JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Ghassan SARKIS et Joel SPECTER

Galois extensions of height-one commuting dynamical systems

Tome 25, n° 1 (2013), p. 163-178.

<http://jtnb.cedram.org/item?id=JTNB_2013__25_1_163_0>

Journal de Théorie des Nombres de Bordeaux **25** (2013), 163-178

Galois extensions of height-one commuting dynamical systems

par Ghassan SARKIS et Joel SPECTER

Résumé. Nous considérons un système dynamique constitué d'une paire de séries formelles commutant pour la composition, l'une non inversible et l'autre inversible d'ordre infini, de hauteur 1 à coefficients dans les entiers p-adiques. En supposant que chaque point du système dynamique engendre une extension galoisienne du corps $\mathbb{Q}_p$, nous montrons que ces extensions sont en fait abéliennes, et, à partir des résultats de la théorie du corps des normes, nous montrons que le système dynamique doit contenir une série d'ordre fini. À partir d'un résultat précédent, cela montre que les deux séries formelles doivent être des endomorphismes d'un groupe formel de hauteur 1.

Abstract. We consider a dynamical system consisting of a pair of commuting power series under composition, one noninvertible and another nontorsion invertible, of height one with coefficients in the p-adic integers. Assuming that each point of the dynamical system generates a Galois extension over the base field, we show that these extensions are in fact abelian, and, using results from the theory of the field of norms, we also show that the dynamical system must include a torsion series. From an earlier result, this shows that the original two series must in fact be endomorphisms of some height-one formal group.

1. Introduction

The study of p-adic dynamical systems has seen increased interest over the past two decades, reflected most recently in a new MSC category: *Arithmetic and non-Archimedean dynamical systems*. This note is concerned with three overlapping ways of looking at such systems—formal power series that commute under composition, iterated morphisms of the open p-adic unit disc, and galoisness of extensions that are obtained by adjoining zeros of dynamical systems. Indeed, the proof of the main result in this note can be viewed as relating commuting power series to formal groups, analytic

Manuscrit reçu le 13 juillet 2011.
The authors were partially supported by NSF Grant DMS-0755540.
Classification math. 11S31, 37P20, 14L05, 11S15.

maps of the open unit disk to locally analytic galois automorphisms, and galois towers to automorphism subgroups of residue fields.

1.1. Notation and motivation. Our power series have no constant term in order for composition to be well defined and finitary. Also, their linear coefficients are nonzero to exclude trivial cases. We adopt therefore some of the notation of [9]. For a commutative ring R, let $\mathcal{S}_0(R) = \{g \in R[\![x]\!] \mid g(0) = 0 \text{ and } g'(0) \neq 0\}$, and let $\mathcal{G}_0(R) = \{g \in \mathcal{S}_0(R) \mid g'(0) \in R^\times\}$ be the group of series that are invertible under composition. For $n \in \mathbb{N}$, let $g^{\circ n}$ be the n-fold iterate of the power series g with itself under composition. If $g \in \mathcal{G}_0(R)$, then $g^{\circ n}$ is defined for $n \in \mathbb{Z}$; if $g'(0) = 1$, then $g^{\circ n}$ is defined for $n \in \mathbb{Z}_p$.

Suppose F is a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field $\kappa = \mathcal{O}/\mathfrak{m}$. Denote by v_F the unique additive valuation on any algebraic extension of F normalized so that $v_F(F^\times) = \mathbb{Z}$; for simplicity, v_p will be used instead of $v_{\mathbb{Q}_p}$. Let $\mathfrak{m}^{\mathrm{alg}}$ be the maximal ideal in the integral closure of $\mathcal{O}$ in F^{alg}, an algebraic closure of F.

The *Newton Polygon* of $g(x) = \sum a_i x^i \in \mathcal{O}[\![x]\!]$, denoted $\mathcal{N}(g)$, is the convex hull of the sequence of points $(i, v_F(a_i))$. If $\mathcal{N}(g)$ has a segment of horizontal length ℓ and slope λ, then g has, counting multiplicity, precisely ℓ roots in F^{alg} of F-valuation $-\lambda$. We are interested in roots that lie in $\mathfrak{m}^{\mathrm{alg}}$; these correspond to segments of the Newton polygon of negative slope. To that end, we define $\mathcal{N}^-(g)$ to be the portion of $\mathcal{N}(g)$ consisting of segments whose slopes are negative.

Let $\bar{g}(x) = \sum \bar{a}_i x^i \in \kappa[\![x]\!]$ be the coefficientwise reduction of g to κ. The *Weierstrass degree* of $\bar{g}$, denoted $\mathrm{ord}_x(\bar{g})$, is defined to equal ∞ if $\bar{g} = 0$, and $\min\{i \mid \bar{a}_i \neq 0\}$ otherwise; the Weierstrass degree of g is defined to equal $\mathrm{ord}_x(\bar{g})$. The *p-adic Weierstrass Preparation Theorem* (WPT) asserts that if $\mathrm{ord}_x(\bar{g}) < \infty$ then there exists a unique factorization $g(x) = P(x)U(x)$, where $P(x) \in \mathcal{O}[x]$ is monic of degree $\mathrm{ord}_x(\bar{g})$ and $U(x) \in \mathcal{O}[\![x]\!]$ has a multiplicative inverse, and hence no zeroes in $\mathfrak{m}^{\mathrm{alg}}$. The roots of $P(x)$ and $g(x)$ in $\mathfrak{m}^{\mathrm{alg}}$ coincide; consequently, so do $\mathcal{N}(P)$ and $\mathcal{N}^-(g)$. See [6, Chapter IV] for a more details on Newton polygons.

If $f, u \in \mathcal{S}_0(\mathcal{O})$ such that f is noninvertible and u is nontorsion invertible, let

$$\Lambda_f(n) = \{\pi \in \mathfrak{m}^{\mathrm{alg}} \mid f^{\circ n}(\pi) = 0\} \qquad \text{and} \qquad \Lambda_f = \cup_{n\geq 0}\Lambda_f(n);$$
$$\Lambda_u(n) = \{\pi \in \mathfrak{m}^{\mathrm{alg}} \mid u^{\circ p^n}(\pi) = \pi\} \qquad \text{and} \qquad \Lambda_u = \cup_{n\geq 0}\Lambda_u(n).$$

Let $\Omega_f(n) = \Lambda_f(n)\backslash\Lambda_f(n-1)$. Observe that $\Omega_f(n+1)$ consists of roots of $f(x) - \pi$ as π ranges through $\Omega_f(n)$.

Although formal groups are not prominent in our results, they provide part of the motivation, which we discuss briefly next. We will call

$f, u \in \mathcal{S}_0(\mathcal{O})$ a *commuting pair* if f is noninvertible, u is nontorsion invertible, and $f \circ u = u \circ f$. Commuting pairs share certain characteristic properties with formal group endomorphisms. For example, $\Lambda_f = \Lambda_u$ by [9, Proposition 3.2]. Also, $\operatorname{ord}_x(\bar{f})$ is either infinite or a power of p by [9, Main Theorem 6.3]. Both of these results are important properties of formal group endomorphisms. Thus, Lubin suggested that commutativity may be enough to indicate the existence of "a formal group somehow in the background" [9, page 341]. Counterexamples to naïve statements and proofs of special cases of this conjecture are both known, though a general case remains elusive. For a more detailed discussion of the issues involved in a precise statement of the conjecture, see [12].

Let $e = p - 1$ if $p > 2$ and $e = 2$ if $p = 2$. The following special case of Lubin's conjecture, proven in [12, Theorem 1.1], makes use of a torsion third series of order e in the dynamical system:

Theorem 1.1. *Let $f, u, z \in \mathcal{S}_0(\mathbb{Z}_p)$ such that f, u is a commuting pair with $\operatorname{ord}_x(\bar{f}) = p$ and $v_p(f'(0)) = v_p(u'(0) - 1) = 1$, and if $p = 2$ then additionally $v_2(u'(0)^2 - 1) = 3$. Suppose also that z is torsion of order e and commutes with f. Then there exists a formal group G over $\mathbb{Z}_p$ such that $f, u, z \in \operatorname{End}_{\mathbb{Z}_p}(G)$.*

It is a straightforward corollary to this theorem that $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. We will show that, conversely, the Galoisness of $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is sufficient to guarantee the existence of a torsion series of order e.

