ILLINOIS JOURNAL OF MATHEMATICS
Volume 41, Number 1, Spring 1997

GENERALIZED PUISEUX EXPANSIONS AND THEIR GALOIS GROUPS

SANJU VAIDYA

Section 1. Introduction

Let k be an algebraically closed field of characteristic p and let X be an indeterminate. Let $k((X))$ be the quotient field of the ring of formal power series (no convergence involved) in X over the field k. The field $k((X))$ is called the *field of meromorphic functions of X over k*. It is well known that in case $p = 0$, the Puiseux field $\cup_{n=1}^{\infty} k((X^{\frac{1}{n}}))$ of all Puiseux expansions is an algebraic closure of the field $k((X))$. But if $p \neq 0$, this is not the case. Chevalley [3] proved that polynomial $Z^p - Z - X^{-1}$ does not have a root in the Puiseux field.

Abhyankar [1] introduced the notion of generalized Puiseux expansion and proved the factorization of the said polynomial $Z^p - Z - X^{-1}$ into generalized Puiseux expansions. Using this, Huang, a doctoral student of Abhyankar, constructed a *generalized Puiseux field* and proved that it contains an algebraic closure of the meromorphic series field. The generalized Puiseux field consists of functions from the set Q of all rational numbers to the field k with some conditions on their support. In greater detail, a function f from the set Q to the field k is in the generalized Puiseux field iff its support $S(f)$ is a well ordered subset of the set Q and there exists an integer $m = m(f)$ such that for every $\alpha \in S(f)$ we have $\alpha m = \frac{n_\alpha}{p^{i_\alpha}}$ for some integers n_α and i_α. Huang [4] proved many fascinating results for generalized Puiseux elements whose supports are subsets of the set $\{\frac{-1}{p}, \frac{-1}{p^2}, \ldots, \frac{-1}{p^i}, \ldots\}$. For instance, he proved a criterion which says that such elements are algebraic over the field $k((X))$ iff they are *periodical* in case the field k is equal to algebraic closure of its prime field.

In this paper, we will investigate some functions of the generalized Puiseux field that are algebraic over the meromorphic series field; moreover, we will calculate their Galois groups. It turns out that Galois group of certain functions over the meromorphic series field is a semidirect product of a cyclic group and a direct sum of p cyclic groups. We also exhibit functions whose Galois groups are dihedral group, a certain type of Burnside group and a direct sum of p cyclic groups. Additionally, we will extend the criterion of Huang to a certain type of functions of the generalized Puiseux field in case the field k is not equal to algebraic closure of its prime field. We will also extend Huang's criterion to some generalized Puiseux elements whose supports are contained in the set $\{\frac{-l_i}{p^i} : i \in N\}$, where $(l_i)_{i \in N}$ is a sequence of positive integers satisfying certain constraints.

Received February 7, 1996.
1991 Mathematics Subject Classification. Primary 13; Secondary 12, 20.

In Section 2 we will describe the notation and terminology to be used throughout the paper. In Section 3 we will review some of the results and the criterion about some special elements of the generalized Puiseux field. These results are proved in Sections II and III of Huang [4]. In subsection (4.2) we will extend the criterion to certain type of elements of the generalized Puiseux field, while subsection (4.1) prepares the groundwork for it. Finally in Section 5, we will calculate Galois groups of some generalized Puiseux elements over the meromorphic series field.

Section 2. Notation and terminology

We will use the notation and terminology introduced in Sections II and III of Huang [4].

Here is greater detail. Let k be an algebraically closed field of characteristic p, where p is a prime number. Let X be transcendental over the field k. Let $k((X))$ denote the field of meromorphic functions in X over the field k. Let $\cup_{n=1}^{\infty} k((X^{\frac{1}{n}}))$ denote the Puiseux field. Let us define the set $A(p)$ by putting

$$A(p) = \left\{ f = \sum_{\alpha \in S(f)} a_\alpha X^\alpha \colon a_\alpha \in k,\ S(f) \text{ is a well ordered subset of } Q \right.$$
$$\text{and for each } f \text{ there exists a natural number } m = m(f) \text{ such}$$
$$\left. \text{that for every } \alpha \in S(f),\ \alpha m = \frac{l_\alpha}{p^{n_\alpha}} \text{ with } l_\alpha, n_\alpha \in Z \right\},$$

where the set Q is the set of all rational numbers which is a totally ordered group under addition with the usual ordering $\leq$ and a subset A of the set Q is well ordered if every non-empty subset S of the set A has a minimal element. Let us define the addition and multiplication for the elements in the set $A(p)$ as follows:

If $f = \sum_{\alpha \in S(f)} a_\alpha X^\alpha$ and $g = \sum_{\alpha \in S(g)} b_\alpha X^\alpha$ are any elements of the set $A(p)$, then

$$f + g = \sum_{\alpha \in S(f) \cup S(g)} (a_\alpha + b_\alpha) X^\alpha$$

and

$$fg = \sum_{(\beta,\gamma) \in S(f) \times S(g)} a_\beta b_\gamma X^{\beta+\gamma} = \sum_{\alpha \in S(f)+S(g)} \left(\sum_{\beta+\gamma=\alpha} a_\beta b_\gamma \right) X^\alpha.$$

Then the set $A(p)$ is a field under the operations of addition and multiplication and it may be called *the generalized Puiseux field.*

Section 3. A criterion

In this section, we will review some of the results and the criterion about some special type of elements of the generalized Puiseux field. These results are proved in Section II and III of Huang [4].

