On 3-class groups of non-Galois cubic fields

by

Kitoaki Imura (Tokyo)

Introduction. In this paper we give information about a certain direct summand of the 3-class group of a non-Galois cubic extension field of the rational numbers $Q$, and show using it that for any finite elementary abelian 3-group $G$, there exist infinitely many pure cubic fields whose 3-class groups are isomorphic to $G$.

Throughout this paper we use multiplicative notation for groups and modules, and the action of a group or a ring on a module is expressed by exponentiation. Furthermore $(a^n)^r = a^{nr}$. The cubical Hilbert symbol \((a, b)_p\) used here corresponds to \((a, b)_p\) in [5].

1. A direct summand of the 3-class group. Let $L$ be a non-Galois cubic extension field of $Q$, let $K$ be the normal closure of $L$, and let $k$ be the quadratic subfield of $K$. Let $x$ be a generator of the Galois group $G(K | k)$, and let $r$ be the generator of $G(K | L)$. Then $G(K | Q)$ is generated by $\{x, r\}$ with the relations $x^3 = r^2 = 1$, $xr = rx$. For any finite algebraic extension field $F$ of $Q$, let $H(F)$ denote the 3-class group of $F$. As the canonical homomorphism $H(L) \to H(K)$ is injective, we may consider $H(L)$ as a subgroup of $H(K)$. For all nonnegative integers $i$, we define

$$H_i(K) = \{ h \in H(K) | h^{3^i} = 1 \}$$

and

$$H_i(L) = \{ h \in H_i(K) | h^3 = h \}.$$ 

Then $H_i(K)$ is a subgroup of $H(K)$ and is a $Z[G(K | Q)]$-module; $H_i(L)$ is a subgroup of $H(L)$ and $H_i(L) = H_i(K)^{3^i}$; $H_i(L) = H_i(K)$ for large $i$ (cf. [4], Proposition 1). Furthermore let $N: H(K) \to H(k)$ be the map induced by the norm map from ideals of $K$ to ideals of $k$. Note that $N(H(L)) = \{ 1 \}$ since $H(L) = H(K)^{3^i}$ and $H(Q) = \{ 1 \}$.

Now we let $H$ be a maximal direct summand of $H(L)$ contained in $H_i(L) = \{ h \in H(K) | h^3 = h^i = h \}$. 

acta arithmetica
xxxv (1979)
Since $H_3(L)$ is an elementary abelian 3-group, then
\[(1.1) \quad H \times (H(L)^3)^{H_3(L)} = H_3(L).\]

Our goal in this section is to compute the rank of $H$. Since $H$ has exponent 3, it suffices to compute $|H|$ (= the order of $H$).

**Lemma 1.1.** $H(L)^3 \cap H_2(L) = H_3(L)^{H_3(L)}$.

**Proof.** We first show that $H(L)^3 \cap H_2(L) = H_3(L)^{H_3(L)} \cap H_2(L)$. Let $h \in H(L)^3 \cap H_2(L)$; i.e. \( h = h^1 \cap H_2(L). \) Then

\[ h^{3^{-1} \cdot 3^{-1}} = h_1 = h_2 = h^{-1} \]

since $h_1^{3^{-1} \cdot 3^{-1}} \in N(H_2(L))$ and $h_2^3 = h$. Also $h_1^{3^{-1} \cdot 3^{-1}} = h$, which implies that $h \in H_3(L)$. So $h = h_1^{3^{-1} \cdot 3^{-1}} \in H_3(L)^{H_3(L)} \cap H_2(L)$. Next let $h \in H_3(L)^{H_3(L)} \cap H_2(L)$; i.e. $h = h_1^{3^{-1} \cdot 3^{-1}}$ with $h_1 \in H_3(L)$. Then $h = h_1^{3^{-1} \cdot 3^{-1}} = h_1^{3^{-1} \cdot 3^{-1}}$ since $h_1^{3^{-1} \cdot 3^{-1}} = 1$. So $h^{3^{-1} \cdot 3^{-1}} = h$ and hence $h \in H(L)^3$. We next show that $H_3(L)^{H_3(L)} \subseteq H_2(L)$. Let $h \in H_3(L)$. Then

\[ h^{3^{-1} \cdot 3^{-1}} = h^{-3} = h \in H_2(L) \cap H_3(L) = H_2(L) \]

since $h_1^{3^{-1} \cdot 3^{-1}} = 1$ and $h_2^{3^{-1} \cdot 3^{-1}} \in H_2(L)$. This proves the lemma.

