J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

Application of the theory of the group of classes of projective modules to the existence problem of independent parameters of invariant

To celebrate Professor Iyanaga's 60th birthday

By Katsuhiko MASUDA

(Received Aug. 22, 1967)
(Revised Dec. 6, 1967)

1. Introduction

Let k be a field and let $K=k(x_1, \cdots, x_n)$ be a purely transcendental extension field over k, obtained by adjunction of n elements $x_i (i=1, \cdots, n)$[1] which are mutually independent over k. Let μ denote the automorphism of K/k such that

$$(1) \qquad \mu(x_1)=x_2, \quad \mu(x_2)=x_3, \quad \cdots, \quad \mu(x_n)=x_1.$$

Let G be the automorphism group of K generated by μ and L the subfield of K consisting of all the elements which are kept elementwise invariant by G. G is a cyclic group of order n, $[K:L]=n$, and K/L is a separable Galois extension, having G as its Galois group. Hence L/k is a finite regular extension of dimension n. Then the following is a classical problem:

PROBLEM. Is L/k a purely transcendental extension?

In this paper we deal only with the non-modular case of this problem. From now on we assume that n is not divisible by the characteristic of k[2]. When k contains a primitive n-th root of 1, the problem is easy and was solved[3] in the affirmative. The most fundamental case of the problem is that k is the rational number field $\boldsymbol{Q}$ and n is a prime integer p. In case of $k=\boldsymbol{Q}$ and $n=p$ the problem has been solved only for $p=2, 3, 5$, and 7[4]. The author proved the pure transcendency of $L/\boldsymbol{Q}$ in cases $p=3, 5$, and 7 as follows (cf. [**3**]). Let T be the p-th cyclomic field and H the Galois group of $T/\boldsymbol{Q}$. Let γ

1) In this paper, we use i and j as index variables. If 0 belongs to the range of the values, we use j exclusively. If not, i.

2) Cf. [1], where the modular case is studied.

3) For example, cf. [**3**], Theorem 1.

4) The first proof for the case $p=3$ is due to E. Nöther. We can see a good bibliography for this classical problem in [**2**].

be a primitive p-th root of 1. $T=\boldsymbol{Q}(\gamma)$. Let A denote the group-ring $\boldsymbol{Z}[H]$ of H over the rational integer ring $\boldsymbol{Z}$. A sufficient condition for $L/\boldsymbol{Q}$ to be purely trrnscendental is that a certain A-module M is A-isomorphic with A itself. This condition is verified in cases $p=3, 5$, and 7 by constructing a base of M over A explicitly ([3], pp. 61-63).

In this paper we shall prove the following: the above stated A-module M is always A-projective and of rank 1. We denote the integral closure of A in its total quotient ring by $\bar{A}$, and the group of classes of $A(\bar{A})$-projective modules by $D(A)(D(\bar{A}))$, respectively. Then we have the following exact sequence:

$$0 \longrightarrow L(\bar{A}/A) \xrightarrow{\nu} D(A) \xrightarrow{\pi} D(\bar{A}) \longrightarrow 0\,. \tag{2}$$

If $p=3, 5, 7$, and 11, we obtain both $\pi([M])=0$ and $L(\bar{A}/A)=0$, which proves $M\cong A$ as A-modules, where we denote by $[M]$ the element (class of A-projective modules of rank 1) of $D(A)$ which contains the A-projective module M.

The author wishes to express his thanks to Mr. M. Miyata who is a graduate student of Nagoya University. The formulation of Lemma 6 is due to his suggestion.

During the preparation of the present paper the author received many useful advices from Professor Y. Kawada and the referee and revised his original manuscript. The author wishes to express them his thanks.

2. Notation and A-module M

As usual we denote the rational number field by $\boldsymbol{Q}$ and the rational integer ring by $\boldsymbol{Z}$. Let p be a prime integer. We denote by K the p dimensional purely transcendental extension $\boldsymbol{Q}(x_1, \cdots, x_p)$ over $\boldsymbol{Q}$ and by μ the automorphism of $K/\boldsymbol{Q}$ such that

$$\mu(x_1)=x_2, \cdots, \mu(x_p)=x_1\,.$$

Let G be the automorphism group of K generated by μ and L the subfield of K consisting of all the elements which are kept elementwise invariant by μ. K/L is a separable Galois extension of degree p having G as its Galois group. We denote

$$\gamma=\cos 2\pi/p+i\sin 2\pi/p\,. \tag{3}$$

γ is a primitive p-th root of 1. We denote by T the p-th cyclotomic field $\boldsymbol{Q}(\gamma)$, and by H the Galois group of $T/\boldsymbol{Q}$. H is a cyclic group of order $p-1$.

