ACTA ARITHMETICA
VIII (1963)

On the Galois cohomology group of the ring of integers in an algebraic number field

by

H. YOKOI (Nagoya)

1. Introduction. In [2] we considered the integral representations of Galois group by the ring of integers in an algebraic number field. There the following theorem was foundamental.

THEOREM 1. *Let k be an algebraic number field of finite degree and let K be a normal extension of k. Then the relative traces of all integers of K to k constitute an integral ideal $\mathfrak{a}$ of k and the ideal $\mathfrak{a}$ is characterized as the maximal divisor of k dividing the relative different $D_{K/k}$.*

Now, let O_K and O_k be the rings of integers in K and k respectively, and let $G = G(K/k)$ be the Galois group of K over k. Then this fundamental theorem means in the cohomology theory that the 0-dimensional Galois cohomology group $H^0(G, O_K)$ of O_K is isomorphic to the residue class group of $O_K \bmod^{+} \mathfrak{a}$.

Further, we knew there the following result (Corollary 2.):

Under the same assumptions as in Theorem 1, if we assume moreover that the 0-dimensional Galois cohomology group of O_K with respect to K/k is trivial, then the Galois cohomology group of O_K with respect to K/Ω is trivial for every dimension and for any intermediate field Ω of K/k.

In the present paper, we shall consider furthermore the 1-dimensional Galois cohomology group $H^1(G, O_K)$ of O_K, and then, by considering $H^0(G, O_K)$, $H^1(G, O_K)$ in the case where K and k are normal over the rational number field Q and the relative degree of K/k is prime p, we shall show that all dimensional Galois cohomology groups are isomorphic to each other and that they are determined by ramification numbers.

2. $H^1(G, O_K)$. In this article, we shall consider the 1-dimensional Galois cohomology group of O_K.

Thus, let k be, as before, a finite algebraic number field, let K/k be a finite normal extension over k, and let $G = G(K/k)$ be the Galois group of K/k. Here we define the symbol $Z(A, a)$ in the following way. We say that the symbol $Z(A, a)$ is well defined for A in O_K and for a

in O_K if and only if there exists a $\{\xi_\sigma\}_{\sigma\in G}$, $\xi_\sigma \in O_K$ such that $A-A^\sigma = a\cdot\xi_\sigma$ for every σ in G. If the symbol $Z(A, a)$ is well defined, then $\{\xi_\sigma\}_{\sigma\in G}$ is uniquely determined and $\{\xi_\sigma\}_{\sigma\in G}$ defines clearly a 1-dimensional Galois cocycle, and hence we may write also $Z(A, a) = \xi$.

PROPOSITION 1. *The symbol $Z(A, a)$ is well defined if and only if $A \equiv A^\sigma \bmod (a)_K$ for every σ in G.*

Proof. Evident from the definition of $Z(A, a)$.

PROPOSITION 2. *The symbol $Z(A, a)$ defines a 1-dimensional Galois coboundary if and only if there exists a b in O_k such that $A \equiv b \bmod (a)_K$.*

Proof. If $Z(A, a)$ defines a 1-dimensional Galois coboundary, then there exists a B in O_K such that $A-A^\sigma = a(B-B^\sigma)$, namely $(A-aB)^\sigma = (A-aB)$ for every σ in G. Hence, there exists a b in O_k such that $A-aB = b$. Therefore, we have $A\equiv b \bmod (a)_K$.

Conversely, if there exists a b in O_k such that $A = b+aB$, then $A-A^\sigma = a(B-B^\sigma)$ and so $Z(A, a)$ defines a 1-dimensional Galois coboundary.

