ON A PROBLEM OF CHEVALLEY

KATSUHIKO MASUDA

Recently Prof. Chevalley in Nagoya suggested to the author the following problem: Let k be a field, $K_5 = k(x_1, x_2, x_3, x_4, x_5)$ be a purely transcendental extension field (of transcendental degree 5) of k, s_5 be the cyclic permutation of x: $s_5 x_1 = x_2 s_5 x_2 = x_3 s_5 x_3 = x_4 s_5 x_4 = x_5 s_5 x_5 = x_1$, and let L_5 be the field of invariants of s_5 in K_5. Is L_5 then purely transcendental over k or not? When the characteristic p of k is not equal to 5, it is answered in the following positively. When the characteristic p of k is equal to 5, it is answered also positively by Mr. Kuniyoshi's result in [2].

Now let $K_n = k(x_1, x_2, x_3, \ldots, x_n)$ be a purely transcendental extension field (of transcendental degree n) of k, s_n be the cyclic permutation of x: $s_n x_1 = x_2$ $s_n x_2 = x_3 \ldots s_n x_n = x_1$, and let L_n be the field of invariants of s_n in K_n. We suppose from now on throghout the present article that n is not divisible by the characteristic p of k. If the ground field k involves a primitive n-th root ζ_n of 1, we can see easily that L_n is purely transcendental over k. From this fact we obtain in the following that existence of certain sets of primitive generators of $L_n(\zeta_n)$ over $k(\zeta_n)$ (the definition is shown in the following) is a necessary and sufficient condition for L_n to be purely transcendental over k, and the existence of such sets of primitive generators are shown for every case of $n \leqq 7$ through calculations on factor sets[1]. It looks that a more arithmetical approach will be necessary to solve the problem with reference to general n.

1. Let $k'_n = k(\zeta_n)$, $K'_n = K_n(\zeta_n)$ and $\mathfrak{G}$ be the Galois group of k' over k. We omit all n as subscripts throughout in the following, unless indispensable. Let L' denote the field of invariants of s in K'. K and K' are clearly Galois extension fields over L and L' of the same rank n respectively. Their Galois groups are generated by the automorphism induced by s. We do not distin-

Received June 1, 1954.

1) Cf. [1] and [3]. Hasse factor sets defined in [3] without the supposition that the absolutely irreducible representations of Galois groups are obtained in the ground field has close relations to the problem of the pure transcendency of L_n over k.

guish these two Galois groups and the cyclic permutation group of x generated by s and denote them by same $\mathfrak{G}$. As K is purely transcendental over k, K and k' are linearly disjoint over k[2] and $[K' : K] = [L(\zeta) : L] = [k' : k]$. The restrictions of the Galois group of K' over K into $L(\zeta)$ and k' are the Galois group of $L(\zeta)$ over L and the Galois group of k' over k respectively. We do not distinguish these three Galois groups and denote them by same $\mathfrak{G}$. Then we can see easily from the Galois theory that $L(\zeta) \cap K = L$ and $[K : L] = [K' : L(\zeta)] = [K' : L']$. As $L(\zeta) \subset L'$, we obtain now the following Lemma.

LEMMA 1. *$L' = L(\zeta)$, $L' \cap K = L$ and $[L' : L] = [k' : k]$.*

Let $y_j = \sum_{i=1}^{n} \zeta^{-ij} x_i$ and $c_{j,k} = y_j y_k / y_{\overline{j+k}}$ for $j,k = 1, 2, \ldots, n$, where we denote by $\overline{j+k}$ the integer determined uniquely by $\overline{j+k} \equiv j+k \bmod n$ and $1 \leqq \overline{j+k} \leqq n$. $c_{j,k}$ belongs clearly to L'. Let M' denote the field generated over k' by all $c_{j,k}$ for $j,k = 1, 2, \ldots, n$. From $c_{i,j} = c_{1,j} c_{1,\overline{j+1}} \ldots c_{1,\overline{j+i}} / c_{1,1} c_{1,2} \ldots c_{1,i-1}$ it follows easily that $M' = k'(c_{1,1} c_{1,2}, \ldots, c_{1,n})$ and $y^n \in M'$. As y_1 gives an isomorphic irreducible representation of $\mathfrak{G}$, $[M'(y_1) : M'] = n$. As $y_2, y_3, \ldots, y_n$ can be written as rational combinations of y_1 and $c_{j,k}$ over M' with coefficients in k', $M'(y_1) = M'(y_1, y_2, \ldots, y_n) = K'$. So $[K' : M'] = n$, $M' = L'$ and $L' = k'(c_{1,1}, c_{1,2}, c_{1,3}, \ldots, c_{1,n})$. As the transcendental degree of L' is n, we obtain

