COMPOSITIO MATHEMATICA

JONATHAN LUBIN

# Nonarchimedean dynamical systems

*Compositio Mathematica*, tome 94, nº 3 (1994), p. 321-346
<http://www.numdam.org/item?id=CM_1994__94_3_321_0>

*Compositio Mathematica* **94**: 321–346, 1994.


# Nonarchimedean dynamical systems

JONATHAN LUBIN

*Department of Mathematics, Brown University, Providence, Rhode Island, U.S.A.*

Received 16 March 1993; accepted in final form 4 November 1993

## Introduction

Some of the standard and well-established techniques of local arithmetic geometry can also be seen as involving dynamical systems: in the theory of formal groups over the ring of integers in a finite extension $k$ of the $p$-adic field $\mathbb{Q}_p$, one constructs a representation module for the Galois group of $k$ out of the torsion points of a particular formal group. These points are the roots of all the iterates of a single power series, the endomorphism of multiplication by $p$ on the formal group; at the same time, these are also the fixed points of the iterates of a single automorphism of the formal group, such as multiplication by $1 + p$. In this sense, formal-group theorists have been studying nonarchimedean dynamical systems for almost as long as we have been speaking prose.

In this note I propose to lay out some techniques for the study of the behavior of the iterates of a general $p$-adic analytic transformation. At all times, the already-existing theory of formal groups stands as a guide, and my attention will always be directed to *analytic transformations of the p-adic open unit disk.* This seems to be the right setting for results that may be of use in algebraic geometry and local class-field theory. I also adhere to the standard algebro-geometric practice of requiring mappings or spaces to be defined over a fixed finite extension of the base, but allowing points (in this case fixed points and roots) to have their coordinates in any extension of the base. This geometric outlook is something of a departure, in comparison with the little work on $p$-adic dynamics that has appeared in the literature up to now. To me, the most interesting works in this field so far are the papers [BM] and [TVW], but these are concerned principally with the behavior of the set of $\mathbb{Z}_p$-rational points under a polynomial transformation.

We deal exclusively with series that have a fixed point at 0, and pay attention exclusively to properties of the associated mapping of the "open unit disk", i.e. the maximal ideal of whatever local ring the points are allowed to have their coordinate in. Under these restrictions the study splits naturally into two almost disjoint parts: if a series $f$ has $f'(0)$ in the maximal ideal, then it is noninvertible and it can have no other fixed points than 0, but the roots of its iterates are of serious interest. In the other case, $f'(0)$ is a unit, and since $f$ is invertible, it and its iterates can have no other roots than 0, but the fixed points of the iterates of $f$, that is, the periodic points of $f$, now play a role parallel to the roots of the iterates of a noninvertible series. These two studies become no longer disjoint in case an invertible series commutes with a noninvertible series, a phenomenon familiar enough when all are endomorphisms of a formal group. But it is an open question whether this can happen if there is no formal group in the background.

A familiarity with formal-group theory is by no means a prerequisite for reading this paper, but readers who are looking for a good introduction to formal groups may wish to refer to [Fr]; more encyclopedic references, not concentrating on the one-dimensional case, are [La2] and [H]. Formal groups come into this study for the following reason: the most familiar example of an algebraic extension of interest being generated by the roots of the iterates of a single power series is the case where $f(x)=(1+x)^p-1=px+\cdots+px^{p-1}+x^p$. This is the $p$-endomorphism of the "multiplicative" formal group $\mathscr{M}(x,y)=x+y+xy$. In this case, the field of roots is abelian, namely the field gotten by adjoining all $p^n$th roots of 1 to the base. More generally, $f$ may be a noninvertible endomorphism of any formal group $F$ over the ring of integers in a local field; if $F$ has "complex multiplications" in the sense of [LT], i.e. in case $F$ is a formal $\mathscr{A}$-module of $\mathscr{A}$-height 1 for some $p$-adic integer ring $\mathscr{A}$, then the field of all roots will be abelian over the base, related in a simple and well understood way to a maximal totally ramified abelian extension of the fraction field of $\mathscr{A}$. When $f$ is an endomorphism of a formal group that is not a formal module of height 1, then the corresponding extension is still fairly well understood [Ser], [Sen], [T]; here, in particular, we have the Tate module of $F$, which provides a natural $\mathbb{Z}_p$-free representation module for the Galois group.

When $f$ does not belong to any formal group, however, the field generated by all roots or fixed points of $f$ is, to my knowledge, almost completely unknown. Although I have examined several examples numerically, I do not present them here. Instead, in this first paper, I do no more than lay out the groundwork, paying particular attention to the structure of the commuting families defined in Section 1, and to certain tools that seem very natural in $p$-adic dynamical systems but have no parallel in the archimedean case, such as the Lie logarithm.

Many of the results in this paper owe their existence to a number of very valuable discussions that I had with K. Zimmermann during his visit to Brown University in 1990. More recently, P. Morton helped me clarify my thinking on many matters, and illuminated for me a number of ideas that I had only been groping toward. His help was particularly useful to me in extending my understanding of the Lie logarithm. In addition, I wish to thank the referee of this paper, whose suggestions have been very helpful.

## 0. Notational conventions and basic tools

Throughout this paper, all rings will be commutative, with multiplicative identity element. We will reserve the letter $\mathfrak{o}$ for a complete local ring, with maximal ideal $\mathfrak{m}$ and residue field $\kappa$. The field of $p$-adic numbers will be denoted $\mathbb{Q}_p$, and the ring of $p$-adic integers will be $\mathbb{Z}_p$. If $R$ is any ring, then $R[[t, u, v]]$ will be the ring of formal power series in the variables $t$, $u$, and $v$ over $R$. The multiplicative inverse of an element of a ring will always be referred to as its reciprocal, and the word "inverse" will be reserved for the inverse of a power series in one variable under the operation of substitution. Those series that have inverses will be called *invertible*, while those that have reciprocals will be called *units*.

When $\mathfrak{o}$ is a complete local ring, and $f(t) \in \mathfrak{o}[[t]]$, but not all coefficients of $f$ are in $\mathfrak{m}$, then the lowest degree in which a unit coefficient appears will be called the *Weierstrass degree* of $f$, denoted wideg($f$). If all coefficients are in $\mathfrak{m}$, we will say that the Weierstrass degree is infinite. When this is not the case, there is, according to the Weierstrass Preparation Theorem, a unique unit power series $U(t) \in \mathfrak{o}[[t]]$ and monic polynomial $P(t) \in \mathfrak{o}[t]$ such that $f = PU$ and $\deg(P) = \text{wideg}(f)$. We will call $P$ the *Weierstrass polynomial* associated to $f$. Since the Weierstrass degree of a product is the sum of the Weierstrass degrees of the factors, the Weierstrass degree of $f$ and $P$ are equal; in particular, all lower coefficients of $P$ are nonunits.

If $A$ is any ring, then we will call $\mathscr{S}_0(A)$ the set of all power series $f \in A[[x]]$ without constant term. This set is a monoid (noncommutative, associative, with a two-sided identity) under substitution, and a necessary and sufficient condition for $f$ to be invertible is that $f'(0)$ should be a unit of $A$. As usual, we write $f(g(x)) = (f \circ g)(x)$; in a less standard notation, we denote by $f^{\circ n}$ the $n$-fold composition of $f$ with itself; this makes sense for negative $n$ in case $f$ is invertible. The set of all invertible elements of $\mathscr{S}_0(A)$ is a group, and it will be denoted $\mathscr{G}_0(A)$. A series $f$ is in $\mathscr{G}_0$ if and only if $f(0) = 0$ and $f'(0)$ is a unit of $A$. The operations of substitution and inversion in $\mathscr{S}_0(A)$ are finitary in the sense that to calculate any particular coefficient of a composition or inverse, there need to be done only finitely many algebraic operations involving the coefficients of the given series. It is easy to see that when two series defined over a local ring $\mathfrak{o}$ are composed, their Weierstrass degrees multiply: $\operatorname{wideg}(f \circ g) = \operatorname{wideg}(f)\operatorname{wideg}(g)$.

In case $A$ is a complete ring under the topology defined by the powers of the ideal $I$, and if $J$ is an ideal of $A$ such that in $A/I$, all elements of $J + I/I$ are nilpotent, then we will call $\mathscr{S}_J(A)$ the set of all $f \in A[[x]]$ whose constant term is in $J$. Since the powers of any element of $J$ converge to 0, the composition of any two elements of $\mathscr{S}_J(A)$ is well defined. Again, $f$ is invertible in this monoid if and only if $f'(0)$ is a unit of $A$; in a notation similar to the one above, we denote by $\mathscr{G}_J(A)$ the group of invertible elements of $\mathscr{S}_J(A)$. In $\mathscr{S}_J(A)$, composition and the operation of inversion are not finitary: even to substitute a nonzero constant into a power series involves a limiting process.

One of the principal topics of this note is the question of which series commute with a given one.

DEFINITION. Let $f \in \mathscr{S}_0(A)$. Then the *commutant monoid* of $f$, denoted $\operatorname{Comm}_A(f)$, is the set of all $g \in \mathscr{S}_0(A)$ with $g \circ f = f \circ g$.

Although significantly many of the results of this paper, especially those of Section 1, are valid over an arbitrary ring, the most important results are special to the context of a local number field $k$ (an algebraic extension of $\mathbb{Q}_p$) and its integer ring $\mathfrak{o}$. In this case we have the (additive) valuation $v = v_k$, which we will always take to be normalized so that $v(p) = 1$.

One tool that we make extensive use of is the valuation function belonging to a series $f \in \mathscr{S}_0(\mathfrak{o})$. The relation between this and the Newton polygon of $f$ comes about as follows: if $f = \Sigma_i a_i x^i \in \mathfrak{o}[[x]]$, the *Newton copolygon* of $f$ is the intersection in the $(\xi, \eta)$-plane of the closed halfplanes defined by the inequalities $\eta \leqslant v(a_i) + i\xi$. It is easy to see that two power series have the same Newton copolygon if and only if they have the same Newton polygon: indeed, the polygon and copolygon are essentially dual convex bodies. The upper boundary of the copolygon is the graph of a real-valued function defined for nonnegative values of the variable $\xi$. This is the *valuation function* of $f$, and we denote it $v_f$. One sees that for any $\alpha$ algebraic over $k$ and with $v(\alpha) > 0$, the relation $v(f(\alpha)) \geqslant v_f(v(\alpha))$ holds. This inequality is strict only when $v(\alpha)$ is the $\xi$-coordinate of a vertex of the copolygon, i.e. when $v(\alpha)$ is the negative of the slope of a segment of the polygon, and thus equal to the value of some root of $f$. It follows from this that if the copolygon of $g$ has no horizontal segment (i.e. if $g$ has no constant term), then $v_f \circ v_g = v_{f \circ g}$. The valuation function is described well in [La1], and its relation to the Newton polygon is made explicit in Section 3 of [Lu].