**Lemma 1.2.** There is an exact sequence

\[1 \to H_4(L) \to H_5(L) \to H_5(L)^{H_5(L)} \to 1.\]

**Proof.** The proof is immediate from the fact that $H_4(L) \cap H_5(L) = H_5(L)$.

**Lemma 1.3.** For $i = 1, 2$, let

\[ V_i = \langle H_i(L), H_{i-1}(K) \rangle \quad \text{and} \quad \tilde{V}_i = \{ h \in H(L) | h^{i-1} \in V_i \}. \]

Then

\[ [H_{i+1}(K)/H_{i+1}(L)] = [\tilde{V}_i/V_i]^{-1} [H_i(K)/H_i(L)]. \]

**Proof.** This lemma is proved in [8], Lemma 6.

We now compute $|H|$ using the above lemmas.

\[ (1.2) \quad |H| = |H_3(L)| \cdot |H(L)| \cdot |H_5(L)| \quad \text{(by (1.1))} \]
\[ = |H_3(L)| \cdot |H_3(L)^{H_3(L)}| \quad \text{(by Lemma 1.1)} \]
\[ = |H_3(L)| \cdot |H_3(L)| \cdot |H_3(L)| \quad \text{(by Lemma 1.2)} \]
\[ = |H_3(L)| \cdot |H_3(L)| \cdot |\tilde{V}_2/V_2| \cdot |H_2(K)| \quad \text{(by Lemma 1.3)} \]
\[ = |H_3(L)| \cdot |H_3(K)| \cdot |\tilde{V}_2/V_2| \cdot |H_2(K)| \cdot |H_2(K)/H_2(K)| \quad \text{(by Lemma 1.3)} \]
\[ = |H_3(K)| \cdot |H_3(K)| \cdot |\tilde{V}_2/V_2| \cdot |H_2(K)| \cdot |H_2(K)| \quad \text{(by Lemma 1.3)} \]
\[ = |H_3(K)| \cdot |H_3(K)| \cdot |\tilde{V}_2/V_2| \cdot |H_2(K)| \cdot |H_2(K)/H_2(K)| \quad \text{(by Lemma 1.3).} \]

Now the four numbers of the last side of the above equation are given as follows (cf. [3], Theorem 4.3 and [6], Section 2):

\[ |H_3(K)| = 3^{r_1-1} |H_3(K)|, \]
\[ |H_3(K)/H_3(L)| = 3^{r_1-1} |H_3(L)/N(H_3(L))|, \]
\[ |\tilde{V}_2/V_2| = 3^{s_2-1} |V_2| / |H_2(K)|, \]
\[ |\tilde{V}_2/V_2| = 3^{s_2-1} |V_2| / |H_2(K)|, \]

where $t$ is the number of primes of $k$ which ramify in $K$, and $r_1, r_2, r_3, r_i$ are all non-negative rational integers, which are in fact defined to be the ranks of certain matrices (over the finite field $F_3$ of 3 elements) associated with the groups $H_3(K) = \langle 1 \rangle$, $H_3(L) = \{ v \}, V_2, V_3, V_4, V_5$ respectively. We note that $0 \leq r_1 \leq r_2 \leq r_3 \leq r_4 \leq \max(0, t-1)$. Using these equations, equation (1.2) becomes

\[ |H| = 3^{r_1-1} |H_3(K)| / |H_3(L)| \cdot |H_2(K)/H_2(L)|, \]

Letting $|H_3(K)| / |H_3(L)| = 3^{t-1} |H_3(L)| / |H_3(L)|$, we obtain the following result.