THEOREM 1. *L' is purely transcendental over k'.*

We call a set $(a_1, a_2, \ldots, a_t)$ of elements in L' a primitive generating set of L' over $k(\zeta)$, if $\sum_{i=1}^{t} \iota(a_i) = n$ and $L' = k'(a_1, a_1', a_1'', \ldots a_1^{(\iota(a_1)-1)}, a_2, a_2', a_2'', \ldots, a_2^{(\iota(a_2)-1)}, \ldots, a_t, a_t', a_t'', \ldots, a_t^{(\iota(a_t)-1)})$, where we denote by $\iota(a_i)$ the number of (different) conjugate elements of a_i over L. So the number t of elements in such a set is not greater than n, $\iota(a_i) = [L(a_i) : L]$ and $a_i^{(j)} \neq a_{i'}^{(j')}$ except only when $i = i'$, $j = j'$. As $\mathfrak{G}$ is an abelian group, $L(a_i)$ is a Galois extension field of L and $L(a_i, a_i', a_i'', \ldots, a_i^{(\iota(a_i)-1)}) = L(a_i)$. Now we prove the following theorem.

THEOREM 2. *L is purely transcendental over k, if and only if there exists a primitive generating set of $L(\zeta)$ over $k(\zeta)$.*

Proof. (i) Sufficiency. Let $(a_1, a_2, \ldots, a_t)$ be a primitive generating set

[2] Cf. Chap. I. §7 in [4].

of L' over k. Let $k_i' = L(a_i) \cap k'$ for $i = 1, 2, \ldots, t$. Then $L(a_i) = Lk_i'$ and the Galois group of $L(a_i)$ over L is equal to the Galois group of k_i' over k. Let $\omega_{i,1}, \omega_{i,2}, \ldots, \omega_{i,\iota(a_i)}$ be a normal basis of k' over k (accordingly also such one of $L(a_i)$ over L). a_i can be written as $a_i = \sum_{j=1}^{\iota(a_i)} \omega_{i,j} m_{j,i}$ with $m_{j,i}$ in L for $i = 1, 2, \ldots, t$. $a_i, a_i', a_i'', \ldots, a_i^{\iota(a_i)-1}$ are clearly written as bilinear combinations of $\omega_{i,1}, \omega_{i,2}, \ldots, \omega_{i,\iota(a_i)}$ and $m_{1,i}, m_{2,i}, \ldots, m_{\iota(a_i),i}$. As $a_i, a_i', a_i'', \ldots, a_i^{(\iota(a_i)-1)}$ are algebraically independent over k', these forms are as linear combinations of $m_{1,i}, m_{2,i}, \ldots, m_{\iota(a_i),i}$ with coefficients in k' linearly independent. So $m_{1,i}, m_{2,i}, \ldots, m_{\iota(a_i),i}$ can be written as linear combinations of $a_i, a_i', a_i'', \ldots, a_i^{(\iota(a_i)-1)}$ with coefficients in k_i' and so $k'(a, a_i', a_i'', \ldots, a_i^{(\iota(a_i)-1)}) = k'(m_{1,i}, m_{2,i}, \ldots, m_{\iota(a_i),i})$. Thus we obtain $L' = k'(a_1, a_1', a_1'', \ldots, a_1^{(\iota(a_1)-1)}, a_2, a_2', a_2'', \ldots, a_2^{(\iota(a_2)-1)}, \ldots, a_t, a_t', a_t'', \ldots, a_t^{(\iota(a_t)-1)}) = k'(m_{1,1}, m_{2,1}, \ldots, m_{\iota(a_1),1}, m_{1,2}, m_{2,2}, \ldots, m_{\iota(a_2),2}, \ldots, m_{1,t}, m_{2,t}, \ldots, m_{\iota(a_t),t})$. Let $M = k(m_{1,1}, m_{2,1}, \ldots, m_{\iota(a_1),1}, m_{1,2}, m_{2,2}, \ldots, m_{\iota(a_2),2}, \ldots, m_{1,t}, m_{2,t}, \ldots, m_{\iota(a_t)t})$. Then $M \subseteqq L$. As $Mk' = L'$, L' is algebraic over M and $[L' : M] \leqq [k' : k]$, so $M = L$. As the transcendental degree of $L(=M)$ is n, m's are algebraically independent generators of L and L is purely transcendental over k.

