, one may define a homomorphism

$$\lambda_p\colon E(\boldsymbol{Q}_p)\to K_p^\times/K_p^{\times 2}$$

and an injection

$$E(\boldsymbol{Q}_p)/2E(\boldsymbol{Q}_p)\to K_p^\times/K_p^{\times 2}$$

by $O \mapsto 1$ and $(x, y) \mapsto [x - T \bmod f(T)]$ whenever $x - T \bmod f(T)$ is invertible in K_p.

The embedding $\iota_p\colon \boldsymbol{Q} \to \boldsymbol{Q}_p$, for each p, induces natural maps

$$E(\boldsymbol{Q}) \to E(\boldsymbol{Q}_p), \qquad K \to K_p, \qquad K^\times/K^{\times 2} \to K_p^\times/K_p^{\times 2}$$

and so on, which we will also denote by ι_p. One can verify the commutativity of the following diagram:

$$\begin{array}{ccccc} E(\boldsymbol{Q}) & \xrightarrow{\lambda} & K^\times/K^{\times 2} & \xrightarrow{\bar{N}} & \boldsymbol{Q}^\times/\boldsymbol{Q}^{\times 2} \\ \downarrow{\scriptstyle \iota_p} & & \downarrow{\scriptstyle \iota_p} & & \downarrow{\scriptstyle \iota_p} \\ E(\boldsymbol{Q}_p) & \xrightarrow[\lambda_p]{} & K_p^\times/K_p^{\times 2} & \xrightarrow[\bar{N}_p]{} & \boldsymbol{Q}_p^\times/\boldsymbol{Q}_p^{\times 2}. \end{array}$$

Here $\bar{N}$ and $\bar{N}_p$ are induced by the norm maps $N = N_{K/\boldsymbol{Q}}$ and $N_p = N_{K_p/\boldsymbol{Q}_p}$, respectively. Particularly, N_p is defined as follows: Choose a basis $\{e_1, e_2, e_3\}$ of K_p over $\boldsymbol{Q}_p$. For any $z \in K_p$, let $r_{ij}(z) \in \boldsymbol{Q}_p$ be such that $e_i z = \sum_{j=1}^3 r_{ij}(z) e_j$ $(i = 1, 2, 3)$, and set $N_p z = \det(r_{ij}(z))$. We remark that $\bar{N}(\operatorname{Im}\lambda) = 1$ and $\bar{N}_p(\operatorname{Im}\lambda_p) = 1$, which are useful later.

LEMMA 1. *Let p be a finite prime which satisfies at least one of the following*:

(a) *E has good reduction at p;*

(b) *p does not split in K.*

Then $\operatorname{Im}\lambda_p \subseteq U_p K_p^{\times 2}/K_p^{\times 2}$.

PROOF. For (a), refer to [1, 3.3, 3.4 and 3.6]. Suppose (b) holds. Then K_p is the cubic extension over $\boldsymbol{Q}_p$ and U_p is the unit group of K_p. Let α be an element of $K_p^\times$ satisfying $[\alpha] \in \operatorname{Im}\lambda_p$. Then, as $\bar{N}_p(\operatorname{Im}\lambda_p) = 1$, we have $N_p\alpha \in \boldsymbol{Q}_p^{\times 2}$. Thus the order of $N_p\alpha$ at p is even. Since the residue degree for $K_p/\boldsymbol{Q}_p$ is 1 or 3, the order of α at the prime of K above p must be even, consequently $\alpha \in U_p K_p^{\times 2}$. □

Now $S_2(E)$ denotes the Selmer group of $E/\boldsymbol{Q}$ for 2-descent. In our case, we can identify this with the subgroup of $K^\times/K^{\times 2}$ given as follows:

$$S_2(E) = \{\xi \in K^\times/K^{\times 2} \mid \iota_p(\xi) \in \operatorname{Im}\lambda_p \text{ for all } p \leq \infty\}.$$