PROPOSITION 3. *Let a be an arbitrarily fixed non-zero number in $S_{K/k}O_K$. Then for any 1-dimensional Galois cocycle, there exists a number A in O_K such that $Z(A, a) = \xi$.*

Proof. If we take an element $B\in S_{K/k}^{-1}a$ and put $A = \sum_{\tau\in G} B^\tau\xi_\tau$, then this number A belongs to O_K clearly, and for every σ in G we have $A-A^\sigma = a\cdot\xi_\sigma$. For

$$\begin{aligned} A-A^\sigma &= \sum_{\tau\in G} B^\tau\xi_\tau - \sum_{\tau\in G} B^{\sigma\tau}\xi_\tau^\sigma \\ &= \sum_{\sigma\tau\in G} B^{\sigma\tau}\xi_{\sigma\tau} - \sum_{\sigma\tau\in G} B^{\sigma\tau}\xi_\tau^\sigma \\ &= \sum_{\sigma\tau\in G} B^{\sigma\tau}(\xi_{\sigma\tau}-\xi_\tau^\sigma) = \sum_{\sigma\tau\in G} B^{\sigma\tau}\xi_\sigma \\ &= (S_{K/k}B)\,\xi_\sigma = a\cdot\xi_\sigma . \end{aligned}$$

PROPOSITION 4. *Let a be an arbitrarily fixed non-zero number in $S_{K/k}O_K$. Then the 1-dimensional Galois cohomology group $H^1(G, O_K)$ of O_K is isomorphic to the factor group of the G-invariant residue class group of $O_K \bmod (a)_K$ by the residue class subgroup $\bmod\, (a)_K$ containing some number in O_k.*

Proof. Evident from the above Propositions 1, 2, 3.

PROPOSITION 5. *For any integral ideal $\mathfrak{a}$ in O_k, we denote by $H_{K/k}(\mathfrak{a})$ the factor group of the G-invariant residue class group of $O_K \bmod \mathfrak{a}_K$ by the residue class subgroup containing some number in O_k. Then, for the prime decomposition $\mathfrak{a} = \Pi_i \mathfrak{p}_i^{s_i}$ of ideal $\mathfrak{a}$ in k, $H_{K/k}(\mathfrak{a})$ is isomorphic to the direct sum of groups $H_{K/k}(\mathfrak{p}_i^{s_i})$ and the order of the factor group $H_{K/k}(\mathfrak{p}_i^{s_i})$ is a power of prime p_i contained in $\mathfrak{p}_i$.*

Proof. We prove

$$H_{K/k}(\mathfrak{a}\mathfrak{b}) \cong H_{K/k}(\mathfrak{a}) \oplus H_{K/k}(\mathfrak{b})$$

for two ideals $\mathfrak{a}, \mathfrak{b}$ in O_k such that $(\mathfrak{a}, \mathfrak{b}) = 1$. Now, we may take $a\in\mathfrak{a}$, $b\in\mathfrak{b}$ such that $(a, b) = 1$. Since there exists an ideal $\mathfrak{m}$ in O_k such that $(\mathfrak{a}, \mathfrak{m}) = 1$ and $\mathfrak{b}\mathfrak{m} = (b)$ is principal in O_k, there exists an ideal $\mathfrak{n}$ in O_k such that $(b, \mathfrak{n}) = 1$ and $\mathfrak{a}\mathfrak{n} = (a)$ is principal in O_k. Here we put $\gamma = a\beta + b\alpha$. Then, if α, β run over a complete system of residues $\bmod\, \mathfrak{a}_K$, $\bmod\, \mathfrak{b}_K$ in O_K respectively, γ also runs over a complete system of residues $\bmod\, (\mathfrak{a}\mathfrak{b})_K$ in O_K, and γ is G-invariant $\bmod\, (\mathfrak{a}\mathfrak{b})_K$ if and only if α, β are G-invariant $\bmod\, \mathfrak{a}_K$, $\bmod\, \mathfrak{b}_K$ respectively.

Further, if $\alpha\equiv a_0 \bmod \mathfrak{a}_K$ and $\beta\equiv b_0 \bmod \mathfrak{b}_K$ for some $a_0\in O_k$, $b_0\in O_k$ then $\gamma\equiv ab_0+ba_0 \in O_k \bmod (\mathfrak{a}\mathfrak{b})_K$.

