References

[1] T. Callahan, *Dihedral field extensions of order 2p whose class numbers are multiples of p*, Canad. J. Math. 28 (1976), pp. 429–439.
[2] F. Gerth, *On 3-class groups of pure cubic fields*, J. Reine Angew. Math. 278/279 (1975), pp. 52–62.
[3] — *Cubic fields whose class numbers are not divisible by* 3, Illinois J. Math. 20 (1976), pp. 486–493.
[4] G. Gras, *Sur les l-classes d'ideaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier 23, 3 (1973), pp. 1–48.
[5] — *Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l à clôture galoisiennes diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), pp. 677–685.
[6] S. Kobayashi, *On the l-class rank in some algebraic number fields*, J. Math. Soc. Japan 26 (1974), pp. 668–676.
[7] J. Martinet, *Sur l'arithmétique des extensions Galoisiennes à groupe de Galois diédral d'ordre 2p*, Ann. Inst. Fourier 19, 1 (1969), pp. 1–80.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
2-1-1 Fukazawa, Setagaya-ku
Tokyo, Japan

Received on 18. 3. 1977 (923)

ACTA ARITHMETICA
XXXV (1979)

On 3-class groups of non-Galois cubic fields

by

KIYOAKI IIMURA (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 $(x^\sigma)^\tau = x^{\sigma\tau}$. The cubic Hilbert symbol $\left(\frac{a, b}{\mathfrak{p}}\right)$ used here corresponds to $(a, b)_{\mathfrak{p}}$ 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 σ be a generator of the Galois group $G(K/k)$, and let τ be the generator of $G(K/L)$. Then $G(K/Q)$ is generated by $\{\sigma, \tau\}$ with the relations $\sigma^3 = \tau^2 = 1$, $\sigma\tau = \tau\sigma^2$. 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

$$H_i(K) = \{h \in H(K) \mid h^{(\sigma-1)^i} = 1\}$$

and

$$H_i(L) = \{h \in H_i(K) \mid h^\tau = h\}.$$

Then $H_i(K)$ is a subgroup of $H(K)$ and is a $\mathbf{Z}[G(K/Q)]$-module; $H_i(L)$ is a subgroup of $H(L)$ and $H_i(L) = H_i(K)^{1+\tau}$; $H_i(K) = H(K)$ 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 $H(L) = H(K)^{1+\tau}$ and $H(Q) = \{1\}$.

Now we let H be a maximal direct summand of $H(L)$ contained in

$$H_1(L) = \{h \in H(K) \mid h^\sigma = h^\tau = h\}.$$

Since $H_1(L)$ is an elementary abelian 3-group, then

$$H\times\big(H(L)^3\cap H_1(L)\big)=H_1(L). \tag{1.1}$$

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. $H(L)^3\cap H_1(L)=H_3(L)^{(\sigma-1)^2}$.

Proof. We first show that $H(L)^3\cap H_1(L)=H_3(L)^{(\sigma-1)^2}\cap H_1(L)$. Let $h\in H(L)^3\cap H_1(L)$; i.e. $h=h_1^3$ with $h_1\in H(L)$. Then

$$h_1^{(\sigma-1)^2}=h_1^{1+\sigma+\sigma^2-3\sigma}=h_1^{-3\sigma}=h^{-\sigma}=h^{-1}$$

since $h_1^{1+\sigma+\sigma^2}\in N\big(H(L)\big)=\{1\}$ and $h^\sigma=h$. Also $h_1^{(\sigma-1)^3}=1$, which implies that $h_1\in H_3(L)$. So $h=h_1^{-(\sigma-1)^2}\in H_3(L)^{(\sigma-1)^2}$. Next let $h\in H_3(L)^{(\sigma-1)^2}\cap\cap H_1(L)$; i.e. $h=h_2^{(\sigma-1)^2}$ with $h_2\in H_3(L)$. Then $h=h_2^{(\sigma-1)^2}=h_2^{-3\sigma}$ since $h_2^{1+\sigma+\sigma^2}=1$. So $h_2^{-3}=h^{\sigma^2}=h$, and hence $h\in H(L)^3$. We next show that $H_3(L)^{(\sigma-1)^2}\subset H_1(L)$. Let $h\in H_3(L)$. Then

$$h^{(\sigma-1)^2}=h^{-3\sigma}=h^{-3}\in H_1(K)\cap H_3(L)=H_1(L)$$

since $h^{1+\sigma+\sigma^2}=1$ and $h^{(\sigma-1)^2}\in H_1(K)$. This proves the lemma.