Since $\iota_p(\operatorname{Im}\lambda) \subseteq \operatorname{Im}\lambda_p$ for any prime p, we have $\operatorname{Im}\lambda \subseteq S_2(E)$. So λ induces an injective homomorphism $E(\boldsymbol{Q})/2E(\boldsymbol{Q}) \to S_2(E)$. The cokernel of this map is called the 2-torsion subgroup of the Shafarevich-Tate group of $E/\boldsymbol{Q}$. Denoting it by $Ш_2(E)$, we obtain the fundamental exact sequence

$$1 \to E(\boldsymbol{Q})/2E(\boldsymbol{Q}) \to S_2(E) \to Ш_2(E) \to 1. \tag{2}$$

We will discuss the relationship between $C_2(K)$ and $E(\boldsymbol{Q})/2E(\boldsymbol{Q})$ which are arranged in the exact sequences (1) and (2) separately. The following lemma links the two sequences together, via $H_2(K)$ and $S_2(E)$.

LEMMA 2. *Suppose every finite prime p satisfies either Condition* (a) *or* (b) *of Lemma* 1. *Then* $S_2(E) \subseteq H_2(K)$.

PROOF. Let $\alpha \in K^\times$ with $[\alpha] \in S_2(E)$. Then $\iota_p([\alpha]) \in \operatorname{Im} \lambda_p$ for all primes $p \leq \infty$. In particular, the condition at $p = \infty$ implies that $\iota_\infty(N\alpha) \in \boldsymbol{Q}_\infty^{\times 2} = \boldsymbol{R}^{\times 2}$. This means that $N\alpha$ is positive. On the other hand, for any finite prime p, it follows from Lemma 1 that $\iota_p(\alpha) \in U_p K_p^{\times 2}$, which shows that the order of α at any prime of K above p is even. Hence the principal ideal (α) is a square. □

2. 2-class groups and elliptic curves. In this section, we deal with cyclic cubic fields, and relate their 2-class groups to the Mordell-Weil groups of the associated elliptic curves. For an elliptic curve E defined over $\boldsymbol{Q}$, we put

$$E^\circ(\boldsymbol{Q}) = \operatorname{Ker}([\cdot] \circ \iota_\infty : E(\boldsymbol{Q}) \to E(\boldsymbol{R})/2E(\boldsymbol{R})) .$$

In other words, $E^\circ(\boldsymbol{Q})$ is the subgroup of $E(\boldsymbol{Q})$ consisting of those points in the connected component of the identity for the real curve $E(\boldsymbol{R})$. Clearly $2E(\boldsymbol{Q}) \subseteq E^\circ(\boldsymbol{Q})$.

PROPOSITION. *Let $f(x)$ be an irreducible monic polynomial in $\boldsymbol{Z}[x]$ of degree three, and K the cubic field determined by $f(x)$. Assume that $K/\boldsymbol{Q}$ is cyclic. Let E be the elliptic curve defined over $\boldsymbol{Q}$ given by $y^2 = f(x)$, and assume that E has a rational point in the form $(a, 1) \in E(\boldsymbol{Q}) - E^\circ(\boldsymbol{Q})$ with $a \in \boldsymbol{Z}$. Moreover assume that for every prime number p, either Condition* (a) *or* (b) *of Lemma* 1 *holds. Then*

$$\operatorname{rk}_2(C_2(K)) \geq \operatorname{rk}_2(E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q})) = \operatorname{rank} E(\boldsymbol{Q}) - 1 .$$

In fact, there is an exact sequence

$$1 \to E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q}) \to C_2' \to Ш_2(E) \to 1 ,$$

where C_2' is a subgroup of $C_2(K)$.

PROOF. Put $P = (a, 1)$. First, we note that $\operatorname{rk}_2(\operatorname{Im} \lambda_\infty) = 1$ ([1, 3.7]) and then $E(\boldsymbol{R})/2E(\boldsymbol{R})$ is generated by the coset $[\iota_\infty(P)]$, for $\iota_\infty(P) \notin 2E(\boldsymbol{R})$. Thus, by the definition of $E^\circ(\boldsymbol{Q})$, we obtain the decomposition

$$E(\boldsymbol{Q})/2E(\boldsymbol{Q}) = (E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q})) \oplus \langle [P] \rangle .$$

