Natural Science Report, Ochanomizu University, Vol. 13, No. 2, 1962
お茶の水女子大学 自然科学報告 第13巻 第2号

On Generalized Artin-Schreier Equations

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 a finite Galois extension of k whose Galois group is denoted by G. In the previous article [1] we showed that K can be defined by matrix equations of a certain type when the order of G is a power of p and that these equations have properties similar to those of Artin-Schreier equations. The aim of the present work is first to show that the above result can be extended to the general case when G is arbitrary, and secondly to investigate relations between the form of generalized Artin-Schreier equations and the type of representations of G determined by these equations. It is hoped that our theory will contribute in some degree to answering the qestion as to how we can construct Galois extensions whose Galois groups are isomorphic to a given group.

1. Generalized Artin-Schreier equations.

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. When a matrix $C=(c_{ij})$ is given, we use the notation C^p for the matrix (c_{ij}^p) without the risk of confusion throughout in the following. Two matrices M_1 and M_2 in k_n are called *p-similar* to each other when there exists a non-singular matrix C in k_n such that

$$M_2=C^pM_1C^{-1}$$

The relation of p-similarity is obviously reflexive, symmetric and transitive, and we call such a transformation a *p-transformation*. We consider an algebraic closure Ω of k and a matrix equation

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

where M is a given non-singular matrix in k_n. If $A^p=MA$ holds for a matrix A in Ω_n, then A is called a *solution* of (1.1), in particular a *non-singular solution* if A is non-singular. If A is a non-singular solution and A' an arbitrary one of (1.1), then we have $(A^{-1}A')^p=A^{-1}A'$ and therefore all elements of $A^{-1}A'$ belong to the prime field P. Thus $A'=AD$ with a matrix D in P_n. By adjunction of all elements of A

to k we obtain a finite extension K of k. Since this extension K does not depend on the choice of a non-singular solution of (1.1), we shall say that K is associated with the matrix M. It is easy to prove that, if a matrix M' is p-similar to a non-singular matrix M, then M and M' yield the same extension of k.

Let Ω be an algebraic closure of k and Ω^* the maximal separable extension of k contained in Ω. The first thing we have to prove is that there always exists a non-singular solution of (1.1) and that this belongs to Ω_n^*, in other words, M is associated with a finite separable extension of k. To accomplish the proof we need a preliminary account of some basic facts.

PROPOSITION 1. *A square matrix $M=(m_{ij})$ is p-similar to a matrix of the form*

$$(1.2) \qquad M^*=\begin{bmatrix} m_{11}^* & m_{12}^* & 0 \cdots\cdots 0 \\ m_{21}^* & m_{22}^* & m_{23}^* \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots \\ m_{n-1,1}^* & m_{n-1,2}^* & \cdots\cdots m_{n-1,n}^* \\ m_{n1}^* & m_{n2}^* & \cdots\cdots m_{nn}^* \end{bmatrix}$$

by a p-transformation with a matrix of the form

$$(1.3) \qquad C=\begin{bmatrix} 1 & 0 & 0\cdots 0 \\ * & * & \cdots\cdots \\ * & * & \cdots\cdots \end{bmatrix},$$

where $m_{ij}^*=0$, when $j-i>1$, and $m_{i,i+1}^*=1$ or $m_{i,i+1}^*=0$, $i=1, \cdots, n-1$.

We prove this proposition by induction on degree n of M. When $n=1$, the lemma holds trivially. When $n>1$, we first show that M is p-similar to a matrix $M'=(m_{ij}')$ for which $m_{13}'=\cdots=m_{1n}'=0$ and m_{12}' is 1 or 0. If $m_{1j}=0$, $j=2, \cdots, n$, then we have only to put $M'=M$. So we consider the case when there exists at least one non-zero element among m_{1j}, $j=2, \cdots, n$. In this case we can assume that $m_{12}\neq 0$. Because, if $m_{1j}\neq 0$ for $j>2$, we consider the matrix $D=(d_{\lambda\mu})$, where $d_{\lambda\lambda}=1$, when $\lambda\neq 2$ and $\lambda\neq j$, $d_{j2}=d_{2j}=1$ and all the other elements of D are zero. Then D is of form (1.3) and

$$D^pMD^{-1}=DMD^{-1}=\begin{bmatrix} m_{11} & m_{1j} \cdots\cdots \\ \cdots\cdots\cdots\cdots \\ \cdots\cdots\cdots\cdots \end{bmatrix}.$$