Before we do that, let us recall the following fundamental result which is proved in Chevalley [3].

THEOREM (3.1). *The polynomial* $Z^p - Z - X^{-1}$ *does not have a root in the Puiseux field* $\cup_{n=1}^{\infty} k((X^{\frac{1}{n}}))$. *Hence the Puiseux field is not algebraically closed.*

Abhyankar [1] introduced the notion of the generalized Puiseux expansion and proved the following factorization of the polynomial $Z^p - Z - X^{-1}$ into generalized Puiseux expansions.

THEOREM (3.2). *The polynomial* $Z^p - Z - X^{-1}$ *can be factored as follows.*

$$Z^p - Z - X^{-1} = \prod_{i=0}^{p-1} \left(Z - i - \sum_{j=1}^{\infty} X^{\frac{-1}{p^j}} \right)$$

Using this factorization, in Section II of [4], Huang constructed the generalized Puiseux field $A(p)$ and proved the following.

THEOREM (3.3). *The generalized Puiseux field* $A(p)$ *contains an algebraic closure of the field* $k((X))$.

In Section III of [4], Huang investigated functions f of the generalized Puiseux field $A(p)$ with supports $S(f) \subset \{\frac{-1}{p}, \frac{-1}{p^2}, \ldots, \frac{-1}{p^i}, \ldots\}$ and proved many elegant results. Some of them are described in Lemma (3.6), Corollary (3.7), Criterion (3.8), and Theorem (3.9). To understand them, we need the following definition.

Definition (3.4). Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in k$ for every $i \in N$. We say that f is *periodical* if $a_i = a_{i+n}$ for $i \geq m$ and $n \geq 1$.

Remark (3.5). If an element is periodical then it is algebraic over the field $k((X))$.

LEMMA (3.6). *Let* F *be a finite field contained in* k. *Let* $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, *with* $a_i \in F$, *for every* $i \in N$. *Then the element* f *is algebraic over the field* $k((X))$ *iff it is periodical.*

COROLLARY (3.7). *Let F_p be the prime field of the field k. Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in F_p$, for every $i \in N$. Then the element f is algebraic over the field $k((X))$ iff the real number $\sum_{i=1}^{\infty} \frac{a_i}{p^i}$ is a rational number.*

CRITERION (3.8). *Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in k$, for every $i \in N$. Assume that k is an algebraic closure of its prime field. Then the element f is algebraic over the field $k((X))$ iff it is periodical.*

In Theorem 9 of Section V of [4], Huang found the minimal polynomial of the element $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in k$, for every $i \in N$, if it is algebraic over the field $k((X))$. For that, he introduced the following notations.

Let Z be transcendental over the field $k((X))$. Given any positive integer n and constants $\alpha_1, \alpha_2, \ldots, \alpha_n$ in the field k, let

$$\begin{aligned} H_1(Z) &= Z^p - \alpha_1^{p-1} Z \\ H_2(Z) &= H_1^p(Z) - H_1^{p-1}(\alpha_2) H_1(Z) \end{aligned}$$

and, inductively,

$$H_n(Z) = H_{n-1}^p(Z) - H_{n-1}^{p-1}(\alpha_n) H_{n-1}(Z).$$

Now we can state Theorem 9 and Remark 3 of Section V of Huang [4]. They are respectively stated here in Theorem (3.9) and Remark (3.10).

THEOREM (3.9). *Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in k$, for every $i \in N$. Let $k((X))(f)$ be an abelian extension of $k((X))$ of degree p^n and all the conjugates of f be $f + m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n$ for $m_i = 0, 1, 2, \ldots, p-1$ for all i and $\alpha_i \in k$ for $i = 1, 2, \ldots, n$. Then the minimal polynomial of f over $k((X))$ is $H_n(Z) - H_n(f)$; or equivalently,*

$$\prod_{m_n=0}^{p-1} \cdots \prod_{m_1=0}^{p-1} (Z - f - m_1\alpha_1 - \cdots - m_n\alpha_n) = H_n(Z) - H_n(f).$$

Remark (3.10). Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$, with $a_i \in k$, for every $i \in N$. Assume that f satisfies a polynomial $F(Z) = Z^{p^n} + b_{n-1} Z^{p^{n-1}} + \cdots + b_1 Z^p + b_0 Z + b(X)$, where, $b_i \in k$ for $0 \leq i \leq n-1$, $b(X) \in k((X))$, and n is minimal. Then the polynomial $F(Z)$ is minimal polynomial of the element f over the field $k((X))$.

