J. Math. Soc. Japan
Vol. 29, No. 2, 1977

Complete determination of the 3-class rank in pure cubic fields*)

By Shinju KOBAYASHI

(Received Oct. 29, 1975)

Introduction.

In a preceding paper [2], we gave an algorithm to compute the 3-rank of the ideal class groups of pure cubic fields $\boldsymbol{Q}(\sqrt[3]{m})$. It consists of finding the coefficients of a certain linear representation by way of a table of Hilbert norm residue symbols in $\boldsymbol{Q}(\sqrt{-3})$. It works for most of the values of m, but fails when all the prime factors of m except 3 are $\equiv\pm1 \pmod 9$. Namely, for this type of m, there may be ambiguous classes containing no ambiguous ideal in the extension $\boldsymbol{Q}(\sqrt{-3}, \sqrt[3]{m})/\boldsymbol{Q}(\sqrt{-3})$, and if so, the table must include an extra column corresponding to such a class. But it is far from easy to find such a class and we are left with an incomplete table.

Now the purpose of this paper is to show that for the type of m described above we can always obtain the correct value of the 3-rank by applying the algorithm to this incomplete table (cf. § 5, Theorem 4). As an example, we shall show in the last section that the 3-rank is 2 for $m=3\cdot17\cdot271$.

Notation used throughout the paper:

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

C_k: the ideal class group of an algebraic number field k.

$d^{(3)}C_k=\dim_{\boldsymbol{F}_3}(C_k/C_k^3)$, i.e. the 3-rank of C_k.

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

ζ: a fixed primitive cube root of 1.

§ 1. Summary of the algorithm.

For a detailed account of the algorithm, we refer the reader to [2], § 1, and we use the same notation as there. So, for a cube free m, $\Omega=\boldsymbol{Q}(\sqrt[3]{m})$, $k=\boldsymbol{Q}(\sqrt{-3})$ and $K=k(\sqrt[3]{m})$. σ and τ are generators of $G(K/k)$ and $G(K/\Omega)$ respectively. $\tilde{K}$ and K_1 are the unramified class fields over K corresponding to the ideal groups C_K^3 and $C_K^{1-\sigma}$ respectively. Then $d^{(3)}C_\Omega$ is equal to the sum

*) This work is part of the author's thesis at the University of Tokyo.

of the number of rational prime factors p of m such that $p\equiv 1 \pmod 3$ and the multiplicity of the eigenvalue 1 of the action of τ defined by $\rho\mapsto\tau\rho\tau^{-1}$ on $G(\tilde{K}/K_1)$ (considered as a vector space over $\boldsymbol{F}_3$).

Let C_K^G be the subgroup of C_K of $G(K/k)$-invariant elements and D_K be the subgroup of C_K generated by $G(K/k)$-invariant ideals in K. We note that $(C_K^G : D_K)=1$ or 3. Renumbering the prime factors of $\mathfrak{f}(K/k)$ in k as $\mathfrak{p}_0, \cdots, \mathfrak{p}_t$, the result of [2] is as follows.

THEOREM 1. *We can choose for each* $\mathfrak{p}_i$, $i=0, \cdots, t$, *an element* $\sigma_i=\sigma_{\mathfrak{p}_i}\in G(\tilde{K}/k)$ *so that* 1), 2) *and* 3) *below hold.*

1) *For any* $i, j, h\in\{0, \cdots, t\}$, *we have*

$$[\sigma_i, \sigma_j]=[\sigma_i, \sigma_h][\sigma_h, \sigma_j].$$

2) *For any* $i\in\{0, \cdots, t\}$, *we have*

$$\tau\sigma_{\mathfrak{p}_i}\tau^{-1}\equiv\sigma_{\tau\mathfrak{p}_i}^{-1} \qquad \textit{modulo } G(\tilde{K}/K_1).$$

3) $G(\tilde{K}/K_1)$ *is the commutator subgroup of* $G(\tilde{K}/k)$ *and is generated by the elements* $[\sigma_0, \sigma_i]$, $i=1, \cdots, t$. *For any set of integers* $(b_1, \cdots, b_t)$, *they satisfy the linear relation*

$$\prod_{i=1}^{t}[\sigma_0, \sigma_i]^{b_i}=1$$

if and only if the following system of equations has a solution in (w, x_j):

$$\left(\frac{\zeta, m}{\mathfrak{p}_i}\right)^w\prod_j\left(\frac{\pi_j, m}{\mathfrak{p}_i}\right)^{x_j}=\zeta^{b_i}, \qquad i=1, \cdots, t.$$

Here the index j runs through $0, \cdots, t$ or $0, \cdots, t+1$ according to whether $C_K^G=D_K$ or not. In both cases, π_j for $j=0, \cdots, t$, is an arbitrarily chosen element of k generating $\mathfrak{p}_j$. If $C_K^G\neq D_K$, take any ideal $\mathfrak{A}$ in K contained in C_K^G but not in D_K and take as π_{t+1} an arbitrarily chosen element of k generating $N_{K/k}(\mathfrak{A})$. (We removed the first equation in [2], Theorem by virtue of the product formula for norm residue symbols.)

Since the commutator $[x, y]$ in $G(\tilde{K}/k)$ is bilinear and depends only on the cosets of x and y modulo $G(\tilde{K}/K_1)$, 1), 2) and 3) above are sufficient for knowing the action of τ on $G(\tilde{K}/K_1)$. In subsequent sections we shall concentrate ourselves upon this action.

§ 2. Preliminary results.