Assuming that $m_{12}\neq 0$, we put

$$C=\begin{bmatrix} 1 & 0 & \cdots\cdots & 0 \\ 0 & m_{12} & \cdots\cdots & m_{1n} \\ 0 & 0 & 1\cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0\cdots\cdots & 1 \end{bmatrix}.$$

From the relation $C^pM=M'C$ we have

$$m_{11}'=m_{11}, \qquad m_{12}'m_{12}=m_{12},$$
$$m_{1j}'+m_{12}'m_{1j}=m_{1j} \quad \text{when} \quad j>2.$$

Therefore $m_{12}'=1$ and $m_{1j}'=0$ for $j>2$. Then we can put

$$M'=\begin{bmatrix} m_{11} & 1 & 0\cdots\cdots 0 \\ M_2 & & M_3 \end{bmatrix},$$

where M_3 is a square matrix of degree $n-1$. By induction hypothesis there exists a non-singular matrix C_3 of form (1.3) such that $C_3^pM_3C_3^{-1}$ is of form (1.2). Putting

$$C=\begin{bmatrix} 1 & 0 \\ 0 & C_3 \end{bmatrix}$$

we can easily verify that the matrix $C^pM'C^{-1}$ is of form (1.2). This completes the proof of our proposition.

A matrix M is called *p-reducible* when it is p-similar to a matrix of the form

$$\begin{bmatrix} M_1 & 0 \\ M_2 & M_3 \end{bmatrix}. \tag{1.4}$$

When M is not p-reducible, it is called *p-irreducible.* We note that an alternative way of defining p-reducibility is: M is p-reducible when it is p-similar to a matrix of the form

$$\begin{bmatrix} M_1 & M_2 \\ 0 & M_3 \end{bmatrix} \tag{1.5}$$

In fact, by repeating the process of interchanging two rows as well as corresponding columns a matrix $M^{(1)}$ of form (1.4) can be transformed into a matrix $M^{(2)}$ of form (1.5). Hence there exists a non-singular matrix D in P_n such that $DM^{(1)}D^{-1}=M^{(2)}$. Since $D^p=D$, $M^{(2)}$ is p-similar to $M^{(1)}$.

LEMMA 1. *If two matrices M_1 and M_2 are p-similar to M_1' and M_2' respectively, then a matrix*

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

is p-similar to a matrix

$$\begin{bmatrix} M_1' & 0 \\ ** & M_2' \end{bmatrix}$$

For, if $C_1^p M_1 C_1^{-1} = M_1'$ and $C_2^p M_2 C_2^{-1} = M_2'$, then we have

$$\begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}^p \begin{bmatrix} M_1 & 0 \\ * & M_2 \end{bmatrix} \begin{bmatrix} C_1 & 0 \\ 0 & C_2 \end{bmatrix}^{-1} = \begin{bmatrix} M_1' & 0 \\ ** & M_2' \end{bmatrix}$$

PROPOSITION 2. *A matrix M is p-irreducible if and only if $m_{i,i+1}^*$, $i=1, \cdots, n-1$, are all 1 whenever M is transformed into a matrix $M^*=(m_{ij}^*)$ of form* (1.2) *by p-transformations.*

It is evident that M^* is p-reducible when one of $m_{i,i+1}^*$ is zero. If M is p-reducible, then M is p-similar to a matrix of form (1.4). Let M_1' and M_3' be p-similar to M_1 and M_3 respectively such that both M_1' and M_3' are of form (1.2), then by Lemma 1 M is p-similar to the matrix

$$\begin{bmatrix} M_1' & 0 \\ * & M_2' \end{bmatrix}$$

This is obviously of form (1.2) and at least one of $m'_{i,i+1}$ is zero.