(ii) Necessity. Suppose that L is purely transcendental over k and $L = k(a_1, a_2, \ldots, a_n)$. $(a_1, a_2, \ldots, a_n)$ is clearly a primitive generating set of L' over $k(\zeta)$. q.e.d.

2. Now we prove the following theorem.

THEOREM 3. *Let $n \leqq 7$ and suppose that the characteristic p of k does not divide n. Then L is purely transcendental over k.*

Proof. (i) When $n = 1$, the theorem is trivial.

(ii) When $n = 2$, it holds $[k' : k] = 1$ from $p \nmid n$ and the theorem follows from Theorem 1.

(iii) When $n = 3$, $[k' : k] = 1$ or 2. If $[k' : k] = 1$, the theorem follows from Theorem 1. If $[k' : k] = 2$, let $a_1 = c_{1,3} = x_1 + x_2 + x_3$ and $a_2 = c_{1,1} = (\zeta_3 x_1 + \zeta_3^2 x_2 + x_3)^2 / \zeta_3^2 x_1 + \zeta_3 x_2 + x_3$. Then $\iota(a_1) + \iota(a_2) = 1 + 2 = 3$ and since $a_2 = c_{2,2} = c_{1,2} c_{1,3} / c_{1,1}$ it follows $k'(a_1, a_2, a_2') = k'(c_{1,1}, c_{1,2}, c_{1,3}) = L_3'$. So (a_1, a_2) is a primitive generating set of L_3' over $k(\zeta_3)$ and the theorem follows from Theorem 2.

(iv) When $n = 4$, $[k' : k] = 1$ or 2. If $[k' : k] = 1$, the theorem follows from Theorem 1. When $[k' : k]=2$, let $a_1=c_{1,4}$, $a_2=c_{1,2}$, $a_3=c_{1,3}$. Then $\iota(a_1)+\iota(a_2)+\iota(a_3)=1+2+1$ and since $a_2'=c_{3,2}=c_{1,3}c_{1,4}/c_{1,1}$ it follows $k'(a_1, a_2, a_2', a_3)=k'(c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4})=L_4'$. So (a_1, a_2, a_3) is a primitive generating set of L_4' over $k(\zeta_4)$ and the theorem follows from Theorem 2.

(v) When $n=5$, $[k' : k]=1$ or 2 or 4. If $[k' : k]=1$, the theorem follows from Theorem 1. When $[k' : k]=4$, let $a_1=c_{1,5}$, $a_2=c_{1,2}$. Then $\iota(a_1)+\iota(a_2)=1+4=5$ and it follows from $a_2'=c_{2,4}=c_{1,4}c_{1,5}/c_{1,1}$, $a_2''=c_{1,3}$, $a_2'''=c_{3,4}=c_{1,4}c_{1,5}/c_{1,2}$ that $k'(a_1, a_2, a_2', a_2'', a_2''')=k'(c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5})=L_5'$. So (a_1, a_2) is a primitive generating set of L_5' over $k(\zeta_5)$, and the theorem follows from Theorem 2. If $[k' : k]=2$ it is easily seen that one of the following three sets $(c_{1,5}, c_{1,2}, c_{2,1})$, $(c_{1,5}, c_{1,2}, c_{1,3})$, $(c_{1,5}, c_{1,2}, c_{3,4})$ becomes a primitive generating set of $L(\zeta_5)$ over $k(\zeta_5)$.

