Natural Science Report, Ochanomizu University, Vol. 14, No. 1, 1963
お茶の水女子大学 自然科学報告 第14巻 第1号

Normal Form of Generalized Artin-Schreier Equations

Eizi Inaba (稲葉栄次)

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

(*Received April 1, 1963*)

Introduction

The concept of generalized Artin-Schreier equation was introduced in the author's previous article [2]. In the present paper we mean by generalized Artin-Schreier equation one that is slightly more general than that which was treated in the above-mentioned. At the beginning we shall briefly sketch the fundamental facts whose proofs are precisely similar to those of the corresponding results stated in [2]. Let k be a field of non-zero characteristic p. We put $q=p^{\nu}$ and assume that primitive $q-1$-th roots of unity are contained in k. The subfield of k which consists of all elements c with $c^q=c$ shall be denoted by P. Further we denote by k_n the ring of all $n\times n$-matrices with elements in k. When a matrix $C=(c_{ij})$ is given, we use the notation C^q for the matrix $(c_{ij}{}^q)$. A matrix M_1 in k_n is called *q-similar over k* to a matrix M_2, if there exists a non-singular matrix C in k_n such that $M_2=C^qM_1C^{-1}$. Let M be a non-singular matrix in k_n. Then the matrix equation $X^q=MX$ is called a *generalized Artin-Schreier equation*. If $A^q=MA$ holds for a non-singular matrix A in Ω_n, where Ω is an algebraic closure of k, then A is called a *non-singular solution*. By adjunction of all elements of A to k we obtain a finite Galois extension K of k, which is determined uniquely by the class of matrices q-similar over k to M, and K is called *the extension of k associated with M*. If G is the Galois group of K/k and $\sigma\in G$, then for a non-singular solution A we have $\sigma A=A\Lambda(\sigma)$, where $\Lambda(\sigma)\in P_n$. The matrices $\Lambda(\sigma)$ yield an isomorphic representation of G in P_n and this is called *the representation of G associated with M*. Now the theorems corresponding to Theorems 2 and 3 in [2] can be stated in the following manner.

THEOREM A. *A class of matrices q-similar over k to M determines the isomorphic representation of the Galois group associated with M uniquely to within equivalence.*

THEOREM B. *For a finite Galois extension K of k and for a class Λ of equivalent isomorphic representations in P_n of the Galois group of K/k there always exists a class of q-similar matrices in k_n such that this is*

determined uniquely by K and Λ.

The fact that these two theorems hold gives rise to the problem of finding a matrix of normal form, to which Section 1 is chiefly devoted. It deserves our notice that this can be solved by using the theory of semi-linear transformation, because the instances which necessitate the use of this theory are yet little known. Further we show in Section 2 that our method is more suitable for studying the nature of Galois extensions than that which was explained in [2]. In addition, it enables us to prove the theorem that there exist Galois extensions whose Galois groups are isomorphic to a given group of a certain kind, provided Hilbert's irreducibility theorem holds for k.

1. Matrices of normal form

In view of the fact that we can deal with ordinary similarity of matrices by considering k-modules, it is natural to do the same in our case. Let $\mathfrak{M}$ be a k-module of rank n and T be a left operator of $\mathfrak{M}$ which satisfies the following conditions

$$T(u+v)=T(u)+T(v)\,, \qquad \text{for} \quad u, v\in\mathfrak{M}$$

$$T(cu)=c^qT(u)\,, \qquad \text{for} \quad u\in\mathfrak{M} \quad \text{and} \quad c\in k\,.$$

Let $u_1, \cdots, u_n$ be a basis of $\mathfrak{M}$ and put

$$Tu_i=\sum_{j=1}^{n} m_{ji}u_j\,, \qquad m_{ji}\in k\,.$$

Then T is completely determined by the matrix $M=(m_{ij})$. If we take another basis $v_1, \cdots, v_n$ of $\mathfrak{M}$ such that

$$v_i=\sum_{j=1}^{n} c_{ji}u_j\,, \qquad c_{ij}\in k$$

and if we put

$$Tv_i=\sum_{j=1}^{n} m'_{ji}v_j\,, \qquad M'=(m'_{ij})\,, \qquad C=(c_{ij})\,,$$

then we have $M'=C^{-1}MC^q$ and hence the transpose of M' is q-similar over k to that of M. Next we consider polynomials $\sum a_ix^i$ of a variable x over k, for which we define multiplication by distributive law and

$$ax^ibx^j=ab^{q^i}x^{i+j}\,.$$

These polynomials form a non-commutative ring $k\langle x\rangle$ which has no zero-divisors. Then $\mathfrak{M}$ becomes a $k\langle x\rangle$-left module by defining

$$\left(\sum_{i=0}^{n} a_ix^i\right)u=\left(\sum_{i=0}^{n} a_iT^i\right)u\,.$$

Here we note that T is not necessarily a semi-linear transformation of $\mathfrak{M}$. Because the mapping $c\to c^q$ is not an automorphism of k unless k is perfect. Moreover every left ideal in $k\langle x\rangle$ is principal but not necessarily so is a right ideal. This fact hampers us from using the theory of elementary divisors. To overcome this difficulty we consider the maximal purely inseparable extension k^* of k.

PROPOSITION 1. *Let M be a non-singular matrix in $k_n^\times$. Then, if r is sufficiently large, M^{q^r} is a matrix in k_n, which is q-similar over k^* to M.*

Since k^* is purely inseparable over k, there certainly exists a positive integer r such that M^{q^r} is in k_n. Now we have $M^q=M^qMM^{-1}$, $M^{q^2}=(M^q)^qM^q(M^q)^{-1}$ and so on. Hence M is q-similar to M^{q^r} by the transitiveness of q-similarity.