We will call a commuting pair $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ *minimal* when $\operatorname{ord}_x(\bar{f}) = p$, $v_p(f'(0)) = 1$, and $v_p(u'(0) - 1) = 1$ if $p > 2$ and $v_p(u'(0) - 1) = 2$ if $p = 2$. Note that the condition on $v_p(u'(0) - 1)$ when $p = 2$ is slightly different than the one in [12] and Theorem 1.1, though the two are equivalent in the contexts we consider. Our main result is the following:

Main Theorem 1.2. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. If $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for each $\pi \in \Lambda_f$, then there exists a torsion series $z \in \mathcal{S}_0(\mathbb{Z}_p)$ of order e commuting with f and u.*

Remark 1.3. By [9, Propositions 1.1 and 1.2], there exists a unique power series $L_f(x) \in \mathcal{G}_0(\mathbb{Q}_p)$ for which $L_f'(0) = 1$ and $L_f \circ f = f'(0) L_f$. And for each $a \in \mathbb{Q}_p$ there exists a unique $[a]_f \in \mathcal{G}_0(\mathbb{Q}_p)$ such that $[a]_f'(0) = a$ and $[a]_f \circ f = f \circ [a]_f$. Let ζ_e be a primitive e^{th} root of unity, and let $z = [\zeta_e]_f$. In order to prove our main result, we need show only that $z \in \mathcal{G}_0(\mathbb{Z}_p)$.

The main theorem asserts that when f, u is a minimal commuting pair for which each torsion point π generates a Galois extension $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$, then the situation is almost identical to when $\bar{f}(x) = x^p$, that is, when there is a Lubin-Tate formal group in the background. The simplest case of the main theorem is $f(x) = (1 + x)^p - 1$, $u(x) = (1 + x)^{1+p} - 1$, and $z(x) =$

$(1+x)^{\zeta_{p-1}}-1$. These series are endomorphisms of the multiplicative formal group $\mathbb{G}_m(x,y)=(1+x)(1+y)-1$. More generally, when $\bar{f}(x)=\varphi(x^p)$ for some invertible φ, the main theorem would imply that $\mathbb{Q}_p(\Lambda_f)$ is still a maximal, totally ramified, abelian extension, and so can be defined via a uniformizer of $\mathbb{Q}_p$ by a Lubin-Tate formal group.

Our proof will rely on embedding $\mathrm{Gal}(\mathbb{Q}_p(\Lambda_f)/\mathbb{Q}_p)$ into the normalizer of $\bar{u}$ in the monoid $\mathcal{S}_0(\mathbb{F}_p)$, and so in Section 2 we make use of some powerful results from the theory of the fields of norms to describe this normalizer. In Section 3, we study the extensions $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ for $\pi\in\Lambda_f$ under the assumption that they are Galois; we show that the Galois groups of these extensions are abelian and use them to construct a torsion series of order e over $\mathbb{F}_p$ that commutes with $\bar{f}$ and $\bar{u}$. We complete the proof of the main result in Section 4.

2. Roots and fixed points

The *Nottingham group* $\mathrm{Nott}(\kappa)=\{g(x)\in\mathcal{S}_0(\kappa)\mid g'(0)=1\}$ is the group of normalized automorphisms of the field $\kappa((x))$. Some of its subgroups (like the one generated by $\bar{u}$, as we show in this section) arise as images of Galois groups under the field-of-norms functor. The Nottingham Group has also elicited interest among group theorists because every countably-based pro-p groups can be embedded in it, and as such, it contains elements of order p^n for all n; the shape of such torsion elements will be important for the proof of our main result when $p=2$. See [1, 5] for more information about the Nottingham group and its subgroups, [2, 3] for the original construction of the field of norms, and [7] for applications of the field of norms to p-adic dynamical systems.

If $\omega\in\mathrm{Nott}(\kappa)$, let $i_n(\omega)=\mathrm{ord}_x(\omega^{\circ p^n}(x)-x)-1$. This sequence of integers, called the *lower ramification numbers* of ω, measures the rapidity with which $\omega^{\circ p^n}$ approaches the identity. According to Sen's Theorem [13], if $\omega^{\circ p^n}(x)\neq x$ then $i_n(\omega)\equiv i_{n-1}(\omega) \mod p^n$. Let $e(\omega)=\lim_{n\to\infty}(p-1)i_n/p^{n+1}$. In light of Sen's Theorem, $e(\omega)$ is finite in those cases when $\omega^{\circ p^n}$ approaches the identity as slowly as possible. The factor $p-1$ normalizes $e(\omega)$ so that, when finite, it is an integer.

Let $\mathcal{A}_\omega=\{\omega^{\circ a}\mid a\in\mathbb{Z}_p\}$ be the closed subgroup of $\mathrm{Nott}(\kappa)$ generated by ω. The *separable normalizer* of $\mathcal{A}_\omega$ is given by $\mathrm{Norm}^{\mathrm{sep}}_\kappa(\mathcal{A}_\omega)=\{\vartheta\in\kappa[\![x]\!]\mid\vartheta'\neq 0$ and $\vartheta\circ\omega=\nu\circ\vartheta$ for some $\nu\in\mathcal{A}_\omega\}$. By [7, Proposition 5.5], $\mathrm{Norm}^{\mathrm{sep}}_\kappa(\mathcal{A}_\omega)$ is in fact a group. If $e(\omega)<\infty$, then by [7, Théorème 5.9], $\mathrm{Norm}^{\mathrm{sep}}_\kappa(\mathcal{A}_\omega)$ is an extension of a finite group of order dividing $e(\omega)$ by $\mathcal{A}_\omega$. These results use the theory of the fields of norms extensively, and we in turn make ample use of them after we show below that $e(\bar{u})=e$, allowing us to apply [7, Théorème 5.9] to $\mathcal{A}_{\bar{u}}$.

2.1. The lower ramification numbers of $\bar{u}$. Continue to denote by F a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}$, maximal ideal $\mathfrak{m}$, and residue field κ.

Lemma 2.1. *Suppose $f \in \mathcal{S}_0(\mathcal{O})$ such that $\mathrm{ord}_x(\bar{f}) = p$ and $v_F(f'(0)) = 1$. Then the roots of $f^{\circ n}$ in $\mathfrak{m}^{\mathrm{alg}}$ are simple for all n. Moreover, if $\pi \in \Omega_f(n)$ then $F(\pi)/F$ is a totally ramified extension of degree $(p-1)p^{n-1}$, and π is a uniformizer in $F(\pi)$.*

Proof. Using WPT, write $f(x) = P_0(x)U_0(x)$. Note that $\Omega_f(1)$ consists of the roots of $P_0(x)/x$. By the hypothesis on f, $\mathcal{N}(P_0(x)/x)$ consists of a single segment from $(0,1)$ to $(p-1,0)$. So $P_0(x)/x$ is a degree $p-1$ Eisenstein polynomial over $\mathcal{O}$. Therefore, the roots of $P_0(x)/x$ are simple, each with F-valuation $1/(p-1)$, and each generating a degree $p-1$ totally ramified extension of F.

Proceeding by induction, assume that the result holds for some $n \geq 0$. Let $\pi \in \Omega_f(n)$. Using WPT again, write $f(x) - \pi = P_n(x)U_n(x)$, where $P_n(x) \in (\mathcal{O}[\pi])[x]$ is a polynomial whose Newton polygon consists of a single segment from $(0,1)$ to $(p,0)$; that is, $P_n(x)$ is a degree p Eisenstein polynomial over $\mathcal{O}[\pi]$. Thus, the roots of $f(x)-\pi$ are simple, each of $F(\pi)$-valuation $1/p$, and each generating a degree p totally ramified extension of $F(\pi)$. Finally, if $\pi' \in \Omega_f(n)$ with $\pi' \neq \pi$, then the roots of $f(x) - \pi$ and $f(x) - \pi'$ are distinct. □

Lemma 2.2. *Suppose $f \in \mathcal{S}_0(\mathcal{O})$ such that $\mathrm{ord}_x(\bar{f}) = p$ and $v_F(f'(0)) = 1$. Let $\pi \in \Omega_f(1)$. Then $F(\pi)/F$ is Galois. Also, for a fixed primitive $p-1$ root of unity ζ_{p-1}, and for each $0 \leq i \leq p-2$, there exists a unique $\pi^{(i)} \in \Omega_f(1)$ such that $\pi^{(i)} \equiv \zeta_{p-1}^i \pi \mod \mathfrak{m}^2$.*

Proof. Using WPT as in Lemma 2.1, write $f = P_0U_0$. Note that $v_p(P_0'(0)) = 1$ and $P_0(x) \equiv x^p \mod p$. Therefore, P_0 is an endomorphism of a height-one formal $\mathcal{O}$-module (see [11]). Since the roots of f and P_0 coincide, the result follows. □

Corollary 2.3. $\mathrm{Gal}(F(\pi)/F)$ *is cyclic of order $p-1$.*

Proof. The Galois group is generated by $\pi \mapsto \pi^{(1)}$. □

We next quote [12, Lemma 1.2] for reference.

