Compositio Mathematica **124:** 123–136, 2000.

Formal Flows on the Non-Archimedean Open Unit Disk

JONATHAN LUBIN
Department of Mathematics, Brown University, Box 1917, Providence, RI 02912, U.S.A.

(Received: 14 December 1998; in final form: 23 November 1999)

Abstract. This paper deals with group actions of one-dimensional formal groups defined over the ring of integers in a finite extension of the p-adic field, where the space acted upon is the maximal ideal in the ring of integers of an algebraic closure of the p-adic field. Given a formal group F as above, a formal flow is a series $\Phi(t, x)$ satisfying the conditions $\Phi(0, x) = x$ and $\Phi\big(F(s, t), x\big) = \Phi\big(s, \Phi(t, x)\big)$. With this definition, any formal group will act on the disk by left translation, but this paper constructs flows Φ with any specified divisor of fixed points, where a point ξ of the open unit disk is a fixed point of order $\leqslant n$ if $(x - \xi)^n \big| \big(\Phi(t, x) - x\big)$. Furthermore, if γ is an analytic automorphism of the open unit disk with only finitely many periodic points, then there is a flow Φ, an element α of the maximal ideal of the ring of constants, and an integer m such that the m-fold iteration of $\gamma(x)$ is equal to $\Phi(\alpha, x)$. All the formal flows constructed here are actions of the additive formal group on the unit disk. Indeed, if the divisor of fixed points of a formal flow is of degree at least two, then the formal group involved must become isomorphic to the additive group when the base is extended to the residue field of the constant ring.

Mathematics Subject Classifications (2000): 11S99, 30D05, 54H20.

Key words: p-adic analysis, algebraic dynamics, non-Archimedean dynamical systems.

This paper extends the investigations begun in [L] in which iterations of analytic transformations of the p-adic open unit disk $\bar{\mathfrak{m}}$ were studied. In both this paper and the preceding, $\bar{\mathfrak{m}}$ denotes the set of elements z of a fixed algebraic closure of $\mathbb{Q}_p$ for which $|z| < 1$, and the transformations to be considered all are defined over a finite extension k of $\mathbb{Q}_p$, with ring of integers $\mathfrak{o}$ and maximal ideal $\mathfrak{m}$. The difference between the two papers is principally that the first dealt only with transformations of $\bar{\mathfrak{m}}$ with a fixed point, and concentrated on those that have infinitely many preperiodic points; this paper emphasizes instead transformations with no fixed point and those with only finitely many preperiodic points. Another distinction between the two papers is that this one concentrates on continuous, and indeed analytic, families of transformations of $\bar{\mathfrak{m}}$, while most of the transformations dealt with in the previous paper could never be members of analytic families. The study of these maps leads naturally to investigation of group actions by formal groups on the p-adic open unit disk: these are the 'flows' of the title of the paper.

This paper could as well have been entitled 'p-adic time in non-Archimedean dynamics': the work here was stimulated in great degree by ideas of D. Arrowsmith and F. Vivaldi's paper [AV]. The other principal sources of inspiration have been the thesis of M. Zieve [Z] and numerous conversations with their author, when he was visiting Brown University.

One of the main results of this paper is Theorem 3.2, according to which an invertible transformation φ of the open unit disk having only finitely many periodic points will have, belonging to it, a flow obtained by exponentiating a suitable scalar multiple of the derivation D_φ that is associated to the Lie logarithm $\widetilde{\varphi}$ of φ. The way that the results of this paper relate to those of [L] is as follows. We denote the ring of integers of k by $\mathfrak{o}$, and its maximal ideal by $\mathfrak{m}$. For a series $f(z) \in \mathfrak{o}[[z]]$ with $f'(0) \in \mathfrak{m}$, the only iterates of f that we expect to give any meaning to are $f^{\circ n}$ for $n \in \mathbb{N}$; these maps f are noninvertible, and have a unique fixed point in $\bar{\mathfrak{m}}$. (I use here the notation in which $f^{\circ 1} = f$ and $f^{\circ(m+n)} = f^{\circ m} \circ f^{\circ n}$.) For an invertible transformation $u(z)$ of the open unit disk, $u^{\circ n}$ makes sense when $n \in \mathbb{Z}$, but if $u'(0) \in 1 + \mathfrak{m}$, the p^m-iterates of u approach the identity, so we may define $u^{\circ \alpha}$ for $\alpha \in \mathbb{Z}_p$. If, moreover, u has only finitely many periodic points, then Theorem 3.2 will show that we may define also $u^{\circ p^m t}$ for a fixed m but with t allowed to run through $\bar{\mathfrak{m}}$, and the coefficients of the resulting series are themselves power series in t with coefficients in $\mathfrak{o}$.

The foundational background necessary for studying this situation is slightly more extensive than required for [L]. So after a short review of notations in Section 0, there is an outline given of the requisite p-adic analysis in Section 1. The new material of the paper begins properly in Section 2.

0. Notational Conventions and Elementary Analytic Considerations.

For the full list of notations used here, we refer the reader back to [L], Sections 0 and 8. We use k to denote a finite algebraic extension field of the field $\mathbb{Q}_p$ of p-adic numbers; the integral closure in k of $\mathbb{Z}_p$ will be denoted $\mathfrak{o}$ and its maximal ideal $\mathfrak{m}$. We define $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$ to be the set of all series $u(x)$ in $\mathfrak{o}[[x]]$ with $u(0) \in \mathfrak{m}$ and $u'(0) \notin \mathfrak{m}$. This is a necessary and sufficient condition for u to be an $\mathfrak{o}$-analytic automorphism of the p-adic open unit disk $\bar{\mathfrak{m}} := \{z \in \overline{k} : |z| < 1\}$, where $\overline{k}$ is an algebraic closure of k and $|*|$ is the unique extension of the p-adic absolute value to $\overline{k}$. Thus $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$ is a group under composition of series. In contrast to the situation with the subgroup $\mathcal{G}_0(\mathfrak{o})$ of all such series with constant term 0, substitution and calculation of the inverse are analytic rather than algebraic operations. That is, in $\mathcal{G}_0(\mathfrak{o})$ degree-by-degree methods may be used for calculating both $u \circ w$ and u^{-1}, whereas in $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$ the calculation of $u \circ w$ involves a limiting process, and to verify the existence of u^{-1} or to calculate it requires the application of Hensel's Lemma or the Weierstrass Preparation Theorem.