First we change Theorem 1, 3) into a form more convenient for application. Express the system of equations in 3) in the following additive form for the exponents of ζ:

$$A\boldsymbol{x}=\boldsymbol{b}\,,$$

where

$$A=\begin{pmatrix}\boldsymbol{a}_1\\ \vdots\\ \boldsymbol{a}_t\end{pmatrix},\qquad \boldsymbol{x}=\begin{pmatrix}w\\ x_0\\ \vdots\end{pmatrix},\qquad \boldsymbol{b}=\begin{pmatrix}b_1\\ \vdots\\ b_t\end{pmatrix},$$

and $\boldsymbol{a}_i$ are row vectors having the exponents of ζ in $\left(\frac{\zeta, m}{\mathfrak{p}_i}\right)$ and $\left(\frac{\pi_j, m}{\mathfrak{p}_i}\right)$ as their components. Everything is considered in $\boldsymbol{F}_3$. To distinguish from the matrix representing τ, we call A the "table".

THEOREM 2. *Suppose that among the row vectors of A, $\boldsymbol{a}_1, \cdots, \boldsymbol{a}_r$ are linearly independent and that*

$$\boldsymbol{a}_i=\sum_{j=1}^{r} c_{ij}\boldsymbol{a}_j\,,\qquad i=r+1, \cdots, t\,.$$

Then in $G(\tilde{K}/K_1)$, the elements $[\sigma_0, \sigma_{r+1}], \cdots, [\sigma_0, \sigma_t]$ are linearly independent and

$$[\sigma_0, \sigma_j]=\prod_{i=r+1}^{t}[\sigma_0, \sigma_i]^{-c_{ij}}\,,\qquad j=1, \cdots, r\,.$$

PROOF. By the theory of linear equations, $A\boldsymbol{x}=\boldsymbol{b}$ has a solution if and only if we have

$$b_i=\sum_{j=1}^{r} c_{ij}b_j\,,\qquad i=r+1, \cdots, t\,.$$

Hence by Theorem 1, 3), the set of relations for the $[\sigma_0, \sigma_i]$'s are given by

$$\prod_{j=1}^{r}[\sigma_0, \sigma_j]^{b_j}\prod_{i=r+1}^{t}[\sigma_0, \sigma_i]^{\sum_{j=1}^{r} c_{ij}b_j}=1\,,\qquad (b_1, \cdots, b_r)\in \boldsymbol{F}_3^r\,.$$

It now suffices to put $(b_1, \cdots, b_r)=(0, \cdots, 0)$ or $(0, \cdots, 1, \cdots, 0)$. q. e. d.

Next we show that the row vectors of A are subject to some natural restrictions. For this, let $\{p_1, \cdots, p_s, q_1, \cdots, q_t\}$ be the set of rational primes totally ramified in Ω, where $p_i\equiv 1 \pmod 3$ and $q_i\equiv -1 \pmod 3$. In the following we shall always use the letters p and q in this sense. Put $p_i=\pi_i\bar{\pi}_i$ in k. If 3 is totally ramified, we count it among the q's and put $q=\sqrt{-3}$. Then $\{(\pi_i), (\bar{\pi}_i), (q_j) \mid i=1, \cdots, s,\ j=1, \cdots, t\}$ is exactly the set of prime factors of $\mathfrak{f}(K/k)$ in k. With these conventions, we take as π_j in Theorem 1, 3), the elements

$$\pi_1, \cdots, \pi_s, \bar{\pi}_1, \cdots, \bar{\pi}_s, q_1, \cdots, q_t, \pi_{t+1}\,,$$

and arrange them always in this order. Here π_{t+1} is the element also denoted by π_{t+1} in Theorem 1, 3), and we suppose that it is a rational number. Such a choice is always possible (cf. [**1**], p. 212, (b). The argument for this fact is independent of the assumption of [**1**] that there are only q's). We use

boldface letters $\boldsymbol{p}_i$, $\bar{\boldsymbol{p}}_i$ and $\boldsymbol{q}_i$ to denote the row vectors corresponding to $\mathfrak{p}=(\pi_i)$, $(\bar{\pi}_i)$ and (q_i).

LEMMA 1. *Divide the row vectors into subvectors as follows:*

$$(e, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, d),$$

where e, $\boldsymbol{a}$, $\boldsymbol{b}$, $\boldsymbol{c}$ *and* d *are row vectors having as their components the exponents of* ζ *in* $\left(\frac{\zeta, m}{\mathfrak{p}}\right)$, $\left(\frac{\pi_i, m}{\mathfrak{p}}\right)$'s, $\left(\frac{\bar{\pi}_i, m}{\mathfrak{p}}\right)$'s, $\left(\frac{q_i, m}{\mathfrak{p}}\right)$'s *and* $\left(\frac{\pi_{t+1}, m}{\mathfrak{p}}\right)$ *respectively (of course, we do not have the last one if* $C_K^G=D_K$*). Then*

1) *Each* $\boldsymbol{q}$ *has the form* $(e, \boldsymbol{a}, -\boldsymbol{a}, \boldsymbol{0}, 0)$.

2) *If* $\boldsymbol{p}=(e, \boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c}, d)$, *we have* $\bar{\boldsymbol{p}}=(e, -\boldsymbol{b}, -\boldsymbol{a}, -\boldsymbol{c}, -d)$.

PROOF. If $\left(\frac{\alpha, m}{\mathfrak{p}}\right)=\zeta^x$ for a prime $\mathfrak{p}$ in k and $\alpha\in k^\times$, we have by complex conjugation $\left(\frac{\bar{\alpha}, m}{\bar{\mathfrak{p}}}\right)=\zeta^{-x}$. q. e. d.

LEMMA 2. *If the row vectors* $\boldsymbol{p}_i$, $\bar{\boldsymbol{p}}_i$ *and* $\boldsymbol{q}_i$ *satisfy a relation*

$$\sum_i u_i\boldsymbol{p}_i+\sum_i v_i\bar{\boldsymbol{p}}_i+\sum_i w_i\boldsymbol{q}_i=\boldsymbol{0},$$

they also satisfy the "conjugate relation"

$$\sum_i u_i\bar{\boldsymbol{p}}_i+\sum_i v_i\boldsymbol{p}_i+\sum_i w_i\boldsymbol{q}_i=\boldsymbol{0}.$$

PROOF. Divide the row vectors into subvectors as in Lemma 1. Then the first relation is equivalent to the set of four or five relations for these subvectors. Multiplying by -1 if necessary, we get the second relation. q. e. d.

