ON PURELY-TRANSCENDENCY OF CERTAIN FIELDS

RYUUKI MATSUDA

(Received March 7, 1964)

Let $K = k(x_1, x_2, \cdots, x_n)$ be a purely transcendental field over k of transcendence degree n. Now we set $\sigma x_j = x_{j+1}$ for any integer j with $1 \leqq j \leqq n - 1$, while $\sigma x_n = x_1$. Then σ induces an automorphism of K over k, which will be also denoted by the same letter σ. If we denote by L the set of all elements of K which remain fixed under σ, then K is a normal extension of degree n with Galois group $\mathfrak{G} = \{I, \sigma, \sigma^2, \cdots, \sigma^{n-1}\}$. Now it arises the question "Is L purely transcendental over k?", which is refered to as "Chevalley's Problem" by Dr. K. Masuda. Let p be the characteristic of k and assume that p does not divide n. For any positive integer n less than or equal to 7, he proved that L is purely transcendental over k [1]. On the same Journal of Nagoya, Dr. Kuniyoshi proved the purely-transcendency for the case of nonzero characteristic p and $n = p$ [2]. Let r be any positive integer and $p(>0)$ the characteristic of k. Dr. Kuniyoshi proved further that L is purely transcendental over k, if $n = p^r$ [3].

All the fields treated in this article are assumed to be of characteristic zero.

Already E. Noether showed that L is purely transcendental over k, if the ground field k contains a primitive n-th root ζ. Accordingly one of our concern is to diminish this restriction concerning the ground field. Now we can state the following main theorem:

MAIN THEOREM. *L is purely transcendental over k, if one of the following conditions holds, where l is an odd prime number:*

(i) $n = l^{2r}$ *and k contains a primitive l^r-th root of unity,*

(ii) $n = l^{2r+1}$ *and k contains a primitive l^{r+1}-th root of unity,*

(iii) $n = 2^{2r}$ *and k contains a primitive 2^{r+1}-th root of unity,*

(iv) $n = 2^{2r+1}$ *and k contains a primitive 2^{r+1}-th root of unity.*

As a special case it holds that L is purely transcendental if $n = 3^3$ and k contains primitive 3^2-th roots of unity. But more precisely we can assert the same result under the weaker condition that the ground field contains merely cube roots of unity. Dr. Kuniyoshi conjectures that more generally following fact will hold:

"If $n = p^r$ (p: prime number) and k contains p-th roots of unity, then L is purely transcendental over k."

Our main theorem was first proved by the method of Dr. Kuniyoshi, which was reported at the seminar of Tôhoku Mathematical Institute, and it concerns with certain properties of algebraic groups. In this article we want to treat the same problem in more simplified form.

Before proceeding to the detailed proof, the author wants to express his sincere gratitudes to Dr. Kuniyoshi and Professor Tannaka, who has encouraged him during his study about this subject.

Let k be a field of characteristic zero and n any positive integer, ζ a primitive n-th root of unity and $k' = k(\zeta)$. If $K = k(x_1, x_2, \cdots, x_n)$ is a purely transcendental extension of k of transcendence degree n, the cyclic permutation $\sigma: x_j \to x_{j+1}$ induces naturally an automorphism of K over k. The suffices of the letters x_j are considered modulo n. Let L be a field consisting of all elements of K which are left fixed under σ. The cyclic permutation naturally induces an automorphism of $K' = k'(x_1, x_2, \cdots, x_n)$ over k'. We will denote this also by σ. Let L' be the fixed field in K' of σ. K is a Galois extension field over L of degree n and the Galois group $\mathfrak{G}$ is generated by σ. Similarly K' is a Galois extension over L' of degree n, and $\mathfrak{G}$ is regarded also as its Galois group. As K is purely transcendental over k, K and k' are linearly disjoint over k. So if we denote the degree of fields by$[\ :\ ]$, $[K' : K] = [L(\zeta) : L] = [k' : k]$. Since any element of $L(\zeta)$ is invariant under σ, $L(\zeta)$ is contained in L'. We have $L(\zeta) = L'$ by the following formula.

$$[L' : L(\zeta)] = \frac{[K' : L]}{[K' : L'][L(\zeta) : L]} = \frac{[K' : K][K : L]}{[L(\zeta) : L][K' : L']} = 1.$$

Therefore K, L', k' are all Galois extensions over K, L and k respectively. Let G be the Galois group of K' with respect to K and τ any element of G. If we restrict τ to L', it defines an automorphism of L' over L. So G can be regarded as the Galois group of L' over L. Similarly G is regarded as the Galois group of k' with respect to k.