On the ring $\mathfrak{o}[[x]]$ there are rank-one valuations of a particularly simple kind. If $\rho$ is any nonnegative real number, and $f(x) = \Sigma\, a_i x^i$, then we may

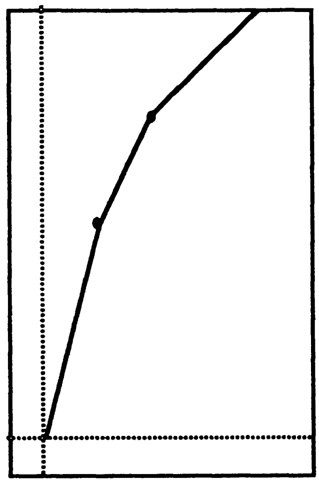

*Fig.* Copolygon of $x^4 + px^2 + p^2x$

define $w_\rho(f) = v_f(\rho) = \min_i(v((a_i) + i\rho)$. If $\rho = 0$, this is just the $p$-adic valuation on $\mathfrak{o}[[x]]$. In case $\rho$ is irrational, $w_\rho$ is not discretely valued when extended to the fraction field, but in all cases, $\mathfrak{o}[[x]]$ is complete under the topology induced by $w_\rho$.

Let us look more closely at the case where $\rho$ is positive. The ring $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k$ is not complete under $w_\rho$ now, but its completion under $w_\rho$ may be interpreted as the set of all $k$-series $\Sigma\, a_i x^i$ such that for every $N$ there are only finitely many values of $i$ for which $v(a_i) < N - \rho i$. In the language of Newton polygons, that is, for each line $l$ of slope $-\rho$ there are only finitely many monomials of $f$ placed below $l$. Let us call this completion $\mathbf{A}_\rho = \mathbf{A}_\rho(k)$. Informally, $\mathbf{A}_\rho$ is the set of $k$-series whose coefficients grow in a controlled enough manner that we may substitute an element $\mu$ of $\bar{\mathfrak{m}}$ for the variable whenever $v(\mu) \geqslant \rho$. We are interested in the intersection (inverse limit) of all the rings $\mathbf{A}_\rho$ for positive $\rho$. Let us call this ring $\mathbf{A} = \mathbf{A}(k)$. All these rings may be considered as subrings of $k[[x]]$. It is clear that for a series $f \in \mathbf{A}$, and for any element $\mu \in \bar{\mathfrak{m}}$, $f(\mu)$ gives a Cauchy series in the field $k(\mu)$, which is finite over $k$, and hence complete.

Another property of the ring $\mathbf{A}$ is that, just as we may substitute an $\mathfrak{o}$-series $f$ without constant term for the variable in a series in $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k$, so we may substitute $f$ for the variable in a series in $\mathbf{A}$ to get a result in $\mathbf{A}$.

## 1. The commutant monoid of a given series when the base ring is a field

The series that most of our results apply to are those that start in degree 1. From the formal standpoint, in characteristic zero, there are two main cases, depending on the first-degree coefficient:

DEFINITION. Let $A$ be an integral domain, and $f(x) \in \mathscr{S}_0(A)$. We say that $f$ is a *torsion* series if there is $n > 1$ with $f^{\circ n}(x) = x$; we say that $f$ is *stable* if $f'(0)$ is not 0 nor a root of 1; and we say that $f$ is *unipotent* if $f$ is not a torsion series, but $f'(0)$ is a root of 1.

In the standard language of complex dynamics, $f$ is stable if 0 is a fixed point of $f$, but 0 is neither superattracting nor rationally indifferent; and unipotence is exactly the same as rational indifference. It is with some hesitation that I use other terms than the standard ones, but the phenomena that arise in the $p$-adic case are not at all well suggested by the traditional words. In the stable case, a very significant fact is that, if $K$ is a field, then modulo torsion, $\mathrm{Comm}_K(f)$ has the natural structure of the multiplicative group scheme $\mathbf{G_m}$. Even more significant is the linearizability of $f$, and beyond that, the importance of the linearizing function (the "logarithm") as a tool for investigating the dynamics of $f$. On the other hand, in the unipotent case, $\mathrm{Comm}_K(f)$ has the natural structure, modulo torsion, of the additive group scheme $\mathbf{G_a}$.

PROPOSITION 1.1. *Let $K$ be a field, and let $f(x)$ be a stable series in $\mathscr{S}_0(K)$. Then the mapping $g(x) \mapsto g'(0)$ gives a bijection between* $\mathrm{Comm}_K(f)$ *and $K$ itself.*

*Proof.* We need only show that if $c \in K$, then the polynomial $cx$ may be extended, degree by degree, to polynomials $g_j(x)$ for which $f(g_j(x)) \equiv g_j(f(x)) \pmod{x^j}$, and that the extension is unique at each stage. Indeed, suppose that $g(f(x)) \equiv f(g(x)) + \lambda x^j \pmod{x^{j+1}}$, for $j \geqslant 2$, and that the first-degree coefficient of $f$ is $a \in K$. Then for $g(x) + \mu x^j$ to commute with $f$ modulo $(x^{j+1})$, it is necessary and sufficient that $\mu = \lambda/(a^j - a)$, which, by the hypothesis on $a$, is always defined.

COROLLARY 1.1.1. *Let $A$ be an integral domain, and let $f(x)$ be a stable series over $A$. Then the mapping $g(x) \mapsto g'(0)$ gives a bijection between* $\mathrm{Comm}_A(f)$ *and a multiplicatively closed subset of $A$.*

This follows because if both $g$ and $h$ commute with $f$, then so does $g \circ h$.

COROLLARY 1.1.2. *Let $K$ and $f$ be as in Proposition* 1.1. *Then there are, for $j \geqslant 2$, polynomials $\Phi_j(t) \in K[t]$, such that $\Psi_t(x) := tx + \Sigma\,\Phi_j(t)x^j$ commutes with $f$.*

This follows directly from the proof of the proposition. One sees easily as well that the degree of $\Phi_j$ is at most $j$. Perhaps the most important consequence of the existence of the $\Phi$'s is the fact that if $\mathfrak{o}$ is the ring of integers in a local field $k$, then $\mathrm{Comm}_{\mathfrak{o}}(f)$ corresponds to a closed subset of $\mathfrak{o}$ under the mapping mentioned in Corollary 1.1.1:

COROLLARY 1.1.2.1. *Let $k$ be a topological field, and $A$ a subring of $k$ that* *is topologically closed. If $f$ is a stable series over $A$, then the set $\{a \in k : \exists g \in \mathrm{Comm}_A(f),\ g'(0) = a\}$ is a closed subset of $A$.*

Indeed, the set in question is the intersection of the inverse images of the set $A$ under the maps $\Phi_j$.

COROLLARY 1.1.3. *Let $A$ be an integral domain, $f$ a stable series over $A$, and $g$, $h$ series over $A$ that commute with $f$. Then $g$ and $h$ commute with each other.*

This is true because $g \circ h$ and $h \circ g$ are $A$-series that commute with $f$ and have the same first-degree coefficient.

COROLLARY 1.1.4. *Among stable series over an integral domain, the relation of commutation is an equivalence relation.*

DEFINITION. Let $A$ be an integral domain. A subset $C$ of $\mathscr{S}_0(A)$ is a *stable commuting family* if there is a stable series $f$ over $A$ such that $C = \mathrm{Commm}_A(f)$.

Most of the results of this and the next two sections will be concerned with the properties of stable commuting families. Experimental evidence seems to indicate that a noninvertible series $f$ will most typically have a commutant monoid of the form $g^{\circ \mathbb{Z}}$, the set of all iterates of a particular series; for an invertible series, the story is more complicated, and will be dealt with in Section 4.

PROPOSITION 1.2. *Let $K$ be a field, and let $f(x)$ be a stable series over $K$. Then there is a unique $\mathbf{L}_f(x) \in K[[x]]$ with $\mathbf{L}_f(x) \equiv x \pmod{x^2}$ and $\mathbf{L}_f(f(x)) = f'(0) \cdot \mathbf{L}_f(x)$.*

*Proof.* One may prove this by a degree-by-degree argument such as was used for the previous proposition. An alternative proof of existence is to put $\mathbf{L}_f(x) = \Psi'_0(x)$, where the differentiation is with respect to $t$, and use the relations $\Psi_t(f(x)) = f(\Psi_t(x))$ and $\Psi_0(x) = 0$.

In conformity with the practice in formal group theory, we will call the series $\mathbf{L}_f(x)$ the *logarithm* of $f$. When $f$ is defined over an integral domain $A$, its logarithm will ordinarily be defined only over the fraction field of $A$.

PROPOSITION 1.3. *Let $K$ be a field, and let $f$ and $g$ be stable series over $K$. Then $f \circ g = g \circ f$ if and only if $\mathbf{L}_f = \mathbf{L}_g$.*

*Proof.* If $f$ and $g$ commute, then $(1/g'(0)) \cdot (\mathbf{L}_f \circ g)$ satisfies the defining condition for $\mathbf{L}_f$, and thus is equal to $\mathbf{L}_f$. But then $\mathbf{L}_f$ satisfies the defining condition for $\mathbf{L}_g$ and must therefore be equal to $\mathbf{L}_g$. Conversely, if the two logarithms are equal, we then have $\mathbf{L}(f(g(x))) = f'(0)g'(0)\mathbf{L}(x) =$

$\mathbf{L}(g(f(x)))$; *since* $\mathbf{L}$, $f$, and $g$ are elements of the group $\mathscr{G}_0(K)$, it follows that $f$ and $g$ commute.

The series that are unipotent seem to play a somewhat less important role in the $p$-adic theory than the stable ones, but we lay out their elementary properties here. When $K$ is a field of characteristic $p > 0$, determination of the commutant monoid of a unipotent series presents problems beyond the scope of this paper, but in characteristic zero, the results are easy enough, and indeed, well known to analysts.

PROPOSITION 1.4. *Let $K$ be a field of characteristic zero, and $u \in K[[x]]$ with $u(x) \equiv x + ax^r \pmod{x^{r+1}}$ for $a \neq 0$. Then there is a series $\varphi(x) \in K[[x]]$ with $\varphi(x) \equiv x \pmod{x^2}$ such that $w := \varphi^{-1} \circ u \circ \varphi$ is of the form $w(x) = x + ax^r + bx^{2r-1}$.*

*Proof.* It is necessary only to suppose that $u$ is of the form $u(x) \equiv x + ax^r + bx^{2r-1} + \gamma x^s \pmod{x^{s+1}}$, and show, if $r < s \neq 2r - 1$, that there is $\psi(x) = x + cx^{s-r+1}$ for which $\psi^{-1}(u(\psi(x))) \equiv x + ax^r + bx^{2r-1} \pmod{x^{s+1}}$.