Instead of using the (multiplicative) p-adic absolute value, we use its negative logarithm v, the additive valuation normalized so that $v(p) = 1$.

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

As in [L], we use the notation $f^{\circ n}$ for the n-fold iteration of f, but in the case when $n = -1$ we will usually denote the inverse mapping of f, if it exists, simply as f^{-1}.

We recall the definition, if $\rho > 0$, of the valuation w_ρ on the ring of power series $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k$: if $f(x) = \sum a_i x^i$, then $w_\rho(f) = \min_i\big(v(a_i) + i\rho\big)$. We define:

$$\mathbf{A}_{(\rho)} = \mathbf{A}_{(\rho)k} := \text{completion of } \mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k \text{ with respect to } w_\rho$$
$$\mathbf{A} = \mathbf{A}_k := \bigcap_{\rho > 0} \mathbf{A}_{(\rho)}.$$

Another way of saying the same thing is that $\mathbf{A}$ is the completion of $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k$ in the topology of uniform convergence on proper subdisks of $\bar{\mathfrak{m}}$. The elements of $\mathbf{A}$ are precisely the series $\sum a_i x^i \in k[[x]]$ for which $\liminf_i\big(v(a_i)/i\big) \geqslant 0$.

To make clear the relationships among these concepts, we state without proof the following:

PROPOSITION 0.1. *Let $\rho > 0$ and let $\{f_j\}$ and F be series in $\mathbf{A}_{(\rho)}$. Then $f_j \to F$ uniformly on the disk $\{\alpha \in \bar{\mathfrak{m}} : v(\alpha) > \rho\}$ if and only if $f_j \to F$ in the topology defined by w_ρ.*

PROPOSITION 0.2. *Let $\rho > 0$ and $f(x) = \sum_i a_i x^i \in k[[x]]$. Then $f \in \mathbf{A}_{(\rho)}$ if and only if $\lim_i\big(v(a_i) + i\rho\big) = \infty$. In particular, if $\rho > \rho' > 0$ and $w_{\rho'}(f) > -\infty$, then $f \in \mathbf{A}_{(\rho)}$.*

PROPOSITION 0.3. Let $\rho > \rho' > 0$. Then $\mathbf{A}_{(\rho')} \subset \mathbf{A}_{(\rho)}$, and if $\lim_j f_j = F$ with respect to $w_{\rho'}$, then $\lim_j f_j = F$ with respect to w_ρ.

1. Analytic Automorphisms of the Open Unit Disk

Let $f(x) \in \mathbf{A}_k$, with the property that for every $\alpha \in \bar{\mathfrak{m}}$, the equation $f(x) = \alpha$ has precisely one solution in $\bar{\mathfrak{m}}$. An examination of the Newton polygon of $f(x) - \alpha$ for such α shows that the constant term of f must be in $\mathfrak{m}$, the first-degree coefficient of f must be in $\mathfrak{o}^\times$, the unit-group of $\mathfrak{o}$, and all other coefficients must be in $\mathfrak{o}$. Thus $f \in \mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$, and it has not merely a set-theoretical but an analytic inverse.

There are elements of $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$ with no periodic points at all. For instance, if $F(x, y) \in \mathfrak{o}[[x, y]]$ is a one-dimensional formal group and $\alpha \in \mathfrak{m}$ is not a torsion point of F, then the series $u(x) = F(x, \alpha) \in \mathfrak{o}[[x]]$ has no periodic points. We will see later on that this is by no means the only way to find invertible series without periodic points.

We now define an important subgroup of $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$, which will turn out to be the largest subgroup that is pro-p-torsion. Let us call $v: \mathfrak{o} \to \kappa = \mathfrak{o}/\mathfrak{m}$ the canonical map to the residue field; then the map $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o}) \to \kappa^\times$ by $\varphi(x) \mapsto v\big(\varphi'(0)\big)$ is a homomorphism of groups, and we call its kernel $\mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$. The series $F(x, \alpha)$ mentioned above is certainly of this type, since $F(x, \alpha) \equiv x \pmod{\mathfrak{m}}$. If we denote the identity transformation of the unit disk by $\mathrm{id}(x) = x$, then we will see that the p-power iterates of any series in $\mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$ approach id uniformly on proper subdisks of $\bar{\mathfrak{m}}$.

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

LEMMA 1.1. *If* $u(x) \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$, *with* $u(x) - x = \epsilon(x)$ *and* $w_\rho(\epsilon) = \lambda$ *for* $0 < \rho < \lambda$, *then* $w_\rho\big(u^{\circ p}(x) - x - p\epsilon(x)\big) \geqslant 2\lambda - \rho$.

We show first that if $u_i(x) = x + \epsilon_i(x) \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$, with $w_\rho(\epsilon_i) \geqslant \lambda$ for $i = 1, 2$, then $u_1\big(u_2(x)\big) = x + \epsilon_1(x) + \epsilon_2(x) + \delta(x)$ with $w_\rho(\delta) \geqslant 2\lambda - \rho$. Indeed, we have

$$\begin{aligned} u_1\big(u_2(x)\big) &= x + \epsilon_2(x) + \epsilon_1\big(x + \epsilon_2(x)\big) \\ &= x + \epsilon_2(x) + \epsilon_1(x) + \epsilon_1'(x)\epsilon_2(x) + g(x)\epsilon_2(x)^2 \end{aligned}$$

for some series $g(x) \in \mathfrak{o}[[x]]$. Since $w_\rho(\epsilon_1') \geqslant w_\rho(\epsilon_1) - \rho$, the claim is proved. Under the hypothesis that $\rho < \lambda$, we have $w_\rho\big(u_1 \circ u_2(x) - x\big) \geqslant \lambda$, so we see, for each n, that if all n of the functions being composed are equal to $u(x) = x + \epsilon(x)$, then $w_\rho\big(u^{\circ n}(x) - x - n\epsilon(x)\big) \geqslant 2\lambda - \rho$.