LEMMA 1.2. *There is an exact sequence*

$$1\to H_2(L)\to H_3(L)\xrightarrow{(\sigma-1)^2}H_3(L)^{(\sigma-1)^2}\to 1.$$

Proof. The proof is immediate from the fact that $H_2(K)\cap H_3(L)=H_2(L)$.

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

$$V_i=\langle H_i(L),H_{i-1}(K)\rangle\quad\textit{and}\quad\tilde V_i=\{h\in H(K)|\ h^{\sigma-1}\in V_i\}.$$

Then

$$|H_{i+1}(K)/H_{i+1}(L)|=|\tilde V_i/V_i|\cdot|H_i(K)/H_i(L)|.$$

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

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

$$\begin{aligned}|H|&=|H_1(L)|/|H(L)^3\cap H_1(L)|\quad\text{(by (1.1))}\\&=|H_1(L)|/|H_3(L)^{(\sigma-1)^2}|\quad\text{(by Lemma 1.1)}\\&=|H_1(L)|\,|H_2(L)|/|H_3(L)|\quad\text{(by Lemma 1.2)}\\&=|H_2(L)|\,|H_1(K)|\,|\tilde V_2/V_2|/|H_3(K)|\quad\text{(by Lemma 1.3)}\\&=|H_2(K)/H_2(L)|^{-1}|H_1(K)|\,|\tilde V_2/V_2|\,|H_3(K)/H_2(K)|^{-1}\\&=|H_1(K)|\,|H_3(K)/H_2(K)|^{-1}|\tilde V_2/V_2|\,|\tilde V_1/V_1|^{-1}\ \text{(by Lemma 1.3)}.\end{aligned}\tag{1.2}$$

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):

$$\begin{aligned}|H_1(K)|&=3^{t-1-r_1}|H(k)|,\\|H_3(K)/H_2(K)|&=3^{t-1-r_3}\big|H(k)/N\big(H_2(K)\big)\big|,\\|\tilde V_2/V_2|&=3^{t-1-\bar r_2}\big|H(k)/N\big(H_1(K)\big)\big|,\\|\tilde V_1/V_1|&=3^{t-1-\bar r_1}|H(k)|,\end{aligned}$$

where t is the number of primes of k which ramify in K, and $r_1,r_3,\bar r_2,\bar r_1$ are all nonnegative rational integers, which are in fact defined to be the ranks of certain matrices (over the finite field $\boldsymbol{F}_3$ of 3 elements) associated with the groups $H_0(K)=\{1\}$, $H_2(K)$, V_2, V_1, respectively. We note that $0\leqslant r_1\leqslant\bar r_1\leqslant\bar r_2\leqslant r_3\leqslant\max(0,t-1)$. Using these equations, equation (1.2) becomes

$$|H|=3^{r_3-\bar r_2+\bar r_1-r_1}\big|N\big(H_2(K)\big)/N\big(H_1(K)\big)\big|.$$

Letting $\big|N\big(H_2(K)\big)/N\big(H_1(K)\big)\big|=3^u$ we obtain the following result.

THEOREM 1.4. *With the above notations,*

$$\operatorname{rank}H=r_3-\bar r_2+\bar r_1-r_1+u.$$

COROLLARY 1.5. *$H(L)$ has an elementary abelian direct factor of rank $r_3-\bar r_2+\bar r_1-r_1+u$ contained in $H_1(L)$.*

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* $\operatorname{rank}H(L)=\bar r_1-r_1$, *then* $H(K)=H_1(K)$, *and hence* $H(L)=H_1(L)$, *which is an elementary abelian 3-group.*

Remark. Let ${}_NH_1(K)=\{h\in H_1(K)|\ N(h)=1\}$. Then ${}_NH_1(K)$ is an elementary abelian 3-group of rank $t-1-r_1+\operatorname{rank}H(k)-z$, where z is the rank of a certain subgroup of $H(k)/H(k)^3$ (cf. [2], Proposition 3.2). So

$$\operatorname{rank}H_1(K)\geqslant t-1-r_1+\operatorname{rank}H(k)-z.$$

Note that if $H(k)=\{1\}$, then $H_1(K)$ is an elementary abelian 3-group of rank $t-1-r_1$ (since ${}_NH_1(K)=H_1(K)$).