Conversely, if we assume $\gamma\equiv r_0 \bmod (\mathfrak{a}\mathfrak{b})_K$ for some $r_0\in O_k$, then since $(a, b) = 1$, we may write $r_0 = a(r_0x)+b(r_0y)$ with some number x, y in O_k such that $ax+by = 1$. Therefore we have

$$a\beta+b\alpha = \gamma \equiv r_0 = a(r_0x)+b(r_0y) \bmod (\mathfrak{a}\mathfrak{b})_K ,$$

whence

$$\alpha \equiv r_0 y \in O_k \bmod \mathfrak{a}_K ,$$
$$\beta \equiv r_0 x \in O_k \bmod \mathfrak{b}_K .$$

On the other hand, since the order of the factor group $O_k/\mathfrak{p}_i^{s_i}$ is a power of p_i, the order of the subgroup $H_{K/k}(\mathfrak{p}_i^{s_i})$ of $O_k/\mathfrak{p}_i^{s_i}$ is also a power of prime p_i.

This completes the proof of our assertion.

THEOREM 2. *For the ideal $S_{K/k}O_K = \mathfrak{a} = \prod_{i=1}^{g} \mathfrak{p}_i^{s_i}$, we have*

1) *$H_{K/k}(\mathfrak{p}^n) = 0$ for any integer $n\geqslant 0$ and for any prime $\mathfrak{p}\neq\mathfrak{p}_i$ $(i = 1, 2, \ldots, g)$,*

2) *$H^1(G, O_K) \cong \operatorname{dir}\sum_{i=1}^{g} H_{K/k}(\mathfrak{p}_i^{s_i})$.*

Proof. We may take an integral ideal $\mathfrak{m}$ in O_k such that $(\mathfrak{a}\mathfrak{p}^n, \mathfrak{m}) = 1$ and that $\mathfrak{a}\mathfrak{p}^n\mathfrak{m} = (a)$ is principal in O_k and an integral ideal $\mathfrak{n}$ in O_k such that $(a, \mathfrak{n}) = 1$ and that $\mathfrak{a}\mathfrak{n} = (a')$ is principal in O_k. Then, since

$$H_{K/k}((a)) \cong H_{K/k}((a')) \cong H^1(G, O_K)$$

by Proposition 4, we have

$$H_{K/k}(\mathfrak{a}) \oplus H_{K/k}(\mathfrak{p}^n) \oplus H_{K/k}(\mathfrak{m}) \cong H_{K/k}(\mathfrak{a}) \oplus H_{K/k}(\mathfrak{n}) \cong H^1(G, O_K)$$

from Proposition 5.

Here, because of $(\mathfrak{p}, \mathfrak{a}\mathfrak{n}) = 1$, we have $H_{K/k}(\mathfrak{p}^n) = 1$ from Proposition 5. Similarly we have $H_{K/k}(\mathfrak{m}) = 1$, and hence $H_{K/k}(\mathfrak{a}) \cong H^1(G, O_K)$. This implies our assertion by Proposition 5.

3. Main theorem. In this article, we consider the Galois cohomology groups in a special case as follows.

Let K be a normal extension over the rational number field Q, and let k be a subfield of K such that K/k is cyclic of prime degree p and that k/Q is normal of degree n.

PROPOSITION 6. *Let v be the common ramification number with respect to K/k of all the prime divisors $\mathfrak{P}_i$ of p in K, and let e be the common ramification order with respect to k/Q of all the prime divisors $\mathfrak{p}_i$ of p in k. Put $s = v-[v/p] \geqslant 0$, where $[x]$ means the Gaussian symbol, i.e. the maximal integer which is not greater than x. Then the 0-dimensional Galois cohomology group $H^0(G, O_K)$ of O_K is isomorphic to the ns/e-ple direct sum of a cyclic group of order p:*

$$H^0(G, O_K) \cong \{\overbrace{p, p, \dots, p}^{ns/e}\}.$$

Remark. In this paper, we understand by the *ramification number* of $\mathfrak{P}$ with respect to K/k an integer v such that $\mathfrak{P}^{1+v}$ is the maximal common $\mathfrak{P}$-component of $A^\sigma - A$ for every integer A in O_K and for every Galois automorphism σ of K/k.

