Generalized Artin-Schreier Equations for Power Series Field

Nobuko Kubouchi (久保内信子)

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

Let $k=\Omega\{t\}$ be a power series field of one variable t whose coefficient field Ω is of characteristic p. We denote by $\wp c$ the element c^p-c and by $\wp k$ the set of all elements $\wp c$ with $c\in k$. If P is the prime field, k and $\wp k$ are P-modules, and $\wp k$ is a sub-module of k. Let $\mathfrak{m}$ be the set of all those elements of k whose terms with positive exponent all vanish. It is well known that we can form a system R of representatives of k modulo $\wp k$ by choosing elements of $\mathfrak{m}$. We assume that R contains zero. If a is a non-zero element of R and if α is a root of the Artin-Schreier equation $x^p-x-a=0$, then $K=k(\alpha)$ is a cyclic extension over k of degree p. In particular it is known that if a is in Ω then K/k is unramified and that, if the constant term of the element a is zero, then K/k is ramified. In the following we shall show that the above result can be extended to generalized Artin-Schreier equations.

Let k_n be the ring of square matrices of degree n with elements in k. We consider a matrix equation $X^p=MX$ for a unipotent matrix M in k_n. By adjoining to k all the elements of a unipotent solution A of $X^p=MX$, we have a Galois extension K over k and the order of its Galois group is a power of p. (cf. [1]). Two unipotent matrices M_1 and M_2 are called p-similar if there exists a non-singular matrix C such that $M_2=C^pM_1C^{-1}$. If M_1 and M_2 are p-similar, then both matrices are associated with the same Galois extension of k. (cf. [1])

THEOREM 1. *Let R be a system of representatives of cosets of k modulo $\wp k$ where we assume that R contains the zero element. Then any unipotent matrix in k_n is p-similar to one of those unipotent matrices whose elements lying outside the principal diagonal all belong to R.*

We shall prove the theorem by induction on n. When $n=2$, we consider the matrix

$$M=\begin{bmatrix}1 & a_{12}\\ 0 & 1\end{bmatrix}$$

in k_2. If $a\equiv a_{12}$ $(\wp k)$ and $a\in R$, we put $a_{12}=a-\wp c$, $c\in k$ and

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

Then we have

$$M^*=C^pMC^{-1}=\begin{bmatrix}1 & c^p\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & a_{12}\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & -c\\ 0 & 1\end{bmatrix}$$

$$=\begin{bmatrix}1 & a_{12}+\wp c\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}.$$

Thus the theorem is true when $n=2$. When $n>2$, we can put

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

where M_1 is a unipotent matrix of degree $n-1$. By induction hypothesis we can find a unipotent matrix C_1 in k_{n-1} such that $M_1'=C_1^pMC_1^{-1}$ satisfies the condition stated in the theorem. We put

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

and we have

$$M^*=C^pMC^{-1}=\begin{bmatrix}C_1^pM_1C_1^{-1} & C_1^pM_2\\ 0 & 1\end{bmatrix}$$

$$=\begin{bmatrix}M_1' & C_1^pM_2\\ 0 & 1\end{bmatrix}.$$

So we can assume from the begining that all elements of M_1 outside the principal diagonal belong to R. Now we put

$$M_1=\begin{bmatrix}m_{11} & \cdots & m_{1,n-1}\\ & & \\ m_{n-1,1} & \cdots & m_{n-1,n-1}\end{bmatrix} \qquad M_2=\begin{bmatrix}m_{1n}\\ m_{2n}\\ \vdots\\ m_{n-1n}\end{bmatrix}$$

and show that there are elements $c_1, c_2, \cdots, c_n$ in k and $m_{1n}^*, m_{2n}^*, \cdots, m_{n-1,n}^*$ in R such that these elements satisfy the following relation.

$$m_{in}-\sum_{i<j<n} m_{ij}c_j=m_{in}^*-\wp c_i \qquad i=1, 2, \cdots, n-1. \tag{1-2}$$