Proof. It is clear that $(\sigma-1)^i$ maps $H_{i+2}(K)/H_{i+1}(K)$ injectively into $H_2(K)/H_1(K)$ for all integers $i\geqslant 0$. So to show that $H(K)=H_1(K)$, it suffices to show that $|H_2(K)/H_1(K)|=1$. Now

$$\begin{aligned}|H_2(K)/H_1(K)|&=|H_2(K)/H_2(L)|\,|H_1(K)|^{-1}|H_2(L)|\\&=|\tilde V_1/V_1|\,|H_1(K)|^{-1}|H_2(L)|\quad\text{(by Lemma 1.3)}\\&=3^{r_1-\bar r_1}|H_2(L)|.\end{aligned}$$

It is easy to see that $H_2(L)=\{h\in H(L)|\ h^3=1\}$; hence $|H_2(L)|=3^{\operatorname{rank}H(K)}$. The lemma is now immediate.

Now we want to describe explicitly a matrix over $\boldsymbol{F}_3$ whose rank is exactly $\bar r_1-r_1$. Let $\mathfrak{p}_1,\ldots,\mathfrak{p}_t$ be the primes of k which ramify in K, let $\mathfrak{P}_i$

be the unique prime of K above $\mathfrak{p}_i$, and let $\bar{\mathfrak{P}}_i$ be any prime of $k(\zeta)$ above $\mathfrak{p}_i$, where ζ is a primitive cube root of unity. Let a be an element of $k(\zeta)$ such that $K(\zeta) = k(\zeta, \sqrt[3]{a})$. Furthermore let $p_1, \ldots, p_s$ 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 $\bar{\mathfrak{P}}_i$'s and by the image in $H(K)$ of $H(k)$, 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 $\mathfrak{A}$ 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 $N(\mathfrak{A}) = (p_{s+1})$ when $H_1(K) \neq H_1'(K)$, and let $p_{s+1} = 1$ when $H_1(K) = H_1'(K)$. Then

$$\bar{r}_1 - r_1 = \operatorname{rank}(a_{ij}) \quad (1 \leqslant i \leqslant s+1,\ 1 \leqslant j \leqslant t),$$

where a_{ij} is an element of the finite field $\boldsymbol{F}_3$ given by

$$\zeta^{a_{ij}} = \left(\frac{p_i, a}{\bar{\mathfrak{P}}_j}\right) \quad (1 \leqslant i \leqslant s+1,\ 1 \leqslant j \leqslant t). \tag{1.3}$$

We note that if $\mathfrak{p}_j$ is not decomposed over $\boldsymbol{Q}$, then $\left(\frac{p_j, a}{\bar{\mathfrak{P}}_j}\right) = 1$ for any p_i (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 $m = \operatorname{rank} G$. Let $p_1, \ldots, p_m, q$ be rational primes satisfying the following conditions:

(i) $p_i \equiv 1 \pmod 9$ for $1 \leqslant i \leqslant m$, $q \equiv 2 \pmod 9$;