If a is any element of L', we will denote $[L(a) : L]$ by $\iota(a)$. Let $\{a_1, a_2, \cdots, a_t\}$ be a set of elements of L' satisfying a condition $\sum_{j=1}^{t} \iota(a_j) = n$, and let $\{a_j, a_j', a_j'' \cdots, a^{(\iota(a_j)-2)}, a_j^{(\iota(a_j)-1)}\}$ be a set of all elements which are conjugate with one another with respect to L, for j such that $1 \leqq j \leqq t$. If a subfield $k'(a_1, a_1', \cdots, a_1^{(\iota(a_1)-1)}, a_2, a_2', \cdots, a_2^{(\iota(a_2)-1)}, \cdots a_t, a_t', \cdots, a_t^{(\iota(a_t)-1)})$ of L' coincides with L', the set $\{a_1, a_2, \cdots, a_t\}$ of elements of L' is called a system of primitive generators of L' with respect to k'. Let L be purely transcendental over k and $\{a_1, a_2, \cdots, a_n\}$ be a purely-transcendence basis of L. Then the set $\{a_1, a_2, \cdots, a_n\}$ is clearly a system of primitive generators of L' with respect to k'. However, if L' has a system of primitive generators, L is

purely transcendental over k [1].

PROPOSITION 1. *Let l be an odd prime number and r any positive integer and $n = l^{2r}$. Let k be a field of characteristic zero containing a primitive l^r-th root of unity, and $K = k(x_1, x_2, \cdots, x_n)$ a purely transcendental extension over k of transcendence degree n. If we define an automorphism σ of K over k by $\sigma x_j = x_{j+1}$, the invariant field L of σ is purely transcendental over k of transcendence degree n.*

PROOF. Let $\bar{k}$ be any overfield of k, $\overline{K} = \bar{k}(x_1, x_2, \cdots, x_n)$ a purely transcendental extension over $\bar{k}$ of transcendence degree n. Then $K = k(x_1, x_2, \cdots, x_n)$ is purely transcendental over k of transcendence degree n. For a primitive n-th root ζ we put $k' = k(\zeta)$, $\bar{k}' = \bar{k}(\zeta)$, $K' = k'(x_1, x_2, \cdots, x_n)$ $\overline{K}' = \bar{k}'(x_1, x_2, \cdots, x_n)$. Let $L, \overline{L}, L'$ and $\overline{L}'$ be the invariant fields of $\sigma: x_j \to x_{j+1}$ in $K, \overline{K}$, K' and $\overline{K}'$ respectively. Now if L' has a system of primitive generators with respect to k', we can easily construct a system of primitive generators of $\overline{L}'$ with respect to $\bar{k}'$. Hence, to prove the purely-transcendency of $\overline{L}$ over $\bar{k}$, it is enough to show that L is purely transcendental over k.

Let Q be the field of all rational numbers, and ζ a primitive n-th root of unity. Then $\eta = \zeta^{l^r}$ is a primitive l^r-th root. By a remark just mentioned we may assume the basic field k to be $Q(\eta)$. The monic irreducible equation over $k = Q(\eta)$ satisfied by ζ being $X^{l^r} - \eta = 0$, it follows that the conjugates of ζ over K(and also over L, and k) are $\zeta, \zeta^{l^r+1}, \zeta^{2l^r+1}, \zeta^{3l^r+1}, \cdots, \zeta^{(l^r-1)l^r+1}$. So that the Galois group G of K' with respect to K is a cyclic group and $\tau: \zeta \to \zeta^{l^r+1}$ is a generator of it. If we put $y_i = \sum_{j=1}^{n} \zeta^{ij} x_j$ $(1 \leqq i \leqq n)$,

then

$$(1) \qquad \sigma y_i = \sum_{j=1}^{n} \zeta^{ij} x_{j+1} = \zeta^{n-i} y_i,$$

and

$$(2) \qquad \tau y_i = \sum_{j=1}^{n} \zeta^{(l^r+1)ij} x_j = y_{(l^r+1)i}.$$

Next we will define a system of elements as follows:

$$a_0 = y_n,$$

$$a_{r,d} = \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{il^r+1}\right)^d} \qquad (d = 1, 2, 3, \cdots, l^r - 1),$$

$$a_{i,m} = \frac{y_{l^i m}}{\left(\prod_{j=0}^{l^i-1} y_{jl}{}^{2r-i} + 1\right)^m} \quad (i = 1, 2, \cdots, r-1.\ 1 \leqq m \leqq l^r - 1, (m, l) = 1),$$

$$a_1 = y_1^2 y_{2l^r+1} y_{3l^r+1} y_{4l^r+1} \cdots y_{(l^r-1)l^r+1},$$

$$a_v = \frac{y_v}{y_1^v} \qquad (2 \leqq v \leqq l^r - 1,\ (v, l) = 1).$$

Using the formula (1) we see easily,

$$\sigma a_0 = \sigma y_n = \zeta^{n-n}\ y_n = a_0,$$

$$\sigma a_{r,d} = \sigma \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{jl^{2r-i}+1}\right)^d} = \frac{\zeta^{n-l^r d} y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} \left(\zeta^{n-(jl^{2r-i}+1)}\ y_{jl^{2r-i}+1}\right)\right)^d}$$

$$= \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{jl^{2r-i}+1}\right)^d} = a_{r,d},$$

