On the 3-rank of the ideal class groups of certain pure cubic fields II

By Shinju KOBAYASHI

(Communicated by Y. Kawada)

Introduction

In a previous paper [4], we determined the 3-rank of the ideal class groups of certain pure cubic fields $\boldsymbol{Q}(\sqrt[3]{m})$, namely those for which m does not contain prime factors of the type $p\equiv+1 \pmod 3$. In [5], we generalized the method and proved that, for any m, the rank is equal to the multiplicity of 1 as an eigenvalue of a certain matrix over $\boldsymbol{F}_3$. But we did not show how to get the matrix in the general case. The purpose of the present article is to give an algorithm for this. It involves only the calculation of the Hilbert's norm residue symbols in $\boldsymbol{Q}(\sqrt{-3})$, and as the reader will see, it can actually be carried out if m contains a prime factor $p\neq 3$ with $p\not\equiv\pm1 \pmod 9$ (of course, this condition guarantees the existence of an ambiguous ideal in every ambiguous class in the extension $\boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{m})/\boldsymbol{Q}(\sqrt{-3})$). In [1], F. Gerth III has already given an algorithm for the determination of the 3-rank. But the two methods are different and the author hopes that there is still some interest in publishing another version.

In § 1, we give a brief but precise formulation of the method used in [5], and the determination of the matrix in question will be done in § 2 (Theorem). Finally in § 3, we show as an example that the 3-rank is equal to 6 for $m=37\cdot 433\cdot 2293\cdot 3307$.

The following notations will be used throughout the paper.

$\boldsymbol{F}_3$: the finite field with 3 elements.

I_k: the group of fractional ideals in a finite algebraic number field k.

C_k: the ideal class group of k.

$d^{(3)}C_k$: the 3-rank of C_k, i.e. $\dim_{F_3}(C_k/C_k^3)$.

$\mathfrak{f}(K/k)$: the conductor of an abelian extension K/k.

$\mathfrak{f}^{(\mathfrak{p})}$: the $\mathfrak{p}$-component of a conductor $\mathfrak{f}$.

§ 1. Reduction step

Let m be a cubic free rational integer and put $\Omega=\boldsymbol{Q}(\sqrt[3]{m})$, $k=\boldsymbol{Q}(\sqrt{-3})$, $K=$

$k(\sqrt[3]{m})$. Let also $\tilde{\Omega}$ (resp. $\tilde{K}$) be the unramified class field over Ω (resp. K) corresponding to the ideal group C_{Ω}^{3} (resp. C_{K}^{3}). By class field theory, $d^{(3)}C_{\Omega}$ is equal to the rank of $G(\tilde{\Omega}/\Omega)$. Denote by σ and τ the generators of $G(K/k)$ and $G(K/\Omega)$ respectively. Then τ operates through the inner automorphism $\rho\mapsto\tau\rho\tau^{-1}$ on $G(\tilde{K}/K)$ which is a vector space over F_3, and we have shown in [5] § 1, that the rank of $G(\tilde{\Omega}/\Omega)$ is equal to the multiplicity of 1 appearing as an eigenvalue of this representation of τ. But if we denote by K_1 the unramified class field over K corresponding to $C_{K}^{1-\sigma}$, then $K_1\subset\tilde{K}$ and $G(\tilde{K}/K_1)$ is a τ-invariant subspace of $G(\tilde{K}/K)$. Hence the multiplicity in question is equal to the sum of those of τ on each of the two spaces $G(\tilde{K}/K)/G(\tilde{K}/K_1)=G(K_1/K)$ and $G(\tilde{K}/K_1)$.

The same argument in [5] § 1 shows that the multiplicity of 1 on $G(K_1/K)$ is equal to the rank of the extension $\tilde{\Omega}K\cap K_1/K$. We saw in [3] § 3 that *this is equal to the number of prime factors p of m such that* $p\equiv+1$ (mod 3).

To deal with the representation of τ on $G(\tilde{K}/K_1)$, we recall the following two facts (cf. [5] §§ 2, 3). Note that they are valid for any Kummer extension of degree 3 over k.

