and $p_1^*, \ldots, p_n^*$ have binary expansions with maximal length $T-1$. Applying this procedure $(T-1)$ more times we replace $p_1, \ldots, p_n$ with $\varepsilon_1, \ldots, \varepsilon_n \in \{0,1\}$ such that

$$\max_{1\leqslant k\leqslant n}\Big|\sum_{j\leqslant k} a_{ij}(\varepsilon_j - p_j)\Big| \leqslant \sum_{h=1}^{T} 2^{-h}\cdot B_i \leqslant B_i.$$

Finally, if $p_1, \ldots, p_n \in [0,1]$ are arbitrary the existence of $\varepsilon_1, \ldots, \varepsilon_n$ follows by a simple compactness argument. ∎

References

[1] J. Beck, *Balancing families of integer sequences*, Combinatorica 1 (3) (1981), pp. 209–216.

[2] K. F. Roth, *Remark concerning integer sequences*, Acta Arith. 9 (1964), pp. 257–260.

MATHEMATICAL INSTITUTE OF THE HUNGARIAN ACADEMY OF SCIENCES
Budapest, Realtanoda u. 13-15, 1053 Hungary
DEPARTMENT OF MATHEMATICS, SUNY
Stony Brook, N. Y. 11 794, U.S.A.

Received on 14. 9. 1982 (1320)

ACTA ARITHMETICA
XLIII (1984)

On the genus group of algebraic number fields

by

KIYOAKI IIMURA (Tokyo)

Introduction. Let K be a finite extension of the field $\boldsymbol{Q}$ of rational numbers. Call $C(K)$ the ideal class group of K in the narrow sense. Call $\tilde{K}$ the genus field of K, i.e., the maximal abelian extension of K which is composed of K and of an abelian extension of $\boldsymbol{Q}$ and is unramified at all the finite primes of K (cf. [1]). Call $G(K)$ the subgroup of $C(K)$ corresponding to the genus field $\tilde{K}$ in the sense of class field theory; $G(K)$ is called the principal genus of K, and the factor group $C(K)/G(K)$ is called the genus group of K. Call μ the canonical homomorphism of $C(K)$ onto $C(K)/G(K)$. Our aim of the paper is to study the image $\mu(c)$ for an element c of $C(K)$. Particularly it will be shown that if $K/\boldsymbol{Q}$ is of odd prime degree and an irreducible polynomial over $\boldsymbol{Q}$ defining K is given, then the image $\mu(H)$, where H is the subgroup of $C(K)$, generated by the classes of all the prime ideals of K ramifying fully over $\boldsymbol{Q}$, can be known by an elementary and purely rational procedure. As its immediate consequence, a generalization of Theorem 3 in [2] is obtained; this theorem states that if a purely rational condition about the rational primes ramified fully in K is satisfied, then the class number of the pure field $K = \boldsymbol{Q}(\sqrt[l]{m})$ of odd prime degree l is divisible by $l^{t+u-(l+1)/2}$, where t (resp. u) is the number of rational primes (resp. those $\equiv 1 \pmod{l}$) ramified in K.

We conclude this introduction with a remark about conventions. By a prime ideal, we will understand a finite prime ideal. Also $\boldsymbol{Z}$ will be the ring of rational integers.

1. Image $\mu(c)$. Let notations be the same as in the introduction. Call k the maximal abelian extension of $\boldsymbol{Q}$, contained in the genus field $\tilde{K}$ of K; then, by definition, $\tilde{K}$ is the compositum of k and K, and so the restriction map: $G(\tilde{K}/K) \to G(k/\boldsymbol{Q})$ is injective, where $G(L/M)$ is the Galois group of a Galois extension L/M. By means of the Artin map, the genus group $C(K)/G(K)$ is isomorphic to $G(\tilde{K}/K)$. So if we call ν the homomorphism of $C(K)$ to $G(k/\boldsymbol{Q})$ obtained by composing these two maps with μ, the study of the image $\mu(c)$ in question is reduced to that of the image $\nu(c)$ in $G(k/\boldsymbol{Q})$. We will use the following basic facts about the abelian field k, which may be found in [4]. For a rational prime p, call $e(p)$ the greatest common divisor of the ramification indices of all the prime divisors of p in K, and call $\boldsymbol{Q}^{(p^\infty)}$ the field obtained by adjoining to $\boldsymbol{Q}$ all the p^ith roots of unity, $i \geqslant 1$. Call U (resp. V) the set of those p which are ramified in K and satisfy $e(p) \not\equiv 0 \pmod p$ and $d(p) = \gcd(e(p), p-1) \neq 1$ (resp. $e(p) \equiv 0 \pmod p$); then each $p \in V$ divides the degree of $K/\boldsymbol{Q}$, since so does $e(p)$. For each $p \in U$, define