§ 3. Representation of τ.

In this section we take into account the different types of prime factors of $\mathfrak{f}(K/k)$, and express the matrix representing τ in terms of the coefficients appearing in the relations among the row vectors of the table A. To avoid studying too many different cases we assume that at least one prime of type p is totally ramified in Ω. This is sufficient for our purpose, since the other case is already settled in [1]. So, in the rest of the paper, let

$$p_0, p_1, \cdots, p_s, q_1, \cdots, q_t$$

be the set of rational primes totally ramified in Ω and put $p_i=\pi_i\bar{\pi}_i$ in k. If 3 is totally ramified, we count it among the q's and put $q=\sqrt{-3}$. Also we use σ_i, $\bar{\sigma}_i$ and ρ_i to denote the elements $\sigma_\mathfrak{p}$ for $\mathfrak{p}=(\pi_i)$, $(\bar{\pi}_i)$ and (q_i) respectively, and take σ_0 as σ_0 in Theorem 1, 3). Thus A consists of the row vectors $\bar{\boldsymbol{p}}_0$, $\boldsymbol{p}_1, \cdots, \boldsymbol{p}_s, \bar{\boldsymbol{p}}_1, \cdots, \bar{\boldsymbol{p}}_s, \boldsymbol{q}_1, \cdots, \boldsymbol{q}_t$. We distinguish two cases.

Case I. $\bar{\boldsymbol{p}}_0 \in \sum_{i=1}^{s} \boldsymbol{F}_3\boldsymbol{p}_i + \sum_{i=1}^{s} \boldsymbol{F}_3\bar{\boldsymbol{p}}_i + \sum_{i=1}^{t} \boldsymbol{F}_3\boldsymbol{q}_i$.

Case II. $\bar{\boldsymbol{p}}_0 \notin \sum_{i=1}^{s} \boldsymbol{F}_3\boldsymbol{p}_i + \sum_{i=1}^{s} \boldsymbol{F}_3\bar{\boldsymbol{p}}_i + \sum_{i=1}^{t} \boldsymbol{F}_3\boldsymbol{q}_i$.

We first treat Case I. Suppose that among the row vectors of A,

$$\boldsymbol{p}_1, \cdots, \boldsymbol{p}_a, \bar{\boldsymbol{p}}_1, \cdots, \bar{\boldsymbol{p}}_a, \bar{\boldsymbol{p}}_{a+1}, \cdots, \bar{\boldsymbol{p}}_b, \boldsymbol{q}_1, \cdots, \boldsymbol{q}_c$$

are linearly independent and

$$\boldsymbol{p}_i = \sum_{\alpha=1}^{a} P_{i\alpha}\boldsymbol{p}_\alpha + \sum_{\alpha=1}^{a} \bar{P}_{i\alpha}\bar{\boldsymbol{p}}_\alpha + \sum_{\beta=a+1}^{b} \bar{P}_{i\beta}\bar{\boldsymbol{p}}_\beta + \sum_{\gamma=1}^{c} P^0_{i\gamma}\boldsymbol{q}_\gamma, \qquad i=a+1, \cdots, s.$$

$$\bar{\boldsymbol{p}}_i = \sum_{\alpha=1}^{a} R_{i\alpha}\boldsymbol{p}_\alpha + \sum_{\alpha=1}^{a} \bar{R}_{i\alpha}\bar{\boldsymbol{p}}_\alpha + \sum_{\beta=a+1}^{b} \bar{R}_{i\beta}\bar{\boldsymbol{p}}_\beta + \sum_{\gamma=1}^{c} R^0_{i\gamma}\boldsymbol{q}_\gamma, \qquad i=0, b+1, \cdots, s.$$

$$\boldsymbol{q}_i = \sum_{\alpha=1}^{a} Q_{i\alpha}\boldsymbol{p}_\alpha + \sum_{\alpha=1}^{a} \bar{Q}_{i\alpha}\bar{\boldsymbol{p}}_\alpha + \sum_{\beta=a+1}^{b} \bar{Q}_{i\beta}\bar{\boldsymbol{p}}_\beta + \sum_{\gamma=1}^{c} Q^0_{i\gamma}\boldsymbol{q}_\gamma, \qquad i=c+1, \cdots, t.$$

In order to facilitate the calculations, we adopt the matrix notation and express the above three sets of relations in the following way:

(1) $$\begin{pmatrix} \boldsymbol{p}_{a+1} \\ \vdots \\ \boldsymbol{p}_s \end{pmatrix} = (P_{i\alpha}\bar{P}_{i\alpha}\bar{P}_{i\beta}P^0_{i\gamma}) \begin{pmatrix} \boldsymbol{p}_\alpha \\ \bar{\boldsymbol{p}}_\alpha \\ \bar{\boldsymbol{p}}_\beta \\ \boldsymbol{q}_\gamma \end{pmatrix},$$

(2) $$\begin{pmatrix} \bar{\boldsymbol{p}}_0 \\ \bar{\boldsymbol{p}}_{b+1} \\ \vdots \\ \bar{\boldsymbol{p}}_s \end{pmatrix} = (R_{i\alpha}\bar{R}_{i\alpha}\bar{R}_{i\beta}R^0_{i\gamma}) \begin{pmatrix} \boldsymbol{p}_\alpha \\ \bar{\boldsymbol{p}}_\alpha \\ \bar{\boldsymbol{p}}_\beta \\ \boldsymbol{q}_\gamma \end{pmatrix},$$

(3) $$\begin{pmatrix} \boldsymbol{q}_{c+1} \\ \vdots \\ \boldsymbol{q}_t \end{pmatrix} = (Q_{i\alpha}\bar{Q}_{i\alpha}\bar{Q}_{i\beta}Q^0_{i\gamma}) \begin{pmatrix} \boldsymbol{p}_\alpha \\ \bar{\boldsymbol{p}}_\alpha \\ \bar{\boldsymbol{p}}_\beta \\ \boldsymbol{q}_\gamma \end{pmatrix}.$$

Here, e. g., $(P_{i\alpha})$ stands for the matrix

$$\begin{pmatrix} P_{a+1,1} & \cdots & P_{a+1,a} \\ \vdots & & \vdots \\ P_{s,1} & \cdots & P_{s,a} \end{pmatrix}$$

and we shall add, if necessary, a line like "$i=a+1, \cdots, s$" to indicate the set of indices. Also, in this section and in § 5, we make the convention that the indices α, β and γ always run the sets $\{1, \cdots, a\}$, $\{a+1, \cdots, b\}$ and $\{1, \cdots, c\}$ respectively.