Section 4. Extension of the criterion

Subsection (4.1). In this subsection, we will prepare the groundwork to extend Criterion (3.8) for some special type of generalized Puiseux elements.

LEMMA (4.1.1). *Let* $f = \sum_{i=1}^{\infty} a_i X^{\frac{-1}{p^i}}$ *be algebraic over the field* $k((X))$, *where* $a_i \in k$ *for every* $i \in N$. *Then there exists a positive integer* n *and constants* $c_0, c_1, c_2, \ldots c_n$ *in the field* k *such that* $c_n \neq 0$ *and* $\sum_{i=1}^{\infty}(\sum_{j=0}^{n} c_j a_{j+i}^{p^j}) X^{\frac{-1}{p^i}} = 0$.

Proof. Since the element f is algebraic over the field $k((X))$, it is clear that the infinite set $\{1, f, f^p, f^{p^2}, \ldots, f^{p^i}, \ldots\}$ is linearly dependent over the field $k((X))$. So there exists a positive integer n and elements $b, b_0, b_1, \ldots, b_n$ in the field $k((X))$ such that $b_n \neq 0$ and

$$b = b_0 f + b_1 f^p + \cdots + b_n f^{p^n}. \tag{1}$$

In equation (1) we may assume that the elements $b_0, b_1, \ldots, b_n$ are in the ring $k[[X]]$. Writing equation (1) explicitly, we get

$$b - \sum_{j=0}^{n} b_j \sum_{i=1}^{j} a_i^{p^j} X^{-p^{j-i}} = \sum_{j=0}^{n} b_j \sum_{i=j+1}^{\infty} a_i^{p^j} X^{\frac{-1}{p^{i-j}}}$$

For $0 \leq j \leq n$, let c_j be the constant term of b_j. Then

$$\sum_{j=0}^{n} c_j \sum_{i=j+1}^{\infty} a_i^{p^j} X^{\frac{-1}{p^{i-j}}} = 0.$$

Hence the result follows.

In the following Lemmas (4.1.2) and (4.1.3), we will prove some interesting inequalities satisfied by permutations on n objects, where n is any positive integer greater than 1.

LEMMA (4.1.2). *Let there be given any integer* $n > 1$. *Then for every permutation* $\sigma \in S_n \setminus \{e\}$, *where* e *is the identity element of the permutation group* S_n, *we have* $\sum_{i=1}^{n}[i - \sigma(i)]p^{i-1} > 0$.

Proof. We will prove the lemma by using mathematical induction on n. In case $n = 2$, the result is obvious. So let $n > 2$. We will assume that the result is true for $n - 1$. Let there be given any permutation $\sigma \in S_n \setminus \{e\}$. Then there exists $j \in \{1, 2, \ldots, n\}$ such that $\sigma(j) = 1$. Let τ: $\{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$ be a function defined by putting

$$\tau(i) = \begin{cases} \sigma(i) - 1, & \text{if } i \in \{1, 2, \ldots, j-1\} \\ \sigma(i+1) - 1, & \text{if } i \in \{j, j+1, \ldots, n-1\}. \end{cases}$$

Then it is easy to see that $\tau \in S_{n-1}$. In case $j = 1$, clearly $\tau \in S_{n-1}$ and τ is not equal to the identity element of the group S_{n-1}. Therefore by induction hypothesis

we have $\sum_{i=1}^{n-1}[i-\tau(i)]p^{i-1} > 0$. Hence it is easy to see that $\sum_{i=3}^{n}[i-\sigma(i)]p^{i-1} > [\sigma(2)-2]p$. Consequently the result follows.

Henceforth assume that $j > 1$. Then we have $\sum_{i=1}^{n-1}[i-\tau(i)]p^{i-1} \geq 0$. Therefore, by expanding the sum, we get

$$\sum_{i=j+1}^{n}[i-\sigma(i)]p^{i-1} \geq \sum_{i=1}^{j-1}[\sigma(i)-(i+1)]p^{i}. \tag{2}$$

Using (2) we have $\sum_{i=1}^{n}[i-\sigma(i)]p^{i-1} \geq \sum_{i=1}^{j}[i-\sigma(i)]p^{i-1} + \sum_{i=1}^{j-1}[\sigma(i)-(i+1)]p^{i}$. By expanding the sums, we get $\sum_{i=1}^{n}[i-\sigma(i)]p^{i-1} \geq 1 - \sum_{i=1}^{j}\sigma(i)p^{i-1} + \sum_{i=1}^{j-1}\sigma(i)p^{i}$. Therefore, using $\sigma(j) = 1$, we get

$$\sum_{i=1}^{n}[i-\sigma(i)]p^{i-1} \geq \left[(p-1)\sum_{i=1}^{j-1}\sigma(i)p^{i-1}\right] - \left(p^{j-1}-1\right).$$

Consequently,

$$\sum_{i=1}^{n}[i-\sigma(i)]p^{i-1} \geq (p-1)\left(\sum_{i=1}^{j-1}[\sigma(i)-1]p^{i-1}\right). \tag{3}$$

From (3), and noting that $\sigma(j) = 1$, we get the result.