Let $\bar{K}=K(\gamma)$, and $\bar{L}=L(\gamma)$. Both the Galois group of $\bar{K}/K$ and that of $\bar{L}/L$ are canonically isomorphic with H. Hence, identifying these three Galois groups, we denote them by the same notation H. G and H are elementwise commutative with each other as automorphism groups of $\bar{K}$.

Let the standard Lagrange's resolvents of $\bar{K}/\bar{L}$ be

(4) $$y_j=\sum_{i=1}^{p}\gamma^{-j(i-1)}x_i \qquad (j=0,1,\cdots,p-1)\,.$$

Let Y^* denote the multiplicative group ($\subset\bar{K}$) generated by $p-1$ elements $y_i(i=1,2,\cdots,p-1)$ and E^* the multiplicative group ($\subset\bar{K}$) generated by γ. Let $Y'=Y^*\cdot E^*(\subset\bar{K})$. Y' is the direct product $Y^*\times E^*$ of Y^* and E^*, and has both G and H as mutually commutative operator groups, though Y^* itself is an H-subgroup but not a G-subgroup of Y'. E^* is a cyclic group of order p, having both G and H as its operator groups. Let M^* be the set of all the elements of Y^* which are kept elementwise invariant by G. Then $M^*=Y^*\cap\bar{L}$.

LEMMA 1. *$Y^*/M^*\cong E^*$ as H-modules.*

PROOF. $y\rightsquigarrow y^{1-\mu}(\forall y\in Y')$ gives an H-homomorphism of Y' onto E^*. The kernel of this homomorphism is $M^*\times E^*$. Hence we have

$$E^*\cong(Y^*\times E^*)/(M^*\times E^*)\cong Y^*/M^*\,, \qquad \text{q. e. d.}$$

For convenience sake we denote the group operation of Y^* by addition, using notations Y and M in place of Y^* and M^*, respectively. We denote by A the group-ring $\boldsymbol{Z}[H]$ of H over $\boldsymbol{Z}$. Then Y and M are A-modules[5].

We take $t\in\boldsymbol{Z}$ such that $1\leqq t<p$ and t is a primitive root mod p. We fix it, throughout this paper. There exists one and only one element τ of H such that

(5) $$\tau(\gamma)=\gamma^t\,.$$

Obviously we have

(6) $$\tau(y_1)=y_t\,,\ \tau(y_t)=y_{t_2}\,,\cdots,\ \tau(y_{t_{p-2}})=y_1\,,$$

where we denote by $t_i(i=2,3,\cdots,p-2)$ the least positive residue of t^i mod p. Then

(7) $$Y\cong A$$

as A-modules. For convenience sake we change the notation of $p-1$ elements $y_i(i=1,2,\cdots,p-1)$ of Y, denoting them by

$$y_1=z_0,\ y_t=z_1,\ y_{t_2}=z_2,\cdots,\ y_{t_{p-2}}=z_{p-2}\,.$$

Thus z_0 is a free base of Y over A and

(8) $$\tau^j(z_0)=z_j \qquad (j=0,1,\cdots,p-2)\,.$$

According to Theorem 2, [3], we have the following

5) We denote the operation of H on Y by $\tau^j(y)$ in place of y^{τ^j}.

LEMMA 2. *$L/\boldsymbol{Q}$ is purely transcendental, if*

$$M \cong A \tag{9}$$

holds as A-modules.