$$k(p) = k \cap \boldsymbol{Q}^{(p^\infty)};$$

by [4], Theorem 3, this equals the unique cyclic extension of $\boldsymbol{Q}$, of degree $d(p)$, contained in the pth cyclotomic field $\boldsymbol{Q}(\zeta_p)$, where ζ_p is a primitive pth root of unity. Call $k(V)$ the intersection of k and of the compositum of all the $\boldsymbol{Q}^{(p^\infty)}$ with $p \in V$. [4], Theorem 3 says also that k is the compositum of $k(V)$ and of the compositum of all the $k(p)$ with $p \in U$:

$$k = k(V) \cdot \prod_{p \in U} k(p);$$

it is clear that

$$k(V) \cap \prod_{p \in U} k(p) = \boldsymbol{Q}.$$

Call W the set of rational primes p ramified in $k(V)$, which is the same as the set of those $p \in V$ ramified in k, and call $k(W)$ the intersection of k and of the compositum of all the $\boldsymbol{Q}^{(p^\infty)}$ with $p \in W$; then $k(W) = k(V)$. From the above it follows that $G(k/\boldsymbol{Q})$ is canonically isomorphic to the direct product

$$G\big(k(W)/\boldsymbol{Q}\big) \times \prod_{p \in U} G\big(k(p)/\boldsymbol{Q}\big);$$

so that the image $\nu(c)$ may be considered in this group. As was mentioned above, for each $p \in U$, $k(p)$ was given explicitly, while, on the other hand, it would be usually difficult to determine $k(W)$ exactly. Some of the cases where $k(W)$ is known are found in [1], [4]–[6]. For our purpose, *from now on, we will assume $k(W)$ has been known*. Now, for the c given, let $\mathfrak{a}$ be an ideal of K contained in c. For each $p \in U$, choose an element $a_p \neq 0$ of K so that the class of (a_p) in $C(K)$ is trivial and $N\mathfrak{a}N(a_p)$ is prime to p, where N is the norm map from K to $\boldsymbol{Q}$; choose an element $a_W \neq 0$ of K so that the class of (a_W) in $C(K)$ is trivial and $N\mathfrak{a}N(a_W)$ is prime to all primes in W. Then, in view of the definition of ν, it follows from the translation theorem in class field theory that

$$\nu(c) = \left(\frac{k(W)}{N\mathfrak{a}N(a_W)}\right) \times \prod_{p \in U} \left(\frac{k(p)}{N\mathfrak{a}N(a_p)}\right), \tag{1}$$

where $\left(\frac{M}{\ }\right)$ is the Artin symbol in an abelian extension $M/\boldsymbol{Q}$. We will call $\left(\frac{k(W)}{N\mathfrak{a}N(a_W)}\right)$ and $\left(\frac{k(p)}{N\mathfrak{a}N(a_p)}\right)$ the W-component and p-component of $\nu(c)$ respectively. So to know $\nu(c)$, it suffices to find these norms $N\mathfrak{a}N(a_W)$ and $N\mathfrak{a}N(a_p)$, $p \in U$. Of course, we may put all these $a = 1$ if $N\mathfrak{a}$ itself is prime to all primes in $U \cup W$.