We simply calculate $u(\psi(x))$ and $\psi(x + ax^r + bx^{2r-1})$ modulo degree $s + 1$:

$$u(\psi(x)) \equiv x + cx^{s-r+1} + ax^r + acrx^s + bx^{2r-1}$$

$$\psi(x + ax^r + bx^{2r-1}) \equiv x + ax^r + bx^{2r-1} + \gamma x^s + cx^{s-r+1} + ca(s - r + 1)x^s \pmod{x^{s+1}}$$

so that we need only solve $\gamma + ac(s - r + 1) = acr$ for the unknown $c$, which is always possible since our hypotheses guarantee $a(s - 2r + 1) \neq 0$. Thus it is possible to define $\psi =: \psi_s$, and we take for $\varphi$ a suitable (convergent) infinite composition of the $\psi_s$'s.

We might remark that if an $(r - 1)$th root of $a$ exists in $K$, then we can even get $w$ to have the form $w(x) = x + x^r + bx^{2r-1}$. More important is the fact that in any case, a suitable $K$-formal change of coordinate transforms $u$ to a series whose only nonzero coefficients are in degrees that are congruent to 1 modulo $r - 1$. Thus $u$ commutes with a $K$-series $\rho$ that starts $\zeta x + \cdots$, where $\zeta$ is a primitive $(r - 1)$th root of 1, and such that $\rho^{\circ(r-1)} = \mathrm{id}$.

PROPOSITION 1.5. *Let $K$ be a field of characteristic zero, and let $g(x) \in \mathscr{G}_0(K)$, with $g(x) \equiv x + ax^r \pmod{x^{r+1}}$, where $a \neq 0$. Then the centralizer of $g$ in $\mathscr{G}_0(K)$ is the direct sum of the cyclic group of all $(r - 1)$th roots of 1 in $K$ and the additive group of $K$.*

The proof of this proposition involves considerations that are more naturally introduced in Sections 4 and 5, and it will be stated again as

Proposition 5.4. We do not make any use of it other than to prove the following:

COROLLARY 1.5.1. *If $A$ is an integral domain of characteristic zero, and $u$ is a unipotent element of $G_0(A)$, then* $\mathrm{Comm}_A(u)$ *is commutative.*

Let $K$ be the fraction field of $A$. The series $u$ does not commute with any stable series, so that $\mathrm{Comm}_A(u)$ is indeed the centralizer of $u$ in $\mathscr{G}_0(A)$. Since the commuting family can only increase in size when we replace $u$ by $u^{\circ n}$, we may assume that $u'(0) = 1$, in which situation the larger group of $K$-series commuting with $u$ is commutative.

## 2. Series over a $p$-adic ring: roots of a noninvertible series and its iterates

The results so far have applied to a general integral domain, but now we specialize to the case where the base ring is the ring of integers $\mathfrak{o}$ in a finite extension $k$ of $\mathbb{Q}_p$. If $k$ is an algebraic closure of $k$, we denote by $\bar{\mathfrak{o}}$ and $\bar{\mathfrak{m}}$ the integral closure of $\mathfrak{o}$ in $\bar{k}$ and the maximal ideal of $\bar{\mathfrak{o}}$, respectively. This latter ideal is not finitely generated, and the integer ring is not complete, but since any finite set of elements of $\bar{\mathfrak{o}}$ lies in a finite extension of $k$, any power series over $\mathfrak{o}$ in finitely many variables may be evaluated at a vector of elements of $\bar{\mathfrak{m}}$. If $f(x) \in \mathfrak{o}[[x]]$, with finite Weierstrass degree $d$, then all roots of the associated Weierstrass polynomial are in $\bar{\mathfrak{m}}$. Counting multiplicity, there are $d$ of them, and they exhaust all roots of $f$ that are in $\bar{\mathfrak{m}}$. Consider any noninvertible stable series $f$ over $\mathfrak{o}$. It is important to know that there are infinitely many elements of $\bar{\mathfrak{m}}$ that are roots of iterates of $f$. For this, it is not enough to observe that multiplicativity of Weierstrass degree implies that $\mathrm{wideg}(f^{\circ n}) = d^n$, unless $f$ and its iterates be known to have all roots simple.

DEFINITION. Let $f$ be a noninvertible stable series over $\mathfrak{o}$. Then an *$f$-consistent sequence* is a sequence $(\alpha_1, \alpha_2 \ldots)$ of elements of $\bar{\mathfrak{m}}$ with $f(\alpha_1) = 0$, and for all $i > 1$, $f(\alpha_i) = \alpha_{i-1}$.

Clearly any nonzero root $\alpha_1$ of such an $f$ may be completed to an $f$-consistent sequence, and one easily sees that for $i$ large enough, $v(\alpha_i) = v(\alpha_{i-1})/d$, where $d = \mathrm{wideg}(f)$. One may argue from the shape of the Newton copolygon, which lies entirely above the line $\eta = \xi$, and has as its leftmost segment the line $\eta = \mathrm{d}\xi$, or along the following lines. If $\pi$ is a generator of $\mathfrak{m}$, then $f(x) = \pi g(x) + x^d U(x)$, where $g \in \mathscr{S}_0(A)$ and $U$ is a unit in $A[[x]]$. Thus $v(\alpha_{i-1}) \geqslant \min(v(\alpha_i) + v(\pi)\, dv(\alpha_i))$, and the desired inequality follows. In any event, an $f$-consistent sequence that has nonzero entries has infinitely many distinct entries, each of them a root of an iterate of $f$.

DEFINITION. Let $f$ be a noninvertible stable series over $\mathfrak{o}$. Then $\Lambda(f)$ is the set of all roots of iterates of $f$.

PROPOSITION 2.1. *Let $f$ and $g$ be noninvertible stable series with $f \circ g = g \circ f$. Then $\Lambda(f) = \Lambda(g)$.*

*Proof.* We need only show that if $\alpha$ is a root of $g$, then it is a root of an iterate of $f$. Whenever $\alpha$ is a root of $g$, $f(\alpha)$ is a root of $g$ also. From the inequality $v_f(\xi) > \xi$ we conclude that $\{v(f^{\circ i}(\alpha))\}$ either is a strictly increasing sequence of real numbers or eventually becomes infinite. The former is impossible, however, since it would imply that $g$ had infinitely many distinct roots in $\bar{\mathfrak{m}}$. Thus $\alpha$ is the root of some $f^{\circ i}$.

The logarithm of a stable series over $\mathfrak{o}$ will usually be a series over the fraction field, $k$, and not even in $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} k$: if $\mathbf{L}_f(x) = \Sigma c_i x^i$, then we expect that the numbers $v(c_i)$ will not be bounded below. Nonetheless, if $f$ is noninvertible, then $\mathbf{L}_f(x)$ is a series into which we may substitute any $\mu \in \bar{\mathfrak{m}}$ and get a convergent series in $\bar{k}$. That is, $\mathbf{L}_f \in \mathbf{A}(k)$, as we now show.

PROPOSITION 2.2. *Let $f$ be a noninvertible stable series in $\mathfrak{o}[[x]]$, with finite Weierstrass degree. Then the logarithm of $f$ is in $\mathbf{A}$, and furthermore $\mathbf{L}_f = \lim_n(f^{\circ n}/f'(0)^n)$.*

REMARKS. The convergence above is with respect to $w_\rho$ for all $\rho$. The relation is also true in the sense of coefficientwise convergence, that is, in the $(\mathfrak{m}, x)$-adic topology on $k[[x]]$, but this topology is too coarse for our purposes here.

*Proof.* We do this by a sequence of simple observations. Call

$$g_n := f^{\circ n}/f'(0)^n, \quad \text{and} \quad \varphi(x) := f(x)/xf'(0).$$

Then

$$g_n(x) = x \prod_{r=0}^{n-1} \varphi(f^{\circ r}(x)).$$

The constant coefficient of $\varphi$ is 1. Let us call $\sigma := \varphi - 1$. The difference $g_{n+1} - g_n$ is equal to $g_n(x) \cdot (\varphi(f^{\circ n}(x)) - 1) = g_n \cdot (\sigma \circ f^{\circ n})$. Next, let $\rho > 0$, then $w_\rho(\sigma \circ f^{\circ n}) = v_{\sigma \circ f^{\circ n}}(\rho) = v_\sigma(v_f^{\circ n}(\rho))$. Now $v_f^{\circ n}$ is the $n$-fold iteration of the increasing polygonal function $v_f$, which has the property that every segment has slope at least 1, and the rightmost segment is the function $\eta = \xi + v(f'(0))$. Since $\rho > 0$, the numbers $v_f^{\circ n}(\rho)$ increase without bound. Since $\sigma$ has no constant term, its valuation function is strictly increasing, and thus the numbers $w_\rho(g_{n+1} - g_n)$ increase without bound as well, and so the sequence of the $g$'s is Cauchy in the $w_\rho$ topology.

It is clear that the limit function satisfies the defining conditions for the logarithm of $f$. Since the series is in $\mathbf{A}$, we may substitute any element $\mu$ of

$\bar{\mathfrak{m}}$ for the variable of $\mathbf{L}_f$. The product expansion not only shows again that when $f$ and $g$ commute, they have the same root set $\Lambda$, but also gives a powerful tool for studying the roots of the logarithm.

## 3. Fixed points of an invertible series: first considerations

The problem of describing the fields generated by fixed or periodic points of invertible series seems about as intractible as the same problem for roots of iterates of noninvertible series. In all other ways, however, the study of fixed or periodic points poses much more subtle problems than the study of roots of iterates. For instance, we know precisely how many roots $f^{\circ n}$ has once we know the number of roots of $f$, since these numbers are the Weierstrass degrees of the functions. But even to count the number of fixed points of an invertible series $u$ and its iterates brings in very delicate questions about the structure of the group $\mathscr{G}_0(\kappa)$ of invertible series over the residue field $\kappa$. Before we attack such questions, however, we can give some elementary results in the spirit of Section 2.

DEFINITION. Let $u$ be an invertible stable series over $\mathfrak{o}$. Then $\Lambda(u)$ is the set of all fixed points of iterates of $u$.