Lemma 2.4. *Suppose $g_1, g_2 \in \mathcal{S}_0(\mathcal{O})$ such that $0 < v_F(g_1'(0)) = v_F(g_2'(0)) < \infty$, and every root of g_1 in $\mathfrak{m}^{\mathrm{alg}}$ is also a root of g_2 of at least the same multiplicity. Suppose further that $g_1 \notin \mathcal{S}_0(\mathfrak{m})$. Then $\mathcal{N}^-(g_1) = \mathcal{N}^-(g_2)$, and so the roots of g_1 and g_2 in $\mathfrak{m}^{\mathrm{alg}}$ coincide.*

Lemma 2.5. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Then $\Lambda_f(\delta) = \Lambda_u(0)$.*

Proof. If π is a nonzero root of f, then $u(f(\pi)) = f(u(\pi)) = 0$. Thus $u(\pi)$ is another nonzero root of f, and by the hypothesis on $u'(0)$, it is in fact of the form $u(\pi) = \pi + \pi^2 d$ for some $d \in \mathbb{Z}_p[\![\pi]\!]$. By Lemma 2.2, $u(\pi) = \pi^{(0)} = \pi$. So $\Lambda_f(1) \subset \Lambda_u(0)$. If $p > 2$, then $\Lambda_f(1) = \Lambda_u(0)$ by Lemma 2.4.

If $p = 2$, then $\Lambda_f(1) \subsetneq \Lambda_u(0)$, and so $\Lambda_u(0)$ contains elements of $\Lambda_u = \Lambda_f$ other than the roots of f. The dotted line in Figure 2.1 corresponds to the smallest possible slope of the second segment of $\mathcal{N}^-(u(x) - x)$. Let

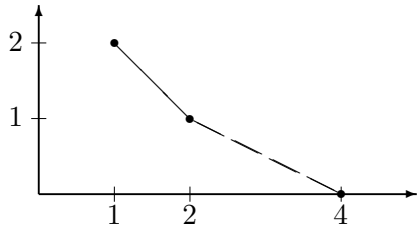

FIGURE 2.1. $\mathcal{N}^-(u(x) - x)$

$\gamma \in \Omega_f(k)$ be a fixed point of u with $k > 1$ (that is, $\gamma \notin \Lambda_f(1)$), and let $\beta = f^{\circ k-2}(\gamma)$. Thus $\beta \in \Omega_f(2)$. Observe that $u(\beta) = u(f^{\circ k-2}(\gamma)) = f^{\circ k-2}(u(\gamma)) = f^{\circ k-2}(\gamma) = \beta$. Since $|\Omega_f(2)| = 2$, u must then fix the other element of $\Omega_f(2)$ as well. Therefore, $\Omega_f(2) \subset \Lambda_u(0)$. By Lemma 2.4, $\Lambda_f(2) = \Lambda_u(0)$. □

Proposition 2.6. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. For all $n \geq \delta$, if $\pi \in \Omega_f(n)$, then $u^{\circ i}(\pi) = u^{\circ j}(\pi)$ if and only if $p^{n-\delta} \mid j - i$. Moreover, $\Lambda_f(n) = \Lambda_u(n - \delta)$.*

Proof. By Lemma 2.5, $\Lambda_f(\delta) = \Lambda_u(0)$; and if $\pi \in \Omega_f(\delta)$ then $u^{\circ i}(\pi) = \pi$ for all $i \geq 0$. Proceeding by induction on n, assume that the result holds for some $n \geq \delta$. Let $\pi \in \Omega_f(n+1)$, so that $f^{\circ n-\delta+1}(\pi) \in \Omega_f(\delta)$. For any $i \geq 0$ we have $u^{\circ i}(f^{\circ n-\delta+1}(\pi)) = f^{\circ n-\delta+1}(\pi) = f^{\circ n-\delta+1}(u^{\circ i}(\pi))$, so $u^{\circ i}(\pi) \in \Omega_f(n+1)$. Suppose that for some i and j we have $u^{\circ i}(\pi) = u^{\circ j}(\pi)$, and so $u^{\circ(j-i)}(\pi) = \pi$. If $i \neq j$, write $j - i = rp^s$ with $p \nmid r$. Applying Lemma 2.4 to $u^{\circ p^s}(x) - x$ and $u^{\circ rp^s}(x) - x$, we get $u^{\circ p^s}(\pi) = \pi$. This is impossible if $s \leq n - \delta$, since $\pi \notin \Lambda_f(n) = \Lambda_u(n - \delta) \supseteq \Lambda_u(s)$. Thus $\{u^{\circ i}(\pi) \mid 0 \leq i \leq p^{n-\delta+1} - 1\}$ constitute the $p^{n-\delta+1}$ distinct roots of $f^{\circ n-\delta+1}(x) - f^{\circ n-\delta+1}(\pi)$, and $u^{\circ p^{n-\delta+1}}(\pi) = \pi$. Therefore, $\Lambda_f(n+1) \subseteq \Lambda_u(n-\delta+1)$. By Lemma 2.4, $\Lambda_f(n+1) = \Lambda_u(n-\delta+1)$, concluding the proof. □

Corollary 2.7. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. Then $e(\bar{u}) = e$. In particular, $\mathrm{Norm}^{\mathrm{sep}}_{\mathbb{F}_p}(\mathcal{A}_{\bar{u}})$ is an extension of a finite group of order dividing e by $\mathcal{A}_{\bar{u}}$.*

Proof. By WPT we have $i_n(\bar{u}) + 1 = |\Lambda_u(n)| = |\Lambda_f(n+\delta)| = p^{n+\delta}$. So $e(\bar{u}) = \lim_{n\to\infty}(p-1)(p^{n+\delta} - 1)/p^{n+1} = (p-1)p^{\delta-1} = e$. The rest of the result follows by an application of [7, Théorème 5.9] to $\mathcal{A}_{\bar{u}}$. □

3. Abelian extensions and torsion series

Consider the following notation:

$$K_n = \mathbb{Q}_p(\Lambda_f(n)) \qquad K = \cup_{n\geq 1} K_n$$
$$\mathfrak{G}_n = \mathrm{Gal}(K_n/\mathbb{Q}_p) \qquad \mathfrak{G} = \varprojlim \mathfrak{G}_n = \mathrm{Gal}(K/\mathbb{Q}_p)$$

For the remainder of the note, we will assume that for each n, K_n is generated by any single element of $\Omega_f(n)$, or equivalently, $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. In this section, we show that $\mathfrak{G}$ is abelian, and that $\bar{u}$ commutes with a torsion series of order e.

Call a sequence $\{\pi_n\}_{n\geq 0}$ of elements in Λ_f *f-consistent* if $\pi_0 = 0$, $\pi_1 \neq 0$, and $f(\pi_{n+1}) = \pi_n$ for all $n \geq 0$ (see [9, Page 329]); in particular, $\pi_n \in \Omega_f(n)$ for all $n > 0$. By Lemma 2.1, for $n > 0$, $K_n/\mathbb{Q}_p$ is a totally ramified Galois extension of degree $(p-1)p^{n-1}$.

Fix an f-consistent sequence $\{\pi_n\}_{n\geq 0}$ and let $\mathfrak{u}_n \in \mathfrak{G}_n$ be defined by $\mathfrak{u}_n(\pi_n) = u(\pi_n)$. Since the coefficients of u are fixed by $\mathfrak{u}_n$, we have $\mathfrak{u}_n^i(\pi_n) = u^{\circ i}(\pi_n)$ for all i. Clearly, $\mathfrak{u}_1$ is trivial, as are $\mathfrak{G}_1$ and $\mathfrak{u}_2$ if $p = 2$.

Lemma 3.1. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$.*

1. *If $p > 2$, then the Sylow p-subgroup of $\mathfrak{G}_n$ is cyclic and generated by $\mathfrak{u}_n$ for all $n \geq 1$.*
2. *If $p = 2$, then $\mathfrak{G}_n$ contains a cyclic subgroup of order 2^{n-2} generated by $\mathfrak{u}_n$ for all $n \geq 2$.*

In both cases, $\mathfrak{u}_{n+1}|_{K_n} = \mathfrak{u}_n$, and so $\mathfrak{u} = \varprojlim \mathfrak{u}_n$ generates a normal procyclic subgroup of $\mathfrak{G}$ of index e.

