Journal of Pure and Applied Algebra 214 (2010) 565–573

Contents lists available at ScienceDirect

Journal of Pure and Applied Algebra

journal homepage: www.elsevier.com/locate/jpaa

Wild tame-by-cyclic extensions

Andrew Obus [a,*], Rachel Pries [b]

[a] Department of Mathematics, University of Pennsylvania, 209 S. 33rd Street, Philadelphia, PA 19104, USA
[b] Department of Mathematics, Colorado State University, 101 Weber Building, Fort Collins, CO 80523, USA

ARTICLE INFO

Article history:
Received 1 August 2008
Received in revised form 3 March 2009
Available online 7 July 2009
Communicated by J. Walker

MSC:
14H30
11S15

ABSTRACT

Suppose G is a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ where p is prime and m is relatively prime to p. Suppose K is a complete discrete valuation field of characteristic $p > 0$ with algebraically closed residue field. The main result states necessary and sufficient conditions on the ramification filtrations that occur for wildly ramified G-Galois extensions of K. In addition, we prove that there exists a parameter space for G-Galois extensions of K with given ramification filtration, and we calculate its dimension in terms of the ramification filtration. We provide explicit equations for wild cyclic extensions of K of degree p^3.

1. Introduction

This paper is about wildly ramified Galois extensions of a complete discrete valuation field $k((t))$ where k is an algebraically closed field of characteristic $p > 0$. We prove that the lower jumps of the ramification filtration of a Galois extension of $k((t))$ with group $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ are all congruent modulo m, Proposition 4.2. We also prove that one can dominate a given Galois extension having group $\mathbb{Z}/p^{n-1} \rtimes \mathbb{Z}/m$ by a Galois extension having group $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$, with control over the last jump in the ramification filtration, Proposition 5.1. Together with well-known results about ramification filtrations of Galois extensions with group $\mathbb{Z}/p^n$ [1], this yields (see Theorem 5.2):

Theorem 1.1. *Let G be a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ where $p \nmid m$. Let $\sigma \in G$ have order p^n and let $m' = |\mathrm{Cent}_G(\sigma)|/p^n$. A sequence $u_1 \leq \cdots \leq u_n$ of rational numbers occurs as the set of positive breaks in the upper numbering of the ramification filtration of a G-Galois extension of $k((t))$ if and only if:*

(a) $u_i \in \frac{1}{m}\mathbb{N}$ *for* $1 \leq i \leq n$;
(b) $\gcd(m, mu_1) = m'$;
(c) $p \nmid mu_1$ *and, for* $1 < i \leq n$, *either* $u_i = pu_{i-1}$ *or both* $u_i > pu_{i-1}$ *and* $p \nmid mu_i$;
(d) *and* $mu_i \equiv mu_1 \bmod m$ *for* $1 \leq i \leq n$.

In the first author's doctoral thesis, Theorem 1.1 yields restrictions on the stable reduction of certain branched covers of the projective line.

Our other main result, Theorem 5.6, states that, given a group G and a ramification filtration η satisfying conditions (a)–(d) as in Theorem 1.1, there exists a parameter space $\mathcal{M}_\eta$ whose k-points are in natural bijection with isomorphism classes of G-Galois extensions of $k((t))$ having ramification filtration η. We calculate the dimension of $\mathcal{M}_\eta$ in terms of the upper jumps of η.

* Corresponding author.
E-mail addresses: obusa@math.upenn.edu (A. Obus), pries@math.colostate.edu (R. Pries).

0022-4049/$ – see front matter © 2009 Elsevier B.V. All rights reserved.
doi:10.1016/j.jpaa.2009.06.017

Here is the paper's outline: in Section 2 we introduce the framework of study, including ramification filtrations and field theory; Section 3 contains several structural descriptions of cyclic p-group extensions; in Section 4, we prove results about tame actions on cyclic extensions; and the main results on ramification filtrations and parameter spaces for G-Galois extensions appear in Section 5.

Our original motivation for this topic was to find explicit equations for $\mathbb{Z}/p^3$-Galois extensions of $k((t))$, see Section 6. Such equations are useful and are difficult to find in the literature. For example, in [2, II, Lemma 5.1], the authors use equations for $\mathbb{Z}/p^2$-Galois extensions in order to prove a case of Oort's Conjecture, namely, that every $\mathbb{Z}/p^2$-Galois extension of $k((t))$ lifts to characteristic 0 [2, Thm. 2].

Similar results for elementary abelian p-group extensions are in [3].

2. Framework of study

This section contains background on extensions of complete discrete valuation fields and ramification filtrations and introduces the situation studied in this paper, in which the Galois group is a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$.

2.1. Extensions of complete discrete valuation fields

Let k be an algebraically closed field of characteristic $p > 0$. We fix a compatible system of roots of unity of k. In particular, this fixes a primitive mth root of unity ζ in k. Let R be an equal characteristic complete discrete valuation ring with residue field k and fraction field K. Then $R \simeq k[\![t]\!]$ and $K \simeq k((t))$ for some uniformizing parameter t.

Suppose L/K is a separable Galois field extension with group G. Let S be the integral closure of R in L. Then S/R is a Galois extension of rings with group G which is totally ramified over the prime ideal (t).

This type of field extension arises in the following context. Suppose $\phi : Y \to X$ is a Galois cover of smooth k-curves. Suppose $y \in Y$ is a ramified point with inertia group G. Consider the complete local rings $S = \hat{\mathcal{O}}_{Y,y}$ and $R = \hat{\mathcal{O}}_{X,\phi(y)}$. Then S/R is a Galois extension of rings with group G which is totally ramified over the unique valuation of R as described in the preceding paragraph.

For a Galois extension L/K as above, the group G is a semi-direct product of the form $P \rtimes \mathbb{Z}/m$ where P is a p-group and $p \nmid m$ [4, IV, Cor. 4]. Throughout the paper, we assume that the subgroup P is cyclic.

2.2. Subgroups of a semi-direct product

Suppose G is a semi-direct product of the form $P \rtimes \mathbb{Z}/m$ where $P \simeq \mathbb{Z}/p^n$ and $p \nmid m$. Let σ be a chosen generator of P. Let c be a chosen element of order m in G and let $M = \langle c \rangle$. Let $m' = |\mathrm{Cent}_G(\sigma)|/p^n$. In other words, $m' = \#\{g \in M \mid g\sigma g^{-1} = \sigma\}$.

For $0 \leq i \leq n$, the element $\sigma_i := \sigma^{p^i}$ has order p^{n-i} and $H_i := \langle \sigma_i \rangle$ is the unique subgroup of order p^{n-i} in G. Then $\{\mathrm{id}\} = H_n \subset H_{n-1} \subset \cdots \subset H_0 = P$.

