Journal of Algebra 344 (2011) 1–13

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Finite p-groups and $k((t))$

Anthony J. Bevelacqua [a,*], Mark Motley [b]

[a] Department of Mathematics, University of North Dakota, Grand Forks, ND 58202, United States
[b] Glen Burnie, MD, United States

ARTICLE INFO

Article history:
Received 13 February 2009
Available online 19 August 2011
Communicated by Aner Shalev

Keywords:
p-Groups
Laurent series

ABSTRACT

Let k be a field of characteristic $p > 0$ and let $K = k((t))$ be the field of Laurent series over k. For each group G of order p^n there exist units $u \in k[\![t]\!]$ such that $K/k((ut^{p^n}))$ is Galois with $\mathrm{Gal}(K/k((ut^{p^n}))) \cong G$. We explore the connections between G and u. Among other results, we prove that if both $K/k((u_1t^{p^n}))$ and $K/k((u_2t^{p^n}))$ are Galois and u_1 and u_2 are sufficiently close in the t-adic topology, then $\mathrm{Gal}(K/k((u_1t^{p^n}))) \cong \mathrm{Gal}(K/k((u_2t^{p^n})))$.

1. Introduction

Let k be a field of characteristic $p \geqslant 0$ and let $K = k((t))$ be the field of Laurent series over k. Let v_t (or even just v) be the t-adic valuation on K/k. Set $\mathcal{U} = k[\![t]\!]^\times$ and $\mathcal{A} = \mathrm{Aut}(K/k)$. We will show that if $L \subseteq K$ is a subfield with K/L a finite Galois extension, then either G is cyclic when $p = 0$ or $G = \mathrm{Gal}(K/L)$ is an extension of a p-group by a cyclic group with order prime to p when $p > 0$. Given this, it is natural to try to investigate the situation when $p > 0$ and $\mathrm{Gal}(K/L)$ is a finite p-group.

Let G be a finite p-group of order p^n. Then for any field k of characteristic $p > 0$ there exists a totally ramified Galois extension E/K with $\mathrm{Gal}(E/K) \cong G$. Since E is complete with respect to the unique extension of v to E, $E = k((s))$ for some $s \in E$ by the structure theory of such fields. Now K and E are analytically isomorphic so there exists $L = k((ut^{p^n})) \subseteq K$ such that K/L is Galois of degree p^n with $G \cong \mathrm{Gal}(K/L)$. We want to understand how information about $G = \mathrm{Gal}(K/k((ut^{p^n})))$ can be determined from u. We will show, among other things, that if $L_1 = k((u_1t^{p^n}))$ and $L_2 = k((u_2t^{p^n}))$ are subfields of K such that K/L_1 and K/L_2 are Galois then there exists an integer N (depending on u_1) so that if $v(u_1 - u_2) > N$ then $\mathrm{Gal}(K/L_1) \cong \mathrm{Gal}(K/L_2)$.

* Corresponding author.
E-mail addresses: anthony.bevelacqua@email.und.edu (A.J. Bevelacqua), mmotley@ms.uky.edu (M. Motley).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2011.08.002

2. Structure of $\mathbf{Aut}(k((t))/k)$

Let $k((t))/k((x))$ be a finite Galois extension with Galois group G. We first determine the possible Galois groups which can occur. We will see that, when the characteristic of k is $p > 0$, the most interesting Galois groups which occur are p-groups.

We know that $v(\sigma(\alpha)) = v(\alpha)$ for all $\sigma \in \mathcal{A}$ and for all $\alpha \in K$. It follows that $v(\frac{\sigma(\alpha)}{\alpha}) = 0$ for all $\alpha \in K^\times$. So for each $\alpha \in K^\times$ we define $\phi_\alpha : \mathcal{A} \to \mathcal{U}$ by $\sigma \mapsto \frac{\sigma(\alpha)}{\alpha}$.

Proposition 1. *Let $\alpha \in K^\times$. Then ϕ_α is a crossed homomorphism (or derivation or 1-cocycle) $\mathcal{A} \to \mathcal{U}$. It is principal (or inner or 1-coboundary) if and only if $\alpha \in \mathcal{U}$.*

Proof. ϕ_α is a crossed homomorphism:

$$\begin{aligned}\phi_\alpha(\sigma\tau) &= \frac{\sigma\tau(\alpha)}{\alpha} \\ &= \frac{\sigma(\alpha)}{\alpha}\frac{\sigma\tau(\alpha)}{\sigma(\alpha)} \\ &= \frac{\sigma(\alpha)}{\alpha}\left(\frac{\tau(\alpha)}{\alpha}\right)^\sigma \\ &= \phi_\alpha(\sigma)\phi_\alpha(\tau)^\sigma.\end{aligned}$$

If $\alpha \in \mathcal{U}$ then, by definition, ϕ_α is principal. Now suppose ϕ_α is a principal crossed homomorphism. Then there exists a $u \in \mathcal{U}$ such that $\phi_\alpha(\sigma) = \frac{\sigma(u)}{u}$ for all $\sigma \in \mathcal{A}$. That is $\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(u)}{u}$ and so $\sigma(\frac{\alpha}{u}) = \frac{\alpha}{u}$ for all $\sigma \in \mathcal{A}$. Therefore $\frac{\alpha}{u} \in (K^\times)^{\mathcal{A}} = k^\times$ and so $\alpha \in k^\times\mathcal{U} = \mathcal{U}$. □

In particular ϕ_t gives a nontrivial element of $H^1(\mathcal{A}, \mathcal{U})$. We also note that ϕ_t is bijective because for any $u \in \mathcal{U}$ there exists a $\sigma \in \mathcal{A}$ with $\sigma(t) = ut$. From now on we will denote $\phi_t(\sigma)$ by u_σ. Thus $\sigma(t) = u_\sigma t$ and $u_{\sigma\tau} = u_\sigma u_\tau^\sigma$ for all $\sigma, \tau \in \mathcal{A}$.

For any $n \geqslant 0$ and $\sigma \in \mathcal{A}$ we have $(t^{n+1})^\sigma = (t^{n+1})$ and thus σ induces an automorphism of $R_n = k[\![t]\!]/(t^{n+1})$ which we'll denote by $\sigma^{[n]}$. If $\sigma, \tau \in \mathcal{A}$ we have $(\sigma\tau)^{[n]} = \sigma^{[n]}\tau^{[n]}$ and thus $h_n : \mathcal{A} \to \mathrm{Aut}_k(R_n)$ given by $\sigma \mapsto \sigma^{[n]}$ is a group homomorphism. We define $\mathcal{A}_n = \ker h_n$. Note that $\mathcal{A}_0 = \mathcal{A}$.