**Theorem 1.4.** With the above notations,

\[ \text{rank } H = r_3 - r_2 + r_1 - t + u. \]

**Corollary 1.5.** $H(L)$ has an elementary abelian direct factor of rank $r_3 - r_2 + r_1 - t + u$ contained in $H_3(L)$.

The following lemma, which provides us a sufficient condition that $H(L)$ is an elementary abelian 3-group, will be useful in the subsequent sections.

**Lemma 1.6.** If rank $H(L) = t - r_1$, then $H(K) = H_3(K)$, and hence $H(L) = H_3(L)$, which is an elementary abelian 3-group.

**Remark.** Let $\chi H_1(K) = \{ h \in H_1(K) | N(h) = 1 \}$. Then $\chi H_1(K)$ is an elementary abelian 3-group of rank $t - 1 - r_1 - u$, where $\chi$ is the rank of a certain subgroup of $H(k)/H(k)^3$ (cf. [2], Proposition 3.2).

So

\[ \text{rank } H_4(K) \geq t - 1 - r_1 + \text{rank } H(k) - \chi. \]

Note that if $H(k) = \{ 1 \}$, then $H_4(K)$ is an elementary abelian 3-group of rank $t - 1 - r_1$ (since $\chi H_4(K) = H_4(K)$).

**Proof.** It is clear that $(\sigma - 1)^t$ maps $H_{i+1}(K)/H_i(K)$ injectively into $H_{i+1}(K)/H_i(K)$ for all integers $i \geq 0$. So to show that $H(K) = H_3(K)$, it suffices to show that $|H_3(K)/H_3(L)| = 1$. Now

\[ |H_3(K)/H_3(L)| = |H_3(K)/H_3(L)| \cdot |H_3(L)| \cdot |H_3(L)|^{-1} \cdot |H_3(L)| \]
\[ = |\tilde{V}_2/V_2| \cdot |H_2(K)| \cdot |H_2(K)|^{-1} \cdot |H_2(K)| \quad \text{(by Lemma 1.3),} \]
\[ = 3^{s_2-1} |H_3(L)|. \]

It is easy to see that $H_3(L) = \{ h \in H(L) | h^3 = 1 \}$; hence $|H_3(L)| = 3^{\text{rank } H(k)}$. The lemma is now immediate.

Now we want to describe explicitly a matrix over $F_3$ whose rank is exactly $r_1 - r_2$. Let $p_1, \ldots, p_i$ be the primes of $k$ which ramify in $K$, let $\mathfrak{p}_i$
be the unique prime of \( K \) above \( p_1 \), and let \( \overline{Q} \) be any prime of \( \mathfrak{h}(\zeta) \) above \( p_1 \), where \( \zeta \) is a primitive cube root of unity. Let \( a \) be an element of \( k(\zeta) \) such that \( \mathcal{K}(\zeta) = k(\zeta, \sqrt[3]{a}) \). Furthermore let \( p_1, \ldots, p_r \) be the rational primes which ramify fully in \( L \). If we let \( H'_1(K) \) be the subgroup of \( H_1(K) \) generated by the ideal classes of the \( \mathfrak{p}_i \)’s and by the image in \( H'(K) \) of \( H_1(k) \), then the factor group \( H_1(K)/H'_1(K) \) is either trivial or cyclic of order 3, and in the latter case there is an ideal \( \mathfrak{m} \) of \( L \) whose ideal class together with \( H'_1(K) \) generates \( H_1(K) \) (cf. [4], proof of Proposition 2). Let \( p_{s+1} \) be a rational number such that \( N(\mathfrak{m}) = (p_{s+1}) \) when \( H_1(K) \neq H'_1(K) \), and let \( p_{s+1} = 1 \) when \( H_1(K) = H'_1(K) \). Then

\[
r_1 - r_s = \text{rank} (a) \quad (1 \leq i \leq s + 1, 1 \leq j \leq t),
\]

where \( a \) is an element of the finite field \( F_2 \) given by

\[
\zeta^a = \left( \frac{p_i}{\mathfrak{p}_j} \right) \quad (1 \leq i \leq s + 1, 1 \leq j \leq t).
\]

We note that if \( p_2 \) is not decomposed over \( Q \), then \( \left( \frac{p_i}{\mathfrak{p}_j} \right) = 1 \) for any \( p_1 \) (cf. [7], proof of Lemma 3).