The semi-direct product is determined by the conjugation action of M on P. Since $c\sigma c^{-1}$ also generates P, then $c\sigma c^{-1} = \sigma^{\alpha'}$ for some integer α' such that $1 \leq \alpha' < p^n$ and $p \nmid \alpha'$. The action of c stabilizes H_i. Let $J_i := (H_{i-1}/H_i) \rtimes M$.

Lemma 2.1. (i) *The value of α' does not depend on the choice of generator of P;*
(ii) *The value of α' depends on the choice of generator of M as follows; if $c_0 = c^\beta$ for some integer β, then $\alpha'_0 \equiv (\alpha')^\beta \bmod p^n$.*

Proof. (i) If $\tau = \sigma^\gamma$, then $c\tau c^{-1} = (c\sigma c^{-1})^\gamma = (\sigma^{\alpha'})^\gamma = \tau^{\alpha'}$.
(ii) By induction, $c^i \sigma c^{-i} = \sigma^{(\alpha')^i}$. Thus $c_0 \sigma c_0^{-1} = \sigma^{\alpha'_0}$. □

Lemma 2.2. *The groups J_i are canonically isomorphic for $1 \leq i \leq n$.*

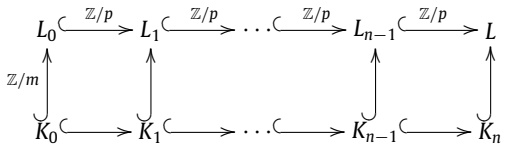
Proof. The groups J_i are semi-direct products of the form $\mathbb{Z}/p \rtimes \mathbb{Z}/m$. Thus it suffices to show that the action of c on the equivalence class of σ_{i-1} modulo $\langle \sigma_i \rangle$ is the same for $1 \leq i \leq n$. Note that $c\sigma^p c^{-1} = (\sigma^p)^{\alpha'}$. Thus $c\sigma_i c^{-1} = \sigma_i^{\alpha'}$. □

The residue of α' modulo p can be canonically identified with an element $\alpha \in \mathbb{F}_p^*$. Also m/m' is the order of α in $\mathbb{F}_p^*$.

2.3. Towers of fields

Suppose L/K is a separable Galois extension whose group G is of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ with $p \nmid m$. We fix an identification of $\mathrm{Aut}(L/K)$ with G and indicate this by writing that L/K is a *G-Galois extension*.

Consider the fixed fields $L_i = L^{H_i}$ and $K_i = L^{H_i \rtimes M}$ for $0 \leq i \leq n$. So, $L_n = L$ and $K_0 = K$. Let v_i be the natural valuation on L_i. Let Θ_i be the integral closure of R in L_i. Then L/L_i is an H_i-Galois extension and L_i/L_0 is a P/H_i-Galois extension. Also L_i/K_{i-1} is a J_i-Galois extension. This yields a tower of fields:



By Kummer theory, there exists $x \in L_0$ such that $L_0 \simeq K[x]/(x^m - 1/t)$. After choosing $c \in G$ such that $c(x) = \zeta x$, one can determine the values of α' and α for the extension L/K.

2.4. Ramification filtrations

Here is a brief review of the theory of ramification filtrations from [4, IV]. Consider the natural valuation $v = v_n$ on L and a uniformizing parameter $\pi \in L$. For $r \in \mathbb{N}$, let I_r be the rth ramification group in the lower numbering for the extension L/K. In other words, I_r is the normal subgroup of all $g \in G$ such that $v(g(\pi) - \pi) \geq r + 1$.

The ramification filtration is important because it determines the degree δ of the different of S/R. Namely, by [4, IV, Prop. 4], $\delta = \sum_{r \geq 0}(|I_r| - 1)$. If $\phi : Y \to X$ is a cover of smooth projective connected k-curves, the genus of Y can be found using the Riemann–Hurwitz formula [5, IV, Cor. 2.4] and this formula relies on the degree of the different at each ramification point of ϕ.

Let $g \in G$ with $g \neq 1$. The *lower jump* for g is the non-negative integer j so that $v(g(\pi) - \pi) = j + 1$. Then $g \in I_j$ and $g \notin I_{j+1}$. By [4, IV, Prop. 11], $p \nmid j$ for any positive lower jump j. If $|P| = p^n$, then there are n positive indices $j_1 \leq \cdots \leq j_n$ at which there is a break in the ramification filtration in the lower numbering, which are called the *lower jumps* of L/K.

There is also a ramification filtration I^ℓ in the upper numbering. The *upper jumps* of L/K are the positive breaks $u_1 \leq \cdots \leq u_n$ in the ramification filtration in the upper numbering. The lower numbering is stable for subextensions [4, IV, Prop. 2] and the upper numbering is stable for quotients [4, IV, Prop. 14]. Using Herbrand's formula [4, IV, Section 3], one can translate between the two ramification filtrations: letting $j_0 = u_0 = 0$, then $u_i - u_{i-1} = (j_i - j_{i-1})/p^{i-1}m$ for $1 \leq i \leq n$.

3. Wild cyclic extensions

In this section, we describe the equations and ramification filtration of the $\mathbb{Z}/p^n$-Galois subextension L/L_0. The material in this section is mostly known, but it is all necessary for later results in the paper.

3.1. Cyclic towers of Artin–Schreier extensions

Lemma 3.1. *The* ith *lower jump* j_i *of* L/K *equals the lower jump of* L_i/L_{i-1}.

Proof. The ith lower jump j_i of L/K is the lower jump of the automorphism σ_{i-1}. This is the same as the lower jump of σ_{i-1} for the extension L/L_{i-1} by [4, IV, Prop. 2]. Since this is the smallest lower jump for the extension L/L_{i-1}, it also equals the upper jump of σ_{i-1} for L/L_{i-1}. By [4, IV, Prop. 14], this is then the same as the upper jump, and thus the lower jump, of L_i/L_{i-1}. □

3.2. Witt Vectors and p-power cyclic extensions

We recall some Witt vector theory. Let $\wp$ be the operation Fr − Id on Witt vectors, where Fr denotes Frobenius. An element a of a field F of characteristic p is a *$\wp$th power* in F if the polynomial $z^p - z - a$ has a root in F.