First we choose $m_{n-1,n}^*\in R$ and $c_{n-1}\in k$ such that $m_{n-1,n}=m_{n-1,n}^*-\wp c_{n-1}$. This means that (1-2) holds for $i=n-1$. We find easily that elements $c_{n-1}, \cdots, c_1$ in k and $m_{n-1,n}^*, \cdots, m_{1,n}^*$ in R can be determined successively so as to satisfy the relation (1-2). Putting

$$\Gamma=\begin{bmatrix}c_1\\ c_2\\ \vdots\\ c_{n-1}\end{bmatrix} \qquad M_2^*=\begin{bmatrix}m_{1n}^*\\ m_{2n}^*\\ \vdots\\ m_{n-1,n}^*\end{bmatrix},$$

we have from (1-2) the relation

$$M_2+\Gamma^p=M_1\Gamma+M_2^*. \tag{1-3}$$

If we consider two unipotent matrices

$$C=\begin{bmatrix} I_{n-1} & \Gamma \\ 0 & 1 \end{bmatrix} \qquad M^*=\begin{bmatrix} M_1 & M_2^* \\ 0 & 1 \end{bmatrix},$$

where I_{n-1} signifies the unit matrix of degree $n-1$. We have

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

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

Thus M is p-similar to M^* and the proof is complete. We note that this theorem is valid whenever k is a field of characteristic p.

We assume that every element m_{ij} of a unipotent matrix $M=(m_{ij})$ belongs to $\mathfrak{m}$. We consider the matrix $\overline{M}=(\overline{m}_{ij})$ in Ω_n where $\overline{m}_{ij}$ represents the constant term of the power series m_{ij}. Let Ω' be the extension over Ω determined by $\overline{M}$. Then the power series field $k'=\Omega'(t)$ with the new coefficient field Ω' is a Galois extension of k associated with $\overline{M}$ and unramified over k. We denote by $\mathfrak{m}_2'$ the set of all those elements of k' whose terms with non-negative exponent all vanish.

THEOREM 2. *Let M be a unipotent matrix whose elements are all in $\mathfrak{m}$, and k' be an extension of k associated with $\overline{M}$. If we consider M as a matrix over k', M is p-similar to a unipotent matrix whose elements outside the principal diagonal all belong to $\mathfrak{m}_2'$.*

If we put $M=\overline{M}+M^*$ and $M^*=(m_{ij}^*)$, then $m_{ij}^*=0$ for $i\geqq j$ and m_{ij}^* belongs to $\mathfrak{m}_2'$ for $i<j$. Let Ω^* be an algebraic closure of Ω and $\bar{C}$ be a unipotent solution of $X^p=\overline{M}X$ in Ω_n^*. From $\bar{C}^p=\overline{M}\bar{C}$ we have

$$(\bar{C}^{-1})^pM\bar{C}=(\bar{C}^{-1})^p(M^*+\overline{M})\bar{C}$$

$$=(\bar{C}^{-1})^pM^*\bar{C}+(\bar{C}^{-1})^p\overline{M}\bar{C}=(\bar{C}^{-1})^pM^*\bar{C}+I,$$

where I signifies the unit matrix. Now it is easy to see that all elements of this matrix belong to $\mathfrak{m}_2'$ except those lying on the principal diagonal.

Next we shall prove that if we regard M as a unipotent matrix in k_n' the Galois extension K' associated with M is purely ramified over k'. In fact this statement follows from the next theorem. We denote by $\mathfrak{m}_1$ the set of all elements of k whose terms with

positive exponent are all zero and whose constant term belongs to the prime field P, and by $\mathfrak{m}_2$ the set of all those elements of $\mathfrak{m}_1$ whose constant term is zero.

THEOREM 3. *The Galois extension K over k associated with a unipotent matrix M whose elements lying outside the principal diagonal all belong to $\mathfrak{m}_2$ is purely ramified over k.*

PROOF: Let $A=(\alpha_{ij})$ be a unipotent solution of $X^p=MX$, where

$$A=\begin{bmatrix} 1 & \alpha_{12} & \alpha_{13} & \cdots \\ 0 & 1 & \alpha_{23} & \cdots \\ \vdots & & 1 & \\ 0 & \cdots\cdots\cdots & & 1 \end{bmatrix}.$$

We place elements α_{ij} in the lexicographical order with respect to $j-i$ and i, namely,

$$\alpha_{12}, \alpha_{23}, \cdots, \alpha_{13}, \alpha_{24}, \cdots, \alpha_{1n}.$$

In this sequence, let α_1 be the first element that is not contained in k and α_2 the first element that is not contained in $k(\alpha_1)$ and so on. Thus we can determine $\alpha_1, \alpha_2, \cdots, \alpha_i$ succesively, where

$$\alpha_i=\alpha_{\lambda_i,\lambda_i+\nu_i} \qquad i=1, 2, \cdots.$$

By putting

$$K_i=k(\alpha_1, \alpha_2, \cdots, \alpha_i),$$

we have $K_i=K_{i-1}(\alpha_i)$ and $\alpha_i \notin K_{i-1}$. On the other hand we have

$$\wp\alpha_i=\sum_{\mu=1}^{\nu_i} m_{\lambda_i,\lambda_i+\mu}\alpha_{\lambda_i+\mu,\lambda_i+\nu_i}.$$