$$\sigma a_{i,m} = \sigma \frac{y_{l^i m}}{\left(\prod_{j=0}^{l^i-1} y_{jl^{2r-i}+1}\right)^m} = \frac{\zeta^{n-l^i m}\ y_{l^i m}}{\left(\prod_{j=0}^{l^i-1} (\zeta^{n-(jl^{2r-i}+1)}\ y_{jl^{2r-i}+1})\right)^m}$$

$$= \frac{y_{l^i m}}{\left(\prod_{j=0}^{l^i-1} y_{jl^{2r-i}+1}\right)^m} = a_{i,m},$$

$$\sigma a_1 = \sigma(y_1^2 y_{2l^r+1} y_{3l^r+1} \cdots y_{(l^r-1)l^r+1})$$

$$= (\zeta^{2(n-1)} \zeta^{n-(2l^r+1)} \zeta^{n-(3l^r+1)} \cdots \zeta^{n-((l^r-1)l^r+1)})(y_1^2 y_{2l^r+1} y_{3l^r+1} \cdots y_{(l^r-1)l^r+1})$$

$$= y_1^2 y_{2l^r+1} y_{3l^r+1} \cdots y_{(l^r-1)l^r+1} = a_1,$$

$$\sigma a_v = \sigma \frac{y_v}{y_1^v} = \frac{\zeta^{n-v} y_v}{\zeta^{v(n-1)} y_1^v} = \frac{y_v}{y_1^v} = a_v.$$

Consequently these a belong to L'.

We have then by utilizing the formula (2),

$$\tau a_0 = \tau y_n = y_{(l^r+1)n} = y_n = a_0.$$

Since the Galois group G of L' with respect to L is generated by τ, we see $a_0 \in L$, whence

$$\iota(a_0) = [L(a_0) : L] = 1.$$

$$\tau a_{r,d} = \tau \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{jl^r+1}\right)^d} = \frac{y_{(l^r+1)l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{(l^r+1)(jl^r+1)}\right)^d} = \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{jl^r+1}\right)^d} = a_{r.d}\,.$$

This means $a_{r,d} \in L$, and so $\iota(a_{r,d}) = [L(a_{r,d}) : L] = 1$.

Now it is seen without difficulty that all elements of G which leave $a_{i,m}$ fixed make a cyclic group $[\tau^{l^{r-i}}]$ generated by $\tau^{l^{r-i}}$.
By the Galois theory we have

$$\iota(a_{i,m}) = [L(a_{i,m}) : L] = (G : [\tau^{l^{r-i}}]) = \frac{l^r}{l^i} = l^{r-i}\,,$$

where (:) denotes the index of the subgroup.
Now taking the relation (2) in mind we see that only the identity mapping τ^{l^r} of G leaves a_1 fixed. Hence $\iota(a_1) = [L(a_1) : L] = (G : [\tau^{l^r}]) = l^r$. Similarly we have $\iota(a_v) = l^r$. Therefore

$$\begin{aligned}
&\iota(a_0) + \sum_{d=1}^{l^r-1} \iota(a_{r,d}) + \sum_{i=1}^{r-1} \sum_{\substack{1 \le m \le l^r-1 \\ (m,l)=1}} \iota(a_{i,m}) + \iota(a_1) + \sum_{\substack{2 \le v \le l^r-1 \\ (v,l)=1}} \iota(a_v) \\
&\quad = 1 + (l^r - 1) + \sum_{i=1}^{r-1} (l^{r-1}(l-1)\, l^{r-i}) + l^r + (l^{r-1}(l-1)-1)l^r \\
&\quad = l^{2r} \\
&\quad = n\,,
\end{aligned}$$

where $(m, l)=1$ means that m is relatively prime to l.

Let M' be a field obtained by adjoining each a and all its conjugates over L to k'. Then we see without difficulty

$$\begin{aligned}
M'(y_1, y_{l^r+1}, y_{2l^r+1}, \cdots, y_{(l^r-1)l^r+1}) &= M'(y_1, y_2, y_3, \cdots, y_{n-1}, y_n) \\
&= k'(y_1, y_2, \cdots, y_{n-1}, y_n) = k'(x_1, x_2, \cdots, x_{n-1}, x_n) = K'\,.
\end{aligned}$$

Using the theorem of elementary divisors for a cyclic matrix

$$A = \begin{pmatrix}
\overbrace{\begin{matrix} 2 & 0 & 1 \cdots\cdots 1 \end{matrix}}^{l^r} \\
\begin{matrix} 1 & 2 & 0 \cdots\cdots 1 \end{matrix} \\
\begin{matrix} 1 & 1 & 2 \cdots\cdots 1 \end{matrix} \\
\qquad\qquad \ddots \\
\begin{matrix} 0 & 1 & 1 \cdots\cdots 2 \end{matrix}
\end{pmatrix},$$

there exist square matrices P, Q of degree l^r with integral coefficients whose determinants $|P|$, $|Q|$ are ± 1, and

$$P^{-1}AQ^{-1} = B = \begin{pmatrix} b_1 & & & \\ & b_2 & & 0 \\ & & b_3 & \\ & 0 & & \ddots \\ & & & b_{l^r} \end{pmatrix}$$