By [6, p. 331, Ex. 50], every Galois extension of $L_0 \cong k((x^{-1}))$ with group $\mathbb{Z}/p^n$ has Witt vector equations

$$(y_1^p, \ldots, y_n^p) = (y_1, \ldots, y_n) +'(x_1, \ldots, x_n). \tag{1}$$

where $x_i \in L_0$ for $1 \leq i \leq n$ such that x_1 is not a $\wp$th power in L_0 and where $+'$ denotes addition of Witt vectors: Moreover, there is a generator τ of $\mathbb{Z}/p^n$ such that the action of τ on Witt vectors is

$$\tau(y_1, \ldots, y_n) = (y_1, \ldots, y_n) +'(1, 0, \ldots, 0). \tag{2}$$

Modifying $(x_1, \ldots, x_n)$ by an element $w \in W^n(L_0)$, where W^n is the nth truncation of the Witt vectors, changes the isomorphism class of the extension precisely when $w \notin \wp(W^n(L_0))$. Thus, since k is algebraically closed, one can choose $(x_1, \ldots, x_n)$ to be in *standard form*, i.e., $x_i \in k[x]$ and either $x_i = 0$ or x_i has no exponent divisible by p.

To make (1) more explicit, for $0 \leq i \leq n-1$, let $W_i = \sum_{d=0}^{i} p^d X_{d+1}^{p^{i-d}}$ be the ith Witt polynomial, [4, II, Section 6]. Define $S_i \in \mathbb{Z}[X_1, \ldots, X_{i+1}, Y_1, \ldots, Y_{i+1}]$ to be the unique formal polynomial such that

$$W_i(X_1, \ldots, X_{i+1}) + W_i(Y_1, \ldots, Y_{i+1}) = W_i(S_0(X_1, Y_1), S_1(X_1, X_2, Y_1, Y_2), \ldots, S_i(X_1, \ldots, X_{i+1}, Y_1, \ldots Y_{i+1})).$$

The indexing of these variables is shifted by one from that of [4, II, Section 6] in order to be more consistent with notation in this paper. By [4, II, Thm. 6], the S_i are well defined and have integer coefficients.

Lemma 3.2. *In* $\mathbb{Z}[X_1, \ldots, X_i, Y_1, \ldots, Y_i]$,

$$S_{i-1}(X_1, \ldots, X_i, Y_1, \ldots, Y_i) = X_i + Y_i + \sum_{d=1}^{i-1} \frac{1}{p^{i-d}}(X_d^{p^{i-d}} + Y_d^{p^{i-d}} - S_{d-1}^{p^{i-d}})$$

and the degree of every monomial of S_{i-1} *is congruent to one modulo* $p-1$.

Proof. The equation follows from $\sum_{d=0}^{i-1} p^d S_d^{p^{i-1-d}} = \sum_{d=0}^{i-1} p^d (X_{d+1}^{p^{i-1-d}} + Y_{d+1}^{p^{i-1-d}})$ (see [1, Footnote 4]) and the statement about degrees from induction. □

For $1 \le i \le n$, let $\bar{S}_{i-1} \in \mathbb{F}_p[X_1, \ldots, X_i, Y_1, \ldots, Y_i]$ be the reduction of S_{i-1} modulo p and let $f_i(Y_1, \ldots, Y_{i-1}, X_1, \ldots X_i) = \bar{S}_{i-1} - Y_i$. Then $f_i = X_i + g_i$ where $g_i \in \mathbb{F}_p[X_1, \ldots, X_{i-1}, Y_1, \ldots, Y_{i-1}]$ is a polynomial whose terms each have degree congruent to one modulo $p-1$. The meaning of (1) is that a Galois extension with group $\mathbb{Z}/p^n$ has equations $y_i^p - y_i = f_i(y_1, \ldots, y_{i-1}, x_1, \ldots x_i)$.

Lemma 3.3. *Let* L/L_0 *be a* $\mathbb{Z}/p^n$*-Galois extension and* σ *a generator of* $\mathbb{Z}/p^n$*. There exist* $x_i \in L_0$ *and* $y_i \in L$ *for* $1 \le i \le n$ *such that* L/L_0 *is isomorphic to the* $\langle\sigma\rangle$*-Galois extension with Witt vector equations and Galois action*

$$(y_1^p, \ldots, y_n^p) = (y_1, \ldots, y_n) +'(x_1, \ldots, x_n)$$
$$\sigma(y_1, \ldots, y_n) = (y_1, \ldots, y_n) +'(1, 0, \ldots, 0).$$

Furthermore, there is a unique choice for $(x_1, \ldots, x_n)$ *in standard form.*

Proof. There exist $x_i \in L_0$ and $y_i \in L$ and a generator τ of $\mathbb{Z}/p^n$ such that L/L_0 has Witt vector Eq. (1) and Galois action (2). Now $\sigma = \tau^b$ for some $b \in (\mathbb{Z}/p^n)^*$. Then $\sigma(y_1, \ldots, y_n) = (y_1, \ldots, y_n) +' b(1, 0, \ldots, 0)$. Since b is invertible in $\mathbb{Z}/p^n \cong W^n(\mathbb{Z}/p) \subset W^n(L_0)$, one can replace $(y_1, \ldots, y_n)$ and $(x_1, \ldots, x_n)$ with the Witt vectors $\frac{1}{b}(y_1, \ldots, y_n)$ and $\frac{1}{b}(x_1, \ldots, x_n)$. Since Fr is a ring homomorphism [6, p. 331, Ex. 48], the extension L/L_0 still has Witt vector Eq. (1) and now $\sigma(y_1, \ldots, y_n) = (y_1, \ldots, y_n) +'(1, 0, \ldots, 0)$.

By a generalization of [7, Lemma 2.1.5], there is a unique choice of $(x_1, \ldots, x_n)$ in standard form compatible with the restriction on the Galois action. □

3.3. Ramification filtrations for cyclic p-group extensions

The ramification filtration of a $\mathbb{Z}/p^n$-Galois extension is completely determined by either its lower or upper jumps, which in turn can be determined by the Witt vector equation.

Lemma 3.4. *Let* L/L_0 *be a* $\mathbb{Z}/p^n$*-Galois extension with Witt vector* $(x_1, \ldots, x_n)$ *in Eq. (1) in standard form. Let* $u = \max\{-p^{n-i} v_0(x_i)\}_{i=1}^n$*. Then* u *is the last upper jump of* L/L_0.

Proof. This follows from [8, Thm. 1.1]; see also [9, Prop. 4.2(1)]. □

We retrieve the following classical result.

Lemma 3.5. *A sequence of positive integers* $w_1 \le \cdots \le w_n$ *occurs as the set of upper jumps of a* $\mathbb{Z}/p^n$*-Galois extension of* L_0 *if and only if* $p \nmid w_1$ *and, for* $1 < i \le n$*, either* $w_i = p w_{i-1}$ *or both* $w_i > p w_{i-1}$ *and* $p \nmid w_i$.

