Galois Theory of Power Series Rings in Characteristic p
Author(s): Tzoung Tsieng Moh
Source: *American Journal of Mathematics*, Vol. 92, No. 4 (Oct., 1970), pp. 919-950
Published by: The Johns Hopkins University Press
Stable URL: http://www.jstor.org/stable/2373403
Accessed: 01/01/2014 23:09

Your use of the JSTOR archive indicates your acceptance of the Terms & Conditions of Use, available at
http://www.jstor.org/page/info/about/policies/terms.jsp

JSTOR is a not-for-profit service that helps scholars, researchers, and students discover, use, and build upon a wide range of content in a trusted digital archive. We use information technology and tools to increase productivity and facilitate new forms of scholarship. For more information about JSTOR, please contact support@jstor.org.

The Johns Hopkins University Press is collaborating with JSTOR to digitize, preserve and extend access to *American Journal of Mathematics.*

http://www.jstor.org

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

GALOIS THEORY OF POWER SERIES RINGS IN CHARACTERISTIC p.*

By TZOUNG TSIENG MOH.

Introduction. 0.1. Let k be an algebraically closed field of characteristic p, $k[[t]]$ be a one variable power series domain over k. One problem in algebraic geometry is to study some algebraic objects of $k[[t]]$ and try to deduce from them useful data concerning the geometry of algebraic curves.

In characteristic $p=0$ case, such useful notions like saturation theory [2] and characteristic pairs [1] are constructed and give a complete classification of singularities. In the $p\neq 0$ case, no applicable generalization of the above notions are easily deduced. One of the main reasons for this is that only in the $p=0$ case every finite algebraic extension is cyclic galois. These lead one to study the galois conditions in $p\neq 0$ case.

To analyze the galois condition of finite algebraic extensions, Professor Abhyankar observed the following: let k be an algebraically closed field of characteristic p, and let τ be an k-automorphism of $k[[t]]$ and $x, y\in k[[t]]$ with $k[[x]]=k[[y]]$, then $\operatorname{ord}(\tau(x)-x)=\operatorname{ord}(\tau(y)-y)$. Moreover, let τ be an k-automorphism of $k[[t]]$ of order p with $\operatorname{ord}(\tau(t)-t)=r$, $k[[x]]$ be the fixed domain of τ, and

$$\text{the differential multiplicity of } x=m\,(=\operatorname{ord}(dx/dt)+1).$$

Without loss of generality, we can assume $x=t^p+\lambda t^m+$ higher terms. Since $\operatorname{ord}(\tau(t^p)-t^p)=rp$, and $\operatorname{ord}(\tau(x-t^p)-(x-t^p))=m-1+r$, $\tau(x)=x$ implies $pr=m-1+r$, i.e., $r=(m-1/p-1)$. In other words $k[[t]]$ is galois over $k[[x]]$ of degree p implies $(m-1/p-1)$ is an integer. The above fact observed by Professor Abhyankar indicates that there is a close relation between "differential multiplicities" and "galois conditions." One consequence of this is the variation of least galois extensions of the local ring of a plane algebroid curve of multiplicity p with respect to different transversal parameters. Namely, let $k[[t]]$ be the integral closure of the local ring 0 of a plane algebroid curve of multiplicity p, and let y, z be transversal

* The work was supported by the National Science Foundation under NSF-GP-6388 at Purdue University in partial fulfillment of the requirements for the Ph. D. degree.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

parameters of 0, the $k[[t]]$ can be a cyclic galois extension over $k[[y]]$ while it is not a galois extension over $k[[z]]$.

Looking closely at the above fact observed by Professor Abhyankar, we were able to prove the converse of it (i.e., suppose $x \in k[[t]]$ with $\operatorname{ord} x = p$ and differential multiplicity of $x = m \neq \infty$, then $(p-1) \mid (m-1)$ implies $k[[t]]$ is galois over $k[[x]]$).

To generalize the method used by Professor Abhyankar, we consider the element $x = \lambda t^{mp^\nu} + \eta t^{np^\mu}$. A necessary and sufficient condition that there exists an k-automorphism τ of $k[[t]]$ such that

$$\operatorname{ord}(\tau(x) - x) > \min(\operatorname{ord}(\tau(t^{mp^\nu} - t^{mp^\nu}), \operatorname{ord}(\tau(t^{np^\mu}) - t^{np^\mu}))$$

will be $\operatorname{ord}(\tau(t^{mp^\nu}) - t^{mp^\nu}) = \operatorname{ord}(\tau(t^{np^\mu}) - t^{np^\mu})$. we observe that

$$\operatorname{ord}(\tau(t^{mp^\nu}) - t^{mp^\nu}) = (m-1+r)p^\nu \text{ and } \operatorname{ord}(\tau(t^{np^\mu}) - t^{np^\mu}) = (n-1+r)p^\mu$$

where $r = \operatorname{ord}(\tau(t) - t)$. Thus, $(m-1+r)p^\nu = (n-1+r)p^\mu$, i.e., $r = \dfrac{mp^\nu - np^\mu}{p^\mu - p^\nu} + 1$. The number $\dfrac{mp^\nu - np^\mu}{p^\mu - p^\nu} + 1$ is of interest and later on we find it is very useful in calculating $k[[t]]$. We call it the "p-distance" $\langle mp^\nu, np^\mu \rangle$ between mp^ν and np^μ. (See §1. Definition 1).

To generalize the notion of differential multiplicity, it is natural to consider "higher-differential multiplicity sequence (H. D. M. S.)." Namely, let $\operatorname{ord} x = d_0$ and d_1 be the order of the next term in x with exponent not divided by $\mid d_0 \mid$; successively let d_i be the order of the first term after $t^{d_{i-1}}$ in x with exponent not divided by $\mid d_{i-1} \mid$. Then $(d_0, d_1, \cdots, d_s)$ will be called the higher-differential multiplicity sequence of x with respect to t. (See §2. Definition 5).

Now let us consider the case that H. D. M. S. of $x = (d_0, d_1, d_2)$, say $x = \lambda_0 t^{d_0} + \lambda_1 t^{d_1} + \lambda_2 t^{d_2}$. Then a sufficient condition that there exists an automorphism τ such that

$$\operatorname{ord}(\tau(x) - x) > \min(\operatorname{ord}(\tau(t^{d_0}) - t^{d_0}),\ \operatorname{ord}(\tau(x - \lambda_0 t^{d_0}) - (x - \lambda_0 t^{d_0}))$$

will be

$$\operatorname{ord}(\tau(t^{d_0}) - t^{d_0}) = \min(\operatorname{ord}(\tau(t^{d_1}) - t^{d_1}),\ \operatorname{ord}(\tau(t^{d_2}) - t^{d_2})),$$

i.e., $r = \min(\langle d_0, d_1 \rangle, \langle d_0, d_2 \rangle)$ where $r = \operatorname{ord}(\tau(t) - t)$. These motivate us to give the definitions of G-character sequence $[t, x]$ and sequence of pre-higher ramification indices $[t, r]_r$ (see § 2. Definition 2 and Definition 3).

Note that if $x \in k[[t]]$ with $\operatorname{ord} x = p$ and differential multiplicity of $x = m < \infty$, then H. D. M. S. of $x = (p, m)$,

$$[t, x] = (p, m) \text{ and } [t, x]_r = \left(\frac{m-1}{p-1}\right).$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

It will be shown that the concepts introduced above are related to Hilbert's higher ramification theory (for the definition of higher ramifications, see [3]).

With above notions we prove:

COROLLARY OF PROPOSITION 7. *Suppose* $[t,x]_r=(r_1)$ *and* $\operatorname{ord}x=p^\nu$. *Then* $k[[t]]$ *is galois over* $k[[x]]$ *if and only if* r_1 *is an integer. Moreover, if* r_1 *is an integer then it is the higher ramification index.*

Note that the "only if" part is a generalization of the fact observed by Professor Abhyankar. Quite naturally we want to know what $[t,x]_r$ indicates in general. The following proposition is a partial generalization of the proceeding proposition.

PROPOSITION 7. *If* $k[[t]]$ *is a galois extension of algebraic degree* p^ν *over* $k[[x]]$, *then* $[t,x]_r=$ *sequence of higher ramification indices.*

Under the instruction of Professor Abhyankar we found that the converse of Proposition 7 was not true, namely, there exists $x\in k[[t]]$ such that $[t,x]_r$ consists of two integers while $k[[t]]$ is not galois over $k[[x]]$. At this time Professor Zariski suggested we study the following weaker problem: under what condition does these exist a y such that $k[[x]]\subset k[[y]]\subset k[[t]]$ with $k[[t]]$ galois over $k[[y]]$?

Following this suggestion we were able to prove Proposition 5 after extensively studying p-distance.

PROPOSITION 5. *Suppose* $\operatorname{ord}x=p^\nu$, $[t,x]=(a_0,\cdots,a_n)$ and $[t,x]_r=(r_1,\cdots,r_n)$ *is a sequence of integers. Then there exists a chain of power series rings*

$$k[[t]]=k[[y_0]]\supset k[[y_1]]\supset\cdots\supset k[[y_{n-1}]]\supset k[[y_n]]=k[[x]]$$

such that $k[[y_i]]$ *is a galois extension of* $k[[y_{i+1}]]$ *with higher ramification index* r_{i+1} *and algebraic degree* $\dfrac{|a_i|}{|a_{i+1}|}$.

To prove the converse we need Proposition 6 which is proved by using the technique of p-distance.

PROPOSITION 6. *Let* $k[[t]]\supset k[[\omega]]\supset k[[x]]$ *be a chain of separable extensions of degree* p^ν *and* p *respectively. If* $[t,\omega]_r$ *and* $[\omega,x]_r$ *are two sequences of integers then* $[t,x]_r$ *is a sequence of integers.*

Combining Propositions 5 and 6 we can state our main theorem:

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

THEOREM. *Suppose* $k[[t]]$ *is a separable algebraic extension over* $k[[x]]$. *Then there exists a chain of successive galois extensions between* $k[[t]]$ *and* $k[[x]]$ *if and only if* $[t,x]_r$ *is a sequence of integers.*

0.2. We wish to indicate the usefulness of the notions of $[t,x]$, $[t,x]_r$ and the theorem. We shall do so by listing some applications and pointing out that some theorems concerning least galois extensions or saturation rings in p-extensions can be generalized to the case that $[t,x]_r$ consists of one number. Namely

PROPOSITION 8 and COROLLARY. *Suppose* $[t,x]=(p^\nu,a_1)$, $[t,x]_r=(r_1)$, $|a_1|=1$. *Then the least galois extension over* $k[[x]]$ *containing* $k[[t]]$ *is tame over* $k[[t]]$. *Furthermore, the galois group is determined by the residue class of* $(a_1-1) \bmod (p^\nu-1)$.

PROPOSITION 10. *Suppose* $x,y \in k[[t]]$, $\operatorname{ord} x = p^\nu$, $\operatorname{ord} y = m$, $m > p^\nu$, $|m|=1$, $0=k[[x,y]]$ *and* $[t,x]_r=(r_1)$. *Then the saturation ring* 0_x *of* 0 *with respect to* x *is* $0+\Sigma M^b+M^m$ *where* $M=tk[[t]]$ *and* b *runs through all integers less than* m *with* $\langle b,m\rangle \leqq r_1$.

For the purpose of application, Professor Abhynakar pointed out the following proposition.

PROPOSITION 9. *Suppose* $\operatorname{ord} x = p^\nu$. *If* $[t,x]_r=(r_1,\cdots,r_n)$ *is a sequence of integers, then the least galois extension of* $k[[x]]$ *containing* $k[[t]]$ *is purely wild, i.e., the corresponding algebraic degree is* p^μ *for some* μ.

Concerning saturation, we have *Proposition* (see

COROLLARY of PROPOSITION 10). *Suppose*

$$z \in 0=k[[x,y]] \quad \operatorname{ord} z = \operatorname{ord} x = p^\nu,$$

and $\operatorname{ord} y = m > p^\nu$, $|m|=1$, $[t,x]=(r_1)$ $[t,z]=(s_1)$. *If* $s_1 \geqq r_1$ *then* $\tilde{0}_x \subset \tilde{0}_z$. *Furthermore, if* $v=1$, *then* $\tilde{0}_x=\tilde{0}_z=0+M^m$. *While in general* $\tilde{0}_x \neq \tilde{0}_z$.

It follows from above that if G-character sequences are different, then the saturation could be different with the same least galois extension and the same galois group.

0.3. In the remainder of the introduction we shall describe the content of each section.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

In § 1, we give the definitions of p-absolute value and p-distance and write down the basic properties of p-distance.