Hence, according as $\mathfrak{P}$ is unramified, tamely ramified or highly ramified in K/k, we have $v=-1$, $v=0$, $v\geqslant 1$, and then $s=0$, $s=0$, $s \geqslant 1$ respectively.

In the former paper [2], we understood by the *ramification number* of $\mathfrak{P}$ with respect to K/k the $v+1$ in this paper.

Proof to Proposition 6. We put $v = pm+t$, $0 \leqslant t < p$ and $r = p-(t+1)$ $(0 \leqslant r < p)$. Then the $\mathfrak{P}_i$-component of the relative different of K/k may be written as $D_{K/k}(\mathfrak{P}_i) = \mathfrak{P}_i^{(p-1)(v+1)} = \mathfrak{p}_i^s \mathfrak{P}_i^r$ because of $\mathfrak{p}_i^s = \mathfrak{P}_i^{ps}$. However, K/k is normal by the assumption, and hence from Theorem 1 we obtain $S_{K/k} O_K = \prod_{\mathfrak{p}_i/p} \mathfrak{p}_i^s$, where the product runs over all the prime divisors $\mathfrak{p}_i$ of p in k, and the index of $S_{K/k}O_K$ in O_k is equal to

$$[O_k\colon S_{K/k}\, O_K] = N_{k/Q} \prod_{\mathfrak{p}_i/p} \mathfrak{p}_i^s = p^{ns/e}.$$

On the other hand, the order of any element of the group $H^0(G, O_K)$ divides p. Now our assertion is immediate.

PROPOSITION 7. *Under the same notations as in Proposition 6, we have $e \geqslant s$. In particular, in case $v \equiv 0\,(p)$, we have $e = s$.*

Proof. Since $p = S_{K/k} 1 \in S_{K/k} O_K \subseteq \mathfrak{p}_i^s$ for any $\mathfrak{p}_i$, we obtain $p \equiv 0\,(\mathfrak{p}_i^s)$, namely $e \geqslant s$.

On the other hand, from Theorem 1, we have

$$(p-1)(v+1) < p(s+1), \quad \text{namely} \quad v < \frac{ps}{p-1} + \frac{1}{p-1}.$$

Since v is integer and $p \geqslant 2$, we have $v \leqslant ps/(p-1)$, and hence $v \leqslant ps/(p-1) \leqslant pe/(p-1)$. In case $v \equiv 0(p)$, we have $v = pe/(p-1)$, whence

$$v = \frac{ps}{p-1} = \frac{pe}{p-1}, \quad \text{i.e.} \quad e = s.$$

This is our assertion.

Now, let Π be a number in $\mathfrak{P}_i$ but not in $\mathfrak{P}_i^2$ $(\mathfrak{P}_i // \Pi)$, let π be a number in $\mathfrak{p}_i$ but not in $\mathfrak{p}_i^2$ $(\mathfrak{p}_i // \pi)$, and let R be a fixed representative in O_k of a basis for the residue class field $O_k/\mathfrak{p}_i$ containing the number 0,1. Then in case $v \geqslant 0$, R is also the representative of a basis for $O_K/\mathfrak{P}_i$.

PROPOSITION 8. *In case $s \geqslant 1$, for any $i = 1, 2, \dots, p-1$, we have*

$$\mathfrak{P}_i^{v+i} // (\Pi^\sigma)^i - \Pi^i, \quad \text{i.e.} \quad (\Pi^\sigma)^i - \Pi^i \equiv 0\,(\mathfrak{P}_i^{v+i}), \ \textit{but} \ \not\equiv 0\,(\mathfrak{P}_i^{v+i+1}),$$

where σ is a generator of the Galois group $G(K/k)$.