Proposition 2. *We have $\sigma \in \mathcal{A}_n$ if and only if $v_t(u_\sigma - 1) \geqslant n$.*

Proof. Since σ fixes the elements of k we have $\sigma \in \mathcal{A}_n$ if and only if $u_\sigma t + (t^{n+1}) = \sigma^{[n]}(t + (t^{n+1})) = t + (t^{n+1})$ iff $u_\sigma t - t \in (t^{n+1})$ iff $u_\sigma - 1 \in (t^n)$ iff $v_t(u_\sigma - 1) \geqslant n$. □

It's now clear that $\mathcal{A} = \mathcal{A}_0 \supseteq \mathcal{A}_1 \supseteq \mathcal{A}_2 \supseteq \cdots$ is a chain of normal subgroups of $\mathcal{A}$ and $\bigcap_{n=0}^\infty \mathcal{A}_n = \{\mathrm{id}_K\}$.

In [1] Camina studies $\mathcal{A}$ for $k = \mathbb{F}_p$, the finite field with p elements. In particular our $\mathcal{A}_1$ is her J. In [2] Johnson studies $t + t^2R[\![t]\!]$ for an arbitrary commutative ring with identity R as the group of formal power series under substitution. This is essentially the group $\mathcal{A}_1$ when $R = k$ is a field.

Proposition 3. $\mathcal{A}/\mathcal{A}_1 \cong k^\times$.

Proof. For any $u = a_0 + a_1t + \cdots \in \mathcal{U}$ and any $\sigma \in \mathcal{A}$ we have $u^\sigma = a_0 + a_1t^\sigma + \cdots$ and so $u \equiv u^\sigma \bmod t$. So $u_{\sigma\tau} = u_\sigma u_\tau^\sigma \equiv u_\sigma u_\tau \bmod t$. Thus the map $\sigma \mapsto u_\sigma \bmod t$ is an epimorphism with kernel $\mathcal{A}_1$. □

In fact, the exact sequence $1 \to \mathcal{A}_1 \to \mathcal{A} \to k^\times \to 1$ splits. Let $\mathcal{B} = \{\sigma \in \mathcal{A} \mid u_\sigma \in k^\times\}$. Clearly $\mathcal{B}$ is a subgroup of $\mathcal{A}$, $\mathcal{B} \cong k^\times$, and $\mathcal{A} = \mathcal{A}_1 \rtimes \mathcal{B}$.

We now focus our attention on $\mathcal{A}_1$. It will be convenient to introduce the standard filtration of $\mathcal{U}$: define $\mathcal{U}_0 = \mathcal{U}$ and for each $n \geqslant 1$ define $\mathcal{U}_n = 1 + t^n k[\![t]\!]$. By an earlier result we have $\sigma \in \mathcal{A}_n$ if and only if $u_\sigma \in \mathcal{U}_n$.

Lemma 4. *If $u \in \mathcal{U}_n$ and $\sigma \in \mathcal{A}_1$, then $u^\sigma \equiv u \bmod t^{n+1}$.*

Proof. We have $u \equiv 1 + a_n t^n \bmod t^{n+1}$ and $u_\sigma = 1 + \lambda_1 t + \cdots$ and so

$$\begin{aligned} u^\sigma &\equiv 1 + a_n(1 + \lambda_1 t + \cdots)^n t^n \mod t^{n+1} \\ &\equiv 1 + a_n t^n \mod t^{n+1} \\ &\equiv u \mod t^{n+1}. \qquad \square \end{aligned}$$

We will use the following identity repeatedly

$$\begin{aligned} u_{\sigma\tau} - 1 &= u_\sigma u_\tau^\sigma - 1 \\ &= (u_\sigma - 1) + \big(u_\tau^\sigma - 1\big) + (u_\sigma - 1)\big(u_\tau^\sigma - 1\big) \\ &= (u_\sigma - 1) + (u_\tau - 1)^\sigma + (u_\sigma - 1)(u_\tau - 1)^\sigma. \end{aligned}$$

Proposition 5. *$\mathcal{A}_n/\mathcal{A}_{n+1} \cong k^+$ for all $n \geqslant 1$.*

Proof. For any $\sigma \in \mathcal{A}_n$ we have $v_t(u_\sigma - 1) \geqslant n$ and so $v_t(\frac{u_\sigma - 1}{t^n}) \geqslant 0$. Thus we can define $f : \mathcal{A}_n \to k^+$ by $\sigma \mapsto \frac{u_\sigma - 1}{t^n} \bmod t$. For any $\sigma, \tau \in \mathcal{A}_n$ we have

$$\begin{aligned} f(\sigma\tau) &= \frac{u_{\sigma\tau} - 1}{t^n} \mod t \\ &\equiv \frac{u_\sigma - 1}{t^n} + \frac{(u_\tau - 1)^\sigma}{t^n} + \frac{u_\sigma - 1}{t^n}(u_\tau - 1)^\sigma \mod t \\ &\equiv \frac{u_\sigma - 1}{t^n} + \frac{u_\tau - 1}{t^n} \mod t \\ &= f(\sigma) + f(\tau). \end{aligned}$$

f is surjective because there exists a $\sigma \in \mathcal{A}_n$ with $u_\sigma = 1 + \lambda t^n$ for any $\lambda \in k$ and $\ker f$ is $\mathcal{A}_{n+1}$. Therefore $\mathcal{A}_n/\mathcal{A}_{n+1} \cong k^+$. $\square$

Proposition 6. *If $\sigma \in \mathcal{A}_d$ and $n \in \mathbb{Z}$ we have*

$$u_{\sigma^n} - 1 \equiv n(u_\sigma - 1) \mod t^{d+1}.$$

Proof. For $n \geqslant 1$ we proceed by induction. The statement is clearly true for $n = 1$; suppose it's true for n. Consider

$$\begin{aligned} u_{\sigma^{n+1}} - 1 &= u_{\sigma^n \sigma} - 1 \\ &= (u_{\sigma^n} - 1) + (u_\sigma - 1)^{\sigma^n} + (u_{\sigma^n} - 1)(u_\sigma - 1)^{\sigma^n} \end{aligned}$$

$$\begin{aligned}
&\equiv (u_{\sigma^n} - 1) + (u_\sigma - 1) \mod t^{d+1} \\
&\equiv n(u_\sigma - 1) + (u_\sigma - 1) \mod t^{d+1} \\
&\equiv (n+1)(u_\sigma - 1) \mod t^{d+1}.
\end{aligned}$$

For $n = 0$ the statement is trivial because we have $u_{\sigma^0} = u_{\mathrm{id}_K} = 1$.
For $n = -1$ we have

$$\begin{aligned}
0 &= u_{\mathrm{id}_K} - 1 \\
&= (u_{\sigma\sigma^{-1}} - 1) \\
&\equiv (u_\sigma - 1) + (u_{\sigma^{-1}} - 1) \mod t^{d+1}
\end{aligned}$$

and so $(u_{\sigma^{-1}} - 1) \equiv -(u_\sigma - 1) \mod t^{d+1}$. Since $\sigma^{-1} \in \mathcal{A}_n$ the result now follows from the first paragraph. □

Corollary 7. *If k has characteristic 0, $\mathcal{A}_1$ is torsion-free. If k has characteristic $p > 0$, the torsion elements of $\mathcal{A}_1$ have p-power order.*

Proof. Let $\sigma \in \mathcal{A}_1$ with $\sigma \neq \mathrm{id}_K$. Then $\sigma \in \mathcal{A}_d - \mathcal{A}_{d+1}$ for some $d \geqslant 1$. Thus $u_\sigma - 1 \equiv \lambda t^d \mod t^{d+1}$ for some $\lambda \in k^\times$. We then have $u_{\sigma^n} - 1 \equiv n(u_\sigma - 1) \mod t^{d+1}$ for all n. Thus we have $\frac{u_{\sigma^n}-1}{t^d} \equiv n\frac{u_\sigma - 1}{t^d} \equiv n\lambda \mod t$ for all n.