Consequently, $\operatorname{rank} E(\boldsymbol{Q}) = \operatorname{rk}_2(E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q})) + 1$, since E has no rational point of order two. Next we see that $S_2(E) \subseteq H_2(K)$ by Lemma 2. Restricting the last map $H_2(K) \to C_2(K)$ in (1) to $S_2(E)$, we have an exact sequence

$$1 \to V_2' \to S_2(E) \to C_2' \to 1 ,$$

where V_2' and C_2' are subgroups of $V_2(K)$ and $C_2(K)$, respectively. We now compute the kernel V_2'. Let ε be a unit of K such that $[\varepsilon] \in S_2(E)$. Then $\iota_\infty([\varepsilon]) \in \operatorname{Im} \lambda_\infty$. Since $\operatorname{Im} \lambda_\infty$ is generated by $\lambda_\infty(\iota_\infty(P)) = \iota_\infty(\lambda(P)) = \iota_\infty([a - \rho])$, we find that $\iota_\infty([\varepsilon]) = 1$ or $\iota_\infty([a - \rho])$. Thus ε is a totally positive unit, or else so is $\varepsilon(a - \rho)$. Note that neither $a - \rho$ nor $-(a - \rho)$

is totally positive, and the existence of such a unit implies that every totally positive unit of K is a square, for $K/\boldsymbol{Q}$ is cyclic. So either ε or $\varepsilon(a-\rho)$ is a square. This means that $[\varepsilon]=1$ or $[a-\rho]$, and hence $V'_2=\langle[a-\rho]\rangle=\langle\lambda(P)\rangle$. Therefore, combining the sequence (2), we obtain a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \langle[P]\rangle & \longrightarrow & S_2(E) & \longrightarrow & C'_2 & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle\sigma} & & \| & & \downarrow{\scriptstyle\tau} & & \\ 1 & \longrightarrow & E(\boldsymbol{Q})/2E(\boldsymbol{Q}) & \longrightarrow & S_2(E) & \longrightarrow & Ш_2(E) & \longrightarrow & 1\,, \end{array}$$

where σ is the inclusion while τ is the induced natural surjection. Finally, by the snake lemma, we have

$$\operatorname{Ker}\tau\simeq\operatorname{Coker}\sigma=(E(\boldsymbol{Q})/2E(\boldsymbol{Q}))/\langle[P]\rangle\simeq E^{\circ}(\boldsymbol{Q})/2E(\boldsymbol{Q})\,.$$

□

In [8], Washington treated the irreducible polynomials for $m\in\boldsymbol{Z}$ in the form

$$f(x)=x^3+mx^2-(m+3)x+1\,. \tag{3}$$

The discriminant of $f(x)$ is $(m^2+3m+9)^2$. So the cubic fields K defined by $f(x)$ are cyclic over $\boldsymbol{Q}$. They are called the simplest cubic fields (cf. [5], [8]). As $f(0)=1$ and $f(1)=-1<0$, the point (0, 1) in the elliptic curve E: $y^2=f(x)$ fulfills the condition of the proposition. His proof is partly carried out by concrete calculations dependent on the form of $f(x)$ itself. In fact, it can be shown that if m^2+3m+9 is square-free then the restricted map $S_2(E)\to C_2(K)$ in the above proof is surjective, hence $C'_2=C_2(K)$.

We remark that the condition "any prime number p satisfies (a) or (b) of Lemma 1" is just a sufficient condition to make the conclusion of Proposition to hold, and the proof of the theorem is done by the property for any finite prime p, $\operatorname{Im}\lambda_p\subseteq U_pK_p^{\times 2}/K_p^{\times 2}$. So, if we adopt this instead of (a) or (b), then the result of Proposition may apply for more general polynomials.

3. The simplest cubic fields. From now on, let K be one of the simplest cubic fields, that is, the cyclic cubic field defined by a polynomial $f(x)$ in the form (3). Let E be the elliptic curve defined over $\boldsymbol{Q}$ given by $y^2=f(x)$. Its conductor divides $16(m^2+3m+9)^2$. We also study the polynomial $g(x)=-f(-x)$ and the elliptic curve F: $y^2=g(x)$, on which Washington have touched ([8, p. 382]). In view of the real locus of F, we find that the point $(-1, 1)$ lies in $F(\boldsymbol{Q})-F^{\circ}(\boldsymbol{Q})$, so Proposition may be also applied to $g(x)$. In the same way as we define the homomorphism λ for $E(\boldsymbol{Q})$ using ρ the root of $f(x)$, we define

$$\lambda'\colon F(\boldsymbol{Q})\to K^{\times}/K^{\times 2}$$

by $(x', y')\mapsto[x'+\rho]$ and $O\mapsto 1$. Note that $g(-\rho)=0$. The Selmer and Shafarevich-Tate

groups $S_2(F)$ and $Ш_2(F)$ of the curve $F/\boldsymbol{Q}$ will be also treated.