Proof. The result follows immediately form Proposition 2.6. With $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$, we have $\mathfrak{u}_n^i = 1 \iff u^{\circ i}(\pi_n) = \pi_n \iff p^{n-\delta} \mid i$, and so $|\mathfrak{u}_n| = p^{n-\delta}$. Also, $\mathfrak{u}_{n+1}(\pi_n) = \mathfrak{u}_{n+1}(f(\pi_{n+1})) = f(\mathfrak{u}_{n+1}(\pi_{n+1})) = f \circ u(\pi_{n+1}) = u \circ f(\pi_{n+1}) = \mathfrak{u}_n(\pi_n)$. □

Remark 3.2. Let $\pi \in \Omega_f(n)$. The Galoisness of $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is equivalent to the following: for each $\mathfrak{g} \in \mathfrak{G}$ there exists a $g \in \mathcal{G}_0(\mathbb{Z}_p)$ such that $g(\pi) = \mathfrak{g}(\pi)$. As such, all the Galois automorphisms are "locally analytic." On the other hand, the relation between $\mathfrak{u}$, $\mathfrak{u}_n$, and u suggests that at least some of the Galois automorphisms are "globally analytic"; in fact, our main result aims to show that they all are. We take a step in that direction by partially extending the relation between $\mathfrak{u}$, $\mathfrak{u}_n$, and u to other elements of the Galois group. For $\mathfrak{g} \in \mathfrak{G}$, write $\mathfrak{g}(\pi_n) = \sum_{i=1}^{\infty} c_{i,n}\pi_n^i$, where the coefficients $c_{i,n}$ are Teichmüller representatives, and let $g_n(x) = \sum_{i=1}^{\infty} c_{i,n}x^i$. Note that $\mathfrak{g}^i(\pi_n) = g_n^{\circ i}(\pi_n)$ for all i. We will call the sequence $\{g_n\}$ the *realization* of $\mathfrak{g}$. Let $\Gamma = \{\sum_{i=1}^{\infty} c_i x^i \in \mathcal{S}_0(\mathbb{Z}_p) \mid c_i^p = c_i\}$. The topology of $\mathbb{Z}_p[\![x]\!]$ induced by the additive $\mathbb{Z}$-valued valuation v_x is equivalent to the product topology

of $\mathbb{Z}_p^{\mathbb{N}}$ where each copy of $\mathbb{Z}_p$ has the discrete topology. Tychonoff's theorem thus implies that Γ is a compact subset of $\mathbb{Z}_p[\![x]\!]$. So $\{g_n\}$ must have an accumulation point $g \in \Gamma$.

Lemma 3.3. *Suppose $\mathfrak{g}, \mathfrak{h} \in \mathfrak{G}$ and $g, h \in \mathcal{S}_0(\mathbb{Z}_p)$ such that for some $\pi \in K$, $\mathfrak{g}(\pi) = g(\pi)$ and $\mathfrak{h}(\pi) = h(\pi)$. Then $\mathfrak{gh}(\pi) = h \circ g(\pi)$.*

Proof. A direct computation yields the result: $\mathfrak{gh}(\pi) = \mathfrak{g}(h(\pi)) = h(\mathfrak{g}(\pi)) = h \circ g(\pi)$. □

Lemma 3.4. *Suppose $h_1, h_2 \in \mathbb{Z}_p[\![x]\!]$ and k is an integer such that $h_1(\pi_n) \equiv h_2(\pi_n) \mod \pi_n^k$ for infinitely many n. Then $\bar{h}_1(x) \equiv \bar{h}_2(x) \mod x^k$.*

Proof. If $\bar{h}_1 \neq \bar{h}_2$, write $\bar{h}_1(x) \equiv \bar{h}_2(x) + \bar{d}x^m \mod x^{m+1}$ for some $d \in \mathbb{Z}_p^\times$ and $m > 0$. Pick n large enough so that $v_p(\pi_n^{m+1}) \leq 1$ and $h_1(\pi_n) \equiv h_2(\pi_n) \mod \pi_n^k$. Then $h_1(\pi_n) \equiv h_2(\pi_n) + d\pi^m \mod \pi_n^{m+1}$, which implies $m \geq k$. □

Lemma 3.5. *With the the notation of Remark 3.2, suppose $\{g_n\}$ is a realization of $\mathfrak{g} \in \mathfrak{G}$ with an accumulation point g. If $\mathfrak{ug} = \mathfrak{gu}^t$ for some $t \in \mathbb{Z}_p$ then $\bar{g} \circ \bar{u} = \bar{u}^{\circ t} \circ \bar{g}$. In particular, $\bar{g} \in \mathrm{Norm}_{\mathbb{F}_p}(\mathcal{A}_{\bar{u}})$*

Proof. Note that Lemma 3.1 guarantees $\mathfrak{ug} = \mathfrak{gu}^t$ for some $t \in \mathbb{Z}_p$. By Lemma 3.3, $\mathfrak{ug}(\pi_n) = g_n \circ u(\pi_n)$ and $\mathfrak{gu}^t(\pi_n) = u^{\circ t} \circ g_n(\pi_n)$ for all n. Let $\{g_{n_\ell}\}$ be a subsequence of $\{g_n\}$ which converges to g. Given $k > 0$, pick l large enough such that if $\ell \geq l$ then $g(x) \equiv g_{n_\ell}(x) \mod x^k$. Thus, if $\ell \geq l$, we have the following congruences $\mod \pi_{n_\ell}^k$: $g \circ u(\pi_{n_\ell}) \equiv \mathfrak{ug}(\pi_{n_\ell}) = \mathfrak{gu}^t(\pi_{n_\ell}) \equiv u^{\circ t} \circ g(\pi_{n_\ell})$. Lemma 3.4 implies $\bar{g} \circ \bar{u} \equiv \bar{u}^{\circ t} \circ \bar{g} \mod x^k$. Since k was arbitrary, our result follows. □

3.1. Proof that $\mathfrak{G}$ is abelian if $p > 2$.

Lemma 3.6. *Suppose $p > 2$, $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. Then for all $n \geq 1$ there exists an automorphism $\mathfrak{w}_n \in \mathfrak{G}_n$ of order $p-1$, and $\mathfrak{w}_{n+1}|_{\mathfrak{G}_n} = \mathfrak{w}_n$.*

Proof. Following Lemma 2.2 and Corollary 2.3, let ζ_{p-1} be a primitive $p-1$ root of unity, and let $\mathfrak{w}_1$ be the generator of $\mathfrak{G}_1$ given by $\mathfrak{w}(\pi_1) \equiv \zeta_{p-1}\pi_1 \mod \pi_1^2$. Proceeding by induction, suppose for some $n \geq 1$ there exists a $\mathfrak{w}_n \in \mathfrak{G}_n$ of order $p-1$. Let $\hat{\mathfrak{w}}_{n+1} \in \mathfrak{G}_{n+1}$ be any lifting of $\mathfrak{w}_n$, and let $\mathfrak{w}_{n+1} = \hat{\mathfrak{w}}_{n+1}^{p^n}$. □

Let $\mathfrak{w} = \varprojlim \mathfrak{w}_n \in \mathfrak{G}$. Clearly, $\mathfrak{w}$ has order $p-1$.

Lemma 3.7. *Suppose $p > 2$, $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. Let $\rho_n = \mathfrak{w}(\pi_n)$. Then $\{\rho_n\}$ is an f-consistent sequence, and $\rho_n \equiv \zeta_{p-1}\pi_n \mod \pi_n^2$ for all $n \geq 1$.*

Proof. The f-consistency of $\{\rho_n\}$ can be verified directly: $f(\rho_{n+1}) = f(\mathfrak{w}(\pi_{n+1})) = \mathfrak{w}(f(\pi_{n+1})) = \mathfrak{w}(\pi_n) = \rho_n$.