So if the characteristic of k is 0, $\frac{u_{\sigma^n}-1}{t^d} \not\equiv 0 \mod t$ for all $n \geqslant 1$ and therefore $u_{\sigma^n} \neq 1$ for all $n \geqslant 1$. Thus σ is not torsion.

If the characteristic of k is $p > 0$ and τ has order $n = mp^e$ for some m with $p \nmid m$ and $e \geqslant 0$, then $\sigma = \tau^{p^e}$ has order m. If $m \neq 1$ (that is, $\sigma \neq \mathrm{id}_K$) we have $0 = \frac{u_{\sigma^m}-1}{t^d} \equiv m\lambda \mod t$ by the first paragraph and therefore $p|m$. This contradiction shows $m = 1$. □

The above proposition and corollary are found, with their notation and emphasis, in [2].

Proposition 8. *Let G be a finite subgroup of $\mathcal{A}$. Then:*

1. *If k has characteristic 0, G is cyclic of order s where s is the order of some root of unity in k and $G \cap \mathcal{A}_1 = \{\mathrm{id}_K\}$.*
2. *If k has characteristic $p > 0$, $G/G \cap \mathcal{A}_1$ is cyclic of order s where s is the order of some root of unity in k and $G \cap \mathcal{A}_1$ is the p-Sylow subgroup of G.*

In either case, G is solvable.

Proof. We have $G \hookrightarrow \mathcal{A} \to \mathcal{A}/\mathcal{A}_1 \cong k^\times$ and so $G/G \cap \mathcal{A}_1$ is isomorphic to a subgroup of $k^\times$. Since $G/G \cap \mathcal{A}_1$ is finite and finite subgroups of $k^\times$ are generated by a root of unity, $G/G \cap \mathcal{A}_1$ is cyclic of order s where s is the order of a root of unity in k.

If k has characteristic 0, $G \cap \mathcal{A}_1 = \{\mathrm{id}_K\}$ because $\mathcal{A}_1$ is torsion-free.

If k has characteristic $p > 0$, $G \cap \mathcal{A}_1$ has p-power order as the torsion elements of $\mathcal{A}_1$ have p-power order. Since $[G : G \cap \mathcal{A}_1] = s$ is the order of a root of unity in k, $p \nmid s$. Thus $G \cap \mathcal{A}_1$ is the p-Sylow subgroup of G.

In either case, $G/G \cap \mathcal{A}_1$ is cyclic and $G \cap \mathcal{A}_1$ is nilpotent; thus G is solvable. □

3. Totally ramified extensions and subfields

We begin with a lemma which confirms that the codimension of $k((ut^s))$ in K is s. The converse of this statement is usually true: if k is a field either of characteristic 0 or of characteristic $p > 0$ and $[k : k^p]$ is finite then every subfield of K of codimension s is of the form $k((ut^s))$ for some unit u. For this result see [3].

Lemma 9. *Let k be any field, $s > 1$, and $u \in \mathcal{U}$. Then $[k((t)) : k((ut^s))] = s$.*

Proof. Let $K = k((t))$ and $L = k((ut^s))$. For notational convenience, set $\pi = ut^s$, and $R = k[\![t]\!]$. Now $\pi R = t^s R$, so $R/\pi R \cong k[t]/t^s k[t]$ has a k-basis $1, t, t^2, \ldots, t^{s-1}$. We prove by induction on n that there exist $\lambda_{i,j}$ for $i = 0, 1, \ldots, s-1$ and for all $j \geqslant 0$ such that

$$t^s \equiv \left(\sum_{j=0}^{n} \lambda_{0,j}\pi^j\right)1 + \left(\sum_{j=0}^{n} \lambda_{1,j}\pi^j\right)t + \cdots + \left(\sum_{j=0}^{n} \lambda_{s-1,j}\pi^j\right)t^{s-1} \mod \pi^{n+1}.$$

This is true for $n = 0$ since

$$t^s \equiv \lambda_{0,0} + \lambda_{1,0}t + \cdots + \lambda_{s-1,0}t^{s-1} \pmod{t^s}$$

with $\lambda_{i,0} = 0$ for each i at this stage. Now suppose the result is true for $n > 0$. Then

$$\begin{aligned}&\frac{1}{\pi^{n+1}}\left(t^s - \left(\sum_{j=0}^{n} \lambda_{0,j}\pi^j\right)1 - \left(\sum_{j=0}^{n} \lambda_{1,j}\pi^j\right)t - \cdots - \left(\sum_{j=0}^{n} \lambda_{s-1,j}\pi^j\right)t^{s-1}\right)\\ &\quad\equiv \lambda_{0,n+1} + \lambda_{1,n+1}t + \cdots + \lambda_{s-1,n+1}t^{s-1} \mod \pi\end{aligned}$$

for some $\lambda_{i,n+1} \in k$. Now multiply by π^{n+1} and collect terms to get the truth of the statement for $n+1$. Therefore $a_i = \sum_{j=0}^{\infty} \lambda_{i,j}\pi^j \in L$ for each i, and

$$t^s = a_0 + a_1 t + \cdots + a_{s-1}t^{s-1}.$$

Thus t is algebraic over L. Then $L(t)/L$ is finite, and since L is complete, so is $L(t)$. Now $k(t) \subseteq L(t)$ and so $L(t)$ contains the closure of $k(t)$, which is $k((t))$. Hence $k((t)) = L(t)$. Since $k((t))/L$ is finite, its ramification index is s, and its inertial degree is 1, we have $[k((t)) : L] = s$. □

We have seen that for any Galois extension $k((t))/k((ut^s))$, the Galois group is an extension of a p-group by a cyclic group with order prime to p. So it is reasonable to consider extensions whose Galois groups are p-groups. We now turn our attention to determining the possible Galois groups which occur. From this point on, we assume k is a field of characteristic $p > 0$.