PROPOSITION 3. *Let $M=(m_{ij})$ be a matrix in k_n and*

$$x_i^p = \sum_{j=1}^{n} m_{ij} x_j + l_i, \qquad l_i \in k \qquad i=1, \cdots, n \tag{1.6}$$

be a simultaneous equation with n unknown quantities x_i. There always exist elements $\alpha_1, \cdots, \alpha_n$ in Ω which satisfy (1.6). *In particular, when M is non-singular, these elements α_i all belong to Ω^*.*

By putting

$$X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}, \qquad L = \begin{bmatrix} l_1 \\ \vdots \\ l_n \end{bmatrix}$$

we can represent (1.6) by the formula

$$X^p = MX + L.$$

If C is a non-singular matrix in k_n, we have

$$(CX)^p = C^p M C^{-1}(CX) + C^p L \tag{1.7}$$

Hence we can assume that $M=(m_{ij})$ is of form (1.2), that is, $m_{ij}=0$, when $j-i>1$, and $m_{i,i+1}$ is 1 or 0. The proof is carried out by induction on degree n of M. When $n=1$, (1.6) becomes $x_1^p = m_{11}x_1 + l_1$ and, if $m_{11} \neq 0$, the derivative of the polynomial $X^p - m_{11}X - l_1$ is $-m_{11}$.

Hence the solution $x_1=\alpha_1$ belongs to Ω^*. When $n>1$, we first consider the case when M is p-reducible. We put

$$M=\begin{bmatrix} M_1 & 0 \\ M_2 & M_3 \end{bmatrix},$$

where $M_1=(m_{ij}^{(1)})$ is of degree λ and $M_3=(m_{ij}^{(3)})$ of degree $n-\lambda$. By induction hypothesis there exist $\alpha_1, \cdots, \alpha_\lambda$ in Ω such that

$$\alpha_i^p=\sum_{j=1}^{\lambda} m_{ij}^{(1)}\alpha_j+l_i\,,\qquad i=1, \cdots, \lambda\,.$$

and also there exist $\alpha_{\lambda+1}, \cdots, \alpha_n$ in Ω such that these elements satisfy the simultaneous equation

$$x_i^p=\sum_{j=\lambda+1}^{n} m_{ij}^{(3)}x_j+l_i+\sum_{j=1}^{\lambda} m_{ij}^{(2)}\alpha_j \qquad i=\lambda+1, \cdots, n$$

with $n-\lambda$ unknown quatities $x_{\lambda+1}, \cdots, x_n$. Then $\alpha_1, \cdots, \alpha_n$ obviously satisfy the equation (1.6). When in particular M is non-singular, so are M_1 and M_3. Then $\alpha_i, i=1, \cdots, n$ all belong to Ω^* by induction hypothesis. It remains to prove the case when M is p-irreducible. Then $m_{i,i+1}=1$, $i=1, \cdots, n-1$. We define polynomials of a variable X successively in the following manner

(1.8)
$$f_1(X)=X, \qquad f_2(X)=f_1(X)^p-m_{11}f_1(X)-l_1\,,$$
$$f_{i+1}(X)=f_i(X)^p-\sum_{j=1}^{i} m_{ij}f_j(X)-l_i\,.$$

It is easy to see that the degree of $f_i(X)$ is p^{i-1}. If α_1 is any root of $f_{n+1}(X)$, we put $f_i(\alpha_1)=\alpha_i, i=1, \cdots, n$, and find that $\alpha_1, \cdots, \alpha_n$ satisfy (1.6). Conversely, if $\alpha_1, \cdots, \alpha_n$ satisfy (1.6), then α_1 is a root of $f_{n+1}(X)$. Next we shall prove that $f_{n+1}(X)$ is separable over k when M is non-singular. For this it suffices to prove that the derivative $f_{n+1}'(X)$ of $f_{n+1}(X)$ is a non-zero constant. Otherwise there would exist $\alpha\in\Omega$ such that $f_{n+1}'(\alpha)=0$. Since