(i) $G(\tilde{K}/K_1)$ is the commutator subgroup of $G(\tilde{K}/k)$ and is contained in its center. So the commutator function $[x, y]$ on $G(\tilde{K}/k)$ is bilinear and depends only on the cosets of x and y in $G(\tilde{K}/k)/G(\tilde{K}/K_1)=G(K_1/k)$.

(ii) For each prime $\mathfrak{p}$ in k with $\mathfrak{p}|\mathfrak{f}$, $\mathfrak{f}=\mathfrak{f}(K/k)$, let $\sigma_{\mathfrak{p}}$ be a generator of the inertia group of $\mathfrak{p}$ in $G(K_1/k)$ and denote by the same symbol any extension of $\sigma_{\mathfrak{p}}$ to $\tilde{K}$. Then $G(\tilde{K}/k)$ is generated by $\{\sigma_{\mathfrak{p}}\}_{\mathfrak{p}|\mathfrak{f}}$ and $G(\tilde{K}/K_1)$ by $\{[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}]\}_{\mathfrak{p},\mathfrak{q}|\mathfrak{f}}$.

Now (i) means that we can know the action of τ on $[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}]$ if we know $\tau\sigma_{\mathfrak{p}}\tau^{-1}$ in $G(K_1/k)$. But in $G(K_1/k)$, $\tau\sigma_{\mathfrak{p}}\tau^{-1}$ is contained in the inertia group of $\tau\mathfrak{p}$ in $G(K_1/k)$ and hence it coincides either with $\sigma_{\tau\mathfrak{p}}$ or $\sigma_{\tau\mathfrak{p}}^{-1}$. As we will see, we can normalize $\sigma_{\mathfrak{p}}$ so that we always have $\tau\sigma_{\mathfrak{p}}\tau^{-1}=\sigma_{\tau\mathfrak{p}}^{-1}$. The calculation of $d^{(3)}C_{\Omega}$, therefore, will be completed if we can find the linear relations among $[\sigma_{\mathfrak{p}}, \sigma_{\mathfrak{q}}]$. This will be done in the next section (see Theorem).

§ 2 Determination of a basis of $G(\tilde{K}/K_1)$

The goal is to find a basis of $G(\tilde{K}/K_1)$ in the notation of § 1. Our method does not depend on the fact that K/k is generated by a rational number. So we assume that K is any Kummer extension of degree 3 over k and put $K=k(\sqrt[3]{\alpha})$, $\alpha\in k^{\times}$.

Let $\mathfrak{f}=\mathfrak{f}(K/k)$ and $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ be the prime factors of $\mathfrak{f}$. Let, for each $\mathfrak{p}_i$, $\sigma_{\mathfrak{p}_i}$ be the element in $G(\tilde{K}/k)$ as described in § 1, and denote them by σ_i for brevity. Let ζ be a primitive cube root of 1 which we fix once and for all through this section. Each σ_i is non-trivial on K. So, replacing σ_i by σ_i^{-1} if necessary, we assume that they act on K by

$$\sigma_i(\sqrt[3]{\alpha})=\zeta\sqrt[3]{\alpha}, \qquad i=1,\dots,t.$$

Then obviously

$$(*) \qquad \prod_{i=1}^{t}\sigma_i^{a_i}\in G(\tilde{K}/K)\Longleftrightarrow\sum_{i=1}^{t}a_i\equiv 0 \pmod{3},$$

and hence, as we have seen in [4] p. 214, $[\sigma_i,\sigma_j]=[\sigma_i,\sigma_h][\sigma_h,\sigma_j]$ for any i, j, h. In particular $G(\tilde{K}/K)$ is generated by $\{[\sigma_1,\sigma_i]\}^t_{i=2}$. We want to find the linear relations among them. There are two steps.

