On Matrix Equations for Galois Extensions of Fields with Characteristic p

Eizi Inaba* (稲 葉 栄 次)

Department of Mathematics, Faculty of Science,
Ochanomizu University, Tokyo

Let k be a field with characteristic p and K be a Galois extension of k, the order of the Galois group being a power of p. When K is cyclic of order p over k, it is well known that equations of Artin-Schreier type are essential for its theory and this result was extended to a more general cyclic case by Albert and Witt [1], [5]. The construction of Galois extensions over k for non-abelian case was first studied by Witt [6], but he did not give equations which characterize these extensions. So it is desirable to consider this problem anew. In the case when the characteristic of k does not divide the order of the Galois group the theory on Galois algebras initiated by Hasse [4] contributed much to the study of Galois extensions, but it does not seem to be applicable for the present case. So we consider this problem apart from his theory. Our method is based on representations of Galois groups and we show that matrix equations of a certain type characterize those extensions mentioned above.

1. Matrix equations and Galois extensions

Let k be a field with characteristic p. We denote by k_n the ring of all square matrices of degree n with elements in k. By *unipotent matrix* we understand a square matrix whose elements below the principal diagonal are all zero, while the elements lying in that diagonal are all 1. For a matrix $A=(a_{ij})$ we denote with A^p the matrix (a_{ij}^p) since no confusion will arise throughout in the following. Given a unipotent matrix $M=(m_{ij})$ in k_n, we consider the matrix equation

$$X^p=MX\,. \tag{1.1}$$

We shall show that there exists a unipotent matrix A satisfying (1.1) in Ω_n, where Ω is an algebraic closure of k. We put $\alpha_{ij}=0$ whenever $i>j$ and $\alpha_{ii}=1$, $i=1,\cdots,n$. When $i<j$ we can determine α_{ij} successively as follows. Supposing that α_{ij} have already been determined when $j-i<r$, let α_{ij} be a root of the equation

* This work was supported by the research fund granted from the Ministry of Education.

$$x^p - x = \sum_{i<\lambda\leq j} m_{i\lambda}\alpha_{\lambda j} \tag{1.2}$$

when $j=i+r$. Then we have

$$\alpha_{ij}^p = \sum_{i\leq\lambda\leq j} m_{i\lambda}\alpha_{\lambda j}\,.$$

Thus the unipotent matrix $A=(\alpha_{ij})$ is a solution of (1.1).

When a solution of (1.1) is a unipotent matrix, we call it a *unipotent solution*. If B is another arbitrary solution of (1.1), then we have $B^p=MB$ and this yields $(A^{-1}B)^p=A^{-1}B$. Therefore $A^{-1}B$ is a matrix in P_n, where P is the prime field. Then we see that all solutions of (1.1) can be obtained by multiplying all matrices in P_n on the right-hand side of a unipotent solution.

Let K be the extension of k generated by adjunction of all elements α_{ij} of A to k. The consideration above shows that K is determined uniquely independent of the choice of a solution of (1.1), provided that the solution is a non-singular matrix in Ω_n. We denote by U_n the group of all unipotent matrices in P_n. We shall prove that K is a Galois extension of k and that its Galois group G is isomorphic to a subgroup of U_n. In fact, from (1.2) we find that K is separable over k. Let A be a unipotent solution of (1.1). Since $\sigma A^p=M\sigma A$ holds for any isomorphism σ of Ω over k, σA is a solution of (1.1). If we put $\sigma A=A\Lambda(\sigma)$, then $\Lambda(\sigma)$ is a unipotent matrix in P_n. This shows that σ is an automorphism of K over k and therefore K is a Galois extension of k. We can verify that $\Lambda(\sigma\tau)=\Lambda(\sigma)\Lambda(\tau)$ and hence G is homomorphically mapped into U_n. If $\Lambda(\sigma)=I$, then it follows that $\sigma A=A$ and therefore $\sigma=1$. This proves that the mapping is an isomorphism. Further we find that the order of the Galois group is a power p^s of p with $s\leq n(n-1)/2$ because the order of U_n is equal to the $n(n-1)/2$-th power of p. We note further that the isomorphic representation Λ of G in U_n is uniquely determined up to equivalence. Because if we choose another solution B of (1.1), where B is non-singular, then we have $B=AD$ with a non-singular matrix D in P_n. From this follows that

$$\sigma B=\sigma A\cdot D=A\Lambda(\sigma)D=BD^{-1}\Lambda(\sigma)D$$

and we have the representation $D^{-1}\Lambda D$.