In § 2, we give the definition of $[t, x]$, and two equivalent definitions of the notion "standard expression" (Definition 4 and Proposition 1) which are useful afterwards. To finish § 2 we show that $[t, x]_r$ is a monotoic increasing sequence and all notions such as $[t, x]$, $[t, x]_r$ and H. D. M. S. are functions of a pair of fields $k[[t]]$, $k[[x]]$, i. e., they are independent of the basis chosen for $k[[t]]$ and $k[[x]]$.

In § 3, Lemmas 11, 12, and 13 are technical lemmas to prove Proposition 3. Lemma 14 is the essential part of the proof of Proposition 4. Combining Proposition 3 and 4, we get the sufficient part of the theorem and Proposition 5. Lemma 15 is the essential part of the proof of Proposition 6. Proposition 6 and Lemma 16 consists of the necessary part of the theorem.

In § 4, we prove Proposition 8 and Proposition 9 about least galois extensions.

In § 5, we discuss saturations. Proposition 10 will give a complete description of saturations if the G-character sequence consists of two elements.

1. *p*-Distance.

DEFINITION 1. *If a is a positive integer, then we define the p-absolute value of a, denoted by $|a|_p$ or $|a|$, as*

$$|a| = |a|_p = \max\{p^\nu : p^\nu \mid a\}.$$

If a and b are positive integers with $a < b$, then we define the p-distance of the pair a, b, denoted by $\langle a, b\rangle$, as

$$\langle a, b\rangle = \infty \text{ if } |a| \leqq |b|$$

$$\langle a, b\rangle = \frac{b - a}{|a| - |b|} + 1 \text{ if } |a| > |b|.$$

In the remaining part of this section, we will prove several lemmas concerning the properties of p-distance which will later be useful.

LEMMA 1. *Suppose $a < b < c$. Then*

1) $\langle a, b\rangle \neq \langle b, c\rangle$ *implies* $\langle a, c\rangle > \min(\langle a, b\rangle, \langle b, c\rangle)$
2) $\langle a, b\rangle = \langle b, c\rangle$ *implies* $\langle a, c\rangle = \min(\langle a, b\rangle, \langle b, c\rangle)$.

Proof.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

1) Consider the case $\langle a, b\rangle \neq \langle b, c\rangle$. If $\langle a, c\rangle = \infty$, then the inequality is obvious because either $\langle a, b\rangle$ or $\langle b, c\rangle$ is finite. If, on the other hand, $\langle a, c\rangle < \infty$, i. e., $|a| > |c|$, we consider the following three situations:

$\alpha)$ $|c| \geqq |b|$ $\beta)$ $|b| \geqq |a|$ $\gamma)$ $|c| < |b| < |a|$;

$\alpha)$ $|c| \geqq |b|$ implies $|a| > |b|$.
Thus since $c - a > b - a$ and $|a| - |c| \leqq |a| - |b|$ then

$\langle a, c\rangle > \langle a, b\rangle$.

$\beta)$ $|b| \geqq |c|$.
Since $c - a > c - b$ and $|a| - |c| \leqq |b| - |c|$ then

$\langle a, c\rangle > \langle b, c\rangle$.

$\gamma)$ $|c| < |b| < |a|$. We consider the following two situations A), B).

A) If $\langle a, b\rangle > \langle b, c\rangle$, i. e., $\dfrac{b-a}{|a|-|b|} > \dfrac{c-b}{|b|-|c|}$ then

$$\frac{(b-a)+(c-b)}{(|a|-|b|)+(|b|-|c|)} = \frac{c-a}{|a|-|c|} > \frac{c-b}{|b|-|c|}$$

B) If $\langle a, b\rangle < \langle b, c\rangle$, i. e., $\dfrac{b-a}{|a|-|b|} < \dfrac{c-b}{|b|-|c|}$ then

$$\frac{(b-a)-(c-b)}{(|a|-|b|)+(|b|-|c|)} = \frac{c-a}{|a|-|c|} > \frac{b-a}{|a|-|b|}$$

2) In the case $\langle a, b\rangle = \langle b, c\rangle$, we consider the following two situations:

$\alpha)$ $\langle a, b\rangle = \langle b, c\rangle = \infty$ $\beta)$ $\langle a, b\rangle = \langle b, c\rangle < \infty$.

$\alpha)$ $\langle a, b\rangle = \langle b, c\rangle = \infty$.

Since $|a| \leqq |b| \leqq |c|$, then $\langle a, c\rangle = \infty$.

$\beta)$ $\langle a, b\rangle = \langle b, c\rangle < \infty$ implies $|a| > |b| > |c|$ and

$$\frac{b-a}{|a|-|b|} = \frac{c-b}{|b|-|c|}, \text{ then } \frac{c-a}{|a|-|c|} = \frac{(b-a)+(c-b)}{(|a|-|b|)+(|b|-|c|)} = \frac{c-b}{|b|-|c|}$$

Q. E. D.

Using Lemma 1 repeatedly, we can prove the following lemma.

LEMMA 2. *Given* $a < b_1 < b_2 < \cdots < b_n < c$ *then*

$$\langle a, c\rangle \geqq \min(\langle a, b_1\rangle, \langle b_1, b_2\rangle \cdots \langle b_n, c\rangle).$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

The equality holds if and only if $\langle a, b_1\rangle = \langle b_1, b_2\rangle = \cdots = \langle b_n, c\rangle$.

LEMMA 3. *Suppose* $a < b < c$. *Then*

1) $\langle a, b\rangle > \langle a, c\rangle$ *implies* $\langle a, c\rangle > \langle b, c\rangle$.
2) $\langle a, b\rangle = \langle a, c\rangle < \infty$ *implies* $\langle a, c\rangle = \langle b, c\rangle$.

Proof.

1) By Lemma 1, $\langle a, c\rangle \geqq \min(\langle a, b\rangle, \langle b, c\rangle)$.
Since $\langle a, b\rangle > \langle a, c\rangle$, then $\langle a, b\rangle > \langle b, c\rangle$.
By Lemma 1 again, $\langle a, c\rangle > \langle b, c\rangle$.

2) $\langle a, b\rangle = \langle a, c\rangle < \infty$ implies $\dfrac{b-a}{|a|-|b|} = \dfrac{c-a}{|a|-|c|}$.
Thus since $c-a > b-a$, $|a|-|c| > |a|-|b|$, then

$$\frac{b-a}{|a|-|b|} = \frac{(c-a)-(b-a)}{(|a|-|c|)-(|a|-|b|)} = \frac{c-b}{|b|-|c|}$$

and $c > b$, $|b| > |c|$. Hence $\langle a, b\rangle = \langle a, c\rangle = \langle b, c\rangle$.

LEMMA 4. *Suppose* $a < b < c$. *Then* $\langle a, b\rangle < \langle b, c\rangle < \infty$ *implies* $\langle a, c\rangle < \langle b, c\rangle$.

Proof. $\langle a, b\rangle < \langle b, c\rangle < \infty$ implies $\dfrac{b-a}{|a|-|b|} < \dfrac{c-b}{|b|-|c|}$ and $|a| > |b| > |c|$. Thus since

$$\frac{c-a}{|a|-|c|} = \frac{(b-a)+(c-b)}{(|a|-|b|)+(|b|-|c|)} < \frac{c-b}{|b|-|c|},$$

then $\langle a, c\rangle < \langle b, c\rangle$.

LEMMA 5. *Suppose* $a < b < c$. *Then* $\langle a, b\rangle < \langle a, c\rangle < \infty$ *implies* $\langle b, c\rangle > \langle a, c\rangle$.

Proof. We consider the following two situations: 1) $\langle b, c\rangle = \infty$, 2) $\langle b, c\rangle < \infty$.

1) $\langle b, c\rangle = \infty$ implies $\langle b, c\rangle > \langle a, c\rangle$.
2) $\langle b, c\rangle < \infty$ implies $|a| > |b| > |c|$. Thus since

$$\frac{b-a}{|a|-|b|} < \frac{c-a}{|a|-|c|} \text{ then}$$

$$\frac{(c-a)-(b-a)}{(|a|-|c|)-(|b|-|a|)} = \frac{c-b}{|b|-|c|} > \frac{c-a}{|a|-|c|}$$

i. e., $\langle b, c\rangle > \langle a, c\rangle$.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

LEMMA 6. *Suppose* $a<b<c$. *Then* $\langle a,c\rangle>\langle b,c\rangle$ *implies* $\langle a,b\rangle \geqq \langle a,c\rangle$. *The equality holds only if* $\langle a,b\rangle=\infty$.

Proof. It is clear that $\langle a,b\rangle=\infty$ implies $\langle a,b\rangle \geqq \langle a,c\rangle$. Suppose $\langle a,b\rangle<\infty$, then since $|a|>|b|>|c|$ and $\langle a,c\rangle<\infty$, thus $\frac{c-a}{|a|-|c|} > \frac{c-b}{|b|-|c|}$, which implies

$$\frac{(c-a)-(c-b)}{(|a|-|c|)-(|b|-|c|)}=\frac{b-a}{|a|-|b|}>\frac{c-a}{|a|-|c|},$$

i.e., $\langle a,b\rangle>\langle a,c\rangle$.

LEMMA 7. *Suppose* $a<b<d$, $a<c<d$. *Then* $\langle a,b\rangle>\langle a,c\rangle$, $\langle b,c\rangle>\langle a,c\rangle$ *and* $|b|>|c|$ *implies* $\langle c,d\rangle \geqq \langle b,d\rangle$. *The equality holds if and only if* $\langle b,c\rangle=\infty$.

Proof. The lemma is clear if $\langle c,d\rangle=\infty$. We can assume $\langle c,d\rangle<\infty$, i.e., $|c|>|d|$. From our assumption that $|a|>|c|$, $|b|>|c|$. Now we consider the following two situations: 1) $|b|\geqq|a|>|c|>|d|$, 2) $|a|>|b|>|c|>|d|$.

1) $|b|\geqq|a|>|c|>|d|$ implies $d-a>d-b$

$|a|-|d|\leqq|b|-|d|$. Thus $\infty>\langle a,d\rangle>\langle b,d\rangle>\langle a,c\rangle$. Then

$$\frac{d-a}{|a|-|d|}>\frac{d-b}{|b|-|d|}>\frac{c-a}{|a|-|c|}$$

implies

$$\frac{d-c}{|c|-|d|}=\frac{(d-a)-(c-a)}{(|a|-|d|)-(|a|-|c|)}$$
$$>\frac{d-a}{|a|-|d|}>\frac{d-b}{|b|-|d|}$$

2) $|a|>|b|>|c|>|d|$.

Since $\infty>\langle a,b\rangle>\langle a,c\rangle$, then

$$\frac{b-a}{|a|-|b|}>\frac{c-a}{|a|-|c|}$$

which implies

$$\frac{d-b}{|b|-|d|}$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

$$= \frac{(d-a)-(b-a)}{(|a|-|d|)-(|a|-|b|)} > \frac{(d-a)-(c-a)}{(|a|-|d|)-(|a|-|d|)}$$
$$= \frac{d-a}{|c|-|d|}$$

i. e., $\langle c, d\rangle \geqq \langle b, d\rangle$. Q. E. D.

2. The standard expression and G-character sequence of a non-zero non-unit element in $k[[t]]$. In the rest of the paper let k be an algebraically closed field of characteristic $p \neq 0$, $k[[t]]$ be a powerseries ring of one variable over k, x be a nonzero non-unit element in $k[[t]]$, and

$$\operatorname{supp}_t x \equiv \operatorname{supp} x \equiv \{i \in Z \mid x = \Sigma a_j t^j, a_j \neq 0\}.$$

We make the following definition:

DEFINITION 2. *Suppose* $x \in k[[t]]$ *with* $0 < \operatorname{ord} x < \infty$. *We define* $[t, x]$, *the G-character sequence of* x *(with respect to* t*), as*

$$[t, x] \equiv (a_0, a_1, a_2, \cdots, a_n)$$

where

$a_0 = \operatorname{ord} x$

$a_1 = \operatorname{Max}\{i \in \operatorname{supp} x \mid \langle a_0, i\rangle = \operatorname{Min}\langle a_0, j\rangle,\ j \in \operatorname{supp} x$ *with* $j > \operatorname{ord} x$ *and* $i > \operatorname{ord} x\}$. *And in general for* $0 \leqq s \leqq n$

$a_s = \operatorname{Max}\{i \in \operatorname{supp} x \mid i > a_{s-1}$
$\langle a_{s-1}, i\rangle = \operatorname{Min}\langle a_{s-1}, j\rangle,\ j \in \operatorname{supp} x,$ *with* $j > a_{s-1}\}$,
$\langle a_n, i\rangle = \infty\ i \in \operatorname{supp} x$ *with* $i > a_n$.