2. Odd prime degree case. Let all notations be as above. In this section we will assume that $K/\boldsymbol{Q}$ is of odd prime degree l, and also that an irreducible polynomial $f(X)$ over $\boldsymbol{Q}$ defining K has been given. In this case, by definition, U consists of all the rational primes $\equiv 1 \pmod l$ ramified fully in K, and each $k(p)$ is the unique cyclic extension of $\boldsymbol{Q}$, of degree l, contained in the pth cyclotomic field. Also $k(W)$ is either $\boldsymbol{Q}$ or the unique cyclic extension of $\boldsymbol{Q}$, of degree l, contained in the l^2th cyclotomic field according as $W = \emptyset$ (empty) or $W = \{l\}$ (cf. [4], p. 56). In [5], Ishida has found an elementary and purely rational procedure to obtain from the given polynomial $f(X)$ "nice polynomials" which enable one to know immediately whether a given rational prime is ramified fully in K or not and whether $W = \{l\}$ or not. The nice polynomial with respect to a rational prime q ramified fully in K is of the following form:

$$f_q(X) = \sum_{i=0}^{l} d_{i,q} X^{l-i}$$

with coefficients $d_{i,q} \in \boldsymbol{Z}$, $d_{0,q} = 1$, $d_{i,q} \equiv 0 \pmod q$, $1 \leqslant i \leqslant l$, and $d_{l,q} \not\equiv 0 \pmod{q^2}$; furthermore, $W = \{l\}$ if and only if the coefficients $d_{i,l}$ of $f_l(X)$ satisfy the congruence

$$d_{1,l} + d_{l,l} \equiv d_{2,l} \equiv \ldots \equiv d_{l-1,l} \equiv 0 \pmod{l^2}.$$

Now we will fix a rational prime q in $U \cup W$. Call $\mathfrak{q}$ the prime ideal of K lying above q, and $c(\mathfrak{q})$ its class in $C(K)$. We want to calculate the image $\nu\big(c(\mathfrak{q})\big)$ by using the nice polynomial $f_q(X)$. Call π a root of this polynomial; then $N\mathfrak{q}N(\pi^{-1}) = q/|d_{l,q}|$ is prime to q. With the notation of formula (1) in Section 1, let $a_p = 1$ if $p \neq q$, and $a_p = \pi^{-1}$ if $p = q$; let $a_W = 1$ if $q \notin W$, and $a_W = \pi^{-1}$ if $q \in W$, or equivalently, $W \neq \emptyset$ and $q = l$. Then the p-component of $\nu\big(c(\mathfrak{q})\big)$ is equal to

$$\left(\frac{k(p)}{q}\right) \quad \text{or} \quad \left(\frac{k(p)}{q/|d_{l,q}|}\right)$$

according as $p \neq q$ or $p = q$. Also its W-component is equal to

$$\left(\frac{k(W)}{q}\right) \quad \text{or} \quad \left(\frac{k(W)}{l/|d_{l,l}|}\right)$$

according as $q \notin W$ or $q \in W$. For $p \in U$, call X_p the multiplicative group of units in the factor ring $\boldsymbol{Z}/p\boldsymbol{Z}$, and fix a generator x_p for X_p. For each $a \in \boldsymbol{Q}$, prime to p, define an element $\xi_p(a)$ of the finite field $\boldsymbol{F}_l$ of l elements by

$$a^{(p-1)/l} \equiv (x_p^{(p-1)/l})^{\xi_p(a)} \pmod p;$$

then it is easily seen that the mapping

$$\left(\frac{k(p)}{a}\right) \mapsto \xi_p(a)$$

is an isomorphism of $G\big(k(p)/\boldsymbol{Q}\big)$ onto $\boldsymbol{F}_l$, which we will call ι_p. Call $k(l)$ the unique cyclic extension of $\boldsymbol{Q}$, of degree l, contained in the l^2th cyclotomic field, and X_l the multiplicative group of units in the factor ring $\boldsymbol{Z}/l^2\boldsymbol{Z}$. Fixing a generator x_l for X_l, we define, for each $a \in \boldsymbol{Q}$, prime to l, an element $\xi_l(a)$ of $\boldsymbol{F}_l$ by

$$a^{l-1} \equiv (x_l^{l-1})^{\xi_l(a)} \pmod{l^2};$$

then the mapping

$$\left(\frac{k(l)}{a}\right) \mapsto \xi_l(a)$$

also is an isomorphism of $G\big(k(l)/\boldsymbol{Q}\big)$ onto $\boldsymbol{F}_l$, which we will call ι_l. Therefore

$$\iota = \iota_l \times \prod_{p \in U} \iota_p$$

is an isomorphism of $G\big(k(l)/\boldsymbol{Q}\big) \times \prod_{p \in U} G\big(k(p)/\boldsymbol{Q}\big)$ into $\boldsymbol{F}_l^{(u+1)}$, where u is the number of elements of U. As we have already known the image $\nu\big(c(\mathfrak{q})\big)$ with $\mathfrak{q}$ lying above $q \in U \cup W$, the image $\iota \circ \nu\big(c(\mathfrak{q})\big)$ in $\boldsymbol{F}_l^{(u+1)}$ can be immediately calculated.