Next we consider whether the converse of the result stated above holds. Let K be a Galois extension of k and the order of the Galois group G of K/k be a power of p. Obviously there exists an isomorphic representation Λ of G in P_n if the degree n is suitably chosen. Here we understand that the identity of G corresponds to the unit matrix. Since in this case there exists no irreducible representation other than the identical representation of degree one, Λ is equivalent to a representation consisting of unipotent matrices in U_n. So we can

assume that Λ is an isomorphic representation of G in U_n. Let $\Lambda(\sigma)$ be the matrix corresponding to $\sigma \in G$. We shall prove that there exists a unipotent matrix A in K_n such that

$$\sigma A = A\Lambda(\sigma) \tag{1.3}$$

for all $\sigma \in G$. In fact, we choose an element $\gamma \in K$ with $\mathrm{Tr}_{K/k}\,\gamma \neq 0$ and put

$$A = \frac{1}{\mathrm{Tr}\,\gamma} \sum_{\sigma} \Lambda(\sigma^{-1})\sigma\gamma \ .$$

Then we can verify that A is unipotent and satisfies (1.3). Moreover K is generated by adjunction of all elements of A to k. For, if K^* be the extension of k generated by all elements of A, then $\sigma A = A$ for any automorphism σ of K over K^*. This yields $\Lambda(\sigma) = I$, whence we have $\sigma = 1$ by the assumption that Λ is an isomorphic representation of G. Hence K^* is identified with K. If B is another unipotent matrix such that $\sigma B = B\Lambda(\sigma)$, then there exists a unipotent matrix C in k_n such that $B = CA$. Since from (1.3) we obtain $\sigma A^p = A^p\Lambda(\sigma)$, we have $A^p = MA$ with a unipotent matrix M in k_n. Thus we find that the matrix M can be associated with the extension K/k.

It should be noted that the matrix M is not uniquely determined by a given extension K/k. In fact, if we take B in place of A as above, then we can put $B^p = M^*B$, where M^* is a unipotent matrix in k_n. Since $B = CA$, we have

$$M^* = C^p M C^{-1}$$

where C is a unipotent matrix in k_n. The matrix $C^p M C^{-1}$ shall be called *p-equivalent* to M, if C is a unipotent matrix in k_n, and we call such a transformation of M a *p-transformation*. Conversely we shall show that if two unipotent matrices M_1 and M_2 are p-equivalent, then they determine the same extension. In fact, if we put

$$A^p = M_1 A\,, \qquad B^p = M_2 B\,, \qquad C^p M_1 C^{-1} = M_2$$

where A and B are non-singular, then we have

$$(A^{-1}C^{-1}B)^p = (A^{-1})^p M_1 C^{-1} B = A^{-1}C^{-1}B\,.$$

Hence $F = A^{-1}C^{-1}B$ is a non-singular matrix in P_n. The relations $B = CAF$ and $A = C^{-1}BF^{-1}$ imply that both A and B generate the same extension. Thus we have the following

THEOREM 1. *Let K be a Galois extension of a field k with characteristic p and the order of the Galois group G of K/k be a power of p. Further let Λ be an isomorphic representation of G in U_n, where U_n is the group of unipotent matrices of degree n with elements in*

the prime field P. Then, to every K/k and Λ there corresponds a unipotent matrix M in k_n uniquely up to p-equivalence such that the matrix equation

$$X^p = MX \tag{1.1}$$

determines the extension K and that a unipotent solution of (1.1) *yields a representation equivalent to Λ. Conversely, to every unipotent matrix M in k_n there exist a unique Galois extension K of k and a representation Λ of the Galois group of K/k in U_n such that M is associated with K and Λ by the correspondence mentioned above, where Λ is determined uniquely by M up to equivalence.*