COROLLARY 1.1.1. *If* $u \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$, *then in* $\mathbf{A}$, $\lim_n u^{\circ p^n} = \mathrm{id}$.

For any $u \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$, the Weierstrass degree of $u(x) - x$ (the first degree in which a unit coefficient occurs) is at least 2, so that $w_\rho\big(u(x) - x\big) \geqslant \min(2\rho, 1/e)$, where e is the ramification index of k over $\mathbb{Q}_p$. So by restricting our choice of ρ to values less than $1/2e$, we see that in $\mathbf{A}$, the sequence of p-power iterates of u has $w_\rho\big(u^{\circ p^n} - \mathrm{id}\big) \to \infty$.

Because of the preceding, we will call series in $\mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$ *analytically unipotent*.

COROLLARY 1.1.2. *If* $u \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$, *then the homomorphism* $\mathbb{Z} \to \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$ *by* $n \mapsto u^{\circ n}$ *is continuous when* $\mathbb{Z}$ *has the p-adic topology, and hence extends to* $\mathbb{Z}_p \to \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$. *In particular, if* $p \nmid n$, $u^{\circ 1/n}$ *is defined, and hence any finite orbit in* $\bar{\mathfrak{m}}$ *under the action of u is of cardinality a power of p.*

The preceding Lemma and Corollaries correspond, in the slightly more difficult situation that we are now dealing with, to Proposition 4.1 of [L]. The fact that $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})/\mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o}) \cong \kappa^\times$, a finite group of order prime to p, justifies the claim made earlier in this section that $\mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$ is the greatest subgroup of $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$ that is pro-p-torsion.

We now construct the *Lie logarithm* $\widetilde{u}$ of a series $u \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$: we define

$$\widetilde{u}(x) = \lim_{n \to \infty} \frac{u^{\circ p^n}(x) - x}{p^n}.$$

It still remains to show that the sequence is convergent in $\mathbf{A}$. As before, we fix a positive ρ and show that the limit exists with respect to the valuation w_ρ on $\mathbf{A}$.

PROPOSITION 1.2. *Let* $u(x) \in \mathcal{G}_{\mathfrak{m}}^1(\mathfrak{o})$. *Then* $\lim_n \big(u^{\circ p^n} - \mathrm{id}\big)/p^n$ *exists as an element of* $\mathbf{A}_k$.

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

In [L], the proof was accomplished by showing that a coefficientwise limit existed, and then verifying that this limit was an element of $\mathbf{A}_k$. The proof here is much more direct and natural, but the expression of the Lie logarithm as an infinite product, which was a byproduct of the proof in [L], will need to be verified separately.

Let ρ be fixed, $0 < \rho < 1$. By Lemma 1.1, we may take m so that $w_\rho\big(u^{\circ p^m} - \mathrm{id}\big) = \lambda \geqslant 2$. We will show, for $i \geqslant 1$, that

$$w_\rho\left(\frac{u^{\circ p^{m+i}} - \mathrm{id}}{p^i} \quad - \quad \frac{u^{\circ p^{m+i-1}} - \mathrm{id}}{p^{i-1}}\right) \to \infty.$$

We put $\alpha_i := u^{\circ p^{m+i}} - \mathrm{id}$, so that $w_\rho(\alpha_0) = \lambda$ and since $\rho < \lambda - 1$, we get $w_\rho(\alpha_i) \geqslant \lambda + i$ by using Lemma 1.1. We need $w_\rho\big(\alpha_i/p^i - \alpha_{i-1}/p^{i-1}\big) \to \infty$. To see this, we set $\epsilon_i := \alpha_i - p\alpha_{i-1}$ for $i \geqslant 1$, and again by Lemma 1.1, we have $w_\rho(\epsilon_i) \geqslant 2w_\rho(\alpha_{i-1}) - \rho = 2(\lambda + i - 1) - \rho$. Since $\alpha_i/p^i - \alpha_{i-1}/p^{i-1} = p^{-i}\epsilon_i$, the desired result follows and the proof is done.

We need to show that, just as in the more special situation of [L], the roots of the Lie logarithm of u are the periodic points of u.

LEMMA 1.3. *Let $g(x) \in \mathfrak{o}[[x]]$, with $g(0) \in \mathfrak{m}$, and let $n \geqslant 1$. Then in $\mathfrak{o}[[x]]$, $g(x) - x$ divides $g^{\circ n}(x) - x$.*

PROPOSITION 1.4. *Let $u(x) \in \mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$, and let $\Phi_n = (u^{p^n} - \mathrm{id})/(u^{p^{n-1}} - \mathrm{id}) \in \mathfrak{o}[[x]]$. Then $\widetilde{u}$ has the convergent infinite product expansion*

$$\widetilde{u}(x) = \big(u(x) - x\big) \prod_{n=1}^{\infty} \frac{\Phi_n(x)}{p}.$$

As in the proof of Proposition 4.3 of [**L**], we need only show that $\lim_n \Phi_n = p$. Using the notation of Proposition 1.2, we have $\Phi_n = \alpha_{n-m}/\alpha_{n-m-1} = p + \epsilon_{n-m}/\alpha_{n-m-1}$. This shows that $\epsilon_{n-m}/\alpha_{n-m-1} \in \mathfrak{o}[[x]]$, and the computation of w_ρ-values in the previous Proposition shows that for $n > m$,

$$\begin{aligned} w_\rho(\Phi_n - p) &= w_\rho(\epsilon_{n-m}) - w_\rho(\alpha_{n-m-1}) \\ &\geqslant 2w_\rho(\alpha_{n-m-1}) - \rho - w_\rho(\alpha_{n-m-1}) \\ &\geqslant \lambda + n - m - 1 - \rho, \end{aligned}$$

which is enough to complete the proof.

The reader should note that in the product expansion for $\widetilde{u}$, the factor outside the product sign accounts for the fixed points of u, and the factor Φ_n accounts for the periodic points of u of period precisely p^n.