Lemma 2.2 provides the second part of the result for $n = 1$, so we proceed by induction on n. Suppose that for some $n \geq 1$, $\rho_n \equiv \zeta_{p-1}\pi_n \mod \pi_n^2$. By Lemma 2.1,

$$v_p(\pi_n^2) = 2/(p^{n-1}(p-1)) > v_p(\pi_{n+1}^{p+1}) = (p+1)/(p^n(p-1)),$$

and so $\rho_n \equiv \zeta_{p-1}\pi_n \mod \pi_{n+1}^{p+1}$. By our hypothesis on the commuting pair, $f(x) \equiv ax^p \mod (p, x^{p+1})$ for some $a \in \mathbb{Z}_p^\times$. And by Lemma 2.1, $v_p(\pi_{n+1}^{p+1}) = v_p(\rho_{n+1}^{p+1}) = (p+1)/(p^n(p-1)) < 1 = v_p(p)$. Thus, $\rho_n = f(\rho_{n+1}) \equiv a\rho_{n+1}^p \mod \pi_{n+1}^{p+1}$. Finally, $\zeta_{p-1}\pi_n = \zeta_{p-1}f(\pi_{n+1}) \equiv \zeta_{p-1}a\pi_{n+1}^p \mod \pi_{n+1}^{p+1}$. Therefore, $a\rho_{n+1}^p \equiv \zeta_{p-1}a\pi_{n+1}^p \mod \pi_{n+1}^{p+1}$, which implies our result. □

Proposition 3.8. *Suppose $p > 2$ and $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair. If $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$ then $\mathfrak{G} \cong Z_{p-1} \times \mathbb{Z}_p$. In particular, $\mathfrak{G}$ is abelian.*

Proof. Recall from Lemma 3.1 that $\langle \mathfrak{u} \rangle \cong \mathbb{Z}_p$ is a normal subgroup of $\mathfrak{G}$ of index $p-1$. Therefore, $\mathfrak{w}\mathfrak{u}\mathfrak{w}^{-1} = \mathfrak{u}^t$ for some $t \in \mathbb{Z}_p$. Moreover, $\mathfrak{w}\mathfrak{u}\mathfrak{w}^{-1} = \mathfrak{w}^p\mathfrak{u}\mathfrak{w}^{-p} = \mathfrak{u}^{t^p}$. So t must be a $p-1$ root of unity. We will complete the proof by showing that $t \equiv 1 \mod p$, and hence $t = 1$.

Following Lemma 3.7, write $\rho_2 = \zeta_{p-1}\pi_2 + c_2\pi_2^2 + c_3\pi_2^3 + \cdots$ with $c_i \in \mathbb{Z}_p$. Recall from the hypothesis on the commuting pair and Lemma 2.5 that $u(x) \equiv x + bx^p \mod (p, x^{p+1})$ for some $b \in \mathbb{Z}_p^\times$, and so $u^{\circ t}(x) \equiv x + tbx^p \mod (p, x^{p+1})$. The following congruences are mod π_2^{p+1}.

$$\begin{aligned}
\rho_2 + b\zeta_{p-1}\pi_2^p &\equiv \rho_2 + b\rho_2^p \equiv u(\rho_2) \\
&= u(\mathfrak{w}(\pi_2)) = \mathfrak{w}(u(\pi_2)) = \mathfrak{w}\mathfrak{u}(\pi_2) = \mathfrak{u}^t\mathfrak{w}(\pi_2) \\
&\equiv \mathfrak{u}^t(\zeta_{p-1}\pi_2 + c_2\pi_2^2 + c_3\pi_2^3 + \cdots) \\
&= \zeta_{p-1}\mathfrak{u}^t(\pi_2) + c_2\mathfrak{u}^t(\pi_2)^2 + c_3\mathfrak{u}^t(\pi_2)^3 + \cdots \\
&= \zeta_{p-1}u^{\circ t}(\pi_2) + c_2u^{\circ t}(\pi_2)^2 + c_3u^{\circ t}(\pi_2)^3 + \cdots \\
&\equiv \zeta_{p-1}(\pi_2 + tb\pi_2^p) + c_2\pi_2^2 + c_3\pi_2^3 + \cdots \\
&= \rho_2 + tb\zeta_{p-1}\pi_2^p.
\end{aligned}$$

Therefore, $t \equiv 1 \mod p$, concluding the proof. □

Corollary 3.9. *Suppose $p > 2$. Then $\mathfrak{G}_n \cong Z_{p-1} \times Z_{p^{n-1}}$.*

3.2. Proof that $\mathfrak{G}$ is abelian if $p = 2$.

Proposition 3.10. *Suppose $p = 2$ and $f, u \in \mathcal{S}_0(\mathbb{Z}_2)$ is a minimal commuting pair. If $\mathbb{Q}_2(\pi)/\mathbb{Q}_2$ is Galois for all $\pi \in \Lambda_f$, then $\mathfrak{G}$ is abelian.*

Proof. By [9, Corollary 6.2.1], write $\bar{f}(x) = \varphi(x^2)$ where $\varphi(x) \in \mathcal{G}_0(\mathbb{F}_2)$. Observe that φ and $\bar{u}$ commute.

If $\varphi \in \mathcal{A}_{\bar{u}}$, then $\varphi = \bar{u}^{\circ t}$ for some $t \in \mathbb{Z}_2$. Therefore, $u^{\circ -t} \circ f$ is congruent to $x^2 \mod 2$, and its linear coefficient is a uniformizer in $\mathbb{Z}_2$. In other words, $u^{\circ -t} \circ f$ is an endomorphism of a rank-one formal $\mathbb{Z}_2$-module (see [11]). Since f and u commute with $u^{\circ -t} \circ f$, they must both be endomorphisms of the same formal module. Our result follows.

If $\varphi \notin \mathcal{A}_{\bar{u}}$, then by [7, Théorème 5.9] and Corollary 2.7, $\mathrm{Norm}^{\mathrm{sep}}_{\mathbb{F}_p}(\mathcal{A}_{\bar{u}})$ must be abelian. By Lemma 3.5, $\mathfrak{G}$ must be abelian as well. □

Suppose $F/\mathbb{Q}_2$ is a totally ramified Galois extension, π is a uniformizer of the ring of integers of F, and $\mathfrak{g} \in \mathrm{Gal}(F/\mathbb{Q}_2)$. Following the notation of [14, Chapter IV], let $i_{\mathrm{Gal}(F/\mathbb{Q}_2)}(\mathfrak{g}) = v_F(\mathfrak{g}(\pi) - \pi)$; that is, $i_{\mathrm{Gal}(F/\mathbb{Q}_2)}$ is one more than the order function of the filtration defined by the ramification groups of $\mathrm{Gal}(F/\mathbb{Q}_2)$.

Corollary 3.11. *If $p = 2$, then $\mathfrak{G} \cong Z_2 \times \mathbb{Z}_2$, and for $n \geq 2$, $\mathfrak{G}_n \cong Z_2 \times Z_{2^{n-2}}$.*

Proof. By Lemma 3.1 and Proposition 3.10, it is sufficient to show that $\mathfrak{G}_3$ is not cyclic. There exist eight totally ramified quartic cyclic extensions $F/\mathbb{Q}_2$, given by $F = \mathbb{Q}_2\left(\sqrt{\alpha(2+\beta)}\right)$, where $\alpha \in \{1,3,5,7\}$ and $\beta \in \{\sqrt{2}, \sqrt{-6}\}$ (see [4, Lemma IX.4]). The only element $\mathfrak{g} \in \mathrm{Gal}(F/\mathbb{Q}_2)$ of order 2 is $\mathfrak{g} : \sqrt{\alpha(2+\beta)} \mapsto -\sqrt{\alpha(2+\beta)}$, and so $i_{\mathrm{Gal}(F/\mathbb{Q}_2)}(\mathfrak{g}) = v_F\left(2\sqrt{\alpha(2+\beta)}\right) = 5$. However, $|\mathfrak{u}_3| = 2$ by Lemma 3.1, and $i_{\mathfrak{G}_3}(\mathfrak{u}_3) = \mathrm{ord}_x(\bar{u}(x) - x) = 4$ by Proposition 2.6. □

Remark 3.12. The f-consistent sequence defined in Lemma 3.7 for $p > 2$ has an analogue for $p = 2$: let $\mathfrak{w}$ be the element of order 2 in $\mathfrak{G}$, and define $\rho_n = \mathfrak{w}(\pi_n)$. For each n, write the π_n-adic expansion of ρ_n as $\rho_n = \sum_{i=1}^{\infty} c_{i,n}\pi_n^i$, where $c_{1,n} = 1$, and $c_{i,n} \in \{0,1\}$ for all i. Let $w_n(x) = \sum_{i=1}^{\infty} c_{i,n}x^i$. Recall from Remark 3.2 that $\{w_n\}$ is a realization of $\mathfrak{w}$ in the compact set Γ, and so it has a convergent subsequence $\{w_{n_\ell}\}$ with accumulation point w.