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

(iii) $p_1 \ldots p_{i-1} q$ 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 choosen from a congruence modulo $9p_1 \ldots p_{i-1}$ (resp. $9p_1 \ldots p_m$), with coefficients in $\boldsymbol{Z}$. Now let $n = p_1 \ldots p_m q$ and $L = \boldsymbol{Q}(\sqrt[3]{n})$. Note that the normal closure K of L is $\boldsymbol{Q}(\zeta, \sqrt[3]{n})$, where ζ is a primitive cube root of unity. We want to show that $H(L)$ is an elementary abelian 3-group of rank m. Using [1], Theorem 4.5, and assumption (i), it is easy to compute that

$$\operatorname{rank} H(L) = 2m - \operatorname{rank}(\gamma_{ij}),$$

where (γ_{ij}) is the $m \times m$ matrix (over $\boldsymbol{F}_3$) whose ij-th element γ_{ij} satisfies

$$\zeta^{\gamma_{ij}} = \left(\frac{p_i, n}{\mathfrak{p}_j}\right),$$

where $\mathfrak{p}_j$ is any prime of $\boldsymbol{Q}(\zeta)$ above p_j. For $1 \leqslant i < j \leqslant m$, we have from assumption (ii) that

$$\zeta^{\gamma_{ij}} = \left(\frac{p_i, n}{\mathfrak{p}_j}\right) = \left(\frac{p_i, p_j}{\mathfrak{p}_j}\right) = \left(\frac{p_i}{\mathfrak{p}_j}\right)_3 = 1,$$

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

$$\zeta^{\gamma_{ii}} = \left(\frac{p_i, n}{\mathfrak{p}_i}\right) = \left(\frac{p_i, p_1 \cdots p_{i-1} q}{\mathfrak{p}_i}\right) = \left(\frac{p_1 \cdots p_{i-1} q}{\mathfrak{p}_i}\right)_3^{-1} \neq 1.$$

So $\operatorname{rank}(\gamma_{ij}) = m$, and hence $\operatorname{rank} H(L) = m$. In view of the definitions of the two matrices (γ_{ij}) and (a_{ij}), where (a_{ij}) is defined by equation (1.3), it is clear that

$$\operatorname{rank}(\gamma_{ij}) \leqslant \operatorname{rank}(a_{ij}) = \bar{r}_1 - r_1.$$

Combining these and Corollary 1.5 we know that $\operatorname{rank} H(L) = \bar{r}_1 - r_1$, 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 stetement 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 $\operatorname{rank} G$ is even. So assume that $\operatorname{rank} G = 2m-1$. 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) $p_i \equiv 1 \pmod 9$ for $1 \leqslant i \leqslant m-1$, $p_m \equiv 4 \pmod 9$, $q \equiv 2 \pmod 9$.

Again Dirichlet's theorem shows that there exist infinitely many such primes $p_1, \ldots, p_m, q$. Let $L = \boldsymbol{Q}(\sqrt[3]{n})$, where $n = p_1 \ldots p_m q$, 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

$$\operatorname{rank} H(L) = 2m - 1 - \operatorname{rank}(\gamma_{ij}),$$

where (γ_{ij}) is the $(m-1)\times m$ matrix whose ij-th element γ_{ij} satisfies

$$\zeta^{\gamma_{ij}} = \left(\frac{p_i\,,\,n}{\mathfrak{p}_j}\right),$$

where $\mathfrak{p}_j$ for each $j=1,\ldots,m-1$, is any prime of $\boldsymbol{Q}(\zeta)$ above p_j. The same argument as in the proof of Theorem 2.1 shows that rank $(\gamma_{ij}) = m-1$, rank $H(L) = m$, and rank $(a_{ij}) = \bar{r}_1 - r_1 \geqslant m$. 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 $x^3-3\cdot 13x+2\cdot 13\cdot 17 = 0$ to Q. Then rank $H(L) = 2$; $k = \boldsymbol{Q}(\sqrt{-23})$ 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 $(a_{ij}) = 2$. To see this, we let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ (resp. $\mathfrak{p}_3$ and $\mathfrak{p}_4$) be distinct primes of k above 13 (resp. 3), and let $\overline{\mathfrak{P}}_i$ for each $i = 1,\ldots,4$, be any prime of $k(\zeta)$ above $\mathfrak{p}_i$, where ζ is a primitive cube root of unity. It is easy to prove that we may take $-\dfrac{b}{2}+\left(\dfrac{b^2}{4}-\dfrac{a^3}{27}\right)^{1/2}$ with $a = 3\cdot 13$ and $b = 2\cdot 13\cdot 17$ as an element α of $k(\zeta)$ such that $K(\zeta) = k(\zeta, \sqrt[3]{\alpha})$. We also note that $H_1(K) = H_1'(K)$ since k is complex and is not $\boldsymbol{Q}(\zeta)$ (cf. [3], p. 28). Then for each $j = 1,\ldots,4$, $\zeta^{a_{1j}} = \left(\dfrac{13,\,\alpha}{\overline{\mathfrak{P}}_j}\right)$ and $\zeta^{a_{2j}} = \left(\dfrac{3,\,\alpha}{\overline{\mathfrak{P}}_j}\right)$. Using the results in [2], Section 4, it is easy to compute that