Consider the following two properties:

(A1) m^2+3m+9 is square-free.

(A2) Any prime number dividing m^2+3m+9 does not split in K.

First we note that (A1) implies (A2), because if m^2+3m+9 is square-free then any prime factor of m^2+3m+9 is totally ramified for $K/\boldsymbol{Q}$. Next, if p is a prime number such that E has bad reduction at p, then p is a factor of the conductor of E, thus p divides $2(m^2+3m+9)$. Therefore, since the prime 2 is inert in K, we see that, under (A2), the condition (a) or (b) of Lemma 1 holds for any finite prime p. Further, as mentioned in the previous section, we have $C_2'=C_2(K)$ in Propositon under (A1). Indeed, one may prove this from (A2), because the surjectivity of the map $S_2(E)\to C_2(K)$ in the proof of Proposition follows from the fact that $\operatorname{Im}\lambda_p\subseteq U_pK_p^{\times 2}/K_p^{\times 2}$ for any finite prime p, which is a consequence of (A2) and Lemma 1. The above arguments of this paragraph hold for $g(x)$ and F as well, since $g(x)$ has the same discriminant as that of $f(x)$. So we have deduced the following:

THEOREM 1 (Washington). *Assume* (A1) *or* (A2). *Then there are exact sequences*

$$1\to E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q})\to C_2(K)\to Ш_2(E)\to 1\,,$$

$$1\to F^\circ(\boldsymbol{Q})/2F(\boldsymbol{Q})\to C_2(K)\to Ш_2(F)\to 1\,,$$

and we have $\operatorname{rk}_2(C_2(K))\geq\max\{\operatorname{rank}E(\boldsymbol{Q}),\operatorname{rank}F(\boldsymbol{Q})\}-1$.

Now it should be noted that F is the twist of E which becomes isomorphic to E over the quadratic field $k=\boldsymbol{Q}(i)$, where $i^2=-1$. The isomorphism $\phi: E\to F$ is given by $(x, y)\mapsto(-x, -iy)$. Let ψ be the inverse of ϕ, that is, $\psi: F\to E$, $(x', y')\mapsto(-x', iy')$:

$$E\underset{\psi}{\overset{\phi}{\rightleftarrows}}F\,.$$

For a point $P=(x, y)$ in $E(k)$ or $F(k)$, let $\bar{P}=(\bar{x}, \bar{y})$ be the complex conjugate of P. It is easy to verify the identities $\phi(\bar{P})=-\overline{\phi(P)}$, $\psi(\bar{Q})=-\overline{\psi(Q)}$. We need the norm map

$$\mathcal{N}: E(k)\to E(\boldsymbol{Q})$$

defined by $\mathcal{N}P=P+\bar{P}$ for $P\in E(k)$, and the norm group

$$\mathcal{N}E(k)=\{\mathcal{N}P\,|\,P\in E(k)\}\,.$$

For F, define also $\mathcal{N}: F(k)\to F(\boldsymbol{Q})$ and $\mathcal{N}F(k)$ similarly. Furthermore, we introduce the *diagonal* norm group, that is, the subgroup of $E(\boldsymbol{Q})\oplus F(\boldsymbol{Q})$ defined to be

$$\mathcal{N}_k(E, F)=\{(\mathcal{N}P, \mathcal{N}\phi(P))\,|\,P\in E(k)\}=\{(\mathcal{N}\psi(Q), \mathcal{N}Q)\,|\,Q\in F(k)\}\,.$$

We join the maps $E(\boldsymbol{Q})\xrightarrow{\lambda}K^\times/K^{\times 2}$ and $F(\boldsymbol{Q})\xrightarrow{\lambda'}K^\times/K^{\times 2}$ together, and define the homomorphism

$$\tilde{\lambda}\colon E(\boldsymbol{Q})\oplus F(\boldsymbol{Q})\to K^{\times}/K^{\times 2},$$

by $\tilde{\lambda}(P, Q)=\lambda(P)\lambda'(Q)$ for $P\in E(\boldsymbol{Q})$ and $Q\in F(\boldsymbol{Q})$.