Corollary 3.13. *Suppose $p = 2$. Then $w_n(x) \equiv x + x^2 \mod x^3$ for all n, and so $w(x) \equiv x + x^2 \mod x^3$ as well.*

Proof. Let $\mathfrak{w}_n = \mathfrak{w}_{|_{K_n}}$. Since $K_3/\mathbb{Q}_2$ is biquadratic, a direct computation shows that the nonidentity elements of $\mathfrak{G}_3$ have $i_{\mathfrak{G}_3}$-values 2, 2, and 4. As seen in the proof of Corollary 3.11, $i_{\mathfrak{G}_3}(\mathfrak{u}_3) = 4$. Thus $i_{\mathfrak{G}_3}(\mathfrak{w}_3) = i_{\mathfrak{G}_3}(\mathfrak{w}_3\mathfrak{u}_3) = 2$. Proceeding by induction, suppose that $i_{\mathfrak{G}_n}(\mathfrak{w}_n) = 2$ for some $n \geq 3$. By [14, Chapter IV, Proposition 3],

$$i_{\mathfrak{G}_n}(\mathfrak{w}_n) = \left(i_{\mathfrak{G}_{n+1}}(\mathfrak{w}_{n+1}) + i_{\mathfrak{G}_{n+1}}(\mathfrak{w}_{n+1}\mathfrak{u}_{n+1}^{2^{n-2}})\right)/2.$$

But $i_{\mathfrak{G}_{n+1}}(\mathfrak{g}) \geq 2$ for all $\mathfrak{g} \in \mathfrak{G}_{n+1}$. So $i_{\mathfrak{G}_{n+1}}(\mathfrak{w}_{n+1}) = i_{\mathfrak{G}_{n+1}}(\mathfrak{w}_{n+1}\mathfrak{u}_{n+1}^{2^{n-2}}) = 2$. □

3.3. Torsion series over $\mathbb{F}_p$. Let $\mathfrak{w} \in \mathfrak{G}$ be an element of order e as described in Lemma 3.7 and Remark 3.12, with realization $\{w_n\}$ and accumulation point w. We end this section by studying $\bar{w}$ in more detail.

Proposition 3.14. *Suppose $f, u \in \mathcal{S}_0(\mathbb{Z}_p)$ is a minimal commuting pair, and $\mathbb{Q}_p(\pi)/\mathbb{Q}_p$ is Galois for all $\pi \in \Lambda_f$. Then $\bar{w}$ commutes with $\bar{u}$. Moreover, $\bar{w}$ is torsion of order $e = e(\bar{u})$.*

Proof. For $k > 0$, pick l such that if $\ell > l$ then $v_p(\pi_{n_\ell}^{k+1}) \leq 1$ and $v_x(w - w_{n_\ell}) \geq k + 1$.

By Lemma 3.3, $\mathfrak{w}\mathfrak{u}(\pi_n) = u \circ w_n(\pi_n)$ and $\mathfrak{u}\mathfrak{w}(\pi_n) = w_n \circ u(\pi_n)$ for all n. Also, $\mathfrak{w}\mathfrak{u} = \mathfrak{u}\mathfrak{w}$ since $\mathfrak{G}$ is abelian. Thus, if $\ell > l$, then $u \circ w(\pi_{n_\ell}) \equiv u \circ w_n(\pi_{n_\ell}) = w_n \circ u(\pi_{n_\ell}) \equiv w \circ u(\pi_{n_\ell})$, where the congruences are mod $\pi_{n_\ell}^{k+1}$. By Lemma 3.4, $\bar{u} \circ \bar{w} \equiv \bar{w} \circ \bar{u} \mod x^{k+1}$. Since k was arbitrary, it follows that $\bar{u} \circ \bar{w} = \bar{w} \circ \bar{u}$.

If $\ell > l$, then $\pi_{n_\ell} = \mathfrak{w}^e(\pi_{n_\ell}) = w_n^{\circ e}(\pi_{n_\ell}) \equiv w^{\circ e}(\pi_{n_\ell}) \mod \pi_{n_\ell}^{k+1}$. By Lemma 3.4, $\bar{w}^{\circ e}(x) \equiv x \mod x^{k+1}$. Since k was arbitrary, we see that the order of $\bar{w}$ divides e. If $p > 2$, then the order is exactly $p - 1$ because $w'(0)$ is a primitive $p - 1$ root of unity by Lemma 3.7. If $p = 2$, then the order of $\bar{w}$ is 2 by Corollary 3.13. □

Corollary 3.15. $\mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}}) = \langle \bar{w} \rangle \times \mathcal{A}_{\bar{u}}$*; in particular,* $\mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}})$ *is abelian.*

Proof. By Corolary 2.7, $\mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}})$ is an extension of a finite group of order dividing e by $\mathcal{A}_{\bar{u}}$, and $\langle \bar{w} \rangle \times \mathcal{A}_{\bar{u}} \leq \mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}})$. □

Corollary 3.16. *Suppose $\theta \in \mathcal{G}_0(\mathbb{F}_p)$ is a torsion series of order e that commutes with $\bar{u}$. If $\theta'(0) = \bar{w}'(0)$ then $\theta = \bar{w}$. In particular, $\bar{w}$ is independent of the choice of accumulation point of $\{w_n\}$.*

Proof. Each of the series θ and $\bar{w}$ generates the unique order-e subgroup of $\mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}})$. □

By [9, Corollary 6.2.1], the noninvertible half of a commuting pair must be of the form $\bar{f}(x) = \varphi(x^p)$ for some $\varphi \in \mathcal{G}_0(\mathbb{F}_p)$.

Corollary 3.17. *The power series $\bar{w}$ and φ commute.*

Proof. Both $\bar{w}$ and φ are elements of the abelian group $\mathrm{Norm}_{\mathbb{F}_p}^{\mathrm{sep}}(\mathcal{A}_{\bar{u}})$. □

If $p = 2$, then $\bar{w} \in \mathrm{Nott}(\mathbb{F}_2)$. Torsion elements of the Nottingham group are well understood and well behaved. For instance, all torsion elements of $\mathrm{Nott}(\mathbb{F}_p)$ have order p^d for some d. Moreover, since any pro-p group can

be embedded in Nott($\mathbb{F}_p$), then in fact there exists a torsion element of order p^d for every d. Two torsion elements of order p, $x + ax^\ell + \cdots$ and $x + bx^m + \cdots$, are conjugate over Nott($\mathbb{F}_p$) if and only if $a = b$ and $\ell = m$. In [10], the results of [5] are generalized to all $d \geq 1$ via local-class-field-theoretic methods that associate to torsion elements of Nott($\mathbb{F}_p$) certain characters on $1 + x\mathbb{F}_p[\![x]\!]$, and explicit elements of any order are exhibited.

Corollary 3.18. *Suppose $p = 2$. Then $\bar{w}(x)$ is conjugate over $\mathcal{G}_0(\mathbb{F}_p)$ to $\sum_{i=1}^{\infty} x^i$.*

Proof. This follows directly from [5, Proposition 3.3]. □

4. Proof of main result

Recall that $\{\pi_n\}$ is a fixed f-consistent sequence, $\mathfrak{w} \in \mathfrak{G}$ is an automorphism of order e, and $\rho_n = \mathfrak{w}(\pi_n)$ is f-consistent as well. The proof of the main result will rely on the relationship between the valuation of $\rho_n - g(\pi_n)$ for some $g \in \mathcal{G}_0(\mathbb{Z}_p)$ and the extent to which the series g commutes with f. We explore that relation in more detail in the next three lemmas. Write $f(x) = \sum a_i x^i$.

Lemma 4.1. *Suppose $g \in \mathcal{S}_0(\mathbb{Z}_p)$ with $f \circ g \equiv g \circ f \mod x^{k+1}$ for some $k > 0$. Suppose further that, for some $n > 0$, $\rho_n \equiv g(\pi_n) + c\pi_n^m \mod \pi_n^{m+1}$, where $c \in \mathbb{Z}_p^\times$ and $m \neq p^{n-1}$. Then $mp \geq \min\{v_{K_n}(\rho_{n-1} - g(\pi_{n-1})), k+1\}$. The inequality is strict if $v_{K_n}(a_p\pi_n^{mp}) > v_{K_n}(a_1\pi_n^m)$.*