PROPOSITION 3.1. *If $u$ and $w$ are series over $\mathfrak{o}$ that are invertible and stable, and if $u \circ w = w \circ u$, then $\Lambda(u) = \Lambda(w)$.*

*Proof.* As in the proof of 2.1, we need only show that every fixed point of $u$ is a fixed point of an iterate of $w$. Now, there are only finitely many fixed points of $u$, since the Weierstrass Preparation Theorem guarantees that a nonzero series over $\mathfrak{o}$ has only finitely many roots. Let $\lambda$ be a fixed point of $u$. Since $u(w(\lambda)) = w(u(\lambda))$, it follows that $w$ permutes the finite set of fixed points of $u$. Thus some iterate of $w$ must act as the identity on the fixed points of $u$, as claimed.

The use of the notation $\Lambda(\cdot)$ for two apparently different constructs is justified by the following:

PROPOSITION 3.2. *If $u$ and $f$ are stable series over $\mathfrak{o}$ with $u$ invertible and $f$ noninvertible, and if $u \circ f = f \circ u$, then $\Lambda(u) = \Lambda(f)$.*

*Proof.* As before, $u$ permutes the roots of $f$, and so an iterate of $u$ is identity on the roots of $f$. On the other hand, if $\lambda$ is a fixed point of $u$, then $u(f(\lambda)) = f(u(\lambda)) = f(\lambda)$, which means that $f(\lambda)$ is also a fixed point of $u$. That is, $f$ induces a mapping of the set of fixed points of $u$ into itself. But $f$ has the property that when $\lambda \neq 0$, $v(f(\lambda)) > v(\lambda)$. It follows that for $n$ large enough, $f^{\circ n}(\lambda) = 0$.

The series that arise from formal groups have the property that their derivatives have no root in $\bar{\mathfrak{m}}$. If the derivative of $f$, an $\mathfrak{o}$-series, has roots in $\bar{\mathfrak{m}}$, then $f$ itself must be noninvertible, and it is not so easy for $f$ to commute with any invertible series:

COROLLARY 3.2.1. *Let $f$ be a stable series over $\mathfrak{o}$, commuting with an invertible stable series over $\mathfrak{o}$. Then every root of $f'$ in $\bar{\mathfrak{m}}$ is also a root of an iterate of $f$.*

*Proof.* Suppose that $u$ is an invertible series that commutes with $f$. From the equation $f'(u(x)) \cdot u'(x) = u'(f(x)) \cdot f'(x)$, we see that $u$ permutes the roots (if any) of $f'$. Thus any root of $f'$ is a fixed point of some iterate of $u$, and the assertion follows.

As an example of this, consider the noninvertible series $f(x) = 4x + x^2$ over $\mathbb{Z}_2$, which commutes with the invertible series $9x + 6x^2 + x^3$. Then $f'$ has the root $-2$, which is also a root of $f \circ f$.

The above is a relatively elementary "noncommutation result": it says that the only way for two series of a particular kind to commute is for certain special phenomena to occur. The strongest result of this type so far is the "Main Theorem" of Section 6.

## 4. Fixed points of an invertible series: the Lie logarithm

In this section we examine more closely the group $\mathcal{G}_0(\mathfrak{o})$, making use of the completeness of $(\mathfrak{o}, \mathfrak{m})$, which is assumed to be a complete discrete valuation ring of characteristic zero with finite residue field $\kappa$ of characteristic $p > 0$. Whereas the iterates of a noninvertible series $f \in \mathfrak{o}[[x]]$ form a discrete set, Proposition 4.1 below shows that the iterates of an invertible series $u$ either form a finite set, or are dense in a group that has the structure of a $p$-adic Lie group with $p$-adic topological dimension 1. In the propositions following, we assume that the series $u$ satisfies $u'(0) \in 1 + \mathfrak{m}$; finiteness of the residue field guarantees that any invertible series has an iterate with this property. Modification of the statements to cover the general case is left to the reader.

PROPOSITION 4.1. *Let $u \in \mathfrak{o}[[x]]$, with $u'(0) \equiv 1 \pmod{\mathfrak{m}}$. Then in the $(\mathfrak{m}, x)$-adic topology, the series $u^{\circ p^n}(x)$ converge to the limit $x$, so that when $\mathbb{Z}$ has the $p$-adic topology, the map $\mathbb{Z} \to \mathcal{G}_0(\mathfrak{o})$ by $m \mapsto u^{\circ m}$ is a continuous homomorphism.*

*Proof.* First we make the elementary observation that if $\operatorname{wideg}(u(x) - x) = d > 1$, then $\operatorname{wideg}(u^{\circ p}(x) - x) > d$. Indeed, if we have any series

$$g(x) \equiv x + ax^r \pmod{(x^{r+1})} \quad \text{and} \quad h(x) \equiv x + bx^r \pmod{(x^{r+1})},$$

then

$$g \circ h \equiv x + (a + b)x^r \pmod{(x^{r+1})}.$$

This applies in particular to series over $\kappa$. So wideg$(u^{\circ p^n}(x) - x) \to \infty$.

The first part of the assertion will follow when we show, for any $N > 1$, that in the $\mathfrak{m}$-adic topology on $\mathfrak{o}[[x]]/(x^N)$, the series $u^{\circ p^n}(x)$ converge to $x$. By the observation above, we may assume that $u(x) \equiv x \pmod{\mathfrak{m}}$. Let $\pi$ be a prime element of $\mathfrak{m}$. Just as before, if $g(x) \equiv x + \pi^m\alpha(x) \pmod{\mathfrak{m}^{m+1}}$ and $h(x) \equiv x + \pi^m\beta(x) \pmod{\mathfrak{m}^{m+1}}$, then $(g \circ h)(x) \equiv x + \pi^m(\alpha(x) + \beta(x)) \pmod{\mathfrak{m}^{m+1}}$, which gives us the result. The second part of the assertion follows directly.

We may thus write $u^{\circ z}$ for any $p$-adic integer $z$. If $u$ is not a torsion series, then the homomorphism $\mathbb{Z}_p \to \mathscr{G}_0(\mathfrak{o})$, defined by $z \mapsto u^{\circ z}$, is an injection, so we get a natural $\mathbb{Z}_p$-coordinatization of a closed subgroup of $\mathscr{G}_0(\mathfrak{o})$ in which the set of iterates of $u$ is dense. In addition, if $u$ is stable, the set of invertible series $w \in \mathrm{Comm}_{\mathfrak{o}}(u)$ for which $w'(0) \equiv 1 \pmod{\mathfrak{m}}$ has the structure of a $\mathbb{Z}_p$-module. One more consequence of this $\mathbb{Z}_p$-action is that if $m$ is an integer prime to $p$, then $u^{\circ(1/m)}$ is well defined, so that any periodic point of $u$ is a fixed point of some $u^{\circ p^n}$. In other words, in $\bar{\mathfrak{m}}$, any finite $u$-orbit has cardinality a power of $p$.

If $u$ is a stable invertible series in $\mathscr{G}_0(\mathfrak{o})$, then its logarithm $L_u(x)$, described in Proposition 1.2, may have a domain of convergence much smaller than $\bar{\mathfrak{m}}$. As an example, take the 2-adic series $3x + x^3$, whose logarithm has the first few terms $x - x^3/24 + 3x^5/640 - 5x^7/7168$ and is not convergent even at $x = 2$. On the other hand, if $u$ is an automorphism of a formal group $F$ over $\mathfrak{o}$, then the logarithm $\mathbf{L}_u(x)$ is equal to $\mathbf{L}_{[p]}(x)$, where $[p](x)$ is the $p$-endomorphism of $F$. This logarithm is convergent on $\bar{\mathfrak{m}}$, since it is a series in $\mathbf{A}$, and its roots are the roots of the iterates of $[p]$, in other words the fixed points of iterates of $u$. It is apparent that the logarithm of Section 1 is less useful for invertible series, and less reliable.

We introduce in this section another construct of logarithmic type, perhaps more universal than $\mathbf{L}_u$, which has the desirable properties that it is defined even in case the invertible series $u$ is not stable; that it is convergent on all of $\bar{\mathfrak{m}}$; and that its roots are the fixed points of iterates of $u$. Its definition is based on the formula for the ordinary logarithm $\log(\alpha) = \lim_{n\to\infty}(\alpha^{p^n} - 1)/p^n$, valid for $\alpha \in 1 + \mathfrak{m}$.

DEFINITION. Let $u(x)$ be a series in $\mathscr{G}_0(\mathfrak{o})$, with $u'(0) \in 1 + \mathfrak{m}$. Then the *Lie logarithm* of $u$ is the series $\tilde{u}$ defined by:

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

As we have seen, the set of $\mathbb{Z}_p$-iterates of $u$ has a natural structure of a commutative $p$-adic Lie group of dimension 1; the Lie logarithm may be viewed as a canonical generator of the corresponding Lie algebra. It remains to be seen, however, that the limit above does exist, and that its value is an element of the ring **A**, so that it describes a function defined on all of $\bar{\mathfrak{m}}$. The first step is to show that there is a coefficientwise limit of the series in question. This is certainly not sufficient for our purpose: the example $0 = \lim_{\mathrm{cw}} x^n/p^n$ shows that a sequence of functions in **A** that have a coefficientwise limit need not be convergent in the $w_\rho$-topologies that are mentioned in Section 0.

To shorten notation, we will often omit mention of the variable $x$; to do this, we denote the identity series $x = \mathrm{id}(x)$.