Lemma 10. *Let K be a field of characteristic $p > 0$, and K_p be the compositum of all p-power Galois extensions of K. Then $\mathrm{Gal}(K_p/K)$ is a free pro-p group. The number of generators of this group is equal to the dimension of the $\mathbb{Z}/p\mathbb{Z}$-vector space $K/\wp(K)$, where $\wp(y) = y^p - y$.*

Proof. See Proposition 30 in Chapter IV of [4]. □

Lemma 11. *Let $K = k((t))$, where k is a field of characteristic $p > 0$. The $\mathbb{Z}/p\mathbb{Z}$-vector space $K/\wp(K)$ is infinite dimensional.*

Proof. The infinite set $\{t^{-n} + \wp(K)\colon\ n > 0 \text{ and } p \nmid n\}$ is linearly independent in $K/\wp(K)$: Assume

$$\alpha = c_0 t^{-n_0} + \cdots + c_s t^{-n_s} = f^p - f \in \wp(K)$$

where $c_i \in \mathbb{Z}/p\mathbb{Z}$, $-n_0 < \cdots < -n_s$, $c_0 \neq 0$, and $p \nmid n_i$ for $i = 0, \ldots, s$. We have $v(\alpha) = -n_0$ and so $v(f)$ must be < 0. But then $v(f^p) < v(f)$ so $v(f^p - f) = v(f^p) = pv(f)$, a contradiction to $p \nmid n_0$. $\square$

Together, the last two lemmas show that the Galois group of K_p/K is a free pro-p group on an infinite number of generators.

Lemma 12. *Let k be a field of characteristic $p > 0$ and $K = k((t))$. Then every finite p-group G is the Galois group of a totally ramified extension of K.*

Proof. Let G be a finite p-group of order p^n.

Suppose first that k is a finite field. Since K_p/K is Galois with Galois group a free pro-p group on an infinite number of generators, we can choose an extension F/K with Galois group isomorphic to $G \times G$. Let $G_1 = G \times \{1\}$ and $G_2 = \{1\} \times G$. If F_i is the fixed field of G_i, then F_i/K is a Galois extension with Galois group isomorphic to G. Let F' be the maximal unramified extension of $k((t))$ in F. Then F'/K is a cyclic extension of p-power order. Since $F_1 \cap F_2 = K$, it follows that at least one of F_i/K is totally ramified, as otherwise each F_i intersects F' nontrivially, and so each F_i must contain the unique degree p extension of K in F', a contradiction. Hence we may assume that F_1/K is totally ramified with Galois group G.

Now suppose k is an arbitrary field of characteristic p. Let k_0 be the prime subfield of k. So k_0 is the finite field with p elements. Let $K_0 = k_0((t))$. By the first paragraph K_0 has a totally ramified Galois extension L_0/K_0 with Galois group G. Since L_0K/K is finite L_0K is complete with respect to a real valuation which extends v. We'll call this valuation v as well, so all our fields are complete with respect to the appropriate restrictions of v.

We have

$$\begin{aligned}
\bigl[v\bigl(L_0^\times\bigr) : v\bigl(K_0^\times\bigr)\bigr] &= [L_0 : K_0] \\
&\geqslant [L_0K : K] \\
&\geqslant \bigl[v\bigl((L_0K)^\times\bigr) : v\bigl(K^\times\bigr)\bigr] \\
&= \bigl[v\bigl((L_0K)^\times\bigr) : v\bigl(K_0^\times\bigr)\bigr] \\
&\geqslant \bigl[v\bigl(L_0^\times\bigr) : v\bigl(K_0^\times\bigr)\bigr].
\end{aligned}$$

Thus we must have equality throughout. In particular we have

$$\bigl[v\bigl((L_0K)^\times\bigr) : v\bigl(K^\times\bigr)\bigr] = [L_0K : K] = \bigl[L_0^\times : K_0^\times\bigr].$$

Thus L_0K/K is totally ramified and $\mathrm{Gal}(L_0K/K) \cong \mathrm{Gal}(L_0/K_0)$ by the Theorem on Natural Irrationalities and the equality of the dimensions. $\square$

Proposition 13. *For any finite p-group G and k a field of characteristic p there exists a unit $u \in \mathcal{U}_1$ such that $K/k((ut^{p^n}))$ is Galois with Galois group isomorphic to G.*

Proof. Let G be a finite p-group of order p^n. By the lemma there exists a field extension E/K such that E/K is totally ramified and Galois with $\mathrm{Gal}(E/K) = G$. By the structure theorem of finite extensions of $K = k((t))$ we see that $E = k((s))$ for some $s \in E$. Since E and K are analytically k-isomorphic we see that K has a subfield L of codimension p^n such that $k \subseteq L$, L is closed (and hence complete) in the t-adic topology on K, and K/L is a totally ramified Galois extension with $\mathrm{Gal}(K/L) = G$. Thus

$L = k((z))$ for some $z \in L$ and since K/L is totally ramified we have $v(z) = p^n$. Therefore $z = ut^{p^n}$ for some $u \in \mathcal{U}$. Since $k((ut^{p^n})) = k((\lambda ut^{p^n}))$ for any $\lambda \in k^\times$ we can suppose $u \in \mathcal{U}_1$. $\square$

There are restrictions on the units $u \in \mathcal{U}$ such that $k((t))/k((ut^{p^n}))$ is Galois extension:

Theorem 14. *If k is a perfect field of characteristic $p > 0$ and $k((t))/L$ is a Galois extension of dimension p^n, then there exists $u \in \mathcal{U}_{(p-1)p^{n-1}}$ such that $L = k((ut^{p^n}))$.*

Proof. Suppose $k((t))/k((ut^{p^n}))$ is a finite Galois extension. Then $[k((t)) : k((ut^{p^n}))] = p^n$ and thus G, the Galois group of this extension, is a finite p-group. Let us proceed by induction on n. For the base case, suppose $k((t))/k((ut^p))$ is a finite Galois extension. Then we may write $k((t)) = k((ut^p))(\alpha)$, where α is a root of the Artin–Schreier polynomial $X^p - X - f$, for some $f \in k((ut^p))$ with $v_t(f) = -mp$ and $\gcd(m, p) = 1$. (See Proposition 11.17 in [5].) For notational convenience, write $y = ut^p$ and $f = \frac{c}{y^m}$ with $c \in k[\![y]\!]^\times$. Now

$$\alpha^p - \alpha = \frac{c}{y^m} \quad \Rightarrow \quad \frac{1}{\alpha^p - \alpha} = c^{-1} y^m = \frac{\frac{1}{\alpha^p}}{1 - \frac{1}{\alpha^{p-1}}} = \frac{1}{\alpha^p}\left(\frac{1}{1 - \frac{1}{\alpha^{p-1}}}\right).$$

Write $\beta = \frac{1}{\alpha}$ and we can rewrite as

$$c^{-1} y^m = \beta^p\left(1 + \beta^{p-1} + \beta^{2p-2} + \cdots\right).$$

Since $v_t(\beta) = m$ there exists $w \in \mathcal{U}$ such that $\beta = wt^m$. Then

$$y^m = c\left(wt^m\right)^p\left(1 + \left(wt^m\right)^{p-1} + \left(wt^m\right)^{2p-2} + \cdots\right)$$

and we may take m-th roots everywhere to get

$$ut^p = y = c^{\frac{1}{m}} w^{\frac{p}{m}} t^p\left(1 + \left(wt^m\right)^{p-1} + \left(wt^m\right)^{2p-2} + \cdots\right)^{\frac{1}{m}}.$$

Thus $u \in k[\![ut^p]\!]^\times k[\![t^p]\!]^\times k[\![wt^{m(p-1)}]\!]^\times$ and so $u \in 1 + k[\![t]\!]t^{p-1}$.