$$\zeta^{a_{11}} = \left(\frac{13,\,13}{\overline{\mathfrak{P}}_1}\right) = 1, \qquad \zeta^{a_{21}} = \left(\frac{3,\,13}{\overline{\mathfrak{P}}_1}\right) = \left(\frac{3}{\overline{\mathfrak{P}}_1}\right)_3 \neq 1,$$

$$\zeta^{a_{13}} = \left(\frac{13,\,\eta_1\eta_3^2}{\overline{\mathfrak{P}}_3}\right) = \left(\frac{13,\,\zeta}{\overline{\mathfrak{P}}_3}\right) \neq 1,$$

where $\eta_1 = 1-(1-\zeta)$ and $\eta_3 = 1-(1-\zeta)^3$ (cf. [3], Proposition 3.3). So rank $(a_{ij}) = 2$, and hence $H(L) = H_1(L)$, which is generated by $\mathrm{cl}_L(\mathfrak{P}_1)$ and $\mathrm{cl}_L(\mathfrak{P}_3)$, where $\mathfrak{P}_1$ (resp. $\mathfrak{P}_3$) is the unique prime of L above 13 (resp. 3), and $\mathrm{cl}_L(\mathfrak{P}_i)$ for $i = 1, 3$, denotes the ideal class of $\mathfrak{P}_i$ in $H(L)$. Furthermore $H(K) = H_1(K)$, which has order $|H_1(K)| = 3^{4-1-0}|H(k)| = 3^4$. Also it is proved in [2], Section 4, that rank ${}_NH_1(K) = 3$, where ${}_NH_1(K)$ is the subgroup of $H_1(K)$ given in the remark following Lemma 1.6. It follows from these that $H(K)$ is either an elementary abelian 3-group of rank 4, or the direct product of an elementary abelian 3-group of rank 2 and a cyclic group of order 9. For another example we let L be a cubic extension of Q obtained by adjoining a root of $x^3-2\cdot 5\cdot 7x+2\cdot 3\cdot 5\cdot 7 = 0$ to Q. Then rank $H(L) = 1$; $k = \boldsymbol{Q}(\sqrt{37})$ and $H(k) = \{1\}$. The rational primes which ramify fully in L are 2, 5, and 7. In k, 2 and 5 remain prime, and 7 decomposes. Now let $\overline{\mathfrak{P}}$ be any prime of $k(\zeta)$ above 7, where ζ is a primitive cube root of unity, let $\mathfrak{P}$ be any prime of K above 7, and let $\alpha = -\dfrac{b}{2}+\left(\dfrac{b^2}{4}-\dfrac{a^3}{27}\right)^{1/2}$ with $a = 2\cdot 5\cdot 7$ and $b = 2\cdot 3\cdot 5\cdot 7$. Then $K(\zeta) = k(\zeta, \sqrt[3]{\alpha})$. Note that $H_1(K) = H_1'(K)$ since a unit $6+\sqrt{37}$ of k is not a norm of any element of K (cf. [2], Section 4, and [3], p. 28). An elementary calculation shows that

$$\left(\frac{7,\,\alpha}{\overline{\mathfrak{P}}}\right) = \left(\frac{7,\,14}{\overline{\mathfrak{P}}}\right) = \left(\frac{7,\,2}{\overline{\mathfrak{P}}}\right) = \left(\frac{2}{\overline{\mathfrak{P}}}\right)_3^{-1} \neq 1,$$