LEMMA (4.1.3). *Let there be given any integer $n > 1$. Let $\omega \in S_n$ be defined by putting $\omega(i) = n - i + 1$ for every $i \in \{1, 2, \ldots n\}$. Then for every permutation $\sigma \in S_n \setminus \{\omega\}$ we have $\sum_{i=1}^{n}[i+\sigma(i)-1]p^{i-1} > \sum_{i=1}^{n} np^{i-1}$.*

Proof. Let there be given any $\sigma \in S_n \setminus \{\omega\}$. Let $\sigma^* \in S_n$ be defined by putting $\sigma^*(i) = n+1-\sigma(i)$ for every $i \in \{1, 2, \ldots n\}$. Then it is easy to see that $\sigma^* \in S_n \setminus \{e\}$, where e is the identity element of the permutation group S_n. Consequently, using Lemma (4.1.2) for permutation σ^*, we get the result.

Subsection (4.2). In Theorems (4.2.1) and (4.2.2), we will extend Criterion (3.8) for some types of functions in case $k \neq$ an algebraic closure of its prime field F_p. Additionally, in Theorem (4.2.3) and Corollary (4.2.4), we will extend the criterion for some functions with special support.

THEOREM (4.2.1). *Assume that k is not an algebraic closure of its prime field F_p and let $Y \in k$ be transcendental over the field F_p. Let $f = \sum_{i=1}^{\infty} a_i Y^i X^{\frac{-1}{p^i}}$ be such that for every $i \in N$, the element a_i is in k and is algebraic over the prime field F_p of the field k. If the element f is algebraic over the field $k((X))$, then there exists a positive integer n such that $a_i = 0$ for every $i > n$.*

Proof. By Lemma (4.1.1), there exists a positive integer n and constants $c_0, c_1, \ldots, c_n$ in the field k such that $c_n \neq 0$ and

$$\sum_{i=1}^{\infty} \left(\sum_{j=0}^{n} c_j a_{j+i}^{p^j} Y^{(j+i)p^j} \right) X^{\frac{-1}{p^i}} = 0. \tag{4}$$

Therefore, for every $i \in N$, we have

$$\sum_{j=0}^{n} c_j a_{j+i}^{p^j} Y^{(j+i)p^j} = 0. \tag{5}$$

Let A be the infinite matrix whose order is $n+1$ by ∞ and whose $(i, j)^{\text{th}}$ term is $a_{j+i-1}^{p^{i-1}} Y^{(j+i-1)p^{i-1}}$. Hence from (4) and (5), it follows that $\operatorname{rank}(A) < n+1$. We will prove that $a_{i+n} = 0$ for every $i \in N$. Suppose there exists a positive integer l such that $a_{l+n} \neq 0$. Since $\operatorname{rank}(A) < n+1$, we have

$$\det \left(a_{l+j+i-2}^{p^{i-1}} Y^{(l+j+i-2)p^{i-1}} \right)_{1 \leq i \leq n+1, 1 \leq j \leq n+1} = 0.$$

Therefore, dividing by $Y^{(l-1)p^{i-1}}$ in the i^{th} row for every $i \in \{1, 2, \ldots, n+1\}$, we get

$$\det \left(a_{l+j+i-2}^{p^{i-1}} Y^{(i+j-1)p^{i-1}} \right)_{1 \leq i \leq n+1, 1 \leq j \leq n+1} = 0. \tag{6}$$

Let us put $m = n+1$. Let $\omega \in S_m$ be defined by putting $\omega(i) = m - i + 1$ for every $i \in \{1, 2, \ldots, m\}$. Then it is easy to see that

$$\operatorname{ord} \left(\prod_{i=1}^{m} a_{l+\omega(i)+i-2}^{p^{i-1}} Y^{(i+\omega(i)-1)p^{i-1}} \right) = \sum_{i=1}^{m} m p^{i-1}.$$

We also note that given any $\sigma \in S_m \setminus \{\omega\}$, if $a_{l+\sigma(i)+i-2} \neq 0$ for every $i \in \{1, 2, \ldots, m\}$, then

$$\operatorname{ord} \left(\prod_{i=1}^{m} a_{l+\sigma(i)+i-2}^{p^{i-1}} Y^{(i+\sigma(i)-1)p^{i-1}} \right) = \sum_{i=1}^{m} (i + \sigma(i) - 1) p^{i-1}.$$

Consequently, using Lemma (4.1.3), we get

$$\det \left(a_{l+j+i-2}^{p^{i-1}} Y^{(i+j-1)p^{i-1}} \right)_{1 \leq i \leq n+1, 1 \leq j \leq n+1} \neq 0. \tag{7}$$

Since statements (6) and (7) contradict each other, $a_{i+n} = 0$ for every $i \in N$.