Now, this time q will be assumed to be a rational prime, not in $U \cup W$, ramified fully in K. Call $\mathfrak{q}$ the prime ideal of K lying above q and $c(\mathfrak{q})$ its class in $C(K)$. Then the p-component and W-component of $\nu\big(c(\mathfrak{q})\big)$ are respectively

$$\left(\frac{k(p)}{q}\right) \quad \text{and} \quad \left(\frac{k(W)}{q}\right),$$

so that $\iota \circ \nu\big(c(\mathfrak{q})\big)$ also can be calculated. Calling H the subgroup of $C(K)$, generated by the classes $c(\mathfrak{q})$ of all the prime ideals $\mathfrak{q}$ ramifying fully over $\boldsymbol{Q}$, we have obtained the following

THEOREM. *Let notations and assumptions be as above. Then both images $\nu(H)$ and $\iota \circ \nu(H)$ can be calculated in the way given above.*

COROLLARY. *Call t the number of rational primes ramified fully in K, call r the number of infinite primes of K, and let $z = \max\{0, t-r\}$ or $z = \max\{0, t+1-r\}$ according to whether or not K is a pure field, i.e., $K = \boldsymbol{Q}(\sqrt[l]{m})$ with $m \in \boldsymbol{Q}$. Call s the number of elements of $U \cup W$, and let $s' = s-1$ or $s' = s$ according to whether or not $K/\boldsymbol{Q}$ is cyclic. Furthermore call d the dimension of the image $\iota \circ \nu(H)$ as a vector space over $\boldsymbol{F}_l$. Then the class number of K is divisible by $l^{z+s'-d}$, and the dimension d can be calculated in the way given above.*

Proof. For a finite group Δ, let $|\Delta|$ denote its order. By definition, H is elementary abelian; it is shown in [4], Chapter 2, and [7], that $|H|$ is a multiple of l^z. From an exact sequence

$$1 \to H \cap G(K) \to H \xrightarrow{\mu} \mu(H) \to 1$$

and from the fact that $\mu(H)$ is isomorphic to $\nu(H)$ hence to $\iota \circ \nu(H)$, it follows that $|H \cap G(K)| = |H| l^{-d}$; this is a multiple of l^{z-d}. Also $|C(K)/G(K)| = |G(k/k \cap K)|$, which is known to be $l^{s'}$ (cf. [4], Theorem 5). Therefore $|C(K)| = |C(K)/G(K)|\,|G(K)|$ is a multiple of $l^{s'+z-d}$, which was to be shown.

To illustrate this corollary we will consider a pure field K of odd prime degree l; in this case it is known that W is empty (cf. [1] and [4]). In what follows we will fix an lth power free natural number m for which $K = \boldsymbol{Q}(\sqrt[l]{m})$. Call T the set of rational primes ramified fully in K; this consists of all the prime factors of m or of those and l according to whether or not $m^{l-1} \equiv 1 \pmod{l^2}$, so that U consists of all the prime factors $\equiv 1 \pmod l$ of m. For $q \in T$, call as before $\mathfrak{q}$ the prime ideal of K lying above q and $c(\mathfrak{q})$ its class in $C(K)$. For each $q \in T$ but $\notin U$ and for each $p \in U$, $\iota_p \circ \nu\big(c(\mathfrak{q})\big)$, by definition, is given by

$$q^{(p-1)/l} \equiv (x_p^{(p-1)/l})^{\iota_p \circ \nu(c(\mathfrak{q}))} \pmod p, \tag{2}$$