(vi) When $n=6$, $[k' : k]=1$ or 2. When $[k' : k]=1$, the theorem follows from Theorem 1. When $[k' : k]=2$, let $a_1=c_{1,6}$, $a_2=c_{1,2}$, $a_3=c_{1,4}$, $a_4=c_{1,5}$, then $\iota(a_1)+\iota(a_2)+\iota(a_3)+\iota(a_4)=1+2+2+1=6$, and it follows from $a_2'=c_{5,4}=c_{1,5}, c_{1,6}/c_{1,3}$, $a_3'=c_{5,2}=c_{1,5}, c_{1,6}/c_{1,1}$ that $k'(a_1, a_2, a_2', a_3, a_3', a_4)=k'(c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}, c_{1,6})=L_6'$. So (a_1, a_2, a_3, a_4) is a primitive generating set of L_6' over $k(\zeta_6)(=k'(\zeta_3))$ and the theorem follows from Theorem 2.

(vii) When $n=7$, $[k' ; k]=1$ or 2 or 3 or 6. If $[k' : k]=1$, the theorem follows from Theorem 1. In the case of $[k' : k]=6$, let $a_1=c_{1,7}$, $a_2=c_{1,3}$. Then $\iota(a_1)+\iota(a_2)=1+6=7$, and $a_2'=c_{2,3}$, $a_2''=c_{2,6}$, $a_2'''=c_{4,6}$, $a_2''''=c_{4,5}$, $a_2'''''=c_{1,5}$. It follows from $c_{1,2}=c_{4,6}$, $c_{1,5}/c_{4,5}$, $c_{1,4}=c_{2,3}$, $c_{4,6}/c_{2,6}$, $c_{1,1}=c_{2,6}/c_{4,6}$, $c_{1,3}$ that $k'(a_1, a_2, a_2', a_2'', a_2''', a_2'''', a_2''''')=k'(c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}, c_{1,5}, c_{1,6}, c_{1,7})=L'$, and (a_1, a_2) is a primitive generating set of L_7' over $k(\zeta_7)$ and the theorem follows from Theorem 2. If $[k' : k]=3$ or 2, we can find easily a primitive generating set in $(c_{1,7}, c_{1,3}, c_{2,3}, c_{2,6}, c_{4,6}, c_{4,5}, c_{1,5})$ and the theorem follows from Theorem 2.

In the following we give polynomials of x which are algebraically independent generators of L_n over k for $n\leqq 4$ obtained easily from the above primitive generators.

When $n=1$; x_1.

$n=2$; x_1+x_2, x_1x_2.

$n=3$; $x_1+x_2+x_3$, $(\sum_{i=1}^{3}x_i x^2_{\overline{i+1}} - x_1x_2x_3)/(\sum_{i=1}^{3}x_i^2 - \sum_{i=1}^{3}x_i x_{\overline{i+1}})$,

$(\sum_{i=1}^{3}x_i x^2_{\overline{i+1}} - x_1x_2x_3)/(\sum_{i=1}^{3}x_i^2 - \sum_{i=1}^{3}x_i x_{\overline{i+1}})$.

$$n = 4; \quad x_1 + x_2 + x_3 + x_4, \ \sum_{i=1}^{4} x_i^2 - 2(x_1x_3 + x_2x_4)$$
$$\sum_{i=1}^{4} x_i^3 - \sum_{i \neq j} x_i^2 x_j + 2\, x_1x_2x_3x_4, \ -\sum_{i=1}^{4} x_i^2 x_{\overline{i+1}} + \sum_{i=1}^{4} x_i^2 x_{i+3}.$$

This shows that $L_n \cap k[x_1, x_2, \ldots, x_n]$ is purely transcendental integral domain over k, when $n = 1, 2, 4$.

References

[1] H. Hasse: Invariante Kennzeichnung Galoisschen Körper mit vorgegebener Galoisgruppe, Crelle J., **187** (1949).

[2] H. Kuniyoshi: On a problem of Chevalley, the present volume of this Journal.

[3] K. Masuda: One valued mappings of groups into fields, Nagoya Math. J., **6** (1953).

[4] A. Weil: Foundations of Algebraic Geometry, New York (1946).

Department of Mathematics
Yamagata University