THEOREM (4.2.2). *Assume that k is not an algebraic closure of its prime field F_p and let $Y \in k$ be transcendental over the field F_p. Let L be a finite field contained in k. Let $f = \sum_{i=1}^{\infty} f_i(Y) X^{\frac{-1}{p^i}}$, where $f_i(Y) \in L[Y]$ for each $i \in N$. Assume that there exists a positive integer M such that* $\deg f_i(Y) \leq M$ *for every $i \in N$. Then the element f is algebraic over the field $k((X))$ iff it is periodical.*

Proof. If the element f is periodical, then by Remark (3.5), it is algebraic over the field $k((X))$. To prove the converse, let the element f be algebraic over the field $k((X))$. By Lemma (4.1.1) there exists a positive integer n and constants $c_0, c_1, c_2, \ldots, c_n$ in the field k such that $c_n \neq 0$ and $\sum_{i=1}^{\infty}(\sum_{j=0}^{n} c_j f_{j+i}^{p^j}) X^{\frac{-1}{p^i}} = 0$. Therefore, for every $i \in N$, we have $\sum_{j=0}^{n} c_j f_{j+i}^{p^j} = 0$. So dividing by the constant c_n we get

$$f_{n+i}^{p^n} = -\left[\frac{c_0}{c_n} f_i + \frac{c_1}{c_n} f_{i+1}^{p} + \cdots + \frac{c_{n-1}}{c_n} f_{i+n-1}^{p^{n-1}}\right] \text{ for every } i \in N.$$

Thus for every $i \in N$, the polynomial f_{n+i} is completely determined by the n-tuple $(f_i, f_{i+1}, \ldots, f_{i+n-1})$. Let $F^{(i)} = (f_i, f_{i+1}, \ldots, f_{i+n-1})$. We note that if $F^{(i)} = F^{(j)}$ for some $i \neq j$ then $f_{n+i} = f_{n+j}$. This in turn implies that $F^{(i+1)} = F^{(j+1)}$ and so $f_{n+i+1} = f_{n+j+1}$. Hence it follows that $f_{n+i+r} = f_{n+j+r}$ for every $r \in N$. So the element f will be periodical. Now for each $i \in N$, the polynomial $f_i(Y)$ is in $L[Y]$, where L is a finite field and $\deg f_i(Y) \leq M$. So $\operatorname{card}\{F^{(i)}: i \in N\} < \infty$. Consequently, it follows that if the element f is algebraic over the field $k((X))$ then it is periodical.

THEOREM (4.2.3). *Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-l_i}{p^i}}$ be algebraic over the field $k((X))$, where, for every $i \in N$, $a_i \in k$, and $(l_i)_{i \in N}$ is a sequence of positive integers satisfying the following conditions.*

(i) $\gcd(l_i, p) = 1$ *for every* $i \in N$.
(ii) $l_i < l_{i+1}$ *for every* $i \in N$.
(iii) $pl_i > l_{i+1}$ *for every* $i \in N$.
(iv) *Given any positive integers n and s, we have $l_{n+t} - l_{m+t} \neq (s-r)p^t$ for any integers m, r, and t such that $0 \leq m < n$ and $0 \leq r < s \leq t$.*

Then there exists a positive integer e such that $a_i = 0$ for every $i > e$.

Proof. Since $pl_i > l_{i+1}$ for every $i \in N$, the sequence $\{\frac{-l_i}{p^i}: i \in N\}$ is increasing. So it follows that $f \in A(p)$. Since the element f is algebraic over the field $k((X))$, it is clear that the infinite set $\{1, f, f^p, f^{p^2}, \ldots, f^{p^i}, \ldots\}$ is linearly dependent over the field $k((X))$. So there exists a positive integer n and elements $b, b_0, b_1, \ldots, b_n$ in the field $k((X))$ such that $b_n \neq 0$ and

$$b = b_0 f + b_1 f^p + \cdots + b_n f^{p^n}. \tag{8}$$

In equation (8) we may assume that the elements $b_0, b_1, \ldots, b_n$ are in the ring $k[[X]]$. Let $b_m = \sum_{r=0}^{\infty} b_{mr} X^r$ for $0 \leq m \leq n$. Let $\operatorname{ord} b_n = s$. Since $b_n \neq 0$, we have $s \geq 0$,