Hence $\wp\alpha_i$ is an element of K_{i-1}, and K_i is a cyclic extension of K_{i-1} with degree p. Now it suffices to prove that K_i is not unramified over K_{i-1} for $i=1, 2, \cdots$. Assume that $K_1/k, K_2/K_1, \cdots, K_{i-1}/K_{i-2}$ are all purely ramified and that K_i/K_{i-1} is unramified. We have only to show that this assumption leads to a contradiction. Since K_i is unramified over K_{i-1}, we have $K_i=K_{i-1}(\gamma)$ where $\wp\gamma=g\in\Omega$. On the other hand, since $K_i=K_{i-1}(\alpha_i)$, we have $\gamma=\rho\alpha_i+d$ where $\rho\in P$ and $d\in K_{i-1}$. Then we obtain

$$g=\rho\wp\alpha_i+\wp d. \tag{3-1}$$

Now any element of $K_i=k(\alpha_1, \cdots, \alpha_i)$ can be represented in the form

$$\sum c_{j_1\cdots j_i}\alpha_1^{j_1}\cdots\alpha_i^{j_i} \qquad 0\leqq j_\nu\leqq p-1. \tag{3-2}$$

where $c_{j_1\cdots j_i}\in k$. Let $L_i^{(1)}$ be the set of all those elements of K_i whose coefficients $c_{j_1\cdots j_i}$ in (3-2) all belong to $\mathfrak{m}_1$, and $L_i^{(2)}$ the set of all those

elements of K_i whose coefficients all belong to $\mathfrak{m}_2$. We consider the following three propositions:

(I) if $\beta\in K_i$ and $\wp\beta\in L_i^{(2)}$, then $\beta\in L_i^{(1)}$.

(II) if $\beta\in K_i$, $\wp\beta\in f+L_i^{(2)}$ and $f\in\Omega$, then $f\in\wp\Omega$.

(III) $\wp\alpha_{i+1}\in L_i^{(2)}$ and moreover for every element $\alpha_{\lambda\mu}$ which precedes α_{i+1} in the sequence we have $\wp\alpha_{\lambda\mu}\in L_i^{(2)}$.

Now if we suppose that (I), (II), and (III) are true, our proof is easy. In fact from (III) we have $\wp\alpha_i\in L_{i-1}^{(2)}$, and hence from (3-1) we get

$$\wp d=g-\rho\wp\alpha_i\in g+L_{i-1}^{(2)}\ .$$

Since $d\in K_{i-1}$ and $g\in\Omega$, we obtain $g\in\wp\Omega$ from (II). If we put $g=\wp h$, $h\in\Omega$, then we have $\gamma-h\in P$ from $g=\wp\gamma=\wp h$. Therefore γ belongs to Ω, which contradicts the fact that $K_i\neq K_{i-1}$.

Now we shall prove (I), (II) and (III) by induction on i. When $i=0$, since $K_0=k$, $L_0^{(1)}=\mathfrak{m}_1$ and $L_0^{(2)}=\mathfrak{m}_2$, our assertions can be stated in the following manner:

$(\mathrm{I})_0$ if $c\in k$ and $\wp c\in\mathfrak{m}_2$, then $c\in\mathfrak{m}_1$.

$(\mathrm{II})_0$ if $c\in k$, $\wp c\in f+\mathfrak{m}_2$ and $f\in\Omega$, then $f\in\wp\Omega$.

$(\mathrm{III})_0$ $\wp\alpha_1\in\mathfrak{m}_2$, and moreover $\wp\alpha_{\lambda\mu}\in\mathfrak{m}_2$ for any element $\alpha_{\lambda\mu}$ that precedes α_1 in the sequence.

$(\mathrm{I})_0$ and $(\mathrm{II})_0$ can be easily proved. The proof of $(\mathrm{III})_0$ runs as follows. When $\alpha_{\lambda,\lambda+\nu}$ is equal to α_1 or precedes α_1, we have

$$\wp\alpha_{\lambda,\lambda+\nu}=\sum_{\mu=1}^{\nu}m_{\lambda,\lambda+\mu}\alpha_{\lambda+\mu,\lambda+\nu}\ , \tag{3-3}$$

where $\alpha_{\lambda+\mu,\lambda+\nu}$ all belong to k. Therefore it suffices to show that $\alpha_{\lambda,\lambda+\nu}\in\mathfrak{m}_1$ if $\alpha_{\lambda,\lambda+\nu}\in k$, since $m_{\lambda,\lambda+\mu}\in\mathfrak{m}_2$ by the assumption. If $\alpha_{\lambda,\lambda+1}\in k$, then $\wp\alpha_{\lambda,\lambda+1}=m_{\lambda,\lambda+1}$, and from $(\mathrm{I})_0$ follows that $\alpha_{\lambda,\lambda+1}\in\mathfrak{m}_1$. If $\alpha_{\lambda,\lambda+2}\in k$, then

$$\wp\alpha_{\lambda,\lambda+2}=\sum_{\mu=1}^{2}m_{\lambda,\lambda+\mu}\alpha_{\lambda+\mu,\lambda+2}\ .$$