3. Representation of M by an ideal $\mathfrak{N}$ of A

Since $z_j (j=0, 1, \cdots, p-2)$ are Lagrange's resolvents, $y=\sum_{j=0}^{p-2} a_j z_j (a_j \in \boldsymbol{Z})$ belongs to M if and only if

$$\sum_{j=0}^{p-2} a_j t \equiv 0 \bmod p . \tag{10}$$

We denote

$$\varepsilon = \cos 2\pi/(p-1) + i \sin 2\pi/(p-1) . \tag{11}$$

ε is a primitive $(p-1)$-th root of 1. We denote the $(p-1)$-th cyclotomic field $\boldsymbol{Q}(\varepsilon)$ by J. By class field theory p is completely decomposed in J into the product of prime divisors of degree 1, different from each other. Each of the residue class fields of these prime divisors is isomorphic with $\boldsymbol{Z}/(p)$. Among these $[\boldsymbol{Q}(\varepsilon):\boldsymbol{Q}]$ prime divisors of p there exists one only one prime divisor $\mathfrak{P}$ which contains $t-\varepsilon$. Let χ denote the absolutely irreducible character of A such that

$$\chi(\tau) = \varepsilon . \tag{12}$$

Let ι denote the A-isomorphism of A onto Y such that

$$\iota\Big(\sum_{j=0}^{p-2} a_j \tau^j\Big) = \sum_{j=0}^{p-2} a_j z_j \qquad (a_j \in \boldsymbol{Z}) . \tag{13}$$

Let $\mathfrak{N}$ be the ideal $\{a \in A ; \chi(a) \in \mathfrak{P}\}$ of A. $\mathfrak{N}$ is clearly a maximal ideal of A. From the characterisation of $\mathfrak{P}$ and from (10) follows

$$\iota(\mathfrak{N}) = M . \tag{14}$$

So M is A-isomorphic with the maximal A-ideal $\mathfrak{N}$.

As is well known, the primitive idempotents of the group-ring $J[H]$ of H over $J=\boldsymbol{Q}(\varepsilon)$ are obtained by

$$\Big(\sum_{i=1}^{p-1} \varepsilon^{ij} \tau^i\Big)/(p-1) \qquad (j=0, 1, \cdots, p-2)$$

Each idempotent e of $\boldsymbol{Q}[H]$ is a sum of primitive idempotents of $J[H]$. Hence $(p-1)e \in A$. $\boldsymbol{Q}[H]$ is isomorphic with a direct sum of cyclotomic fields, and an element of $\boldsymbol{Q}[H]$ is regular if and only if it is not a zero-divisor. As is easily seen, an element of A is a zero-divisor of A, if and only if it is a zero-divisor of $\boldsymbol{Q}[H]$. Then the total quotient ring A_S of A is isomorphic with

$\boldsymbol{Q}[H]$. Let $\bar{A}$ denote the integral closure of A in $A_S(=\boldsymbol{Q}[H])$. Every idempotent of $A_S(=\boldsymbol{Q}[H])$ belongs to $\bar{A}$. $\bar{A}$ is isomorphic with a direct sum of replicas of Dedekind domains of cyclotomic fields (subfields of J). Let $\bar{A}=D_1\oplus D_2\oplus\cdots\oplus D_r$ be the direct decomposition. Considering the fact that the discriminants of $(p-1)$-th roots (not necessarily primitive) of 1 divide a suitable power of $p-1$, we easily obtain a natural number m such that for every $i=1,\cdots,r$

$$(p-1)^m D_i\subset \boldsymbol{Z}[\varepsilon]\,.$$

Since $(p-1)^{m+1}\bar{A}e_i=(p-1)e_i(p-1)^m D_i$ we have

$$(p-1)^{m+1}\bar{A}\subseteqq A\,, \tag{1}$$

where we denote by e_i the idempotent of $\bar{A}$ contained in D_i.

Obviously there exists one and only one extension of χ to $\bar{A}$, which we denote by the same notation χ. Let

$$\bar{\mathfrak{N}}=\{a\in\bar{A}\,;\ \chi(a)\in\mathfrak{P}\}\,.$$

$\bar{\mathfrak{N}}$ is a maximal ideal of $\bar{A}$. Clearly

$$A/\mathfrak{N}\cong\bar{A}/\bar{\mathfrak{N}}\cong\boldsymbol{Z}/(p)\quad\text{and}\quad A\frown\bar{\mathfrak{N}}=\mathfrak{N}\,.$$