$b_{ns} \neq 0$ and $b_{nr} = 0$ for every $r < s$. Hence it follows that

$$(9) \qquad b - \sum_{m=0}^{n} b_m \sum_{i=1}^{m} a_i^{p^m} X^{-l_i p^{m-i}} = \sum_{m=0}^{n} b_m \sum_{i=m+1}^{\infty} a_i^{p^m} X^{\frac{-l_i}{p^{i-m}}}.$$

$$= \sum_{r=0}^{\infty} \left(\sum_{m=0}^{n} b_{mr} \sum_{i=m+1}^{\infty} a_i^{p^m} X^{\frac{-l_i}{p^{i-m}}+r} \right)$$

$$= \sum_{r=0}^{\infty} \left(\sum_{m=0}^{n} b_{mr} \sum_{j=1}^{\infty} a_{m+j}^{p^m} X^{\frac{-l_{m+j}}{p^j}+r} \right).$$

We will prove that $b_{ns} a_{n+t}^{p^n} X^{\frac{-l_{n+t}}{p^t}+s} = 0$ for all $t \geq s$. So henceforth let $t \geq s$. Since the sequence $(l_i)_{i \in N}$ satisfies the conditions (i) and (ii), we get

$$\frac{-l_{n+t}}{p^t} + s \neq \frac{-l_{m+j}}{p^j} + r$$

for any positive integer $j \neq t$, any nonnegetive integer r and $0 \leq m \leq n$ and

$$\frac{-l_{n+t}}{p^t} + s \neq \frac{-l_{m+t}}{p^t} + r$$

for any positive integer $r > s$ and $0 \leq m \leq n$. Additionally, if $s > 0$, due to condition (iv), we get

$$\frac{-l_{n+t}}{p^t} + s \neq \frac{-l_{m+t}}{p^t} + r$$

for any m and r such that $0 \leq r < s$ and $0 \leq m < n$. We also note that on the left hand side of equation (9) all the exponents of X are integers. Consequently, it follows that $b_{ns} a_{n+t}^{p^n} X^{\frac{-l_{n+t}}{p^t}+s} = 0$. Since $b_{ns} \neq 0$, we get $a_{n+t} = 0$. Hence the result follows.

COROLLARY (4.2.4). *Let q be any given prime number. Let $f = \sum_{i=1}^{\infty} a_i X^{\frac{-q^i}{p^i}}$, where, for every $i \in N$, $a_i \in k$. If $p > q$, then the element f is algebraic over the field $k((X))$ iff there exists a positive integer n such that $a_i = 0$ for every $i > n$.*

Proof. Follows from Theorem (4.2.3).

Section 5. Galois groups

In this section we will calculate Galois groups of some special types of elements. It may be noted that Theorem (5.1) and Corollaries (5.2) to (5.4) deal with Galois groups of certain periodical generalized Puiseux elements while Theorem (5.5) and

Corollary (5.6) give Galois groups of some generalized Puiseux elements which are not periodical. Throughout this section, let L denote the field $k((X))$ and Z be transendental over an algebraic closure of the field L.

THEOREM (5.1). *Let m be any positive integer which is relatively prime to p. Let n be any given positive integer. Let $f = \sum_{i=1}^{\infty} X^{\frac{-1}{mp^{ni}}}$. Let G be the group of all L-automorphisms of the field $L(f)$. If the integer m divides the integer $p^n - 1$, then we have the following.*

(5.1.1) *The field $L(f)$ is a Galois (finite, normal, separable) extension of the field L of degree mp^n with the group G as the Galois group.*

(5.1.2) *There exists subgroups H and K of the Galois group G such that the subgroup H is isomorphic to a direct sum of n copies of cyclic group of order p and the subgroup K is isomorphic to the cyclic group of order m. Moreover, if $m > 1$, then the Galois group G is isomorphic to the semidirect product of H and K.*

Proof. Let $F(Z) = Z^{p^n} - Z - X^{\frac{-1}{m}}$. Clearly $F(f) = 0$ and all the roots of the polynomial $F(Z)$ are distinct. Therefore, the element f is separable algebraic over the field $k((X^{\frac{1}{m}}))$. Since $X^{\frac{1}{m}}$ is algebraic over the field L and the integer m is relatively prime to the integer p, it follows that the field $L(f)$ is a finite, algebraic, separable extension of the field L.

Let $S = \{Z^{p^r} + \cdots + b_i Z^{p^i} + \cdots + b\colon r \in N, b_i \in k$ for all i such that $0 \leq i \leq r-1$ and $b \in k((X^{\frac{1}{m}}))\}$. Let $G(Z)$ be any polynomial in the set S of degree p^r such that $G(f) = 0$. Then by Theorem (3.9) and Remark (3.10), it is enough to prove that $n \leq r$. Suppose $n > r$. Let $G(Z) = Z^{p^r} + \cdots + b_i Z^{p^i} + \cdots + b$, where $b_i \in k$ for $0 \leq i \leq r-1$ and $b \in k((X^{\frac{1}{m}}))$. Since $G(f) = 0$, we get

$$\sum_{j=1}^{\infty} X^{\frac{-1}{mp^{nj-r}}} + \cdots + b_i \sum_{j=1}^{\infty} X^{\frac{-1}{mp^{nj-i}}} + \cdots + b_0 \sum_{j=1}^{\infty} X^{\frac{-1}{mp^{nj}}} = -b$$

which gives a contradiction. (For example, the coefficient of the term $X^{\frac{-1}{mp^{n-r}}}$ is equal to 1 on one side and 0 on the other side of the equation.) Hence it follows that the polynomial $F(Z)$ is the minimal polynomial of the element f over the field $k((X^{\frac{1}{m}}))$. Therefore, $[L(f) : k((X^{\frac{1}{m}}))] = p^n$. Also obviously we have $[k((X^{\frac{1}{m}})) : L] = m$. Hence we get $[L(f) : L] = mp^n$.