PROPOSITION 2. *If two non-singular matrices M_1 and M_2 in k_n are q-similar over k^*, then they are also q-similar over k.*

Let $M_2=C^qM_1C^{-1}$, where C is a non-singular matrix in $k_n^\times$, and Σ be the extension of k obtained by adjoining all the elements of C to k. If Σ were distinct from k, then the exponent of inseparability of Σ^q over k would be less than that of Σ. Since we have $C=M_2^{-1}C^qM_1$ and since all the elements of the matrix on the right-hand side belong to Σ^q, we have a contradiction and our proposition is proved.

Now that the above two propositions have been established, we have every reason to expect that the present method will lead us to our destination. First we extend $\mathfrak{M}$ to the k^*-module $\mathfrak{M}^*$ with the same basis. Then T can be extended to a left operator of $\mathfrak{M}^*$, which is also denoted by T. Since the mapping $c\to c^q$ is an automorphism of k^*, T is a semi-linear transformation of $\mathfrak{M}^*$. Here we shall call T *regular* if T is an automorphism of $\mathfrak{M}^*$. The matrix M associated with T is non-singular if and only if T is regular. Next we extend $k\langle x\rangle$ to $k^*\langle x\rangle$. Then we see that every left ideal as well as every right ideal in $k^*\langle x\rangle$ is principal and that $\mathfrak{M}^*$ becomes a $k^*\langle x\rangle$-left module. Now let us use the abridged notation $\mathfrak{o}=k^*\langle x\rangle$. By a submodule of $\mathfrak{M}^*$ we understand an $\mathfrak{o}$-submodule of $\mathfrak{M}^*$. A submodule $\mathfrak{N}$ of $\mathfrak{M}^*$ is called cyclic when it is generated by a single element u. All elements $\gamma\in\mathfrak{o}$ with $\gamma u=0$ constitute a principal left ideal $\mathfrak{o}\alpha$ in $\mathfrak{o}$, which is called the order of u, and $\mathfrak{o}/\mathfrak{o}\alpha$ is $\mathfrak{o}$-isomorphic to $\mathfrak{N}$. We know that $\mathfrak{o}\beta$ is also the order of a generating element of $\mathfrak{N}$ if and only if $\mathfrak{o}/\mathfrak{o}\beta$ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{o}\alpha$. In the following we have to consider two cases separately: either k is infinite or finite. It is obvious that when k is finite we have $k^*=k$ and $\mathfrak{M}^*=\mathfrak{M}$.

LEMMA. *If k is infinite, every two-sided ideal $\mathfrak{J}$ in $\mathfrak{o}=k^*\langle x\rangle$ is generated by a power of x.*

It is known that there exists an element $\alpha\in\mathfrak{J}$ such that $\mathfrak{J}=\mathfrak{o}\alpha=\alpha\mathfrak{o}$. Let c be an arbitrary non-zero element of k^*. Then $c\alpha=\alpha d$

holds with $d\in k^*$. If α were not a power of x, then we would be able to put

$$\alpha=a_r x^r+\cdots+a_m x^m\ ,$$

where $r<m$ and $a_r\neq 0$, $a_m\neq 0$. Then

$$\alpha d=a_r d^{q^r}x^r+\cdots+a_m d^{q^m}x^m=c\alpha=c(a_r x^r+\cdots+a_m x^m)\ .$$

From this follows that $c^{q^{m-r}}=c$ for every non-zero element $c\in k^*$, which contradicts the assumption that k be infinite.

PROPOSITION 3. *Let T be a regular semi-linear transformation of $\mathfrak{M}^*$. If k is infinite, the $k^*\langle x\rangle$-module $\mathfrak{M}^*$ is cyclic and the order of its generating element is generated by a polynomial not divisible by x. If k is finite, then $\mathfrak{M}$ is a direct sum of cyclic submodules $\mathfrak{M}_i$, $i=1,\cdots,r$, where the order of any generating element u_i of $\mathfrak{M}_i$ is generated by a polynomial not divisible by x. Moreover, when $r>1$, we can choose generating elements u_i of $\mathfrak{M}_i$ such that the order of u_i is a total divisor of the order of u_{i+1}.*

By the theory of elementary divisors $\mathfrak{M}^*$ is a direct sum of cyclic submodules $\mathfrak{M}_i$, $i=1,\cdots,r$, such that the order $\mathfrak{o}\alpha_i$ of a generating element u_i of $\mathfrak{M}_i$ is a total divisor of the order $\mathfrak{o}\alpha_{i+1}$ of a generating element u_{i+1} of $\mathfrak{M}_{i+1}$. ([4], p. 44). Here we can assume that $\mathfrak{o}\alpha_i\neq\mathfrak{o}$, $i=1,\cdots,r$. If α_i were divisible by x, then, putting $\alpha_i=x\beta_i$, $\beta_i\in\mathfrak{o}$, we would have $\beta_i u_i\neq 0$ and $\alpha_i u_i=x\beta_i u_i=T\beta_i u_i=0$. This contradicts the assumption that T be regular. Hence $\alpha_1,\cdots,\alpha_r$ are all not divisible by x. When k is infinite we have to prove that $r=1$. If it were not the case, $\mathfrak{o}\alpha_1$ would be a total divisor of $\mathfrak{o}\alpha_r$. Then there would exist a two-sided ideal $\mathfrak{J}$ such that $\mathfrak{o}\alpha_1\supset\mathfrak{J}\supset\mathfrak{o}\alpha_r$, where $\mathfrak{J}\neq\mathfrak{o}$. Since by Lemma $\mathfrak{J}$ is generated by a power of x, α_r is divisible by x, which contradicts the above result.