Proof. Write $\rho_n = g(\pi_n) + c\pi_n^m + D\pi_n^{m+1}$ for some $D \in \mathbb{Z}_p[\![\pi_n]\!]$. Then

$$\begin{aligned} f(\rho_n) &= \sum_{i=1}^{\infty} a_i(g(\pi_n) + c\pi_n^m + D\pi_n^{m+1})^i \\ &= f(g(\pi_n)) + a_1 c\pi_n^m + a_p(c\pi_n^m)^p + D_1 p\pi_n^{m+1} + D_2(\pi_n^{m+1})^p \end{aligned}$$

for some $D_1, D_2 \in \mathbb{Z}_p[\![\pi_n]\!]$. Since $m \neq p^{n-1}$, then

$$p^{n-1}(p-1) + m = v_{K_n}(a_1 c\pi_n^m) \neq v_{K_n}(a_p(c\pi_n^m)^p) = mp$$

and so $v_{K_n}(f(\rho_n) - f(g(\pi_n))) = \min\{v_{K_n}(a_1 c\pi_n^m), v_{K_n}(a_p(c\pi_n^m)^p)\}$. But $f(\rho_n) - f(g(\pi_n)) = \rho_{n-1} - g(\pi_{n-1}) + M\pi_n^{k+1}$ for some $M \in \mathbb{Z}_p[\![\pi_n]\!]$. Therefore,

$$\begin{aligned} mp &\geq \min\{v_{K_n}(a_1 c\pi_n^m), v_{K_n}(a_p(c\pi_n^m)^p)\} \\ &= v_{K_n}(f(\rho_n) - f(g(\pi_n))) \\ &= v_{K_n}(\rho_{n-1} - g(\pi_{n-1}) + M\pi_n^{k+1}) \\ &\geq \min\{v_{K_n}(\rho_{n-1} - g(\pi_{n-1})), k+1\} \end{aligned} \tag{4.1}$$

Finally, if $v_{K_n}(a_p\pi_n^{mp}) > v_{K_n}(a_1\pi_n^m)$ then (4.1) is a strict inequality. □

Lemma 4.2. *Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Suppose $g \in \mathcal{G}_0(\mathbb{Z}_p)$. For each $c \in \mathbb{Z}_p^\times$ and $n \geq \delta$ there exists a unique integer $1 \leq j \leq p-1$ depending on $\bar{c}$, $\overline{g'(0)}$, and n such that $g \circ u^{\circ jp^{n-\delta}}(\pi_{n+1}) \equiv g(\pi_{n+1}) - c\pi_{n+1}^{p^n} \mod \pi_{n+1}^{p^n+1}$.*

Proof. By Proposition 2.6, $\operatorname{ord}_x(\bar{u}^{\circ p^{n-\delta}}(x) - x) = p^n$. Write $u^{\circ p^{n-\delta}}(x) - x = \sum_{i=1}^{\infty} b_i x^i$. Thus, $b_{p^n} \in \mathbb{Z}_p^\times$, and if $1 \leq i < p^n$ then $v_{K_{n+1}}(b_i \pi_{n+1}^i) \geq p^n(p-1) + i > p^n$. So $u^{\circ p^{n-\delta}}(\pi_{n+1}) \equiv \pi_{n+1} + b_{p^n}\pi_{n+1}^{p^n} \mod \pi_{n+1}^{p^n+1}$. A direct computation then shows $u^{\circ jp^{n-\delta}}(\pi_{n+1}) \equiv \pi_{n+1} + jb_{p^n}\pi_{n+1}^{p^n} \mod \pi_{n+1}^{p^n+1}$. So the proof is completed by solving for j in $jb_{p^n}g'(0) \equiv -c \mod p$. □

Lemma 4.3. *Suppose $h \in \mathcal{G}_0(\mathbb{Z}_p)$ such that $h'(0) = \zeta_{p-1}$ if $p > 2$ and $\bar{h}(x) \equiv x + x^2 \mod x^3$ if $p = 2$. If $f \circ h(x) - h \circ f(x) \equiv 0 \mod x^{k+1}$, then there exists $\ell \in \mathbb{Z}_p$ such that $v_{K_n}(\rho_n - h \circ u^{\circ \ell}(\pi_n)) \geq (k+1)/p$ for all n. The inequality is strict if $v_{K_n}(a_p \pi_n^{mp}) > v_{K_n}(a_1 \pi_n^m)$. Moreover, $v_{K_n}(\rho_n - h \circ u^{\circ \ell}(\pi_n)) \neq p^{n-1}$.*

Proof. We will construct a Cauchy sequence of integers $\{\ell_n\}$ for which $v_{K_s}(\rho_s - h \circ u^{\circ \ell_n}(\pi_s)) \geq (k+1)/p$ whenever $s \leq n$.

Let $\ell_1 = 0$. If $\rho_1 = h(\pi_1)$ the result follows trivially. If not, write $\rho_1 \equiv h(\pi_1) + c_{m,1}\pi_1^m \mod \pi_1^{m+1}$ for some $c_{m,1} \in \mathbb{Z}_p^\times$. Note that $m > 1 = p^0$ by Lemma 2.2 and so $p - 1 + m < mp$. Therefore, by Lemma 4.1, $mp > \min\{v_{K_1}(0), k+1\} = k+1$.

If $p = 2$, let $\ell_2 = 0$ as well. The result follows trivially if $\rho_2 = h(\pi_2)$. Otherwise, write $\rho_2 \equiv h(\pi_2) + c_{m,2}\pi_2^m \mod \pi_2^{m+1}$ for some $c_{m,2} \in \mathbb{Z}_2^\times$. Note that $m > 2$ by Corollary 3.13, and so $2(2-1) + m < 2m$. Therefore, by Lemma 4.1, $2m > \min\{v_{K_2}(\rho_1 - h(\pi_1)), k+1\} = \min\{2v_{K_1}(\rho_1 - h(\pi_1)), k+1\} = k+1$.

Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Suppose that for some $n \geq \delta$ there exists an integer ℓ_n for which $v_{K_s}(\rho_s - h \circ u^{\circ \ell_n}(\pi_s)) \geq (k+1)/p$ whenever $s \leq n$. If $\rho_{n+1} - h \circ u^{\circ \ell_n}(\pi_{n+1}) \equiv c\pi_{n+1}^{p^n} \mod \pi_{n+1}^{p^n+1}$ for some $c \in \mathbb{Z}_p^\times$, then by Lemma 4.2 there exists a $1 \leq j_{n+1} \leq p-1$ such that $h \circ u^{\circ \ell_n} \circ u^{\circ j_{n+1}p^{n-\delta}}(\pi_{n+1}) \equiv h \circ u^{\circ \ell_n}(\pi_{n+1}) - c\pi_{n+1}^{p^n} \mod \pi_{n+1}^{p^n+1}$. If on the other hand $v_{K_{n+1}}(\rho_{n+1} - h \circ u^{\circ \ell_n}(\pi_{n+1})) \neq p^n$, let $j_{n+1} = 0$. Let $\ell_{n+1} = \ell_n + j_{n+1}p^{n-\delta}$. If $\rho_{n+1} = h \circ u^{\circ \ell_{n+1}}(\pi_{n+1})$ then the result follows trivially. Otherwise, write $\rho_{n+1} - h \circ u^{\circ \ell_{n+1}}(\pi_{n+1}) \equiv c_{m,n+1}\pi_{n+1}^m \mod \pi_{n+1}^{m+1}$ for some $c_{m,n+1} \in \mathbb{Z}_p^\times$. Observe that if $s < n+1$, then $u^{\circ p^{n-\delta}}(\pi_s) = \pi_s$ by Proposition 2.6, so that $u^{\circ \ell_{n+1}}(\pi_s) = u^{\circ \ell_n}(\pi_s)$. The choice of j_{n+1} guarantees that $m \neq p^n$. Therefore, by Lemma 4.1, $mp \geq \min\{v_{K_{n+1}}(\rho_n - h \circ u^{\circ \ell_{n+1}}(\pi_n)), k+1\} = \min\{v_{K_{n+1}}(\rho_n - h \circ u^{\circ \ell_n}(\pi_n)), k+1\} = \min\{pv_{K_n}(\rho_n - h \circ u^{\circ \ell_n}(\pi_n)), k+1\} = k+1$, and the inequality is strict if $v_{K_{n+1}}(a_p \pi_{n+1}^{mp}) > v_{K_{n+1}}(a_1 \pi_{n+1}^m)$. □

We are now ready to complete the proof of Theorem 1.2. Recall from Remark 1.3 that if ζ_e is a primitive e^{th} root of unity, then $z(x) = \sum_{i=1}^{\infty} d_i x^i = [\zeta_e]_f(x) = L_f^{\circ -1}(\zeta_e L_f(x)) \in \mathcal{G}_0(\mathbb{Q}_p)$ is the unique e-torsion series with linear coefficient $d_1 = \zeta_e$ that commutes with f and u. Let $z_k(x) = \sum_{i=1}^{k} d_i x^i$ and continue to write $f(x) = \sum_{i=1}^{\infty} a_i x^i$. Clearly, $z_1(x) = \zeta_e x \in \mathcal{G}_0(\mathbb{Z}_p)$ and $z_1 \circ f \equiv f \circ z_1 \mod x^2$. Moreover, if $p = 2$ and $z_2(x) = -x + d_2 x^2$, then $f \circ z_2 \equiv z_2 \circ f \mod x^3$ implies $d_2 = 2a_2/(a_1^2 - a_1) \in \mathbb{Z}_2^{\times}$.