DEFINITION 3. *Suppose* $x \in k[[t]]$ *with* $0 < \operatorname{ord} x < \infty$,

$$[t, x] = (a_0, a_1, a_2, \cdots, a_n).$$

We define $[t, x]_r$, *the pre-higher ramification indices sequence of* x *(with respect to* t*), as*

$$[t, x]_r \equiv (r_1, r_2, \cdots, r_n)$$

where

$$r_i = \langle a_{i-1}, a_i\rangle.$$

DEFINITION 4. *Each* x *has a unique expression of the form*

$$x = x_0 + x_1 + \cdots + x_n$$

with

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

1) $\operatorname{ord} x_i = a_i$ *where* $(a_0, a_1, \cdots, a_n) = [t, x]$
2) $\deg x_i < \operatorname{ord} x_{i+1}$.

We call such an expression of x the standard expression of x with respect to t.

We next give another characterization of the standard expression of x.

PROPOSITION 1. *The standard expression of x is $x = x_0 + x_1 + \cdots + x_n$ if and only if*

1) $\operatorname{ord} x_{i+1} > \deg x_i$
2) $x_i \neq 0$
3) $\langle \operatorname{ord} x_i, a\rangle \geqq \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle$ $a \in \operatorname{supp} x_i$ *with* $a > \operatorname{ord} x_i$
4) $\langle \operatorname{ord} x_n, a\rangle = \infty$ $a \in \operatorname{supp} x_n$ *with* $a > \operatorname{ord} x_n$
5) $\infty > \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle > \langle \operatorname{ord} x_{i-1}, \operatorname{ord} x_i\rangle$.

Proof. $\Leftarrow$ It suffices to prove

$$\langle \operatorname{ord} x_i, j\rangle > \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle$$

for each $j \in \operatorname{supp} x$ with $j > \operatorname{ord} x_{i+1}$.

Let $j \in \operatorname{supp} x_{i+s}$ where $i+1 \leqq i+s \leqq n$. Using Lemma 2 and conditions 3) and 5), we conclude $\langle \operatorname{ord} x_i, j\rangle > \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle$.

$\Rightarrow$ 1), 2), 3), 4) are obvious from the definitions of $[t, x]$ and the standard expression. From the fact

$$\infty > \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle > \langle \operatorname{ord} x_{i-1}, \operatorname{ord} x_i\rangle$$

and Lemma 5 we deduce

$$\infty > \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1}\rangle > \langle \operatorname{orw} x_{i-1}, \operatorname{ord} x_i\rangle$$

which proves 5).

Given $x \in k[[t]]$, we associate with x another sequence of numbers, the higher differential multiplicity sequence (H. D. M. S.), defined as follows::

DEFINITION 5. *Given any positive integer i, let*

$$\operatorname{ord} x \bmod R^{|i|} = \max\{\operatorname{ord} y \mid y \in x + R^{|i|}\}$$

where

$$x \in R = k[[t]].$$

The higher differential multiplicity sequence (H. D. M. S.) *of x is given by:*

$$\text{H. D. M. S.} = (d_0, d_1, \cdots, d_s)$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

where

$$\begin{aligned} d_0 &= \operatorname{ord} x \\ d_1 &= \operatorname{ord} x \bmod R^{|d_0|} \\ &\vdots \\ d_i &= \operatorname{ord} x \bmod R^{|d_{i-1}|} \\ &\vdots \\ d_s &= \operatorname{ord} x \bmod R^{|d_{s-1}|} \end{aligned}$$

and

$$\operatorname{ord} x \bmod R^{|d_s|} = \infty .$$

Remark. $d_i = \min\{j \mid j \in \operatorname{supp} x \text{ with } |j| < |d_{i-1}|\}$.

Using the notion of the higher differential multiplicity sequence, we will give another way of calculating the G-character sequence.

PROPOSITION 2. *Suppose* $x \in k[[t]]$ *with* $0 < \operatorname{ord} x < \infty$. *Let*

$$(a_0, a_1, \cdots, a_n)$$

be the G-character sequence of x *with respect to* t *and let* $(d_0, d_1, \cdots, d_n)$ *be the higher differential multiplicity sequence of* x *with respect to* t. *Then*

1) $a_0 = d_0$

2) $a_i = \max\{d_j \mid d_j > a_{i-1} \text{ with } \langle a_{i+1}, d_j\rangle = \min\langle a_{i-1}, d_k\rangle\}$.

Proof. Let $\alpha \in \operatorname{supp} x$ with $\alpha > a_{i-1}$. Suppose $a_{i-1} \leqq d_k < \alpha < d_{k+1}$ and $\langle a_{i-1}, \alpha\rangle < \infty$. Then $|a_{i-1}| > |\alpha|$, which implies $a_{i-1} < d_k$. By the definition of H. D. M. S. we have $|\alpha| \geqq |d_k|$, hence $\langle a_{i-1}, \alpha\rangle > \langle a_{i-1}, d_k\rangle$. This means $\langle a_{i-1}, \alpha\rangle$ can not assume the minimum value.

LEMMA 8. *Suppose* a *is a positive integer, and* $x \in k[[t]]$ *with* $\operatorname{ord} x \neq 0, \infty$. *In addition, let* H. D. M. S. *of* $x = (d_0, d_1, \cdots, d_s)$ *and* $[t, x] = (a_0, \cdots, a_n)$. *Then* H. D. M. S. *of*

$$x^a = (ad_0, \cdots, (a - |a|)d_0 + |a| d_i, \cdots, (a - |a|)d_0 + |a| d_s),$$

$$[t, x^a] = (aa_0, \cdots, (a - |a|)d_0 + |a| a_i, \cdots, (a - |a|)a_0 + |a| a_n)$$

and $[t, x]_r = [t, x^a]_r$.

Proof. Using the remark after Definition 5 and $x^a = (x^{\frac{a}{|a|}})^{|a|}$, it is easy to prove the statement about H. D. M. S. of x^a. Since

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

$$\begin{aligned}
&\langle ad_0, (a - |a|)d_0 + |a|d_i\rangle \\
&\quad = \frac{|a|d_i - |a|d_0 + ad_0 - ad_0}{||a|d_i - |a|d_0 + ad_0| + |ad_0|} + 1 \\
&\quad = \frac{|a|d_i - |a|d_0}{|a||d_0| - |a||d_i|} + 1 \\
&\quad = \frac{d_i - d_0}{|d_0| - |d_i|} + 1 \\
&\quad = \langle d_0, d_i\rangle,
\end{aligned}$$

the statements about $[t, x^a]$ and $[t, x]_r$, $[t, x^a]_r$ are clearly true. Q. E. D.

LEMMA 9. *Given* $k[[t]] \supset k[[x]]$ *with* $\operatorname{ord} x \neq 0, \infty$ *if* $k[[t]] = k[[t']]$, $k[[x]] = k[[x']]$, *then* H. D. M. S. *of* x *with respect to* $t =$ H. D. M. S. *of* x' *with respect to* t' *and* $[t, x] = [t', x']$.

Proof. In view of Proposition 2, it is enough to prove the statement about H. D. M. S.

Since H. D. M. S. is defined relative to the notion of $\operatorname{ord} x \bmod R^{|i|}$ which is independent of the base chosen for $R = k[[t]]$ then H. D. M. S. is also independent of the base. Therefore, let us assume $t = t'$ and let

$$x' = \lambda_0 x + \cdots + \lambda_j x^j + \cdots, \lambda_0 \neq 0,$$

H. D. M. S. of $x = (d_0, d_1, \cdots, d_i, \cdots)$

and H. D. M. S. of $x' = (d'_0, d'_1, \cdots, d'_i, \cdots)$,

clearly $d_0 = \operatorname{ord} x = \operatorname{ord} x' = d'_0$. Now assume $d_i = d'_i$ for some i.

From the remark following Definition 5, $d_{i+1} = \min\{j \mid j \in \operatorname{supp} x \mid j| < |d_i|\}$. In addition

$$\min\{j \mid j \in \operatorname{supp} x^\mu \mid j| < |d_i|\} = (\mu - |\mu|)d_0 + |\mu| d_{i+1} > d_{i+1}\mu > 1.$$

Here

$$\begin{aligned}
d'_{i+1} &= min\{j \mid j \in \operatorname{supp} x', |j| < |d_i|\} \\
&= \min\{j \mid j \in \operatorname{supp} \lambda_0 x, |j| < |d_i|\} \\
&= d_{i+1}.
\end{aligned}$$

Q. E. D.

From Lemma 9, we conclude H. D. M. S. [,], [,]$_r$ are functions of a pair of fields.

LEMMA 10. $r_1 < r_2 < \cdots < r_n$.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Proof. By the definition of a_i, $\langle a_i, a_{i+2}\rangle > \langle a_i, a_{i+1}\rangle = r_{i+1}$. Hence by Lemma 5

$$\langle a_{i+1}, a_{i+2}\rangle = r_{i+2} > \langle a_i, a_{i+1}\rangle = r_{i+1}.$$

Q. E. D.

3. G-character sequences and sequences of Galois extensions. Note that if τ is an k-automorphism of finite order of $k[[t]]$, then it can be deduced that $\operatorname{ord}\tau = p^\nu$ iff $\operatorname{ord}(\tau(t) - t) > 1$, i. e., $\tau(t) = t + \sum_{i>1} \lambda_i t^i$.

LEMMA 11. *Given τ of finite order p^ν such that $\tau(t) = t + \sum_{i>1} \lambda_i t^i$, and $a > 0$ an integer, we have*

$$\tau(t^a) = (\tau(t))^a = t^a + \sum_{i>a} \mu_i t^i$$

where

$$\mu_i = 0 \text{ if } |i| < |a|, \text{ if } |i| \geqq |a|$$

then

$$\mu_i = \frac{a}{|a|}\lambda^{\frac{|a|}{|a|} - \frac{a}{|a|} + 1} + h_i[\lambda_2, \cdots, \lambda^{\frac{i}{|a|} - \frac{a}{|a|}}]$$

with h_i a universal polynomial over k determined by a.

Proof. For any $x \in k[[t]]$, $x^{|a|} \in k[[t^{|a|}]]$. Hence $\mu_i = 0$ if $|i| < |a|$.

We know that 1) $\tau(t)^a = [\tau(t)^{\frac{a}{|a|}}]^{|a|}$ and 2) raising any element of $k[[t]]$ to a power p^ν is equivalent to raising every term to the power p^ν, i. e., $(a_0 + a_1 t + a_2 t^2 + \cdots)^{p^\nu} = a_0^{p^\nu} + a_1^{p^\nu} t^{p^\nu} + a_2^{p^\nu} t^{2p^\nu} + \cdots$. It is enough to prove the lemma for the case $|a| = 1$, which is the classic characteristic zero case.

In the expression $\tau(t)^a$ consider the coefficient of the term of degree $a - 1 + j$, we observe that it contains the term $a\lambda_j$, and it does not contain any term with factor λ_k for $k > j$, or any term with factor $\lambda_j\lambda_k$ for $k > 1$. Hence

$$\mu_{a-1+j} = a\lambda_j + h_{a-1+j}(\lambda_2, \cdots, \lambda_{j-1}).$$

Let $i = a - 1 + j$, then $j = i - a + 1$ and

$$\mu_i = a\lambda_{i-a+1} + h_i(\lambda_2, \cdots, \lambda_{i-a}).$$

It is routine to check that h_i is a universal polynomial. This proved the lemma.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Remark. $h_i(0, 0, \cdots, 0) = 0$.

Let $x \in k[[t]]$ ord $x \neq 0, \infty$, $k[[t]]$ be a separable algebraic extension of degree p^ν over $k[[x]]$, $[t, x] = (a_0, a_1, \cdots, a_n)$. $[t, x]_r = (r_1, \cdots, r_n)$. H. D. M. S. of $x = (d_0, d_1, \cdots, d_s)$, and $x = x_0 + x_1 + \cdots + x_n$ is the standard expression of x.

LEMMA 12. $\langle a, a_n \rangle < r_n \; \forall \, a \in \operatorname{supp} x - x_n - x_{n-1}$.

Proof. Let $a \in \operatorname{supp} x_i$ such that $a > \operatorname{ord} x_i$ for some $i < n-1$, then $\langle \operatorname{ord} x_i, a \rangle \geqq \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1} \rangle$. By Lemma 3, $a \geqq \operatorname{ord} x_i$ implies

$$\langle a, \operatorname{ord} x_{i+1} \rangle \leqq \langle \operatorname{ord} x_i, \operatorname{ord} x_{i+1} \rangle < \langle \operatorname{ord} x_{i+1}, \operatorname{ord} x_{i+2} \rangle.$$

Hence by Lemma 4

$$\langle a, \operatorname{ord} x_{i+2} \rangle < \langle \operatorname{ord} x_{i+1}, \operatorname{ord} x_{i+2} \rangle \langle \operatorname{ord} x_{i+2}, \operatorname{ord} x_{i+3} \rangle.$$

Repeating this argument several times, we conclude

$$\langle a, a_n \rangle < \langle \operatorname{ord} x_{n-1}, x_n \rangle = r_n. \qquad \text{Q. E. D.}$$

LEMMA 13. *Let* $|a_n| = 1$ *and let* τ *be an automorphism of finite order* p^ν *of* $k[[t]]$; *say*

$$\tau(t) = t + \sum_{i>1} \lambda_i t^i \qquad x = \sum \eta_i t^i$$
$$\tau(x) = \sum \mu_i t^i.$$

Then $\forall i \ni : i - a_n + 1 > r_n$, $\mu_i = \eta a_n \lambda_{i-a_n+1} + h_i(\lambda_2, \cdots, \lambda_{i-a_n}) + \eta_i$ *where* η *is the coefficient of* t^{a_n} *in* x *and* h_i *is a universal polynomial over* k *determined by* x.