THEOREM 1. *Let k be a field of non-zero characteristic p that contains q-1-th primitive roots of unity. If k is infinite, a non-singular matrix M in k_n is q-similar over k to a matrix of the form*

$$M'=\begin{pmatrix} 0 & 1 & 0\cdots\cdots 0\\ 0 & 0 & 1\cdots\cdots 0\\ \cdots & \cdots & \cdots\cdots\\ 0 & 0 & 0\cdots\cdots 1\\ -a_0 & -a_1 & -a_2\cdots\cdots -a_{n-1}\end{pmatrix}\tag{1.1}$$

If k is finite, then M is q-similar over k to a matrix of the form

$$\begin{pmatrix} M_1 & 0\cdots\cdots 0\\ 0 & M_2\cdots\cdots 0\\ \cdots & \cdots\cdots\\ 0 & 0\cdots\cdots M_r\end{pmatrix}\tag{1.2}$$

where each M_i is a matrix of form (1.1).

Let T be the regular semi-linear transformation of the k^*-module $\mathfrak{M}^*$ determined by the transpose of M. Then by Proposition 3 the $k^*\langle x\rangle$-module $\mathfrak{M}^*$ is a direct sum of cyclic submodules $\mathfrak{N}_i$, $i=1,\cdots,r$. We can choose a generating element u_i of $\mathfrak{N}_i$ such that the order of u_i is $\mathfrak{o}\alpha_i$ with $\alpha_i=x^{n_i}+\cdots+a_{i_1}x+a_{i_0}$, $a_{ij}\in k^*$. Then $u_i, xu_i, \cdots, x^{n_i-1}u_i$ constitute a k^*-basis of $\mathfrak{N}_i$. If k is finite, then $k^*=k$, $\mathfrak{M}^*=\mathfrak{M}$ and M is q-similar over k to a matrix of form (1.2). If k is infinite, then $r=1$ by Proposition 3 and M is q-similar over k^* to a matrix of the form

$$M^*=\begin{pmatrix} 0 & 1 & 0 \cdots\cdots 0 \\ 0 & 0 & 1 \cdots\cdots 0 \\ \cdots\cdots & & \cdots\cdots \\ 0 & 0 & 0 \cdots\cdots 1 \\ -a_0^* & -a_1^* & -a_2^* \cdots\cdots -a_{n-1}^* \end{pmatrix}$$

where $a_i^*\in k^*$. If $a_i^{*q^s}\in k$, $i=0,\cdots,n-1$, then we observe that the matrix $M'=M^{*q^s}$ is q-similar over k^* to M by Proposition 1. Hence M' is q-similar over k to M by Proposition 2 and the proof is concluded.

If a non-singular matrix M in k_n is of form (1.1), then it is called a *matrix of normal form* and the equation $X^q=MX$ a *normal generalized Artin-Schreier equation*. It is to be noted that, when M is of form (1.1), the $k\langle x\rangle$-module $\mathfrak{M}$ determined by the transpose of M is cyclic. In fact, there exists an element u in the $k\langle x\rangle$-module $\mathfrak{M}$ such that $u, xu, \cdots, x^{n-1}u$ form a k-basis of $\mathfrak{M}$. Morever the order of u is the left ideal generated by the polynomial $x^n+a_{n-1}x^{n-1}+\cdots+a_0$. This polynomial is called the *characteristic polynomial* of M (with respect to $k\langle x\rangle$).

REMARK. When k is finite, we can choose the matrix (1.2) such that the characteristic polynomial of M_{i+1} is divisible by that of M_i, $i=1,\cdots,r-1$.

PROPOSITION 4. *Let M and N be matrices of normal form in k_n, and α and β be the characteristic polynomials of M and N respectively. M is q-similar over k to N if and only if there exists $\gamma\in k\langle x\rangle$ such that $\beta\gamma$ is the least common multiple of α and γ and that α is relatively prime to γ.*

We put $\mathfrak{o}=k\langle x\rangle$. According to Ore, $\mathfrak{o}/\mathfrak{o}\alpha$ is $\mathfrak{o}$-isomorphic to $\mathfrak{o}/\mathfrak{o}\beta$ if and only if there exists γ in $\mathfrak{o}$ such that $\mathfrak{o}\gamma\cup\mathfrak{o}\alpha=\mathfrak{o}$ and $\mathfrak{o}\gamma\cap\mathfrak{o}\alpha=\mathfrak{o}\beta\gamma$. This verifies our Proposition. ([4], p. 33).

A non-singular matrix in k_n is called *q-reducible* over k, if it is q-similar over k to a matrix of the form

$$\begin{pmatrix} M_1 & 0 \\ M_3 & M_2 \end{pmatrix}$$

If M is not q-reducible over k, it is called *q-irreducible* over k.

PROPOSITION 5. *A non-singular matrix M of normal form in k_n is q-irreducible over k if and only if the characteristic polynomial of M with respect to $k\langle x\rangle$ is irreducible over k.*

We note that M is q-irreducible over k if and only if there exist no proper submodules of $\mathfrak{M}$. If α is the characteristic polynomial of M, then $\mathfrak{o}\alpha$ is the order of a generating element of $\mathfrak{M}$. We can easily verify that $\mathfrak{M}$ has no proper submodule if and only if α is irreducible. This concludes the proof of our proposition.

A non-singular matrix M in k_n is said to be *q-decomposable* if it is q-similar over k to a matrix of the form

$$\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} \tag{1.3}$$

M is called *q-indecomposable* if it is not q-decomposable.