is diagonal, where the elements b_i are integers satisfying $b_{i+1} \equiv 0\ (b_i)$, i.e. b_i divides b_{i+1}. Let p_{ij} be the (i,j) element of the matrix P and q_{ij} the (i,j) element of Q. Let next Ω be an algebraically closed overfield of K', and denote by $\Omega^\times$ the multiplicative group consisting of all non-zero elements of Ω. Let further $H = \underbrace{\Omega^\times \times \Omega^\times \times \cdots \times \Omega^\times}_{l^r}$ be a direct product of l^r groups $\Omega^\times$ and $Y_1, Y_2, \cdots, Y_{l^r}$, l^r variables. Then $f_Q(Y_1, Y_2, Y_3, \cdots, Y_{l^r}) = \left(\prod_{j=1}^{l^r} Y_j^{q_{1j}}, \prod_{j=1}^{l^r} Y_j^{q_{2j}}, \prod_{j=1}^{l^r} Y_j^{q_{3j}}, \cdots, \prod_{j=1}^{l^r} Y_j^{q_{l^r j}}\right)$ determines a group homomorphism f_Q of H into H. Similariy we define f_A, f_P and f_B. It is easy to see by the fact $A = PBQ$ that it holds $f_A = f_P f_B f_Q$. As the matrix B is diagonal, the order of the kernel of f_B, that is the group $f_B^{-1}\underbrace{(1, 1, 1, \cdots, 1)}_{l^r}$, is $\prod_{j=1}^{l^r} (\text{abs. } b_j) = \text{abs.}|B|$ $= \text{abs.}|A| = l^{2r} = n$, where (abs.) denotes the absolute value of a number. $|A| = n$ is easily verified directly. As P, Q are unimodular, f_P, f_Q are automorphisms. We see therefore the kernel of f_A is of order n. And we conclude as follows:

$$\text{The kernel of } f_A = \{(\zeta^\alpha, \zeta^{(l^r+1)\alpha}, \zeta^{(2l^r+1)\alpha}, \zeta^{(3l^r+1)\alpha}, \cdots \cdots, \zeta^{((l^r-1)l^r+1)\alpha});\ \alpha = 1, 2, 3, \cdots, n\}.$$

A set $\{a_1, a_1', a_1'', \cdots, a_1^{(l^r-1)}\}$ of all conjugates of a_1 over L is obviously algebraically independent over k'. So that if we put $\mathfrak{A} = k'(y_1, y_{l^r+1}, y_{2l^r+1}, \cdots, y_{(l^r-1)l^r+1})$ and $\mathfrak{B} = k'(a_1, a_1', a_1'', \cdots, a_1^{(l^r-1)})$, $\mathfrak{A}$ is an algebraic extension field of $\mathfrak{B}$. Now we will take any conjugate $(z_1, z_{l^r+1}, z_{2l^r+1}, \cdots, y_{(l^r-1)l^r+1})$ of an ordered tuple $(y_1, y_{l^r+1}, y_{2l^r+1}, y_{3l^r+1}, \cdots, y_{(l^r-1)l^r+1})$ over $\mathfrak{B}$.

Since $y_1^2 y_{l^r+1}^0 y_{2l^r+1}^1 y_{3l^r+1}^1 \cdots y_{(l^r-1)l^r+1}^1 = a_1$, we have $z_1^2 z_{l^r+1}^0 z_{2l^r+1}^1 z_{3l^r+1}^1 \cdots z_{(l^r-1)l^r+1}^1 = a_1$. Hence $\left(\frac{z_1}{y_1}\right)^2 \left(\frac{z_{l^r+1}}{y_{l^r+1}}\right)^0 \left(\frac{z_{2l^r+1}}{y_{2l^r+1}}\right)^1 \left(\frac{z_{3l^r+1}}{y_{3l^r+1}}\right)^1 \cdots \left(\frac{z_{(l^r-1)l^r+1}}{y_{(l^r-1)l^r+1}}\right)^1 = 1$. By the similar considerations to 2nd, 3rd $\cdots$, and l^r-th components, it follows

that $\left(\frac{z_1}{y_1}, \frac{z_{l^r+1}}{y_{l^r+1}}, \frac{z_{2l^r+1}}{y_{2l^r+1}}, \cdots, \frac{z_{(l^r-1)l^r+1}}{y_{(l^r-1)l^r+1}}\right)$ belongs to the kernel of f_A. Accordingly $z_{jl^r+1} = \zeta^{(jl^r+1)\alpha_j} y_{jl^r+1}$ $(j=0, 1, 2, \cdots, l^r-1)$, for certain α's. Consequently $\mathfrak{A}$ is a normal extension of $\mathfrak{B}$ of degree less than or equal to n. Since $\mathfrak{A} \subset K'$, $\mathfrak{B} \subset M'$, $\mathfrak{B}(y_1, y_{l^r+1}, y_{2l^r+1}, \cdots, y_{(l^r-1)l^r+1}) = \mathfrak{A}$ and $M'(y_1, y_{l^r+1}, y_{2l^r+1}, \cdots, y_{(l^r-1)l^r+1}) = K'$, we see $[K' : M'] \leqq [\mathfrak{A} : \mathfrak{B}]$. Hence we have $M' = L'$, because $M' \subset L' \subset K'$, and $[K' : L'] = n$.