2. Decomposable matrices and canonical form

Let a unipotent matrix M in k_n be associated with a Galois extension K over k. We can write M in the form

$$M=\begin{bmatrix} M_1 & M_{12} \\ 0 & M_2 \end{bmatrix}.$$

Then M_1 and M_2 are also unipotent. If the matrix

$$A=\begin{bmatrix} A_1 & A_{12} \\ 0 & A_2 \end{bmatrix}$$

is a unipotent solution of the equation $X^p=MX$, then we have $A_1{}^p=M_1A_1$ and $A_2{}^p=M_2A_2$. By Theorem 1 we find immediately that M_1 and M_2 are associated with two intermediate extensions K_1 and K_2 respectively. If Λ is the isomorphic representation of the Galois group of K/k determined by Theorem 1, then we can put

$$\Lambda=\begin{bmatrix} \Lambda_1 & \Lambda_{12} \\ 0 & \Lambda_2 \end{bmatrix}$$

and we have $\sigma A_1=A_1\Lambda_1(\sigma)$ and $\sigma A_2=A_2\Lambda_2(\sigma)$. Therefore Λ_1 and Λ_2 are the isomorphic representations of the Galois groups of K_1/k and K_2/k respectively. We note that when $M_{12}=0$ we have $K=K_1K_2$. Because then we can choose A such that $A_{12}=0$. A matrix M is called *p-decomposable* if it is p-equivalent to a matrix of the form

$$\begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix}.$$

We can prove that M is p-decomposable if and only if the representation associated with M is decomposable. More generally we obtain the following

THEOREM 2. *If a representation Λ of the Galois group of the Galois extension K/k associated with a unipotent matrix M is decomposable such that*

$$\Lambda=\begin{pmatrix} \Lambda_1 & 0 & \cdots & 0 \\ 0 & \Lambda_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & \Lambda_r \end{pmatrix},$$

then M is p-equivalent to a matrix of the form

$$\begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & M_r \end{pmatrix}$$

such that the extensions K_i/k associated with M_i have the isomorphic representations Λ_i of their Galois groups and that $K=K_1K_2\cdots K_r$ holds.

The proof runs as follows. In the course of the proof of Theorem 1 we see that we can find a unipotent matrix A in K_n such that $\sigma A=A\Lambda(\sigma)$ for all $\sigma\in G$ and that A is of the form

$$A=\begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & A_r \end{pmatrix}.$$

Hence we have $\sigma A_i=A_i\Lambda_i(\sigma)$ and from this we obtain unipotent matrices M_i such that $A_i^p=M_iA_i$. If we put

$$M^*=\begin{pmatrix} M_1 & 0 & \cdots & 0 \\ 0 & M_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & M_r \end{pmatrix},$$

then we have $A^p=M^*A$. By Theorem 1 we conclude that M^* is p-equivalent to M. Further it is clear that $K=K_1K_2\cdots K_r$ holds.

Next we consider an invariant property of a unipotent matrix M under p-transformations. We use the notation $\wp x$ for x^p-x as usual and denote by $\wp k$ the set of all elements $\wp x$ with $x\in k$. Obviously $\wp k$ is a subgroup of the additive group k. Since for any element ρ in the prime field P

$$\rho\wp x=\rho x^p-\rho x=(\rho x)^p-\rho x=\wp(\rho x)$$

holds, $\wp k$ is a vector space over P. Let $m_{i,i+1}$, $i=1,\cdots,n-1$, be the elements lying in the line next parallel to the principal diagonal of M. We use the abbreviated notation m_i for $m_{i,i+1}$. We consider the vector space S over P generated by m_i, $i=1,\cdots,n-1$, and $\wp k$. Then we find that this vector space is invariant under p-transformations of M. In fact, if $C^pMC^{-1}=M'$, then we have

$$c_{i,i+1}^p+m_{i,i+1}=m'_{i,i+1}+c_{i,i+1}.$$

The consideration above suggests that we can define a canonical form of M in the following manner. A unipotent matrix of the form

$$\begin{pmatrix} 1 & m_1 & 0 & 0 & \cdots \\ 0 & 1 & m_2 & 0 & \cdots \\ 0 & 0 & 1 & m_3 & \cdots \\ 0 & 0 & 0 & 1 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix},$$