PROPOSITION 6. *Let M be a non-singular matrix of normal form in k_n and α be the characteristic polynomial of M with respect to $k\langle x\rangle$. If α is the least common multiple of β and γ such that β is relatively prime to γ, we put $\alpha=\gamma^*\beta=\beta^*\gamma$. Then M is q-similar to a matrix of form* (1.3), *where β^* and γ^* are the characteristic polynomial of M_1 and M_2 respectively.*

Let u be the generating element of $\mathfrak{M}$ whose order is $\mathfrak{o}\alpha$. Since $\mathfrak{o}\beta\cup\mathfrak{o}\gamma=\mathfrak{o}$ and $\mathfrak{o}\beta\cap\mathfrak{o}\gamma=\mathfrak{o}\alpha$, $\mathfrak{M}$ is the direct sum of two submodules which are generated by βu and γu respectively. Furthermore the orders of βu and γu are $\mathfrak{o}\gamma^*$ and $\mathfrak{o}\beta^*$ respectively. This completes the proof of our proposition.

COROLLARY. *Let M be a non-singular matrix of normal form in k_n and α be the characteristic polynomial of M with respect to $k\langle x\rangle$. M is q-indecomposable if and only if α is not a least common multiple of two elements which are of positive degree and relatively prime to each other.*

PROPOSITION 7. *Let M be a non-singular matrix of normal form in k_n and α be the characteristic polynomial of M with respect to $k\langle x\rangle$. We put $\alpha=\pi_1\pi_2\cdots\pi_r$, where π_i is irreducible in $k\langle x\rangle$ with* deg $\pi_i=n_i$. *Then M is q-similar over k to the matrix*

$$\left(\begin{array}{c|c|c|c} M_1 & 0 & 0 & \cdots\cdots \\ \hline \begin{matrix}0\cdots\cdots 0\\ \cdots\cdots\cdots\\ 0\cdots\cdots 1\end{matrix} & M_2 & 0 & \cdots\cdots \\ \hline 0 & \begin{matrix}0\cdots\cdots 0\\ \cdots\cdots\cdots\\ 0\cdots\cdots 1\end{matrix} & M_3 & \cdots\cdots \\ \hline \multicolumn{4}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \end{array}\right) \tag{1.4}$$

where M_i is a q-irreducible matrix of normal form in k_{n_i} such that π_i is the characteristic polynomial of M_i.

Let u be the generating element of $\mathfrak{M}$ whose order is $o\alpha$. If we put

$$\begin{aligned} u_i^{(1)} &= x^{i-1}\pi_2 \cdots \pi_r u\,, \qquad i=1, \cdots, n_1\,; \\ u_i^{(2)} &= x^{i-1}\pi_3 \cdots \pi_r u\,, \qquad i=1, \cdots, n_2\,, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ u_i^{(r)} &= x^{i-1}u\,, \qquad i=1, \cdots, n_r\,, \end{aligned}$$

then $u_i^{(j)}$ constitute a P-basis of $\mathfrak{M}$, whence follows our assertion by using Proposition 5.

COROLLARY. *Let M be a non-singular matrix of normal form in k_n and α be the characteristic polynomial of M with respect to $k\langle x\rangle$ such that*

$$\alpha=(x-a_1)\cdots(x-a_r)\,, \qquad a_i \in k\,.$$

Then M is q-similar over k to a matrix of the form

$$\begin{pmatrix} a_1 & 0 & 0 & \cdots\cdots & 0 \\ 1 & a_2 & 0 & \cdots\cdots & 0 \\ 0 & 1 & a_3 & \cdots\cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 \cdots 1 & & a_r \end{pmatrix}$$

2. Galois extensions associated with matrices of normal form.

Let $k[x]$ be the commutative integral domain consisting of polynomials of x over k. In this section a polynomial of the form

$$\sum_{j=0}^{n} a_j x^{q^j} \tag{2.1}$$

plays an important role. By associating a polynomial $\sum a_j x^j$ in $k\langle x\rangle$ with the polynomial $\sum a_j x^{q^j}$ in $k[x]$, we obtain a one-to-one mapping φ of $k\langle x\rangle$ into $k[x]$. We can verify that φ satisfies the following equalities for any two polynomials $f(x)$ and $g(x)$ in $k\langle x\rangle$.

$$\varphi(f(x)+g(x))=\varphi f(x)+\varphi g(x)\,, \tag{2.2}$$

$$\varphi(f(x)g(x))=\varphi f(\varphi g(x))\,. \tag{2.3}$$

PROPOSITION 8. *If a polynomial $F(x)$ of form (2.1) is divisible by a polynomial $H(x)$ of form (2.1), then there exists a polynomial $Q(x)$ of form (2.1) such that $F(x)=Q(H(x))$.*

We put $F(x)=\varphi f(x)$, $H(x)=\varphi h(x)$, where $f(x)$ and $h(x)$ belong to $k\langle x\rangle$. There exist polynomials $q(x)$ and $r(x)$ in $k\langle x\rangle$ such that $f(x)=q(x)h(x)+r(x)$

with $\deg r(x)<\deg h(x)$. Then by virtue of (2.2) and (2.3) we have

$$F(x)=\varphi q(H(x))+\varphi r(x)\,,$$

and $\deg \varphi r(x)<\deg H(x)$. Since both $F(x)$ and $\varphi q(H(x))$ are divisible by $H(x)$, we have $\varphi r(x)=0$ and hence $F(x)=\varphi q(H(x))$.

COROLLARY. *A polynomial $f(x)$ of n-th degree is irreducible in $k\langle x\rangle$ if and only if $\varphi f(x)$ is not divisible by a polynomial $H(x)$ of form* (2.1) *with* $1<\deg H(x)<q^n$.