Now for the inductive step. Suppose that $n > 0$ is given, and that the result is true for $n - 1$. G is a p-group, and so G contains a normal subgroup H of index p. Let E be the fixed field of H. Then $k((t))/E$ is a Galois extension of degree p^{n-1} and $E/k((ut^{p^n}))$ is Galois of degree p. By the induction hypothesis, there exists a unit $u_1 \in \mathcal{U}$ such that $v_t(u_1 - 1) \geqslant p^{n-2}(p-1)$ and $E = k((u_1 t^{p^{n-1}}))$. $E/k((ut^{p^n}))$ is Galois of degree p, so there exists a unit $u_2 \in k[\![u_1 t^{p^{n-1}}]\!]$ such that $\frac{1}{p^{n-1}} v_t(u_2 - 1) > p - 1$ and $k((ut^{p^n})) = k((u_2(u_1 t^{p^{n-1}})^p))$. Now $u_2(u_1 t^{p^{n-1}})^p = u_2 u_1^p t^{p^n}$ and $v_t(u_1^p - 1) = p v_t(u_1 - 1) \geqslant p p^{n-2}(p-1) = p^{n-1}(p-1)$ and $v_t(u_2 - 1) \geqslant p^{n-1}(p-1)$. Thus $v_t(u_2(u_1)^p - 1) \geqslant p^{n-1}(p-1)$ and $u_2 u_1^p$ is a unit in $k[\![t]\!]$. Note that the last inequality follows from the identity $ab - 1 = (a-1)(b-1) + (a-1) + (b-1)$. Thus we see that for any Galois extension $k((t))/L$ of degree p^n, there exists some $u \in \mathcal{U}_{(p-1)p^{n-1}}$ such that $L = k((ut^{p^n}))$. $\square$

4. Extended depth

For $\alpha \in K$ we have $\alpha = \sum_{i=-\infty}^{\infty} a_i t^i$ where $a_i \in k$ and $a_i = 0$ for all $i < N$ for some N depending on α. When convenient we will denote a_i, the i-th coefficient of α, by $[\alpha]_i$. The *support* of α is the set $\mathrm{Supp}(\alpha) = \{i\colon\ [\alpha]_i \neq 0\}$. We have, of course, $v(\alpha) = \inf(\mathrm{Supp}(\alpha))$.

In the study of $\mathrm{Aut}(K/k)$ the *depth* of a unit $u \in \mathcal{U}$ is defined to be $d(u) = v(u - u(0))$, where $u(0)$ is the nonzero zeroth coefficient of u. For $\sigma \in \mathrm{Aut}(K/k)$, $d(\sigma) = d(u_\sigma)$, where $\sigma(t) = u_\sigma t$. In this work we often consider $u_1t^{m_1} \in k((u_2t^{m_2}))$ for some $u_1, u_2 \in \mathcal{U}$ and try to estimate the depth of u_2 in terms of the depth of u_1. In order to get more precise relations, we introduce a related concept.

We define the *extended depth* of $\alpha \in K$ to be

$$e(\alpha) = \inf\bigl(\mathrm{Supp}(\alpha) - p\mathbb{Z}\bigr) \in \mathbb{Z} \cup \{\infty\}.$$

Note that $e(\alpha)$ is either ∞ or an integer not divisible by p. Of course for any $\alpha \in \mathcal{U}$ we have $e(\alpha) \geqslant d(\alpha)$ with equality if and only if $p \nmid d(\alpha)$. Similarly for $\sigma \in \mathcal{A}$ we define $e(\sigma)$ to be $e(u_\sigma)$ where $\sigma(t) = u_\sigma t$.

4.1. Extended depth of elements

The following lemma collects the basic properties of $e(\cdot)$ we will need.

Lemma 15. *Let $\alpha, \beta \in K$.*

1. *$e(\alpha) \geqslant v(\alpha)$ with equality if and only if $p \nmid v(\alpha)$ or $\alpha = 0$. (In particular e is continuous.)*
2. *$e(\alpha) = \infty$ if and only if $\alpha \in k((t^p))$. (Note $K^p \subseteq k((t^p))$.)*
3. *$e(\alpha + \beta) \geqslant \min(e(\alpha), e(\beta))$ with equality if $e(\alpha) \neq e(\beta)$.*
4. *If $\gamma \in k((t^p))$ then $e(\alpha + \gamma) = e(\alpha)$.*
5. *If $\gamma \in k((t^p))$ then $e(\alpha\gamma) = e(\alpha) + v(\gamma)$. (In particular if $u \in k[\![t^p]\!]^\times$ then $e(\alpha u) = e(\alpha)$.)*
6. *α can be written as $\alpha_0 + \gamma$ where $\alpha_0 \in K$, $\gamma \in k((t^p))$, $e(\alpha) = v(\alpha_0) = e(\alpha_0)$, and $v(\alpha) = \min(v(\alpha_0), v(\gamma))$.*

Proof. The proofs of 1. through 5. follow immediately from the definition of e. As for 6. we set $\alpha_0 = \sum_{i=-\infty}^{\infty} c_i t^i$ and $\gamma = \sum_{i=-\infty}^{\infty} d_i t^i$ where

$$c_i = \begin{cases} [\alpha]_i & \text{if } p \nmid i, \\ 0 & \text{if } p \mid i \end{cases} \quad \text{and} \quad d_i = \begin{cases} 0 & \text{if } p \nmid i, \\ [\alpha]_i & \text{if } p \mid i. \end{cases}$$

Then $\alpha = \alpha_0 + \gamma$ and the rest follows. $\square$

Proposition 16. *Suppose $\alpha, \beta \in \mathcal{U}$ and $e = \min(e(\alpha), e(\beta)) < \infty$. Then*

$$[\alpha\beta]_e = [\alpha]_e[\beta]_0 + [\beta]_e[\alpha]_0 \quad \textit{and} \quad e(\alpha\beta) \geqslant e$$

with equality if and only if $[\alpha\beta]_e \neq 0$.

Proof. Without loss of generality $e(\alpha) \leqslant e(\beta)$. So $e(\alpha) = e < \infty$ and $\alpha = at^e + r_1 + \gamma_1$ where $a = [\alpha]_e \neq 0$, $v(r_1) > e$, and $\gamma_1 \in k((t^p))$.

If $e(\beta) = \infty$ then $\beta \in k((t^p))$ so $\alpha\beta = a\beta t^e + r_1\beta + \gamma_1\beta$ where $v(r_1\beta) = v(r_1) > e$ and $[\alpha\beta]_e = [\alpha]_e[\beta]_0 + [\beta]_e[\alpha]_0 \neq 0$ as $[\beta]_e = 0$.