x_p being, as before, the fixed generator for X_p. For $q \in U$, call $a(q)$ the exponent of the q-part of m; i.e., $a(q)$ is such that $m \equiv 0 \pmod{q^{a(q)}}$ but $m \not\equiv 0 \pmod{q^{a(q)+1}}$. Since m is assumed to be lth power free, each $a(q)$ is prime to l (in fact, $1 \leqslant a(q) \leqslant l-1$). So choosing $g(q) > 0$, $h(q)$ in $\boldsymbol{Z}$ so that $a(q)g(q) - lh(q) = 1$, we have the nice polynomial with respect to q:

$$f_q(X) = X^l - m^{g(q)}/q^{lh(q)};$$

so that $d_{l,q} = -m^{g(q)}/q^{lh(q)}$ and $q/|d_{l,q}| = q^{1+lh(q)}/m^{g(q)}$. Therefore $\iota_q \circ \nu\big(c(\mathfrak{q})\big)$ is given by

$$(q^{1+lh(q)}/m^{g(q)})^{(q-1)/l} \equiv (x_q^{(q-1)/l})^{\iota_q \circ \nu(c(\mathfrak{q}))} \pmod q.$$

Also, for $p \in U$ with $p \neq q$, $\iota_p \circ \nu(c(\mathfrak{q}))$ is given by

$$q^{(p-1)/l} \equiv (x_p^{(p-1)/l})^{\iota_p \circ \nu(c(\mathfrak{q}))} \pmod p.$$

For a finite set $\mathscr{F}$ of ideals of K whose classes in $C(K)$ generate H, we let

$$\mathscr{M}(\mathscr{F}) = \left(\iota_p \circ \nu(c(\mathfrak{a}))\right), \quad p \in U, \ \mathfrak{a} \in \mathscr{F},$$

be a $u \times f$ matrix with components $\iota_p \circ \nu(c(\mathfrak{q}))$ in $\boldsymbol{F}_l$, where $c(\mathfrak{a})$ is the class of $\mathfrak{a}$ in $C(K)$, and u (resp. f) is the number of elements of U (resp. $\mathscr{F}$). Clearly the rank of $\mathscr{M}(\mathscr{F})$ is the dimension d of the space $\iota \circ \nu(H)$. From what we have obtained above, $\mathscr{M}(\mathscr{F}_0)$ in which

$$\mathscr{F}_0 = \{\mathfrak{q};\ \mathfrak{q}^l = (q) \text{ with } q \in T\}$$

can be calculated at once; note that this involves the integers $g(q)$ and $h(q)$. But, as will be shown below, $\mathscr{M}(\mathscr{F}_1)$ in which

$$\mathscr{F}_1 = \{\mathfrak{q};\ \mathfrak{q}^l = (q) \text{ with } q \in T \text{ but } \notin U\} \cup \{\mathfrak{q}^{-a(q)};\ \mathfrak{q}^l = (q) \text{ with } q \in U\}$$

involves them no longer, and further is of simpler form. For $q \in U$, we have $N(\mathfrak{q}^{-a(q)}(\sqrt[l]{m})) = q^{-a(q)}m$; this is prime to q; so that $\iota_q \circ \nu(c(\mathfrak{q}^{-a(q)}))$ satisfies

$$(q^{-a(q)}m)^{(q-1)/l} \equiv (x_q^{(q-1)/l})^{\iota_q \circ \nu(c(\mathfrak{q}^{-a(q)}))} \pmod q. \tag{3}$$

Also, for each $p \in U$ with $p \neq q$, $\iota_p \circ \nu(c(\mathfrak{q}^{-a(q)}))$ is the same as $\iota_p \circ \nu(c(\mathfrak{q}^{l-a(q)}))$, and so satisfies

$$(q^{l-a(q)})^{(p-1)/l} \equiv (x_p^{(p-1)/l})^{\iota_p \circ \nu(c(\mathfrak{q}^{-a(q)}))} \pmod p. \tag{4}$$

Now, with the notation of our corollary $z = \max\{0, t-(l+1)/2\}$, and $s = u$, which is the number of prime factors $\equiv 1 \pmod l$ of m; so that the corollary then says that the class number of the pure field $K = \boldsymbol{Q}(\sqrt[l]{m})$ is divisible by l^{z+u-d}, where d is the rank of the matrix $\mathscr{M}(\mathscr{F}_1)$ with components given explicitly by equations (2)–(4). Particularly it is clear that $d = 0$ if and only if for each $q \in T$ and for each $p \in U$ with $p \neq q$, q is lth power residue modulo p; this gives an alternative proof of Theorem 3 in [2] (see also Theorem 3.6 in [8]).