a) By (i) of § 1,

$$\prod_{i=2}^{t}[\sigma_1,\sigma_i]^{a_i}=[\sigma_1,\prod_{i=2}^{t}\sigma_i^{a_i}]=[\sigma_1,\sigma_1^{-a_1}\prod_{i=2}^{t}\sigma_i^{a_i}],$$

where we put $a_1=\sum_{i=2}^{t}a_i$. Then, by (*), the second element in the last commutator belongs to $G(\tilde{K}/K)$, so that it is equal to the Artin symbol $((\tilde{K}/K)/c)$ for an element $c\in C_K$, hence the last commutator in the above equality is equal to $((\tilde{K}/K)/c^{1-\sigma_1})$. But $\sigma_1|K$ is a generator of $G(K/k)$, hence $\tilde{K}$ corresponds to the ideal group $C_K{}^3=C_K{}^{(1-\sigma_1)^2}$ (cf. [3] § 2, Proposition 1) and therefore we see that

$$\prod_{i=2}^{t}[\sigma_1,\sigma_i]^{a_i}=1\Longleftrightarrow c\in C_K{}^{1-\sigma_1}C_K{}^G,$$

where $C_K{}^G$ is the subgroup of C_K of $G=G(K/k)$-invariant elements.

Next let D_K be the subgroup of C_K generated by G-invariant ideals in K. D_K is generated by the prime factors $\mathfrak{P}_i$ of $\mathfrak{p}_i$ in K, and $(C_K{}^G:D_K)=1$ or 3 (cf. [2] Ia, Satz 13). If $C_K{}^G\neq D_K$, take any ideal $\mathfrak{P}_{t+1}$ (not necessarily prime) from a class in $C_K{}^G$ not contained in D_K, and put $\mathfrak{p}_{t+1}=N_{K/k}(\mathfrak{P}_{t+1})$. Then $C_K{}^G$ is generated by these $\mathfrak{P}_j$'s. If now we take any ideal $\mathfrak{A}$ in c, we see,

$$\begin{aligned} c\in C_K{}^{1-\sigma_1}C_K{}^G &\Longleftrightarrow \mathfrak{A}=\mathfrak{B}^{1-\sigma_1}\prod_j\mathfrak{P}_j{}^{x_j}(\gamma),\ {}^\exists\mathfrak{B}\in I_K,\ {}^\exists\gamma\in K^\times,\ {}^\exists(x_j)\\ &\Longleftrightarrow N_{K/k}(\mathfrak{A})=\prod_j\mathfrak{p}_j{}^{x_j}(N_{K/k}(\gamma)),\ {}^\exists\gamma\in K^\times,\ {}^\exists(x_j)\\ &\Longleftrightarrow \zeta^w\prod_j\pi_j{}^{x_j}N_{K/k}(\gamma)=\beta,\ {}^\exists\gamma\in K^\times,\ {}^\exists(w,x_j), \end{aligned}$$

where we denoted by β and π_j arbitrarily chosen elements in k generating the ideals $N_{K/k}(\mathfrak{A})$ and $\mathfrak{p}_j$ respectively. Using the Hasse norm Theorem, we have thus shown that

$$\prod_{i=2}^{t}[\sigma_1, \sigma_i]^{a_i}=1$$

if and only if the following system of equations for all primes $\mathfrak{p}$ *in* k *has a solution in* (w, x_j):

$$\left(\frac{\zeta, \alpha}{\mathfrak{p}}\right)^{w} \prod_{j}\left(\frac{\pi_j, \alpha}{\mathfrak{p}}\right)^{x_j}=\left(\frac{\beta, \alpha}{\mathfrak{p}}\right).$$

We note that $((\zeta, \alpha)/\mathfrak{p})=((\pi_j, \alpha)/\mathfrak{p})=1$ for $^{\forall}\mathfrak{p}\nmid\mathfrak{f}$, since ζ is a unit and (π_j) is a norm from K.

b) What remains is to know the value of $((\beta, \alpha)/\mathfrak{p})$ for a given set of integers $(a_2, \ldots, a_t)$. First we look for an ideal $\mathfrak{A}$ in K such that

$$\sigma_1^{-a_1}\prod_{i=2}^{t}\sigma_i^{a_i}=\left(\frac{\tilde{K}/K}{\mathfrak{A}}\right), \qquad a_1=\prod_{i=2}^{t}a_i.$$