$$f_{i+1}'(X)+\sum_{j=1}^{i} m_{ij}f_j'(X)=0 \qquad i=1, 2, \cdots, n$$

we would have

$$\sum_{j=1}^{i} m_{ij}f_j'(\alpha)+f_{i+1}'(\alpha)=0, \qquad i=1, \cdots, n-1\,,$$

$$\sum_{j=1}^{n} m_{nj}f_j'(\alpha)=0$$

From this follows that $f_1'(\alpha) = \cdots = f_n'(\alpha) = 0$ since M is non-singular. This contradicts the fact that $f_1'(X) = 1$. Thus we have proved that α_1 is separable over k. Next we have from (1.8) the relations

$$\alpha_{i+1} = \alpha_i^p - \sum_{j=1}^{i} m_{ij}\alpha_j - l_i$$

$$i = 1, \cdots, n-1 .$$

and hence $\alpha_2, \cdots, \alpha_n$ all belong to $k(\alpha_1)$. This proves that $\alpha_2, \cdots, \alpha_n$ are also separable over k.

PROPOSITION 4. *Let $M = (m_{ij})$ be a non-singular matrix in k_n and*

$$x_i^p = \sum_{j=1}^{n} m_{ij}x_j , \qquad i = 1, \cdots, n , \tag{1.9}$$

be a simultaneous equation with n unknown quantities x_j. Then there exists a non-trivial solution $x_i = \alpha_i$, $i = 1, \cdots, n$ of (1.9) *such that α_i all belong to Ω^*. When in particular M is of form* (1.2), *we have $\alpha_1 \neq 0$.*

By virtue of the relation (1.7) we can assume without loss of generality that M is of form (1.2). Further, when we examine the proof of Proposition 3, we observe that it suffices to prove the case when M is p-irreducible. Assuming that notations are the same as in the proof of that proposition, we see that $f_i(X)$ are all divisible by X since $l_1 = \cdots = l_n = 0$. If we put $f_{n+1}(X) = Xg_{n+1}(X)$ we find that the degree of $g_{n+1}(X)$ is $p^n - 1$ and that $g_{n+1}(X)$ is not divisible by X. For we have

$$f_{n+1}'(X) = Xg_{n+1}'(X) + g_{n+1}(X) ,$$

where $f_{n+1}'(X)$ is a non-zero constant. Hence any root α_1 of $g_{n+1}(X)$ is not equal to zero.

THEOREM 1. *If $M = (m_{ij})$ is a non-singular matrix in k_n, then the matrix equation*

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

has a non-singular solution in Ω_n^*. In other words, M is associated with a finite separable extension.

We can assume that M is of the form (1.2) stated in Proposition 1 and prove the theorem by induction on the degree n of M. When $n = 1$, it is clear that the theorem is true. When $n > 1$, by Proposition 4 there exist elements $\alpha_1, \cdots, \alpha_n$ in Ω^* such that $\alpha_1 \neq 0$ and

$$\alpha_i^p = \sum_{j=1}^{n} m_{ij}\alpha_i , \qquad i = 1, \cdots, n .$$

If we put

$$C=\begin{bmatrix} \alpha_1 & 0\cdots\cdots 0 \\ \alpha_2 & 1\cdots\cdots 0 \\ \vdots & \cdots\cdots\cdots\cdots \\ \alpha_n & 0\cdots\cdots 1 \end{bmatrix}$$

and $(C^{-1})^p MC = M' = (m_{ij}')$, then we have

$$\alpha_1^p m_{11}' = \sum_{j=1}^{n} m_{1j}\alpha_j = \alpha_1^p ,$$

$$\alpha_i^p m_{11}' + m_{i1}' = \sum_{j=1}^{n} m_{ij}\alpha_j = \alpha_i^p , \qquad \text{when } i>1 ,$$