2. Applications to pure cubic fields. Let notations be the same as in Section 1. We first prove the following theorem.

**Theorem 2.1.** Let \( G \) be any finite elementary abelian 3-group. Then there exist infinitely many pure cubic fields whose 3-class groups are isomorphic to \( G \).

**Proof.** Let \( n = \text{rank} \mathfrak{g} \). Let \( p_1, \ldots, p_m, q \) be rational primes satisfying the following conditions:

(i) \( p_i \equiv 1 \pmod{9} \) for \( 1 \leq i \leq m \), \( q \equiv 2 \pmod{9} \);

(ii) \( p_i \) is a cubic residue modulo \( p_j \) if \( i < j \);

(iii) \( p_1 \cdots p_{r-1} = q \) is a cubic nonresidue modulo \( p_i \) for each \( i \).

By Dirichlet’s theorem on rational primes in an arithmetic progression, there exist infinitely many such primes \( p_1, \ldots, p_m, q \). In fact, \( p \) (resp. \( q \)) can be chosen from a congruence modulo \( 9p_1 \cdots p_{r-1} \) (resp. \( 9p_1 \cdots p_{r-1} \)) with coefficients in \( \mathbb{Z} \). Note that the normal closure \( K \) of \( L = Q(\zeta, \sqrt[3]{n}) \), where \( \zeta \) is a primitive cube root of unity. We want to show that \( H(K) \) is an elementary abelian 3-group of rank \( n \). Using [1], Theorem 4.5, and assumption (I), it is easy to compute that

\[
\text{rank} H(K) = 2m - \text{rank} (\gamma_q),
\]

where \( (\gamma_q) \) is the \( m \times m \) matrix (over \( F_2 \)) whose \( ij \)-th element \( \gamma_{ij} \) satisfies

\[
\gamma_{ij} = \left( \frac{p_{ij, n}}{p_j} \right),
\]

where \( p_{ij} \) is any prime of \( Q(\zeta) \) above \( p_i \). For \( 1 \leq i < j \leq m \), we have from assumption (II) that

\[
\gamma_{ij} = \left( \frac{p_{ij, n}}{p_j} \right) = \left( \frac{p_{ij}}{p_j} \right) = \left( \frac{1}{p_j} \right) = 1,
\]

which implies that \( \gamma_{ij} = 0 \) if \( i < j \). Also from assumptions (ii) and (iii),

\[
\gamma_{ii} = \left( \frac{p_{ii, n}}{p_i} \right) = \left( \frac{p_{ii}}{p_i} \right) = \left( \frac{1}{p_i} \right) = 1.
\]

So \( \text{rank} (\gamma_q) = m \), and hence \( \text{rank} H(K) = m \). In view of the definitions of the two matrices \( (\gamma_q) \) and \( (a) \), where \( (a) \) is defined by equation (1.3), it is clear that

\[
\text{rank} (\gamma_q) = \text{rank} (a) = r_1 - r s.
\]

Combining these and Corollary 1.5 we know that \( \text{rank} H(L) = r_1 - r s \), which together with Lemma 1.6 shows that \( H(L) \) is an elementary abelian 3-group of rank \( m \).

**Remark.** In the above proof, Lemma 1.6 together with the remark following this lemma shows that \( H(K) \) is also an elementary abelian 3-group of rank \( 2m \).

A statement similar to Theorem 2.1 is true for the normal closures of pure cubic fields.