We shall say that $\varphi f(x)$ is *φ-irreducible over k* if $f(x)$ is irreducible in $k\langle x\rangle$. Let M be a matrix of normal form in k_n and $f(x)$ be the characteristic polynomial of M with respect to $k\langle x\rangle$. Then we shall call $\varphi f(x)$ the *characteristic polynomial* of M with respect to $k[x]$. The characteristic polynomial of M is separable over k if and only if M is non-singular. Because $\sum a_j x^{q^j}$ is separable if and only if $a_0\neq 0$. From (2.2), (2.3) and Proposition 4 we can derive the following

THEOREM 2. *Let M_1 and M_2 be two matrices of normal form in k_n with characteristic polynomials $F_1(x)$ and $F_2(x)$ respectively. M_1 is q-similar over k to M_2 if and only if there exists a polynomial $H(x)$ of form* (2.1) *such that the following conditions are satisfied:*

(1) *$H(x)/x$ is relatively prime to $F_1(x)/x$.*

(2) *Among polynomials of form* (2.1) *$F_2(H(x))$ is the common multiple of $F_1(x)$ and $H(x)$ with the least degree.*

We consider a polynomial $F(x)=\sum_{j=0}^{n} a_j x^{q^j}$ in $k[x]$, where $a_n\neq 0$ and $a_0\neq 0$. Since $F(x)$ is separable over k, it has exactly q^n distinct roots in an algebraic closure of k. If $\alpha_1,\cdots,\alpha_r$ are roots of $F(x)$, then we readily find that $\sum \rho_i\alpha_i$, $\rho_i\in P$, is also a root of $F(x)$. Hence all the roots of $F(x)$ form a P-module of rank n. Thus there exist roots $\alpha_1,\alpha_2,\cdots,\alpha_n$ of $F(x)$ such that these elements are linearly independent over P. Now we shall prove that the matrix

$$A=\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_n \\ \alpha_1^{q} & \alpha_2^{q} & \cdots\cdots & \alpha_n^{q} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{q^{n-1}} & \alpha_2^{q^{n-1}} & \cdots\cdots & \alpha_n^{q^{n-1}} \end{pmatrix} \tag{2.4}$$

is non-singular. For this it suffices to prove by induction on r that the determinant

$$\Delta_r=\begin{pmatrix} \alpha_1 & \alpha_2 & \cdots\cdots & \alpha_r \\ \alpha_1^{q} & \alpha_2^{q} & \cdots\cdots & \alpha_r^{q} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_1^{q^{r-1}} & \alpha_2^{q^{r-1}} & \cdots\cdots & \alpha_r^{q^{r-1}} \end{pmatrix}$$

is non-zero. It is obvious that $\Delta_1\neq 0$. When $r<n$, we assume that

$\Delta_r \neq 0$. If Δ_{r+1} were zero, there would exist $\gamma_i \in \Omega$, $i=1, \cdots, r$ such that

$$\alpha_{r+1}{}^{q^j} = \sum_{i=1}^{r} \gamma_i \alpha_i{}^{q^j}, \qquad j=0, 1, \cdots, r.$$

Raising both sides to the q-th power we have

$$\alpha_{r+1}{}^{q^j} = \sum_{i=1}^{r} \gamma_i{}^{q} \alpha_i{}^{q^j}, \qquad j=1, \cdots, r.$$

These two relations give rise to the equation

$$\sum_{i=1}^{n} (\gamma_i{}^{q} - \gamma_i) \alpha_i{}^{q^j} = 0, \qquad j=1, \cdots, r.$$

Since $\Delta_r{}^{q} \neq 0$, we have $\gamma_i{}^{q} = \gamma_i$ and therefore $\gamma_i \in P$. Then α_{r+1} would be a linear combination of $\alpha_1, \cdots, \alpha_r$ over P, which is contrary to our assumption. Hence $\Delta_{r+1} \neq 0$. From the above argument we have immediately the following

THEOREM 3. *Let M be a non-singular matrix of normal form in k_n and $F(x)$ be the characteristic polynomial of M. Then the matrix* (2.4) *is a non-singular solution of the normal generalized Artin-Schreier equation $X^q = MX$. Moreover the Galois extension K/k associated with M is the splitting field of $F(x)$.*

We note that Theorem 3 provides us with another proof of the theorem that any non-singular matrix in k_n is associated with a Galois extension of k.

THEOREM 4. *Let k be a field of non-zero characteristic p, in which $q-1$-th primitive roots of unity are contained. Then every finite Galois extension of k is the splitting field of a polynomial of form* (2.1).

When k is infinite, this theorem is immediate from Theorems B, 1 and 3. When k is finite, any finite Galois extension K of k is associated with a matrix of form (1.2) by Theorems B and 1. Let K_i be the Galois extension of k associated with M_i. Then we have $K_1 \subset K_2 \subset \cdots \subset K_r$ by the remark in the preceding section. Hence $K = K_r$, q. e. d.

Let M be a non-singular matrix of normal form in k_n. In the following we shall investigate close relationship between the characteristic polynomial $F(x)$ of M and the representation of the Galois group G of its splitting field K/k. Let $\alpha_1, \cdots, \alpha_n$ be a basis of the P-module $\mathfrak{L}(F)$, which consists of all roots of $F(x)$. Further let $P(G)$ be the group ring of G over P. Since every element of G permutes the roots of $F(x)$ among themselves, $\mathfrak{L}(F)$ becomes a $P(G)$-module, which yields an isomorphic representation Λ of G in P_n. If we consider the matrix (2.4), we see that Λ is nothing other than the representation of G associated with M.