Since p belongs to $\mathfrak{N}$, from (15) follows that primitive idempotents $e(e_i$ with $i=1,\cdots,r-1)$ of $\bar{A}$ which do not correspond to the character χ (up to conjugate characters) belong to $\mathfrak{N}\bar{A}$; $\mathfrak{N}\bar{A}\supset(pe,(p-1)^{m+1}e)\ni e$. Then, since $\chi(\mathfrak{N})=\mathfrak{P}$, we have

$$\mathfrak{N}\bar{A}=\bar{\mathfrak{N}}=\bar{\mathfrak{N}}_1\oplus\cdots\oplus\bar{\mathfrak{N}}_r \tag{16}$$

where we denote $\bar{\mathfrak{N}}e_i$ by $\bar{\mathfrak{N}}_i$.

4. Application of the exact sequence $0\to L(\bar{A}/A)\xrightarrow{v}D(A)\xrightarrow{\pi}D(\bar{A})\to 0$

We follow the notations of Serre's paper [**5**] and use its results freely.

LEMMA 3. *M is A-projective and of rank* 1.

PROOF. To prove the lemma, we can deal with $\mathfrak{N}$ in place of M. $\mathfrak{N}\ni p$ and $\mathfrak{N}\not\ni 1$. Hence $\mathfrak{N}$ does not contain $p-1$. So every maximal ideal of A which contains $p-1$ does not coincide with $\mathfrak{N}$. Let B be a maximal ideal of A. There are two cases (a) and (b):

(a) $B\neq\mathfrak{N}$. Since $0\to\mathfrak{N}\to A\to\boldsymbol{Z}/(p)\to 0$ is exact, $\mathfrak{N}\underset{A}{\otimes}A_B\to A_B\to\boldsymbol{Z}/(p)\underset{A}{\otimes}A_B\to 0$ is exact, where we denote by A_B the localization of A with respect to B. From $B\neq\mathfrak{N}$ there exists an element $u\in\mathfrak{N}$ such that $u\notin B$. Since u is regular in A_B, we easily obtain $\boldsymbol{Z}/(p)\underset{A}{\otimes}A_B=0$. Thus $\mathfrak{N}\underset{A}{\otimes}A_B\to A_B\to 0$ is exact. As is easily seen, this is an exact sequence of A_B-modules.

Now we prove that $0 \rightarrow \mathfrak{N}_B \rightarrow A_B$ is exact, where we denote $\mathfrak{N} \underset{A}{\otimes} A_B$ by $\mathfrak{N}_B$. Suppose $n \otimes (r/s) \rightsquigarrow nr/s = 0$, where $n \in \mathfrak{N}$, r, $s \in A$, and $s \notin B$. Then there exists $s' \in A$ such that $s' \notin B$ and $nrs' = 0$. Obviously $r/s = rs'/ss'$ as elements of A_B, and we have $n \underset{A}{\otimes} (r/s) = n \underset{A}{\otimes} (rs'/ss') = nrs' \underset{A}{\otimes} (1/ss') = 0$. Next, suppose $n_1 \otimes (r_1/s_1) + \cdots + n_m \otimes (r_m/s_m) \rightarrow 0$. Then $(n_1 s_1' + \cdots + n_m s_m') \otimes (1/u) \rightarrow 0$, where $u = \prod_{i=1}^m s_i$ and $s_i' = s_1 \cdots s_{i-1} s_{i+1} \cdots s_m$. Applying the above result, we have

$$0 = (n_1 s_1' + \cdots + n_m s_m') \otimes (1/u) = n_1 \otimes (r_1/s_1) + \cdots + n_m \otimes (r_m/s_m).$$

Hence $0 \rightarrow \mathfrak{N}_B \rightarrow A_B$ is exact.

Combining the above two exact sequences (of A_B-modules), we have $\mathfrak{N}_B \cong A_B$ as A_B-modules.