Proof. The result, originally found in [1], follows from Lemma 3.4; see also [10, Lemma 19]. □

The following lemma will be used to compare the upper jumps of the G-Galois extension L/K and the $\mathbb{Z}/p^n$-Galois extension L/L_0.

Lemma 3.6. *Suppose* L/K *has upper jumps* $u_1 \le \cdots \le u_n$*. Then* L/L_0 *has upper jumps* $w_1 \le \cdots \le w_n$ *where* $w_i = m u_i$ *for* $1 \le i \le n$.

Proof. By [4, IV, Prop. 2], the lower jumps of L/L_0 equal the lower jumps $j_1 \le \cdots \le j_n$ of L/K. Herbrand's formula [4, IV, Section 3] implies that $u_i - u_{i-1} = (j_i - j_{i-1})/p^{i-1}m$ and that $w_i - w_{i-1} = (j_i - j_{i-1})/p^{i-1}$ for $1 \le i \le n$. □

4. Tame-by-cyclic extensions

Suppose L/K is a separable G-Galois field extension as in Section 2.2–3.1. In this section, we find necessary conditions on the ramification filtrations and equations arising from the $\mathbb{Z}/m$-Galois action on L.

4.1. The case of Galois extensions with group $\mathbb{Z}/p \rtimes \mathbb{Z}/m$

Lemma 4.1. *Consider the J_1-Galois extension L_1/K with equations $x^m = 1/t$ and $y_1^p - y_1 = x_1$ and Galois action $c(x) = \zeta x$ and $\sigma(y_1) = y_1 + 1$.*

(i) *The lower jump j of L_1/L_0 satisfies $m' = \gcd(m, j)$.*
(ii) *Also $m|j(p-1)$. In particular, $j \equiv jp^r \bmod m$ for any $r \in \mathbb{N}$.*
(iii) *Also $c(y_1) = \alpha^{-1} y_1 = \zeta^j y_1$.*

Proof. (i) This follows from [4, IV, Prop. 9], see also [7, Lemma 1.4.1(iv)].
(ii) The conjugation action of $\mathbb{Z}/m$ on $\mathbb{Z}/p$ gives a homomorphism $\nu : \mathbb{Z}/m \to \mathrm{Aut}(\mathbb{Z}/p)$. By definition, $\mathrm{Im}(\nu)$ has order m/m' and $\mathrm{Ker}(\nu) = \langle c^{m/m'} \rangle$. Thus $m|m'(p-1)$. By part (i), $m' = \gcd(m, j)$, so $m|j(p-1)$.
(iii) [7, Lemma 1.4.1(ii)–(iii)]. □

4.2. A congruence condition on the ramification filtration

Proposition 4.2. (i) *The lower jumps in the ramification filtration of the P-Galois extension L/L_0 are all congruent modulo m.*
(ii) *The upper jumps in the ramification filtration of the P-Galois extension L/L_0 are all congruent modulo m.*

Proof. (i) The ith lower jump of L/L_0 is j_i by [4, IV, Prop. 2]. Let π be a uniformizer of Θ_n and let $u = c(\pi)/\pi \in \Theta_n^*$. In the notation of [4, IV, Prop. 7], recall that θ_0 is a map from I_0/I_1 to k^* and θ_j is a map from I_j/I_{j+1} to k for $j \geq 1$. Then u equals $\theta_0(c) \in k^*$. The order of u is m by [4, IV, Prop. 7]. By the proof of Lemma 2.2, $c\sigma_{i-1}c^{-1} = \sigma_{i-1}^{\alpha'}$ for $1 \leq i \leq n$. Since σ_{i-1} generates $H_{i-1}/H_i = I_{j_i}/I_{j_i+1}$, [4, IV, Prop. 9] shows that $\theta_{j_i}(\sigma_{i-1}^{\alpha'}) = u^{j_i}\theta_{j_i}(\sigma_{i-1})$ for $1 \leq i \leq n$. Thus $u^{j_i} = \alpha \in k^*$ for $1 \leq i \leq n$ and so $j_1 \equiv \cdots \equiv j_n \bmod m$.
(ii) Let $w_1 \leq \cdots \leq w_n$ be the upper jumps of the P-Galois extension L/L_0. Since P is abelian, the Hasse–Arf Theorem implies that $w_i \in \mathbb{N}$. By Herbrand's formula, $w_i - w_{i-1} = (j_i - j_{i-1})/p^{i-1}$. Thus $w_i - w_{i-1} \equiv 0 \bmod m$ by part (i). □

Class field theory approach: If k is instead a finite field, here is a different proof of Proposition 4.2 which uses class field theory.

Second proof of Proposition 4.2. The G-Galois extension L/K dominates the $\langle c \rangle$-Galois extension L_0/K where $L_0 \simeq k((x^{-1}))$, $x^m = 1/t$, and $c(x) = \zeta x$. Let L/L_0 be the P-Galois subextension, which has upper jumps $w_1 \leq \cdots \leq w_n$ where $w_i = mu_i$ by Lemma 3.6. Thus the upper ramification group I^ℓ of L/L_0 equals H_i if $w_i < \ell \leq w_{i+1}$.

Let $Q = (x^{-1})$ be the maximal ideal of $k[\![x^{-1}]\!]$. Consider the unit groups $U^d = 1 + Q^d$ of $k[\![x^{-1}]\!]$ [4, IV.2]. By [4, IV, Prop. 6], U^d/U^{d+1} is canonically isomorphic to Q^d/Q^{d+1}. Now, Q^d carries a natural $\langle c \rangle$-module structure where $c((x^{-1})^d) = \zeta_m^{-d}(x^{-1})^d$. Thus U^d/U^{d+1} carries a natural structure as a $\langle c \rangle$-module, and this structure depends on the congruence class of d modulo m.

By [4, XV.2, Cor. 3 & pg. 229], there is a reciprocity isomorphism $\omega : L_0^*/NL^* \to P$ and thus there are isomorphisms $\omega_n : U^d/(U^{d+1}NU_L^{\psi(d)}) \to I^d/I^{d+1}$. Here $N : L \to L_0$ is the norm map and ψ is Herbrand's function. In particular, taking $d = w_i$, then $U^{w_i}/(U^{w_i+1}NU_L^{\psi(w_i)}) = H_{i-1}/H_i$.

Now H_{i-1}/H_i has a $\langle c \rangle$-module structure and this $\langle c \rangle$-module structure is independent of i by Lemma 2.2. After pulling back by ω, this implies that the $\langle c \rangle$-module structure of $U^{w_i}/(U^{w_i+1}NU_L^{\psi(w_i)})$ and thus of U^{w_i} is independent of i. Thus $\zeta_m^{-w_i}$ is independent of i and so $w_i \equiv w_1 \bmod m$.