In this paper we will be interested principally in transformations u of the open unit disk with only finitely many periodic points, i.e. those for which $\widetilde{u}$ has only finitely many roots. When this is the case, there is a constant $a \in k$, a Weierstrass polynomial $P(x)$ (monic, with all roots in $\bar{\mathfrak{m}}$) in $\mathfrak{o}[x]$, and $U(x) \in \mathfrak{o}[[x]]^\times$ such that $\widetilde{u} = aPU$. In

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

particular, if u has no periodic points, then the Lie logarithm of u is a constant times a unit $\mathfrak{o}$-series. In any case, we will abuse language and call the polynomial P the *divisor of periodic points* of u.

Our principal aim for the rest of this section is to show that if two series in $\mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$, say u and w, have the same Lie logarithm, then there is a power q of p such that $u^{\circ q} = w^{\circ q}$. To do this we start with a fact about the commutator of two series in $\mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$.

LEMMA 1.5. *Let* $u, w \in \mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$ *with* $u(x) = x + \lambda U(x)$, $w(x) = x + \mu W(x)$ *for* $\lambda, \mu \in \mathfrak{m}$ *and* $U, W \in \mathfrak{o}[[x]]$. *Then*

$$(u^{-1} \circ w^{-1} \circ u \circ w)(x) \equiv x + \lambda\mu\big(U'(x)W(x) - U(x)W'(x)\big)(\mathrm{mod}\ \lambda\mu\mathfrak{m}[[x]]).$$

We omit the proof, which is perfectly straightforward and predictable. The Lemma is particularly useful for seeing how a change in u induces a change in $\widetilde{u}$.

COROLLARY 1.5.1. *Under the hypotheses of Lemma* 1.5, *u and w commute modulo $\lambda\mu$, and in particular* $(u \circ w)^{\circ p} \equiv u^{\circ p} \circ w^{\circ p} (\mathrm{mod}\ \lambda\mu\mathfrak{o})$.

For the following Proposition, we use the p-adic (in other words, $\mathfrak{m}$-adic) valuation on $\mathfrak{o}[[x]]$, which corresponds to the topology of uniform convergence on the whole open disk. We say that $v\big(f(x)\big) = h$ if $f(x) = ag(x)$ where $a \in \mathfrak{o}$ with $v(a) = h$ and $g \in \mathfrak{o}[[x]]$ is a series with at least one unit coefficient: in other words, the Weierstrass degree of g is finite. Recall that v is normalized so that $v(p) = 1$.

PROPOSITION 1.6. *Let* $u, w \in \mathfrak{o}[[x]]$ *be series such that* $v(u - \mathrm{id}) \geqslant 2$ *and* $v(w - \mathrm{id}) \geqslant 2$. *Then* $v(u - w) = v(u \circ w^{-1} - \mathrm{id}) = v(u^{\circ p} - w^{\circ p}) - 1 = v(\widetilde{u} - \widetilde{w})$.

The first equality is immediate, having nothing to do with the special hypothesis on the closeness of u and w to the identity. We may assume without loss of generality that $v(u - \mathrm{id}) \leqslant v(w - \mathrm{id})$; let us suppose now that $u = \mathrm{id} + \lambda U$ and $u \circ w^{-1} = \mathrm{id} + \delta\Delta$, both U and Δ being series over $\mathfrak{o}$ of finite Weierstrass degree, and $\lambda, \delta \in p^2\mathfrak{o}$. We get:

$$\begin{aligned} u^{\circ p} \circ w^{\circ(-p)} &\equiv \big(u \circ w^{-1}\big)^{\circ p} (\mathrm{mod}\ \lambda\delta) \\ &\equiv \mathrm{id} + p\delta\Delta (\mathrm{mod}\ \delta^2), \end{aligned}$$

where the first congruence comes from Corollary 1.5.1 and the second comes from Lemma 4.2.1 of [L]. Having chosen u to be not closer to the identity than w, we can say that $\lambda | \delta$, and thus that $v\big(u^{\circ p} - w^{\circ p}\big) = v(p\delta)$, which verifies the second equality.

For the Lie logarithms,

$$\begin{aligned}\widetilde{u} - \widetilde{w} &= \lim_{n\to\infty}\left(\frac{u^{\circ p^n} - \mathrm{id}}{p^n} - \frac{w^{\circ p^n} - \mathrm{id}}{p^n}\right)\\ &= \lim_{n\to\infty}\frac{u^{\circ p^n} - w^{\circ p^n}}{p^n},\end{aligned}$$

and by our second equality, the approximants all have v-value equal to $v(u - w)$.

THEOREM 1.7. *Let $u, w \in \mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$ with $\widetilde{u} = \widetilde{w}$. Then there is n such that for $q = p^n$, we have $u^{\circ q} = w^{\circ q}$.*

The proof uses techniques developed in this paper and [L], dividing the proof into three cases depending on the nature of the fixed points of u, if any.

In the first case, $u(x) - x$ has a multiple root, which we may assume (after making a finite extension of k) to be at the origin, so that u has the form $x + a_1x^2 + a_2x^3 + \cdots$, what we called a unipotent series in [L]. The discussion at the end of Section 4 of [L] shows that $\widetilde{u}$ has the form $A_1x^2 + A_2x^3 + \cdots$ where each A_i is a polynomial expression in the a_j's that is isobaric of weight i, if each a_j is endowed with the weight j; and that A_i contains the monomial a_i with coefficient 1. The first few terms of $\widetilde{u}$ are

$$\begin{aligned}&\widetilde{\left(x + a_1x^2 + a_2x^3 + a_3x^4 + \cdots\right)}\\ &\quad = a_1x^2 + (a_2 - a_1^2)x^3 + (a_3 - 5a_1a_2/2 - 3a_1^3/2)x^4 + \cdots\end{aligned}$$

The form of $\widetilde{u}$ shows that $\widetilde{u}$ determines the unipotent series u completely. If $\widetilde{w} = \widetilde{u}$ then some p-power iterate of w has a fixed point of multiple order at 0 as well, so we may replace u and w by their iterates of this order, when w is now seen to be equal to u.