Let $H(Z) = (Z^{p^n} - Z)^m - X^{-1}$. Then clearly $H(f) = 0$. Since $[L(f) : L] = mp^n$, the polynomial $H(Z)$ is the minimal polynomial of the element f over the field L. Let u be the m^{th} primitive root of unity and w the $(p^n - 1)^{\text{th}}$ primitive root of unity. Then it is easy to see that the set $\{u^i f\colon 1 \leq i \leq m\} \cup \{u^i f + w^j\colon 1 \leq i \leq$

m and $1 \leq j \leq p^n - 1\}$ is the set of all roots of the polynomial $H(Z)$. Consequently we get (5.1.1).

Let H be the Galois group of the field $L(f)$ over the field $k((X^{\frac{1}{m}}))$. As noted above, the polynomial $F(Z) = Z^{p^n} - Z - X^{\frac{-1}{m}}$ is the minimal polynomial of the element f over the field $k((X^{\frac{1}{m}}))$. Additionally, if f' is any root of the polynomial $F(Z)$ such that $f' \neq f$, then there exists $\alpha \in \{w^i\colon 1 \leq i \leq p^n - 1\}$ such that $f' = f + \alpha$. Hence it follows that the group H is isomorphic to a direct sum of n copies of cyclic group of order p. Let $\sigma \in H$ be such that $\sigma(f) = f + w$. Let $\tau \in G$ be such that $\tau(f) = uf$. Let K be the subgroup of the group G generated by the element τ. Obviously $\operatorname{ord}(K) = m$. It is also clear that if $m > 1$, then $\sigma\tau \neq \tau\sigma$ and $H \cap K = \{e\}$, where e is the identity element of the group G. Further we note that since the field $k((X^{\frac{1}{m}}))$ is a normal extension of the field L, the subgroup H is normal in the group G. Consequently, it follows that if $m > 1$, then the group G is isomorphic to the semidirect product of H and K. Thus we get (5.1.2).

COROLLARY (5.2). *Let n be any given positive integer. Let $f = \sum_{i=1}^{\infty} X^{\frac{-1}{p^{ni}}}$. Then the field $L(f)$ is a Galois extension of the field L. Moreover, the Galois group of the field $L(f)$ over the field L is isomorphic to a direct sum of n copies of cyclic group of order p.*

Proof. Follows from (5.1) by taking $m = 1$.

COROLLARY (5.3). *Let $f = \sum_{i=1}^{\infty} X^{\frac{-1}{2p^i}}$. Assume that $p > 2$. Then the field $L(f)$ is a Galois extension of the field L. Moreover, the Galois group of the field $L(f)$ over the field L is the dihedral group of order $2p$.*

Proof. Follows from (5.1) by taking $m = 2$ and $n = 1$.

COROLLARY (5.4). *Let $f = \sum_{i=1}^{\infty} X^{\frac{-1}{3p^i}}$. Assume that 3 divides the integer $p-1$. Then the field $L(f)$ is a Galois extension of the field L. Moreover, the Galois group of the field $L(f)$ over the field L is a nonabelian group of order $3p$. Additionally, if $p = 2.3^i + 1$ for some integer $i > 2$, then the Galois group is a Burnside group.*

Proof. Follows from (5.1) by taking $m = 3$ and $n = 1$ and the Theorem of Nagai [6].

THEOREM (5.5). *Let m and n be positive integers. Let $(r_i)_{i \in N}$ be a sequence of positive integers such that each integer r_i is prime to the integer p for $1 \leq i \leq n-1$, $r_n = 1$, and $r_{i+n} = r_i + mp^i$ for every $i \in N$.*

Let $f = \sum_{i=1}^{\infty} a_i^{\frac{1}{p^i}} X^{\frac{r_i}{p^i}}$, *where for every* $i \geq 1$, *the element* a_i *is a nonzero element of the field* k. *Let* $s = p^n - 1$, $d = \gcd(m, s)$, *and* $s^* = \frac{s}{d}$. *Assume that* $s^* > 1$. *Let* G *be the group of all* L*-automorphisms of the field* $k((X^{\frac{1}{s^*}}))(f)$. *Then we have the following.*

(5.5.1) *The field* $L(f)$ *is a finite, algebraic, separable extension of the field* L *of degree* p^n.