Proof. Let $\tau(t^a) = (\tau(t))^a + \sum_{i>a} \mu_{a,i} t^i$, then

$$\mu_i = \sum_{i>a} \eta_a \mu_{a,i} + \eta_i.$$

By Lemma 11

$$\mu_{a,i} = \frac{a}{|a|} \lambda^{\frac{|a|}{\frac{i}{|a|} - \frac{a}{|a|} + 1}} + h_{a,i}[\lambda_2, \cdots, \lambda^{\frac{i}{|a|} - \frac{a}{|a|}}].$$

Assume i is such that $i - a_n + 1 > r_n$, for $a \in \operatorname{supp}(x - x_n - x_{n-1})$, Lemma 12 implies

$$i - a_n + 1 > \frac{a_n - a}{|a| - 1} + 1$$

and for $a \in \operatorname{supp} x_{n-1}$, Lemma 3 implies

$$i - a_n + 1 > \langle a, a_n \rangle = \frac{a_n - a}{|a| - 1} + 1.$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Hence $i-a_n+1>\frac{a_n-a}{|a|-1}+1$ if $a\in \operatorname{supp} x-x_n$. This implies

$$i(|a|-1)>a_n|a|-a$$

$$\Rightarrow i[1-\frac{1}{|a|}]>a_n-\frac{a}{|a|}$$

$$\Rightarrow i-a_n+1>\frac{i}{|a|}-\frac{a}{|a|}+1.$$

Next let $a\in \operatorname{supp} x_n$ and $a>a_n$; then it is clear $i-a<i-a_n$. Thus we conclude $\mu_{a,i}$ is a polynomial in $\lambda_2,\cdots,\lambda_{i-a_n}$ if $a\in \operatorname{supp} x\backslash a_n$. Also from Lemma 10

$$\mu_{a_n,i}=\eta a_n\lambda_{i-a_n+1}+h_{a_n,i}[\lambda_2,\cdots,\lambda_{i-a_n}].$$

Hence

$$\mu_i=\sum \eta_a\mu_{a,i}+\eta_i=\eta a_n\lambda_{i-a_n+1}+h_i[\lambda_2,\cdots,\lambda_{i-a_n}]+\eta_i.$$

Remark. $h_i(0,0,\cdots,0)=0$.

PROPOSITION 3. *If r_n is an integer, then there exists an abelian group G_n of automorphisms of $k[[t]]$ with (only one) higher ramification index r_n and of order $|a_{n-1}|$ which fixes x.*

Proof.

1) Since $\operatorname{ord} x=p^\nu$, any automorphism τ with the property $\operatorname{ord}(\tau(t)-t)=1$ cannot fix x.

Let τ be an automorphism such that $\operatorname{ord}(\tau(t)-t)=r>r_n$, then by Lemma 13

$$\mu_{r+a_{n-1}}=\eta a_n\lambda_r+\eta_i\neq\eta_i$$

and hence $\tau(x)\neq x$.

2) Let $\tau(t)=t+\sum_{i\geqq r_n}\lambda_i t^i$ be an automorphism which fixes x, and let $x=\sum_{i\leqq p^\nu}\eta_i t^i$.

By Lemma 13

$$\eta_i=\eta_n a_n\lambda_{i-a_n+1}+h_i[\lambda_2,\cdots,\lambda_{i-a_n}]+\eta_i \;\forall i\ni: i-a_n+1>r_n.$$

Hence for $i\ni: i>r_n+a_n-1$, λ_i satisfies

$$\eta a_n\lambda_i+h_{i+a_{n-1}}[\lambda_2,\cdots,\lambda_{i-1}]=0.$$

By Lemma 11 and the remark following it, $\operatorname{ord}(\tau(t^a)-t^a)=a-|a|+r_n|a|$ and the leading form of $(\tau(t^a)-t^a)$ is $\frac{a}{|a|}\lambda_{r_n}{}^{|a|_t a-|a|+r_n|a|}$. If

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

$a \in \operatorname{supp}(x - x_n - x_{n-1})$, we have by Lemma 12,

$$a_n > \langle a, a_n \rangle = \frac{a_n - a}{|a| - 1} + 1 \Rightarrow |a| r_n - r_n > a_n - a + |a| - 1$$
$$\Rightarrow a - |a| + r_n |a| > r_n + a_n - 1.$$

If $a \in \operatorname{supp} x_{n-1}$, $a > a_{n-1}$ and $|a| \geqq |a_{n-1}|$ then $\langle a_{n-1}, a \rangle = \infty$. By Lemma 3 it follows that $\langle a, a_n \rangle < \langle a_{n-1}, a_n \rangle = r$, hence by the same reasoning as in the case of $a \in x - x_{n-1}$, $a - |a| + r_n |a| > r_n + a_n - 1$. If $a \in \operatorname{supp} x_n$ and $a > a_n$ then it is obvious that $a - |a| + r_n |a| > r_n + a_n - 1$. Finally we note that while

$$\operatorname{ord}(\tau(t^{a_{n-1}}) - t^{a_{n-1}}) = a_{n-1} - |a_{n-1}| + r_n |a_{n-1}| = r_n + a_n - 1$$
$$= \operatorname{ord}(\tau(t^{a_n}) - t^{a_n}) = \operatorname{ord}(\tau(t^a) - t^a) \forall a \in \operatorname{supp} x_{n-1} \ni : \langle a_{n-1}, a \rangle = r_n.$$

Hence

$$\eta_{r_n + a_{n-1}} = \eta_{a_{n-1}} \frac{a_{n-1}}{|a_{n-1}|} \lambda_{r_n}{}^{|a_{n-1}|} + \cdots$$
$$+ \eta_a \frac{a}{|a|} \lambda_{r_n}{}^{|a|} + \cdots + \eta_{a_n a_n} \lambda_{r_n} + \eta_{r_n + a_{n-1}}$$

where $a \in \operatorname{supp}(x_{n-1})$ with $\langle a_{n-1}, a \rangle = r_n$, $a > a_{n-1}$. Thus λ_{r_n} satisfies

$$\eta_{a_{n-1}} \frac{a_{n-1}}{|a_{n-1}|} \lambda_{r_n}{}^{|a_{n-1}|} + \cdots + \eta_a \frac{a}{|a|} \lambda_{r_n}{}^{|a|} + \cdots + \eta_{a_n} \lambda_{r_n} = 0;$$

this is a separable equation with exactly $|a_{n-1}|$ solutions since $|a_{n-1}| > |a| > 1$.

3) Conversely, take λ_{r_n} which satisfies the above equation. Then there exists a unique sequence $\{\lambda_{r_{n+1}}, \cdots, \lambda_i, \cdots\}$ which satisfies

$$\eta_{a_n} \lambda_i + h_{i + a_{n-1}}[\lambda_2, \cdots, \lambda_{i-1}] = 0.$$

Moreover the automorphism τ defined by

$$\tau(t) = t + \sum_{i \geqq r_n} \lambda_i t^i$$

fixes x. By 1) these $|a_{n-1}|$ different elements form a group of higher ramification index r_n. Q. E. D.

LEMMA 14. *Given* $0 < r_1 < r_2 < \cdots < r_{n-1}$, r_i *real number,* $0 < a_0 < a_1 < \cdots < a_{n-1}$, a_i *integer,* $\eta_0, \eta_1, \cdots, \eta_{n-1} \in k$ *and* $\langle a_i, a_{i+1} \rangle = r_{i+1}$. *Let* $y, x \in k[[t]]$ *such that* $\operatorname{ord} y, \operatorname{ord} z \neq 0, \infty$, $[t, z]_r = (r_n, \cdots)$, $r_n > r_{n-1}$ *and* $\operatorname{ord}(y - z) > \operatorname{ord}(y)$.

If y *satisfies the following conditions*

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

1) $a \in \operatorname{supp}(y), a_i < a \leqq a_{i+1} \Rightarrow \langle a_i, a\rangle \geqq r_{i-1}$.
$a \in \operatorname{supp}(y), a_{n-1} < a \Rightarrow \langle a_{n-1}, a\rangle > r_{n-1}$ *and*;
2) $a_i \in \operatorname{supp}(y)$ *and* η_i *is the coefficient of* t^{a_i} *of* y $a_i \geqq \operatorname{ord} y$.

Then $y - z$ satisfies 1) and 2) and $\operatorname{ord}(y-z) \leqq a_i$ if $\operatorname{ord} y < a_i$.

Proof.

Case A. $\operatorname{ord} y = \operatorname{ord} z \geqq a_{n-1}$.

Since $\operatorname{supp}(y-z) \subset \operatorname{supp} y \cup \operatorname{supp} z$ condition 1) is satisfied, while 2) is trivially true.

Case B. $\operatorname{ord} y = \operatorname{ord} z = a_i < a_{n-1}$.

Suppose $a \in \operatorname{supp} z$ with $a \neq \operatorname{ord} z$ and $a_s \leqq a < a_{s+1} \leqq a_{n-1}$. We note that $\langle a_i, a\rangle = \infty \Rightarrow \langle a_{s-1}, a\rangle = \infty$, i. e., $a \neq a_s$, hence we may assume $\langle a_i, a\rangle < \infty$. Moreover since $\langle a_i, a\rangle \geqq r_n > r_{n-1} > \langle a_i, a_{i+1}\rangle$, Lemma 5 implies $\langle a_{i+1}, a\rangle > r_{n-1}$. Repeating this argument we find that $\langle a_{s-1}, a\rangle > r_{n-1} \geqq r_s = \langle a_{s-1}, a_s\rangle$, i. e., $a \neq a_s$ and $\langle a_s, a\rangle > r_{n-1} \geqq r_{s+1}$. Hence the first part of 1) is satisfied since $\operatorname{supp}(y-z) \subset \operatorname{supp} y \cup \operatorname{supp} z$. Also $a_s \notin \operatorname{supp}(z)$ $a_s > \operatorname{ord} z$; thus 2) is satisfied. Now suppose $a \in \operatorname{supp} z$ and $a > a_{n-1}$. Since $\langle a_i, a\rangle \geqq r_n > r_{n-1}$, repeating the same argument it follows that $\langle a_{n-1}, a\rangle > r_{n-1}$. We conclude 1) is satisfied completely.

Case C. $a_i < \operatorname{ord} y = \operatorname{ord} z < a_{i+1} \leqq a_{n-1}$.

Since $\langle a_i, ord\, y\rangle \geqq \langle a_i, a_{i+1}\rangle = r_{i+1}$ by 1), it follows from Lemma 3 that $\langle \operatorname{ord} y, a_{i+1}\rangle \leqq \langle a_i, a_{i+1}\rangle$. Suppose $a \in \operatorname{supp} z$, $a_s \leqq a < a_{s+1} \leqq a_{n-1}$ and $a \neq \operatorname{ord} z$. Since $\langle \operatorname{ord} z, a\rangle \geqq r_n > r_{n-1} \geqq \langle \operatorname{ord} z, a_{i+1}\rangle$, and

$$\langle \operatorname{ord} z, a\rangle = \infty \Rightarrow |\operatorname{ord} z| \leqq |a| \Rightarrow |a| > |a_{i+1}| \Rightarrow |a| > |a_s| \Rightarrow \langle a_s, a\rangle = \infty,$$

i. e., hence assume $\langle \operatorname{ord} z, a\rangle < \infty$, then by Lemma 5, $\langle a_{i+1}, a\rangle > \langle \operatorname{ord} z, a\rangle > r_{n-1}$. Successively $\langle a_{s-1}, a\rangle > r_{n-1} \geqq r_s$, i. e., $a \neq a_s$, and $\langle a_s, a\rangle > r_{n-1} > r_{s+1}$. Hence the first part of 1) is satisfied since $\operatorname{supp}(y-z) \subset \operatorname{supp} y \cup \operatorname{supp} z$. While $a_s \notin \operatorname{supp} z \,\forall\, a_s > \operatorname{ord} z$, thus 2) is satisfied.