LEMMA 3. *The following relations hold*:

(a) $\operatorname{Ker}\tilde{\lambda}=\mathcal{N}_k(E, F)$.

(b) $\mathcal{N}E(k)\subseteq E^{\circ}(\boldsymbol{Q})$ *and* $\mathcal{N}F(k)\subseteq F^{\circ}(\boldsymbol{Q})$.

(c) $\mathcal{N}_k(E, F)\subseteq E^{\circ}(\boldsymbol{Q})\oplus F^{\circ}(\boldsymbol{Q})$.

PROOF. Let $L=k(\rho)=K(i)$ and define $\lambda_k\colon E(k)\to L^{\times}/L^{\times 2}$ by $(x, y)\mapsto[x-\rho]$, $O\mapsto 1$ in our usual way. It is known that the kernel of λ_k is exactly $2E(k)$. Define the homomorphism $\mu\colon E(\boldsymbol{Q})\oplus F(\boldsymbol{Q})\to E(k)$ by $(P, Q)\mapsto P+\psi(Q)$. If $(P, Q)\in\operatorname{Ker}\mu$, i.e., $P+\psi(Q)=O$, then, taking the complex conjugate, we have $P-\psi(Q)=O$ thus $(P, Q)=(O, O)$. Hence μ is injective. Next, let $\nu\colon K^{\times}/K^{\times 2}\to L^{\times}/L^{\times 2}$ be the natural mapping. By the Kummer theory, $\operatorname{Ker}\nu$ is generated by $[-1]$. Note, however, that $[-1]\notin\operatorname{Ker}(\bar{N}\colon K^{\times}/K^{\times 2}\to\boldsymbol{Q}^{\times}/\boldsymbol{Q}^{\times 2})$. Thus $\operatorname{Im}\tilde{\lambda}\cap\operatorname{Ker}\nu=\{1\}$, for $\operatorname{Im}\tilde{\lambda}\subseteq\operatorname{Ker}\bar{N}$. Straightforward calculations show that the diagram

$$\begin{array}{ccc} E(k) & \xrightarrow{\lambda_k} & L^{\times}/L^{\times 2} \\ \uparrow{\scriptstyle\mu} & & \uparrow{\scriptstyle\nu} \\ E(\boldsymbol{Q})\oplus F(\boldsymbol{Q}) & \xrightarrow[\tilde{\lambda}]{} & K^{\times}/K^{\times 2} \end{array}$$

is commutative. We are now ready to prove (a), (b) and (c) as follows:

(a) Since $2P=\mathcal{N}P+\psi(\mathcal{N}\phi(P))=\mu(\mathcal{N}P, \mathcal{N}\phi(P))$ for any point $P\in E(k)$, it follows that $\mathcal{N}_k(E, F)\simeq 2E(k)$ with the injection μ. The desired result follows from the relations $\operatorname{Ker}\lambda_k=2E(k)$ and $\operatorname{Im}\tilde{\lambda}\cap\operatorname{Ker}\nu=\{1\}$.

(b) Let $P=(x, y)\in E(k)$ and put $\alpha=N_{L/K}(x-\rho)$, that is, $(x-\rho)(\bar{x}-\rho)$. Then, by the above commutative diagram, $\nu(\lambda(\mathcal{N}P))=\lambda_k(P)\lambda_k(\bar{P})=\nu([\alpha])$. As $N_{K/\boldsymbol{Q}}\alpha=N_{k/\boldsymbol{Q}}N_{L/k}(x-\rho)=N_{k/\boldsymbol{Q}}y^2\in\boldsymbol{Q}^{\times 2}$, we have $[\alpha]\in\operatorname{Ker}\bar{N}$, thus $\lambda(\mathcal{N}P)=[\alpha]$. Since α is totally positive, we see that $\mathcal{N}P\in E^{\circ}(\boldsymbol{Q})$, which gives the relation we want.