In the second case, $u(x) - x$ has a simple root, which we again may assume is at the origin, so $u(x) \equiv ax (\mathrm{mod}\ x^2$ with $a \neq 1$. In case a is a root of 1, a suitable p-power iterate of u will fall into the first case; otherwise, u is what was called in [L] a stable series, in which case we have the fundamental identity of Proposition 4.5 of [L] that $\widetilde{u}(x) = \log\big(u'(0)\big)\mathbf{L}_u(x)/\mathbf{L}_u'(x)$. But because the logarithm $\mathbf{L}_u$ of u has first-degree coefficient 1, and the characteristic of k is zero, this differential equation determines $\mathbf{L}_u$ completely. Thus if $\widetilde{w} = \widetilde{u}$, we have $w'(0) = \zeta u'(0)$ for ζ a p-power root of 1, and so for a suitable $q = p^n$, $w^{\circ q}$ and $u^{\circ q}$ have the same Lie logarithm, and thus the same logarithm, and because they have the same first-degree coefficient, they are equal.

The third case uses the machinery that we have developed in this paper so far. It is the case where $u(x) - x$ has no roots whatever. For $u(x) - x$ to have no roots in $\bar{\mathfrak{m}}$ it must be a constant times a unit series, and that constant will necessarily be in $\mathfrak{m}$, since the first-degree coefficient of $u(x) - x$ is in $\mathfrak{m}$. In other words, $u(x) - x \in \mathfrak{m}[[x]]$. Then a suitable p-power iterate of u has $v(u - \mathrm{id}) \geqslant 2$, and similarly for any given series w that has $\widetilde{w} = \widetilde{u}$, by Lemma 1.1 of this paper or Lemma 4.2.1 of [L]. But Proposition 1.6 says that these iterates of u and w are equal.

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

To speak more conceptually, the mapping $u \mapsto \widetilde{u}$ must surely be an analytic morphism from one infinite-dimensional p-adic Banach space to another, and a close study of the nature of this morphism would presumably prove the result easily and directly.

We close this section with a simple computation showing what the Lie logarithm is when $\varphi(x) = F(\alpha, x)$ for a formal group F defined over $\mathfrak{o}$ and α is in $\mathfrak{m}$, but not a torsion point of F. We use the notation $F_1(x, y)$ for $\frac{\partial}{\partial x} F(x, y)$, and $\mathbf{L}_F(x)$ for the the logarithm of F, which is the unique k-series for which $\mathbf{L}_F\big(F(x, y)\big) = \mathbf{L}_F(x) + \mathbf{L}_F(y)$ and $\mathbf{L}_F'(0) = 1$. Recall that $\mathbf{L}_F \in \mathbf{A}_k$ and that the roots of $\mathbf{L}_F$ in $\bar{\mathfrak{m}}$ are the torsion points of F.

EXAMPLE 1.8. Let $F(x, y) \in \mathfrak{o}[[x, y]]$ be a one-dimensional formal group, let $\alpha \in \mathfrak{m}$ be a nontorsion point of F, and let $\varphi(x) = F(a, x)$. Then $\widetilde{\varphi}(x) = F_1(0, x)\mathbf{L}_F(a)$.

Calling $[n]_F(x)$ the endomorphism of F corresponding to multiplication by n, we see that $\varphi^{\circ n}(x) = F\big([n]_F(\alpha), x\big)$. Calculating the Lie logarithm, we get

$$\begin{aligned}
\widetilde{\varphi}(x) &= \lim_n \frac{F\big([p^n](\alpha), x\big) - x}{p^n} \\
&= \lim_n \left(\frac{F\big([p^n](\alpha), x\big) - x}{[p^n](\alpha)} \cdot \frac{[p^n]_F(\alpha)}{p^n} \right) \\
&= \lim_{\epsilon \to 0} \frac{F\big(\epsilon, x\big) - F(0, x)}{\epsilon} \cdot \lim_n \frac{[p^n]_F(\alpha)}{p^n} \\
&= F_1(0, x) \cdot \mathbf{L}_F(\alpha)
\end{aligned}$$

2. Formal Flows

In this section we define formal flows and introduce some of their elementary properties.

DEFINITION. Let A be a commutative ring, and F a formal group law of dimension n defined over A. An m-tuple Φ of power series in $A[[t_1, \cdots, t_n, x_1, \cdots, x_m]]$ is a *formal action of F on formal affine m-space defined over A* if

(i) $\Phi(0, \mathbf{x}) = \mathbf{x}$; and
(ii) $\Phi\big(F(\mathbf{s}, \mathbf{t}), \mathbf{x}\big) = \Phi\big(\mathbf{s}, \Phi(\mathbf{t}, \mathbf{x})\big)$.

When m and n are both equal to 1, we will say simply that the pair (F, Φ) is a *formal flow on the formal affine line*, and when the base is the ring of integers $\mathfrak{o}$ in a finite

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

field extension of $\mathbb{Q}_p$, we will call (F, Φ) a *formal flow on the p-adic open unit disk* defined over $\mathfrak{o}$.

If F is an n-dimensional A-formal group and Φ is a formal action of F on formal affine m-space defined over A, and if R is a noetherian A-algebra with a complete topology defined by the powers of the ideal $I \subset R$, and if moreover J is a closed subideal of I, then $J^{\times n}$ has the structure of group defined by the group law F, often denoted $F(J)$, and this group acts on the set $J^{\times m}$, by the law

$$(\alpha_1, \cdots, \alpha_n) \star (\xi_1, \cdots, \xi_m) = \Phi(\alpha_1, \cdots, \alpha_n, \xi_1, \cdots, \xi_m).$$

We may specialize to the case where the ring A is the ring $\mathfrak{o}$ of local integers in a local field k, a finite extension of $\mathbb{Q}_p$, and where $I = J$ is the maximal ideal $\mathfrak{m}$ of $\mathfrak{o}$. But in this case, the set $\bar{\mathfrak{m}}^n$ has the structure of a group, furnished by F, since each finite subset of $\bar{\mathfrak{m}}$ is contained in some finite (and therefore complete) extension of k; we denote this group $F(\bar{\mathfrak{m}})$. Similarly $\bar{\mathfrak{m}}^m$ takes on, from Φ, the structure of a set acted upon by $F(\bar{\mathfrak{m}})$.