The lower jumps are also congruent modulo m by Herbrand's formula. □

At this point, one can prove that the conditions in Theorem 1.1 are necessary; we will postpone this until Section 5.2.

4.3. Actions and isomorphisms

This section contains two results that will be needed in Section 5.

Proposition 4.3. *Suppose $L_0 \simeq K[x]/(x^m - 1/t)$ and $c(x) = \zeta x$. Suppose L/L_0 is a P-Galois extension with Witt vector Eq. (1), Galois action (2), and first lower jump j such that $\zeta^j = \alpha^{-1}$. Then L/K is a G-Galois extension if and only if $c(x_i) = \zeta^j x_i$ and $c(y_i) = \zeta^j y_i$ for $1 \leq i \leq n$.*

Proof. Suppose L/K is a G-Galois extension. Then L_1/K is a J_1-Galois extension. By Lemma 4.1(iii), $c(y_1)/y_1 = \alpha^{-1} = \zeta^j$. Since $y_1^p - y_1 = x_1$, this implies that $c(x_1) = \zeta^j x_1$. As an inductive hypothesis, suppose that $c(x_i) = \zeta^j x_i$ and $c(y_i) = \zeta^j y_i$ for $1 \leq i \leq n-1$.

Now L_n/K_{n-1} is a J_n-Galois extension of discrete valuation fields and J_n and J_1 are canonically isomorphic by Lemma 2.2. In other words, the value of α for $\mathrm{Aut}(L_n/K_{n-1})$ is the same as for $\mathrm{Aut}(L_1/K)$. By Kummer theory, there exists a uniformizer π_{n-1} of L_{n-1} such that c acts on π_{n-1} via multiplication by some γ in μ_m. Then L_n/K_{n-1} satisfies the hypotheses of Lemma 4.1, with $1/\pi_{n-1}$, y_n, j_n, and γ^{-1} replacing x, y_1, j, and ζ respectively. Applying Lemma 4.1(iii) to L_n/K_{n-1} implies that $c(y_n)/y_n = \gamma^{-j_n} = \alpha^{-1} = \zeta^j$.

The equation for L_n/L_{n-1} is $y_n^p - y_n = x_n + g_n$ where the terms of the polynomial $g_n \in \mathbb{F}_p[x_1, \ldots, x_{n-1}, y_1, \ldots, y_{n-1}]$ each have degree congruent to one modulo $p-1$. By the inductive hypothesis and Lemma 4.1(ii), c scales g_n by ζ^j. Thus c scales both $y_n^p - y_n - x_n$ and y_n by ζ^j, which implies $c(x_n) = \zeta^j x_n$.

Conversely, suppose $c(x_i) = \zeta^j x_i$ and $c(y_i) = \zeta^j y_i$ for $1 \leq i \leq n$. The proof that L/K is G-Galois proceeds by induction on n; the case $n = 1$ can be computed explicitly, see e.g. [7, Lemma 1.4.1]. As an inductive hypothesis, suppose that L_{n-1}/K is a G/H_{n-1}-Galois extension. To finish, it suffices to show that the action of c extends to an automorphism of L_n, i.e., that c stabilizes the equation $y_n^p - y_n = f_n$ for L_n/L_{n-1}. By Lemmas 3.2 and 4.1(ii), the action of c scales every term of this equation by ζ^j. □

Lemma 4.4. *Suppose L/K is a G-Galois extension as in Section 2.3.*

(i) *There is a Witt vector $(x_1, \ldots, x_n)$ in standard form for the subextension L/L_0 and it is uniquely determined up to multiplication by $\mu_{m/m'}$.*
(ii) *There are $\varphi(m)/\varphi(m/m')$ different non-isomorphic G-Galois structures on the field extension L/K such that the action of σ on L is as in (2).*

Proof. For part (i), by Lemma 3.3, for fixed x, there is a uniquely determined Witt vector $(x_1, \ldots, x_n)$ in standard form for the subextension L/L_0. Now x is determined up to multiplication by ζ^d, for $d \in \mathbb{Z}$. By Proposition 4.3, every monomial in x_i has degree congruent to $j \mod m$. Replacing x with $\zeta^d x$ scales x_i by ζ^{dj}. The values of ζ^{dj} range over $\mu_{m/m'}$ by Lemma 4.1(i).

For part (ii), a G-Galois structure on L/K satisfying the requirement for σ is determined by an isomorphism $\iota : G \to \mathrm{Aut}(L/K)$ such that $\iota(\sigma)(y_1, \ldots, y_n) = (y_1, \ldots, y_n) +'(1, 0, \ldots, 0)$. If $h \in \mathrm{Aut}(L/K)$, then the map $h : L \to L$ yields an isomorphism of G-Galois extensions $L/K \to L/K$, the first with structure morphism ι and the second with structure morphism $h\iota h^{-1}$. Thus, modifying ι by an inner automorphism yields an isomorphic G-Galois structure on L/K. So the number of isomorphism classes of G-Galois structures with this requirement on σ is given by the number of elements of $\mathrm{Aut}(G)$ fixing σ, divided by the number of $\mathrm{Inn}(G)$ fixing σ.

An automorphism γ of G which fixes σ is determined by $\gamma(c)$. Also $\gamma(c)$ must have order m and have the same conjugation action as c on σ, as determined by Lemma 2.1(ii). When G is abelian, then $\alpha' = 1$ and there are $\varphi(m)$ choices for $\gamma(c)$. This yields the count $\varphi(m)/\varphi(m/m')$ since $m' = m$ and since $\mathrm{Inn}(G)$ is trivial. If G is non-abelian, then the image of $\gamma(c)$ in M must have order m and be congruent to c modulo $\langle c^{m/m'} \rangle = \ker(v)$. There are $p^n\varphi(m)/\varphi(m/m')$ choices for $\gamma(c)$. This yields the desired count, since there are p^n inner automorphisms of G which fix σ, namely conjugation by powers of σ. □

5. Main results

Let G be a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$. This section contains three results: first we prove that one can dominate a given Galois extension having group $\mathbb{Z}/p^{n-1} \rtimes \mathbb{Z}/m$ by a Galois extension having group $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$, with control over the last upper jump; second, we give necessary and sufficient conditions for the ramification filtration of a G-Galois extension; third, we define a parameter space for G-Galois extensions of K with given ramification filtration η and calculate its dimension in terms of the upper jumps.