(5.5.2) *The field* $k((X^{\frac{1}{s^*}}))(f)$ *is the least normal extension of the field* L *containing the element* f. *Moreover, it is a Galois extension of the field* L *of degree* $s^* p^n$ *with the group* G *as the Galois group.*

(5.5.3) *There exist subgroups* H *and* K *of the Galois group* G *such that the subgroup* H *is isomorphic to a direct sum of* n *copies of cyclic group of order* p *and the subgroup* K *is isomorphic to the cyclic group of order* s^*. *Moreover, the Galois group* G *is isomorphic to the semidirect product of* H *and* K.

Proof. Let $F(Z) = Z^{p^n} - X^m Z - (a_n X^{r_n} + \sum_{i=1}^{n-1} a_i^{p^{n-i}} X^{r_i p^{n-i}})$. Then it is easy to see that $F(f) = 0$. Moreover, the polynomial $F(Z)$ is irreducible and separable over the field L. Hence (5.5.1) follows.

Let w be the $(p^n - 1)^{\text{th}}$ primitive root of unity. Let $m^* = \frac{m}{d}$. Then it is easy to see that the set $\{f + w^i X^{\frac{m^*}{s^*}} : 1 \leq i \leq s\} \cup \{f\}$ is the set of all roots of the polynomial $F(Z)$. Let E be a root field of the polynomial $Z^{p^n-1} - X^m$ over the field $L(f)$. Then by Lemma A5 of Abhyankar [2] we have $[E : L(f)] = s^*$. Therefore, $[E : L] = s^* p^n$. Let E^* be a root field of the polynomial $Z^{p^n-1} - X^m$ over the field L in the field E. Then by Lemma A5 of Abhyankar [2] we have $[E : E^*] = p^n$. Hence $E^* = k((X^{\frac{1}{s^*}}))$. Therefore it follows that $E = E^*(f)$. Since $[E : E^*] = p^n$, the polynomial $F(Z)$ is the minimal polynomial of the element f over the field $k((X^{\frac{1}{s^*}}))$. Consequently we get (5.5.2).

Let H be the Galois group of the field $k((X^{\frac{1}{s^*}}))(f)$ over the field $k((X^{\frac{1}{s^*}}))$. Let $\sigma_i(f) = f + w^i X^{\frac{m^*}{s^*}}$ for $1 \leq i \leq p^n - 1$. Then it is easy to see that the group H is isomorphic to a direct sum of n copies of cyclic group of order p. Additionally, since the field $k((X^{\frac{1}{s^*}}))$ is a normal extension of the field L, the subgroup H is normal in the group G. Let $\tau \in G$ be such that $\tau(f) = f$ and $\tau(X^{\frac{1}{s^*}}) = u X^{\frac{1}{s^*}}$, where u is an $(s^*)^{th}$ primitive root of unity. Let K be the subgroup of the group G generated by the element τ. Clearly $\text{ord}(K) = s^*$. It is also easy to see that $\sigma_1 \tau \neq \tau \sigma_1$ and $H \cap K = \{e\}$, where e is the identity element of the group G. Consequently it follows that the group G is isomorphic to the semidirect product of H and K. Thus we get (5.5.3).

COROLLARY (5.6). *Let m and n be positive integers. Let $(r_i)_{i\in N}$ be a sequence of positive integers such that each integer r_i is prime to p for $1 \leq i \leq n-1$, $r_n = 1$, and $r_{i+n} = r_i + mp^i$ for every $i \in N$. Let $f = \sum_{i=1}^{\infty} a_i^{\frac{1}{p^i}} X^{\frac{r_i}{p^i}}$, where for every $i \geq 1$, the element a_i is a nonzero element of the field k. If the integer $p^n - 1$ divides the integer m then the field $L(f)$ is a Galois extension of the field L of degree p^n and the Galois group is isomorphic to a direct sum of n copies of cyclic group of order p.*

Proof. The proof is subsumed in the proof of Theorem (5.5).

REFERENCES

1. S. Abhyankar, *Two notes on formal power series*, Proc. Amer. Math. Soc. **7** (1956), 903–905.
2. ———, *Coverings of algebraic curves*, Amer. J. Math. **LXXIX** (1957), 825–856.
3. C. Chevalley, *Introduction to the theory of algebraic functions of one variable*, Amer. Math. Soc., 1951.
4. Men-Fon Huang, Ph.D. Thesis, Purdue University, 1968.
5. N. Jacobson, *Basic algebra*, vol. 1, W. H. Freeman, San Francisco, 1974.
6. O. Nagai, *On transitive groups that contain non-abelian regular subgroups*, Osaka Math J. **13** (1961), 199–207.
7. O. Zariski and P. Samuel, *Commutative algebra*, vol. 1, 1959.
8. ———, *Commutative algebra*, vol. 2, 1960.

Dept. of Mathematics, Mount Saint Mary College, Newburgh, NY 12550
vaidya@whall1.msmc.edu