Suppose $a \in \operatorname{supp} z$ and $a > a_{n-1}$. Since $\langle a_i, a\rangle \geqq r_n > r_{n-1}$ repeat the same argument $\langle a_{n-1}, a\rangle > r_{n-1}$. We conclude 1) is satisfied completely.

It is clear from the above argument $\operatorname{ord}(y-z) \leqq a_i$ if $\operatorname{ord} y < a_i$.

PROPOSITION 4. *If* r_n *is an integer, let* $k[[\omega]]$ *be the fixed domain of* G_n *in Proposition* 3. *Then*

$$[\omega, x] = \left(\frac{a_0}{|a_{n-1}|}, \frac{a_1}{|a_{n-1}|}, \cdots, \frac{a_{n-1}}{|a_{n-1}|}\right)$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

and

$$[\omega, x]_r = (r_1, r_2, \cdots, r_{n-1}).$$

Proof. Since $\langle a_i, a_{i+1}\rangle = \langle \frac{a_i}{|a_{n-1}|}, \frac{a_{i+1}}{|a_{n-1}|}\rangle$, it is enough to prove the statement about $[\omega, x]$.

From Lemma 9 we know $[t, x]$ and $[\omega, x]$ are independent of the chosen basis, so we can assume

$$\begin{aligned}\omega &= t^q + \sum_{i>q} \lambda_i t^i \\ x &= t^{p^\nu} + \sum_{i>p^\nu} \mu_i t^i \\ &= \omega^{q/p^\nu} + \sum_{i>p^\nu/q} \xi_i \omega^i\end{aligned}$$

where $q = |a_{n-1}|$.

Let $\eta_0 = 1$, $\eta_i = \mu_{a_i}$ $0 < i \leqq a_{n-1}$.

By Lemma 8 $[t, \xi_i\omega^i] = [t, \omega^i] = (r_n)$, and since x satisfies conditions 1) and 2) of Lemma 14, we conclude

$$x - [\omega^{p^\nu/q} + \sum_{b \geqq i > p^\nu/q} \xi_i \omega^i]$$

satisfies conditions 1) and 2) of Lemma 14.

To conclude the proof, we need only prove

1) $a \in \mathrm{supp}_\omega(x)$ and $\frac{a_i}{q} < a \leqq \frac{a_{i+1}}{q}$

$$\Rightarrow \langle \frac{a_i}{q}, a\rangle \geqq \langle \frac{a_i}{q}, \frac{a_{i+1}}{q}\rangle = r_{i+1}$$

$$\forall\, i+1 \leqq n-1$$

and

2) $\frac{a_i}{q} \in \mathrm{supp}_\omega(x)$ and $\xi_{a_i/q} = \mu_{a_i} = \eta_i$

$$\forall\, i \leqq n-1.$$

Proof. Suppose 1) and 2) are true for all $a \in \mathrm{supp}_\omega(x)$, $a \leqq c$ and $a_i \leqq c$ for some c. Let

$$\begin{aligned}x - [\omega^{p^\nu/q} + \sum_{c>i>p^\nu/q} \xi_i \omega^i] &= \xi_d \omega^d + \cdots \\ &= \xi_d t^{qd} + \cdots\end{aligned}$$

where $\xi_d \omega^d$ is the leading term.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Since $x - [\omega^{p^\nu/q} + \sum_{c \geqq i > p^\nu/q} \xi_i \omega^i]$ satisfies condition 1) and 2) of Lemma 14, $\langle a_i, qd \rangle \geqq r_{i+1}$ if $a_i < qd \leqq a_{i+1}$. Also since

$$x - [\omega^{p^\nu/q} + \sum_{c > i > p^\nu/q} \omega^i]$$

satisfies conditions 1) and 2) of Lemma 14, if

$$\operatorname{ord}_t [x - \omega^{p^\nu/q} + \sum_{c > i > p^\nu/q} \omega^i - \xi_c \omega^c] \geqq a_i$$

for some $a_i \geqq cq$ then $a_i = qd$ and $\xi_d = \eta_i$. Hence 1) and 2) are proved for all $a \in \operatorname{supp}_\omega(x) a \leqq d$ and all $a_i \leqq d$. Q. E. D.

Now let $x = y_0 + y_1 + \cdots + y_{n-1}$ where $y_i = \sum_{a_i/q > j \geqq a_{i-1}/q} \xi_j \omega^j$ if $i < n-1$ and $y_{n-1} = \sum_{j \geqq a_{n-1}/|a_{n-1}|} \xi_j \omega^j$. Then from Proposition 1 and conditions 1 and 2, this is the standard expression of x with respect to ω. Hence

$$[\omega, x] = \left(\frac{a_0}{|a_{n-1}|}, \frac{a_1}{|a_{n-1}|}, \cdots, \frac{a_{n-1}}{|a_{n-1}|} \right).$$

Q. E. D.

From Proposition 4 it is easy to conclude

PROPOSITION 5. *If* $[t, x]_r = (r_1, \cdots, r_n)$ *is a sequence of integers then there exist a chain of power series rings* $k[[t]] \supset k[[y_1]] \supset \cdots \supset k[[y_{n-1}]] \supset k[[x]]$ *such that each is a galois extension of the next one with higher ramification index* r_i *and algebraic degree* $\frac{|a_{i-1}|}{|a_i|}$ *respectively.*

LEMMA 15. *Let* $y, z \in k[[t]]$ $\operatorname{ord} y$, $\operatorname{ord} z \neq 0, \infty$. *Suppose*

$$[t, y] = (dp^\nu + a_0, dp^\nu + a_1, \cdots, dp^\nu + a_n), [t, z] = (pa_0, pa_1, \cdots, pa_n)$$

where $p^\nu \geqq |a_0|$, $dp^\nu + a_0 > pa_0$ $[t, z]_r = (r_1, r_2, \cdots, r_n)$. *Then*

1) *if* $\langle pa_0, dp^\nu + a_0 \rangle < r_1$ *then* $[t, z + y]_r = (r_0, r_1, \cdots, r_n)$

where $r_0 = \langle pa_0, dp^\nu + a_0 \rangle$ *and*

2) *if* $\langle pa_0, dp^\nu + a_0 \rangle = r_1$ *then* $[t, z + y] = (r_1, \cdots, r_n)$.

Proof. Let

$$y = y_0 + y_1 + \cdots + y_n$$
$$z = z_0 + z_1 + \cdots + z_n$$

be standard expressions and $x = y + z$. It is easy to check that

$$[t, y]_r = (r_1, r_2, \cdots, r_n).$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

1) It is enough to show

$$[t, x] = (pa_0, dp^\nu + a_0, dp^\nu + a_1, \cdots, dp^\nu + a_n).$$

From our assumption $\operatorname{ord} x = pa_0$. Given $a \in \operatorname{supp} z$, it follows that $\langle \operatorname{ord} x, a\rangle = \langle \operatorname{ord} z, a\rangle \geqq r_1 > \langle \operatorname{ord} x, dp^\nu + a_0\rangle$, and $dp^\nu + a_0 \notin \operatorname{supp} z$. Suppose $a \in \operatorname{supp} y$ and $a > \operatorname{ord} y = dp^\nu + a_0$; then since $\langle dp^\nu + a_0, a\rangle \geqq r_1 > \langle a_0 p, dp^\nu + a_0\rangle$. Lemma 1 implies that $\langle a_0 p, a\rangle > \langle a_0 p, dp^\nu + a_0\rangle = r_0$.

Let $x = x_0 + x_1 + \cdots + x_{n+1}$ be the standard expression of x. From the above argument $\operatorname{ord} x_0 = pa_0$ and $\operatorname{ord} x_1 = dp^\nu + a_0$. Moreover, since $|dp^\nu + a_0| = |a_0| \geqq |a_1|p = |pa_1|$ if $pa_1 \leqq dp^\nu + a_0$, it follows that $r_1 = \langle pa_0, pa_1\rangle \geqq \langle pa_0, dp^\nu + a_0\rangle$, hence $pa_1 > dp^\nu + a_0$. Furthermore since $\langle pa_0, pa_1\rangle = r_1 > \langle pa_0, dp^\nu + a_1\rangle$, we have $\langle dp^\nu + a_0, pa_1\rangle > r_1$ by Lemma 5.

Suppose we have proved

$$\operatorname{ord} x_{j+1} = dp^\nu + a_j$$
$$pa_{j+1} > dp^\nu + a_j$$
$$\langle dp^\nu + a_j, pa_{j+1}\rangle > r_{j+1} \;\forall\; 0 \leqq j \leqq i < n+1.$$

We will make induction on i.

Let $a \in \operatorname{supp} y$, $a > \operatorname{ord} y_i$ then $\langle dp^\nu + a_i, a\rangle \geqq r_{i+1}$. Also

$$a > dp^\nu + a_{i+1} a \in \operatorname{supp} y \Rightarrow \langle dp^\nu + a_i, a\rangle > r_{i+1}.$$

To show $\operatorname{ord} x_{i+2} = dp^\nu + a_{i+1}$ we must show that $dp^\nu + a_{i+1} \notin \operatorname{supp} z$, $\langle dp^\nu + a_i, a\rangle > r_{i+1} \;\forall\; a \in \operatorname{supp} z$, $a > dp^\nu + a_i$.

By Lemma 3, $\langle dp^\nu + a_i, pa_{i+1}\rangle > r_{i+1} \geqq \langle a, pa_{i+1}\rangle$ a $\in \operatorname{supp} z_i$ $a > dp^\nu + a_i$. By Lemma 6, we conclude that $\langle dp^\nu + a_i, a\rangle \geqq \langle dp^\nu + a_i, pa_{i+1}\rangle > g_{i+1}$. For any $a > pa_{i+1}$ $a \in \operatorname{supp} z$, we have $\langle pa_{i+1}, a\rangle \geqq r_{i+2} > r_{i+1} = \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle$. By Lemma 1 $\langle dp^\nu + a_i, a\rangle > \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle = r_{i+1}$ $a \geqq pa_{i+1}$, $a \in \operatorname{supp} z$. Hence $dp^\nu + a_{i+1} \notin \operatorname{supp} z$ and $\operatorname{ord} x_{i+2} = dp^\nu + a_{i+1}$.

Since $|dp^\nu + a_{i+1}| = |a_{i+1}| \geqq |a_{i+2}| \cdot p$,

$$pa_{i+2} \leqq dp^\nu + a_{i+1} \Rightarrow \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle \geqq \langle dp^\nu + a_i, pa_{i+2}\rangle.$$

Hence we conclude $pa_{i+2} > dp^\nu + a_{i+1}$.

Since $\langle pa_{i+1}, pa_{i+2}\rangle = r_{i+2} > \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle$, $\langle dp^\nu + a_i, pa_{i+1}\rangle > r_{i+1} = \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle$ and $|pa_{i+1}| > |dp^\nu + a_{i+1}|$, we conclude by Lemma 7 that $\langle dp^\nu + a_{i+1}, pa_{i+2}\rangle > \langle pa_{i+1}, pa_{i+2}\rangle = r_{i+2}$.

The inductive process is proved.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

2) By Lemma 1

$$\langle pa_0, dp^\nu + a_0\rangle = r_1 = \langle dp^\nu + a_0, dp^\nu + a_1\rangle \Rightarrow \langle pa_0, dp^\nu + a_1\rangle = r_1.$$

Hence it is enough to show $[t, x] = (pa_0, dp^\nu + a_1, \cdots, dp^\nu + a_n)$.

From our assumption $\operatorname{ord} x = pa_0$. Since $|dp^\nu + a_1| = |a_1| < |a_1| \cdot p = |pa_1|$ and $\langle ap_0, dp^\nu + a_1\rangle = \langle pa_0, pa_1\rangle = r_1$, $dp^\nu + a_1 > pa_1$. Given $a \in \operatorname{supp} z$ with $a > pa_1$, since $\langle pa_1, a\rangle \geqq r_2 > r_1 = \langle pa_0, pa_1\rangle$, by Lemma 1 it follows that $\langle pa_0, a\rangle > \langle pa_0, pa_1\rangle = r_1$, hence $dp^\nu + a_1 \notin \operatorname{supp} z$. For any $a \in \operatorname{supp} y$ with $a < dp^\nu + a_1$, since $\langle dp^\nu + a_0, a\rangle \geqq r_1 = \langle pa_0, dp^\nu + a_0\rangle$, by Lemma 1 it follows that $\langle pa_0, a\rangle \geqq r_1$. While for any $a \in \operatorname{supp} y$ with $a > dp^\nu + a_1$, since $\langle dp^\nu + a_1, a\rangle \geqq r_2 > r_1 = \langle pa_0, dp^\nu + a_1\rangle$, Lemma 1 implies $\langle pa_0, a\rangle > r_1 = \langle pa_0, dp^\nu + a_1\rangle$.