$$\alpha_1^p m_{1j}' = m_{1j} , \qquad \text{when } j>1 ,$$

$$\alpha_i^p m_{1j}' + m_{ij}' = m_{ij} , \qquad \text{when } i>1,\ j>1 .$$

Hence we have

$$m_{11}' = 1, \qquad m_{21}' = \cdots\cdots = m_{n1}' = 0 ,$$

$$m_{13}' = \cdots\cdots = m_{1n}' = 0 ,$$

$$m_{ij}' = m_{ij}, \qquad \text{when } j>2 .$$

If we put

$$M' = \begin{bmatrix} 1 & M_2' \\ 0 & M_3' \end{bmatrix} ,$$

then we see that M_3' is also of form (1.2) and non-singular. By induction hypothesis there exists a non-singular matrix A_3 in Ω_{n-1}^* such that $A_3^p = M_3' A_3$. Since a polynomial of the form $x^p - x + a$ is separable, there also exists an $n-1$-dimensional row vector A_2 such that $A_2^p = A_2 + M_2' A_3$ and that all the elements of A_2 belong to Ω^*. Then we can verify that

$$A = \begin{bmatrix} 1 & A_2 \\ 0 & A_3 \end{bmatrix}$$

is a non-singular solution of (1.1) and that A belongs to $\Omega_n{}^*$. This completes the proof of our theorem.

Let K be the separable extension of k associated with a non-singular matrix M in k_n. In the following we shall show that K is a Galois extension of k and that its Galois group is isomorphic to a subgroup of the general linear group $GL(n, P)$. If A is a non-singular solution of the matrix equation $X^p = MX$, then we have $\sigma A^p = M\sigma A$ for any isomorphism σ of K over k. Since σA is also a non-singular solution of (1.1), there exists a non-singlar matrix $A(\sigma)$ in P_n such that

(1.10) $$\sigma A = A\Lambda(\sigma)\ .$$

This shows that σ is an automorphism of K over k and therefore K is Galois over k. By virtue of the relation (1.10) we see that $\Lambda(\sigma\tau) = \Lambda(\sigma)\Lambda(\tau)$ holds. Hence the Galois group G of K/k is homomorphically mapped into $GL(n, P)$. Further we can verify that this mapping is an isomorphism. For, if $\Lambda(\sigma) = I$, then we have $\sigma A = A$, whence it follows that $\sigma = 1$. We shall say that this isomorphic representation Λ of G is associated with the matrix M. We contend that, if two non-singular matrices M and M' are p-similar to each other, then the representation Λ' of G associated with M' is equivalent to the representation Λ of G associated with M. In fact, if we put

$$A^p = MA\ , \qquad A'^p = M'A'\ ,$$

$$\sigma A = A\Lambda(\sigma)\ , \qquad \sigma A' = A'\Lambda'(\sigma)\ ,$$

$$M' = C^p MC^{-1}\ .$$

then CA is a non-singular solution of the equation $X = M'X^p$ and therefore we have

(1.11) $$A' = CAD$$

with a non-singular matrix D in P_n. From (1.11) we have

$$CAD\Lambda'(\sigma) = A'\Lambda'(\sigma) = \sigma A' = \sigma CAD = CA\Lambda(\sigma)D$$

and hence $\Lambda'(\sigma) = D^{-1}\Lambda(\sigma)D$. Thus we have the following

THEOREM 2. *The class of all matrices p-similar to a non-singular matrix M in k_n determines a Galois extension of k uniquely and the representation of its Galois group in P_n uniquely up to equivalence.*

Next we investigate whether the converse of this theorem holds. Let K be a finite Galois extension of k and G its Galois group. There certainly exists an isomorphic representation of G in P_n if we choose n suitably. (For instance we can take the regular representation of G). Let Λ be an isomorphic representation of G in P_n, where the identity of G corresponds to the unit matrix, and β an element of K such that $\sigma\beta, \sigma \in G$ constitute a normal basis of K over k. If we put

(1.12) $$A = \sum_{\sigma} \Lambda(\sigma^{-1})\sigma\beta\ ,$$

then we can verify that A is non-singular. In fact, we can choose an element γ of K such that

$$\mathrm{Tr}_{K/k}(\gamma\beta) = 1,$$

$$\mathrm{Tr}_{K/k}(\gamma\sigma\beta) = 0, \qquad \text{when } \sigma \neq 1\ .$$

