Natural Science Report, Ochanomizu University, Vol. 14, No. 2, 1963
お茶の水女子大学 自然科学報告 第14巻 第2号

Galois Extensions Associated with Generalized Artin-Schreier Equations

Eizi Inaba (稲 葉 栄 次)

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

(*Received September 10, 1963*)

Let k be a field of non-zero characteristic p that contains a finite field P with $q=p^r$ elements. We denote by k_n the ring of all $n\times n$-matrices with elements in k and by C^q the matrix (c_{ij}^q) when a matrix $C=(c_{ij})$ is given. For a non-singular matrix M in k_n 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 of the equation. By adjunction of all elements of A to k we obtain a Galois extension K of k which is associated with the matrix M. It is known that the Galois group $\mathfrak{G}$ of K/k is isomorphic to a subgroup of $GL(n, P)$ (cf. Theorems 1 and 2 in [1]). It is desirable, however, to study more precisely the relationship between the form of the matrix M and the representation of the Galois group $\mathfrak{G}$. In the present note we shall give a theorem regarding this question and apply it to the problem of constructing Galois extensions over k.

Let $\mathfrak{o}$ be an arbitrary P-subalgebra of P_n and put $G(\mathfrak{o})=\mathfrak{o}\cap GL(n, P)$. Then $G(\mathfrak{o})$ is a subgroup of $GL(n,P)$ if $G(\mathfrak{o})$ is non-empty. The P-algebra $\mathfrak{o}$ can be extended to the algebra $\mathfrak{o}_k=k\otimes\mathfrak{o}$ over k. If we put $G_k(\mathfrak{o})=\mathfrak{o}_k\cap GL(n, k)$, then it is clear that $G_k(\mathfrak{o})\cap GL(n, P)=G(\mathfrak{o})$. A non-singular matrix M in k_n can be put into the form $M=\sum_{i=1}^{m} a_i u_i$, where $u_1, \cdots, u_m$ are matrices in P_n linearly independent over P and $a_1, \cdots, a_m$ elements in k linearly independent over P. Then $u_1, \cdots, u_m$ generate an algebra $\mathfrak{o}$ over P and M belongs to $G_k(\mathfrak{o})$. We can readily verify that $\mathfrak{o}$ is uniquely determined by the matrix M. We first prove the following

THEOREM 1. *If a non-singular matrix M belongs to $G_k(\mathfrak{o})$, then the Galois group $\mathfrak{G}$ of the Galois extension K over k associated with M is isomorphic to a subgroup of $G(\mathfrak{o})$.*

Before entering upon the proof of this theorem we need the following

LEMMA. *Let K be an arbitrary field containing P.*

(A) *$G_K(\mathfrak{o})$ is non-empty if and only if $\mathfrak{o}$ contains a unit matrix.*

(B) *If $G_K(\mathfrak{o})$ is non-empty, then $G_K(\mathfrak{o})$ is a subgroup of $GL(n, K)$.*

We have only to show that if $A \in G_K(\mathfrak{o})$ then $A^{-1} \in G_K(\mathfrak{o})$. Since $\mathfrak{o}_K$ is of finite rank over K, there exists the least integer s such that

$$\sum_{i=0}^{s} c_i A^i = 0, \quad c_i \in K, \quad c_s \neq 0 .$$

Here we have $c_0 \neq 0$, since otherwise we would have $\sum_{i=0}^{s-1} c_{i+1} A^i = 0$. Then $I = A \sum_{i=0}^{s-1} (-c_{i+1}/c_0) A^i$, where I is the unit matrix. Since $A^i \in \mathfrak{o}_K$ we have $A^{-1} \in G_K(\mathfrak{o})$.

Proof of Theorem 1. Let $u_1, \cdots, u_r$ be a P-basis of $\mathfrak{o}$ and consider the matrix

$$Y = \sum_{i=1}^{r} y_i u_i , \tag{1}$$

where $y_1, \cdots, y_r$ are quantities algebraically independent over k. Since $\mathfrak{o}$ contains the unit matrix I by the lemma, we can put $I = \sum \varepsilon_i u_i$, $\varepsilon_i \in P$. By specializing y_i to ε_i, we see that Y is a non-singular matrix. We put $\Sigma = k(y_1, \cdots, y_r)$. Since $Y^q Y^{-1} \in G_\Sigma(\mathfrak{o})$ by the lemma, we can put

$$N = Y^q Y^{-1} = \sum_{i=1}^{r} x_i u_i, \quad x_i \in \Sigma .$$

If we put $K = k(x_1, \cdots, x_r)$, then K is a subfield of Σ. Now Y is a non-singular solution of the generalized Artin-Schreier equation $X^q = NX$ with a matrix N in K_n. Substituting (1) into $Y^q = NY$, we obtain the relations

$$y_i^q = \sum_{j=1}^{r} y_j \sum_{s=1}^{r} x_s \rho_{ji}^{(s)}, \quad i = 1, \cdots, r , \tag{2}$$