**Theorem 2.2.** Let \( G \) be any elementary abelian 3-group. Then there exist infinitely many pure cubic fields such that the 3-class groups of their normal closures are isomorphic to \( G \).

**Proof.** The above remark gives the proof when \( \text{rank} G \) is even. So assume that \( \text{rank} G = 2m - 1 \). Let \( p_1, \ldots, p_m, q \) be rational primes satisfying the conditions (ii), (iii) given in the proof of Theorem 2.1 and following another one:

(i) \( p_i = 1 \pmod{9} \) for \( 1 \leq i \leq m - 1 \), \( p_m = 4 \pmod{9} \), \( q = 2 \pmod{9} \).

Again Dirichlet’s theorem shows that there exist infinitely many such primes \( p_1, \ldots, p_m, q \). Let \( L = Q(\sqrt[3]{n}) \), where \( n = p_1 \cdots p_m q \), and let \( K \) be its normal closure. We want to show that \( H(K) \) has exponent 3 and rank \( 2m - 1 \). Again by [1], Theorem 4.5, and assumption (I), we have

\[
\text{rank} H(K) = 2m - 1 - \text{rank} (\gamma_q),
\]
where \((\gamma_d)\) is the \((m-1) \times m\) matrix whose \(ij\)-th element \(\gamma_d\) satisfies

\[
\zeta^{\gamma_d} = \left(\frac{p_i \cdot N_d}{p_j}\right),
\]

where \(p_j\) for each \(j = 1, \ldots, m-1\) is any prime of \(Q(\zeta)\) above \(p_j\). The same argument as in the proof of Theorem 3.1 shows that rank \((\gamma_d)\) = \(m-1\), rank \(H(L) = m\), and rank \((a_d) = r_1 - r > m\). Hence, these, Corollary 1.5, Lemma 1.6, and the remark following this lemma combine to yield the desired result.

3. Some examples. In this section we further illustrate Corollary 1.5 and Lemma 1.6 with some of the examples that appear in [2], Section 4. We use the notation in Section 1. As our first example we let \(L\) be a cubic extension of \(Q\) obtained by adjoining a root of \(x^3 - 3 - 13x + 2 - 13 - 17 = 0\) to \(Q\). Then rank \(H(L) = 2\); \(k = Q(\sqrt{23})\) and \(H(k)\) is cyclic of order 3. Furthermore the rational primes which ramify fully in \(L\) are 3 and 13, and both of them decompose in \(k\). We want to show that \(H(L)\) is in fact equal to \(H_1(L)\) which has exponent 3. By Corollary 1.5 and Lemma 1.6, this follows if we can show that rank \((a_d) = 2\). To see this, we let \(p_1\) and \(p_2\) (resp. \(p_3\) and \(p_4\)) be distinct primes of \(k\) above 13 (resp. 3) and \(\mathfrak{P}_i\) for each \(i = 1, \ldots, 4\), be any prime of \(H(\zeta)\) above \(p_i\), where \(\zeta\) is a primitive cube root of unity. It is easy to prove that we may take

\[
\frac{b}{2} + \frac{b^2}{4} - \frac{a^3}{27} \quad \text{with} \quad a = 3 - 13 \quad \text{and} \quad b = 2 - 13 - 17\] as an element \(a\) of \(H(\zeta)\) such that \(K(\zeta) = K(\sqrt[3]{\alpha})\). We also note that \(H_1(K) = H_1(\zeta)\) since \(K(\zeta) = K(\sqrt[3]{\alpha})\) and \(H(\zeta)\) is not a norm of any element of \(K\). An elementary calculation shows that

\[
\left(\frac{7, 14, \alpha}{\mathfrak{P}_3}\right) = \left(\frac{7, 14, \alpha}{\mathfrak{P}_2}\right) = \left(\frac{7, 2, \alpha}{\mathfrak{P}_1}\right) = \left(\frac{2, \alpha}{\mathfrak{P}_1}\right)^{-1} \neq 1,
\]