Now suppose $e(\beta) < \infty$. Then $\beta = bt^f + r_2 + \gamma_2$ where $f = e(\beta)$, $b = [\beta]_f \neq 0$, $v(r_2) > f$, and $\gamma_2 \in k((t^p))$. So

$$\begin{aligned} \alpha\beta &\equiv \bigl(at^e + \gamma_1\bigr)\bigl(bt^f + \gamma_2\bigr) \mod t^{e+1} \\ &\equiv abt^{e+f} + a\gamma_2 t^e + b\gamma_1 t^f + \gamma_1\gamma_2 \mod t^{e+1} \\ &\equiv a[\beta]_0 t^e + b[\alpha]_0 t^f + \gamma_1\gamma_2 \mod t^{e+1} \end{aligned}$$

remembering that $[\alpha]_0 = [\gamma_1]_0$ and $[\beta]_0 = [\gamma_2]_0$ as $\alpha, \beta \in \mathcal{U}$. Thus if $e = f$ we have $[\alpha\beta]_e = [\alpha]_e[\beta]_0 + [\beta]_e[\alpha]_0$, and if $e < f$ we have $[\alpha\beta]_e = [\alpha]_e[\beta]_0 = [\alpha]_e[\beta]_0 + [\beta]_e[\alpha]_0$ as $[\beta]_e = 0$. In either case $e(\alpha\beta) \geqslant e$ and the result follows. $\square$

Corollary 17. *If $\alpha \in \mathcal{U}$ and $e = e(\alpha) < \infty$ then*

$$\left[\alpha^m\right]_e = m[\alpha]_0^{m-1}[\alpha]_e \quad \textit{and} \quad e\left(\alpha^m\right) \geqslant e$$

with equality if and only if $p \nmid m$.

Theorem 18. *Suppose $u, w \in \mathcal{U}$ are such that $e(u) < \infty$ and $ut^{p^a} \in k((wt^{p^b}))$ for some $a \geqslant b \geqslant 1$. Then*

$$e(u) = \begin{cases} e(w) & \textit{if } a = b, \\ e(w) + mp^b & \textit{if } a > b \end{cases}$$

for some $m \geqslant 1$, $p \nmid m$. In particular, we have $e(w) \leqslant e(u)$.

Proof. Since $ut^{p^a} \in k((wt^{p^b}))$ we have $ut^{p^a} \in k[\![wt^{p^b}]\!]$ as ut^{p^a} has positive valuation. So $ut^{p^a} = \sum_{i=0}^{\infty} c_i (wt^{p^b})^i$ where $c_i \in k$. By valuation again $c_i = 0$ for all $0 \leqslant i < p^{a-b}$ and $c_{p^{a-b}} \neq 0$. Thus

$$ut^{p^a} = \sum_{i=p^{a-b}}^{\infty} c_i \left(wt^{p^b}\right)^i = \sum_{j=0}^{\infty} \tilde{c}_j w^{p^{a-b}+j} t^{p^a+jp^b}$$

where $\tilde{c}_0 \neq 0$ and so

$$u = \sum_{j=0}^{\infty} \tilde{c}_j w^{p^{a-b}+j} t^{jp^b}.$$

If $a - b > 0$ we have

$$\begin{aligned} e\left(\tilde{c}_j w^{p^{a-b}+j} t^{jp^b}\right) &= e\left(w^j\right) + v\left(\tilde{c}_j w^{p^{a-b}} t^{jp^b}\right) \\ &= e\left(w^j\right) + v(\tilde{c}_j) + jp^b \\ &= \begin{cases} e(w) + jp^b & \text{if } p \nmid j \text{ and } \tilde{c}_j \neq 0, \\ \infty & \text{otherwise.} \end{cases} \end{aligned}$$

Since $e(u) < \infty$ we must have $p \nmid j$ and $\tilde{c}_j \neq 0$ for at least one j and since for these indices the e-values are distinct we have $e(u) = e(w) + jp^b$ for the least j such that $p \nmid j$ and $\tilde{c}_j \neq 0$.

If $a - b = 0$ we have

$$\begin{aligned} e\left(\tilde{c}_j w^{1+j} t^{jp^b}\right) &= e\left(w^{1+j}\right) + v\left(\tilde{c}_j t^{jp^b}\right) \\ &= e\left(w^{1+j}\right) + v(\tilde{c}_j) + jp^b \\ &= \begin{cases} e(w) + jp^b & \text{if } p \nmid (1+j) \text{ and } \tilde{c}_j \neq 0, \\ \infty & \text{otherwise.} \end{cases} \end{aligned}$$

Since for $j = 0$ we have $p \nmid (1 + j)$ and $\tilde{c}_j \neq 0$ and since the finite e-values are distinct with their minimum occurring when $j = 0$ we have $e(u) = e(w)$. $\square$

Corollary 19. *If k is perfect and $K/k((ut^{p^n}))$ is Galois then*

$$e(u) \geqslant (p-1)p^{n-1}.$$

Proof. By Theorem 14 there exists a unit $u_0 \in \mathcal{U}_{(p-1)p^{n-1}}$ such that $k((ut^{p^n})) = k((u_0 t^{p^n}))$. Now $e(u_0) \geqslant (p-1)p^{n-1}$ and by Theorem 18 we have $e(u) = e(u_0)$. □

4.2. Extended depth of automorphisms

We first note that for all $\sigma \in \mathcal{A}_1$ we have $[u_\sigma]_0 = 1$.

Lemma 20. *Let $\alpha \in K$ and $\sigma, \tau \in \mathcal{A}$.*

1. $e(\alpha^\sigma) = e(\alpha)$.
2. *If $e = e(\alpha) < \infty$ then $[\alpha^\sigma]_e = [u_\sigma]_0^e [\alpha]_e$.*

Proof. For 1. we write $\alpha = \alpha_0 + \gamma$ where $\alpha_0 \in K$, $\gamma \in k((t^p))$, and $e(\alpha) = v(\alpha_0)$. Now $\alpha^\sigma = \alpha_0^\sigma + \gamma^\sigma$ and since $\gamma^\sigma \in k((t^p))$ we have $e(\alpha^\sigma) = e(\alpha_0^\sigma)$. Since $v(\alpha_0^\sigma) = v(\alpha_0) = e(\alpha)$ is not divisible by p we have $e(\alpha_0^\sigma) = v(\alpha_0^\sigma)$ and thus $e(\alpha^\sigma) = e(\alpha)$.

For 2. we write $\alpha = [\alpha]_e t^e + t^{e+1} f + \gamma$ where $f \in k[\![t]\!]$ and $\gamma \in k((t^p))$. Then $\alpha^\sigma = [\alpha]_e (u_\sigma t)^e + t^{e+1} g + \gamma^\sigma$ where $g \in k[\![t]\!]$. Thus $\alpha^\sigma = [\alpha]_e [u_\sigma]_0^e t^e + t^{e+1} h + \gamma^\sigma$ where $h \in k[\![t]\!]$ and the result follows. □

Proposition 21. *If $\sigma \in \mathcal{A}_1$ and $e = e(\sigma) < \infty$ then*

$$[u_{\sigma^m}]_e = m[u_\sigma]_e \quad \textit{and} \quad e\big(\sigma^m\big) \geqslant e$$

with equality if and only if $p \nmid m$.