Proof. To prove this Proposition, we set

$$\Pi^\sigma \equiv \Pi + g(\Pi)\Pi^{v+1} \bmod \mathfrak{P}_i^{ps},$$

where

$$g(\Pi) = c_0 + c_2\Pi + \dots + c_{ps-v-1}\Pi^{ps-v-2}$$

with uniquely determined $c_0 \neq 0$, $c_2, \dots, c_{ps-v-1} \in R$. Since

$$(\Pi^\sigma)^k \equiv (\Pi + g\Pi^{v+1})^k = \sum_{j=0}^{k} {}_kC_j \Pi^{k-j} g^j \Pi^{(v+1)j}$$
$$= \sum_{j=0}^{k} {}_kC_j g^j \Pi^{k+vj} \bmod \mathfrak{P}_i^{ps}$$

for every $k = 1, \dots, p-1$, we have

$$(\Pi^\sigma)^i - \Pi^i = (\Pi^\sigma - \Pi) \sum_{k=0}^{i-1} \Pi^{i-1-k} (\Pi^\sigma)^k$$
$$\equiv (\Pi^\sigma - \Pi) \sum_{k=0}^{i-1} \sum_{j=0}^{k} {}_kC_j g^j \Pi^{i-1+vj}$$
$$= (\Pi^\sigma - \Pi)\Pi^{i-1} \sum_{k=0}^{i-1} \sum_{j=0}^{k} {}_kC_j g^j \Pi^{vj} \bmod \mathfrak{P}_i^{ps}.$$

On the other hand, we have $\mathfrak{P}_i^{v+i} // (\Pi^\sigma - \Pi)\Pi^{i-1}$ from the definition of v, and, since $(i, p) = 1$ for $i = 1, 2, \dots, p-1$, we have

$$\sum_{k=0}^{i-1} \sum_{j=0}^{k} {}_kC_j g^j \Pi^{vj} = \sum_{k=0}^{i-1} \Big({}_kC_0 + \sum_{j=1}^{k} {}_kC_j g^j \Pi^{vj}\Big)$$
$$= i + \sum_{k=1}^{i-1} \sum_{j=1}^{k} {}_kC_j g^j \Pi^{vj} \not\equiv 0 \bmod \mathfrak{P}_i^{ps},$$

whence follows our assertion.

PROPOSITION 9. *Let* $A \equiv \sum_{i=0}^{p-1} f_i(\pi)\Pi^i$ $(\mathfrak{P}_i^{ps})$ *be the residue class* $\bmod \mathfrak{P}_i^{ps}$ *containing a number* A *in* O_K, *where*

$$f_i(\pi) = \sum_{j=0}^{s-1} a_{i+pj}\pi^j, \quad a_{i+pj} \in R \quad (0 \leqslant i < p, 0 \leqslant j < s) .$$

Then A *is* G*-invariant* $\bmod \mathfrak{P}_i^{ps}$ *if and only if condition* $(*)$ *is satisfied;*

$$(*) \begin{cases} \text{in case } r = 0 , \\ \quad a_i = a_{i+p} = \ldots = a_{i+p(s-m-2)} = 0 \quad \text{for every} \quad i = 1, 2, \ldots, p-1 , \\ \text{in case } r > 0 , \\ \quad a_i = a_{i+p} = \ldots = a_{i+p(s-m-1)} = 0 \quad \text{for every} \quad i = 1, 2, \ldots, r , \\ \quad a_i = a_{i+p} = \ldots = a_{i+p(s-m-2)} = 0 \quad \text{for every} \quad i = r+1, \ldots, p-1 . \end{cases}$$

Proof. In case $s = 0$, this Proposition is trivial and hence we consider case $s \geqslant 1$ only.