which implies that rank \((a_d) = 2\), and that the unique prime \(\mathfrak{P}_1^{14}\) of \(L\) above \(\sqrt[3]{7}\) is non-principal. These results, Corollary 1.5, Lemma 1.6, and the remark following this lemma combine to show that \(H(L) = H_1(L) = \langle\mathfrak{c}_L(\mathfrak{P}_1^{13}), \mathfrak{c}_L(\mathfrak{P}_2)\rangle\), which is cyclic of order 3, and that \(H(K) = H_1(K) = \langle\mathfrak{c}_L(\mathfrak{P}_1), \mathfrak{c}_L(\mathfrak{P}_2)\rangle\), which is an elementary abelian 3-group of rank 2, where \(\mathfrak{c}_L(\mathfrak{P}_i)\) denotes the ideal class of an ideal \(\mathfrak{P}_i\) of a number field \(F\).

We conclude this section with a remark concerning Lemma 1.6. The proof of this lemma shows that \(H(L) = H_1(L)\) if and only if rank \(H(L) = \gamma_1 - r_1\). Clearly \(H(L) = H_1(L)\) implies that \(H(L) = H_1(L)\); but the converse is not always true. For example, let \(L = Q(\sqrt[3]{182})\) and \(K = Q(\zeta, \sqrt[3]{182})\), where \(\zeta\) is a primitive cube root of unity. It is proved in [4], Section 3, that \(H(L) = H_1(L)\), but that \(H(K) = H_1(K)\). In this example the four numbers \(r_2, r_1, r_3, r_4\) that appear in Theorem 1.4 are as follows: \(r_2 = 5, r_1 = 4, r_3 = 3, r_4 = 1\).

References

Добавление к работе: „Об одной теореме Харди–Литтлвуда в теории дзета-функции Римана”

Acta Arith. 31 (1976), стр. 45–51

Ян Мохер (Братислава)

1. Харди и Литтлвуд ([1], 177–184) доказали следующую теорему: оператор

$$
\frac{1}{2} + iT, \quad \frac{1}{2} + iT + T^{1/2 + \epsilon}, \quad T \geq T_0(\epsilon),
$$

содержит нечетный нуль функции $\zeta(s)$. При этом, метод предложенный упоминавшимися учеными оставил открытым вопрос о влиянии гипотезы Линделяфа на расстояния нечетных нулей функции $\zeta(\frac{1}{2} + it)$.

В этом направлении показано, что имеет место

Теорема. Если справедлива гипотеза Линделяфа, то оператор

$$
\frac{1}{2} + iT, \quad \frac{1}{2} + iT + T^{1/2 + \epsilon}, \quad T \geq T_0(\epsilon),
$$

содержит нечетный нуль функции $\zeta(s)$.

Пусть

$$
S(a, b) = \sum_{\|n\| < b} \frac{e^{2\pi i an}}{n}, \quad b \leq \sqrt{\frac{1}{2\pi}},
$$

(ср. [3], стр. 33, 34) обозначает элементарную тригонометрическую сумму. В работе [4] мы показали, что при условии

$$
|S(a, b)| < A(d)t^{\Theta d}, \quad 0 < \Theta < \frac{1}{2},
$$

отреко

$$
\frac{1}{2} + iT, \quad \frac{1}{2} + iT + T^{1/2 + \epsilon} \psi(T), \quad T \geq T_0(\epsilon, \psi),
$$

содержит нечетный нуль функции $\zeta(s)$ ($\psi(T)$ —сколько медленно возрастает к $+\infty$ функция).

Гипотеза Линделяфа ([5], стр. 97, 333) запрашивает в том, что

$$
|\zeta(\frac{1}{2} + it)| < A(\epsilon)t^\Theta, \quad t \geq T_0(\epsilon),
$$

для любого $\epsilon > 0$. Далее напомним (см. [2], стр. 89), что для


- K. Iimura, Dihedral extensions of $Q$ of degree $2l$ which contain non-Galois extensions with class number not divisible by $l$, Acta Arith., this volume, pp. 385–394.

Received on 18. 3. 1977

(924)