which implies that rank $(a_{ij}) \geqslant 1$, and that the unique prime $\mathfrak{P}^{1+\tau}$ of L above 7 is non-principal. These results, Corollary 1.5, Lemma 1.6, and the remark following this lemma combine to show that $H(L) = H_1(L) = \langle \mathrm{cl}_L(\mathfrak{P}^{1+\tau})\rangle$, which is cyclic of order 3, and that $H(K) = H_1(K) = \langle \mathrm{cl}_K(\mathfrak{P}), \mathrm{cl}_K(\mathfrak{P}^{\tau})\rangle$, which is an elementary abelian 3-group of rank 2, where $\mathrm{cl}_F(\mathfrak{A})$ denotes the ideal class of an ideal $\mathfrak{A}$ of a number field F.

We conclude this section with a remark concerning Lemma 1.6. The proof of this lemma shows that $H(K) = H_1(K)$ if and only if rank $H(L) = \bar{r}_1 - r_1$. Clearly $H(K) = H_1(K)$ implies that $H(L) = H_1(L)$; but the converse is not always true. For example, let $L = \boldsymbol{Q}(\sqrt[3]{182})$ and $K = \boldsymbol{Q}(\zeta, \sqrt[3]{182})$, where ζ is a primitive cube root of unity. It is proved in [4], Section 3, that $H(L) = H_1(L)$, but that $H(K) = H_2(K) \neq H_1(K)$. In this example the four numbers $r_3, \bar{r}_2, \bar{r}_1, r_1$ that appear in Theorem 1.4 are as follows: $r_3 = 5$, $\bar{r}_2 = 4$, $\bar{r}_1 = 3$, $r_1 = 1$.

References

[1] F. Gerth, *On 3-class groups of pure cubic fields*, J. Reine Angew. Math. 278/279 (1975), pp. 52–62.

[2] — *Ranks of 3-class groups of non Galois cubic fields*, Acta Arith. 30 (1976), pp. 307–322.

[3] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier 23, 3 (1973), pp. 1–48.
[4] — *Sur les l-classes d'idéaux des extensions non galoisiennes de Q de degré premier impair l à clôture galoisiennes diédrale de degré 2l*, J. Math. Soc. Japan 26 (1974), pp. 677–685.
[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Wurzburg/Wien 1970.
[6] 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.
[7] S. Kobayashi, *On the l-class rank in some algebraic number fields*, J. Math. Soc. Japan 26 (1974), pp. 668–676.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
2–1–1 Fukazawa, Setagaya-ku
Tokyo, Japan

Received on 18. 3. 1977 (924)

ACTA ARITHMETICA
XXXV (1979)

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

Acta Arith. 31 (1976), стр. 45–51

Ян Мозер (Братислава)

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

$$\tfrac{1}{2}+iT,\ \tfrac{1}{2}+i(T+T^{1/4+\varepsilon}),\quad T\geqslant T_0(\varepsilon),$$

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

В этом направлении покажем, что имеет место

Теорема. *Если справедлива гипотеза Линделёфа, то отрезок*

$$\tfrac{1}{2}+iT,\ \tfrac{1}{2}+i(T+T^{1/8+\varepsilon}),\quad T\geqslant T_0(\varepsilon),$$

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

Пусть

(1) $$S(a,b)=\sum_{0<a\leqslant n<b\leqslant 2a} e^{it\ln n},\quad b\leqslant\sqrt{\frac{t}{2\pi}},$$

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

(2) $$|S(a,b)|<A(\Delta)\sqrt{a}\,t^{\Delta},\quad 0<\Delta<\tfrac{1}{4},$$

отрезок

(3) $$\tfrac{1}{2}+iT,\ \tfrac{1}{2}+i\big(T+T^{1/8+\Delta/2}\psi(T)\big),\quad T\geqslant T_0(\Delta,\psi),$$

содержит нечетный нуль функции $\zeta(s)$ ($\psi(T)$ — сколь угодно медленно возрастающая к $+\infty$ функция).

Гипотеза Линделёфа ([5], стр. 97, 323) заключается в том, что

$$|\zeta(\tfrac{1}{2}+it)|<A(\varepsilon)t^{\varepsilon},\quad t\geqslant T_0(\varepsilon),$$

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