LEMMA 4.2.1. *Let $\pi$ be a prime element in $\mathfrak{m}$ and let $u \in \mathfrak{o}[[x]]$, with $u(x) = x + \pi^r\alpha(x)$. Then $u^{\circ p}(x) \equiv x + \pi^r p\alpha(x) \pmod{\pi^{2r}}$.*

LEMMA 4.2.2. *Let $u \in \mathfrak{o}[[x]]$ with $u(0) = 0$ and $u'(0) \in 1 + \mathfrak{m}$. Then for every $N$, the sequence $(u^{\circ p^n} - \mathrm{id})/p^n$ is convergent in $k[[x]]/(x^N)$.*

*Proof.* We fix $N$, and work in $k[[x]]/(x^N)$. By Proposition 4.1, there is an $m$ for which $u^{\circ p^m}(x) - x \in p^2\mathfrak{o}[[x]]/(x^N)$. We show inductively that

$$\frac{u^{\circ p^{m+i}}(x) - x}{p^i} \equiv \frac{u^{\circ p^{m+i+1}}(x) - x}{p^{i+1}} \pmod{p^{i+1}},$$

that is, that the difference of the two series is in $p^{i+1}\mathfrak{o}[[x]]/(x^N)$. We note first that as a consequence of the preceding lemma,

$$\begin{aligned} u^{\circ p^{m+i}}(x) &= x + p^{i+2}\alpha_i(x) \\ &\Downarrow \\ u^{\circ p^{m+i+1}}(x) &\equiv x + p^{i+3}\alpha_i(x) \pmod{p^{2i+2}} \\ &\Downarrow \\ u^{\circ p^{m+i+1}}(x) &= x + p^{i+3}\alpha_{i+1}(x), \end{aligned}$$

for each $i \geqslant 0$, where the $\alpha_i$'s are in $\mathfrak{o}[[x]]/(x^N)$. Combining the upper two lines of this sorites, we get

$$\begin{aligned} \frac{u^{\circ p^{m+1}}(x) - x}{p^i} &= p^2\alpha_i(x) \\ &\equiv \frac{u^{\circ p^{m+i+1}}(x) - x}{p^{i+1}} \pmod{p^{i+1}}. \end{aligned}$$

LEMMA 4.2.3. *Let $A$ be a commutative ring, and $f \in \mathscr{S}_0(A)$, an arbitrary series with no constant term. Then in $A[[x]]$, $(f - \mathrm{id}) \mid (f^{\circ n} - \mathrm{id})$, for any $n > 0$.*

We need in addition something that will amount to a significant strengthening of Lemma 4.2.2. It says, in essence, that the operator that forms the $n$-fold iterate of series in $\mathfrak{o}[[x]]$ has derivative $n$ when evaluated at id.

LEMMA 4.2.4. *Let* $\{g_i\}$ *be a sequence of elements of* $\mathscr{G}_0(\mathfrak{o})$ *with limit* id *in the* $(\mathfrak{m}, x)$*-adic topology. Then for* $n > 0$, *there is a sequence* $\{H_i\}$ *of series in* $\mathfrak{o}[[x]]$, *with* $(\mathfrak{m}, x)$*-adic limit* 0, *such that* $g_i^{\circ n}(x) = x+(g_i(x)-x)(n+H_i(x))$.

*Proof.* Let us call $\alpha_i := g_i - \mathrm{id}$, so that we wish to show that $(\mathrm{id}+\alpha_i)^{\circ n} - \mathrm{id} = (n + H_i)\alpha_i$. We assume inductively that there are functions $K_i$ with limit 0 such that $g_i^{\circ n-1} - \mathrm{id} = (n - 1 + K_i)\alpha_i$, and, omitting the subscripts $i$, write

$$\begin{aligned} g^{\circ n} - \mathrm{id} &= (g^{\circ n} - g^{\circ n-1}) + (g^{\circ n-1} - \mathrm{id}) \\ &= \alpha \circ g^{\circ n-1} + g^{\circ n-1} - \mathrm{id} \\ &= \alpha \circ (\mathrm{id} + (n - 1 + K)\alpha) + (n - 1 + K)\alpha. \end{aligned}$$

We need to get the left-hand half of the bottom line into more manageable form. Write $\alpha(x + t) = \alpha(x) + \alpha'(x)t + t^2\gamma(x, t)$. Then, substituting

$$(n - 1 + K(x))\alpha(x) \quad \text{for } t, \text{ we get}$$

$$\alpha(x+(n-1+K(x))\alpha(x)) = \alpha(x)+\alpha'(x)(n-1+K(x))\alpha(x)+\alpha(x)^2\Gamma(x),$$

where the series $\Gamma$ are in $\mathfrak{o}[[x]]$. Now when $\alpha_i \to 0$, then $\alpha_i' \to 0$ as well, so that we may combine all the series that go to 0 as $\alpha_i \to 0$ to get a formula for $g^{\circ n} - \mathrm{id}$ of the desired form.

In preparation for the next proposition, we remark that for series in $\mathfrak{o}[[x]]$, coefficientwise convergence, $(\mathfrak{m}, x)$-adic convergence, convergence with respect to one $w_\rho$ for positive $\rho$, and convergence with respect to all $w_\rho$ for positive $\rho$ are equivalent. This is not the case for series in $k[[x]]$, however.

PROPOSITION 4.3. *If* $u \in \mathscr{G}_0(\mathfrak{o})$ *and* $u'(0) \in 1 + \mathfrak{m}$, *then the Lie logarithm* $\tilde{u}$ *is the limit of the functions* $(u^{\circ p^n} - \mathrm{id})/p^n$ *not only coefficientwise but also in the topology given by any* $w_\rho$ *for* $\rho > 0$. *It follows that* $\tilde{u}$ *is in* $\mathbf{A}$.

*Proof.* As in the proof of Proposition 2.2, we show that the limit exists by constructing an infinite product expansion of the Lie logarithm. Let us set

$$\Phi_n = \frac{u^{\circ p^n} - \mathrm{id}}{u^{\circ p^{n-1}} - \mathrm{id}},$$

so that by Lemma 4.2.3, $\Phi_n \in \mathfrak{o}[[x]]$. Since $u^{\circ p^n} - \mathrm{id} = (u - \mathrm{id})\Pi_{i=1}^n \Phi_i$, we have

$$\frac{u^{\circ p^n} - \mathrm{id}}{p^n} - \frac{u^{\circ p^{n-1}} - \mathrm{id}}{p^{n-1}} = \frac{u - \mathrm{id}}{p^n}\left(\prod_{i=1}^{n} \Phi_i - p \prod_{i=1}^{n-1} \Phi_i\right)$$
$$= (u(x) - x)\left(\prod_{i=1}^{n-1} \frac{\Phi_i}{p}\right)\left(\frac{\Phi_n}{p} - 1\right).$$

We clearly need to show, then, for each real $\rho > 0$, that for large enough $i$, $w_\rho(\Phi_i) = 1$, and that the limit in the $w_\rho$ topology of the $\Phi_n$'s is $p$. Since the second statement implies the first, there is only one thing to prove, and that follows directly from Lemma 4.2.4, since $\Phi_n = (g_n^{\circ p} - \mathrm{id})/(g_n - \mathrm{id})$, for $g_n = u^{\circ p^{n-1}}$, a sequence that has coefficientwise limit id, by Lemma 4.2.1. The already-constructed series $\tilde{u}$ is thus the limit, with respect to every $w_\rho$, of series in $\mathfrak{o}[[x]] \otimes_{\mathfrak{o}} K$, and thus is in $\mathbf{A}$.

The following proposition follows directly from Lemma 4.2.1, but its statement has been delayed so as not to interrupt the preceding exposition:

COROLLARY 4.3.1. *Let $u(x) \in \mathfrak{o}[[x]]$ with $u(0) = 0$ and $u(x) \equiv x \pmod{\mathfrak{m}}$, but $u \neq \mathrm{id}$. Then $u$ has only finitely many periodic points in $\bar{\mathfrak{m}}$, and thus cannot commute with a noninvertible $f \in \mathfrak{o}[[x]]$ of finite Weierstrass degree.*

*Proof.* By Lemma 4.2.1, there is an $i$ such that $u^{\circ p^i}(x) \equiv x \pmod{p}$, and so, if $\pi$ is a prime element of $\mathfrak{o}$, there is $j$ for which $u^{\circ p^i}(x) - x = \pi^j \alpha_i(x)$ with $0 < \mathrm{wideg}(\alpha_i) < \infty$ and with $j$ greater than the ramification index of $k$ over $\mathbb{Q}_p$. The number of roots of $u^{\circ p^i} - \mathrm{id}$ is equal to $\mathrm{wideg}(\alpha_i)$. But 4.2.1 again shows that for $n \geqslant 0$, $\mathrm{wideg}(\alpha_{i+n}) = \mathrm{wideg}(\alpha_i)$, and this is thus the number of periodic points of $u$. The noncommutation result follows because if $f$ has finite Weierstrass degree, then $\Lambda(f)$ is infinite.

Let us return to our discussion of the Lie logarithm $\tilde{u}$ of $u$. This series is convergent on all of $\bar{\mathfrak{m}}$, since it is in $\mathbf{A}$; its roots are precisely the periodic points of $u$, because of the product expansion $\tilde{u} = (u - \mathrm{id})\Pi_{i=1}^{\infty}(\Phi_i/p)$; $\tilde{u}'(0) = 0$ if and only if $u'(0)$ is a root of 1; and $\tilde{u} = 0$ if and only if $u$ itself is periodic. The construct has some of the properties of a logarithm, as the following shows.

LEMMA 4.4.1. *Let $u$ and $w$ be series in $\mathscr{G}_0(\mathfrak{o})$ that commute with each other. Then $(u \circ w)^\sim = \tilde{u} + \tilde{w}$. In particular, for $n \geqslant 0$, $(u^{\circ n})^\sim = n\tilde{u}$. By continuity, this relation remains true for $n \in \mathbb{Z}_p$.*

*Proof.* We have:

$$(u \circ w)^\sim(x) = \lim_{n \to \infty} \frac{(u \circ w)^{\circ p^n}(x) - x}{p^n}$$
$$= \lim \frac{u^{\circ p^n}(w,^{\circ p^n}(x)) - w^{\circ p^n}(x)}{p^n} + \lim \frac{w^{\circ p^n}(x) - x}{p^n}$$

$$= \tilde{u}(\lim w^{\circ p^n}(x)) + \tilde{w}$$
$$= \tilde{u} + \tilde{w},$$

and the remaining statements follow. Note that since $\tilde{u} \in \mathbf{A}$, it does make sense to substitute an $\mathfrak{o}$-series for the variable of $\tilde{u}$.

Consider any series $w$ that commutes with $u$: it permutes the fixed points of $u$, that is, the roots of $\tilde{u}$, and if we ignore the question of multiplicity of these roots, then $\tilde{u} \circ w$ should be related to $\tilde{u}$ by a factor that is a function in $\mathbf{A}$ without roots. These are simply the units of $\mathfrak{o}[[x]]$. Still ignoring the question of multiplicity, we have $w \mapsto \varphi_w$, satisfying $\tilde{u} \circ w = \varphi_w \cdot \tilde{u}$. One sees immediately that $\varphi$ is a one-cocycle of the centralizer of $u$, with values in the group of units of $\mathfrak{o}[[x]]$. The following lemma shows which cocycle $\varphi$ is.