PROPOSITION 1. *In Case I, we can take as a basis of* $G(\tilde{K}/K_1)$ *the following elements:*

$$[\sigma_0, \bar{\sigma}_0],$$

$$[\sigma_0, \sigma_{a+1}], \cdots, [\sigma_0, \sigma_s], [\sigma_0, \bar{\sigma}_{b+1}], \cdots, [\sigma_0, \bar{\sigma}_s], [\sigma_0, \rho_{c+1}], \cdots, [\sigma_0, \rho_t],$$

and the matrix representing τ w.r.t. this basis (taken in this order) is

$$\begin{array}{l} \\ i=a+1,\cdots,b \\ i=b+1,\cdots,s \\ i=b+1,\cdots,s \\ i=c+1,\cdots,t \end{array}\left(\begin{array}{c|c|c|c|c} -1 & -1-\bar{R}_{0\beta} & -1\cdots-1 & -1\cdots-1 & -1\cdots-1 \\ \hline 0 & -\bar{P}_{i\beta} & 0 & 0 & 0 \\ \hline 0 & -\bar{P}_{i\beta} & 0 & I & 0 \\ \hline 0 & -\bar{R}_{i\beta} & I & 0 & 0 \\ \hline 0 & -\bar{Q}_{i\beta} & 0 & 0 & I \end{array}\right).$$

PROOF. By Theorem 1, 1), 2), Theorem 2 and the bilinearity of $[x, y]$, we see for $\beta=a+1,\cdots,b$,

$$\tau[\sigma_0,\sigma_\beta]\tau^{-1}=[\bar{\sigma}_0^{-1},\bar{\sigma}_\beta^{-1}]=[\bar{\sigma}_0,\bar{\sigma}_\beta]=[\bar{\sigma}_0,\sigma_0][\sigma_0,\bar{\sigma}_\beta]$$

$$=[\sigma_0,\bar{\sigma}_0]^{-1-\bar{R}_{0\beta}}\prod_{i=a+1}^{s}[\sigma_0,\sigma_i]^{-\bar{P}_{i\beta}}\prod_{i=b+1}^{s}[\sigma_0,\bar{\sigma}_i]^{-\bar{R}_{i\beta}}\prod_{i=c+1}^{t}[\sigma_0,\rho_i]^{-\bar{Q}_{i\beta}}.$$

For the other elements of the basis, we see

$$\tau[\sigma_0,\bar{\sigma}_0]\tau^{-1}=[\sigma_0,\bar{\sigma}_0]^{-1},$$

$$\tau[\sigma_0,\sigma_i]\tau^{-1}=[\sigma_0,\bar{\sigma}_0]^{-1}[\sigma_0,\bar{\sigma}_i], \qquad i=b+1,\cdots,s,$$

$$\tau[\sigma_0,\bar{\sigma}_i]\tau^{-1}=[\sigma_0,\bar{\sigma}_0]^{-1}[\sigma_0,\sigma_i], \qquad i=b+1,\cdots,s,$$

$$\tau[\sigma_0,\rho_i]\tau^{-1}=[\sigma_0,\bar{\sigma}_0]^{-1}[\sigma_0,\rho_i], \qquad i=c+1,\cdots,t. \quad \text{q. e. d.}$$

Next we treat Case II. Suppose that among the row vectors of A,

$$\bar{\boldsymbol{p}}_0,\boldsymbol{p}_1,\cdots,\boldsymbol{p}_a,\bar{\boldsymbol{p}}_1,\cdots,\bar{\boldsymbol{p}}_a,\bar{\boldsymbol{p}}_{a+1},\cdots,\bar{\boldsymbol{p}}_b,\boldsymbol{q}_1,\cdots,\boldsymbol{q}_c$$

are linearly independent. By assumption, $\bar{\boldsymbol{p}}_0$ does not appear in the expressions for the remaining vectors. We suppose, therefore, that the relations are again given by (1), (2) and (3) in Case I, except that we do not have the row for $\bar{\boldsymbol{p}}_0$ this time. Then $[\sigma_0,\bar{\sigma}_0]=1$, and hence

PROPOSITION 2. *In Case II, we can take as a basis of $G(\tilde{K}/K_1)$ the following elements:*

$$[\sigma_0,\sigma_{a+1}],\cdots,[\sigma_0,\sigma_s],[\sigma_0,\bar{\sigma}_{b+1}],\cdots,[\sigma_0,\bar{\sigma}_s],[\sigma_0,\rho_{c+1}],\cdots,[\sigma_0,\rho_t],$$

and the matrix representing τ w.r.t. this basis (taken in this order) is

$$\begin{array}{l} i=a+1,\cdots,b \\ i=b+1,\cdots,s \\ i=b+1,\cdots,s \\ i=c+1,\cdots,t \end{array}\left(\begin{array}{c|c|c|c} -\bar{P}_{i\beta} & 0 & 0 & 0 \\ \hline -\bar{P}_{i\beta} & 0 & I & 0 \\ \hline -\bar{R}_{i\beta} & I & 0 & 0 \\ \hline -\bar{Q}_{i\beta} & 0 & 0 & I \end{array}\right).$$

PROPOSITION 3. *In both cases, the multiplicity of the eigenvalue* 1 *of* τ *on* $G(K/K_1)$ *is equal to the sum of* $(s-b)+(t-c)$ *and the multiplicity of the eigenvalue* -1 *of the matrix* $(\bar{P}_{i\beta})$, i, $\beta=a+1, \cdots, b$.