Let $x = x_0 + x_1 + \cdots + x_n$ be the standard expression of x. From the above argument $\operatorname{ord} x_0 = pa_0$ and $\operatorname{ord} x_1 = dp^\nu + a_1$. Moreover, since $|dp^\nu + a_1| = |a_1| \geqq |a_2| p = |pa_2|$, $dp^\nu + a_1 \notin \operatorname{supp} z$, i.e., $dp^\nu + a_1 \neq pa_2$ and $\langle pa_0, pa_2\rangle > r_1 = \langle pa_0, dp^\nu + a_1\rangle$, it follows that $pa_2 > dp^\nu + a_1$. Furthermore, since $\langle pa_1, pa_2\rangle = r_2 > r_1 = \langle pa_1, dp^\nu + a_1\rangle$ (Lemma 3), we have $\langle dp^\nu + a_1, pa_2\rangle > r_2$ by Lemma 5.

Suppose we have proved

$$\operatorname{ord} x_j = dp^\nu + a_j$$
$$pa_{j+1} > dp^\nu + a_j$$
$$\langle dp^\nu + a_j, pa_{j+1}\rangle > r_{j+1} \;\forall\; 0 < j \leqq i < n$$

We will make induction on i.

Let $a \in \operatorname{supp} y$ with $a > \operatorname{ord} y_i = dp^\nu + a_i$ then $\langle dp^\nu + a_i, a\rangle \geqq r_{i+1}$. Also $a > dp^\nu + a_{i+1}$, $a \in \operatorname{supp} y \Rightarrow \langle dp^\nu + a_i, a\rangle > r_{i+1}$. To show $\operatorname{ord} x_{i+1} = dp^\nu + a_{i+1}$ we must show that $dp^\nu + a_{i+1} \in \operatorname{supp} z$, $\langle dp^\nu + a_i, a\rangle > r_{i+1} \;\forall\; a \in \operatorname{supp} z$, $a > dp^\nu + a_i$.

If $a \in \operatorname{supp}(z_0 + \cdots + z_{i+1})$ with $a > dp^\nu + a_i$ then $|a| \geqq |pa_i| > |dp^\nu + a_i|$ and $\langle dp^\nu + a_i, a\rangle = \infty$, hence it is enough to show that

$$dp^\nu + a_{i+1} \notin \operatorname{supp} z, \langle dp^\nu + a_i, a\rangle > r_{i+1} \;\forall\; a \in \operatorname{supp}(z_i + z_{i+1} + \cdots + z_n)$$

with $a > dp^\nu + a_i$.

By Lemma 3, $\langle dp^\nu + a_i, pa_{i+1}\rangle > r_{i+1} \geqq \langle a, pa_{i+1}\rangle \forall a \in \operatorname{supp} z_i$, $a > dp^\nu + a_i$. By Lemma 6, we conclude that $\langle dp^\nu + a_i, a\rangle \geqq \langle dp^\nu + a_i, pa_{i+1}\rangle > g_{i+1}$. For any $a > pa_{i+1}$, $a \in \operatorname{supp} z$, $\langle pa_{i+1}, a\rangle \geqq r_{i+1} > r_{i+1} = \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle$. By Lemma 1 $\langle dp^\nu + a_i, a\rangle > \langle dp^\nu + a_i, dp^\nu + a_{i+1}\rangle = r_{i+1} \;\forall\; a \geqq pa_{i+1}$, $a \in \operatorname{supp} z$. Hence $dp^\nu + a_{i+1} \notin \operatorname{supp} z$ and $\operatorname{ord} x_{i+1} = dp^\nu + a_{i+1}$.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Since

$$| dp^\nu + a_{i+1} | = | a_{i+1} | \geqq | a_{i+1} | \cdot p, pa_{i+2} \leqq dp^\nu + a_{i+1}$$
$$\Rightarrow \langle dp^\nu + a_i, dp^\nu + a_{i+1} \rangle \geqq \langle dp^\nu + a_i, pa_{i+2} \rangle.$$

Hence we conclude $pa_{i+2} > dp^\nu + a_{i+1}$.

Since $\langle pa_{i+1}, pa_{i+2} \rangle = r_{i+2} > \langle dp^\nu + a_i, dp^\nu + a_{i+1} \rangle, \langle dp^\nu + a_i, pa_{i+1} \rangle > r_{i+1} = \langle dp^\nu + a_i, dp^\nu + a_{i+1} \rangle$ and $| pa_{i+1} | > | dp^\nu + a_{i+1} |$, one concludes by Lemma 7 that $\langle dp^\nu + a_{i+1}, pa_{i+2} \rangle > \langle pa_{i+1}, pa_{i+2} \rangle = r_{i+2}$.

PROPOSITION 6. *Let $k[[t]] \supset k[[\omega]] \supset k[[x]]$ be a chain of separable algebraic extensions of algebraic degree p^ν and p respectively. If $[t, \omega]_r = (r_1, \cdots, r_n)$ and $[\omega, x]_r = (b)$ are two sequences of integers then $[t, x]_r$ is a sequence of integers.*

Proof. By Lemma 9 we can choose ω, x

$$x = \omega^p + \sum_{i \geqq m} \mu_i \omega^i$$

where $m = (p-1)b + 1$, $| m | = 1$, $\mu_m \not\equiv 0$.

Let

$$[t, \omega] = (a_0, a_1, \cdots, a_n), \quad a_0 = p^\nu$$
$$[t, \omega]_r = (r_1, r_2, \cdots, r_n)$$

and let

$$\omega = \omega_0 + \omega_1 + \cdots + \omega_n$$

be the standard expression, then by Lemma 9 and Lemma 8

$$[t, x - \omega^p] = (mp^\nu, (m-1)p^\nu + a_1, \cdots, (m-1)p^\nu + a_n)$$
$$[t, x - \omega^p]_r = (r_1, r_2, \cdots, r_n)$$
$$[t, \omega^p] = (pa_0, pa_1, \cdots, pa_n)$$
$$[t, \omega^p]_r = (r_1, r_2, \cdots, r_n)$$

and

$$\omega^p = \omega_0{}^p + \omega_1{}^p + \cdots + \omega_n{}^p$$

is the standard expression. Let $x - \omega^p = y_0 + y_1 + \cdots + y_n$ be the standard expression, then

$$x = \omega_0{}^p + \omega_1{}^p + \cdots + \omega_n{}^p + y_0 + y_1 + \cdots + y_n.$$

Now suppose $b < r_1$ or $b = r_1$. Then by Lemma 15,

$$[t, x]_r = (b, r_1, r_2, \cdots, r_n) \text{ or } (r_1, r_2, \cdots, r_n).$$

Hence we can assume $b > r_1$,,

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Let $x = \sum x_i$ be the standard expression of x. Then it is trivial to check that $x - \sum_{i \leqq c} x_i = \sum_{i > c} x_i$ is the standard expression of $x - \sum_{i \leqq c} x_i$.

Since $\langle pa_0, mp^\nu \rangle = b > r_1$ and $\langle mp^\nu, a \rangle \geqq r_1 \; \forall \, a \in \operatorname{supp} y$, $a > mp^\nu$, it is clear by Lemma 1 that $\langle pa_0, a \rangle > r_1 \; \forall \, a \in \operatorname{supp} y$.

Hence $\operatorname{ord} x_1 = pa_1$ and $pa_1 \notin \operatorname{supp} y$. Let $a \in \operatorname{supp} y_0$, then

$$| a | > | (m-1) p^\nu + a_1 | = | a_1 |,$$

hence $| a | \geqq | pa_1 |$. Thus $\langle pa_1, a \rangle = \infty \; \forall \, a \in \operatorname{supp} y_0$ with $a > pa_1$. Moreover since $| (m-1) p^\nu + a_1 | = | a_1 | < | pa_1 |$ and

$$\langle pa_0, pa_1 \rangle \leqq \langle pa_0, (m-1) p^\nu + a_1 \rangle,$$

one concludes $(m-1) p^\nu + a_1 > pa_1$. Hence

$$[t, x - x_0] = [t, \omega_1{}^p + \cdots + \omega_n{}^p + y_1 + \cdots + y_n]$$

and

$$[t, x - x]_r = [t, \omega_1{}^p + \cdots + \omega_1{}^n + y_1 + \cdots + y_n]_r.$$

We have

$$[t, \omega_1{}^p + \cdots + \omega_n{}^p] = (pa_1, \cdots, pa_n)$$
$$[t, y_1 + \cdots + y_n] = ((m=1) p^\nu + a_1, \cdots, (m-1) p^\nu + a_n)$$
$$[t, \omega_1{}^p + \cdots + \omega_n{}^p]_r = [t, \omega_1{}^p + \cdots + \omega_n{}^p]_r = (r_2, \cdots, r_n)$$

and

$$p^\nu > | a_1 |, \; (m-1) p^\nu + a_1 > pa_1.$$

Moreover, let $b_1 = \langle pa_1, (m-1) p^\nu + a_1 \rangle$

$$= \frac{(m-1) p^\nu + a_1 - pa_1}{p | a_1 | - | a_1 |} + 1$$

$$= \frac{m-1}{p-1} \frac{p^\nu}{| a_1 |} - \frac{a_1}{| a_1 |} + 1$$

$$= b \frac{p^\nu}{| a_1 |} - \frac{a_1}{| a_1 |} + 1 \equiv b_1.$$

We note that b_1 is an integer.

By Lemma 15 if $b_1 \leqq r_2$ then $[t, x - x_0]_r = (b_1, r_2, r_3, \cdots, r_n)$ or $(r_2, r_3, \cdots, r_n)$. Hence $[t, x] = (r_1, b_1, r_2, r_2, \cdots, r_n)$ or $(r_1, r_2, \cdots, r_n)$. Now we can assume $b_1 > r_2$. Successively we assume for some $i \geqq 0$

$$[t, x - x_0 \cdots x_i]$$
$$= [t, \omega_{i+1}{}^p + \cdots + \omega_n{}^p + y_{i+1} + \cdots + y_n]$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

$$[t, x - x_0 \cdot \cdot \cdot x_i]_r$$
$$= [t, \omega_{i+1}{}^p + \cdot \cdot \cdot + \omega_n{}^p + y_{i+1} + \cdot \cdot \cdot + y_n]_r$$
$$[t, \omega_{i+1}{}^p + \cdot \cdot \cdot + \omega_n{}^p] = (pa_{i+1}, \cdot \cdot \cdot, pa_n)$$
$$[t, y_{i+1} + \cdot \cdot \cdot + y_n] = ((m-1)p^\nu + a_{i+1}, \cdot \cdot \cdot, (m-1)p^\nu + a_n)$$
$$[t, \omega_{i+1}{}^p + \cdot \cdot \cdot + \omega_n{}^p]_r = [t, y_{i+1} + \cdot \cdot \cdot + y_n]_r$$
$$= (r_{i+2}, \cdot \cdot \cdot, r_n)$$
$$p^\nu > |a_{i+1}|, (m-1)p^\nu + a_{i+1} > pa_{i+1}$$

and let

$$b_{i+1} \equiv \langle pa_{i+1}, (m-1)p^\nu + a_{i+1} \rangle$$
$$= \frac{(m-1)p^\nu + a_{i+1} - pa_{i+1}}{p|a_{i+1}| - |a_{i+1}|} + 1$$
$$= \frac{p^\nu}{p|a_{i+1}|} - \frac{a_{i+1}}{|a_{i+1}|} + 1,$$

be an integer.

By Lemma 15, if $b_{i+1} \leqq r_{i+2}$, then $[t, x - x_0 \cdot \cdot \cdot x_i]_r = (b_{i+1}, r_{i+2}, \cdot \cdot \cdot, r_n)$ or $(r_{i+2}, \cdot \cdot \cdot, r_n)$. Hence

$$[t, x]_r = (r_1, \cdot \cdot \cdot, r_{i+1}, b_{i+1}, r_{i+2}, \cdot \cdot \cdot, r_n) \text{ or}$$
$$(r_1, \cdot \cdot \cdot, r_{i+1}, r_{i+2}, \cdot \cdot \cdot, r_n).$$

Now we may assume $b_{i+1} > r_{i+2}$.

Since $\langle pa_{i+1}, (m-1)p^\nu + a_{i+1} \rangle = b_{i+1} > r_{i+2}$ and

$$\langle (m-1)p^\nu + a_{i+1}, a \rangle \geqq r_{i+2} \; \forall \, a \in \operatorname{supp}(y_{i+1} + \cdot \cdot \cdot + y_n),$$
$$a > (m-1)p^\nu + a_{i+1},$$

it is clear by Lemma 1 that $\langle pa_{i+1}, a \rangle > r_{i+2} \; \forall \, a \in \operatorname{supp}(y_{i+1} + \cdot \cdot \cdot + y_n)$.