LEMMA 4.4.2. *If $u$ and $w$ are series in $\mathscr{G}_0(\mathfrak{o})$ that commute with each other, then $\tilde{u} \circ w = w' \cdot \tilde{u}$.*

*Proof.* We may write $u^{\circ p^n}(x) - x = p^n\tilde{u}(x) + p^n g_n(x)$, where $\{g_n\}$ is a sequence of elements of $\mathbf{A}$ with limit 0. A fundamental difficulty in the calculation displayed below is that the operation of substituting a series in $\mathbf{A}$ for the variable in an $\mathfrak{o}$-series is not defined. So we will show that the series $\tilde{u} \circ w$ and $w' \cdot \tilde{u}$ are equal by working in $k[[x]]/(x^N)$ for an arbitrary $N$ and using $\mathfrak{m}$-adic convergence in this $N$-dimensional $k$-space. We have:

$$\tilde{u} \circ w = \lim_n \frac{u^{\circ p^n} \circ w - w}{p^n}$$
$$= \lim_n \frac{w \circ (\mathrm{id} + p^n\tilde{u} + p^n g_n) - w}{p^n}$$
$$= \lim_n \frac{w + (p^n\tilde{u} + p^n g_n)w' + (p^n\tilde{u} + p^n g_n)^2\gamma_n - w}{p^n}$$
$$= w' \cdot \tilde{u},$$

where the term $\gamma_n$ comes from the identity $w(x + t) = w(x) + tw'(x) + t^2\gamma(x, t)$, for $\gamma(x, t) \in \mathfrak{o}[[x, t]]$.

PROPOSITION 4.5. *Let $u$ be a stable invertible series in $\mathfrak{o}[[x]]$. Then $\mathbf{L}_u$, the logarithm of $u$, and the Lie logarithm $\tilde{u}$ satisfy the relation $\tilde{u} = \log(u'(0))\mathbf{L}_u/\mathbf{L}'_u$.*

*Proof.* Recall that for $\alpha \in 1 + \mathfrak{m}$, $\log \alpha$ is given by the familiar formula

$$\alpha - 1 - (\alpha - 1)^2/2 + (\alpha - 1)^3/3 - \cdots,$$

but also by the limit formula $\lim_n (\alpha^{p^n} - 1)/p^n$. The series $G = \tilde{u}$ and $G = \mathbf{L}_u/\mathbf{L}'_u$ satisfy the identity $G \circ u = u' \cdot G$ in $K[[x]]$. Thus $H = \tilde{u}\mathbf{L}'_u/\mathbf{L}_u \in k[[x]]$, a series for which $H \circ u = H$. It follows that $H$ is constant, and equal to the first-degree coefficient of $\tilde{u}$, which is $\log(u'(0))$.

COROLLARY 4.5.1. *If $u$ is stable and invertible, then no matter what the domain of convergence of the series $\mathbf{L}_u \in k[[x]]$, the formal series $\mathbf{L}_u/\mathbf{L}'_u$ is in $\mathbf{A}$, and thus is convergent on all of $\bar{\mathfrak{m}}$, and its roots are the periodic points of $u$.*

COROLLARY 4.5.2. *If $u$ is stable and invertible, then the domain of convergence of $\mathbf{L}_u$ cannot be so large as to contain any multiple roots of $\tilde{u}$.*

For, if the logarithm is defined and equal to zero at $\zeta$, then $\zeta$ is a simple root of $\mathbf{L}/\mathbf{L}'$.

Since the ordinary logarithm $\mathbf{L}_u$ is effectively computable by a degree-by-degree calculation, Proposition 4.5 gives a relatively quick way to calculate the Lie logarithm of $u$ if $u$ is stable. In case $u'(0) = 1$, there is an entirely different way to calculate $\tilde{u}$, which seems to be well known to combinatorialists. The interested reader may find much more material in the spirit of the rest of this section, in Chapter 3.7 of [C], on "fractionary iterates of formal series".

Indeed, consider two generic series $F = x + \Sigma_1^\infty a_i x^{i+1}$ and $G = x + \Sigma_1^\infty b_i x^{i+1}$, as well as $F \circ G = x + \Sigma_1^\infty C_i x^{i+1}$, where each $C_i$ is a polynomial in $a_1, \ldots, a_i, b_i, \ldots, b_i$ that is isobaric of weight $i$, where $a_j$ and $b_j$ have weight $j$. The linear part of $C_i$ is $a_i + b_i$, and these two are, furthermore, the only "pure" terms, every other monomial in $C_i$ necessarily containing at least one $a$ and at least one $b$, as one sees by specializing all the $a$'s or all the $b$'s to zero. It follows from this that we may write $F^{\circ n} = x + \Sigma_1^\infty A_{i,n} x^{i+1}$ where likewise $A_{i,n}$ is a polynomial that is isobaric in the $a_j$'s of weight $i$, and is a polynomial in $n$ of degree at most $i$. To see the dependence of $A_{i,n}$ on $n$, let us look first at $A_{1,n}$, clearly equal to $na_1$, and proceed inductively. We get the relation

$$\begin{aligned} A_{i,n} &= C_i(a_1, \ldots, a_i, A_{1,n-1}, \ldots, A_{i,n-1}) \\ &= a_i + A_{i,n-1} + \Gamma(a_1, \ldots, a_{i-1}, A_{1,n-1}, \ldots, A_{i-1,n-1}), \end{aligned}$$

where $\Gamma$ is the part of $C_i$ containing the monomials of degree greater than 1. Since every monomial of $\Gamma(a_1, \ldots, b_i)$ has at least one factor $a_j$, the total weight contributed by the $b$-factors is *less than* $i$, and as a result the degree of $\Gamma(a_1, \ldots, a_{i-1}, A_{1,n-1}, \ldots, A_{i-1,n-1})$ as a polynomial in $n$ is at most $i - 1$. But the relation

$$A_{i,n} - A_{i,n-1} = a_i + \Gamma(a_1, \ldots, a_{i-1}, A_{1,n-1}, \ldots, A_{i-1,n-1})$$

then guarantees that $A_{i,n}$ is a polynomial in $n$, of degree at most $i$. The coefficients of these polynomials are not integers, but rational numbers, but of course when the polynomials are written as linear combinations of the functions $\binom{n}{j}$, the coefficients are in $\mathbb{Z}[a_1, a_2, \ldots]$. These formulas also allow us to define $F^{\circ t} := x + \Sigma_1^\infty A_{i,t} x^{i+1}$, a series with coefficients in $K[t]$. Now from the original defining formula $\tilde{u} = \lim(u^{\circ p^n} - \mathrm{id})/p^n$, we see that if we denote

$$\frac{\partial}{\partial t} A_{i,t} = A'_{i,t}, \quad \text{then } \tilde{u}(x) = \Sigma\, A'_{i,0} x^i.$$

Thus we have a consistent definition, valid when $K$ is any field of characteristic zero and $u$ is a unipotent series over $K$, that $\tilde{u}$ is $\lim_{t \to 0}(u^{\circ t} - \mathrm{id})/t$. For the generic power series $F$ mentioned above, the Lie logarithm has the first few terms $a_1 x^2 + (a_2 - a_1^2)x^3 + (a_3 - \frac{5}{2}a_1 a_2 - \frac{3}{2}a_1^3)x^4$.

## 5. More Lie theory

In this section, we continue the investigation of the Lie logarithm of an invertible series, but we abandon the precise methods of proof used in the previous section, in favor of rather sketchier methods, to which the reader may add the necessary details.

Many of the results in this section are true in two settings: for invertible series over the complete local ring $\mathfrak{o}$, and, purely formally, for unipotent series over any field $K$ of characteristic zero. We state propositions in the latter case, but all proofs are left to the reader. We observe that $\mathbf{A}$ itself has the structure of a Lie algebra, not precisely the Lie algebra of the proalgebraic group $\mathscr{G}_0(\mathfrak{o})$, but close enough for our purposes. Similarly, $K[[x]]$ is the Lie algebra of the unipotent proalgebraic group $\mathscr{G}_0(K)$.

LEMMA 5.1. *The ring* $\mathbf{A}$ *has the structure of a k-Lie algebra, with the Lie bracket* $[f, g] = f' \cdot g - f \cdot g'$.

LEMMA 5.1(a). *The ring* $K[[x]]$ *has the structure of a K-Lie algebra, with the Lie bracket* $[f, g] = f' \cdot g - f \cdot g'$.

PROPOSITION 5.2. *Let u and w be invertible series over* $\mathfrak{o}$ *with* $u'(0) \equiv w'(0) \equiv 1 \pmod{\mathfrak{m}}$. *Then* $(w^{-1} \circ u \circ w)^{\sim} = \tilde{u} \circ w/w'$.

PROPOSITION 5.2(a). *Let u and w be unipotent series over K. Then* $(w^{-1} \circ u \circ w)^{\sim} = \tilde{u} \circ w/w'$.

*Proof of* 5.2. From the definition of $\tilde{u}$, we may approximate $u^{\circ p^n} \sim \mathrm{id} + p^n \tilde{u}$. Now let us write:

$$\begin{aligned}(w^{-1} \circ u \circ w)^{\circ p^n} &= w^{-1} \circ u^{\circ p^n} \circ w \\ &\sim w^{-1} \circ (\mathrm{id} + p^n \tilde{u}) \circ w \\ &= w^{-1} \circ (w + p^n \tilde{u} \circ w)\end{aligned}$$

$$\sim \mathrm{id} + ((w^{-1})' \circ w) \cdot p^n\tilde{u} \circ w$$
$$= \mathrm{id} + p^n(\tilde{u} \circ w)/w',$$

which shows the heart of the proof.

Note that in case $u$ and $w$ commute with each other, this is simply Lemma 4.4.2.

PROPOSITION 5.3. *Let $u$ and $w$ be invertible series over $\mathfrak{o}$ with $u'(0) \equiv w'(0) \equiv 1 \pmod{\mathfrak{m}}$. Then:*

$$\lim_{m,n\to\infty} \frac{u^{\circ p^m} \circ w^{\circ p^n} - w^{\circ p^n} \circ u^{\circ p^m}}{p^{m+n}} = [\tilde{u}, \tilde{w}].$$

PROPOSITION 5.3(a). *Let $u$ and $w$ be unipotent series over $K$. Then:*

$$\lim_{s,t\to 0} \frac{u^{\circ s} \circ w^{\circ t} - w^{\circ t} \circ u^{\circ s}}{st} = [\tilde{u}, \tilde{w}].$$

*Proof of* 5.3. As before, we approximate:

$$u^{\circ p^m} \circ w^{\circ p^n} \sim (\mathrm{id} + p^m\tilde{u}) \circ (\mathrm{id} + p^n\tilde{w})$$
$$= \mathrm{id} + p^n\tilde{w} + p^m\tilde{u} \circ (\mathrm{id} + p^n\tilde{w})$$
$$\sim \mathrm{id} + p^n\tilde{w} + p^m\tilde{u} + p^{m+n}\tilde{u}' \cdot \tilde{w},$$

which shows the idea of the proof.