THEOREM 5. *Let M be a non-singular matrix of normal form in k_n and $F(x)$ the characteristic polynomial of M. The isomorphic representation Λ of the Galois group G associated with M is irreducible if and only if $F(x)$ is φ-irreducible over k.*

If $F(x)$ is divisible by a polynomial $H(x)$ of form (2.1) with $1<\deg H(x)<q^n$, then by Proposition 8 there exists a polynomial $Q(x)$ of form (2.1) such that $F(x)=Q(H(x))$, where both $H(x)$ and $Q(x)$ are separable. Then $\mathfrak{L}(H)$ is a proper $P(G)$-submodule of $\mathfrak{L}(F)$ and hence Λ is reducible. Conversely, if Λ is reducible, there exists a proper $P(G)$-submodule $\mathfrak{N}$ of $\mathfrak{L}(F)$. It suffices to prove that there exists a separable polynomial $H(x)$ of form (2.1) in $k[x]$ such that $\mathfrak{N}=\mathfrak{L}(H)$. Let $\beta_1, \cdots, \beta_r$ be a basis of $\mathfrak{N}$ over, P, where $1\leqq r<n$. It is evident that all the roots of the polynomial $H_1(x)=x^q-\beta_1^{q-1}x$ form a P-module generated by β_1. We put successively

$$H_{i+1}(x)=H_i(x)^q-\beta_{i+1}^{q-1}H_i(x)\,, \qquad i=1, \cdots, r-1\,.$$

Then we see from (2.3) that $H_r(x)$ is of form (2.1) and that all the roots of $H_r(x)$ form the P-module $\mathfrak{N}$. Since $\mathfrak{N}$ is a $P(G)$-module, all the coefficients of $H_r(x)$ are left fixed by G. Hence $H_r(x)\in k[x]$ and $F(x)$ is divisible by $H_r(x)$. This concludes the proof of our theorem.

By making use of Proposition 5 and Corollary to Proposition 8 we can derive from the above theorem the following

COROLLARY. *The isomorphic representation of G associated with a non-singular matrix M in k_n is irreducible if and only if M is q-irreducible over k.*

THEOREM 6. *Let M be a non-singular matrix of normal form in k_n and $F(x)$ the characteristic polynomial of M. If there exist polynomials $F_1(x)$ and $F_2(x)$ of form (2.1) such that among polynomials of form (2.1) $F(x)$ is the common multiple of $F_1(x)$ and $F_2(x)$ with the least degree and that $F_1(x)/x$ is relatively prime to $F_2(x)/x$, and if we put $F(x)=H_2(F_1(x))=H_1(F_2(x))$, then M is q-similar to a matrix*

$$\begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix},$$

where $H_1(x)$ and $H_2(x)$ are the characteristic polynomials of M_1 and M_2 respectively. The Galois extension K/k associated with M is the composite of the two Galois extensions K_1 and K_2 associated with M_1 and M_2 respectively. Moreover the representation of the Galois group associated with M is equivalent to

$$\begin{pmatrix} \Lambda_1 & 0 \\ 0 & \Lambda_2 \end{pmatrix},$$

where Λ_1 and Λ_2 are the representations of the Galois groups associated with

M_1 and M_2 respectively.

The first part of this theorem follows from Proposition 6. To prove the second and the last part, let $\alpha_1, \cdots, \alpha_r$ be a basis of $\mathfrak{L}(F_1)$ and $\beta_1, \cdots, \beta_s$ be a basis of $\mathfrak{L}(F_2)$. Then $\alpha_1, \cdots, \alpha_r, \beta_1, \cdots, \beta_s$ form a basis of $\mathfrak{L}(F)$, because $\mathfrak{L}(F)$ is of rank $r+s$ over P and $F_1(x)$ has no root in common with $F_2(x)$. Hence we have $\mathfrak{L}(F)=\mathfrak{L}(F_1)+\mathfrak{L}(F_2)$. Then by Theorems 1 and 2 K is the composite of K_1 and K_2. By associating any root γ of $F(x)$ with $F_2(\gamma)$ we have a $P(G)$-homomorphic mapping of $\mathfrak{L}(F)$ onto $\mathfrak{L}(H_1)$, the kernel being $\mathfrak{L}(F_2)$. Therefore $\mathfrak{L}(H_1)$ is $P(G)$-isomorphic to $\mathfrak{L}(F_1)$ and similarly $\mathfrak{L}(H_2)$ to $\mathfrak{L}(F_2)$.

THEOREM 7. *Let M be a non-singular matrix of normal form in k_n and $F(x)$ be the characteristic polynomial of M. There exist φ-irreducible polynomials $F_i(x)$, $i=1, \cdots, r$ over k such that $F_i(x)$ is of form* (2.1) *with* $\deg F_i=q^{n_i}$ *and* $F(x)=F_1(F_2(\cdots F_r(x)\cdots))$. *Then the isomorphic representation of the Galois group associated with M is equivalent to the representation*

$$\begin{pmatrix} \Lambda_1 & 0 & & 0 \\ * & \Lambda_2 & & 0 \\ \cdots & \cdots & \cdots & \cdots \\ * & * & \cdots & \Lambda_i \end{pmatrix}$$

where Λ_i is an irreducible representation of G with degree n_i. Moreover Λ_i is the isomorphic representation of the Galois group of the splitting field of $F_i(x)$, which is a subfield of the splitting field of $F(x)$.