The most familiar examples are those where $m = n$ and $\Phi = F$, but the purpose of this paper is to exhibit and construct many more than these in case $m = n = 1$. Let us take note here of two one-dimensional examples that are already well known. The multiplicative formal group $\mathcal{M}(s, t) = s + t + st$ acts on the formal affine line via the *multiplicative flow*, $\Phi_{\mathrm{m}}(t, x) = (1 + t)x$, in which $\{0\}$ is an orbit. And the additive formal group $\mathcal{A}(s, t) = s + t$ acts, via the *parabolic flow*, $\Phi_{\mathrm{p}}(t, x) = 1/(-t + 1/x) = x \sum_0^\infty t^i x^i$. Here also, $\{0\}$ is an orbit. For completeness, we mention the *trivial flow* $\Phi_{\mathrm{triv}}(t, x) = x$.

DEFINITION. Let A be a commutative ring, and let (F, Φ) and (G, Ψ) be formal flows on the formal affine line defined over A. Then a *formal morphism* from (F, Φ) to (G, Ψ) is a pair (f, φ) where $f \in \mathrm{Hom}_A(F, G)$ and $\varphi(x) \in A[[x]]$ is a power series without constant term, such that $\varphi\big(\Phi(t, x)\big) = \Psi\big(f(t), \varphi(x)\big)$. In case A is complete and separated under the topology defined by the powers of an ideal J, a *J-adic analytic morphism* from (F, Φ) to (G, Ψ) is a pair (f, φ) satisfying the same identity, but where $\varphi \in A[[x]]$ has a constant term with some power lying in J.

When k is a finite field extension of $\mathbb{Q}_p$ with ring of integers $\mathfrak{o}$, it is clear that the set of formal flows on the formal affine line over $\mathfrak{o}$ with formal morphisms, respectively analytic morphisms, is a category. In particular, if (F, Φ) is a formal flow on the open unit disk defined over $\mathfrak{o}$, the most general $\mathfrak{o}$-analytically isomorphic flow has the form (G, Ψ), where

$$G(s, t) = f\big(F(f^{-1}s, f^{-1}t)\big),$$
$$\Psi(t, x) = \varphi\big(\Phi(f^{-1}t, \varphi^{-1}x)\big)$$

and where f and φ are elements of the groups $\mathcal{G}_0(\mathfrak{o})$ and $\mathcal{G}_{\mathfrak{m}}(\mathfrak{o})$, respectively. Notice that the trivial flow is isomorphic to no other flow than itself.

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

DEFINITION. Let (F, Φ) be a formal flow on the open unit disk defined over $\mathfrak{o}$, and let $\xi \in \bar{\mathfrak{m}}$. We say that ξ is a *fixed point* of the flow if $\Phi(t, \xi) = \xi$. If Φ is not trivial, we say that ξ is a fixed point *of order n* if $(x - \xi)^n$ is the highest power of $x - \xi$ dividing $\Phi(t, x) - x$.

By the Weierstrass Preparation Theorem and uniqueness of factorization in $\mathfrak{o}[[t, x]]$, there is a maximal monic polynomial in x only that divides $\Phi(t, x) - x$, so there are only finitely many fixed points of Φ in all of $\bar{\mathfrak{m}}$ if Φ is nontrivial. It is certainly possible to have $\Phi(\alpha, \xi) = \xi$ without ξ being a fixed point of the flow. Indeed, let q be a power of p and consider the q-power multiplicative flow $\mathcal{Q}(t, x) = x(1 + t)^q$. Then if $\alpha + 1$ is a q-th root of 1, we have $\mathcal{Q}(\alpha, \xi) = \xi$ for all $\xi \in \mathfrak{m}$, but 0 is the only fixed point of the flow.

DEFINITION. If (F, Φ) is a formal flow on the open unit disk, the *kernel* of Φ is the set of all $\alpha \in \bar{\mathfrak{m}}$ such that $\Phi(\alpha, x) = x$. The kernel is a subgroup of $F(\bar{\mathfrak{m}})$, which we denote $\ker(\Phi)$.

A more abstract viewpoint defines the kernel as a subgroup scheme of the formal group scheme associated to F, but the more elementary set-theoretic viewpoint taken here will suffice for our purposes.

In the following, we use the notation $\Phi_1(t, x)$ for the derivative with respect to the first-named variable.

PROPOSITION 2.1. *Let (F, Φ) be a nontrivial formal flow on the open unit disk defined over $\mathfrak{o}$, the ring of integers in a finite extension k of $\mathbb{Q}_p$. Then for $\xi \in \bar{\mathfrak{m}}$, the following are equivalent:*

(1) *ξ is a fixed point of Φ;*
(2) *for all $\alpha \in \bar{\mathfrak{m}}$, $\Phi(\alpha, \xi) = \xi$;*
(3) *for infinitely many $\alpha \in \bar{\mathfrak{m}}$, $\Phi(\alpha, \xi) = \xi$;*
(4) *there is $\alpha \in \bar{\mathfrak{m}}$ with $\alpha \notin \ker(\Phi)$ such that $\Phi(\alpha, \xi) = \xi$;*
(5) $(x - \xi) | \Phi_1(0, x)$.

Furthermore, the order of ξ as a fixed point of Φ is equal to the order of divisibility of $\Phi_1(0, x)$ by $x - \xi$.

It will be sufficient to prove the assertions in the case $\xi = 0$. The implications (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) and (1) $\Rightarrow$ (5) follow directly. If 0 is not a fixed point of Φ, then $\Phi(t, 0)$ is a nonzero $\mathfrak{o}$-series, which can have only finitely many roots, by the Weierstrass Preparation Theorem, so (3) $\Rightarrow$ (1). Now we show that (4) $\Rightarrow$ (3). If α is not a torsion point of $F(\bar{\mathfrak{m}})$, then for every integer n, $\Phi\big([n]_F(\alpha), 0\big) = 0$, and (3) is verified. In case α is a torsion point, we must appeal to a different argument. Let β be any nontorsion element of $F(\mathfrak{m})$, and let

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

$\psi(x) = \Phi(\beta, x)$. In case 0 is a periodic point of ψ, say $\psi^{\circ m}(0) = 0$, then $\Phi\big([mn]_F(\beta), 0\big) = 0$ for all n, so that (3) is satisfied. In case 0 is not a periodic point of ψ, we set $\varphi(x) = \Phi(\alpha, x) \neq x$ and use the identity $\varphi \circ \psi = \psi \circ \varphi$ to see that $\psi(0)$ is a fixed point of φ, as is every $\psi^{\circ n}(0)$. But φ can have only finitely many fixed points, so that this case can not occur.