COROLLARY 5.3.1. *If $u$ and $w$ are invertible series over $\mathfrak{o}$ that commute with each other, then $[\tilde{u}, \tilde{w}] = 0$, and $\tilde{u}$ and $\tilde{w}$ are linearly dependent over $k$.*

COROLLARY 5.3.1(a). *If $u$ and $w$ are commuting unipotent series over $K$, then $[\tilde{u}, \tilde{w}] = 0$, and $\tilde{u}$ and $\tilde{w}$ are linearly dependent over $K$.*

*Proof of* 5.3.1. We need prove only the second assertion. As Laurent series over $k$, either $\tilde{u}/\tilde{w}$ or $\tilde{w}/\tilde{u}$ is in $k[[x]]$, say the former. Then under our hypotheses, the formal derivative of $\tilde{u}/\tilde{w}$ is zero, by the first part of the conclusion, and so this series is a constant in $k$.

If $u$ and $w$ should happen to be stable, then the second part of the conclusion would follow from Proposition 4.5, since the hypothesis implies that $\mathbf{L}_u = \mathbf{L}_w$.

COROLLARY 5.3.2(a). *Let $u$ and $w$ be commuting unipotent series over $K$, and suppose that $u(x) \equiv x + ax^r \pmod{x^{r+1}}$ where $a \neq 0$, but $w(x) \equiv x \pmod{x^{r+1}}$. Then $w = \mathrm{id}$.*

Proof. Since $u^{\circ k}(x) \equiv x + akx^r \pmod{x^{r+1}}$, $\tilde{u} \equiv ax^r \pmod{x^{r+1}}$. But $\tilde{w} = b\tilde{u}$ for $b \in K$ and $w(x) \equiv x \pmod{x^{r+1}}$ together imply that $b = 0$. But $\tilde{w} = 0$ and $w(x) \equiv x \pmod{x^2}$ imply that $w = \mathrm{id}$.

PROPOSITION 5.4 ($=1.5$). *Let $K$ be a field of characteristic zero, and let $g(x) \in \mathcal{G}_0(K)$, with $g(x) \equiv x + ax^r \pmod{x^{r+1}}$, where $a \neq 0$. Then the centralizer of $g$ in $\mathcal{G}_0(K)$ is the direct sum of the cyclic group of all* $(r-1)$th *roots of 1 in $K$ and the additive group of $K$.*

*Proof.* By Proposition 1.4, we may assume from the outset that $g$ has nonzero coefficients only in monomials of degree congruent to 1 modulo $r-1$. Now, as remarked at the end of Section 4, $g^{\circ n}(x) = \Sigma_i A_{i,n} x^{i+1}$, where the coefficients are $K$-polynomials in $n$. So we may write $g^{\circ t}(x) \in K[[t]][[x]]$, an algebraic family of series, necessarily commuting with $g$. Furthermore, $A_{i,t} = 0$ whenever $(r-1) \nmid i$, since these are polynomials that vanish at every natural integer in $K$. In particular, if we define $U_\zeta(x) = \zeta x$ for any $(r-1)$th root $\zeta$ of 1 in $K$, then $U_\zeta$ and $g^{\circ c}$ commute with $g$ and each other no matter what $c$ is in $K$. So the centralizer of $g$ in $\mathcal{G}_0(K)$ is at least as large as claimed. On the other hand, suppose that $h \in \mathcal{G}_0(K)$ and $h$ commutes with $g$. Then $h$ cannot be stable, since in that case, $g$ would be a nonidentity series commuting with $h$ with $g'(0) = 1$, contradicting Proposition 1.1. Thus $h'(0)$ is a root of 1, say $\zeta^{-1}$, and we write $\bar{h} := U_\zeta \circ h \equiv x \pmod{x^2}$. This new series commutes with $g$, so that its Lie logarithm is a $K$-multiple of $\tilde{g}$, and consequently $\bar{h}(x) \equiv x + acx^r \pmod{x^{r+1}}$, for some $c \in K$. Finally, $\bar{h} \circ g^{\circ -c}$ commutes with $g$ and is congruent to $x$ modulo $x^{r+1}$, and so equals the identity, by 5.3.2(a).

## 6. The Main Theorem

In the case that a dynamical system over the ring of local integers $\mathfrak{o}$ arises from a formal group, i.e. when we are discussing the properties of the iterates of an endomorphism of a formal group defined over $\mathfrak{o}$, the full commuting family contains both invertible and noninvertible series. Recall that an endomorphism of a formal group has Weierstrass degree $p^H$ for some natural number $H$, and is invertible if and only if $H = 0$; $p$ is the residue characteristic of $\mathfrak{o}$. Experimental evidence seems to suggest that for an invertible series to commute with a noninvertible series, there must be a formal group somehow in the background. Our Main Theorem supports this conjecture, in that it says that the only possible finite Weierstrass degree for such a noninvertible series is a power of $p$.

To prove this theorem we make use of several of our previous results, as well as some considerations special to series in characteristic $p$.

DEFINITION. Let $\kappa$ be a field of characteristic $p > 0$, and $f(x) \in \mathscr{S}_0(\kappa)$. We will call $f$ *separable* when $f' \neq 0$. If $f \neq 0$ and $d$ is the largest integer for which there is a series $g \in \kappa[[x]]$ with $f(x) = g(x^{p^d})$, we call $p^d$ the *radicial degree* of $f$.

One sees easily, for instance via Weierstrass preparation, that $f$ is separable if and only if the field extension $\kappa(x))/\kappa((f(x))$ is separable. It is also the case that the series $g$ mentioned in the definition above will necessarily be separable, and that $p^d$ and wideg($g$) are the radicial (inseparable) degree and separable degree, respectively, of $\kappa((x))$ over $\kappa((f(x)))$.

LEMMA 6.1. *Let $\kappa$ be a finite field of cardinality $q = p^m$, and let $\Phi(x) = x^q$. Let $f \in \mathscr{S}_0(\kappa)$, with radicial degree $p^d$. Then $f^{\circ m} = F \circ \Phi^{\circ d}$, where $F$ is a separable series in $\kappa[[x]]$.*

*Proof.* Let us call $\varphi(x) = x^p$. Our hypothesis is that $f = g \circ \varphi^{\circ d}$, with $g$ separable. We have $\varphi \circ g = g^{(p)} \circ \varphi$, where for any natural number $r$ we call $g^{(r)}$ the series gotten from $g$ by raising its coefficients to the $r$th power, and thus

$$f^{\circ m} = g \circ g^{(p^d)} \circ g^{(p^{2d})} \circ \cdots \circ g^{(p^{(m-1)d})} \circ \varphi^{\circ md}.$$

A composition of separable series is separable, and $\varphi^{\circ md} = \Phi^{\circ d}$, so we are done.

COROLLARY 6.1.1. *Let $\kappa$ be a field of cardinality $q = p^m$, and let $u$ and $f$ be commuting elements of $\mathscr{S}_0(\kappa)$. Then $u$ commutes as well with the series $F$ of Lemma 6.1.*

*Proof.* The series $u$ commutes with $\Phi$.

LEMMA 6.2. *Let $\kappa$ be a field of characteristic $p > 0$, and let $F$ be a separable noninvertible element of $\mathscr{S}_0(\kappa)$. If $u(x) \equiv x \pmod{x^2}$ is an element of $\mathscr{G}_0(\kappa)$ that commutes with $F$, then $u$ is a torsion element of the group $\mathscr{G}_0(\kappa)$.*

*Proof.* We mean to show that series $u(x) \neq x$ that are too close to the identity series $x$ cannot commute with $F$.

Let the initial (Weierstrass) degree of $F$ be $\delta$, and the initial degree of $F'$ be $\delta'$, so that $\delta' \geqslant \delta - 1$. Take $u(x) \equiv x + ax^r \pmod{x^{r+1}}$ with $a \neq 0$, and let us compare $u \circ F$ and $F \circ u$. In $\kappa[[x, t]]$ we have $F(x + t) = F(x) + F'(x)t + t^2\psi(x, t)$ for a suitable $\psi \in \kappa[[x, t]]$. If we write $u(x) = x + ax^r + x^{r+1}g(x)$ for $g \in \kappa[[x]]$, we then have

$$F(u(x)) = F(x) + ax^rF'(x) + x^{r+1}F'(x)g(x) + (ax^r + x^{r+1}g(x))^2\Psi(x)$$

for a suitable $\Psi \in \kappa[[x]]$, so that $F \circ u - F$ has initial degree $r + \delta'$ if $r > \delta'$. On the other hand $u(F(x)) - F(x) \equiv 0 \pmod{x^{\delta r}}$, and since $\delta > 1$, the inequality $r > \delta'$ guarantees that $\delta r > r + \delta'$: $F \circ u$ and $u \circ F$ cannot be equal. The proof is now complete, because as remarked at the beginning of the proof of

Proposition 4.1, in the $(x)$-adic topology the $p$-power iterates of $u$ approach the identity.

COROLLARY 6.2.1. *Let $\kappa$ be a finite field, and let $u$, $f \neq 0$ be invertible and noninvertible, respectively, in $\mathcal{S}_0(\kappa)$, commuting with each other. Then either $u$ is a torsion element of $\mathcal{G}_0(\kappa)$ or $f$ has the form $f(x) = g(x^{p^d})$ with $d > 0$, and $g \in \mathcal{G}_0(\kappa)$.*

*Proof.* Let $p^d$ be the radicial degree of $f$, and write $f(x) = g(x^{p^d})$ with $g$ separable. Let $m = [\kappa : \mathbb{F}_p]$, so that by 6.1.1, we have $f^{\circ m} = F \circ \Phi^{\circ d}$, with $F$ a separable element of $\mathcal{S}_0(\kappa)$ that commutes with $u$. Now either $F$ is noninvertible, in which case $u$ must be torsion, or $F$ is invertible, and since $F = g \circ h$ for a suitable $h$, as in the proof of 6.1, it follows that $g$ is also invertible, and thus $\Phi^{\circ d}$ is noninvertible: $d > 0$.

MAIN THEOREM. 6.3. *Let $\mathfrak{o}$ be the ring of integers in a finite extension field $k$ of $\mathbb{Q}_p$, and let $u$, $f$ be invertible and noninvertible, respectively, in $\mathcal{S}_0(\mathfrak{o})$. Suppose further that $u \circ f = f \circ u$ and that $f$ has finite Weierstrass degree $\delta$. Then either some iterate of $u$ is the identity, or $\delta = p^d$ for some $d > 0$.*

*Proof.* By replacing $u$ by $u^{\circ n}$ for suitable $n$, we may assume that $u'(0) \equiv 1 \pmod{\mathfrak{m}}$. Let $\bar{u}$ and $\bar{f}$ be the corresponding series over the residue field $\kappa$; the previous corollary applies, so that either $\bar{f}$ has initial degree $p^d$ with $d > 0$ or $\bar{u}$ is torsion. In the latter case, we again replace $u$ by an iterate, so that $u(x) \equiv x \pmod{\mathfrak{m}}$, and Corollary 4.3.1 now implies that $u = \mathrm{id}$.