5.1. A wild embedding problem

We prove that one can embed a given Galois extension having group $\mathbb{Z}/p^{n-1} \rtimes \mathbb{Z}/m$ by a Galois extension having group $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$, with control over the last upper jump. See [11, 24.42] for an earlier version of this result, in which $m = 1$ and there is no control over the upper jump. Recall that G/H_{n-1} is a semi-direct product of the form $\mathbb{Z}/p^{n-1} \rtimes \mathbb{Z}/m$.

Proposition 5.1. *Suppose L_{n-1}/K is a G/H_{n-1}-Galois extension with upper jumps $u_1 \leq \cdots \leq u_{n-1}$. Let $u_n \in \frac{1}{m}\mathbb{N}$ be such that either $u_n = pu_{n-1}$ or both $u_n > pu_{n-1}$ and $p \nmid mu_n$. Suppose also that $mu_n \equiv mu_1 \bmod m$. Then there exists a G-Galois extension L_n/K with upper jumps $u_1 \leq \cdots \leq u_n$ that dominates L_{n-1}/K.*

Proof. Without loss of generality, one can suppose $L_0 \simeq K[x]/(x^m - 1/t)$ and $c(x) = \zeta x$. The $\mathbb{Z}/p^{n-1}$-Galois extension L_{n-1}/L_0 has upper jumps $mu_1 \leq \cdots \leq mu_{n-1}$ by Lemma 3.6. By Section 3.2, L_{n-1}/L_0 is given by a Witt vector equation $(y_1^p, \ldots, y_{n-1}^p) = (y_1, \ldots, y_{n-1}) +'(x_1, \ldots, x_{n-1})$ for some $x_i \in L_0$, such that x_1 is not a $\wp$th power in L_0. Furthermore, one can choose $(x_1, \ldots, x_{n-1})$ to be in standard form. In particular, if $x_i \neq 0$, then $p \nmid v_0(x_i)$.

By Proposition 4.3, if $1 \leq i \leq n-1$, then $c(x_i) = \zeta^j x_i$ and $c(y_i) = \zeta^j y_i$ where $j = mu_1$. By Lemma 3.4, $mu_{n-1} = \max\{-p^{n-i}v_0(x_i)\}_{i=1}^{n-1}$.

If $u_n \neq pu_{n-1}$, let $x_n = x^{mu_n}$. In this case, $-v_0(x_n) = mu_n$. If $u_n = pu_{n-1}$, let $x_n = 0$. In this case, $-v_0(x_n) = -\infty < pmu_{n-1}$. In both cases, $(x_1, \ldots, x_n)$ is a Witt vector in standard form. Then the Witt vector equation $(y_1^p, \ldots, y_n^p) = (y_1, \ldots, y_n) +'(x_1, \ldots, x_n)$ yields a P-Galois extension L_n/L_0 dominating L_{n-1}/L_0, with upper jumps $mu_1 \leq \cdots \leq mu_n$ by Lemma 3.4 (i.e., [8, Thm. 1.1]).

By the definition of x_n, then $c(x_n) = \zeta^j x_n$. Let $c(y_n) = \zeta^j y_n$. By Proposition 4.3, L_n/K is a G-Galois extension dominating L_{n-1}/K, and it has upper jumps $u_1 \leq \cdots \leq u_n$ by Lemma 3.6. □

5.2. Conditions on the ramification filtration

The ramification filtration of a Galois extension with group G of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ is completely determined by either its lower or upper jumps. Here are the statement and proof of Theorem 1.1, giving necessary and sufficient conditions on the ramification filtrations of G-Galois extensions of K.

Theorem 5.2. *Let G be a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ where $p \nmid m$. Let $\sigma \in G$ have order p^n and let $m' = |\mathrm{Cent}_G(\sigma)|/p^n$. A sequence $u_1 \leq \cdots \leq u_n$ of rational numbers occurs as the set of positive breaks in the upper numbering of the ramification filtration of a G-Galois extension of $k((t))$ if and only if:*
(a) $u_i \in \frac{1}{m}\mathbb{N}$ *for* $1 \leq i \leq n$;
(b) $\gcd(m, mu_1) = m'$;
(c) $p \nmid mu_1$ *and, for* $1 < i \leq n$, *either* $u_i = pu_{i-1}$ *or both* $u_i > pu_{i-1}$ *and* $p \nmid mu_i$;
(d) *and* $mu_i \equiv mu_1 \bmod m$ *for* $1 \leq i \leq n$.

Proof. Conditions (a)–(d) are necessary: let $u_1 \leq \cdots \leq u_n$ be the set of upper jumps of a G-Galois extension of $k((t))$. The upper jumps of the $\mathbb{Z}/p^n$-subextension L/L_0 are $w_1 \leq \cdots \leq w_n$ where $w_i = mu_i$ by Lemma 3.6. Condition (a) follows since $w_i \in \mathbb{N}$ by the Hasse–Arf Theorem. Condition (b) follows from Lemma 4.1(i). Condition (c) is due to [1], see Lemma 3.5. Condition (d) follows from Proposition 4.2(ii).

Conditions (a)–(d) are sufficient: recall that G has generators σ (of order p^n) and c (of order m) and $c\sigma c^{-1} = \sigma^{\alpha'}$ for some integer α' such that $1 \leq \alpha' < p^n$ and $p \nmid \alpha'$. Let $\alpha \in \mathbb{F}_p^* \simeq (\mathbb{Z}/p)^*$ be such that $\alpha \equiv \alpha' \bmod p$. Let $j = mu_1$. By condition (b), ζ^j has order m/m' in k^*. Likewise, α^{-1} has order m/m' in k^*. Thus there exists an integer β such that $\zeta^{\beta j} = \alpha^{-1}$.

Consider the $\langle c\rangle$-Galois extension L_0/K with equation $x^m = 1/t$ and Galois action $c(x) = \zeta^\beta x$. Let $x_1 \in x^j k[\![x^{-m}]\!]^*$. Consider the $\mathbb{Z}/p$-Galois extension L_1/L with equation $y_1^p - y_1 = x_1$ and Galois action $\sigma(y_1) = y_1 + 1$. By [7, Lemma 1.4.1], L_1/K is a J_1-Galois extension. It has lower jump j and thus upper jump u_1. By conditions (a), (c), (d), and Proposition 5.1, there exists a G-Galois extension L/K dominating L_1/K with upper jumps $u_1 \leq \cdots \leq u_n$. □

Corollary 5.3. *Let G be a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ where $p \nmid m$. Suppose η is a ramification filtration of G satisfying conditions (a)–(d). Let f be the order of p modulo m/m' and let $q = p^f$. Then there exists a G-Galois extension L/K with ramification filtration η which is defined over $\mathbb{F}_q$.*