where the elements m_{ij} are all zero whenever $j-i>1$, while the elements m_i, $i=1, \cdots, n-1$ are all non-zero, shall be called a *canonical form* for a unipotent matrix. We shall prove by induction on the degree n that every unipotent matrix M can be transformed into a canonical form by choosing a suitable p-transformation, if the field k is infinite. When $n=2$, we can choose $c \in k$ such that $m'_{12}=\wp c+m_{12} \neq 0$. Putting

$$C=\begin{bmatrix} 1 & c \\ 0 & 1 \end{bmatrix},$$

we have

$$C^p M C^{-1}=\begin{bmatrix} 1 & m'_{12} \\ 0 & 0 \end{bmatrix}.$$

Hence the assertion is true when $n=2$. When $n>2$, we put

$$M=\begin{bmatrix} M_1 & M_2 \\ 0 & 1 \end{bmatrix},$$

where M_1 is of degree $n-1$. By induction hypothesis we can find a unipotent matrix C_1 in k_{n-1} such that $M_1'=C_1^p M_1 C_1^{-1}$ is canonical and that $m_i' \neq 0$, $i=1, \cdots, n-2$. Putting

$$C^*=\begin{bmatrix} C_1 & 0 \\ 0 & 1 \end{bmatrix},$$

we have

$$C^{*p} M C^{*-1}=\begin{bmatrix} M_1' & * \\ 0 & 1 \end{bmatrix}.$$

Hence, by the transitivity of p-equivalence we can assume from the beginning that M_1 is canonical with $m_i \neq 0$, $i=1, \cdots, n-2$. Then we choose $c_1 \in k$ arbitrarily and next determine $c_2, \cdots, c_{n-1}$ in k successively such that these elements satisfy the equations

$$m_{in}+\wp c_i=m_i c_{i+1} \qquad i=1, 2, \cdots, n-2 . \tag{2.1}$$

We put

$$m_{n-1}+\wp c_{n-1}=m'_{n-1} \tag{2.2}$$

$$\Gamma=\begin{pmatrix} c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}, \qquad C=\begin{bmatrix} I_{n-1} & \Gamma \\ 0 & 1 \end{bmatrix}, \qquad M_2'=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ m'_{n-1} \end{pmatrix}$$

where I_{n-1} signifies the unit matrix of degree $n-1$. From (2.1) and (2.2) we obtain

$$M_2+\Gamma^p=M_1\Gamma+M_2' \ .$$

Then we get

$$C^pM=\begin{bmatrix} M_1 & M_2+\Gamma^p \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} M_1 & M_1\Gamma+M_2' \\ 0 & 1 \end{bmatrix}$$
$$=\begin{bmatrix} M_1 & M_2' \\ 0 & 1 \end{bmatrix}\begin{bmatrix} I_{n-1} & \Gamma \\ 0 & 1 \end{bmatrix}=\begin{bmatrix} M_1 & M_2' \\ 0 & 1 \end{bmatrix}C \ .$$

It remains to prove that we can choose c_1 such that $m'_{n-1}\neq 0$. For this we replace c_1 by x in (2.1) and consider m'_{n-1} as a polynomial of x over k. Since the coefficients of this polynomial are not all zero, the assertion is true by the assumption that k is infinite. We note that in the above proof we never use the fact that M is p-indecomposable. Therefore a canonical matrix is not necessarily p-indecomposable.

When M is of a canonical form, then a unipotent solution $A=(\alpha_{ij})$ of the matrix equation $X^p=MX$ can be obtained by

$$\wp\alpha_{ij}=m_i\alpha_{i+1,j}$$
$$i=1, 2, \cdots, n-1 ; \qquad j=i+1, \cdots, n$$

These equations are often convenient when we deal with the Galois extension associated with M.

3. Intermediate extensions and their Galois groups

We consider intermediate extensions between k and K when K is associated with an arbitrary unipotent matrix M in k_n. Among them we investigate only those which shall be used later. Let $\Lambda(\sigma)=(\lambda_{ij}(\sigma))$ be a representation of the Galois group G of K/k in U_n. The set G_ν of all $\sigma\in G$, for which $\lambda_{ij}(\sigma)$ vanish whenever $\nu\geqq j-i\geqq 1$, is a subgroup of G. Because from the relation

$$\lambda_{ij}(\sigma\tau)=\sum_{i\leq k\leq j}\lambda_{ik}(\sigma)\lambda_{kj}(\tau)$$

we see that if $\nu\geqq j-i\geqq 1$ and $\sigma,\ \tau\in G_\nu$ then $\nu\geqq k-i$, $\nu\geqq j-k$ and therefore $\lambda_{ij}(\sigma\tau)=0$, whence we have $\sigma\tau\in G_\nu$. When $\nu=0$, we put $G_0=G$. Let $A=(\alpha_{ij})$ be a unipotent solution of the matrix equation $X^p=MX$ and $K^{(\nu)}$ be the extension of k generated by adjunction of all elements