PROOF. It suffices to divide the matrix into suitable blocks. q. e. d.

We call the matrix $(\bar{P}_{i\beta})$, i, $\beta=a+1, \cdots, b$, the essential part.

PROPOSITION 4. *The coefficient matrices in* (1), (2) *and* (3) *satisfy the following relations:*

$$(4)\qquad (\bar{P}_{i\alpha}P_{i\alpha}\ 0\ P^0_{i\tau})+(\bar{P}_{i\lambda})(P_{\lambda\alpha}\bar{P}_{\lambda\alpha}\bar{P}_{\lambda\beta}P^0_{\lambda\tau})=\begin{cases}(0\quad 0\quad I\quad 0), & i=a+1, \cdots, b.\\ (R_{i\alpha}\bar{R}_{i\alpha}\bar{R}_{i\beta}R^0_{i\tau}), & i=b+1, \cdots, s.\end{cases}$$

$$(5)\qquad (\bar{Q}_{i\alpha}Q_{i\alpha}\ 0\ Q^0_{i\tau})+(\bar{Q}_{i\lambda})(P_{\lambda\alpha}\bar{P}_{\lambda\alpha}\bar{P}_{\lambda\beta}P^0_{\lambda\tau})= (Q_{i\alpha}\bar{Q}_{i\alpha}\bar{Q}_{i\beta}Q^0_{i\tau}),\quad i=c+1, \cdots, t.$$

In both (4) *and* (5), $\lambda=a+1, \cdots, b$.

PROOF. We have only to apply Lemma 2 to (1) and (3), and replace $(\boldsymbol{p}_\beta)$ which appear in the right hand sides by (1) for $i=a+1, \cdots, b$. q. e. d.

REMARK. If there exists a prime q (including $\sqrt{-3}$), we can also take $\sigma_{(q)}$ for σ_0 in Theorem 1, 3). Then $\tau\sigma_0\tau^{-1}\equiv\sigma_0^{-1}$ modulo $G(\tilde{K}/K_1)$, and it is easy to see that we get a matrix of the same form as that in Proposition 2.

§ 4. A bound for the difference.

If m contains a rational prime $\not\equiv\pm1 \pmod 9$ other than 3, we know that $C_K^G=D_K$ (cf. [2], § 2, Remark 2), and the complete table is available through a simple calculation of cubic power residue symbols in k (cf. [2], § 3). So, in the rest of the paper, we assume that all the prime factors of m except 3 are $\equiv\pm1 \pmod 9$. Now for this type of m, we do not even know whether $C_K^G=D_K$ or not, and hence the table without the column for the extra element π_{t+1} should always be considered as potentially incomplete. For this reason, we call it the "temporary table" (regardless of whether $C_K^G=D_K$ or not).

Now suppose that we have $C_K^G\neq D_K$. Denote the temporary table by B, its row vectors by $\bar{\boldsymbol{p}}$, $\boldsymbol{p}$, $\boldsymbol{q}$ and the complete table by A. We show in this section, that "by applying Theorem 2 to B" in a suitable sense we can still define a representation space for τ, and that the multiplicity of the eigenvalue 1 of τ on this space differs at most by 1 from that on $G(\tilde{K}/K_1)$. Then in the next section, we shall show that the two multiplicities are at least congruent modulo 3.

To show the first assertion, we put ourselves in a somewhat abstract situation. Namely, let I be a finite set of indices and τ be a permutation of order 2 on I. Let $\{\tilde{X}(i,j) \mid i,j\in I,\ i\neq j\}$ be a set of indeterminates and $\tilde{V}$ be the vector space over $\boldsymbol{F}_3$ having $\{\tilde{X}(i,j)\}$ as a basis. Then τ induces an automorphism of order 2 on $\tilde{V}$ by

$$\tau(\tilde{X}(i, j))=\tilde{X}(\tau(i), \tau(j)) .$$

Let $\tilde{V}_0$ be the subspace of $\tilde{V}$ generated by the set

$$\{\tilde{X}(i, j)+\tilde{X}(j, i),\ \tilde{X}(i, j)+\tilde{X}(j, h)+\tilde{X}(h, i) \mid i, j, h \in I,\ i \neq j,\ i, j \neq h\} .$$

$\tilde{V}_0$ is τ-invariant, so that $V=\tilde{V}/\tilde{V}_0$ is again a τ-vector space. We denote the images of $\tilde{X}(i, j)$ in V by $X(i, j)$.

LEMMA 3. *If we fix an element $i_0 \in I$, the elements $X(i_0, j)$, $j \neq i_0$, constitute a basis of V.*

PROOF. Put $x_{ij}=\tilde{X}(i, j)+\tilde{X}(j, i)$, $i \neq j$, and $y_{ij}=\tilde{X}(i, j)+\tilde{X}(j, i_0)+\tilde{X}(i_0, i)$, $i \neq j$, $i, j \neq i_0$. Then we see

$$x_{ij}=x_{ji},\quad y_{ij}+y_{ji}=x_{ij}+x_{ji_0}+x_{i_0i} ,$$

$$\tilde{X}(i, j)+\tilde{X}(j, h)+\tilde{X}(h, i)=y_{ij}+y_{jh}+y_{hi}-x_{i_0i}-x_{i_0j}-x_{i_0h} .$$

Hence, if n is the number of elements of the set I, $\tilde{V}_0$ is generated by $\binom{n}{2}+\binom{n-1}{2}=(n-1)^2$ elements. q. e. d.