(b) $B = \mathfrak{N}$. From the same arguments as in the above proof of the exactness of $0 \rightarrow \mathfrak{N}_B \rightarrow A_B$ we obtain that $0 \rightarrow \mathfrak{N}_\mathfrak{N} \rightarrow A_\mathfrak{N}$ is exact. Since $\mathfrak{N}$ does not contain $(p-1)^{m+1}$, and since $(p-1)^{m+1}\bar{A} \subset A$, we have $A_\mathfrak{N} = \bar{A}_\mathfrak{N}$ (cf. [5], p. 15). So $A_\mathfrak{N}$ is isomorphic to the localization of the Dedekind domain D_r of all the algebraic integers of $J = \boldsymbol{Q}(\varepsilon)$ with respect to the prime divisor $\mathfrak{P}$. $A_\mathfrak{N}$ is a principal ideal domain. Then from the exactness of $0 \rightarrow \mathfrak{N}_\mathfrak{N} \rightarrow A_\mathfrak{N}$ follows that $\mathfrak{N}_\mathfrak{N} \cong A_\mathfrak{N}$ as $A_\mathfrak{N}$-modules.

Thus we have obtained that for every maximal ideal B of A holds $\mathfrak{N}_B \cong A_B$ as A_B-modules. So the rank of $\mathfrak{N}$ is 1. Applying Proposition 3 of Serre's paper [5], we obtain that $\mathfrak{N}$ is A-projective, q. e. d.

According to [5], p. 16, we have an exact sequence

$$0 \longrightarrow L(\bar{A}/A) \xrightarrow{\nu} D(A) \xrightarrow{\pi} D(\bar{A}) \longrightarrow 0 \tag{17}$$

We denote by $[M]$ the element of $D(A)$ containing M. By the above exact sequence we have $[M] = 0$, i.e. $M \cong A$ as A-modules if the following both equalities hold:

$$\pi([M]) = 0, \tag{18}$$

and

$$L(\bar{A}/A) = 0. \tag{19}$$

5. Examples of p satisfying (18) and (19)

From now on we suppose that $p-1 = 2l$, where l is a prime. If l is an odd prime we call p as a higher odd prime. Let A' be a group-ring of a cyclic group of order l (prime) over $\boldsymbol{Z}$ and $\bar{A}'$ the integral closure of A' in the total quotient ring of A'. We can identify $\bar{A}'$ with the direct sum $\boldsymbol{Z} \oplus \boldsymbol{Z}[\beta]$ of $\boldsymbol{Z}$ and the Dedekind domain $\boldsymbol{Z}[\beta]$, where we denote by β a primitive l-th root of 1. As is stated in [5], p. 17, $a \oplus b (a \in \boldsymbol{Z},\ b \in \boldsymbol{Z}[\beta])$ belongs to A' if and only if

$$a \equiv b \mod (1-\beta)\,. \tag{20}$$

By the above assumption H is a cyclic group of order $2l$ and A is its group-ring over $\boldsymbol{Z}$. Then we can identify $\bar{A}$ with the direct sum

$$\bar{A} = \boldsymbol{Z}_1 \oplus \boldsymbol{Z}_2 \oplus O_1 \oplus O_2 \tag{21}$$

where $\boldsymbol{Z}_i \cong \boldsymbol{Z}$ and O_i are isomorphic (as rings) with the Dedekind domain $O = \boldsymbol{Z}[\varepsilon] = \boldsymbol{Z}[-\varepsilon] = \boldsymbol{Z}[\beta]$ of l-th cyclotomic field $J (i=1, 2)$.

We assume that $\boldsymbol{Z}_1$, $\boldsymbol{Z}_2$, O_1, and O_2 correspond to the characters χ_1, χ_2, χ_3, and χ (up to conjugate characters) such that $\chi_1(\iota)=1$, $\chi_2(\iota)=-1$, $\chi_3(\iota)=-\varepsilon$, and $\chi(\iota)=\varepsilon$. $-\varepsilon$ is a primitive l-th root of 1, and we obtain

LEMMA 5. *Let p be a higher odd prime (i.e. l is odd). Let a_i and $b_i (i=1, 2)$ be arbitrary elements of $\boldsymbol{Z}$ and elements of $\boldsymbol{Z}[-\varepsilon] = \boldsymbol{Z}[\varepsilon] = O$, respectively. Then $a_1 \oplus a_2 \oplus b_1 \oplus b_2$ belongs to A if and only if*

$$a_1 \equiv a_2 \bmod (2),\ b_1 \equiv b_2 \bmod (2),\ \text{and}\ a_i \equiv b_i \bmod \mathfrak{l}\ (i=1, 2), \tag{22}$$

where we denote by $\mathfrak{l}$ the prime ideal $(1+\varepsilon)$ of J.