Now we first assume that A is G-invariant $\bmod \mathfrak{P}_i^{ps}$, namely $A^\sigma \equiv A \bmod \mathfrak{P}_i^{ps}$. Then, since

$$A^\sigma - A \equiv \sum_{i=0}^{p-1} f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} = \sum_{i=1}^{p-1} f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} ,$$

we have

$$(**) \qquad \sum_{i=1}^{p-1} f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} \equiv 0 \bmod \mathfrak{P}_i^{ps} .$$

On the other hand, because of $ps = (v+1) + p(s-m-1) + r$, we first consider $(**)$ $\bmod \mathfrak{P}_i^{v+1}, \ldots, \mathfrak{P}_i^{v+p}$ respectively. Then we have $f_1(\pi) \equiv 0, \ldots, f_{p-1}(\pi) \equiv 0 \bmod \mathfrak{P}_i$, whence we obtain $a_1 = 0, \ldots, a_{p-1} = 0$ respectively.

We next consider $(**)$ $\bmod \mathfrak{P}_i^{(v+2)+p}, \ldots, \mathfrak{P}_i^{(v+p)+p}$, and similarly we have $f_1(\pi) \equiv 0, \ldots, f_{p-1}(\pi) \equiv 0 \bmod \mathfrak{P}_i^{1+p}$, whence $a_{1+p} = 0, \ldots, a_{(p-1)+p} = 0$ respectively. We repeat this argument and finally obtain

$$a_{1+p(s-m-2)} = 0 , \ldots , a_{(p-1)+p(s-m-2)} = 0 .$$

In case $r > 0$, we further consider $(**)$ $\bmod \mathfrak{P}_i^{(v+2)+p(s-m-1)}, \ldots$ $\ldots, \mathfrak{P}_i^{(v+1+r)+p(s-m-1)}$, and obtain similarly

$$a_{1+p(s-m-1)} = 0 , \ldots , a_{r+p(s-m-1)} = 0 .$$

Conversely, we assume condition $(*)$. Since condition $(*)$ means that

$$f_i(\pi) = a_{i+p(s-m)}\pi^{s-m} + \ldots + a_{i+p(s-1)}\pi^{s-1} \equiv 0 \bmod \mathfrak{p}_i^{s-m} \quad \text{for} \quad i = 1, \ldots, r,$$

$$f_i(\pi) = a_{i+p(s-m-1)}\pi^{s-m-1} + \ldots + a_{i+p(s-1)}\pi^{s-1} \equiv 0 \bmod \mathfrak{p}_i^{s-m-1} \quad \text{for} \quad i = r+1, \ldots, p-1,$$

it follows by Proposition 8 that

$$f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} \equiv 0 \bmod \mathfrak{P}_i^{p(s-m)+v+i} \quad \text{for} \quad i = 1, 2, \ldots, r ,$$
$$f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} \equiv 0 \bmod \mathfrak{P}_i^{p(s-m-1)+v+i} \quad \text{for} \quad i = r+1, \ldots, p-1 .$$

On the other hand, we have

$$p(s-m) + v + i = ps + t + i > ps$$

because of $i \geqslant 1$, and in case $i \geqslant r+1$ we have

$$p(s-m-1) + v + i \geqslant p(s-1) + t + r + 1 = ps .$$

Therefore, in both cases we have

$$A^\sigma - A \equiv \sum_{i=1}^{p-1} f_i(\pi)\{(\Pi^\sigma)^i - \Pi^i\} \equiv 0 \bmod \mathfrak{P}_i^{ps} ,$$

which completes our proof.

PROPOSITION 10. *The* 1*-dimensional Galois cohomology group* $H^1(G, O_K)$ *of* O_K *with respect to* K/k *is isomorphic to the* ns/e*-ple direct sum of cyclic group of order* p:

$$H^1(G, O_K) \cong \{\overbrace{p, p, \ldots, p}^{ns/e}\} .$$

Proof. From Theorem 2 and Proposition 9, it follows immediately that the order of the 1-dimensional Galois cohomology group $H^1(G, O_K)$ of O_K is equal to $p^{ns/e}$. On the other hand, the order of any element of the group $H^1(G, O_K)$ divides p. Now follows our Proposition.