We conclude this section with a remark about the dimension d of the $\boldsymbol{F}_l$-space $\iota \circ \nu(H)$ in the pure field case. As is easily seen from [8], § 2, d equals the rank of the $u \times t$ matrix

$$(\beta(p, q)), \quad p \in U, \ q \in T$$

with components $\beta(p, q)$ in $\boldsymbol{F}_l$ defined by

$$\zeta_l^{\beta(p,q)} = (\sqrt[l]{m})^{(q, L/F)_\mathfrak{p} - 1}.$$

Here ζ_l is a primitive lth root of unity; $F = \boldsymbol{Q}(\zeta_l)$, the lth cyclotomic field; $L = F(\sqrt[l]{m})$, a Kummer extension of F, of degree l; $\mathfrak{p}$ is a prime ideal of F lying above p; $(\ ,L/F)_\mathfrak{p}$ is the norm residue symbol for L/F at $\mathfrak{p}$. With the notation of [3], Teil II, § 13, we have

$$\zeta_l^{\beta(p,q)} = \left(\frac{q, m}{\mathfrak{p}}\right);$$

the symbol $\left(\frac{\ ,\ }{\ }\right)$ is called the lth Hilbert (norm residue) symbol. By virtue of basic properties of this symbol, one can easily see that for every $p \in U$, there is an element $\gamma_p \neq 0$ of $\boldsymbol{F}_l$ such that $\beta(p, q) = \gamma_p \circ \iota_p \circ \nu(c(\mathfrak{q}))$ for all $q \in T$ (cf. [8], § 3).

3. Pure field of prime power degree. Let notations be the same as in Section 1. In this section K will be a pure field $\boldsymbol{Q}(\sqrt[l^n]{m})$ of degree l^n, where l is a prime number, n is a natural number, and m is an l^nth power free rational integer. Call P the set of rational prime factors of m and T the set of rational primes ramified in K; then T is either P or $P \cup \{l\}$. For $q \in P$, call $a(q)$ the exponent of the q-part of m and call $b(q)$ the exponent of the q-part of $a(q)$. Then it is easy to see that if $q \neq l$, $e(q)$ defined in Section 1 is $l^{n-b(q)}$ (cf. [6], p. 219). By definition, U consists of all the primes $\equiv 1 \pmod l$ in P, and W is either empty or $\{l\}$; the latter case occurs only when $l \in T$. As to the field $k(W)$, its complete determination has been done in [6] under the condition that every $b(q)$, $q \in P$, is 0 or $l \notin P$; this says that particularly if $l \neq 2$, $k(W) = \boldsymbol{Q}$. But, most of other cases are still open. For each $q \in T$, by the definition of $e(q)$, $(q)^{1/e(q)}$ may be viewed as an ideal of K, so we will call c_q its class in $C(K)$. The image $\nu(c_q)$ in $G(k/\boldsymbol{Q})$ is what we will find under the previous assumption that $k(W)$ has been known. For each $q \in P$ and for each $p \in U$ with $p \neq q$, the p-component and W-component of $\nu(c_q)$ are respectively

$$\left(\frac{k(p)}{q^{l^n/e(q)}}\right) \quad \text{and} \quad \left(\frac{k(W)}{q^{l^n/e(q)}}\right);$$

if, in addition, $q \neq l$, these become respectively

$$\left(\frac{k(p)}{q^{l^{b(q)}}}\right) \quad \text{and} \quad \left(\frac{k(W)}{q^{l^{b(q)}}}\right)$$

since $e(q) = l^{n-b(q)}$. For $q \in U$, put $j(q) = a(q)/l^{b(q)}$; then $j(q)/e(q) = a(q)/l^n$, so that we have in K:

$$(\sqrt[l^n]{m}) = \prod_{q \in U} (q)^{j(q)/e(q)} \prod_{\substack{q \in P \\ q \notin U}} (q)^{a(q)/l^n},$$