PROOF. The only-if-part follows trivially from the facts that $\chi_1(\tau)=1\equiv -1 = \chi_2(\tau) \bmod (2)$, $\chi_3(\tau) = -\varepsilon \equiv \varepsilon = \chi(\tau) \bmod (2)$, $\chi_1(\tau) = 1 \equiv -\varepsilon = \chi_3(\tau) \bmod \mathfrak{l}$, and $\chi_2(\tau) = -1 \equiv \varepsilon = \chi(\tau) \bmod \mathfrak{l}$.

To prove the if-part, we assume (22). Then $a' = (a_1+a_2)/2$, $a'' = (a_1-a_2)/2$, $b' = (b_1+b_2)/2$, and $b'' = (b_1-b_2)/2$ are all algebraic integers. Since l is odd, 2 belongs to a regular class mod $\mathfrak{l}$. Then from the last two congruences of (22) we have

$$a' \equiv b',\ a'' \equiv b'' \bmod \mathfrak{l}\,. \tag{23}$$

Let $H^2 = \{\tau^{2j}; j=0, 1, \cdots, l-1\}$. H^2 is a cyclic subgroup of order $l=(p-1)/2$. (23) shows that both pairs (a', b') and (a'', b'') satisfy the congruence condition (20). Hence both $a' \oplus b'$ and $a'' \oplus b''$ can be considered as elements of the group-ring $\boldsymbol{Z}[H^2] = \boldsymbol{Z}[\tau^2] (\subset \boldsymbol{Z}[H])$ of H^2 over $\boldsymbol{Z}$. Then we can take c_j and $d_j \in \boldsymbol{Z} (j=0, 1, \cdots, l-1)$ such that

$$\chi_1\Big(\sum_{j=0}^{l-1} c_j \tau^{2j}\Big) = a',\quad \chi_3\Big(\sum_{j=0}^{l-1} c_j \tau^{2j}\Big) = b'$$

$$\chi_1\Big(\sum_{j=0}^{l-1} d_j \tau^{2j}\Big) = a'',\quad \chi_3\Big(\sum_{j=0}^{l-1} d_j \tau^{2j}\Big) = b''\,.$$

Since $\chi_1(\tau) = \chi_3(\tau^l) = 1$ we have

$$\chi_1\Big(\sum_{j=0}^{l-1} d_j \tau^{2j+l}\Big) = a'',\quad \chi_3\Big(\sum_{j=0}^{l-1} d_j \tau^{2j+l}\Big) = b''\,.$$

Let $a \in A$ be

$$a=\sum_{j=0}^{l-1} c_j\tau^{2j})+\sum_{j=0}^{l-1} d_j\tau^{2j+l}.$$

$\chi_2(\tau)=\chi(\tau^l)=-1$, and $\chi_1=\chi_2$, $\chi_3=\chi$ hold if restricted to H^2. Hence we have $\chi_1(a)=a'+a''=a_1$, $\chi_2(a)=a'-a''=a_2$, $\chi_3(a)=b'+b''=b_1$, and $\chi(a)=b'-b''=b_2$. Thus $a_1+a_2+b_1+b_2=a \in A$, q. e. d.

We denote by $\mathfrak{c}$ the ideal of $\bar{A}$ which is the direct sum $(2l)_1+(2l)_2+(2+2\varepsilon)_1+(2+2\varepsilon)_2$ of ideals $(2l)_i$ of $\boldsymbol{Z}_i$ and ideals $(2+2\varepsilon)_i$ of $O_i(i=1,2)$. From Lemma 5 follows clearly