Hence $\operatorname{ord} x_{i+2} = pa_{i+2}$ and $pa_{i+2} \notin \operatorname{supp}(y_{i+1} + \cdot \cdot \cdot + y_n)$. Let $a \in \operatorname{supp} y_{i+1}$. Then $|a| > |(m-1)p^\nu + a_{i+2}| = |a_{i+2}|$ and hence $|a| \geqq |pa_{i+2}|$. Thus $\langle pa_{i+2}, a \rangle = \infty \; \forall \, a \in \operatorname{supp} y_{i+1}, a > pa_{i+2}$. Moreover, since $|(m-1)p^\nu + a_{i+2}| = |a_{i+2}| < |pa_{i+2}|$ and by $\langle pa_{i+1}, pa_{i+2} \rangle \leqq \langle pa_{i+1}, (m-1)p^\nu + a_{i+2} \rangle$ one concludes $(m-1)p^\nu + a_{i+2} > pa_{i+2}$.

To finish the inductive process, we need only to show

$$b_{i+2} \equiv \langle pa_{i+2}, (m-1)p^\nu + a_{i+2} \rangle$$
$$= b \frac{p^\nu}{|a_{i+2}|} - \frac{a_{i+2}}{|a_{i+2}|} + 1$$

is an integer, which is celar. Q. E. D.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

COROLLARY. *Let* $k[[t]] \supset k[[\omega]] \supset k[[x]]$ *be a chain of separable algebraic extensions of algebraic degree* p^ν *and* p *respectively. Let*

$$[t,\omega] = (a_0, a_1, \cdots, a_n), \quad [t,\omega]_r = (r_1, r_2, \cdots, r_n),$$

$$[\omega, x]_r = (b), b_0 = b, \cdots, b_i = b\frac{p^\nu}{|a_{i+1}|} - \frac{a_{i+1}}{|a_{i+1}|} + 1, \cdots, b_{n-1} = b^p = a_{n+1}.$$

If $b_i > r_{i+1}$ $0 \leqq i \leqq n-1$ *then* $[t,x]_r = (r_1, \cdots, r_n, b_{n-1})$. *Otherwise, let* i *be the smallest integer such that* $b_i \leqq r_{i+1}$. *Then* $b_i < r_{i+1}$ *implies*

$$[t,x]_r = (r_1, \cdots, r_i, b_i, r_{i+1}, \cdots, r_n),$$

and

$$b_i = r_{i+1} \Rightarrow [t,x]_r = (r_1, \cdots, r_i, r_{i+1}, \cdots, r_n).$$

Proof. It is clear from the proof of Proposition 6.

The following proposition will justify the term pre-higher ramification index.

PROPOSITION 7. *If* $k[[t]]$ *is a galois extension of algebraic degree* p^ν *over* $k[[x]]$ *then* $[t,x]_r =$ *sequence of higher ramification indices.*

Proof. Let

$$[t,x]_r = (r_1, r_2, \cdots, r_n)$$
$$x = x_0 + x_1 + \cdots + x_n$$

be the standard expression.

We divide the proof into several steps.

1) Given τ an automorphism $\operatorname{ord}(\tau(t) - t) = r \neq r_i \; \forall \, i$, we proceed to prove $\tau(x) \neq x$. If $r > r_n$ then by 1) of the proof of Proposition 3 $\tau(x) \neq x$.

Now suppose $r_{i+1} > r > r_i$ for $0 \leqq i \leqq n-1$, where $r_0 = 0$. Since

$$\tau(x) - x = \tau(x_0 + x_1 + \cdots + x_i) - (x_0 + \cdots + x_i) + (x_{i+1} + \cdots + x_n) - (x_{i+1} + \cdots + x_n),$$

it follows from 1) of Proposition 3 and Lemma 8 that

$$\operatorname{ord}(\tau(x_0 + \cdots + x_i) - (x_0 + \cdots + x_i)) = (r + \frac{a_i}{|a_i|} - 1)|a_i| = r|a_i| + a_i - |a_i|.$$

For any $a \in \operatorname{supp}(x_{i+1} + \cdots + x_n)$,

$$\operatorname{ord}(\tau(t)^a - t^a) = (\frac{a}{|a|} - 1 + r)|a| = r|a| + a - |a|.$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

If $|a| \geqq |a_i|$ clearly $r|a| + a - |a| > r|a_i| + a_i - |a_i|$, while if $|a| < |a_i|$, then $r < \langle a_i, a \rangle = \dfrac{a - a_i}{|a_i| - |a|} + 1$ implies

$$r|a| + a - |a| > r|a_i| + a_i - |a_i|.$$

Hence we conclude

$$\begin{aligned} \operatorname{ord}(\tau(x) - x) &= \operatorname{ord}(\tau(x_0 + \cdots + x_i) - (x_0 + \cdots + x_i)) \\ &= r|a_i| + a_i - |a_i| \neq \infty ; \end{aligned}$$

i. e., $\tau(x) \neq x$.

2) Suppose $\operatorname{ord}(\tau(t) - t) = r_i$ for some $0 < i \leqq n$. Since

$$\operatorname{ord}(\tau(x_{i+1} + \cdots + x_n) - (x_{i+1} + \cdots + x_n)) > r_i|a_i| + a_i - |a_i|,$$

$$\operatorname{ord}(\tau(x_0 + x_1 + \cdots + x_i) - (x_0 + \cdots + x_i)) > r_i|a_i| + a_i - |a_i|.$$

Using the same reasoning as in 2) of the proof of Proposition 3, we conclude that the coefficient y_r of t^r in $\tau(t)$ satisfies

$$\eta_{a_{i-1}} \frac{a_{i-1}}{|a_{i-1}|} \lambda_r^{|a_{i-1}|} + \cdots + \eta_a \frac{a}{|a|} \lambda_r^{|a|} + \cdots + \eta_{a_i} \frac{a_i}{|a_{i-1}|} \lambda_r^{|a_i|} = 0.$$

This expression has $\dfrac{|a_{i-1}|}{|a_i|}$ different solutions.

3) Let $G = G_1 \rhd G_2 \rhd \cdots \rhd G_n$ be the sequence of the higher ramification groups. Then by 1) and 2)

$$\begin{aligned} p^\nu = \operatorname{ord} G &= \Pi \operatorname{ord} G_i/G_{i+1} \leqq \Pi |a_i|/|a_{i+1}| \\ &= |a_0| = p^\nu \end{aligned}$$

hence $\operatorname{ord} G_i/G_{i+1} = \dfrac{|a_{i-1}|}{|a_i|}$. We conclude any r_i is a higher ramification index and $\operatorname{ord} G_i/G_{i+1} = \dfrac{|a_{i-1}|}{|a_i|}$.

COROLLARY. *If* $k[[t]] \supset k[[x]]$, $\operatorname{ord} x = p^\nu$, $[t, x]_r = (r_1)$, *then* $k[[t]]$ *is galois over* $k[[x]] \Leftrightarrow r_1$ *is an integer.*

Proof. $\Rightarrow$ Proposition 7.
$\Leftarrow$ Proposition 3.

LEMMA 16. *Given* $k[[t]] \supset k[[\omega]] \supset k[[x]]$ *where* $k[[t]]$ *is a galois extension over* $k[[\omega]]$ *of algebraic degree* $n \ni : |n| = 1$, *and* $k[[\omega]]$ *is a*

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

galois extension over $k[[x]]$ of algebraic degree p. Then there exists $k[[y]]$ such that $k[[t]]$ is a galois extension over $k[[y]]$ of algebraic degree p, and $k[[y]]$ is a galois extension over $k[[x]]$ of algebraic degree n.

Proof. We can choose t, ω, x such that

$$t = \omega^{1/n}, x = \omega^p + \lambda\omega^m = 1 = t^{np} + \lambda t^{nm} + \cdots \lambda \neq 0, \mid m \mid .$$

Let $y = x^{1/n} = t^p + \frac{\lambda}{n} t^{mn-(n-1)p} + \cdots$. Then

$$[t, y]_r = \langle p, mn - (n-1)p \rangle = \frac{mn - np}{p-1} + 1 = n[\omega, x]_r + (n-1).$$

Hence by the corollary and Proposition 3, $k[[t]]$ is a galois extension over $k[[y]]$. Q. E. D.

THEOREM. *Given $k[[t]]$ a separable algebraic extension over $k[[x]]$. Then there exists a chain of successive galois extensions between $k[[t]]$ and $k[[x]]$ if and only if $[t, x]_r$ is a sequence of integers.*

Proof. $\Leftarrow$ Let $\operatorname{ord} x = a$. Since $[t, x^{|a|/a}]_r = [t, x]_r$, Lemma 8 shows that it is enough to prove the case $\mid a \mid = a$, which is Proposition 5.

$\Rightarrow$

Using Lemma 16, we can assume there exists a chain of galois extensions between $k[[t]]$ and $k[[x^{|a|/a}]]$. Since $[t, x^{|a|/a}]_r = [t, x]_r$, we can assume $\mid a \mid = a = p^\nu$.

If $v = 1$, then from Proposition 7 $[t, x]_r$ is an integer. Using mathematical induction and Proposition 6, the theorem is proved.

4. Least Galois extension and G-character sequence.

LEMMA 17. *Given* $[t, x]_r = (r_1, r_2, \cdots, r_n)$, H. D. M. S. *of x with respect to* $t = (d_0, d_1, \cdots, d_s)$, $\mid a \mid = 1$. *Then*

$$[t^{1/a}, x^{1/a}]_r = (ar_1 - (a-1), ar_2 - (a-1) \cdots ar_n - (a-1))$$

and

H. D. M. S. *of* $x^{1/a}$ *with respect to*

$$t^{1/a} = (d_0, ad_1 - (a-1)d_0, \cdots, ad_s - (a-1)d_0).$$

Proof. It is clear that

H. D. M. S. of x wilth respect to $t^{1/a} = (ad_0, ad_1, \cdots, ad_s)$.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

By Lemma 8 we conclude

H. D. M. S. of $x^{1/a}$ with respect to

$$t^{1/a} = (d_0, ad_1 - (a-1)d_0, \cdots, ad_s - (a-1)d_0).$$

Since

$$|d_0| > |d_i| \; i > 0, \langle ad - (a-1)d_0, ad_j - (a-1)d_0\rangle = a\langle d_i, d_j\rangle - (a-1) \quad 0 \leqq i < j \leqq s.$$

Hence by Proposition 2,

$$[t^{1/a}, x^{1/a}]_r = (ar_1 - (a-1), \cdots, ar_n - (a-1)).$$

The following proposition is a generalization of one of Professor Abhyankar's lemmas: the least galois extension of a p-extension is tame.

PROPOSITION 8. *Suppose* $[t, x] = (a_0, a_1)$, $a_0 = p^\nu$, $|a_1| = 1$ $[t, x]_r = (r_1)$, *and* $[t, y] = (b_0, b_1)$, $b_0 = p^\nu$, $|b_1| = 1$ $[t, y]_r = (s_1)$. *Let* $a = \dfrac{p^\nu - 1}{(p^\nu - 1, a_1 - 1)}$ *Then* $k[[t^{1/a}]]$ *is the least galois extension of* $k[[x]]$ *containing* $k[[t]]$. *Moreover, the galois group of the least galois extension of* $k[[x]]$ *containing* $k[[t]]$ *iff* $(p^\nu - 1, a_1 - 1) = (p^\nu - 1, b_1 - 1)$ *and* $b_1 - 1 \equiv a_1 - 1 (p^\nu - 1)$.

Proof. By Lemma 1?, $k[[t^{1/c}]]$ is galois over $k[[x^{1/c}]]$ iff cr_1 is an integer. Since $r_1 = \langle a_0, a_1\rangle = \dfrac{a_1 - 1}{p^\nu - 1}$, cr_1 is an integer iff $a \mid c$. Thus for any $c < a$, $k[[t^{1/c}]]$ is not galois over $k[[x^{1/c}]]$; hence $k[[t^{1/c}]]$ is not galois over $k[[x]]$. It suffices to prove $k[[t^{1/a}]]$ is galois over $k[[x]]$.

Let $t^{1/a} = \omega$, $\tau^i(\omega) = \theta^i\omega$ $0 \leqq i < a$ where θ is an a-th primitive root of unity, and let G be the galois group of $k[[\omega]]$ over $k[[x^{1/a}]]$. Since $x \in k[[t]] = k[[\omega^a]]$, x is fixed by τ^i $0 \leqq i < a$. Since $k[[\omega]]$ is of degree ap^ν over $k[[x]]$, it is sufficient to show:

$$\phi\tau^i = \pi\tau^j \Rightarrow \phi = \pi, \tau^i = T^j$$

for any $\phi, \pi \in G$.