If we put $B=\sum_{\tau} \Lambda(\tau)\tau\gamma$, then

$$AB=\sum_{\varphi} \mathrm{Tr}\,(\beta\varphi\gamma)\Lambda(\varphi)=I\,.$$

From (1.12) we have

$$\sigma A=A\Lambda(\sigma) \quad \text{for} \quad \sigma\in G\,. \tag{1.10}$$

Since $\rho^p=\rho$ if $\rho\in P$, we see from (1.10) that $\sigma A^p=A^p\Lambda(\sigma)$ also holds. Then $\sigma(A^pA^{-1})=A^pA^{-1}$ for $\sigma\in G$ and therefore A^pA^{-1} is a non-singular matrix M in k_n. Thus A is a non-singular solution of the equation $X^p=MX$. Since the elements of A all belong to K, the extension K^* generated by adjunction of all elements of A to k is an intermediate field between K and k. If σ is any automorphism of K over K^*, then we have $\Lambda(\sigma)=I$ from (1.10). But this yields $\sigma=1$ by the assumption that Λ is an isomorphic representation of G. Hence $K^*=K$ and the matrix M is associated with K and Λ.

Further we assert that, if two non-singular matrices M and M' determine the same extension of k and if the representation Λ of G associated with M is equivalent to the representation Λ' associated with M', then M' is p-similar to M. In fact, if we put

$$A^p=MA\,, \qquad A'^p=M'A'\,,$$

$$\sigma A=A\Lambda(\sigma)\,, \qquad \sigma A'=A'\Lambda'(\sigma)\,,$$

$$\Lambda'(\sigma)=D^{-1}\Lambda(\sigma)D\,, \qquad D\in P_n\,,$$

then $\sigma(A'D^{-1}A^{-1})=A'D^{-1}A^{-1}$ for $\sigma\in G$ and therefore $C=A'D^{-1}A^{-1}$ is a non-singular matrix in k_n. Then we can easily verify that $M'=C^pMC^{-1}$. Thus we have the following

THEOREM 3. *Let K be a finite Galois extension of k and Λ an isomorphic representation of its Galois group G in P_n, where $\Lambda(\sigma)$ is a unit matrix when $\sigma=1$. There exists a matrix equation $X=MX^p$ such that M is associated with K and Λ. Furthermore the class of p-similar matrices is determined uniquely by the extension K and by the class of equivalent representations of G.*

2. Matrix equations and representation of Galois groups.

In this section we shall show relations between the form of a non-singular matrix M and the type of the representation Λ of the Galois group G of the Galois extension associated with M.

LEMMA 2. *If a non-singular matrix M in k_n is of the form*

$$M=\begin{bmatrix} M_1 & 0 \\ M_2 & M_3 \end{bmatrix},$$

then there exists a non-singular solution A of $X^p=MX$ with the form

$$A=\begin{bmatrix} A_1 & 0 \\ A_2 & A_3 \end{bmatrix}$$

By Theorem 1 there exist non-singular matrices A_1 and A_3 such that $A_1^p=M_1A_1$ and $A_3^p=M_3A_3$. By Proposition 3 we can verify that there exists a matrix A_2 such that $A_2^p=M_3A_2+M_2A_1$. Then, putting

$$A=\begin{bmatrix} A_1 & 0 \\ A_2 & A_3 \end{bmatrix},$$

we find that A is a non-singular solution of $X^p=MX$.

THEOREM 4. *If a non-singular matrix M in k_n is p-similar to a matrix of the form*

$$\begin{bmatrix} M_1 & 0 \\ M_2 & M_3 \end{bmatrix}, \tag{2.1}$$

then the representation Λ of G associated with M is reducible such that Λ is equivalent to a representation of the type

$$\begin{bmatrix} \Lambda_1 & 0 \\ \Lambda_2 & \Lambda_3 \end{bmatrix}, \tag{2.2}$$

where Λ_1 and Λ_3 are representations of the Galois groups of the intermediate extensions K_1 and K_3 associated with M_1 and M_3 respectively. Furthermore the converse of this statement holds.