THEOREM 3. *Let* K *be a normal extension over the rational number field* Q, *and let* k *be a subfield of* K *such that* K/k *is cyclic of prime degree* p *and that* k/Q *is normal of degree* n. *Then, for every dimension* m, *the Galois cohomology group* $H^m(G, O_K)$ *of* O_K *with respect to* K/k *is isomorphic to the* ns/e*-ple direct sum of a cyclic group of order* p:

$$H^m(G, O_K) \cong \{\overbrace{p, p, \ldots, p}^{ns/e}\} .$$

Proof. From Proposition 6 and Proposition 10 it follows that the 0-dimensional Galois cohomology group $H^0(G, O_K)$ of O_K with respect to K/k is isomorphic to the 1-dimensional Galois cohomology group $H^1(G, O_K)$ of O_K with respect to K/k. Since $G(K/k)$ is cyclic, by the well-known theorem (cf. [1]) of cohomology groups we obtain our Theorem.

Added in proofs: In the meantime the writer was obtained a somewhat simpler second proof to the main result in the present paper by considering 1-dimensional Galois cohomology groups in place of 1-dimensional ones. See H. Yokoi, *On an isomorphism of Galois cohomology groups* $H^m(G, O_K)$ *of integers in an algebraic number field*, Proc. Japan Acad. 38 (1962), pp. 499-501.

References

[1] C. Chevalley, *Class field theory*, Nagoya University (1953-1954), p. 38.

[2] H. Yokoi, *On the ring of integers in an algebraic number field as a representation module of Galois group*, Nagoya Math. J. 16 (1960), pp. 83-90.

DEPARTMENT OF MATHEMATICS
NAGOYA INSTITUTE OF TECHNOLOGY

Reçu par la Rédaction le 8. 7. 1962

ACTA ARITHMETICA
VIII (1963)

On primitive prime factors of Lehmer numbers II

by

A. Schinzel (Warszawa)

The present paper is devoted to the investigation of Lehmer numbers with more than two primitive prime factors. We retain the notation of [3] with small changes that will be clear from the sequel.

In particular,

$$P_n(\alpha, \beta) = \begin{cases} (\alpha^n - \beta^n)/(\alpha - \beta), & n \text{ odd}, \\ (\alpha^n - \beta^n)/(\alpha^2 - \beta^2), & n \text{ even}, \end{cases}$$

where α and β are roots of the trinomial $z^2 - L^{1/2}z + M$, and L and M are rational integers, $K = L - 4M \neq 0$. Further, $\bar{z}$ denotes the complex conjugate of any given z and $k_e(n)$ denotes a positive integer n divided by the greatest eth power dividing it. The main result of the paper runs as follows.

Theorem. *Let $(L, M) = 1$, $e = 3$, 4 or 6. If $L^{1/2}$ is rational, $K^{1/2}$ is an irrational integer of the field $K(\zeta_e)$, K is divisible by the cube of the discriminant of this field, $\varkappa_e = k_e(M)$ is squarefree,*

$$\eta_e = \begin{cases} 2 & \text{if } e = 6,\ M \equiv 3 \pmod 4, \\ 1 & \text{otherwise}, \end{cases}$$

and $n/\eta_e\varkappa_e$ is an integer relatively prime to e, then for $n > n_e(L, M)$, P_n has at least e primitive prime factors, and $n_e(L, M)$ can be effectively computed.

Lemma 1. *Let e, m, n be positive integers, $m|n$, and let χ be a character $\bmod m$ such that $\chi^{e+1} = \chi$ and that for all $i \not\equiv 0 \pmod e$ characters χ^i are primitive. Further, let*

$$\tau_i = \tau(\chi^i|\zeta_m) = \sum_{\substack{r=1 \\ (r,m)=1}}^{m} \chi^i(r)\zeta_m^r,$$

let χ_n be a character $\bmod n$ induced by χ, and let $\chi(-1)^{1/e}$ be any fixed e-th root of $\chi(-1)$.