$$\mathfrak{c}=\mathfrak{c}\bar{A}\subset A. \tag{24}$$

Let $\mathfrak{c}=\prod_{i=1}^{s}\bar{\mathfrak{m}}_i^{n_i}$ be the decomposition of $\mathfrak{c}$ into the product of maximal ideals of $\bar{A}$. We denote by $\bar{\Omega}$ the maximal spectrum of $\bar{A}$ and by $\bar{F}$ the set of the maximal ideals $\bar{\mathfrak{m}}_i(i=1,\cdots,s)$ which contain $\mathfrak{c}$. $\bar{F}\subset\bar{\Omega}$. Let F be the set of the maximal ideals of A which contain $\mathfrak{c}$. $\bar{F}$ coincides with the set of maximal ideals of $\bar{A}$ which contain at least one element of F. Let R_i be the quotient of multiplicative group $\bar{A}^*_{\bar{\mathfrak{m}}_i}$ by the subgroup consisting of the elements α such that $v_{\bar{\mathfrak{m}}_i}(1-\alpha)\geqq n_i$, and let R be the product of groups $R_i(i=1,\cdots,s)$. Let U be the subgroup of R generated by the units of $\bar{A}$. Let V be the subgroup of R generated by the units of A^*_S which are inversible at every point M of F. Then, according to [**5**], p. 17, we have

$$R/UV=L(\bar{A}/A). \tag{25}$$

From Lemma 5 follows

LEMMA 6. *If the order of H is $2l$ where l is an odd prime and if every non-zero class of integers of J* mod (2) *contains at least a unit of J, then $R=UV$.*

PROOF. Obviously J coincides with the l-th cyclotomic field $\boldsymbol{Q}(-\varepsilon)$ and

$$1,\ 1+(-\varepsilon),\ 1+(-\varepsilon)+(-\varepsilon)^2,\cdots,1+(-\varepsilon)+\cdots+(-\varepsilon)^{l-2} \tag{26}$$

are units of J and consist a complete representative system of the set of the non-zero classes of algebraic integers of J mod $(1+\varepsilon)$. From the definition of $\mathfrak{c}$ we can easily see that R is a direct product of replicas of multiplicative groups consisting of regular classes of $\boldsymbol{Z}/(2)(=1)$, $\boldsymbol{Z}/(l)$, $O/(1+\varepsilon)$, and $O/(2)$. The units of J given by (26) eliminate the components of R mod UV with respect to $O/(1+\varepsilon)$. Considering these units of (26) and using the characterization of the elements of A stated in Lemma 5, suitable elements of V and the units of (26) eliminate the components of R/UV with respect to $Z/(l)$. Then if the condition in Lemma 6 is satisfied, we can eliminate the components of R/UV with respect to $O/(2)$. Thus R/UV consists only of 1, and we have obtained the lemma, q. e. d.

Now there is no difficulty to verify the condition in Lemma 6 for $p=7(l=3)$, and $p=11(l=5)$. When $l=3$, (2) is a prime ideal in $J=\boldsymbol{Q}(-\varepsilon)$, where $-\varepsilon=(-1-i\sqrt{3})/2$. Then all the third roots 1 and $(-1\pm i\sqrt{3})/2$ of 1 verify the assumption of Lemma 6, i.e. they represent all the non-zero classes of $\boldsymbol{Z}[\varepsilon]$ mod (2). When $l=5$, (2) is a prime ideal of the fifth cyclotomic field J. Obviously $2^4-1=3\cdot 5$. Then the non-zero classes of $O=\boldsymbol{Z}[-\varepsilon]$ mod (2) consist a cyclic group of order $15=3\cdot 5$. All the fifth roots of 1 represent the classes which consist a subgroup of order 5. Obviously $(1+\zeta)^5-1=4\zeta+9\zeta^2+9\zeta^3+4\zeta^4 \not\equiv 0 \bmod (2)$, where $\zeta=\cos 2\pi/5+i\sin 2\pi/5$. Hence the units obtained as products of powers of ζ and $1+\zeta$ represent all the non-zero classes of $O=\boldsymbol{Z}[\zeta]$ mod (2), and the condition in Lemma 6 is satisfied for $l=5(p=11)$.

When $p=5$, $l=2$. So 5 is not a higher odd prime and we can not apply Lemma 5, 6. But, when $p=5$, $O=\boldsymbol{Z}[i]$, and it is an easy task to prove $R=UV$ directly. We omit its detail here.