Since $\alpha_{\lambda,\lambda+1}$ all belong to $\mathfrak{m}_1$, $\wp\alpha_{\lambda,\lambda+2}\in\mathfrak{m}_2$, and hence $\alpha_{\lambda,\lambda+2}\in\mathfrak{m}_1$ by $(\mathrm{I})_0$. Thus we can repeat the same argument as long as $\alpha_{\lambda,\lambda+\nu}$ does not surpass α_1. Next, supposing that (I), (II) and (III) hold when $i=r-1$, we shall show that they also hold when $i=r$.

(I). If $\beta\in K_r$ and $\wp\beta\in L_r^{(2)}$, we have

$$\beta=\sum_{j=0}^{p-1}b_j\alpha_r^{\,j}$$

with $b_j\in K_{r-1}$, since $K_r=K_{r-1}(\alpha_r)$, and

$$\wp\beta=\beta^p-\beta=\sum_{j=0}^{p-1}b_j^{\,p}(\alpha_r+\wp\alpha_r)^j-\sum_{j=0}^{p-1}b_j\alpha_r^{\,j}\ . \tag{3-4}$$

Since $\wp\beta \in L_r^{(2)}$, every coefficient $c_{j_1\cdots j_i}$ in $\wp\beta = \sum c_{j_1\cdots j_i}\alpha_1^{j_1}\cdots\alpha_r^{j_r}$ is an element of $\mathfrak{m}_2$, and therefore every coefficient of $\alpha_r^{j_r}$ in (3-4) belongs to $L_{r-1}^{(2)}$. From (3-4) we have $\wp b_{p-1} = b_{p-1}^p - b_{p-1} \in L_{r-1}^{(2)}$. Hence $b_{p-1} \in L_{r-1}^{(1)}$ by induction hypothesis. Next we show that $b_\nu \in L_{r-1}^{(1)}$ when $b_{p-1}, \cdots, b_{\nu+1} \in L_{r-1}^{(1)}$. The coefficient of α_r^ν on the right-hand side of (3-4) becomes

$$\wp b_\nu + \sum_{j>\nu} b_j^p \binom{j}{\nu} (\wp\alpha_r)^{j-\nu} \in L_{r-1}^{(2)} . \tag{3-5}$$

Now, since by induction hypothesis $\wp\alpha_i \in L_{r-1}^{(2)}$ whenever $i \leqq r-1$, by making use of the relation $\alpha_i^p = \alpha_i + \wp\alpha_i$ we see that if $c_{j_1\cdots j_i}$ all belong to $\mathfrak{m}_1$ then $\sum c_{j_1\cdots j_i}\alpha_1^{j_1}\cdots\alpha_i^{j_i} \in L_i^{(1)}$ even when the exponents $j_1, \cdots, j_i$ surpass $p-1$. Hence we have seen that $L_{r-1}^{(1)}$ is a ring and moreover $L_{r-1}^{(2)}$ is an ideal in $L_{r-1}^{(1)}$. Since $\wp\alpha_r \in L_{r-1}^{(2)}$ by induction hypothesis, $(\wp\alpha_r)^{j-\nu} \in L_{r-1}^{(2)}$ for $j-\nu \geqq 1$. So we get

$$\sum_{j>\nu} b_j^p \binom{j}{\nu} (\wp\alpha_r)^{j-\nu} \in L_{r-1}^{(2)} .$$

From (3-5) we have $\wp b_\nu \in L_{r-1}^{(2)}$ and by induction hypothesis $b_\nu \in L_{r-1}^{(1)}$. Thus we have proved that $b_0, b_1, \cdots, b_{p-1} \in L_{r-1}^{(1)}$, and hence $\beta \in L_r^{(1)}$.