But by (i) of § 1, it is sufficient to find an ideal $\mathfrak{A}$ with

$$\sigma_1^{-a_1}\prod_{i=2}^{t}\sigma_i^{a_i}=\left(\frac{K_1/K}{\mathfrak{A}}\right)=\left(\frac{K_1/k}{N_{K/k}(\mathfrak{A})}\right) \text{ on } K_1.$$

This is achieved by means of the norm residue symbol (for the definition and properties of it, see [2] II, §§ 6–12). Namely, for each $\mathfrak{p}_i$, $((\beta, K_1/k)/\mathfrak{p}_i)$ with $\beta\not\equiv 0$ (mod $\mathfrak{p}_i$) covers the inertia group of $\mathfrak{p}_i$ in $G(K_1/k)$. So, for each i, let β_i be an element in k satisfying the following three conditions:

$$\beta_i\not\equiv 0 \ (\text{mod } \mathfrak{p}_i), \ \ \beta_i\equiv 1 \ (\text{mod } \mathfrak{f}_1/\mathfrak{f}_1^{(\mathfrak{p}_i)}), \ \ \left(\frac{\beta_i, \alpha}{\mathfrak{p}_i}\right)=\zeta,$$

where we put $\mathfrak{f}_1=\mathfrak{f}(K_1/k)$. Then the element $((\beta_i, K_1/k)/\mathfrak{p}_i)=((K_1/k)/(\beta_i))$ sends $\sqrt[3]{\alpha}$ to $\zeta\sqrt[3]{\alpha}$ and hence coincides on K_1 with the σ_i chosen at the beginning of this section (since $G(K_1/k)$ is of type $(3, .., 3)$, the relation $\sigma_i(\sqrt[3]{\alpha})=\zeta\sqrt[3]{\alpha}$ determines σ_i uniquely on K_1). This gives

$$\sigma_1^{-a_1}\prod_{i=2}^{t}\sigma_i^{a_i}=\left(\frac{K_1/k}{(\beta_1^{-a_1}\prod_{i=2}^{t}\beta_i^{a_i})}\right) \text{ on } K_1.$$

Finally take a prime element π in k satisfying

$$\pi\equiv\beta_1^{-a_1}\prod_{i=2}^{t}\beta_i^{a_i} \ (\text{mod } \mathfrak{f}_1).$$

Such an element does exist by the Theorem of arithmetic progression. Then (π)

splits in K/k and $(\pi)=N_{K/k}(\mathfrak{P})$ for a prime ideal $\mathfrak{P}$ in K. We can take $\mathfrak{P}$ and π as $\mathfrak{A}$ and β in a) and we get

$$\left(\frac{\beta,\alpha}{\mathfrak{p}}\right)=\begin{cases}\zeta^{-a_1} & \mathfrak{p}=\mathfrak{p}_1\\ \zeta^{a_i} & \mathfrak{p}=\mathfrak{p}_i, \quad i=2,\dots,t\,.\\ 1 & \mathfrak{p}\nmid\mathfrak{f}\end{cases}$$

In fact, by the same reason as we indicated at the end of a), $((\pi,\alpha)/\mathfrak{p})=1$ for $\mathfrak{p}\nmid\mathfrak{f}$.

Putting a) and b) together, we get the following result.

THEOREM. *Let $k=Q(\sqrt{-3})$, $K=k(\sqrt[3]{\alpha})$, $\alpha\in k^{\times}$, σ be a generator of $G(K/k)$, and $\tilde{K}$ and K_1 be the unramified class fields over K corresponding to the ideal groups $C_K{}^3$ and $C_K{}^{1-\sigma}$ respectively. Let $\mathfrak{p}_1,\dots,\mathfrak{p}_t$ be the prime factors of $\mathfrak{f}=\mathfrak{f}(K/k)$ and ζ be a fixed primitive cube root of* 1. *For each $\mathfrak{p}_i$, let β_i be an element of k such that*

$$\beta_i\not\equiv 0 \ (\mathrm{mod}\ \mathfrak{p}_i),\quad \beta_i\equiv 1\ (\mathrm{mod}\ \mathfrak{f}_1/\mathfrak{f}_1{}^{(\mathfrak{p}_i)}),\quad \left(\frac{\beta_i,\alpha}{\mathfrak{p}_i}\right)=\zeta,$$