## 7. Examples

Foremost among examples is the commuting family coming from the multiplicative formal group $\mathcal{M}(x, y) = x + y + xy$. Its endomorphisms are precisely the series $[a](x) := (1 + x)^a - 1$ for $a \in \mathbb{Z}_p$. Note that the binomial coefficients that appear are necessarily $p$-integral. The identity $[a_1] \circ [a_2] = [a_1 a_2]$ always holds. The polynomials

$$[p](x) = (1 + x)^p - 1 = px + p(p - 1)x^2/2 + \cdots + px^{p-1} + x^p$$

and $[p + 1](x)$ are particularly interesting, as noninvertible and invertible series, respectively. The reader will recognize this commuting family as the $p$-adic local version of the family of complex mappings $z \mapsto z^n$. The logarithm of this family is the ordinary log, appropriately shifted: $\mathbf{L}(x) = x - x^2/2 + x^3/3 - \cdots$. The derivative of $\mathbf{L}$ is $1/(1 + x)$. The set $\Lambda$ is the set of all $\zeta - 1$, where $\zeta$ runs through the $p$-power roots of 1 in an algebraic closure of $\mathbb{Q}_p$. If $a \in \mathbb{Z}_p$ and $a \equiv 1 \pmod{p}$, then according to 4.5, $[a]^{\sim}(x) = \log(a)(1 + x)\mathbf{L}(x) = \log(a)(x + x^2/2 - x^3/6 + x^4/12 - \cdots)$.

If $F = F(x, y)$ is a one-dimensional formal group over $\mathfrak{o}$, then the endomorphism ring of $F$ always contains $\mathbb{Z}_p$. More precisely for each $a \in \mathbb{Z}_p$

there is an endomorphism $[a]_F(x) \in \mathfrak{o}[[x]]$ with $[a](x) = ax + \cdots$, and these series commute with each other, although the total commuting family $\mathrm{End}_F$ may be larger than $\mathbb{Z}_p$. The logarithm of the commuting family satisfies $\mathbf{L}'(x) = 1/F_1(0, x)$, where the subscript denotes partial differentiation with respect to the left-hand variable of $F$. In particular, every root of $\mathbf{L}$ is simple.

If $F$ is any one-dimensional formal group over $\mathfrak{o}$, then it is an easy exercise to use the existence of the group of $p - 1$th roots of 1 in $\mathbb{Z}_p$ to recoordinatize $F$ so that its only nonzero coefficients belong to monomials of total degree $\equiv 1 \pmod{p-1}$. The same happens to the recoordinatized endomorphisms, and this commuting family clearly has what might be called a "condensation": for $f$ in the original family, we write $\hat{f}(x) := (f(x^{1/(p-1)})^{p-1}$. That is, if $f(x) = xg(x^{p-1})$, then $\hat{f}(x) = x(g(x))^{p-1}$. These condensed series certainly are not endomorphisms of any formal group, since with the exception of 0, every root of $\mathbf{L}_{\hat{f}}$ has multiplicity $p - 1$.

The Čebyšev polynomials commute with each other in the sense of substitution, so we can expect that they belong to a commuting family of the type we have been examining. In fact there are two such families, closely related. Recall that the Čebyšev polynomials $T_n(x) \in \mathbb{Z}[x]$ satisfy the defining relation $T_n(\frac{1}{2}(x + 1/x)) = \frac{1}{2}(x^n + 1/x^n)$. It is clear from this that all the Čebyšev polynomials have 1 for a fixed point, and that the odd-index polynomials have the common fixed point 0. Let us look first at the odd Čebyšev polynomials. We have $T_{2k+1}(x) = 2^{2k}x^{2k+1} + \cdots + (-1)^k(2k + 1)x$, and if $p$ is an odd prime, then $T_p(x) \equiv x^p \pmod{p}$, and $T_p(x) \equiv (-1)^{(p-1)/2}px \pmod{x^2}$. It follows from Tate's basic construction lemma in [LT] that $T_p$ is an endomorphism of a formal group $\mathscr{F}_p$ defined over the local ring $\mathbb{Z}_{(p)} \subset \mathbb{Q}$. If we call $T_p$'s logarithm $\mathbf{L}_p$, then $\mathscr{F}_p$ can be described as $\mathbf{L}_p^{\circ(-1)}(\mathbf{L}_p(x) + \mathbf{L}_p(y))$. Since the various Čebyšev polynomials commute with each other, all the logarithms are equal, and thus all the formal groups are equal: we have one formal group $\mathscr{F}$, coefficients $p$-integral for all odd $p$, so that $\mathscr{F}(x, y) \in \mathbb{Z}[\frac{1}{2}][[x, y]]$, and it has the odd-index Čebyšev polynomials among its endomorphisms. Indeed, we might call $\mathscr{F}$ the "Čebyšev formal group"; it has the expansion

$$\begin{aligned}\mathscr{F}(x, y) = x + y &- 2^{-1}(x^2y + xy^2) - 2^{-3}(x^4y + xy^4)\\ &- 2^{-4}(x^6y + xy^6) - 5\cdot 2^{-7}(x^8y + xy^8)\\ &- 7\cdot 2^{-8}(x^{10}y + xy^{10}) - 21\cdot 2^{-10}(x^{12}y + xy^{12})\\ &- 33\cdot 2^{-11}(x^{14}y + xy^{14}) - 429\cdot 2^{-15}(x^{16}y + xy^{16}) + \cdots,\end{aligned}$$

which is astonishing in that the $n$th degree form, instead of having $n - 1$ terms, seems to have only two.

By a change of coordinates, we may move the common fixed point 1 of all the Čebyšev polynomials to the origin: put $\mathcal{T}_n(x) = T_n(x+1) - 1$. One checks that the $r$th-degree coefficient of $\mathcal{T}_n$ is divisible by $2^{r-1}$, so that we may modify the 2-adic radius of convergence to get $\hat{\mathcal{T}}_n(x) = 2\mathcal{T}_n(x/2) \in \mathbb{Z}[x]$; indeed these polynomials are all monic. They too fit into a $p$-adic commuting family for each prime $p$, but they are not endomorphisms of any formal group, since for $p = 2$, every $\hat{\mathcal{T}}_{4n}$ has double roots, and for odd $p$, every $\hat{\mathcal{T}}_{pn}$ has double roots. The $\hat{\mathcal{T}}$'s of odd index may also be derived from the corresponding $T$'s by a homothetic change of coordinate and a condensation of degree 2.

## 8. Index of notations

$\mathcal{S}_0(A))$: the monoid of series over $A$ with no constant term (§0).
$\mathcal{G}_0(A))$: the group of invertible elements of $\mathcal{S}_0(A)$. (§0)
$\mathbb{Q}_p$: field of $p$-adic numbers.
$\mathbb{Z}_p$: ring of $p$-adic integers.
$\mathrm{Comm}_A(f)$: the commutant monoid of a stable series $f$ (§0).
$\kappa$: any field of characteristic $p$.
$\mathfrak{o}$: complete local ring, with maximal ideal $\mathfrak{m}$ and residue field $\kappa$. Especially, the ring of integers in a finite extension $k$ of $\mathbb{Q}_p$.
$v$: additive valuation on $\mathbb{Q}_p$, normalized so that $v(p) = 1$, extended to any algebraic extension $k$ of $\mathbb{Q}_p$.
$v_f$: the valuation function of a series $f$ (§0).
$w_\rho$: rank-one valuation of $\mathfrak{o}[[x]] \otimes_\mathfrak{o} k$ belonging to elements of $\bar{k}$ of valuation $\rho$ (§0).
$\mathbf{A} = \mathbf{A}(k)$: completion of $\mathfrak{o}[[x]] \otimes_\mathfrak{o} k$ with respect to uniform convergence on "bounded subdisks" of the unit disk (§0).
$\mathrm{wideg}(f)$: the Weierstrass degree of the series $f$ (§0).
$\Lambda(f)$: the set of roots of iterates of the noninvertible series $f$ (2.1).
$\Lambda(u)$: the set of periodic points of the invertible series $u$ (3.1).
$f^{\circ n}$: the $n$-fold iterate of $f$.
$\mathbf{L}_f$: the logarithm of the transformation $f$, satisfying the identity $\mathbf{L}_f \circ f = f'(0)\mathbf{L}_f$ and the normalization $\mathbf{L}_f(x) \equiv x \pmod{x^2}$ (1.2).
$\tilde{u}$: the Lie logarithm of an invertible series $u$ (4.1).

## References

[BM] S. Ben-Menahem: $p$-adic iterations, preprint, Tel-Aviv University Physics 1627–88 (1988).
[C] L. Comtet: *Advanced Combinatorics*, Reidel, 1974.
[Fr] A. Fröhlich: *Formal Groups*, Lecture Notes in Mathematics, vol. 74, Springer-Verlag, 1968.
[H] M. Hazewinkel: *Formal Groups and Applications*, Academic Press, 1978.

[La1] M. Lazard: Les zéros des fonctions analytiques d'une variable sur un corps valué complet, *Inst. Hautes Etudes Sci. Publ. Math.* 14 (1962) 47–75.

[La2] M. Lazard: *Commutative Formal Groups*, Lectures Notes in Mathemaics, vol 443, Springer-Verlag, 1975.

[Lu] J. Lubin: Canonical subgroups of formal groups, *Trans. Amer. Math. Soc.* 251 (1979) 103–127.

[LT] J. Lubin and J. Tate: Formal complex multiplication in local fields, *Ann. Math.* 81 (1965) 380–387.

[Sen] S. Ren: Ramification in $p$-adic Lie extensions, *Invent. Math.* 17 (1972) 44–50.

[Ser] J.-P. Serre: Sur les groupes de Galois attachés aux groupes $p$-divisibles, in *Proceedings of a Conference on Local Fields held at Driebergen*, Springer-Verlag, 1966.

[T] J. Tate: $p$-divisible groups, in *Proceedings of a Conference on Local Fields held at Driebergen*, Springer-Verlag, 1966.

[TVW] E. Thiran, D. Verstegen and J. Weyers: $p$-adic dynamics, *J. Stat. Phys.* 54 (1989) 893–913.