Therefore these a are a system of primitive generators of L' with respect to k'. This completes the proof of Propositi n 1.

PROPOSITION 2. *Let l be an odd prime number and r any positive integer and $n = l^{2r+1}$. Let k be a field of characteristic zero containing a primitive l^{r+1}-th root of unity. If $K = k(x_1, x_2, x_3, \cdots, x_n)$ is a purely transcendental extension of k of transcendence degree n, the fixed field L of the automorphism $\sigma : x_j \to x_{j+1}$ is purely transcendental over k.*

PROOF. Let ζ be a primitive n-th root of unity. Then $\eta = \zeta^{l^r}$ is primitive l^{r+1}-th root of unity. As we pointed out at the beginning of the proof of Proposition 1, it is enough to prove the theorem for the case $k = Q(\eta)$. The monic irreducible equation of ζ over $k = Q(\eta)$ is $X^{l^r} - \eta = 0$. Hence the conjugates of ζ over K are $\zeta, \zeta^{l^{r+1}+1}, \zeta^{2l^{r+1}+1}, \zeta^{3l^{r+1}+1}, \cdots, \zeta^{(l^r-1)l^{r+1}+1}$. It follows that the automorphism $\tau : \zeta \to \zeta^{l^{r+1}+1}$ is a generator of the Galois group G of K' with respect to K.

Putting $y_i = \sum_{j=1}^{n} \zeta^{ij} x_j$, we see

(1′) $\sigma y_i = \zeta^{n-i} y_i$,

(2′) $\tau y_i = y_{(l^{r+1}+1)i}$.

We will define the system a as follows.

$$a_0 = y_n,$$

$$a_{r,d} = \frac{y_{l^r d}}{\left(\prod_{j=0}^{l^r-1} y_{jl^{r+1}+1}\right)^d} \qquad (d = 1, 2, 3, \cdots, l^{r+1}-1),$$

$$a_{i,m} = \frac{y_{l^i m}}{\left(\prod_{j=0}^{l^i-1} y_{jl^{2r+1-i}+1}\right)^m} \qquad \begin{pmatrix} i = 1, 2, 3, \cdots, r-1 \\ 1 \leqq m \leqq l^{r+1}-1, \quad (m, l) = 1 \end{pmatrix},$$

$$a_1 = y_1^{l+1} y_{l^{r+1}+1}^{l-1} y_{2l^{r+1}+1}^{l} y_{3l^{r+1}+1}^{l} \cdots\cdots y_{(l^r-1)l^{r+1}+1}^{l},$$

$$a_v = \frac{y_v}{y_1^v} \qquad (2 \leqq v \leqq l^{r+1} - 1,\ (v, l) = 1).$$

Using the formula (1′) we see easily that $\sigma a = a$ for each a. Consequently these a belong to L'.

Using the formula (2′) we have,

$$\tau a_0 = a_0,$$

$$\tau a_{r,d} = a_{r,d}.$$

Hence

$$\iota(a_0) = [L(a_0) : L] = 1,$$

$$\iota(a_{r,d}) = [L(a_{r,d}) : L] = 1.$$

The subgroup of G which leaves $a_{i,m}$ fixed is found without difficulty to be a cyclic group $[\tau^{l^{r-i}}]$. This brings $\iota(a_{i,m}) = (G : [\tau^{l^{r-i}}]) = l^{r-i}$. We see at once that the only element of G which leaves a_1 fixed is the identity mapping I, and the only element which leaves a_v invariant is also I.

Accordingly it follows $\iota(a_1) = \iota(a_v) = l^r$.

Therefore

$$\iota(a_0) + \sum_{d=1}^{l^{r+1}-1} \iota(a_{r,d}) + \sum_{i=1}^{r-1} \sum_{\substack{1 \leqq m \leqq l^{r+1}-1 \\ (m,\, l)=1}} \iota(a_{i,m}) + \iota(a_1) + \sum_{\substack{2 \leqq v \leqq l^{r+1}-1 \\ (v,\, l)=1}} \iota(a_v)$$

$$= l^{2r+1}$$

$$= n.$$

Let M′ be a field obtained by adjoining each a and all its conjugates over L to k'. Then $M'(y_1, y_{l^{r+1}+1}, y_{2l^{r+1}+1}, \cdots, y_{(l^r-1)l^{r+1}+1}) = k'(y_1, y_2, y_3, \cdots, y_n) = K'$. If we make an endomorphism f_A of a multiplicative group $H = \underbrace{\Omega^\times \times \Omega^\times \times \cdots \times \Omega^\times}_{l^r}$ from a cyclic matrix

$$A = \begin{pmatrix} \overbrace{\begin{matrix} l+1 & l-1 & l & l & \cdots & l \\ l & l+1 & l-1 & l & \cdots & l \end{matrix}}^{l^r} \\ \ddots \\ \begin{matrix} l-1 & l & l & l & \cdots & l+1 \end{matrix} \end{pmatrix},$$

we see as in the proof of Proposition 1 that the kernel of f_A is

$\{(\zeta^{\alpha}, \zeta^{(l^{r+1}+1)\alpha}, \zeta^{(2l^{r+1}+1)\alpha}, \zeta^{(3l^{r+1}+1)\alpha}, \cdots, \zeta^{((l^r-1)l^{r+1}+1)\alpha}); \alpha = 1, 2, 3, \cdots, n\}$.