where we put $u_s u_j = \sum \rho_{ji}^{(s)} u_i$, $\rho_{ji}^{(s)} \in P$. From (2) we infer that $y_1, \cdots, y_r$ are algebraic over K. (cf. the proof of Proposition 3 in [1]). Then Σ is finite over K and therefore $x_1, \cdots, x_r$ are algebraically independent over k. Let $\mathfrak{J}$ be the integral closure of the polynomial ring $R = k[x_1, \cdots, x_r]$ in Σ. Then $\mathfrak{J}$ is Noetherian since R is Noetherian. We contend that y_i all belong to $\mathfrak{J}$. In fact, choose a non-zero element c in R such that $cy_i \in \mathfrak{J}$, $i = 1, \cdots, r$. By using (2) repeatedly we see that $cy_i^{q^\lambda} \in \mathfrak{J}$ holds for $\lambda = 0, 1, 2, \cdots$. We consider the ideal $\mathfrak{A}_\lambda$ in $\mathfrak{J}$ generated by $cy_i, cy_i^q, \cdots, cy_i^{q^\lambda}$. Then we have a sequence of ideals: $\mathfrak{A}_0 \subset \cdots \subset \mathfrak{A}_\lambda \subset \mathfrak{A}_{\lambda+1} \subset \cdots$. Since $\mathfrak{J}$ is Noetherian, there exists $\mathfrak{A}_t$ such that $\mathfrak{A}_t = \mathfrak{A}_{t+1}$, whence it follows that y_i is integral over $\mathfrak{J}$ and hence $y_i \in \mathfrak{J}$. Now we put $M = \sum a_i u_i$, $a_i \in k$ and consider the k-homomorphism φ of R into k, which maps x_i on a_i, $i = 1, \cdots, r$. According to the theory of places, the homomorphism φ can be extended to a homomorphism of $\mathfrak{J}$ into the algebraic closure Ω of k. We denote this homomorphism also by φ and put $\varphi(y_i)=\alpha_i$, $i=1, \cdots, r$ with $\alpha_i \in \Omega$. Then $A=\sum \alpha_i u_i$ is a solution of the equation $X^q=MX$. Since $(\det Y)^{q-1}=\det N$ holds, we have $(\det A)^{q-1}=\det M \neq 0$. This shows that A is non-singular and consequently $A \in G_\Omega(\mathfrak{o})$. Now it is known that for $\sigma \in \mathfrak{G}$ we have $\sigma A=A\Lambda(\sigma)$ with a matrix $\Lambda(\sigma)$ in P_n and that $\Lambda(\sigma)$ yields an isomorphic representation of $\mathfrak{G}$ in P_n. Since both A and σA belong to $G_\Omega(\mathfrak{o})$, we have $\Lambda(\sigma) \ni G_\Omega(\mathfrak{o})$ by the lemma and hence $\Lambda(\sigma) \in G(\mathfrak{o})$. Thus $\mathfrak{G}$ is isomorphic to a subgroup of $G(\mathfrak{o})$.

THEOREM 2. *We assume that Hilbert's irreducibility theorem holds for* k. *Let* $\mathfrak{o}$ *be a* P-*subalgebra of* P_n *that contains the unit matrix. Then there exist infinitely many matrices* M *in* $G_k(\mathfrak{o})$ *such that the Galois group of the Galois extension associated with* M *is isomorphic to* $G(\mathfrak{o})$.

Let $u_1, \cdots, u_r$ be a P-basis of $\mathfrak{o}$ and $x_1, \cdots, x_r$ be quantities algebraically independent over k. We consider the non-singular matrix $N=\sum x_i u_i$. We observe, as in the proof of Theorem 1, that there exist elements $y_1, \cdots, y_r$ such that $Y=\sum y_i u_i$ is a non-singular solution of the equation $X^q=NX$. We put $K=k(x_1, \cdots, x_r)$ and denote by L the Galois extension of K associated with N. L is obviously contained in $K(y_1, \cdots, y_r)$. Since $Y^qY^{-1}=N$ holds, we see that K is a subfield of $k(y_1, \cdots, y_r)$ and therefore $K \subset L \subset k(y_1, \cdots, y_r)$. This also verifies that $y_1, \cdots, y_r$ are algebraically independent over k. Now we shall prove that the Galois group of L/K is isomorphic to $G(\mathfrak{o})$. For any matrix v in $G(\mathfrak{o})$ we put

$$u_i v=\sum_{j=1}^{r} \lambda_{ij}(v) u_j, \quad \lambda_{ij}(v) \in P, \quad i=1, \cdots, r .$$

Here the matrix $(\lambda_{ij}(v))$ is non-singular, because $u_1 v, \cdots, u_r v$ form a P-basis of $\mathfrak{o}$. We associate v with the k-automorphism σ_v of $k(y_1, \cdots, y_r)$ determined by

$$\sigma_v y_i=\sum_{j=1}^{r} \lambda_{ji}(v) y_j, \quad i=1, \cdots, r . \tag{3}$$

We readily see that in this way $G(\mathfrak{o})$ is isomorphically mapped onto a group $\mathfrak{G}$ of automorphisms of $k(y_1, \cdots, y_r)$. From (3) we have

$$\sigma_v Y=Yv, \quad \sigma_v Y^q=Y^q v ,$$

$$\sigma_v N=\sigma_v Y^q(\sigma_v Y)^{-1}=(Y^q v)(Yv)^{-1}=N ,$$

whence it follows that $\sigma_v x_i=x_i$. This verifies that every automorphism of $\mathfrak{G}$ leaves all elements of K fixed. By associating σ_v with the automorphism of L/K induced by σ_v, we obtain a homomorphic mapping of $\mathfrak{G}$ into the Galois group of L/K. But, since $\sigma_v Y=Y$ holds only when v is the unit matrix, this homomorphism is really an isomorphism. Thus, taking Theorem 1 into consideration, we find that the Galois group of L/K is isomorphic to $G(\mathfrak{o})$. Now it is easy to prove Theorem

2 by the well known technique if we consider the fact that K is purely transcendental over k.

It is to be noted that Theorem 2 is a generalization of Theorem 9 in [2].

Addendum to the author's previous article

Theorems 5 and 7 in [2] have already been proved by Ore in [3].

References

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

[2] E. Inaba, Normal form of generalized Artin-Schreier equations, Nat. Sci. Rep. Ochanomizu Univ. **14** (1963), pp. 1–15.

[3] O. Ore, A special class of polynomials, Trans. Amer. Math. Soc. **35** (1933), pp. 559–584.