The implication (5) $\Rightarrow$ (1) depends on the characteristic of the base being zero. To prove it, let us suppose that $x|\Phi_1(0, x)$ and show that $x|\Phi(t, x)$. We write

$$\Phi(t, x) = x + t\Phi_1(0, x) + \sum_{i=2}^{\infty} t^i g_i(x)$$

and wish to show that for every i, $g_i(0) = 0$. If r is the smallest integer for which this is not so, say $g_r(0) = a \neq 0$, then we look at the equation $\Phi\big(F(s, t), x\big) = \Phi\big(s, (\Phi(t, x)\big)$ modulo the ideal $\big((s, t)^{r+1}, x\big)$. On the left is $aF(s, t)^r \equiv a(s + t)^r$ while on the right there is just $as^r + at^r$, unequal because $r > 1$ and the characteristic is zero. The final statement is proved the same way, but by reading the fundamental identity modulo the ideal $\big((s, t)^{r+1}, x^m\big)$ where m is the order of divisibility of $\Phi_1(0, x)$ by x.

COROLLARY 2.1.1. *If (F, Φ) is a nontrivial formal flow on the open unit disk defined over $\mathfrak{o}$, then the kernel of Φ is finite.*

Nontriviality of the flow means that there is a point $\xi \in \mathfrak{m}$ that is not a fixed point of Φ, and so there are only finitely many $\alpha \in \bar{\mathfrak{m}}$ such that $\Phi(\alpha, \xi) = \xi$. This finite set clearly contains the kernel of Φ.

Given a nontrivial formal flow (F, Φ), then, we may use Weierstrass Preparation to form from $\Phi_1(0, x)$ the associated monic polynomial with all roots in $\bar{\mathfrak{m}}$, which we will call the *divisor of fixed points* of (F, Φ).

LEMMA 2.2. *Let (F, Φ) be a nontrivial formal flow on the unit disk over $\mathfrak{o}$, the ring of integers in a finite extension k of $\mathbb{Q}_p$. Let α be in $\mathfrak{m}$, but not a torsion point of F, and let $\varphi(x) = \Phi(\alpha, x) \in \mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$. Then $\widetilde{\varphi}(x) = \Phi_1(0, x)\mathbf{L}_F(\alpha)$, where $\mathbf{L}_F$ is the logarithm of F, the unique k-formal group homomorphism from F to the additive formal group $\mathcal{A}$ for which $\mathbf{L}_F{}'(0) = 1$.*

The proof is exactly the computation already done for Example 1.8.

COROLLARY 2.2.1. *Let (F, Φ) and α be as in the preceding Proposition. Then every periodic point of $\varphi(x) = \Phi(\alpha, x)$ is a fixed point of φ and of Φ.*

Our aim in the next section is to demonstrate a kind of converse to Lemma 2.2, that if we have a transformation γ of the open unit disk with only finitely many periodic points, then it is almost of the form $\Phi(\alpha, x)$ for some formal flow Φ. In

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

this case 'almost' means that an integral iterate of γ will be of the desired form, even if γ itself is not.

3. Constructing Flows on the Open Unit Disk

In this section, we show that any monic $\mathfrak{o}$-polynomial whose roots all are in $\bar{\mathfrak{m}}$ occurs as the divisor of fixed points of a formal flow.

THEOREM 3.1. *Let $f(x) \in p\mathfrak{o}[[x]]$ be a power series. Then there is a formal action $(\mathcal{A}, \Phi)$ of the additive formal group on $\bar{\mathfrak{m}}$, with $\Phi_1(0, x) = f(x) \in \mathfrak{o}[[t, x]]$.*

The proof is standard, though perhaps it takes place in a nonstandard context. Form the $\mathfrak{o}$-derivation $D: \mathfrak{o}[[x]] \to \mathfrak{o}[[x]]$ such that $D(x) = f(x)$, and define the mapping

$$\Gamma: \mathfrak{o}[[x]] \longrightarrow \mathfrak{o}[[t, x]]$$
$$\Gamma = \exp(tD) = \mathrm{id} + \sum_{n=1}^{\infty} \frac{t^n}{n!} D^{\circ n}.$$

The values of Γ are in $\mathfrak{o}[[t, x]]$ because $p^n/n! \in \mathbb{Z}_p$ for all n; of course for $p \neq 2$ a somewhat weaker hypothesis on the coefficients of f than that they all lie in $p\mathfrak{o}$ would have sufficed. Then it is a matter of verification to see that the mapping Γ is in fact a ring homomorphism, and that when we set $\Gamma(x) = \Phi(t, x) \in \mathfrak{o}[[t, x]]$, the relation $\Phi\big(s, \Phi(t, x)\big) = \Phi(s + t, x)$ also holds. Thus $(\mathcal{A}, \Phi)$ is a formal flow on $\bar{\mathfrak{m}}$, and the construction itself shows that $\Phi_1(0, x) = f(x)$.