where we put $\mathfrak{f}_1=\mathfrak{f}(K_1/k)$, and σ_i be any extension of $((\beta_i, K_1/k)/\mathfrak{p}_i)$ to $\tilde{K}$. Then $G(\tilde{K}/K_1)$ is generated by $\{[\sigma_1,\sigma_i]\}^t{}_{i=2}$. For any set of integers $(a_2,\dots,a_t)$, they satisfy the linear relation

$$\prod_{i=2}^{t}[\sigma_1,\sigma_i]^{a_i}=1$$

if and only if the following system of equations for $\mathfrak{p}|\mathfrak{f}$ has a solution in (w,x_j):

$$\left(\frac{\zeta,\alpha}{\mathfrak{p}}\right)^{w}\prod_{j}\left(\frac{\pi_j,\alpha}{\mathfrak{p}}\right)^{x_j}=\begin{cases}\zeta^{-a_1} & \mathfrak{p}=\mathfrak{p}_1,\quad a_1=\sum\limits_{i=2}^{t}a_i\\ \zeta^{a_i} & \mathfrak{p}=\mathfrak{p}_i,\quad i=2,\dots,t.\end{cases}$$

Here the index j runs through $1,\dots,t$ or $1,\dots,t+1$ according to whether or not every ambiguous class in C_K contains an ambiguous ideal. In both cases, π_j, for $j=1,\dots,t$, is an arbitrarily chosen element of k generating $\mathfrak{p}_j$. In the latter case, find any ideal $\mathfrak{B}$ in K contained in an ambiguous class but not equivalent to any ambiguous ideal, and then we take as π_{t+1} an arbitrarily chosen element of k generating $N_{K/k}(\mathfrak{B})$.

REMARK 1. By virtue of the product-formula for the norm residue symbol, we can drop one of the equations, e.g. the one for $\mathfrak{p}=(\sqrt{-3})$ if it is ramified.

REMARK 2. When $\alpha=m$, every ambiguous class contains an ambiguous ideal if m has a prime factor $p\neq 3$ with $p\not\equiv\pm 1$ (mod 9). cf. [2] Ia, Satz 13.

In order to carry out the procedure described in § 1, we need one more fact which is easily verified from the definition of the σ_i's.

LEMMA. *Under the assumptions of Theorem, let $\alpha=m\in Z$ and τ be as in* §1. *Then writing $\sigma_{\mathfrak{p}_i}$ for σ_i, we have*

$$\tau\sigma_{\mathfrak{p}_i}\tau^{-1}=\sigma_{\tau\mathfrak{p}_i}{}^{-1} \quad \textit{on } K_1.$$

§3. Example

Let $m=37\cdot433\cdot2293\cdot3307$. All the prime factors of m satisfy $p\equiv+1 \pmod 3$ and the multiplicity of the eigenvalue 1 of τ on $G(K_1/K)$ is equal to 4.

Next put

$$\zeta=\frac{-1+\sqrt{-3}}{2},\ \pi_{37}=\frac{11+3\sqrt{-3}}{2},\ \pi_{433}=\frac{37+11\sqrt{-3}}{2},\ \pi_{2293}=\frac{95+7\sqrt{-3}}{2},$$
$$\pi_{3307}=\frac{115+\sqrt{-3}}{2},$$

$\mathfrak{p}_{37}=(\pi_{37})$ etc.,

and denote their complex conjugates by $\bar{\pi}$ and $\bar{\mathfrak{p}}$. In the table below, the $(\mathfrak{p},\pi)$-component shows the exponent x of ζ in $((\pi, m)/\mathfrak{p})=\zeta^x$. Since our equations are non-homogeneous, we have to find these values "canonically", e.g. by means of the formulas:

$$\left(\frac{\beta,\alpha}{\mathfrak{p}}\right)=\left(\frac{\alpha}{\mathfrak{p}}\right)^{-b} \quad \text{if } \mathfrak{p}\nmid\mathfrak{f}(k(\sqrt[3]{\alpha})/k),\ \mathfrak{p}^b\|\beta,$$
$$\left(\frac{\alpha}{\mathfrak{p}}\right)\equiv\alpha^{(N\mathfrak{p}-1)/3} \quad (\mathrm{mod}\ \mathfrak{p}) \text{ if } \mathfrak{p}\nmid\alpha.$$