α_{ij} with $\nu \geqq j-i$ to k. We shall prove that G_ν is the Galois group of $K/K^{(\nu)}$.

From $\sigma A = A\Lambda(\sigma)$ we have

$$\sigma\alpha_{ij} = \sum_{i \leq k \leq j} \alpha_{ik}\lambda_{kj}(\sigma) \tag{3.1}$$

and we find that if $\nu \geqq j-i$ and $\sigma \in G_\nu$ then $\sigma\alpha_{ij} = \alpha_{ij}$. Therefore every element in $K^{(\nu)}$ is invariant under any automorphism $\sigma \in G_\nu$. Conversely suppose that all elements of $K^{(\nu)}$ are invariant under an automorphism $\tau \in G$. It suffices to prove that by induction on ν that τ belongs to G_ν. This is clear when $\nu = 0$ if we put $K^{(0)} = k$. Since $K^{(\nu-1)}$ is a subfield of $K^{(\nu)}$, we have $\tau \in G_{\nu-1}$ by induction hypothesis and from (3.1) we obtain

$$\alpha_{i,i+\nu} = \tau\alpha_{i,i+\nu} = \alpha_{i,i+\nu} + \lambda_{i,i+\nu}(\tau) .$$

Hence we have $\lambda_{i,i+\nu}(\tau) = 0$, $i = 1, \cdots, n-\nu$, whence follows that τ belongs to G_ν. This concludes the proof of our assertion.

We see that $K^{(\nu)}$ are Galois extensions of k by virtue of (3.1) and therefore G_ν are normal subgroups of G. Furthermore we find that the Galois group $G_{\nu-1}/G_\nu$ of $K^{(\nu)}/K^{(\nu-1)}$ is abelian of type $(p, \cdots, p)$. This follows from the fact that

$$K^{(\nu)} = K^{(\nu-1)}(\alpha_{1,1+\nu}, \cdots, \alpha_{n-\nu,n}) ,$$
$$\wp(\alpha_{i,i+\nu}) = \sum_{i < j \leq i+\nu} m_{ij}\alpha_{j,i+\nu} \in K^{(\nu-1)} .$$

In particular we have

$$K^{(1)} = k(\alpha_{12}, \alpha_{23}, \cdots, \alpha_{n-1,n}) ,$$
$$\wp(\alpha_{i,i+1}) = m_i .$$

This shows that the vector space S generated by m_i and $\wp k$ determines $K^{(1)}$ completely. We remark further that $K^{(\nu)}$ are invariant under p-transformations of the matrix M. Because if $A' = CA$, then $A = C^{-1}A'$ and

$$\alpha'_{ij} = \sum_{i \leq k \leq j} c_{ik}\alpha_{kj} , \qquad \alpha_{ij} = \sum_{i \leq k \leq j} c'_{ik}\alpha'_{kj}$$

with elements c_{ik} and c'_{ik} in k. Therefore the extension generated by adjunction of all α'_{ij} with $\nu \geqq j-i$ to k is equal to $K^{(\nu)}$. The following lemma will be used in the next section.

LEMMA. *$G_{\nu-1}/G_\nu$ lies in the center of G/G_ν.*

If $\sigma \in G_{\nu-1}$ and $s \in G$, then we have

$$\lambda_{i,i+\nu}(\sigma s) = \lambda_{i,i+\nu}(\sigma) + \lambda_{i,i+\nu}(s) , \quad \lambda_{ij}(\sigma s) = \lambda_{ij}(s) \quad \text{when} \quad \nu > j-i .$$
$$\lambda_{i,i+\nu}(s\sigma) = \lambda_{i,i+\nu}(s) + \lambda_{i,i+\nu}(\sigma) , \quad \lambda_{ij}(s\sigma) = \lambda_{ij}(s) \quad \text{when} \quad \nu > j-i .$$

From these relations follows that $\lambda_{ij}(\sigma s)=\lambda_{ij}(s\sigma)$ whenever $\nu \geqq j-i$. This shows that the assertion is true.