Now take as I the set of prime factors $\{\mathfrak{p}_0, \cdots, \mathfrak{p}_t\}$ of $\mathfrak{f}(K/k)$ in k, τ being understood in the obvious sense (we go back to the notation in Theorem 1, 3) for a moment for the sake of simplicity), take $\mathfrak{p}_0$ as i_0, and put

$$W=\{\sum_{i=1}^{t} b_i X(\mathfrak{p}_0, \mathfrak{p}_i) \in V \mid B\boldsymbol{y}=(b_i) \text{ has a solution}\} ,$$

$$W'=\{\sum_{i=1}^{t} b_i X(\mathfrak{p}_0, \mathfrak{p}_i) \in V \mid A\boldsymbol{x}=(b_i) \text{ has a solution}\} ,$$

where $\boldsymbol{y}$ is the set of unknowns corresponding to the coefficient matrix B. Then it is easily verified that W and W' are subspaces of V and that $W \subset W'$. On the other hand, it is clear that the map $\tilde{X}(\mathfrak{p}_i, \mathfrak{p}_j) \mapsto [\sigma_{\mathfrak{p}_i}, \sigma_{\mathfrak{p}_j}]$ induces a τ-homomorphism of V onto $G(\tilde{K}/K_1)$, and Theorem 1, 3) implies that W' is its kernel. Hence W' is τ-invariant and V/W' is τ-isomorphic to $G(\tilde{K}/K_1)$.

LEMMA 4. *W is τ-invariant.*

PROOF. Returning to the notation at the beginning of § 3, if

$$Y=\bar{b}_0 X(\pi_0, \bar{\pi}_0)+\sum_{i=1}^{s} b_i X(\pi_0, \pi_i)+\sum_{i=1}^{s} \bar{b}_i X(\pi_0, \bar{\pi}_i)+\sum_{i=1}^{t} c_i X(\pi_0, q_i)$$

is an element of W, there exists a vector $\boldsymbol{y}$ such that

$$B\boldsymbol{y}={}^t(\bar{b}_0, b_1, \cdots, b_s, \bar{b}_1, \cdots, \bar{b}_s, c_1, \cdots, c_t) .$$

By the same calculation as in § 3, we see

$$\tau(Y)=\{-\bar{b}_0-\sum_{i=1}^{s} b_i-\sum_{i=1}^{s} \bar{b}_i-\sum_{i=1}^{t} c_i\} X(\pi_0, \bar{\pi}_0)$$

$$+\sum_{i=1}^{s} \bar{b}_i X(\pi_0, \pi_i)+\sum_{i=1}^{s} b_i X(\pi_0, \bar{\pi}_i)+\sum_{i=1}^{t} c_i X(\pi_0, q_i) .$$

But if ${}^t\boldsymbol{y}=(y, {}^t\boldsymbol{y}_1, {}^t\boldsymbol{y}_2, {}^t\boldsymbol{y}_3)$ is the division of $\boldsymbol{y}$ corresponding to that of the row vectors of B as in Lemma 1, the same Lemma shows that ${}^t\boldsymbol{y}'=(y, -{}^t\boldsymbol{y}_2, -{}^t\boldsymbol{y}_1, -{}^t\boldsymbol{y}_3)$ satisfies

$$B'\boldsymbol{y}'={}^t(\bar{b}_0, \bar{b}_1, \cdots, \bar{b}_s, b_1, \cdots b_s, c_1, \cdots, c_t),$$

where B' is the matrix obtained from B by replacing $\bar{\boldsymbol{p}}_0$ with $\boldsymbol{p}_0$. Since we have

$$\bar{\boldsymbol{p}}_0=-\boldsymbol{p}_0-\sum_{i=1}^{s}\boldsymbol{p}_i-\sum_{i=1}^{s}\bar{\boldsymbol{p}}_i-\sum_{i=1}^{t}\boldsymbol{q}_i$$

by the product formula, we get the conclusion. q. e. d.

By Lemma 4, V/W is also a τ-vector space. When we say "the space defined by Theorem 2 from the temporary table B", we shall mean the factor space V/W just defined. By construction, Propositions 1, 2 and 3 are valid on V/W, too. Now $G(\tilde{K}/K_1)$ is τ-isomorphic to a factor space of V/W. So, if $\{v_1, \cdots, v_r\}$ is a basis of V/W consisting of eigenvectors of τ (such a basis does exist, because τ is of order 2 on V/W, cf. [3], § 1), we can choose a basis of $G(\tilde{K}/K_1)$ among the images of $v_1, \cdots, v_r$. But clearly $\mathrm{rank}(A)\leqq \mathrm{rank}(B)+1$, and hence

THEOREM 3. *The multiplicity of the eigenvalue* 1 *of* τ *on* $G(\tilde{K}/K_1)$ *differs at most by* 1 *from that on the space defined by Theorem* 2 *from the temporary table.*

§ 5. A congruence for the difference.

Always supposing that $C_K^G\neq D_K$, let A and B be respectively the complete table and the temporary one as in § 4, and denote by $\boldsymbol{p}_i'$, $\bar{\boldsymbol{p}}_i'$ and $\boldsymbol{q}_i'$ the row vectors of A corresponding to $\mathfrak{p}=(\pi_i)$, $(\bar{\pi}_i)$ and (q_i). Then by Lemma 1, $\boldsymbol{q}_i'=(\boldsymbol{q}_i, 0)$, and if we put $\boldsymbol{p}_i'=(\boldsymbol{p}_i, x_i)$, we have $\bar{\boldsymbol{p}}_i'=(\bar{\boldsymbol{p}}_i, -x_i)$. If $\mathrm{rank}(A)=\mathrm{rank}(B)$, the row vectors of the two tables satisfy the same set of relations and we obtain the same multiplicity of the eigenvalue 1. So assume that $\mathrm{rank}(A)=\mathrm{rank}(B)+1$. Then we can get a maximal set of linearly independent row vectors in A by adding a new vector to the set of vectors corresponding to those of a maximal set in B. Assuming that the row vectors of B satisfy the relations given in § 3, there are three cases (whether we are in Case I or in Case II w. r. t. B).