The proof of our main result, that $z \in \mathcal{G}_0(\mathbb{Z}_p)$, will proceed inductively. As before, let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Suppose for some $k \geq \delta$ that $z_k \in \mathcal{G}_0(\mathbb{Z}_p)$ and $z_k \circ f \equiv f \circ z_k \mod x^{k+1}$. For $z_{k+1}(x) = z_k(x) + d_{k+1}x^{k+1}$ to commute with $f(x) \mod x^{k+2}$, we must have

$$d_{k+1}(a_1^{k+1} - a_1)x^{k+1} \equiv f \circ z_k(x) - z_k \circ f(x) \mod x^{k+2}$$

Therefore, our proof will be completed once we show that $\bar{f} \circ \bar{z}_k(x) - \bar{z}_k \circ \bar{f}(x) \equiv 0 \mod x^{k+2}$, which we do next.

Proposition 4.4. *Let $\delta = 1$ if $p > 2$ and $\delta = 2$ if $p = 2$. Suppose $z_k \in \mathcal{G}_0(\mathbb{Z}_p)$ with $z_k'(0) = \zeta_e$ for some $k \geq \delta$. If $p = 2$, suppose also that $\bar{z}_2(x) = x + x^2$. If $f \circ z_k(x) - z_k \circ f(x) \equiv 0 \mod x^{k+1}$ then $\bar{f} \circ \bar{z}_k(x) - \bar{z}_k \circ \bar{f}(x) \equiv 0 \mod x^{k+2}$.*

Proof. Write $f \circ z_k(x) - z_k \circ f(x) \equiv dx^{k+1} \mod x^{k+2}$ for some $d \in \mathbb{Z}_p$.

If $p \nmid k+1$ then $d \in p\mathbb{Z}_p$ by [9, Corollary 6.2.1].

If $p \mid k+1$, let $m = (k+1)/p$. By Lemma 4.3, there exists $\ell \in \mathbb{Z}_p$ such that, for all n, $\rho_n \equiv z_k \circ u^{\circ \ell}(\pi_n) + c_n \pi_n^m \mod \pi_n^{m+1}$, and if $m = p^{n-1}$ then $c_n = 0$.

Let $N = \min\{n \mid v_{K_n}(a_1 \pi_n^m) > v_{K_n}(a_p \pi_n^{mp})\}$; note that $N \geq 2$. By Lemma 4.3 again, $c_{N-1} = 0$. Moreover, for all $n \geq N$, we have mod π_n^{mp+1}:

$$\begin{aligned}
\rho_{n-1} &\equiv z_k \circ u^{\circ \ell}(\pi_{n-1}) + c_{n-1}\pi_{n-1}^m \\
&= z_k \circ u^{\circ \ell}(f(\pi_n)) + c_{n-1} f(\pi_n)^m \\
&\equiv z_k \circ u^{\circ \ell}(f(\pi_n)) + c_{n-1}(a_p \pi_n^p)^m
\end{aligned}$$

and

$$\begin{aligned}
\rho_{n-1} &= f(\rho_n) \\
&\equiv f(z_k \circ u^{\circ \ell}(\pi_n) + c_n \pi_n^m) \\
&\equiv f(z_k \circ u^{\circ \ell}(\pi_n)) + a_p (c_n \pi_n^m)^p
\end{aligned}$$

Therefore, $f(z_k \circ u^{\circ \ell}(\pi_n)) + a_p(c_n \pi_n^m)^p \equiv z_k \circ u^{\circ \ell}(f(\pi_n)) + c_{n-1}(a_p \pi_n^p)^m \mod \pi_n^{pm+1}$, and so

$$c_n \equiv \frac{z_k \circ u^{\circ \ell}(f(\pi_n)) - f(z_k \circ u^{\circ \ell}(\pi_n))}{a_p \pi_n^{mp}} + c_{n-1} a_p^{m-1} \mod \pi_n$$

Observe that $z_k \circ u^{\circ\ell} \circ f(x) - f \circ z_k \circ u^{\circ\ell}(x) \equiv 0 \mod x^{mp}$, and so the fraction $\alpha = \dfrac{z_k \circ u^{\circ\ell}(f(\pi_n)) - f(z_k \circ u^{\circ\ell}(\pi_n))}{a_p \pi_n^{mp}}$ is independent of π_n mod π_n. Iterating the congruence $c_n \equiv \alpha + c_{n-1} a_p^{m-1} \mod \pi_n$, we get $c_n \equiv \alpha \sum_{i=N}^{n} a_p^{(m-1)(n-i)} \mod \pi_n$. But $\sum_{i=N}^{n} a_p^{(m-1)(n-i)} \equiv 0 \mod p$ for infinitely many n, and so too $c_n \equiv 0 \mod p$ and $\rho_n \equiv z_k \circ u^{\circ\ell}(\pi_n) \mod \pi_n^{m+1}$ for infinitely many n. Thus by Lemma 3.4, $\bar{w}(x) \equiv \bar{z}_k \circ \bar{u}^{\circ\ell}(x) \mod x^{m+1}$.

Now recall that $\bar{w}$ commutes with φ by Corollary 3.17. So $0 = \varphi \circ \bar{w}(x) - \bar{w} \circ \varphi(x) \equiv \varphi \circ \bar{z}_k \circ \bar{u}^{\circ\ell}(x) - \bar{z}_k \circ \bar{u}^{\circ\ell} \circ \varphi(x) = \varphi \circ \bar{z}_k \circ \bar{u}^{\circ\ell}(x) - \bar{z}_k \circ \varphi(x) \circ \bar{u}^{\circ\ell} \mod x^{m+1}$. Thus $\varphi \circ \bar{z}_k(x) - \bar{z}_k \circ \varphi(x) \equiv 0 \mod x^{m+1}$, and so

$$0 \equiv \varphi \circ \bar{z}_k(x^p) - \bar{z}_k \circ \varphi(x^p) \mod x^{mp+1},$$

yielding our desired result since $mp = k + 1$ and $\varphi(x^p) = \bar{f}(x)$. □

Acknowledgments

The second author would like to thank David Pollack for reading a preliminary version these results and making valuable comments.

References

[1] R. Camina, *Subgroups of the Nottingham group.* J. Algebra **196** (1997), no. 1, 101–113.
[2] J.-M. Fontaine, J.-P. Wintenberger, *Le "corps des normes" de certaines extensions algébriques de corps locaux.* C. R. Acad. Sci. Paris **288** (1979), 367–370.
[3] J.-M. Fontaine, J.-P. Wintenberger, *Extensions algébriques et corps des normes des extensions APF des corps locaux.* C. R. Acad. Sci. Paris **288** (1979), 441–444.
[4] G. Klaas, C. R. Leedham-Green, W. Plesken, *Linear Pro-p-groups of Finite Width.* Lecture Notes in Mathematics 1674 (Springer-Verlag), 1997.
[5] B. Klopsch, *Automorphisms of the Nottingham group.* J. Algebra **223** (2000), no. 1, 37–56.
[6] N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions.* Springer, New York, 1977.
[7] F. Laubie, A. Movahhedi, A. Salinier, *Systèmes dynamiques non archimédiens et corps des normes.* Compos. Math. **132** (2002), 57–98.
[8] J. Lubin, *One-parameter formal Lie groups over $\mathfrak{P}$-adic integer rings.* Ann. Math. **80** (1964), 464–484.
[9] J. Lubin, *Nonarchimedean dynamical systems.* Compos. Math. **94** (1994), 321–346.
[10] J. Lubin *Torsion in the Nottingham group.* Bull. Lond. Math. Soc. **43** (2011), 547–560.
[11] J. Lubin, J. Tate, *Formal complex multiplication in local fields.* Ann. Math. **81** (1965), no. 2, 380–387.
[12] G. Sarkis, *Height one commuting dynamical systems over $\mathbb{Z}_p$.* Bull. Lond. Math. Soc. **42** (2010), no. 3, 381–387.
[13] S. Sen, *On automorphisms of local fields.* Ann. of Math. (2) **90** (1969), 33–46.
[14] J.-P. Serre, *Local Fields.* Springer, New York, 1979.
[15] J.-P. Wintenberger, *Extensions abéliennes et groupes dÕautomorphismes de corps locaux.* C.R. Acad. Sci. Paris **290** (1980), 201–203.

Ghassan Sarkis
Pomona College
610 North College Avenue
Claremont, CA 91711, USA
E-mail: ghassan.sarkis@pomona.edu

Joel Specter
Northwestern University
2033 Sheridan Road
Evanston, IL 60208, USA
E-mail: jspecter@math.northwestern.edu