By this Lemma we see that $K^{(\nu)}/k$ is a central extension of $K^{(\nu-1)}/k$.

4. Determination of the Galois group of the Galois extension associated with a given unipotent matrix

For a given unipotent matrix M in k_n we consider the vector space S over P generated by m_i, $i=1, \cdots, n-1$, and $\wp k$. The elements m_i, $i=1, \cdots, n-1$, are said to be linearly independent over P mod $\wp k$, if $m_i+\wp k$, $i=1, \cdots, n-1$, are linearly independent over P in the quotient space $S/\wp k$. The problem how to determine the Galois group G of the Galois extension K/k associated with M is much related to the properties of the vector space $S/\wp k$. But, since this problem is complicated in the general case, we shall prove only a theorem concerning the most important special case when G is isomorphic to the full group U_n of unipotent matrices in P_n.

THEOREM 3. *In order that the Galois group G of the Galois extension K/k associated with a unipotent matrix M be isomorphic to U_n, it is necessary and sufficient that m_i, $i=1, \cdots, n-1$, are linearly independent over P* mod $\wp k$.

From arguments in the preceding section it is clear that we have

$$[K^{(\nu)} : K^{(\nu-1)}] \leqq p^{n-\nu}, \qquad [K : k]=\prod_{\nu=1}^{n-1} [K^{(\nu)} : K^{(\nu-1)}] .$$

If m_i, $i=1, \cdots, n-1$, are linearly dependent over P mod $\wp k$, then we have $[K^{(1)} : k]<p^{n-1}$ and therefore $[K : k]$ is less than the order of U_n. This shows that the condition is necessay. Let $A=(\alpha_{ij})$ be a unipotent solution of the matrix equation $X^p=MX$. In order to prove the sufficiency of the condition, we first observe that $k(\alpha_{i,i+1})$ cannot be contained in the extension generated by adjoining all $\alpha_{j,j+1}$ except $\alpha_{i,i+1}$ to k. If it were so, we would have

$$\alpha_{i,i+1}-\sum_{j\neq i} \rho_j \alpha_{j,j+1} \in k$$

with $\rho_j \in P$ by the well known theory. Since $\wp(\alpha_{i,i+1})=m_i$, it follows that

$$m_i-\sum_{j\neq i} \rho_j m_j \in \wp k .$$

This contradicts the condition. Hence we can choose $\sigma \in G$ such that $\sigma(\alpha_{i,i+1}) \neq \alpha_{i,i+1}$ and $\sigma(\alpha_{j,j+1})=\alpha_{j,j+1}$ when $j \neq i$. Thus there exist $\sigma_i \in G$, $i=1, \cdots, n-1$, such that

$$\lambda_{j,j+1}(\sigma_i)=\delta_{ij} ,$$

where by $\lambda_{kj}(\sigma_i)$ we denote the elements of $\Delta(\sigma_i)$ and where $\delta_{ii}=1$ and $\delta_{ij}=0$ if $j\neq i$. Next we shall show by induction on ν that there exist

$$\sigma_i^{(\nu)} \in G_\nu \qquad i=1, 2, \cdots, n-\nu-1\,; \quad \nu=0, 1, \cdots, n-2$$

such that

$$\lambda_{j,j+\nu+1}(\sigma_i^{(\nu)})=\delta_{ij}\,. \tag{4.1}$$

When $\nu=0$, we can put $\sigma_i^{(0)}=\sigma_i$ and the assertion holds. Supposing that there exist $\sigma_i^{(\nu-1)} \in G_{\nu-1}$, $i=1, \cdots, n-\nu$, satisfying the above requirement, we put

$$\sigma_i^{(\nu)}=\sigma_i^{(\nu-1)}\sigma_{i+\nu}(\sigma_i^{(\nu-1)})^{-1}\sigma_{i+\nu}^{-1} \qquad i=1, 2, \cdots, n-\nu-1\,.$$