$\mathfrak{A}=k'(y_1, y_{l^{r+1}+1}, y_{2l^{r+1}+1}, \cdots, y_{(l^r-1)l^{r+1}+1})$ is an algebraic extension field of $\mathfrak{B}=k'(a_1, a_1', a'', \cdots, a_1^{(l^r-1)})$. For any conjugate $(z_1, z_{l^{r+1}+1}, z_{2l^{r+1}+1}, z_{3l^{r+1}+1}, \cdots, z_{(l^r-1)l^{r+1}+1})$ with respect to $\mathfrak{B}$ of an ordered tuple $(y_1, y_{l^{r+1}+1}, y_{2l^{r+1}+1}, \cdots, y_{(l^r-1)l^{r+1}+1})$ we can prove that $\left(\frac{z_1}{y_1}, \frac{z_{l^{r+1}+1}}{y_{l^{r+1}+1}}, \frac{z_{2l^{r+1}+1}}{y_{2l^{r+1}+1}}, \frac{z_{3l^{r+1}+1}}{y_{3l^{r+1}+1}}, \cdots, \frac{z_{(l_i-1)l^{r+1}+1}}{y_{(l^r+1)l^{r+1}+1}}\right)$ belongs to the kernel of f_A. So, $z_{jl^{r+1}+1} = \zeta^{(jl^{r+1}+1)\alpha_j} y_{jl^{r+1}+1}$ $(j = 0, 1, 2, 3, \cdots, l^r-1)$ for certain integers α's. This shows that $\mathfrak{A}$ is a normal extension of $\mathfrak{B}$ of degree less than or equal to n. Since $n = [K' : L'] \leqq [K' : M'] \leqq [\mathfrak{A} : \mathfrak{B}] \leqq n$, we have $L' = M'$.

Therefore these a make a system of primitive generators of L' with respect to k'. This completes the proof of Proposition 2.

PROPOSITION 3. *Let r be a positive integer greater than or equal to 2(*) and $n=2^{2r}$. Let k be a field of characteristic zero containing a primitive 2^{r+1}-th root of unity and $K=k(x_1, x_2, x_3, \cdots, x_n)$ be a purely transcendental extension of k transcendence degree n. Then the invariant field L in K under an automorphism $\sigma : x_j \to x_{j+1}$ is purely transcendental over k.*

PROOF. Let ζ be a primitive n-th root of unity. Then $\eta=\zeta^{2^{r-1}}$ is a primitive 2^{r+1}-th root of unity. We may assume the basic field is $k = Q(\eta)$. Since the monic irreducible equation of ζ over $k = Q(\eta)$ is $X^{2^{r-1}} - \eta = 0$, the conjugates of ζ over K are

$$\zeta, \zeta^{2^{r+1}+1}, \zeta^{2\cdot 2^{r+1}+1}, \zeta^{3\cdot 2^{r+1}+1}, \cdots, \zeta^{(2^{r-1}-1)\cdot 2^{r+1}+1}.$$

So that the Galois group G of K' with respect to K is generated by $\tau : \zeta \to \zeta^{2^{r+1}+1}$.

Putting $y_i = \sum_{j=1}^{n} \zeta^{ij} x_j$, we have easily

(1″) $\sigma y_i = \zeta^{n-i} y_i$,

(2″) $\tau y_i = y_{(2^{r+1}+1)i}$.

We will now define the system a as follows. a_0 is simply defined by

$$a_0 = y_n .$$

Obviously there exists a positive integer b such that $(2^{2r-1} - 2^r + 1)\, b \equiv 1 \pmod{2^{r+1}}$. We will fix such an integer b, and define

(*) When $r=1$, the purely-transcendency has been proved by Dr. Masuda [1], as was already mentioned.

$$a_{r-1,d} = \frac{y_{2^{r-1}d}}{\left(\prod_{j=0}^{2^{r-1}-1} y_{j2^{r+1}+1}\right)^{hd}} \qquad (d = 1, 2, 3, \cdots, 2^{r+1}-1).$$