By Theorem 2 we can assume that M is of form (2.1). Then by Lemma 2 we have a non-singular solution

$$A=\begin{bmatrix} A_1 & 0 \\ A_2 & A_3 \end{bmatrix}.$$

Since σA is also of the same form, we have

$$\Lambda(\sigma)=\begin{bmatrix} \Lambda_1(\sigma) & 0 \\ \Lambda_2(\sigma) & \Lambda_3(\sigma) \end{bmatrix}$$

and $\sigma A_1=A_1\Lambda_1(\sigma)$, $\sigma A_3=A_3\Lambda_3(\sigma)$. Conversely, if Λ is equivalent to a representation of type (2.2), then by Theorem 3 we can assume that Λ itself is of type (2.2). By considering the relation (1.12) in the preceding section we see that both matrices A and A^p can be of form (2.1). Then M is a matrix of the same form. This concludes the proof of our theorem.

In the preceding section we showed that a matrix of form (2.1) is p-similar to a matrix of the form

$$\begin{bmatrix} M_1 & M_2 \\ 0 & M_3 \end{bmatrix}.$$

We note that a statement silmilar to one in Theorem 4 is true when we consider representations of the type

$$\begin{bmatrix} A_1 & A_2 \\ 0 & A_3 \end{bmatrix}$$

in place of those of type (2.2).

A matrix M is called *p-decomposable* if M is p-similar to a matrix of the form

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

THEOREM 5. *If a non-singular matrix M in k_n is p-decomposable such that M is p-similar to a matrix of the form*

$$\begin{bmatrix} M_1 & 0 \\ 0 & M_2 \end{bmatrix}, \tag{2.3}$$

then the representation A of G associated with M is decomposable such that A is equivalent to a representation of the type

$$\begin{bmatrix} A_1 & 0 \\ 0 & A_2 \end{bmatrix}. \tag{2.4}$$

Furthermore, if K_1 and K_2 are intermediate extensions associated with M_1 and M_2 respectively, then A_1 vnd A_2 are representations of their Galois groups respectively and moreover $K=K_1K_2$ hold. Conversely, if the representation A is equivalent to a representation of type (2.4), *then M is p-similar to a matrix of form* (2.3).

The proof is almost immediate if we examine the proofs of Lemma 2 and Theorem 4. By a *left* (*right*) *unipotent matrix* we understand a square matrix whose elements lying above (below) the principal diagonal are all zero, while the elements lying in that diagonal are all one. From the argument in the preceding section we can infer that a right unipotent matrix is p-similar to a left unipotent matrix. So there is no need of making distinction between right and left unipotent matrices. In the following we shall call them simply *unipotent matrix.*

THEOREM 6. *Let K be associated with a non-singular matrix M. In order that the order of the Galois group G of K/k be a power of p, it is necessary and sufficient that M be p-similar to a unipotent matrix.*

First we prove the sufficiency of the condition. By Theorem 2 we can assume that M is a unipotent matrix. Then by Theorem 4 the representation of G is of the type

$$(2.5)\qquad A=\begin{bmatrix} 1 & 0\cdots\cdots 0 \\ * & 1\cdots\cdots 0 \\ \multicolumn{2}{c}{\cdots\cdots\cdots\cdots\cdots} \\ * & *\cdots\cdots 1 \end{bmatrix}$$

Because the extension of k associated with the unit matrix of degree one is k itself. Since the order of the group of all unipotent matrices in P_n is a power of p, so is the order of G. To prove the necessity we make use of the well known fact that, when the order of G is a power of p, there exists no other irreducible representation of G than the identical representation of degree one if we consider it over a finite field of characteristic p. Then A is equivalent to a representation of type (2.5). Therefore by Theorem 4 M is p-similar to a matrix of the form

$$M'=\begin{bmatrix} m_{11} & 0\cdots\cdots 0 \\ * & m_{22}\cdots\cdots 0 \\ \multicolumn{2}{c}{\cdots\cdots\cdots\cdots\cdots} \\ * & *\cdots m_{nn} \end{bmatrix}.$$

Since by Theorem 4 the extension of k associated with the matrix m_{ii} of degree one is k itself, there exist $c_i \in k$ such that $c_i^p = m_{ii}c_i$ and $c_i \neq 0$. If we put

$$C=\begin{bmatrix} c_1 & 0\cdots\cdots 0 \\ 0 & c_2\cdots\cdots 0 \\ \multicolumn{2}{c}{\cdots\cdots\cdots\cdots\cdots} \\ 0 & 0\cdots\cdots c_n \end{bmatrix},$$

then $(C^{-1})^p M'C$ is a unipotent matrix. This justifies the validity of our theorem.