Proof. The result is trivial if $m = 1$. Now suppose we have $[u_{\sigma^m}]_e = m[u_\sigma]_e$ and $e(\sigma^m) \geqslant e$ with equality if and only if $p \nmid m$. We have $u_{\sigma^{m+1}} = u_\sigma^{\sigma^m} u_\sigma$ and so, by Proposition 16, we have

$$\begin{aligned} [u_{\sigma^{m+1}}]_e &= \big[u_\sigma^{\sigma^m} u_\sigma\big]_e \\ &= \big[u_\sigma^{\sigma^m}\big]_e [u_\sigma]_0 + [u_\sigma]_e \big[u_\sigma^{\sigma^m}\big]_0 \\ &= m[u_\sigma]_e 1 + [u_\sigma]_e 1 \\ &= (m+1)[u_\sigma]_e \end{aligned}$$

and

$$e(u_{\sigma^{m+1}}) = e\big(u_\sigma^{\sigma^m} u_\sigma\big) \geqslant e$$

with equality if and only if $[u_{\sigma^{m+1}}]_e \neq 0$ if and only if $p \nmid m+1$. □

We define the *canonical unit* of a totally ramified Galois extension as follows: Suppose K/L is Galois and totally ramified with Galois group G of order n. Then $N_{K/L}(t) = \prod_{\sigma \in G} \sigma(t)$ has valuation n. Thus $N_{K/L}(t) = u_L t^n$ for some unit u_L. Note that $u_L = \prod_{\sigma \in G} u_\sigma$. We call this u_L the *canonical unit* for K/L. Since $k((u_L t^n)) \subseteq L$ and both have codimension n in K, we have $L = k((u_L t^n))$.

Theorem 22. *Suppose $K/k((ut^{p^n}))$ is Galois with Galois group G. Then $e(\sigma) \leqslant e(u)$ for all $\sigma \in G$, $\sigma \neq \mathrm{id}_K$.*

Proof. Let $\sigma \in G$, $\sigma \neq \mathrm{id}_K$. Suppose σ has order p^e with $e \geqslant 2$. Since $\sigma^{p^{e-1}}$ has order p and $e(\sigma) < e(\sigma^{p^{e-1}})$, it suffices to prove the result when σ has order p.

Let $\sigma \in G$ have order p. Let $e = e(\sigma)$. Let L be the fixed field of σ. Then $[K : L] = p$ so $L = k((u_L t^p))$ where u_L is the canonical unit for K/L. We have $u_L = 1u_\sigma \cdots u_{\sigma^{p-1}}$ and thus $e(u_L) \geqslant \min(e(u_\sigma), \ldots, e(u_{\sigma^{p-1}})) = e$ as $e = e(u_\sigma) = \cdots = e(u_{\sigma^{p-1}})$. Finally $e(u) \geqslant e(u_L)$ by Theorem 18 of the last section. Thus $e \leqslant e(u_L) \leqslant e(u)$ as desired. □

5. Canonical units of Galois extensions

We are now able to prove a theorem about the relationship between Galois extensions and their canonical units. We need two lemmas.

Lemma 23. *Let $k((t))/k((ut^{p^n}))$ be a finite Galois extension with Galois group G. Suppose that $\{d(\sigma) \mid \mathrm{id}_K \neq \sigma \in G\}$ is bounded above by N. Then the map*

$$G \longrightarrow \mathrm{Aut}\big(k[\![t]\!]/\big(t^{N+1}\big)\big) \quad \textit{given by } \sigma \mapsto \sigma^{[N]}$$

is an embedding. In particular, if $N > e(u)$ the above map is an embedding.

Proof. As in Section 2, the map $G \to \mathrm{Aut}(R_N)$ given by $\sigma \mapsto \sigma^{[N]}$ is a group homomorphism. We have $\sigma^{[N]} = \mathrm{id}_{R_N}$ if and only if $u_\sigma t \equiv t \bmod t^{N+1}$ if and only if $v(u_\sigma - 1) \geqslant N$ if and only if $d(\sigma) \geqslant N$. Thus if $N > d(\sigma)$ for all $\sigma \neq \mathrm{id}_K$, our map is an embedding.

Finally, if $N > e(u)$ then $N > e(\sigma) \geqslant d(\sigma)$ for all $\sigma \neq \mathrm{id}_K$ by Theorem 22 and our result follows. □

Lemma 24. *If $f, g \in \mathrm{Aut}(K/k)$ satisfy $v(f(t) - g(t)) > m$ then*

$$v\big(f(rt) - g(rt)\big) > m + v(r)$$

for any $r \in k[\![t]\!]$. In particular, if $h \in \mathrm{Aut}(K/k)$ as well we have

$$v\big(f\big(h(t)\big) - g\big(h(t)\big)\big) > m.$$

Proof. We have $f(tt^n) - g(tt^n) = f(t)^{n+1} - g(t)^{n+1} = (f(t) - g(t))z$ where $z = \sum_{i=0}^n f(t)^{n-i} g(t)^i$. Since f, g are continuous we have $v(f(t)) = v(g(t)) = 1$ and so $v(z) \geqslant n$. Thus $v(f(tt^n) - g(tt^n)) > m + n$.

Now $r = a_0 + a_1 t + a_2 t^2 + \cdots \in k[\![t]\!]$ and so

$$f(rt) - g(rt) = a_0\big(f(t) - g(t)\big) + a_1\big(f(tt) - g(tt)\big) + a_2\big(f\big(tt^2\big) - g\big(tt^2\big)\big) + \cdots$$

and the result follows. □

Theorem 25. *Let $L_1 = k((u_1 t^{p^n}))$ and $L_2 = k((u_2 t^{p^n}))$ be such that both K/L_1 and K/L_2 are Galois with Galois groups G_1 and G_2 respectively.*

If $v(u_1 - u_2) > (e(u_1) + 1)p^n$ then $G_1 \cong G_2$.

Proof. Let $N = v(u_1 - u_2) > (e(u_1) + 1)p^n$. Let $R_N = k[\![t]\!]/(t^{N+1})$ and let S be the image of $k[\![u_1 t^{p^n}]\!]$ in R_N. Since $N > e(u_1)$ we have $G_1 \hookrightarrow \overline{G_1} \leqslant \mathrm{Aut}_k(R_N)$ by Lemma 23. And since $v(u_1 - u_2) = N > e(u_1)$ we have $e(u_1) = e(u_2)$ and so $G_2 \hookrightarrow \overline{G_2} \leqslant \mathrm{Aut}_k(R_N)$ as well. Since $u_1 \equiv u_2 \bmod t^N$ we have $u_1 t^{p^n} \equiv u_2 t^{p^n} \bmod t^{N+1}$. Hence $\overline{G_2}$ fixes the elements of S because G_2 fixes the elements of $L_2 = k((u_2 t^{p^n}))$.