(II). We assume that $\beta \in K_r$, $\wp\beta \in f + L_r^{(2)}$ and $f \in \Omega$. If we put

$$\beta = \sum_{j=0}^{p-1} b_j \alpha_r^j$$

with $b_j \in K_{r-1}$, we have

$$\wp\beta - f = \sum_{j=0}^{p-1} b_j^p (\alpha_r + \wp\alpha_r)^j - \sum_{j=0}^{p-1} b_j \alpha_r^j - f . \tag{3-6}$$

Since $\wp\beta - f \in L_r^{(2)}$, we can prove in the same manner as above that $b_1, b_2, \cdots, b_{p-1}$ all belong to $L_{r-1}^{(1)}$. In (3-6), the coefficient of α_r^0 is

$$\wp b_0 - f + \sum_{j=1}^{p-1} b_j^p (\wp\alpha_r)^j$$

and this belongs to $L_{r-1}^{(2)}$. Since $\wp\alpha_r \in L_{r-1}^{(2)}$ by induction hypothesis, we have

$$\sum_{j=1}^{p-1} b_j^p (\wp\alpha_r)^j \in L_{r-1}^{(2)} .$$

Hence $\wp b_0 - f$ is an element of $L_{r-1}^{(2)}$. Then $\wp b_0 \in f + L_{r-1}^{(2)}$ and $b_0 \in K_{r-1}$. By induction hypothesis we have $f \in \wp\Omega$.

(III). When $\alpha_{\lambda,\lambda+\nu}$ is equal to α_{r+1} or precedes α_{r+1}, we have

$$\wp\alpha_{\lambda,\lambda+\nu} = \sum_{\mu=1}^{\nu} m_{\lambda,\lambda+\mu}\alpha_{\lambda+\mu,\lambda+\nu} , \tag{3-7}$$

where $\alpha_{\lambda+\mu,\lambda+\nu}$ all belong to K_r. Therefore it suffices to show that

$\alpha_{\lambda,\lambda+\nu}\in L_r^{(1)}$ if $\alpha_{\lambda,\lambda+\nu}\in K_r$. This is true when $\alpha_{\lambda,\lambda+\nu}$ is equal to α_r or precedes α_r, since $\alpha_{\lambda,\lambda+\nu}\in L_{r-1}^{(1)}$ because of the fact that $\wp\alpha_{\lambda,\lambda+\nu}\in L_{r-1}^{(2)}$. Since $L_{r-1}^{(1)}\subset L_r^{(1)}$, we have $\alpha_{\lambda,\lambda+\nu}\in L_r^{(1)}$. By making use of the relation (3-7) we can repeat the same argument as long as $\alpha_{\lambda,\lambda+\nu}$ does not surpass α_{r+1}. Thus we conclude the proof of our theorem.

In particular, when the coefficient field Ω is perfect, we can choose elements of R in the set $\mathfrak{m}_3$ of all elements of k whose terms with positive exponent vanish and whose terms with negative exponent divisible by p also vanish. In this case, if $c\in\mathfrak{m}_3$ and $c\notin\Omega$, then $c\notin\wp k$.

THEOREM 4. *Let k be a power series field with a perfect field Ω as its coefficient field and R be a system of representatives of k modulo $\wp k$ as was mentioned above. We assume that elements of a unipotent matrix M all belong to R except those on the principal diagonal. In order that the extension of k associated with M be unramified, it is necessary and sufficient that every element of M is contained in Ω.*

Since the sufficiency of the condition is clear, we shall prove its necessity. If Ω' is the extension of Ω defined by $\bar{M}$. We see in the course of the proof of Theorem 2 that there is a matrix $C\in\Omega_n'$ such that $C^pMC^{-1}=M'$, where elements of M' outside the principal diagonal all belong to $\mathfrak{m}_3'$. If M' is a unit matrix, then $M\in\Omega_n$ since $\Omega'\cap k=\Omega$. If we suppose that at least one of the elements of M does not belong to Ω, then there exists a non-zero element of M' which belongs to $\mathfrak{m}_3'$. Put $M'=(m_{ij}')$ and place elements m_{ij} $(i<j)$ in the order mentioned before. If $m_{i,i+\nu}'$ is the first non-zero element in this sequence, then we have $m_{i,i+\nu}'\notin\wp k'$ as was remarked above and for a solution $A=(\alpha_{ij})$ of $X^p=M'X$ holds the relation

$$\wp\alpha_{i,i+\nu}'=m_{i,i+\nu}'.$$

Then we see that $k'(\alpha_{i,i+\nu}')$ is ramified over k'. This shows that the extension of k' defined by M' is ramified over k'. Then the extension of k' associated with M is ramified over k' and hence the extension of k associated with M is also ramified over k. This completes the proof of our theorem.

References

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

[2] E. Inaba, On generalized Artin-Schreier equations, forthcoming in this journal.