(c) is an immediate consequence of (b) and the definiton of $\mathcal{N}_k(E, F)$. □

Let $S_2(E, F)=S_2(E)S_2(F)$, which is a subgroup of $K^{\times}/K^{\times 2}$. By (a) of the above lemma, $\tilde{\lambda}$ induces an injection $(E(\boldsymbol{Q})\oplus F(\boldsymbol{Q}))/\mathcal{N}_k(E, F)\to S_2(E, F)$. Denote the cokernel of this by $Ш_2(E, F)$, and we have an exact sequence

$$1\to(E(\boldsymbol{Q})\oplus F(\boldsymbol{Q}))/\mathcal{N}_k(E, F)\to S_2(E, F)\to Ш_2(E, F)\to 1\,. \tag{4}$$

We remark that, if (A1) or (A2) holds, then the map $H_2(K)\to C_2(K)$ induces a surjective homomorphism $S_2(E, F)\to C_2(K)$. We are now ready to prove a theorem giving a more precise estimate than Theorem 1.

THEOREM 2. *Under the assumption* (A1) *or* (A2), *there is an exact sequence*

$$1 \to (E^\circ(\boldsymbol{Q}) \oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E, F) \to C_2(K) \to Ш_2(E, F) \to 1 ,$$

and we have

$$\begin{aligned} \mathrm{rk}_2(C_2(K)) &\geq \mathrm{rk}_2((E^\circ(\boldsymbol{Q}) \oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E, F)) \\ &= \mathrm{rank}\, E(\boldsymbol{Q}) + \mathrm{rk}_2(F^\circ(\boldsymbol{Q})/\mathcal{N}F(k)) - 1 \\ &= \mathrm{rank}\, F(\boldsymbol{Q}) + \mathrm{rk}_2(E^\circ(\boldsymbol{Q})/\mathcal{N}E(k)) - 1 . \end{aligned}$$

PROOF. For the exact sequence, we may use a method similar to that for Proposition. Let $P=(0, 1)$ and $Q=(-1, 1)$. Denote by X the subgroup of $(E(\boldsymbol{Q}) \oplus F(\boldsymbol{Q}))/\mathcal{N}_k(E, F)$ generated by the cosets (P, O) and $(O, Q) \bmod \mathcal{N}_k(E, F)$. Then $X \simeq \langle [-\rho], [-1+\rho] \rangle \subseteq K^\times/K^{\times 2}$. Since none of the units $-\rho$, $-1+\rho$ and their product $\rho(1-\rho)$ are totally positive, we see that X has rank two. So there exists a natural isomorphism

$$X \simeq (E(\boldsymbol{R})/2E(\boldsymbol{R})) \oplus (F(\boldsymbol{R})/2F(\boldsymbol{R})) ,$$

which gives a decomposition

$$(E(\boldsymbol{Q}) \oplus F(\boldsymbol{Q}))/\mathcal{N}_k(E, F) = ((E^\circ(\boldsymbol{Q}) \oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E, F))) \oplus X .$$

Next, the induced homomorphism $S_2(E, F) \to C_2(K)$ is surjective, as remarked above. Its kernel is isomorphic to X by the same method as in the proof of Proposition. So there is an exact sequence

$$1 \to X \to S_2(E, F) \to C_2(K) \to 1 .$$

Connect this with (4), and we obtain the desired exact sequence by the snake lemma and the above decomposition.