We put $f(x)=f_1(x)f_2(x)\cdots f_r(x)$ and $h_i(x)=f_i(x)\cdots f_r(x)$, where $f_i(x)$ is irreducible in $k\langle x\rangle$ with $\deg f_i(x)=n_i$. Putting $\varphi f_i(x)=F_i(x)$, $\varphi h_i(x)=H_i(x)$, we have

$$H_i(x)=F_i(H_{i+1}(x)), \qquad i=1, \cdots, r,$$

where $H_1(x)=F(x)$ and $H_{r+1}(x)=x$. Then $F_i(x)$ is φ-irreducible by Corollary to Proposition 8. Since all the coefficients of $H_i(x)$ belong to k, $\mathfrak{L}(H_i)$ is a $P(G)$-module. By associating $\gamma\in\mathfrak{L}(H_i)$ with $H_{i+1}(\gamma)\in\mathfrak{L}(F_i)$ we obtain a $P(G)$-homomorphic mapping of $\mathfrak{L}(H_i)$ onto $\mathfrak{L}(F_i)$, its kernel being $\mathfrak{L}(H_{i+1})$. Therefore the representation Λ_i of G determined by $\mathfrak{L}(H_i)/\mathfrak{L}(H_{i+1})$ is equivalent to the representation which is determined by $\mathfrak{L}(F_i)$. From this follows immediately our theorem.

From Theorem 7 we can deduce the following theorem which is a sharpened form of Theorem 6 in [2].

THEOREM 8. *Let k be a field of non-zero characteristic p that contains $q-1$-th primitive roots of unity. The order of the Galois group G associated with a non-singular matrix M in k_n is a power of p if and only if M is q-similar over k to a matrix of the form*

$$(2.5)\qquad \begin{pmatrix} 1 & 0 & 0 \cdots\cdots\cdots 0 \\ c_1 & 1 & 0 \cdots\cdots\cdots 0 \\ 0 & c_2 & 1 \cdots\cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \\ 0 & 0 & 0 \cdots c_{n-1} \quad 1 \end{pmatrix}$$

By Theorems 1 and 6 it suffices to prove the case when M is a q-indecomposable matrix of normal form. Let us use the same notation as in Proposition 7. By virtue of this proposition and Theorem 1 we see that M is q-similar over k to a matrix of form (1.4), where the characteristic polynomial π_i of M_i with respect to $k\langle x\rangle$ is irreducible. Now we can put

$$\varphi\pi_i = x g_{i_1}(x) \cdots\cdots g_{is_i}(x)\,,$$

where $g_{ij}(x)$ is irreducible in $k[x]$. Suppose that the order of G is a power of p. Since the splitting field K_{ij} of $g_{ij}(x)$ over k is a subfield of the Galois extension associated with M, the order of the Galois group G_{ij} of K_{ij}/k is also a power of p. Now G_{ij} is isomorphic to a permutation group of the roots of $g_{ij}(x)$. Since the degree of a transitive group divides its order, the order of G_{ij} is divisible by $\deg g_{ij}(x)$. If $\deg g_{ij}(x) > 1$, $j = 1, \cdots, s_i$, then $\sum \deg g_{ij}(x)$ would be divisible by p, which contradicts the fact that $\deg \varphi\pi_i$ is a power of p. Hence there exists a factor $g_{ij}(x)$ with $\deg g_{ij}(x) = 1$. If we put $g_{ij}(x) = x - a_i$ with $a_i \in k$, then $a_i \neq 0$ and $\varphi\pi_i$ is divisible by $x^q - a_i^{q-1}x$. Since $\varphi\pi_i$ is φ-irreducible over k, we have $\varphi\pi_i = x^q - a_i^{q-1}x$ and therefore $\pi_i = x - a_i^{q-1}$. Now Corollary to Proposition 7 shows that M is q-similar over k to the matrix

$$(2.6)\qquad M^* = \begin{pmatrix} a_1^{q-1} & 0 & 0 \cdots\cdots\cdots 0 \\ 1 & a_2^{q-1} & 0 \cdots\cdots\cdots 0 \\ 0 & 1 & a_3^{q-1} \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots & \cdots\cdots\cdots \\ 0 & 0 & 0 \quad 1 \quad a_n^{q-1} \end{pmatrix}.$$

If we put

$$C = \begin{pmatrix} a_1^{-1} & 0 \cdots\cdots 0 \\ 0 & a_2^{-1} \cdots\cdots 0 \\ \cdots\cdots & \cdots\cdots\cdots \\ 0 & 0 \cdots\cdots a_n^{-1} \end{pmatrix}$$

then $C^q M^* C^{-1}$ is of form (2.5), where $c_i \neq 0$, $i = 1, \cdots, n-1$.

Conversely, if M is q-similar over k to a matrix of form (2.5), where $c_i \neq 0$, $i = 1, \cdots, n-1$, then we easily find that there exists a matrix of form (2.6) such that it is q-similar over k to M. Since the

splitting field of $x^q-a_i^{q-1}x$ over k is k itself, we infer from Theorem 7 that the isomorphic representation of G is of the type

$$\begin{pmatrix} 1 & 0 \cdots\cdots 0 \\ * & 1 \cdots\cdots 0 \\ \cdots\cdots\cdots\cdots \\ * & * \cdots\cdots 1 \end{pmatrix}.$$

Then the order of G is a power of p, because so is the order of the group of all unipotent matrices in P_n. This completes the proof of our theorem.

Next we shall deal with an example which shows that our theory is quite instrumental in proving the existence of Galois extensions with Galois group isomorphic to a given group. Let $\mathfrak{G}$ be the group of all those non-singular matrices in P_n which are of the form

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

where Λ_i are $n_i \times n_i$-matrices, $i=1, \cdots, r$ and $n_1+\cdots+n_r=n$.