Let $f = \prod_{\rho \in G_1}(X - \rho(t))$. We see that f has degree p^n and coefficients in $k[\![u_1 t^{p^n}]\!]$. Let $M = \max\{v(\rho(t) - \mu(t))\colon \rho, \mu \in G_1,\ \rho \neq \mu\}$. We have $M > 0$. Since $v(\rho(t) - \mu(t)) = v((\mu^{-1}\rho)(t) - t)$ we have $M = \max\{v(\rho(t) - t)\colon \rho \in G_1,\ \rho \neq \mathrm{id}_{G_1}\}$. Finally since $\rho(t) - t = (u_\rho - 1)t$ we have $v(\rho(t) - t) \leqslant e(\rho) + 1 \leqslant e(u_1) + 1$ for $\rho \neq \mathrm{id}_{G_1}$ by Theorem 22. Thus $M \leqslant e(u_1) + 1$.

Now for any $\sigma \in G_2$ we have

$$f\big(\sigma(t)\big) \equiv \sigma\big(f(t)\big) \equiv \sigma(0) \equiv 0 \mod t^{N+1}$$

and therefore

$$\sum_{\rho\in G_1} v\big(\sigma(t)-\rho(t)\big) = v\bigg(\prod_{\rho\in G_1}\big(\sigma(t)-\rho(t)\big)\bigg) > N.$$

Since $N > (e(u_1)+1)p^n$ we have $v(\sigma(t)-\rho(t)) > e(u_1)+1 \geqslant M$ for at least one $\rho \in G_1$ and since $M = \max\{v(\rho(t)-\mu(t))\colon\ \rho,\mu \in G_1,\ \rho \neq \mu\}$ this ρ is unique. That is, for each $\sigma \in G_2$ there is a unique $\tilde{\sigma} \in G_1$ such that $v(\sigma(t)-\tilde{\sigma}(t)) > e(u_1)+1$.

We have

$$\sigma\tau(t) - \tilde{\sigma}\tilde{\tau}(t) = \big[\sigma\tau(t) - \tilde{\sigma}\tau(t)\big] + \big[\tilde{\sigma}\tau(t) - \tilde{\sigma}\tilde{\tau}(t)\big].$$

Since $\tau(t) = u_\tau t$ and $v(\sigma(t)-\tilde{\sigma}(t)) > e(u_1)+1$ we have $v(\sigma\tau(t)-\tilde{\sigma}\tau(t)) > e(u_1)+1$ by Lemma 24. Since $\tilde{\sigma}$ is continuous and $v(\tau(t)-\tilde{\tau}(t)) > e(u_1)+1$ we have $v(\tilde{\sigma}\tau(t)-\tilde{\sigma}\tilde{\tau}(t)) > e(u_1)+1$ as well. Thus $v(\sigma\tau(t)-\tilde{\sigma}\tilde{\tau}(t)) > e(u_1)+1$ and $\tilde{\sigma}\tilde{\tau} \in G_1$ so $\widetilde{\sigma\tau} = \tilde{\sigma}\tilde{\tau}$.

Thus the map $G_2 \to G_1$ given by $\sigma \mapsto \tilde{\sigma}$ is a group homomorphism. Now $\tilde{\sigma} = \mathrm{id}_{G_1}$ implies $v(\sigma(t)-t) > e(u_1)+1$. Since $e(\sigma)+1 \geqslant v(\sigma(t)-t)$ we have $e(\sigma) > e(u_1)$ and therefore $\sigma = \mathrm{id}_{G_2}$ by Theorem 22. Hence $G_2 \to G_1$ given by $\sigma \mapsto \tilde{\sigma}$ is an injective group homomorphism between two groups of order p^n, so $G_1 \cong G_2$. $\square$

Corollary 26. *If $K/k((ut^{p^n}))$ is Galois then the Galois group is determined by the first $(e(u)+1)p^n$ terms of u.*

6. An example

Again k is a field of characteristic $p \geqslant 0$ and $K = k((t))$.

For each $\lambda \in k$ we define $\phi_\lambda : K \to K$ given by $t \mapsto \frac{1}{1+\lambda t}t$. So $\phi_\lambda \in \mathcal{A}_1$ for each $\lambda \in k$. An easy calculation shows that $\phi_{\lambda_1} \circ \phi_{\lambda_2} = \phi_{\lambda_1+\lambda_2}$. Therefore $k^+ \to \mathcal{A}_1$ given by $\lambda \mapsto \phi_\lambda$ is a group embedding. Thus if $p > 0$ we have a family of convenient elements of order p.

Unfortunately these are the only easily described elements of finite order in $\mathcal{A}_1$: Suppose $\phi \in \mathcal{A}_1$ has order d and is given by $t \mapsto \frac{f}{g}t$ where $f, g \in k[t]$. Then $k(t) \supseteq k(\phi(t)) \supseteq \cdots \supseteq k(\phi^d(t)) = k(t)$ and so $k(t) = k(\phi(t)) = k(\frac{ft}{g})$. Thus $1 = [k(t) : k(\frac{ft}{g})] = \max(\deg(ft), \deg(g))$. It follows that $\deg(f) = 0$ and $\deg(g) \leqslant 1$. Since $\phi \in \mathcal{A}_1$ we have $\phi(t) = \frac{1}{1+\lambda t}t$ for some $\lambda \in k$.

Now suppose $p > 0$ and $\lambda \in k^\times$. So ϕ_λ has order p. Let L be the fixed field of $\langle\phi_\lambda\rangle$. Then $L = k((ut^p))$ where

$$ut^p = N_{K/L}(t) = \prod_{i=0}^{p-1}\phi^i(t) = \prod_{i=0}^{p-1}\frac{1}{1+i\lambda t}t = \left(\prod_{i=1}^{p-1}(1+i\lambda t)\right)^{-1} t^p.$$

Now $\prod_{i=1}^{p-1}(1+i\lambda t) = \prod_{i=1}^{p-1} i(\lambda t + \frac{1}{i}) = -(\lambda^{p-1}t^{p-1} - 1)$ by Wilson's theorem and the identity $X^{p-1} - 1 = \prod_{j=1}^{p-1}(X-j)$. Thus

$$u = \frac{1}{1-\lambda^{p-1}t^{p-1}}$$

is the canonical unit for a Galois K/L with Galois group cyclic of order p. Similarly but more tediously, if k has at least p^n elements we could construct the canonical unit for a Galois K/L with Galois group elementary abelian of order p^n.

7. Some questions

We have provided a few examples of the relations between the Galois group of $k((t))/k((ut^{p^n}))$ and the structure of the unit u. There are many questions which remain. For example:

1. How easily can one determine interesting information about G directly from the coefficients of u? Is there a way of seeing when G is cyclic, abelian, etc.?
2. Conversely, can one begin with a p-group G and construct the sequence of coefficients of u?

References

[1] R. Camina, Subgroups of the Nottingham group, J. Algebra 196 (1997) 101–113.
[2] D.L. Johnson, The group of formal power series under substitution, J. Aust. Math. Soc. (Ser. A) 45 (1988) 296–302.
[3] A. Bevelacqua, M. Motley, Finite codimension subfields of a field complete with respect to a real valuation, Comm. Algebra 34 (1) (2006) 335–345.
[4] S. Shatz, Profinite Groups, Arithmetic, and Geometry, Ann. of Math. Stud., Princeton University Press, 1972.
[5] D. Bump, Algebraic Geometry, World Scientific Publishing, 1998.