THEOREM 3.2. *Let $\gamma(x) \in \mathfrak{o}[[x]]$ define an invertible analytic transformation of $\bar{\mathfrak{m}}$ with only finitely many periodic points. Then there is a formal flow $(\mathcal{A}, \Phi)$ on the open unit disk, an $m \in \mathbb{Z}$, and $\alpha \in \mathfrak{m}$ such that $\gamma^{\circ m}(x) = \Phi(\alpha, x)$.*

We may assume, by replacing γ by $\gamma^{\circ m_0}$, $p \nmid m_0$, that $\gamma \in \mathcal{G}^1_{\mathfrak{m}}(\mathfrak{o})$. Since γ has only finitely many periodic points, its Lie logarithm $\widetilde{\gamma}$ has only finitely many roots, and so the coefficients of $\widetilde{\gamma}$ are bounded. That is, there is n such that $p^n\widetilde{\gamma}(x) \in p\mathfrak{o}[[x]]$. So there is a formal flow $(\mathcal{A}, \Phi)$ on the open unit disk for which $\Phi_1(0, x) = p^n\widetilde{\gamma}(x)$. Using the formula of Lemma 2.2 and the fact that $L_{\mathcal{A}}(x) = x$, we get $g(x) = \Phi(p, x)$, satisfying $\widetilde{g} = p^{n+1}\widetilde{\gamma}$. Finally, by Theorem 1.7, we may iterate further so that $g^{\circ p^r} = \gamma^{\circ p^{n+1+r}}$, in other words, $\gamma^{\circ p^{n+1+r}}(x) = \Phi(p^{r+1}, x)$.

When F is any one-dimensional formal group over $\mathfrak{o}$, there is an associated formal group $F^0 = (1/p)F(ps, pt)$ if $p > 2$, $F^0 = \frac{1}{4}F(4s, 4t)$ if $p = 2$, which is $\mathfrak{o}$-isomorphic to the additive formal group $\mathcal{A}(s, t) = s + t$, by the logarithm $L_{F^0}(t) = (1/p)L_F(pt)$, resp. $\frac{1}{4}L_F(4t)$. In this sense, every formal group has a neighborhood of 0 isomorphic to the additive formal group. Similarly, if (F, Φ) is a formal flow on the open unit disk, then (F^0, Φ^0) is also a flow, when we define $\Phi^0(t, x)$ to be $\Phi(pt, x)$, resp. $\Phi(4t, x)$. And then

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

(F^0, Φ^0) is isomorphic to an action of the additive formal group on the disk. If we think of (F^0, Φ^0) as a restriction of (F, Φ), then we may ask whether the actions of the additive formal group on the disk that were found in Theorems 3.1 and 3.2 may be the restriction of actions of formal groups F that are not isomorphic to $\mathcal{A}$. The answer, in a word, is not usually. To make the statement of the following Theorem a little neater, let us make the nonstandard definition that a formal group $F(s, t) \in \mathfrak{o}[[s, t]]$ that becomes isomorphic over $\mathfrak{o}/\mathfrak{m}$ to the additive formal group has *height zero*. (The standard terminology is that such a formal group has infinite height.)

THEOREM 3.3. *Let (F, Φ) be a nontrivial formal flow defined over $\mathfrak{o}$.*

(a) *If Φ has a fixed point of multiplicity greater than one, then the only torsion of F is in the kernel of Φ, and in particular the height of F is zero;*
(b) *If there is more than one fixed point of Φ, then F has only finitely much torsion, and in particular the height of F is zero;*
(c) *If Φ has a single fixed point of multiplicity one, then the height of F is at most one.*

In all cases, we may assume, perhaps after an extension of k, that 0 is one of the fixed points of Φ.

Part (a) is the most direct: if α is a torsion element of $F(\bar{\mathfrak{m}})$ that is not in the kernel of Φ, then $\Phi(\alpha, x) = \varphi(x)$ is not the identity, but has an iterate that is identity: $\varphi^{\circ p^m}(z) = z$ for some m. But for 0 to be a fixed point of order 2 or more, $\varphi(z) \equiv z (\mathrm{mod}\ z^2)$, and no nonzero iterate of such a series can be identity.

Let 0 and $\xi \neq 0$ be two of the fixed points of Φ, let α be a torsion point of F not in the kernel of Φ, and let $\varphi(x) = \Phi(\alpha, x)$. Let p^m be the order of α in the group $F(\bar{\mathfrak{m}})/\ker(\Phi)$, so that $\varphi^{\circ p^m}$ is the first positive-order iterate of φ that is identity. Since 0 and ξ also are fixed points of φ, we may write $\varphi(x) = x + x(x - \xi)g(x)$ for some $g(x) \in \mathfrak{o}[[x]]$. Differentiating, we get

$$\varphi'(x) = 1 + (x - \xi)g(x) + xg(x) + x(x - \xi)g'(x),$$
$$\varphi'(0) = 1 - \xi g(0).$$

Now, since 0 is a fixed point of φ of multiplicity 1, we see that $\varphi'(0)$ is a primitive p^m-th root of unity, so that

$$v\big(\varphi'(0) - 1\big) = \frac{1}{(p-1)p^{m-1}} \geqslant v(\xi).$$

If F were to have infinitely many torsion points α, then the numbers m that occur above would be unbounded, and $v(\xi) = 0$, which is impossible.

Finally, suppose that Φ has the fixed point 0, at which the multiplicity is one, and that F has height $h > 1$. In this case, $\alpha \mapsto \varphi(x) = \Phi(\alpha, x) \mapsto \varphi'(0) = \Phi_2(\alpha, 0)$ defines a group homomorphism from $F(\bar{\mathfrak{m}})$ to $\mathfrak{o}^\times$, the group of units of $\bar{\mathfrak{o}}$, and this homomorphism factors through $F(\bar{\mathfrak{m}})/\ker(\Phi)$. The torsion subgroup of $F(\bar{\mathfrak{m}})$ is

https://doi.org/10.1023/A:1026412227043 Published online by Cambridge University Press

the sum of h groups isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, and the same is true of $F(\bar{\mathfrak{m}})/\ker(\Phi)$; in this group the torsion subgroup is mapped to the torsion subgroup of $\bar{\mathfrak{o}}^\times$, with a nontrivial kernel. Thus there is a torsion element $\alpha \notin \ker(\Phi)$ with $\Phi(\alpha, x) \equiv x (\mathrm{mod}\ x^2)$, and this cannot happen.

References

[AV] Arrowsmith, D. K. and Vivaldi, F.: Geometry of p-adic Siegel disks, *Physica D* **71** (1994), 222–236.

[L] Lubin, J.: Nonarchimedean dynamical systems, *Compositio Math.* **94** (1994), 321–346.

[Z] Zieve, M.: Cycles of polynomial mappings, Doctoral thesis, University of California, Berkeley (1996).