Case a). We can find a new vector among $\boldsymbol{p}_{a+1}', \cdots, \boldsymbol{p}_b'$. Then we suppose (without loss of generality) that it is $\boldsymbol{p}_{a+1}'$.

Case b). We can not find a new vector among $\boldsymbol{p}_{a+1}', \cdots, \boldsymbol{p}_b'$, but can find one among $\boldsymbol{p}_{b+1}', \cdots, \boldsymbol{p}_s', \bar{\boldsymbol{p}}_{b+1}', \cdots, \bar{\boldsymbol{p}}_s'$. Then we suppose that it is $\bar{\boldsymbol{p}}_{b+1}'$.

Case c). Otherwise.

LEMMA 5. *In Case* a), *the multiplicities of the eigenvalue* 1 *obtained from*

A and B are congruent modulo 3.

PROOF. We have by (1) in § 3,

$$(1') \qquad \begin{pmatrix} \boldsymbol{p}'_{a+1} \\ \vdots \\ \boldsymbol{p}'_b \end{pmatrix} = (P_{i\alpha}\bar{P}_{i\alpha}\bar{P}_{i\beta}P^0_{i\tau}) \begin{pmatrix} \boldsymbol{p}'_\alpha \\ \bar{\boldsymbol{p}}'_\alpha \\ \bar{\boldsymbol{p}}'_\beta \\ \boldsymbol{q}'_\tau \end{pmatrix} + \begin{pmatrix} \mathbf{0}, \varepsilon_{a+1} \\ \vdots \quad \vdots \\ \mathbf{0}, \varepsilon_b \end{pmatrix},$$

where $\varepsilon_i=0, \pm 1$ and $\varepsilon_{a+1}\neq 0$ by assumption. Then we get for $i=a+2, \cdots, b$,

$$\boldsymbol{p}'_i=(P_{i\alpha}\bar{P}_{i\alpha}\bar{P}_{i\beta}P^0_{i\tau}) \begin{pmatrix} \boldsymbol{p}'_\alpha \\ \bar{\boldsymbol{p}}'_\alpha \\ \bar{\boldsymbol{p}}'_\beta \\ \boldsymbol{q}'_\tau \end{pmatrix} + \varepsilon_i\varepsilon_{a+1}\{\boldsymbol{p}'_{a+1} - (P_{a+1,\alpha}\bar{P}_{a+1,\alpha}\bar{P}_{a+1,\beta}P^0_{a+1,\tau}) \begin{pmatrix} \boldsymbol{p}'_\alpha \\ \bar{\boldsymbol{p}}'_\alpha \\ \bar{\boldsymbol{p}}'_\beta \\ \boldsymbol{q}'_\tau \end{pmatrix}\}.$$

Hence the essential part from A is

$$(\bar{P}'_{i\beta})=(\bar{P}_{i\beta}-\varepsilon_i\varepsilon_{a+1}\bar{P}_{a+1,\beta}), \qquad i,\ \beta=a+2, \cdots, b.$$

But (1′) implies for $i=a+1, \cdots, b$ (recall $\boldsymbol{p}'_i=(\boldsymbol{p}_i, x_i)$, etc.),

$$(x_i)=(P_{i\alpha})(x_\alpha)-(\bar{P}_{i\alpha})(x_\alpha)-(\bar{P}_{i\beta})(x_\beta)+(\varepsilon_i).$$

Multiplying the two sides by $(\bar{P}_{i\lambda})$, $i, \lambda=a+1, \cdots, b$, we get by Proposition 4, (4),

$$(\bar{P}_{i\lambda})(x_\lambda)=-(\bar{P}_{i\alpha})(x_\alpha)+(P_{i\alpha})(x_\alpha)-(x_i)+(\bar{P}_{i\lambda})(\varepsilon_\lambda).$$

This shows $(\bar{P}_{i\lambda})(\varepsilon_\lambda)=(\varepsilon_i)$, $i, \lambda=a+1, \cdots, b$. Since $(\varepsilon_i)\neq 0$, we see that 1 is an eigenvalue of $(\bar{P}_{i\beta})$, and moreover,

$$\sum_{\lambda=a+1}^{b} \bar{P}_{a+1,\lambda}\varepsilon_\lambda=\varepsilon_{a+1},$$

or multiplying by ε_{a+1}, $\sum_{\lambda=a+1}^{b} \varepsilon_\lambda\varepsilon_{a+1}\bar{P}_{a+1,\lambda}=1$. Then

$$\operatorname{tr}(\bar{P}_{i\beta})-1=\sum_{i=a+1}^{b} \bar{P}_{ii}-\sum_{i=a+1}^{b} \varepsilon_i\varepsilon_{a+1}\bar{P}_{a+1,i}=\operatorname{tr}(\bar{P}'_{i\beta}),$$

where in the left hand side, $i, \beta=a+1, \cdots, b$. Since the essential parts obtained from A and B both have only ± 1 as their eigenvalues, the above equality shows that the multiplicities of the eigenvalue -1 in the two are congruent modulo 3. Proposition 3 now gives the conclusion. q. e. d.