Proof. It suffices to produce a G-Galois extension L/K whose equations and Galois action have coefficients in $\mathbb{F}_q$. Note that ζ^{j_1} has order m/m' in k^*. By the definition of f, the field $\mathbb{F}_{p^f}$ contains the (m/m')th roots of unity, and thus contains ζ^{j_1}. The case $n = 1$ follows by direct computation with the equation $y_1^p - y_1 = x_1^{mu_1}$, see [7, Lemma 1.4.1]. The result then proceeds by induction on n. For the inductive step, one produces an equation for the extension L/L_{n-1} using Proposition 5.1. In the proof of that result, recall that $x_n \in \mathbb{F}_p[x]$ by definition. Thus the equation has coefficients in $\mathbb{F}_p$ by Lemma 3.2. The Galois action is defined over $\mathbb{F}_q$ by (2) and Proposition 4.3. □

5.3. Parameter space for G-Galois extensions

Given a sequence $u_1 \leq \cdots \leq u_n$ satisfying conditions (a)–(d), let η be the ramification filtration of G having upper jumps $u_1 \leq \cdots \leq u_n$. By Theorem 5.2, there exists a G-Galois extension of $k((t))$ with ramification filtration η. We prove there is a scheme $\mathcal{M}_\eta$ such that there is a natural bijection between the k-points of $\mathcal{M}_\eta$ and isomorphism classes of G-Galois extensions of $k((t))$ with ramification filtration η. We calculate the dimension of $\mathcal{M}_\eta$ in terms of the sequence $u_1 \leq \cdots \leq u_n$.

Notation 5.4. Given positive integers w and m, let

$$\epsilon_p(w, m) = \#\{e \in \mathbb{Z} \mid 1 \leq e \leq w, e \equiv w \bmod m, p \nmid e\}.$$

Lemma 5.5. *Let $\delta_p(w, m) = 1$ if $w \equiv ap \bmod m$ for some $1 \leq a \leq r$, where r is the remainder when $\lfloor w/p \rfloor$ is divided by m, and $\delta_p(w, m) = 0$ otherwise. Then $\epsilon_p(w, m) = \lceil w/m \rceil - \lfloor w/mp \rfloor - \delta_p(w, m)$.*

Proof. The number of integers e such that $1 \leq e \leq w$ and $e \equiv w \bmod m$ is $\lceil w/m \rceil$. To count the number of these which are divisible by p, consider the set $A = \{p, 2p, \ldots, \lfloor w/p \rfloor p\}$. Then A contains at least $\lfloor \lfloor w/p \rfloor / m \rfloor = \lfloor w/mp \rfloor$ elements e such that $e \equiv w \bmod m$. Let r be the remainder when $\lfloor w/p \rfloor$ is divided by m. Then A contains one additional element $e \equiv w \bmod m$ if and only if an element of $\{p, 2p, \ldots, rp\}$ is congruent to w modulo m. The formula holds since $\delta_p(w, m) = 1$ precisely in this case. □

Given a positive integer N, the root of unity $\zeta_{m/m'}$ acts on the affine variety $\mathbb{A}^N$ via multiplication on each coordinate. Let $\mathbb{A}^N/\mu_{m/m'}$ denote the quotient.

Theorem 5.6. *Let G be a semi-direct product of the form $\mathbb{Z}/p^n \rtimes \mathbb{Z}/m$ where $p \nmid m$. Let $u_1 \leq \cdots \leq u_n$ be a sequence satisfying conditions (a)–(d) and η be the ramification filtration of G with upper jumps $u_1 \leq \cdots \leq u_n$. Let $N_\eta = \sum_{i=1}^n \epsilon_p(mu_i, m)$. Then there is an open subscheme $U_\eta \subset \mathbb{A}^{N_\eta}/\mu_{m/m'}$ and a finite étale map $\pi : \mathcal{M}_\eta \to U_\eta$ of degree $\varphi(m)/\varphi(m/m')$ such that the k-points of $\mathcal{M}_\eta$ are in natural bijection with isomorphism classes of G-Galois extensions of $k((t))$ with ramification filtration η.*

It is clear that $\dim(\mathcal{M}_\eta) = N_\eta$ depends only on $p, m, u_1, \ldots, u_n$.

Proof. By Lemma 4.4, it suffices to show that the collection of Witt vectors $(x_1, \ldots, x_n)$ in standard form, which, as in Proposition 4.3, yield G-Galois extensions L/K with ramification invariants $u_1 \leq \cdots \leq u_n$, is in natural bijection with the k-points of an open subscheme of $\mathbb{A}^{N_\eta}$.

The proof is by induction on n. For the case $n = 1$, Lemma 3.4 shows that $x_1 \in k[x]$ must have degree mu_1. By Proposition 4.3, the extension L_1/K is J_1-Galois if and only if $c(x_1) = \zeta^{mu_1}x_1$, in other words, if and only if all exponents of x_1 are congruent to mu_1 modulo m. Since x_1 is in standard form, it has no exponents with degree divisible by p. Thus the number of possible exponents is $\epsilon = \epsilon_p(mu_1, m)$. Since the leading coefficient of x_1 is non-zero, the choice of x_n is equivalent to the choice of a k-point in an open subscheme of $\mathbb{A}^\epsilon$. (See also [7, Proposition 2.2.6]).

Now, suppose that $(x_1, \ldots, x_{n-1})$ is a Witt vector in standard form, which yields a G/H_{n-1}-Galois extension L_{n-1}/K with upper jumps $u_1 \leq \cdots \leq u_{n-1}$. Let $\epsilon = \epsilon_p(mu_n, m)$. It suffices to show that Witt vectors $(x_1, \ldots, x_n)$ in standard form which yield an extension L/K dominating L_{n-1}/K with upper jumps $u_1 \leq \cdots \leq u_n$ are in natural bijection with the k-points of an open subscheme $\tilde{U}_n \subset \mathbb{A}^\epsilon$.

The Witt vector $(x_1, \ldots, x_n)$ for the extension L/K is determined by the choice of $x_n \in k[x]$ in standard form. By Proposition 4.3, the extension L/K is G-Galois if and only if $c(x_n) = \zeta^{mu_1}x_n$, in other words, if and only if all exponents of x_n are congruent to mu_1 modulo m. Recall that $mu_1 \equiv mu_n \bmod m$ by Proposition 4.2.