In the following we shall give an example which shows how our theory can explain classical results regarding Artin-Schrier equations. By using the notation $\wp c$ for $c^p - c$, we denote by $\wp k$ the set of all elements $\wp c$ with $c \in k$. $\wp k$ is obviously a module over the prime field P. Let $\mathfrak{m}$ be a P-module with elements from k such that $\mathfrak{m}$ contains $\wp k$ and that the factor module $\mathfrak{m}/\wp k$ is of finite rank. It is well known that $\mathfrak{m}$ determines a finite abelian extension K of k whose Galois group is abelian of type $(p, \cdots, p)$. Assuming that the rank of $\mathfrak{m}/\wp k$ is $n-1$, we choose $m_2, \cdots, m_n$ as a system of representatives of a basis of $\mathfrak{m}/\wp k$. We consider a unipotent matrix M of degree n

$$M=\begin{bmatrix} 1 & N \\ 0 & I \end{bmatrix},$$

where $N=(m_2, \cdots, m_n)$ and I signifies the unit matrix of degree $n-1$. Putting $\wp\alpha_j=m_j$ with $\alpha_j \in \Omega$, we form a unipotent matrix A of degree n

$$A=\begin{bmatrix} 1 & A_2 \\ 0 & I \end{bmatrix},$$

where $A_2=(\alpha_2, \cdots, \alpha_n)$. Then A is a solution of $X^p=MX$. We see immediately that M is associated with $K=k(\alpha_2, \cdots, \alpha_n)$ and that the representation of its Galois group is of the type

$$A(\sigma)=\begin{bmatrix} 1 & \lambda_{12}(\sigma)\cdots\cdots\lambda_{1n}(\sigma) \\ 0 & 1\cdots\cdots\cdots\cdots 0 \\ \cdots & \cdots\cdots\cdots\cdots\cdots\cdots \\ 0 & 0\cdots\cdots\cdots\cdots 1 \end{bmatrix}.$$

For another basis $m_2', \cdots, m_n'$ of $\mathfrak{m}/\wp k$ we form the corresponding matrix

$$M'=\begin{bmatrix} 1 & N' \\ 0 & I \end{bmatrix},$$

where $N'=(m_2', \cdots, m_n')$. Since there exist elements $c_{\nu j}$ such that

$$m_j'+c_{1j}^p=c_{1j}+\sum_{\nu=2}^{n} m_\nu c_{\nu j},$$

$$j=2, \cdots, n$$

where $c_{1j} \in k$ and $c_{\nu j} \in P$ when $\nu>1$, we have

$$\begin{bmatrix} 1 & C_2 \\ 0 & C_1 \end{bmatrix}^p \begin{bmatrix} 1 & N' \\ 0 & I \end{bmatrix}=\begin{bmatrix} 1 & N \\ 0 & I \end{bmatrix}\begin{bmatrix} 1 & C_2 \\ 0 & C_1 \end{bmatrix},$$

where $C_2=(c_{12}, \cdots, c_{1n})$ and $C_1 \in P_{n-1}$. This shows that M' is p-similar to M.

The above example illustrates the fact that our theory generalizes the classical theory. However it should be noted that, when the Galois group is cyclic and its order a power of p, equations of Witt type are more convenient than ours. In view of this fact it is conjectured that a theory similar to ours may be established when we consider matrices with elements in the ring of Witt vectors.

References

[1] E. Inaba, On matrix equations for Galois extensions of fields with characteristic p, Natural Science Report of the Ochanomizu University, **12**, 26–36 (1961)

[2] E. Witt, Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, J. Reine Angew. Math., **176**, 126–140 (1936)