	ζ	π_{37}	π_{433}	π_{2293}	π_{3307}	$\bar{\pi}_{37}$	$\bar{\pi}_{433}$	$\bar{\pi}_{2293}$	$\bar{\pi}_{3307}$
$\mathfrak{p}_{37}$	0	0	0	0	0	0	0	0	0
$\bar{\mathfrak{p}}_{37}$	0	0	0	0	0	0	0	0	0
$\mathfrak{p}_{433}$	0	0	0	0	0	0	0	0	0
$\bar{\mathfrak{p}}_{433}$	0	0	0	0	0	0	0	0	0
$\mathfrak{p}_{2293}$	-1	0	-1	-1	0	0	1	1	0
$\bar{\mathfrak{p}}_{2293}$	-1	0	-1	-1	0	0	1	1	0
$\mathfrak{p}_{3307}$	1	0	1	0	1	0	-1	1	1
$\bar{\mathfrak{p}}_{3307}$	1	0	1	-1	-1	0	-1	0	-1

If we write σ_{37} for $\mathfrak{p}_{37}$ and $\sigma_{\overline{37}}$ for $\bar{\mathfrak{p}}_{37}$ etc., and take σ_{37} for σ_1, we get the system of equations in Theorem in the following form:

$$\begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \boldsymbol{a} \\ \boldsymbol{a} \\ \boldsymbol{b} \\ \boldsymbol{a-b} \end{pmatrix} \begin{pmatrix} w \\ x_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ x_8 \end{pmatrix} = \begin{pmatrix} -(a+\cdots+g) \\ a \\ b \\ c \\ d \\ e \\ f \\ g \end{pmatrix}$$

Hence the linear relations sought are

$$[\sigma_{37}, \sigma_{2293}]^d [\sigma_{37}, \sigma_{\overline{2293}}]^d [\sigma_{37}, \sigma_{3307}]^f [\sigma_{37}, \sigma_{\overline{3307}}]^{d-f} = 1,$$

and we can take as a basis of $G(\tilde{K}/K_1)$ the following five elements:

$$[\sigma_{37}, \sigma_{\overline{37}}], [\sigma_{37}, \sigma_{433}], [\sigma_{37}, \sigma_{\overline{433}}], [\sigma_{37}, \sigma_{2293}], [\sigma_{37}, \sigma_{\overline{2293}}].$$

The representation of τ on $G(\tilde{K}/K_1)$ w.r.t. this basis is

$$\begin{pmatrix} -1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and the multiplicity of the eigenvalue 1 of this matrix is 2. Thus we get $d^{(3)}C_\Omega = 6$.

References

[1] Gerth, F. III., Ranks of Sylow 3-subgroups of ideal class groups of certain cubic fields, Bull. Amer. Math. Soc. **79** (1973), 521-525.
See, for details, On 3-class groups of pure cubic fields, to appear in J. Number Theory.

[2] Hasse, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, I, Jber. der Deutsch. Math.-Verein. **36** (1927), 231-311, II, ibid. **39** (1930), 1-204.

[3] Kobayashi, S., On the l-dimension of the ideal class groups of Kummer extensions of a certain type, J. Fac. Sci. Univ. Tokyo Sec. IA **18** (1971), 399-404.

[4] Kobayashi, S., On the 3-rank of the ideal class groups of certain pure cubic fields, ibid. **20** (1973), 209-216.

[5] Kobayashi, S., On the l-class rank in some algebraic number fields, to appear in J. Math. Soc. Japan, Vol. 26.

(Received November 13, 1973)

Department of Mathematics
Faculty of Science
Tokyo Metropolitan University
Fukazawa, Setagaya-ku
158 Japan