By Lemma 3.4, the extension L/K has upper jump u_n if and only if $\deg(x_n) = -v_0(x_n) \leq mu_n$, where equality must hold if $u_n > pu_{n-1}$. Thus, an exponent e appearing in x_n satisfies $0 \leq e \leq mu_n$, and $e \equiv mu_n \bmod m$, and $p \nmid e$. The number of these exponents is $\epsilon = \epsilon_p(mu_n, m)$. The leading coefficient of x_n must be non-zero when $u_n > pu_{n-1}$. The choice of x_n is thus equivalent to the choice of a k-point in an open subscheme of $\mathbb{A}^\epsilon$. □

Remark 5.7. Consider the contravariant functor F_η from the category of schemes to sets, which associates to a scheme B the set of G-Galois extensions of $\mathcal{O}_B((t))$ whose geometric fibres have ramification filtration η. The scheme $\mathcal{M}_\eta$ does not represent F_η on the category of k-schemes because there are non-constant G-Galois covers defined over a base scheme B, which become constant after pullback by a finite morphism $B' \to B$. The scheme $\mathcal{M}_\eta$ is a fine moduli space for F_η on a category where such morphisms are trivialized; see [7, Thm. 2.2.10] for the case $n = 1$.

Remark 5.8. In [12, Prop. 4.1.1], the authors calculate the dimension of the tangent space of the versal deformation space of a $\mathbb{Z}/p^n$-Galois extension in terms of its ramification filtration. Theorem 5.6 is less technical than their result and it is not clear how to compare them directly.

6. Equations for $\mathbb{Z}/p^3$-Galois extensions

It is well known that the methods of Section 3.2 can be used to find equations for $\mathbb{Z}/p^n$-extensions [13], but the equations themselves are difficult to find in the literature. Here are formulae for the general $\mathbb{Z}/p^3$-Galois extension of K.

Example 6.1. Suppose L/K is a $\mathbb{Z}/p^3$-Galois extension of $K \cong k((t))$. Then there exist $x_1, x_2, x_3 \in K$ so that L/K is isomorphic to the following extension:

$$y_1^p - y_1 = x_1;$$
$$y_2^p - y_2 = \frac{x_1^p + y_1^p - (x_1 + y_1)^p}{p} + x_2;$$
$$y_3^p - y_3 = \frac{x_1^{p^2} + y_1^{p^2} - (x_1 + y_1)^{p^2}}{p^2} + \frac{x_2^p + y_2^p - (x_2 + y_2 + \frac{x_1^p + y_1^p - (x_1+y_1)^p}{p})^p}{p} + x_3.$$

A generator σ of the Galois group can be chosen so that its action is given by:

$$\sigma(y_1) = y_1 + 1;$$
$$\sigma(y_2) = y_2 + \frac{y_1^p + 1 - (y_1 + 1)^p}{p};$$
$$\sigma(y_3) = y_3 + \frac{y_1^{p^2} + 1 - (y_1 + 1)^{p^2}}{p^2} + \frac{y_2^p - (y_2 + \frac{y_1^p + 1 - (y_1+1)^p}{p})^p}{p}.$$

The integral coefficients in Example 6.1 can be considered to be in $\mathbb{F}_p \subset k$.

Proof. For the equations, it suffices to recursively compute $f_i = \overline{S}_{i-1} - y_i$ for $1 \leq i \leq 3$, starting with $S_0(x_1, y_1) = x_1 + y_1$ and $S_1(x_1, x_2, y_1, y_2) = x_2 + y_2 + (x_1^p + y_1^p - (x_1 + y_1)^p)/p$. The Galois action is given by $\sigma(y_i) = y_i + \tilde{f}_i$, where $\tilde{f}_i = f_i(y_1, \ldots, y_{i-1}, 1, 0, \ldots, 0)$. To see this, note that $y_i^p = y_i + f_i$ and (1) imply that $(y_1 + f_1, \ldots, y_n + f_n) = (y_1, \ldots, y_n) +'(x_1, \ldots, x_n)$. Substituting $(1, 0, \ldots, 0)$ for $(x_1, \ldots, x_n)$ yields $(y_1 + \tilde{f}_1, \ldots, y_n + \tilde{f}_n) = (y_1, \ldots, y_n) +' (1, 0, \ldots, 0)$, which equals $\sigma(y_1, \ldots, y_n)$ by Lemma 3.3. □

Example 6.2. When $p = 2$ and $x = t^{-j}$, here are equations for a $\mathbb{Z}/8$-Galois extension of $k((t))$, which is defined over $\mathbb{F}_2$ and has upper jumps j, $2j$, and $4j$:

$$y^2 - y = x; \qquad z^2 - z = xy; \qquad w^2 - w = x^3y + y^3x + xyz.$$

The Galois action is given by $y \mapsto y + 1$, $z \mapsto z + y$, and $w \mapsto w + y^3 + y + yz$.

Acknowledgements

First author was supported by an NDSEG Graduate Research Fellowship. Second author was partially supported by NSF grant DMS-07-01303.

The authors thank D. Harbater and an anonymous reader for help with Proposition 4.2, and J. Achter, S. Corry, G. Elder, M. Matignon, and the referee for useful comments.

References

[1] H. Schmid, Zur Arithmetik der zyklischen p-Körper, J. Reine Angew. Math. 176 (1937) 161–167.
[2] B. Green, M. Matignon, Liftings of Galois covers of smooth curves, Compos. Math. 113 (1998) 237–272.
[3] V. Deolalikar, Determining irreducibility and ramification groups for an additive extension of the rational function field, J. Number Theory 97 (2) (2002) 269–286.
[4] J.-P. Serre, Corps Locaux, Hermann, 1968.
[5] R. Hartshorne, Algebraic Geometry, in: Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.
[6] S. Lang, Algebra, 3rd ed., in: Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.
[7] R. Pries, Families of wildly ramified covers of curves, Amer. J. Math. 124 (4) (2002) 737–768.
[8] M. Garuti, Linear systems attached to cyclic inertia, in: Arithmetic Fundamental Groups and Noncommutative Algebra (Berkeley, CA, 1999), in: Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 377–386.
[9] L. Thomas, Ramification groups in Artin–Schreier–Witt extensions, J. Théor. Nombres Bordeaux 17 (2005) 689–720.
[10] R. Pries, Wildly ramified covers with large genus, J. Number Theory 119 (2) (2006) 194–209.
[11] M. Fried, M. Jarden, Field Arithmetic, Springer-Verlag, Berlin, 1986.
[12] J. Bertin, A. Mézard, Déformations formelles des revêtements sauvagement ramifiés de courbes algébriques, Invent. Math. 141 (1) (2000) 195–238.
[13] H. Schmid, Zyklische algebraische Funktionenkörper vom Grade p^n über endlichem Konstantenkörper der Charakteristik p, J. Reine Angew. Math. 175 (1936) 108–123.