LEMMA 6. *In Case* b), *the multiplicities of the eigenvalue* 1 *obtained from A and B are equal.*

PROOF. By assumption, we have by (1) and (2) in § 3,

$$(1'') \qquad \begin{pmatrix} \boldsymbol{p}'_{a+1} \\ \vdots \\ \boldsymbol{p}'_b \\ \boldsymbol{p}'_{b+1} \end{pmatrix} = (P_{i\alpha}\bar{P}_{i\alpha}\bar{P}_{i\beta}P^0_{i\tau}) \begin{pmatrix} \boldsymbol{p}'_\alpha \\ \bar{\boldsymbol{p}}'_\alpha \\ \bar{\boldsymbol{p}}'_\beta \\ \boldsymbol{q}'_\tau \end{pmatrix} + \begin{pmatrix} \mathbf{0}, 0 \\ \vdots \quad \vdots \\ \mathbf{0}, 0 \\ \mathbf{0}, \varepsilon_{b+1} \end{pmatrix},$$

$$(2'')\qquad \bar{\boldsymbol{p}}'_{b+1}=(R_{b+1,\alpha}\bar{R}_{b+1,\alpha}\bar{R}_{b+1,\beta}R^{0}_{b+1,r})\begin{pmatrix}\boldsymbol{p}'_{\alpha}\\ \bar{\boldsymbol{p}}'_{\alpha}\\ \bar{\boldsymbol{p}}'_{\beta}\\ \boldsymbol{q}'_{r}\end{pmatrix}+(\mathbf{0},\bar{\varepsilon}_{b+1}),\ \bar{\varepsilon}_{b+1}\neq 0\,.$$

Then by the same calculation as in Lemma 4, we see that the essential part from A is

$$\left(\begin{array}{c|c}\bar{P}_{i\beta} & 0\\ \hline \bar{P}_{b+1,\beta}-\varepsilon_{b+1}\bar{\varepsilon}_{b+1}\bar{R}_{b+1,\beta} & \varepsilon_{b+1}\bar{\varepsilon}_{b+1}\end{array}\right),\qquad i,\beta=a+1,\cdots,b\,.$$

But (1″) and (2″) imply in particular

$$(*)\qquad \begin{pmatrix}x_{a+1}\\ \vdots\\ x_{b}\end{pmatrix}=(P_{i\alpha}\bar{P}_{i\alpha}\bar{P}_{i\beta})\begin{pmatrix}x_{\alpha}\\ -x_{\alpha}\\ -x_{\beta}\end{pmatrix},$$

$$x_{b+1}=(P_{b+1,\alpha})(x_{\alpha})-(\bar{P}_{b+1,\alpha})(x_{\alpha})-(\bar{P}_{b+1,\beta})(x_{\beta})+\varepsilon_{b+1}\,,$$

$$-x_{b+1}=(R_{b+1,\alpha}\bar{R}_{b+1,\alpha}\bar{R}_{b+1,\beta})\begin{pmatrix}x_{\alpha}\\ -x_{\alpha}\\ -x_{\beta}\end{pmatrix}+\bar{\varepsilon}_{b+1}$$

$$=(\bar{P}_{b+1,\alpha})(x_{\alpha})-(P_{b+1,\alpha})(x_{\alpha})+(\bar{P}_{b+1,\beta})(x_{\beta})+\bar{\varepsilon}_{b+1}\,,$$

where in the last equality, we used Proposition 4, (4) and (*). Hence $\varepsilon_{b+1}\bar{\varepsilon}_{b+1}=-1$. q. e. d.

LEMMA 7. *In Case* c), *the multiplicities of* 1 *obtained from A and B are equal.*

PROOF. By assumption we have again (*) in the proof of Lemma 6. Then, applying the two sides of Proposition 4, (5) to ${}^{t}(x_{\alpha},-x_{\alpha},-x_{\beta})$, we get for $i=c+1,\cdots,t$,

$$(\bar{Q}_{i\alpha})(x_{\alpha})-(Q_{i\alpha})(x_{\alpha})+(\bar{Q}_{i\beta})(x_{\beta})=(Q_{i\alpha})(x_{\alpha})-(\bar{Q}_{i\alpha})(x_{\alpha})-(\bar{Q}_{i\beta})(x_{\beta})\,.$$

Hence the two sides are equal to $\mathbf{0}$, and this means that we can not find a new vector among $\boldsymbol{q}'_{c+1},\cdots,\boldsymbol{q}'_{t}$, either. Then we are necessarily in Case I with the vectors in B, but in Case II with those in A, and there is no change in the essential part. q. e. d.

Lemma 5 combined with Theorem 3, Lemma 6 and Lemma 7 now give

THEOREM 4. *If all the prime factors of* m *except* 3 *are* $\equiv\pm1\pmod 9$, *the multiplicity of the eigenvalue* 1 *of* τ *on* $G(\tilde{K}/K_{1})$ *is equal to that on the space defined by Theorem* 2 *from the temporary table.*

As an algorithm for $d^{(3)}C_{\mathfrak{Q}}$, therefore, we can make calculations as if we had $C_{K}^{G}=D_{K}$.

§ 6. Example.

Let $m=3\cdot 17\cdot 271=24^3-3$. Then $N_{\mathbb{Q}/\mathbb{Q}}(24-\sqrt[3]{m})=3$ and the same argument as in [1], § 2, Remark shows that $C_K^G \neq D_K$. The temporary table is

	ζ	π_{271}	$\bar{\pi}_{271}$	17	$\sqrt{-3}$
(π_{271})	0	−1	0	1	0
$(\bar{\pi}_{271})$	0	0	1	−1	0
(17)	0	1	−1	0	0
$(\sqrt{-3})$	0	0	0	0	0 ,

where we put $\zeta=(-1+\sqrt{-3})/2$, $\pi_{271}=(29+9\sqrt{-3})/2$. We are in Case II in the sense of § 3, and by virtue of Theorem 4 we get $d^{(3)}C_{\mathbb{Q}}=2$.

References

[1] S. Kobayashi, On the 3-rank of the ideal class groups of certain pure cubic fields, J. Fac. Sci. Univ. Tokyo Sec. IA, 18 (1973), 209-216.

[2] S. Kobayashi, On the 3-rank of the ideal class groups of certain pure cubic fields II, ibid., 21 (1974), 263-270.

[3] S. Kobayashi, On the l-class rank in some algebraic number fields, J. Math. Soc. Japan, 26 (1974), 668-676.

Shinju KOBAYASHI
Department of Mathematics
Faculty of Education
Chiba University
Yayoicho, Chiba
Japan