These elements belong to G_ν by the Lemma in the preceding section. If we take into consideration the fact that $\lambda_{j,j+\lambda}(\sigma_i^{(\nu-1)})=0$ whenever $\lambda<\nu$, we have

$$\begin{aligned}\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)}\sigma_{i+\nu}) &=\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)})+\lambda_{j,j+\nu-1}(\sigma_{i+\nu})+\lambda_{j,j+\nu}(\sigma_i^{(\nu-1)})\lambda_{j+\nu,j+\nu+1}(\sigma_{i+\nu}) \\ &=\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)})+\lambda_{j,j+\nu+1}(\sigma_{i+\nu})+\delta_{ij}\,,\end{aligned} \tag{4.2}$$

$$\begin{aligned}\lambda_{j,j+\nu+1}(\sigma_{i+\nu}\sigma_i^{(\nu-1)}) &=\lambda_{j,j+\nu+1}(\sigma_{i+\nu})+\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)})+\lambda_{j,j+1}(\sigma_{i+\nu})\lambda_{j+1,j+\nu+1}(\sigma_i^{(\nu-1)}) \\ &=\lambda_{j,j+\nu+1}(\sigma_{i+\nu})+\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)})\,.\end{aligned} \tag{4.3}$$

On the other hand, since $\sigma_i^{(\nu-1)}\sigma_{i+\nu}=\sigma_i^{(\nu)}\sigma_{i+\nu}\sigma_i^{(\nu-1)}$ and $\lambda_{j,j+\lambda}(\sigma_i^{(\nu)})=0$ whenever $\lambda\leqq\nu$, we have

$$\begin{aligned}\lambda_{j,j+\nu+1}(\sigma_i^{(\nu-1)}\sigma_{i+\nu}) &=\lambda_{j,j+\nu+1}(\sigma_i^{(\nu)}\sigma_{i+\nu}\sigma_i^{(\nu-1)}) \\ &=\lambda_{j,j+\nu+1}(\sigma_i^{(\nu)})+\lambda_{j,j+\nu+1}(\sigma_{i+\nu}\sigma_i^{(\nu-1)})\,.\end{aligned}$$

Then from (4.2) and (4.3) follows that $\sigma_i^{(\nu)}$ satisfy the condition (4.1). Now, if $\tau=\sigma_1^{(\nu)e_1}\sigma_2^{(\nu)e_2}\cdots$ belongs to $G_{\nu+1}$, then by (4.1) we have

$$\lambda_{j,j+\nu+1}(\tau)=e_j=0\,, \qquad j=1, 2, \cdots, n-\nu-1\,.$$

Therefore the order of $G_\nu/G_{\nu+1}$ is not less than $p^{n-\nu-1}$ and from this we infer that the order of G is equal to that of U_n. This concludes the proof of our theorem.

When G is isomorphic to U_n, we see from the proof of the above theorem that G_1 is the commutator group of G and therefore $K^{(1)}$ is the maximal abelian subfield of K/k. Furthermore the subgroups G_ν, $\nu=0, 1, \cdots, n-1$, of G constitute the descending central series of G and therefore $K^{(\nu)}$ is the maximal subfield of K such that $K^{(\nu)}/k$ is a central extension of $K^{(\nu-1)}/k$.

References

[1] A. A. Albert, Cyclic fields of degree p^n over F of characteristic p, Bull. Amer. Math. Soc. **40** (1934).
[2] E. Artin and O. Schreier, Über eine Kennzeichnung der reell abgeschlossenen Körper, Abh. Math. Sem. Hamburg, **5** (1927).
[3] E. Artin, Algebraic numbers and algebraic functions I-2, Princeton Uniuersity, 1950-1951.
[4] H. Hasse, Invariante Kennzeichnung galoisscher Körper mit vorgegebener Galoisgruppe, J. Reine Angew. Math. **187**, 14-43 (1950).
[5] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, J. Reine Angew. Math. **176**, 126-140 (1936).
[6] E. Witt, Konstruktion von galoisschen Körpern der Charakteristik p zu vorgegebener Gruppe der Ordnung p^f, J. Reine Angew. Math. **174**, 237-245 (1936).
[7] P. Wolf, Algebraische Theorie der Galoisschen Algebren, Mathematische Forschungsberichte (1956).

(Received September 1, 1961)