We now show the latter part. Consider a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & E(\boldsymbol{Q}) & \longrightarrow & E(\boldsymbol{Q}) \oplus F(\boldsymbol{Q}) & \longrightarrow & F(\boldsymbol{Q}) & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & 2E(\boldsymbol{Q}) & \longrightarrow & \mathcal{N}_k(E, F) & \longrightarrow & \mathcal{N}F(k) & \longrightarrow & 1 , \end{array}$$

where the top row is generated by the canonical injection and projection, the maps in the bottom row are their restrictions, and the vertical maps are the inclusions. Clearly the top row is exact. It is not difficult to see that the bottom row is also exact. Consequently, this diagram yields an exact sequence

$$1 \to E(\boldsymbol{Q})/2E(\boldsymbol{Q}) \to (E(\boldsymbol{Q}) \oplus F(\boldsymbol{Q}))/\mathcal{N}_k(E, F) \to F(\boldsymbol{Q})/\mathcal{N}F(k) \to 1 .$$

Similarly, we obtain an exact sequence

$$1 \to E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q}) \to (E^\circ(\boldsymbol{Q}) \oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E, F) \to F^\circ(\boldsymbol{Q})/\mathcal{N}F(k) \to 1 .$$

Therefore

$$\begin{aligned}\mathrm{rk}_2(C_2(K)) &\geq \mathrm{rk}_2((E^\circ(\boldsymbol{Q})\oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E,F))\\ &= \mathrm{rk}_2(E^\circ(\boldsymbol{Q})/2E(\boldsymbol{Q})) + \mathrm{rk}_2(F^\circ(\boldsymbol{Q})/\mathcal{N}F(k))\\ &= \mathrm{rank}\, E(\boldsymbol{Q}) - 1 + \mathrm{rk}_2(F^\circ(\boldsymbol{Q})/\mathcal{N}F(k))\,.\end{aligned}$$

By symmetry one may choose the formula for which the rôles of E and F are changed. □

COROLLARY. *Under the assumption* (A1) *or* (A2), *we have*

$$\mathrm{rk}_2(C_2(K)) \geq \frac{1}{2}\{\mathrm{rank}\, E(k) + \mathrm{rk}_2(E^\circ(\boldsymbol{Q})/\mathcal{N}E(k)) + \mathrm{rk}_2(F^\circ(\boldsymbol{Q})/\mathcal{N}F(k))\} - 1\,.$$

PROOF. Use the formula $\mathrm{rank}\, E(k) = \mathrm{rank}\, E(\boldsymbol{Q}) + \mathrm{rank}\, F(\boldsymbol{Q})$. (cf. [3].) □

Finally, we remark that, from the proof of Lemma 3, there are isomorphisms

$$(E^\circ(\boldsymbol{Q}) + \psi(F^\circ(\boldsymbol{Q})))/2E(k) \simeq (E^\circ(\boldsymbol{Q})\oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E,F) \simeq (\phi(E^\circ(\boldsymbol{Q})) + F^\circ(\boldsymbol{Q}))/2F(k)\,.$$

The groups on the left and right hand sides are subgroups of $E(k)/2E(k)$ and $F(k)/2F(k)$, respectively. Then, using the 2-descent on $E(k)$ or $F(k)$, we may be able to compute the group $(E^\circ(\boldsymbol{Q})\oplus F^\circ(\boldsymbol{Q}))/\mathcal{N}_k(E,F)$.

REFERENCES

[1] A. BRUMER AND K. KRAMER, The rank of elliptic curves, Duke Math. J. 44 (1977), 715–743.

[2] H. COHN, A device for generating fields of even class number, Proc. Amer. Math. Soc. 7 (1956), 595–598.

[3] K. KRAMER, Arithmetic of elliptic curves upon quadratic extension, Trans. Amer. Math. Soc. 264 (1981), 121–135.

[4] S. NAKANO, Ideal class groups of cubic cyclic fields, Acta Arith. 46 (1986), 297–300.

[5] D. SHANKS, The simplest cubic fields, Math. Comp. 28 (1974), 1137–1152.

[6] J. H. SILVERMAN, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, Berlin, Heidelberg, Tokyo, 1986.

[7] K. UCHIDA, Class numbers of cubic cyclic fields, J. Math. Soc. Japan 26 (1974), 447–453.

[8] L. C. WASHINGTON, Class numbers of the simplest cubic fields, Math. Comp. 48 (1987), 371–384.

DEPARTMENT OF MATHEMATICS
FACULTY OF SCIENCE
TOKYO METROPOLITAN UNIVERSITY
HACHIOJI 192-03
JAPAN

DEPARTMENT OF MATHEMATICS
COLLEGE OF GENERAL EDUCATION
NAGOYA UNIVERSITY
NAGOYA 464-01
JAPAN