When $p=3$, $p-1=2$ is a prime. Then we can use Rim's theorem (cf. [**5**], p. 17), and we have $L(\bar{A}/A)=0$. Now we have obtained

LEMMA 7. *If the order of the cyclic group H is equal to one of* $2, 2\cdot 2=4, 2\cdot 3=6, 2\cdot 5=10$, *it holds*

$$L(\bar{A}/A)=0\,^{6)}.$$

When $p=3$, 5, 7, or 11, every component field of the group-ring $\boldsymbol{Q}[H]$ of H over $\boldsymbol{Q}$ has 1 as its class number. Hence $D(\bar{A})=0$, accordingly $\pi([M])=0$. Combining Lemma 7, we obtain $[M]=0$ for these four special values of p. Then from Lemma 2 follows the pure transcendency of $L/\boldsymbol{Q}$ in these special cases.

6. Explicit generators of $L/\boldsymbol{Q}$ for $p=11$

For $p=11$ we can prove the pure transcendency of $L/\boldsymbol{Q}$ also by the same method as in [**3**], which gives explicit independent generators (parameters) of $L/\boldsymbol{Q}$. Following the notations of [**3**], we denote y_1y_2/y_3 by $c_{1,2}$. 2 is a primitive root mod 11. We take 2 as t. Then we can represent $c_{1,2}$ as $z_0+z_1-z_8$ in the sense in §1. Clearly the cyclic determinant of degree 10

$$\det\begin{vmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{vmatrix}$$

6) In the proofs of Lemmas 6, 7 we do not use that $2l+1$ is a prime. Hence these lemmas are independent of the assumptions of §5 that p is a prime and l (prime) is equal to $(p-1)/2$.

$$=(1+1-1)(1-1-1)N_{J/Q}(1+(-\varepsilon)-(-\varepsilon)^8)N_{J/Q}(1+\varepsilon-\varepsilon^8)=-11\,.$$

The above intermediate term is obtained easily from the usual formula of cyclic determinants.

In this case $\bar{K}/\bar{L}$ is a Kummer extension with cyclic Galois group of order 11. Hence we easily obtain $[Y^*:M^*]=11$. Since the above cyclic determinant has 11 as its absolute value, the subgroup of M^* generated by $c_{1,2}$ over $A=\boldsymbol{Z}[H]$ has 11 as its degree to Y^*. So $c_{1,2}$ is a free base of M^* over A. Then from Lemma 2 follows the pure transcendency of $L/\boldsymbol{Q}$. According to [3] $p_0=\sum_{i=1}^{11}x_i, p_1, p_2, \cdots, p_{10}$ generate L over $\boldsymbol{Q}$, where we take $p_i (i=1,\cdots,10)\in L$ such that

$$c_{1,2}=\sum_{i=1}^{10}p_i\gamma^i \quad\text{and}\quad \gamma=\cos 2\pi/10+i\sin 2\pi/10\,. \tag{27}$$

REMARK. When Professor E. Artin came to Japan in 1955, he conjectured the pure transcendency of $L/\boldsymbol{Q}$ for every prime p. Then he asked the reason why the author did not try to apply his method in [3] for $p=11$ or 13. At that time the author thought it quite difficult even for $p=11$.

The author does not know whether the new obtained method stated in this paper be effective for other primes $p>11$. But at least it has made clear, the author thinks, the reason why it is difficult for greater values of p, e.g. $p=13$, 17, 19, or 23. Roughly speaking, if $p>11$, some of the following three facts will happen, that $(p-1)/2$ is not a prime, that the behavior of units of $(p-1)$-th cyclotomic field J mod (2) is not known, and especially that we do not have a good characterization for $\pi([M])=0$.

Even if one, in future, could find a prime $p>11$ for which $A\ncong M$, of course it would not give any inconvenience to one who has the affirmative conjecture to the proper problem concerning the pure transcendency of $L/\boldsymbol{Q}$, because $M\cong A$ as A-modules is only a sufficient, but not a necessary condition for it.

Nagoya University

Bibliography

[1] H. Kuniyoshi, On a problem of Chevalley, Nagoya Math. J., **8** (1955), 65–68.

[2] W. Kuyk, Over het omkeerprobleem van de Galoistheorie, Amsterdam, 1960.

[3] K. Masuda, On a problem of Chevalley, Nagoya Math. J., **8** (1955), 59–63.

[4] D. S. Rim, Modules over finite groups, Ann. of Math., **69** (1959), 700–717.

[5] J.-P. Serre, Modules projectifs et espaces fibrés à fibre vectorielle, Seminaire P. Dubreil, 1957/58, Exposé 23, 1–17.