which implies that

$$N(q)^{j(q)/e(q)} = q^{a(q)}.$$

So putting $a_q = (m - \sqrt[l^n]{m})^{-1}$, we have

$$N(q)^{j(q)/e(q)} N(a_q) = q^{a(q)}/(m^{l^n} - m);$$

this is congruent to $-q^{a(q)}/m$ modulo the conductor q of the abelian field $k(q)$ since $m \equiv 0 \pmod{q}$, and the class of (a_q) in $C(K)$ is trivial; so that our formula (1) in Section 1 then says that the q-component of $\nu(c_q^{j(q)})$ is equal to

$$\left(\frac{k(q)}{-q^{a(q)}/m}\right).$$

From this, the q-component of $\nu(c_q)$ can be found, since, by definition, $k(q)/\mathbf{Q}$ is of lth power degree and $j(q)$ is prime to l. In the case where $l \in P$ and $a(l)$ is prime to l (i.e., $b(l) = 0$), l is ramified fully in K, and so $e(l) = l^n$ (cf. [4], Chapter 7). Put $a_W = (m^\varrho - \sqrt[l^n]{m})^{-1}$, where $\varrho \in \mathbf{Z}$ is chosen so that m^ϱ is a multiple of the conductor of the abelian field $k(W)$; then, by formula (1), the W-component of $\nu(c_l^{a(l)})$ is equal to

$$\left(\frac{k(W)}{-l^{a(l)}/m}\right),$$

and so this also gives that of $\nu(c_l)$. The case where $l \in P$ and $b(l) \neq 0$, however, would be difficult to deal with, and so we will leave it. It now remains to consider the case where $l \in T$ but $\notin P$. It is easy to see that the p-component of $\nu(c_l)$, for each $p \in U$, is

$$\left(\frac{k(p)}{l^{n/e(l)}}\right);$$

but it is necessary to know $e(l)$. Now it is shown in [6], p. 220, that $k(W) = \mathbf{Q}$ if $l \neq 2$, and that $k(W)$ is the ith cyclotomic field if $l = 2$, where i is the minimum of 2^{n+1} and the 2-part of $m+1$. Since we are now interested only in the W-component, we may assume that $l = 2$ and $i \geqslant 4$. Put then $a_W = (m - \sqrt[2^n]{m})^{-1}$; the class of (a_W) in $C(K)$ is trivial, and $N(a_W) = (m^{2^n} - m)^{-1}$, where 2-part is 2^{-1} since $m \equiv -1 \pmod{4}$; a_W satisfies an Eisenstein polynomial with respect to 2, so that 2 is ramified fully in K, and $e(2) = 2^n$ (cf. [4], Chapter 2). Therefore, by formula (1), the W-component of $\nu(c_l)$ is equal to

$$\left(\frac{k(W)}{2/(m^{2^n} - m)}\right).$$

An elementary calculation then shows that this component is either trivial or the generator of the Galois group of $k(W)$ over the $(i/2)$th cyclotomic field according to whether or not $m \equiv -1 \pmod{2^{n+2}}$.

References

[1] A. Fröhlich, *The genus group and genus field in finite number fields*, (I) Mathematika 6 (1959), pp. 40–46; (II) ibid. 6 (1959), pp. 142–146.

[2] — *On the l-classgroup of the field* $P(\sqrt[l]{m})$, J. London Math. Soc. 37 (1962), pp. 189–192.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica-Verlag, Würzburg–Wien 1970.

[4] M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math. 555, Springer-Verlag, Berlin–Heidelberg–New York 1976.

[5] — *An algorithm for constructing the genus field of an algebraic number field of odd prime degree*, J. Fac. Sci. Univ. Tokyo, Sec. IA, 24 (1977), pp. 61–75.

[6] — *On the genus fields of pure number fields*, (I) Tokyo J. Math. 3 (1980), pp. 163–171; (II) ibid. 4 (1981), pp. 213–220.

[7] P. Roquette and H. Zassenhaus, *A class rank estimate for algebraic number fields*, J. London Math. Soc. 44 (1969), pp. 31–38.

[8] C. Walter, *The ambiguous class group and the genus group of certain non-normal extensions*, Mathematika 26 (1979), pp. 113–124.

DEPARTMENT OF MATHEMATICS
TOKYO METROPOLITAN UNIVERSITY
2-1-1, Fukazawa, Setagaya
Tokyo, 158, Japan

Received on 23. 9. 1982 (1321)