Next we will fix positive integers c_i for $i=1, 2, \cdots, r-2$, such that $c_i \equiv 2^{r-2} - 2^{r-i-2} \pmod{2^{r-i-1}}$, and define

$$a_{i,m} = \frac{y_{2^i m}}{\left(\prod_{j=0}^{2^i-1} y_{j2^{2r-i}-2^{r+1}c_i+1}\right)^{m}} \qquad \begin{pmatrix} i = 1, 2, 3, \cdots, r-2\,. \\ 1 \leqq m \leqq 2^{r+1}-1, \quad (m, 2) = 1, \end{pmatrix}$$

$$a_1 = y_1^5 y_{2^{r+1}+1}^3 y_{2\cdot 2^{r+1}+1}^4 y_{3\cdot 2^{r+1}+1}^4 \cdots y_{(2^{r-1}-1)\cdot 2^{r+1}+1}^4,$$

$$a_v = \frac{y_v}{y_1^v} \qquad (2 \leqq v \leqq 2^{r+1}-1, \ (v, 2) = 1).$$

Obviously $\sigma a = a$ for each a by (1''). Hence these a belong to L'. We will make use of the formula (2'') for calculating the ι.

$$\tau a_0 = a_0\,,$$

$$\tau a_{r-1,d} = a_{r-1,d} \quad \text{immediately.}$$

Hence

$$\iota(a_0) = 1\,,$$

$$\iota(a_{r-1,d}) = 1\,.$$

All elements of G which leave $a_{i,m}$ invariant make a group $[\tau^{2^{r-i-1}}]$ generated by $\tau^{2^{r-i-1}}$, accordingly $\iota(a_{i,m}) = (G : [\tau^{2^{r-i-1}}]) = 2^{r-i-1}$.
Since only element of G which leaves a_1 fixed is the identity mapping,

$$\iota(a_1) = 2^{r-1}\,.$$

Quite similarly

$$\iota(a_v) = 2^{r-1}\,.$$

Therefore

$$\iota(a_0) + \sum_{d=1}^{2^{r+1}-1} \iota(a_{r-1,d}) + \sum_{i=1}^{r-2} \sum_{\substack{1 \leqq m \leqq 2^{r+1}-1 \\ (m,2)=1}} \iota(a_{i,m}) + \iota(a_1) + \sum_{\substack{2 \leqq v \leqq 2^{r+1}-1 \\ (v,2)=1}} \iota(a_v)$$

$$= 2^{2r}$$

$$= n\,.$$

Let M' be a field obtained by adjoining each a and all its conjugates

with respect L to k'. Then $M'(y_1, y_{2^{r+1}+1}, y_{2\cdot 2^{r+1}+1}, y_{3\cdot 2^{r+1}+1}, \cdots, y_{(2^{r-1}-1)\cdot 2^{r+1}+1}) = K'$. $\mathfrak{A} = k'(y_1, y_{2^{r+1}+1}, y_{2\cdot 2^{r+1}+1}, \cdots, y_{(2^{r-1}-1)\cdot 2^{r+1}+1})$ is an algebraic extension of $\mathfrak{B} = k'(a_1, a_1', a_1'', \cdots, a_1^{(2^{r+1}-1)})$. Taking $|A| = n$ into account, where

$$A = \begin{pmatrix} \overbrace{\begin{matrix} 5 & 3 & 4 & 4 & \cdots & 4 \\ 4 & 5 & 3 & 4 & \cdots & 4 \\ & & \ddots & & & \\ 3 & 4 & 4 & 4 & \cdots & 5 \end{matrix}}^{2^{r-1}} \end{pmatrix}$$

is a cyclic matrix, $\mathfrak{A}$ proves to be a normal extension of $\mathfrak{B}$ of degree less than or equal to n.

But, as $n = [K' : L'] \leqq [K' : M'] \leqq [\mathfrak{A} : \mathfrak{B}] \leqq n$, we have $L' = M'$.

Therefore these a make a system of primitive generators of L' with respect to k'.

PROPOSITION 4. *Let r be any positive integer and $n = 2^{2r+1}$ and k a field of characteristic zero containing a primitive 2^{r+1}-th root. The invariant field L of an automorphism $\sigma : x_j \to x_{j+1}$ of K is purely transcendental over k, where $K = k(x_1, x_2, \cdots, x_n)$ is a purely transcendental extension over k of transcendence degree n.*

PROOF. Let ζ be a primitive n-th root of unity. Then $\eta = \zeta^{2^r}$ is a primitive 2^{r+1}-th root of unity. We may assume $k = Q(\eta)$. Since the monic irreducible equation of ζ over $k = Q(\eta)$ is $X^{2^r} - \eta = 0$, the conjugates of ζ with respect to k are

$$\zeta, \zeta^{2^{r+1}+1}, \zeta^{2\cdot 2^{r+1}+1}, \zeta^{3\cdot 2^{r+1}+1}, \cdots, \zeta^{(2^r-1)\cdot 2^{r+1}+1}.$$

So that the Galois group G of K' with respect to K is generated by $\tau : \zeta \to \zeta^{2^{r+1}+1}$.