THEOREM 9. *Let k be a field of non-zero characteristic p and P be a finite field with q elements which are contained in k. Further we assume that Hilbert's irreducibility theorem holds for k. Then there exist Galois extensions of k with Galois group isomorphic to $\mathfrak{G}$.*

Let $y_1, y_2, \cdots, y_n$ be algebraically independent over k. We put $s_0=0$, $s_i=n_1+\cdots+n_i$, $i=1, \cdots, r$ and

$$F_i(x)=x^{q^{n_i}}+y_{s_{i-1}+1}x^{q^{n_i-1}}+\cdots+y_{s_i}x\,.$$

We define $H_i(x)$, $i=1, \cdots, r$, successively by

$$H_r(x)=F_r(x)\,, \qquad H_i(x)=F_i(H_{i+1}(x))\,, \qquad i=1, \cdots, r-1\,.$$

We put $\Sigma=k(y_1, \cdots, y_n)$ and denote by L the splitting field of $H_1(x)$ over Σ. We choose a basis $Y_1, \cdots, Y_n$ of $\mathfrak{L}(H_1)$ such that $Y_{s_{i-1}+1}, \cdots, Y_n$ form a basis of $\mathfrak{L}(H_i)$, $i=1, \cdots, r$. Then Σ is a subfield of $k(Y_1, \cdots, Y_n)$, because $y_1, \cdots, y_n$ are coefficients of $F_i(x)$, $i=1, \cdots, r$. Therefore we have $L=k(Y_1, \cdots, Y_n)$. Now we can define an automorphism σ of L by the relation

$$(\sigma Y_1, \cdots, \sigma Y_n)=(Y_1, \cdots, Y_n)N\,,$$

where N is an arbitrary matrix in $\mathfrak{G}$. The group $\mathfrak{G}^*$ of all these automorphisms of L is isomorphic to $\mathfrak{G}$. We have to show that the

field Σ^* of elements which are left fixed by $\mathfrak{G}^*$ in L is identical with Σ. Since $\mathfrak{L}(H_i)$ is left fixed by σ, the coefficients of $H_i(x)$ are all left fixed by σ. Hence the coefficients $y_1, \cdots, y_n$ of $F_i(x)$, $i=1, \cdots, r$, are all invariant under $\mathfrak{G}^*$. This shows that Σ is contained in Σ^*. Since the degree of L over Σ^* is equal to the order of $\mathfrak{G}$ and since the degree of L over Σ is not greater than the order of $\mathfrak{G}$ by Theorem 7, we see that $\Sigma^*=\Sigma$. Since Σ is purely transcendental over k, we can apply the well known technique as follows. ([5]). First we choose $b_i \in k$, $i=1, \cdots, n$, such that $\sigma\sum_{i=1}^{n} b_i Y_i$, $\sigma \in \mathfrak{G}^*$, are all distinct. Here we note that k is infinite, because Hilbert's irreducibility theorem holds for k. We put

$$F(x, y_1, \cdots, y_n)=\prod_{\sigma}(x-\sigma\sum_{i=1}^{n} b_i Y_i),$$

where σ ranges over $\mathfrak{G}^*$. Then the polynomial

$$y_{s_1} y_{s_2} \cdots y_{s_r} F(x, y_1, \cdots, y_n)$$

is irreducible with coefficients in Σ. By Hilbert's irreducibility theorem there exist $c_i \in k$, $i=1, \cdots, n$ such that $c_{s_1} c_{s_2} \cdots c_{s_r} F(x, c_1, \cdots, c_n)$ is irreducible over k. Let $\mathfrak{J}$ be the integral closure of the ring $k[y_1, \cdots, y_n]$ in L. By associating a polynomial $g(y_1, \cdots, y_n)$ with $g(c_1, \cdots, c_n)$ we obtain a homomorphism of $k[y_1, \cdots, y_n]$ onto k. The theory of places assures us that this homomorphism can be extended to a homomorphism ψ of $\mathfrak{J}$ into the algebraic closure of k. ([6]). Since Y_i all belong to $\mathfrak{J}$, ψY_i is finite. Further $\psi H_1(x)$ is separable over k since $c_{s_i} \neq 0$, $i=1, \cdots, r$. Let $\boldsymbol{L}$ be the splitting field of $\psi H_1(x)$ over k. The Galois group of $\boldsymbol{L}/k$ is isomorphic to a subgroup of $\mathfrak{G}$ by Theorem 7. Since $\boldsymbol{L}$ contains ψY_i, $i=1, \cdots, n$, all the roots of $F(x, c_1, \cdots, c_n)$ belong to $\boldsymbol{L}$. But $F(x, c_1, \cdots, c_n)$ is irreducible over k with degree equal to the order of $\mathfrak{G}$. Thus $[\boldsymbol{L}:k]$ is not less than the order of $\mathfrak{G}$ and hence the Galois group of $\boldsymbol{L}/k$ is isomorphic to $\mathfrak{G}$.

REMARK. It is known that Hilbert's irreducibility theorem holds for k if k is finitely generated and transcendental over the prime field ([3], [7]).

References

[1] E. Inaba, On matrix equations for Galois extensions of fields with characteristic p, Nat. Sci. Rep. Ochanomizu Univ., 12 (1961), pp. 26-36.

[2] E. Inaba, On generalized Artin-Schreier equations, Nat. Sci. Rep. Ochanomizu Univ., 13 (1962), pp. 1-13.

[3] E. Inaba, Über den Hilbertschen Irreduzibilitätssatz, Jap. Journ. of Math., 19 (1944), pp. 1-25.

[4] N. Jacobson, Theory of rings, New York, 1943.

[5] W. Krull, Elementare und Klassische Algebra, Berlin, 1959.
[6] S. Lang, Introduction to algebraic geometry, New York, 1958.
[7] G. Preuss und F.K. Schmidt, Über den Hilbertschen Irreduzibilitätssatz, Math. Nachr. 4 (1950), pp. 348–365.