Let the higher ramification index of G be r. *Then* $r = ar_1 - (a-1)$ by Proposition 7 and Lemma 1?. Given any $\phi \in G$ let

$$\phi(\omega) = \omega + \lambda\phi\omega^r + \cdots.$$

Then $\phi = \pi \Leftrightarrow \lambda\phi = \lambda_\pi$ for any $\phi, \pi \in G$. Suppose $\phi\tau^i = \pi\tau^j$; then

$$\begin{aligned}\phi\tau^i(\omega) &= \theta^i\phi(\omega) = \theta^i\omega + \theta^i\lambda_\phi\omega^r + \cdots \\ &= \pi\tau^j(\omega) = \theta^j\omega + \theta^j\lambda_\pi\omega^r + \cdots.\end{aligned}$$

Hence $\theta^i = \theta^j$, $\lambda_\phi = \lambda_\pi$, i. e., $\tau^i = \tau^j$, $\phi = \pi$.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

We have proved that $k[[t^{1/a}]]$ is the least galois extension of $k[[x]]$ containing $k[[t]]$.

Before we proceed to prove the conditions for isomorphism, we study more closely the galois group H of $k[[t^{1/a}]]$ over $k[[x]]$.

The multiplicative rule af the group H is

$$(\phi\tau^i)(\pi\tau^j) = \phi(\tau^i\pi\tau^{-i})\tau^{i+j}$$

where

$$(\tau^i\pi\tau^{-i})(\omega) = \omega + \theta^{i(r-1)}\lambda_\pi\omega^r + \cdots$$

hence

$$\tau^i\pi\tau^{-i} \in G.$$

Since the inner automorphisms induced by $\{\tau^i\}$ define a group of automorphisms on G as a vector space over the prime field, G can be written as a direct sum of irreducible subspaces under the group of automorphisms. Let $G = G_1 + G_2, \cdots, + G_m$. Since $\lambda_{\tau^i\pi\tau^{-i}} = \theta^{i(r-1)}\lambda_\pi$, G_i is isomorphic to the additive group of $P(\theta^{r-1})$ where P is the prime field. Now H is isomorphic to the group of $m+1$-tuples $(\lambda_1, \lambda_2, \cdots, \lambda_m\theta^i)$ where $\lambda_j \in P(\theta^{r-1})$, and the group structure is defined by

$$\begin{aligned}(\lambda_1, \lambda_2, \cdots, \lambda_m, \theta^i) \cdot (\mu_1, \mu_2, \cdots, \mu_m, \theta^j)\\ = (\lambda_1 + \theta^{i(r-1)}\mu_1, \cdots, \lambda_m + \theta^{i(r-1)}\mu_m, \theta^{i+j}).\end{aligned}$$

Now we proceed to prove the conditions on isomorphism.

Let H^* be the galois group of the least galois extension of $k[[y]]$ containing $k[[t]]$. Then the order of H equals the order of H^* since $\operatorname{ord}(H) = p^\nu a = p^\nu \dfrac{p-1}{(p^\nu-1, a_1-1)}$, $\operatorname{ord}(H^*) = p^\nu \dfrac{p^\nu-1}{(p^\nu-1, k_1-1)}$, it is obvious $(p^\nu-1, a_1-1) = (p^\nu-1, b_1-1)$.

Let the isomorphism be $f: H \to H^*$, and g_{τ^i}, $g^*_{\tau^i}$ be the inner automorphisms induced by τ^i on H, H^* respectively. Then $fg_{\tau^i}(\pi) = f(\tau^i\pi\tau^{-i}) = f(\tau^i)f(\pi)f(\tau^{-i}) = g^*_{f(\tau)^i}f(\pi)$. Thus the cardinal number of the orbit of π under $\{g_{\tau^i}\}$ equals the cardinal number or the orbit of $f(\pi)$ under $\{g^*_{\tau^i}\}$ since $f: \{\tau^i\} \to \{\tau^i\}$. Hence

$$\begin{aligned}r-1 &= ar_1 - (a-1) - 1\\ &= a(r_1-1) \equiv a(s_1-1) \bmod(a)\end{aligned}$$

i.e.

$$\frac{a_1-1}{p^\nu-1}\left[\frac{p^\nu-1}{(p^\nu-1, a_1-1)}\right] \equiv \frac{b_1-1}{p^\nu-1}\left[\frac{p^\nu-1}{(p^\nu-1, a_1-1)}\right] \bmod(a).$$

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

Hence we conclude:

$$a_1 - 1 \equiv b_1 - 1 \bmod (p^\nu - 1).$$

$\Leftarrow$

It is clear from our discussion on the representation of H as $m+1$-tuples. Q. E. D.

The following corollary follows from the proof of the preceding proposition.

COROLLARY. *The galois group of the least galois extension is abelian iff* $a_1 - 1 \equiv 0 (p^\nu - 1)$.

The following proposition is pointed out by Professor Abhyankar.

PROPOSITION 9. *Suppose* $\operatorname{ord} x = p^\nu$. *If* $[t, x]_r = (r_1, \cdots, r_n)$ *is a sequence of integers, then the least galois extension of* $k[[x]]$ *containing* $k[[t]]$ *is purely wild; i. e., the corresponding algebraic degree is* p^u *for some* u.

Proof. If $\operatorname{ord} x = p$, then $k[[t]]_1$ is galois over $k[[x]]$. Therefore we assume $\operatorname{ord} x = p^\nu$ for some $\nu > 1$. By our theorem we know there exists a $\omega \in k[[t]]$ such that $k[[t]] \overset{p}{\supset} k[[\omega]] \overset{p^{\nu-1}}{\supset} k[[x]]$ and $[\omega, x]_r$ is a sequence of integers. Assume the least galois extension of $k[[x]]$ containing $k[[\omega]]$ is purely wild over $k[[x]]$ and call it $k[[y]]$.

If $t \in k[[y]]$ then $k[[y]]$ is the least galois extension of $k[[x]]$ containing $k[[t]]$, hence we are done.

If $t \notin k[[y]]$, let $k[[z]]$ be the integral closure of $k[[y]][t]$ in $k((y, t))$. Then $k[[z]]$ is a galois extension of degree p over $k[[y]]$, and the least galois extension $k[[u]]$ of $k[[x]]$ containing $k[[t]]$ is the one containing $k[[z]]$.

Imbed $k[[z]]$ in an algebraic closure Ω of $k[[x]]$. Let $k[[z_i]]$ be the conjugates of $k[[z]]$ under the k-automorphisms of Ω which induce $k[[x]]$-automorphisms on $k[[y]]$. It is obvious that $k[[z_i]]$ is galois over $k[[y]]$ with isomorphic galois groups for all i. Since $k[[u]]$ is the compositum of all $k[[z_i]]$, we can imbed the galois group of $k[[u]]$ over $k[[y]]$ in the direct sum of the galois groups of $k[[z_i]]$ over $k[[y]]$ for all i, which is isomorphic to a finite direct sum of the galois groups of $k[[z]]$ over $k[[y]]$. Hence the galois group of $k[[u]]$ over $k[[y]]$ is a subgroup of a group of order p^λ for some λ. Thus the order of $k[[u]]$ over $k[[x]]$ is only divisible by p. Q. E. D.

5. Saturation and G-character sequences. We summarize the proof of Proposition 3 in the following lemma.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

LEMMA 18. *Given* $[t,x]=(a_0,a_1,\cdots,a_n)$, $[t,x]_r=(r_1,\cdots,r_n)$ *and a group* G *of automorphisms of* $k[[t]]$ *with higher ramification index* r, *then*

1) $r\neq r_i$ *i implies* $\operatorname{ord}(\tau(x)-x)=\min\operatorname{ord}(\tau(t^a)-t^a)$ *where* a *runs through* $\operatorname{supp}(x)$, $\tau\in G$.

2) $r=r_i \operatorname{ord} G>\dfrac{|a_{i-1}|}{|a_i|}$ *implies* $\min\{\operatorname{ord}(\tau(x)-x)\mid \tau\in G\}$
$=\min\{\operatorname{ord}\tau(t^a)-t^a\mid \tau\in G\, a\in\operatorname{supp}(x)\}$.

PROPOSITION 10. *Let* $x,y\in k[[t]]$ *with* $\operatorname{ord}x=p^\nu$, $\operatorname{ord}y=m$ *with* $m>p^\nu$, $|m|=1$, $0=k[[x,y]]$. *Suppose* $[t,x]_r=(r_1)$. *Then the saturation* $\tilde{0}_x$ *of* 0 *with respect to* x *is* $0+\Sigma M^b+M^m$ *where* M *is the maximum ideal of* $k[[t]]$ *and* b *runs through all integers less than* m *with* $\langle b,m\rangle\leqq r_1$.

Proof. By Proposition 8 let $k[[t^{1/a}]]$ be the least galois extension of $k[[x]]$ containing $k[[t]]$, G be the galois group of $k[[t^{1/a}]]$ over $k[[x^{1/a}]]$ and let r be the higher ramification index of G. Let τ^i be the automorphism defined by $\tau^i(t^{1/a})=\theta^i t^{1/a}$ where θ is a-th primitive root of unity.

Clearly $M^m\subset\tilde{0}_x$. Let $z\in M^b$ for some $b<m$ with $\langle b,m\rangle\leqq r_1$. By Lemma 3 $\langle c,m\rangle\leqq r_1$ $c\in\operatorname{supp}z$ and $c<m$. To show $0+\Sigma M^b+M^m\subset\tilde{0}_x$, it is enough to show that $t^b\in\tilde{0}_x$ $b<m$ and $\langle b,m\rangle\leqq r_1$. Since for any $\pi\in G$, we have

$$\operatorname{ord}(\pi(t^b)-t^b)=ba-|b|+r|b|$$
$$\operatorname{ord}(\pi(t^m)-t^m)=am-1+r.$$

Furthermore

$$\langle b,m\rangle\leqq r_1$$

implies

$$\frac{m-b}{|b|-1}+1\leqq r_1$$
$$\frac{am-ba}{|b|-1}+a\leqq ar_1$$
$$\frac{am-ba}{|ab|-1}+1\leqq ar_1-(a-1)=r.$$

Hence

$$am-1+r\leqq ba-|b|+r|b|.$$

Thus

$$t^b\in\tilde{0}_x, b<m \text{ and } \langle b,m\rangle.$$

On the other hand, suppose $z\in\tilde{0}_x$. By subtracting some element in 0, we can assume $|\operatorname{ord}z|<p^\nu$. Using Lemma 18, we conclude that

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions

$\operatorname{ord}(\pi(t^b) - t^b) \geqq am - 1 + r \quad b \in \operatorname{supp} z$. Reversing the above calculation we conclude

$$\langle b, m \rangle \leqq r_1 \quad b < m, \quad b \in \operatorname{supp} z.$$

i. e.,

$$z \in \tilde{0} + \Sigma M^b + M^m \qquad \text{Q. E. D.}$$

COROLLARY. *Suppose* $z \in 0$, $\operatorname{ord} z = p^\nu$ *and* $[t, z] = (s_1)$. *If* $s_1 \geqq r_1$ *then* $\tilde{0}_x \subset \tilde{0}_z$.

COROLLARY. *If* $\operatorname{ord} x = p$ *then the saturations are independent of transversal parameters.*

Remark. In general saturations are dependent on transversal parameters. If G-character sequences are different, then the saturations could be different with the same least galois extension and the same galois group.

The following example is about a case such that $[t, x]_r$ is not one number;

Example. Let k be an algebraically closed field of characteristic 2, $k[[t]]$ be a powerseries ring, and $x, \omega \in k[[t]]$ with

$$\omega = t^3 + t^5 + t^7$$
$$x = \omega^3 + \omega^7 = t^9 + t^{15} + t^{21} + t^{23} + t^{25} + t^{27} + \cdots.$$

Since $[t, \omega]_r = (2)$, and $[t, x]_r = (2.5)$ we have by Proposition 2 that there exists at least 9 different automorphisms which fix x. Hence $k[[t]]$ is galois over $k[[x]]$ with abelian galois group.

Let $y = t^{15} + \lambda^{21} + t^{23}$, $\lambda \in k$, $\lambda \neq 1$. Then y is not fixed by any of the 9 automorphisms because $[t, x - y]_r = (3)$. Hence $k((x, y)) = k((t))$, and $k[[t]]$ is galois over $k[[x - y]]$ with abelian galois group.

Now it is routine to check $t^{19} \in \tilde{0}_{x-y}$, while $t^{19} \notin \tilde{0}_x$.

REFERENCES.

[1] S. S. Abhyankar, "Inversion and invariance of characteristic pairs," *American Journal of Mathematics*, vol. 89 (1967), pp. 363-372.

[2] O. Zariski, *Studies in equisingularity*, III, saturation of local rings and equisingularity. Lecture note. Harvard University.

[3] O. Zariski and P. Samuel, *Commutative Algebra*, vols. I & II, Van Nostrand, Princeton, New Jersey.

This content downloaded from 128.163.2.206 on Wed, 1 Jan 2014 23:09:35 PM
All use subject to JSTOR Terms and Conditions