Putting now $y_i = \sum_{j=1}^{n} \zeta^{ij} x_j$, we have

(1‴) $$\sigma y_i = \zeta^{n-i} y_i,$$

(2‴) $$\tau y_i = y_{(2^{r+1}+1)i}.$$

We will define a system a as follows,

$$a_0 = y_n,$$

$$a_{r,d}=\frac{y_{2^r d}}{\left(\prod_{j=0}^{2^r-1} y_{j2^{r+1}+1}\right)^{bd}} \qquad (d=1,2,3,\cdots,2^{r+1}-1),$$

where b is a fixed positive integer satisfying $(2^{2r}-2^r+1)\,b\equiv 1 \pmod{2^{r+1}}$,

$$a_{i,m}=\frac{y_{2^i m}}{\left(\prod_{j=0}^{2^i-1} y_{j2^{2r-i+1}-2^{r+1}c_i+1}\right)^{m}} \qquad \begin{pmatrix} i=1,2,3,\cdots,r-1\,. \\ 1\leqq m\leqq 2^{r+1}-1,\ (m,2)=1 \end{pmatrix},$$

where the c_i are fixed positive integers satisfying $c_i\equiv 2^{r-1}-2^{r-i-1} \pmod{2^{r-i}}$, for $i=1,2,3,\cdots,r-1$,

$$a_1=y_1^3 y_{2^{r+1}+1}^1 y_{2\cdot 2^{r+1}+1}^2 y_{3\cdot 2^{r+1}+1}^2\cdots y_{(2^r-1)\cdot 2^{r+1}+1}^2,$$

$$a_v=\frac{y_v}{y_1^v} \qquad (2\leqq v\leqq 2^{r+1}-1,\quad (v,2)=1).$$

These a are contained in L'.

Now
$$\iota(a_0)=1,$$
$$\iota(a_{r,d})=1,$$
$$\iota(a_{i,m})=2^{r-i},$$
$$\iota(a_1)=2^r,$$
$$\iota(a_v)=2^r.$$

Hence

$$\iota(a_0)+\sum_{d=1}^{2^{r+1}-1}\iota(a_{r,d})+\sum_{i=1}^{r-1}\sum_{\substack{1\leqq m\leqq 2^{r+1}-1\\(m,2)=1}}\iota(a_{i,m})+\iota(a_1)+\sum_{\substack{2\leqq v\leqq 2^{r+1}-1\\(v,2)=1}}\iota(a_v)$$
$$=2^{2r+1}$$
$$=n.$$

Taking the relation $|A|=n$ into account, where

$$A=\begin{pmatrix} \overbrace{\begin{matrix} 3 & 1 & 2 & 2 & \cdots & 2 \\ 2 & 3 & 1 & 2 & \cdots & 2 \\ & & & & & \\ & & & & & \\ 1 & 2 & 2 & 2 & \cdots & 3 \end{matrix}}^{2^r} \end{pmatrix}$$

is a cyclic matrix, a field M' obtained by adjoining each a and all its conjugates with respect to L to k' coincides with L'.

REMARK. Let k be a field of characteristic zero containing a primitive 3rd root of unity and $K=k(x_1, x_2, x_3, \cdots, x_{27})$ a purely transcendental extension over k of transcendence degree 27. Then the fixed field of an automorphism $\sigma: x_j \to x_{j+1}$ of K is purely transcendental over k.

PROOF. Let ζ be a primitive 27-th root of unity. Then $\eta = \zeta^9$ is a primitive 3rd root of unity. We may assume $k=Q(\eta)$. The monic irreducible equation of ζ over $k = Q(\eta)$ is $X^9-\eta = 0$, hence the Galois group G of K' with respect to K is generated by $\tau: \zeta \to \zeta^4$.

Putting $$y_i = \sum_{j=1}^{27} \zeta^{ij} x_j, \qquad \text{we see}$$

$$\sigma y_i = \zeta^{27-i} y_i,$$

$$\tau y_i = y_{4i}.$$

We will now define a's as follows.

$$a_0 = y_{27},$$

$$a_1 = y_4 y_{10} y_{13},$$

$$a_2 = \frac{y_2}{y_1^2},$$

$$a_3 = \frac{y_9}{\prod_{j=0}^{8} y_{3j+1}},$$

$$a_4 = \frac{y_{18}}{\left(\prod_{j=0}^{8} y_{3j+1}\right)^2},$$

$$a_5 = \frac{y_3}{y_1 y_{10} y_{19}},$$

$$a_6 = \frac{y_6}{(y_1 y_{10} y_{19})^2}.$$

These a are certainly contained in L'.

Now, $$\iota(a_0) = 1,$$

$$\iota(a_1) = 9,$$

$$\iota(a_2) = 9,$$

$$\iota(a_3) = 1,$$

$$\iota(a_4) = 1,$$

$$\iota(a_5) = 3,$$

$$\iota(a_6) = 3.$$

Therefore $\sum_{j=0}^{6} \iota(a_j) = 27.$

Thus

$$9\left\{\begin{vmatrix} 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ & & & & \ddots & & & & \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{vmatrix}\right. = 27$$

completes the proof of our remark.

REFERENCES

[1] K. MASUDA, On a problem of Chevalley, Nagoya Math. Journ., 8(1955), 59-63.
[2] H. KUNIYOSHI, On a problem of Chevalley, Nagoya Math. Journ., 8(1955), 65-67.
[3] H. KUNIYOSHI, On purely-transcendency of a certain field, Tôhoku Math. Journ., 6 (1954), 101-108.

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY.