

# $p$ -adic Dynamics and Formal Groups

Cam McLeman

August 25, 2002

## Abstract

We present an expository introduction to the theory relating the world of  $p$ -adic numbers to that of formal groups. We deal specifically with the theory behind, and progress toward, a conjecture by Lubin [6] dealing with sets of power series that commute, under formal composition, with a given power series. In addition, we prove a new result concerning limits of these sets.

## 1 Introduction

The topic at hand revolves around the operation of formal function composition. The formality of this operation is important. Given two functions  $f(x)$  and  $g(x)$ , their composition is the function  $(f \circ g)(x) = f(g(x))$ . We say that two functions commute under composition if the functions  $(f \circ g)(x)$  and  $(g \circ f)(x)$  are equal. It is clear that the polynomials  $f(x) = x^m$  and  $g(x) = x^n$  commute under composition for any  $m, n \in F$  (i.e.  $(f \circ g)(x) = (g \circ f)(x) = x^{m+n}$ ). Thus we have a set of polynomials  $\{f_k = x^k\}_{k \in F}$  that all commute with each other. We call such a set a *commuting family*. A slightly less trivial commuting family is the set of functions  $g_\ell = (x+1)^\ell - 1$ . The reader can verify that any two of these polynomials indeed commute under composition. More generally, we will give our attention to the theory of commuting power series. The notion of commuting families of power series gives rise to some fundamental questions. Can we partition the set of power series into sets of commuting power series? What deeper underlying structure governs which power series fit in which partition?

The purpose of this paper is to exposit an introduction to the general theory behind this phenomenon, tying these questions to the theory of formal groups and  $p$ -adic analysis. In addition, we will examine a conjecture by Jonathan

Lubin attempting in part to answer some of the above questions, as well as introduce a new result. We begin with a brief introduction to formal groups.

## 2 Formal Groups

The need for an introduction to formal groups is exasperated by their somewhat misleading name. Specifically, a source of confusion stems from the fact that formal groups are (brace yourself) *not groups*. Quite to the contrary, a formal group isn't even associated with a collection of objects. Loosely, we use the term "formal group" to represent a possible group law, though in actuality, they are defined as power series [9].

**Definition 2.1.** *If  $R$  is a ring, then a formal group defined over  $R$  is a power series  $F(x, y) \in R[[x, y]]$  satisfying:*

- $F(x, y) = x + y \pmod{xy}$
- $F(x, F(y, z)) = F(F(x, y), z)$
- $F(x, y) = F(y, x)$ .
- *There is a unique power series  $i(t) \in R[[t]]$  satisfying  $f(t, i(t)) = 0$ .*
- $F(x, 0) = x$  and  $F(0, y) = y$ .

The definition essentially guarantees us that, in a sense, we have commutativity, associativity, inverses, and an identity for this formal group. Of course, this identity and these inverses are not elements of any set or group, per se, but merely perform a function which, when applied in our formal group, resembles that of being an identity or an inverse. This set of requirements is not minimal. For example, we show below how the last of these requirements can be derived from the first three.

*Proof.* We wish to show that  $F(x, 0) = x$ . The proof that  $F(0, y) = y$  is nearly identical. We first note that  $F(x, 0)$  must contain only powers of  $x$ , since any term with a  $y$  will vanish upon setting  $y = 0$ . Thus, write  $F(x, 0) = x + a_2x^2 + a_3x^3 + \dots$ . Now, by the associativity requirement, we have  $F(x, F(0, 0)) = F(F(x, 0), 0)$ . Evaluating the left-hand side, we get  $F(x, F(0, 0)) = F(x, 0)$ . Evaluating the right-hand side, we get  $F(F(x, 0), 0) = F(x, 0) + a_2F(x, 0)^2 + \dots$ . Equating these two, we get that  $F(x, 0) = F(x, 0) + a_2F(x, 0)^2 + a_3F(x, 0)^3 + \dots$ , implying that all  $a_i$  are 0 for  $i \geq 2$ .  $\square$

It is worth noting that the notion of whether or not a particular formal group's power series converges is *not* an issue, since  $x$  and  $y$  have no numerical value with respect to any absolute value. In an attempt to solidify the definition of a formal group, it will be helpful to have a range of examples in one's mind.

**Example 2.2.** *The formal additive group is given by the power series:*

$$F^+(x, y) = x + y.$$

**Example 2.3.** The formal multiplicative group is given by the power series:

$$F^*(x, y) = (1 + x)(1 + y) - 1 = x + y + xy.$$

In addition to these simple arithmetic formal groups, there are many other examples of formal groups, often quite elaborate:

**Example 2.4** ([10]). The Jacobi formal group is given, for  $a, b \in R$ , by

$$F_{a,b}(x, y) = \frac{x\sqrt{1 - 2ay^2 + by^4} + y\sqrt{1 - 2ax^2 + bx^4}}{1 - bx^2y^2}.$$

## 2.1 Maps Between Formal Groups

Perhaps more directly useful to us than formal groups are the maps between formal groups. We will see later this chapter that it is through these maps that we begin to relate this topic to that of  $p$ -adic numbers.

**Definition 2.5.** A homomorphism between formal groups  $F$  and  $G$ , both over a ring  $R$ , is a power series  $f(T) \in R[[T]]$  satisfying

- $f(0) = 0$
- $f(F(x, y)) = G(f(x), f(y))$ .

**Example 2.6.** The power series<sup>1</sup>  $f(T) = \text{LOG}(T) = \sum_{n=1}^{\infty} (-1)^{n-1} T^n / n$  is a homomorphism from the formal multiplicative group  $F^*$  to the formal additive group  $F^+$ .

This should mesh with our intuitions of the logarithm function. The arithmetic identity that  $\log(ab) = \log(a) + \log(b)$  illustrates that, in a sense, the logarithm maps multiplication to addition via a formal group homomorphism. Properties of the real and complex logarithms can be viewed as corollaries of this result, once convergence issues are taken into consideration. Similarly, we can define an analog of the exponential function that is a homomorphism from  $F^+$  to  $F^*$ :

**Example 2.7.** The power series  $\text{EXP}(x) = \sum_{n=1}^{\infty} x^n / n!$  is a homomorphism from the formal additive group  $F^+$  to the formal multiplicative group  $F^*$ .

Of particular importance to us is the set of all homomorphisms of a formal group to itself (endomorphisms). The collection of endomorphisms with coefficients in a ring  $R$  is denoted  $\text{End}_R(F)$ . It is not difficult to show that the sum and product of two endomorphisms of a given formal group are themselves endomorphisms of that formal group. Consequently, one often refers to the *endomorphism ring* of a formal group  $F$ ,  $\text{End}_R(F)$ .

---

<sup>1</sup>We use the term *LOG* to distinguish from the real logarithm function. This function has no branch cuts, is defined everywhere, doesn't have convergence issues, etc.

**Example 2.8.** All functions  $f_n(x) = (x + 1)^n - 1$  are endomorphisms of the multiplicative formal group  $F^*(x, y) = (1 + x)(1 + y)$ .

*Proof.*

$$\begin{aligned}
 F^*(f_n(x), f_n(y)) &= F^*((x + 1)^n - 1, (y + 1)^n - 1) \\
 &= (1 + (x + 1)^n - 1)(1 + (y + 1)^n - 1) - 1 \\
 &= (x + 1)^n (y + 1)^n - 1 \\
 &= ((x + 1)(y + 1))^n - 1 \\
 &= (F^*(x, y) + 1)^n - 1 \\
 &= f_n(F^*(x, y)).
 \end{aligned}$$

□

This development of the relationship between formal groups and power series, via these endomorphisms, will be important in the upcoming sections, particularly once Lubin's conjecture is addressed. In the meantime, we have yet to link power series with  $p$ -adic numbers, so we do so now.

## 3 The Link

### 3.1 $p$ -adic Dynamics and Formal Groups

A crucial bump in the road toward comprehension of the topic at hand lies in understanding the link between the two centerpieces of this theory:  $p$ -adic analysis and formal groups. At first, the two seem tangential at best, but the relating process begins when we set the above ring  $R$  to be any finite algebraic extension of the field of  $p$ -adic numbers  $\mathbb{Q}_p$ ,  $K$ . We will also be interested in extensions  $\mathcal{O}$  of the set of  $p$ -adic integers  $\mathbb{Z}_p$ . We will use the notation  $K$  and  $\mathcal{O}$  for the remainder of the paper, but the reader should keep in mind the respective instantiations of  $\mathbb{Q}_p$  and  $\mathbb{Z}_p$ . The specific property of interest here is that  $\mathbb{Z}_p$  is a *local ring*, a ring with a unique maximal ideal consisting of the ring's non-invertible elements.

**Proposition 3.1** ([1]). *If  $K$  is a field and  $|\cdot|$  is a non-archimedean absolute value on  $K$ , then the set*

$$\mathcal{O} = \{x \in K : |x| \leq 1\}$$

*is a (local) subring of  $K$ , with unique maximal ideal*

$$\mathcal{M} = \{x \in K : |x| < 1\}.$$

**Remark 3.2.** *In the special case from above where  $K = \mathbb{Q}_p$  and  $\mathcal{O} = \mathbb{Z}_p$ , we have that  $\mathcal{M} = p\mathbb{Z}_p$ .*

We let  $\mathcal{O}^*$  denote the complement of  $\mathcal{M}$  in  $\mathcal{O}$ , so that  $\mathcal{O}^*$  is the set of invertible elements in  $\mathcal{O}$ . We can express  $\mathcal{O}$  as the disjoint union  $\mathcal{O} = \mathcal{M} \cup \mathcal{O}^*$ . We also now define the residue field  $k = \mathcal{O}/\mathcal{M}$ , though we will not discuss  $k$  extensively. We now turn to the ring of 1-variable power series over the algebraic structures  $K$  and  $\mathcal{O}$ , respectively denoted  $K[[x]]$  and  $\mathcal{O}[[x]]$ .

### 3.2 Invertibility of Power Series

A natural question arising when dealing with the composition of power series is when a particular series  $u(x) \in \mathcal{O}[[x]]$  is *invertible* under composition; i.e. for what power series  $u$  does there exist a  $v$  such that  $u(v(x)) = x$  formally. A non-invertible series is a series  $f(x)$  with no such inverse  $v$ . The following surprising theorem establishes the link between the above algebraic structures and the theory of power series:

**Theorem 3.3 (Invertibility Theorem).** *A power series  $f(x) \in \mathcal{O}[[x]]$  is invertible iff  $f'(0) \in \mathcal{O}^*$ . Consequently,  $f$  is non-invertible iff  $f'(0) \in \mathcal{M}$ .*

**Remark 3.4.** *First, note that  $f'(0)$  is simply the coefficient of the  $x$  term in the power series  $f$ . Thus, the (surprising) result of this theorem is that the invertibility of a power series under composition is dependent entirely on the invertibility of its  $x$  coefficient in the field  $K$ .*

*Proof.* For the first direction of the proof, assume that  $f(x) = a_1x + a_2x^2 + \dots$  is invertible, with inverse  $g(x)$ . By the above remark, we need only show that  $f'(0) \in \mathcal{O}^*$ . Write  $g(x) = b_1x + b_2x^2 + \dots$ . Now, we note that the  $x$  coefficient of  $f(g(x))$  is  $a_1b_1$ . For  $f(g(x))$  to equal  $x$ , we must have  $a_1b_1 = 1$ . But, of course, this implies that  $b_1 = a_1^{-1}$ , so that  $a_1 = f'(0) \in \mathcal{O}^*$ . The opposite direction is similar, but somewhat more lengthy.  $\square$

The following theorem gives an example of a powerful link between the theory of formal groups and that of invertible power series.

**Proposition 3.5 ([10]).** *If  $R$  is an algebra over  $\mathbb{Q}$ , then there is a bijection between the set of invertible power series over  $R$  and the set of all formal groups over  $R$ .*

### 3.3 Introduction to Commuting Power Series

We now turn specifically to some of the theory relating to power series which commute under composition, beginning with a few definitions.

**Definition 3.6.** *If  $R$  is a ring, then we denote by  $\mathfrak{F}_0(R)$  the set of all power series  $f \in R[[x]]$  with  $f(0) = 0$  (i.e.  $f$  has zero constant term).*

The theory of commuting power series becomes much more concrete upon placing a couple of restrictions on the power series  $f$ , and we will use these assumptions to define a new class of power series.

**Definition 3.7.** A power series  $f \in \mathfrak{F}_0$  is stable if  $f'(0)$  is neither 0 nor a root of unity. The set of stable series over  $R$  is denoted by  $S_0(R)$ .

It is these stable series that attract our attention the most. The motivation for these restrictions are not immediately clear, but we will defer their motivation until more of the theory has been developed.

**Definition 3.8.** The commutant monoid  $\text{Comm}_R(f)$  of a power series is the set of power series in  $R[[x]]$  that commute with  $f(x)$  under composition.<sup>2</sup> A subset  $\mathfrak{C}$  of  $\mathfrak{F}_0$  is a commuting family if  $\mathfrak{C} = \text{Comm}_R(f)$  for some  $f \in \mathfrak{F}_0$ .

In the case where our base structure is a field, we get a somewhat amazing theorem:

**Theorem 3.9 (Comm Isomorphism Theorem).** If  $K$  is a field and  $f \in S_0(K)$ , then the map  $\phi : \text{Comm}_K(f) \rightarrow K$  given by  $\phi(g) = g'(0)$  is a bijection. The operation of addition in the field corresponds to addition of power series, and field multiplication corresponds to power series composition.

This theorem says that the commutant monoid of a stable series over a field is isomorphic to the field itself. Given  $f$  and an element  $c \in K$ , in other words, we can find the unique power series  $g \in \mathfrak{F}_0$  such that  $(f \circ g)(x) = (g \circ f)(x)$  and  $g'(0) = c$ . We introduce notation for this phenomenon, and then provide an example of how to construct such a commutant monoid.

**Definition 3.10.** We denote by  $[c]_f$  the unique power series in  $\mathfrak{F}_0$  with  $f \circ [c]_f(x) = [c]_f \circ g(x)$  and whose  $x$ -coefficient is  $c$ . Note that for any  $f$ , we have  $[0]_f(x) = 0$  and  $[1]_f(x) = x$ .

**Remark 3.11.** Via the analogy between commutant monoids and endomorphism rings of formal groups, we similarly denote by  $[c]_F$  the unique endomorphism of a formal group  $F$  whose linear term is  $cx$ . Consequently, we have that  $\{[a]_F\}_{a \in \mathcal{O}} \subset \text{End}_{\mathcal{O}}(F)$ . The question of when this containment is proper is very interesting, and discussed, for example, in [9]. Like above, we have  $[0]_F(x) = 0$ ,  $[1]_F(x) = x$ , and can define  $[n]_F(x) = F([n-1]_F(x), x)$  recursively for any  $n \in \mathbb{N}$ .

We now return to apply our definition of a stable series to the theory of commuting power series. Over a field, in fact, Lubin gives a relatively simple test for determining whether or not two power series commute under composition:

**Theorem 3.12 (Logarithm Existence Theorem [6]).** If  $f$  is a stable series over a field  $R$ , then there exists a unique series  $L_f(x) \in \mathfrak{F}_0$  with  $L_f'(0) = 1$  satisfying the functional equation  $(L_f \circ f)(x) = f'(0)L_f(x)$ . (This series is called the logarithm of  $f$ ).

---

<sup>2</sup>A monoid is an algebraic structure that is non-commutative, associative, and has an identity. The fact that this set is a monoid is unimportant, but the terminology is standard so we use it here.

**Remark 3.13.** *The reasons behind calling this function a logarithm is intimately connected with an analogous function in formal group theory [10]. Although the connection is not terribly complicated, explaining the relation would take us too far afield.*

The proof of this theorem is a degree-by-degree argument that is similar to the proof of Theorem 3.3.

The relevance of a stable power series' logarithm is made clear by the following theorem.

**Theorem 3.14 (Logarithmic Commutativity Theorem [6]).** *Let  $f$  and  $g$  be stable series over a field  $R$ . Then  $f \circ g = g \circ f$  iff  $L_f = L_g$ .*

*Proof.* ( $\Rightarrow$ ): First we claim that the function  $\mathcal{L} = \frac{1}{g'(0)}(L_f \circ g)$  satisfies the functional equation for  $L_f$ . Then by the uniqueness clause of Theorem 3.12, we have that  $\mathcal{L} = L_f$ .

Assume that  $f$  and  $g$  commute. Then  $\mathcal{L}$  satisfies the functional equation for  $L_f$ , since

$$\begin{aligned} \mathcal{L}(f(x)) &= \frac{1}{g'(0)}(L_f \circ g)(f(x)) \\ &= \frac{1}{g'(0)}(L_f \circ f)(g(x)) \\ &= \frac{1}{g'(0)}(f'(0)L_f)(g(x)) \\ &= \frac{f'(0)}{g'(0)}(L_f \circ g)(x) = f'(0)\mathcal{L}(x). \end{aligned}$$

So  $\mathcal{L}$  fits the functional equation of  $L_f$ . Last, we need to verify that  $\mathcal{L}$  has the other defining property of logarithms, namely that  $\mathcal{L}'(0) = 1$ . This is true as

$$\begin{aligned} \mathcal{L}'(0) &= \frac{1}{g'(0)}(L_f \circ g)'(0) \\ &= \frac{1}{g'(0)}L'_f(g(0))g'(0) \\ &= L'_f(0) = 1, \end{aligned}$$

since  $g(0)$  has no constant term, and the  $x$  coefficient of  $L_f$  is 1 by definition.

Consequently,  $\mathcal{L}$  is equal to  $L_f$ , the logarithm of  $f$ . The amazing part is that since  $L_f = \frac{1}{g'(0)}(L_f \circ g)(x)$ , we have that  $L_f$  also satisfies the functional equation for  $L_g$ . By uniqueness, the two must therefore be equal:  $L_f = L_g$ .

( $\Leftarrow$ ): The converse follows, since if  $L_f = L_g$ , then by the defining equation for logarithms, we have that

$$\begin{aligned}
L_f(f(g(x))) &= f'(0)g'(0)L_f(x) \\
&= f'(0)g'(0)L_g(x) \\
&= L_f(g(f(x))),
\end{aligned}$$

so that  $f(g(x)) = g(f(x))$ , and  $f$  and  $g$  commute.  $\square$

Logarithms are not difficult to compute, as they can be constructed coefficient by coefficient. In general, however, a closed-form expression for an arbitrary coefficient of a logarithm can be difficult to derive. Below is an example where each coefficient can be easily determined.

**Example 3.15.** *The logarithm of  $f(x) = (1+x)^p - 1$  is given by*

$$L_f(x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots = \sum_{n=1}^{\infty} \frac{x^n}{n}. \quad (1)$$

We have seen that over a field, we have essentially determined when two power series commute. Unfortunately, life is not so easy when our background structure is simply a local ring, which is the case in the scenarios we wish to address. As previously mentioned, we'll be looking primarily at series—stable, then invertible, then non-invertible—over our local integer ring  $\mathcal{O}$ .

### 3.4 An Application: Limits of Monoids

A natural question to ask is how commutant monoids of “close” power series relate. How would the commutant monoid of a power series be changed if one of its coefficients were altered slightly? In this section, we provide a partial answer to these types of questions, showing that the commutant monoid of a limit of a sequence of functions is the limit of the commutant monoids of those functions. Of course, this concept needs to be made more precise before a proof is attempted.

First and foremost, we need to define convergence for a sequence of power series. To do this, we define a notion of convergence strongly analogous to convergence with respect to the  $p$ -adic absolute value. Heuristically, we will mirror the  $p$ -adic notion of convergence as follows: a sequence of power series  $\{f_n\}$  converges to  $f$  if for every  $k$ , the sequence of power series eventually agrees with  $f$  on the first  $k$  coefficients. We define this notion of convergence more precisely below:

**Definition 3.16.** *A sequence of power series  $\{f_n\} = \{c_{n,1}x + c_{n,2}x^2 + \dots\}$  in  $\mathcal{O}[[x]]$  converges to  $f = a_1x + a_2x^2 + \dots$  as  $n \rightarrow \infty$  if for any  $k \in \mathbb{Z}$ , there exists an  $N$  such that for all  $n \geq N$  and all  $j \leq k$ ,  $c_{n,j} = a_j$ . In this case, we write  $\{f_n\} \rightarrow f$ .*

**Theorem 3.17 (Commutant Monoid Limit Theorem).** *Let  $\{f_n\} \rightarrow f \in K[[x]]$ . Then*

$$\lim_{n \rightarrow \infty} \text{Comm}_K(f_n) = \text{Comm}_K(f).$$

*Proof.* We start by clarifying what we need to show through a series of equivalence claims. First, we note that what we are trying to show is that the limit of the set of sequences converging with each  $f_n$  is a set of power series commuting with  $f$ . Writing  $\text{Comm}_K(f) = \{[a]_f\}_{a \in K}$ , we can express this last sentence as

$$\lim_{n \rightarrow \infty} \{[a]_{f_n}\}_{a \in K} = \{[a]_f\}_{a \in K}.$$

Now, we claim that we need look only at *one* of the power series in this sequence, and not the entire set of them: i.e., showing that for some  $a \in K$ ,

$$\lim_{n \rightarrow \infty} [a]_{f_n} = [a]_f,$$

as showing this equality for all  $a$  clearly implies the set equality. By definition of  $[a]_f$ , this means we need to show that  $\lim_{n \rightarrow \infty} [a]_{f_n}$  is the unique function beginning with  $ax$  that commutes with  $f$  under composition. By Theorem 3.14, this means we need only show that their logarithms are equal:

$$L_{\lim_{n \rightarrow \infty} [a]_{f_n}} = L_f.$$

In order to simplify the notation used in the proof, we will look at a convenient subsequence of the  $f_n$ ; namely,  $\{f_{N_j}\}$ , where  $N_j$  is the place in the sequence after which every element of the series agrees with  $f$  on the first  $j$  coefficients (i.e.  $f_{N_j} \equiv f \pmod{x^{j+1}}$ ). Thus, we need to show the following:

$$L_{\lim_{j \rightarrow \infty} [a]_{f_{N_j}}} = L_f.$$

For ease of notation, we will denote  $L_{[a]_{f_{N_j}}}$  by  $L_j$ , thereby reducing our goal to simply showing that  $L_j(x) \rightarrow L_f(x)$  as  $j \rightarrow \infty$ .

We now show that  $L_j \rightarrow L_f$ . We do this by proving that  $L_j(x) \equiv L_f(x) \pmod{x^{j+1}}$ , so letting  $j \rightarrow \infty$  gives the desired result.

As a base case, we note that  $L_1(x) \equiv L_f(x) \equiv x \pmod{x^2}$ , since each of these sequences begins with a linear term with coefficient 1. Now, assume as an induction hypothesis, that  $L_j(x) \equiv L_f(x) \pmod{x^{j+1}}$ . We now show that  $L_{j+1}(x) \equiv L_f(x) \pmod{x^{j+2}}$ .

Write  $f(x) = ax + a_2x^2 + \dots$ . Then by definition of  $f_{N_j}$ , we can write

$$f_{N_j}(x) = ax + a_2x^2 + \dots + a_jx^j + b_{j+1}x^{j+1} + \dots$$

Let  $L_{f,j}$  be the reduction of  $L_f$  modulo  $x^{j+1}$ . We need a better grasp on how the two functions  $L_j$  and  $L_{j+1}$  relate. We have that  $L_{f,j+1} = L_{f,j} + cx^{j+1}$  for some  $c \in K$ . We wish to determine this  $c$ . We begin by noting that via the functional equation for the logarithm we know that  $L_{f,j}(f(x)) - aL_{f,j}(x) \equiv dx^{j+1}$  for some  $d \in K$ . Thus, we have that

$$L_{f,j+1}(f(x)) - aL_{f,j+1}(x) \equiv (b + d(f'(0)^{j+1} - f'(0))) x^{j+1} \pmod{x^{j+2}}.$$

Since  $f$  is stable,  $a^{j+1} - a$  is never zero, and so we can solve the above for  $c$ :

$$c = -\frac{d}{f'(0)^{j+1} - f'(0)} = \frac{aL_{f,j}(1) - L_{f,j}(f(1))}{a^{j+1} - a}.$$

As  $L_{f,j}$  is taken mod  $x^{j+1}$ , the above constant  $c$  is determined entirely by  $f(1) \pmod{x^{j+1}}$  and  $f'(0) = a$ . Consequently, the point of this construction is that the above  $c$  does not depend on any properties of  $f$  other than its first  $j$  coefficients. The coefficients  $\{a_k\}_{k=1}^j$  are shared, however, both by  $f$  and by the power series  $f_{N_j}$ . Thus, we have shown both that  $L_{j+1}(x) - L_j(x) \equiv cx^{j+1} \pmod{x^{j+2}}$  and that  $L_{f,k+1}(x) - L_{f,k}(x) \equiv cx^{j+1} \pmod{x^{j+2}}$ . And now we are finished, as

$$\begin{aligned} L_f(x) &\equiv L_{f,j+1}(x) && \pmod{x^{j+2}} \\ &\equiv L_{f,j}(x) + cx^{j+1} && \pmod{x^{j+2}} \\ &\equiv L_j(x) + cx^{j+1} && \pmod{x^{j+2}} \\ &\equiv L_{j+1} && \pmod{x^{j+2}}, \end{aligned}$$

where the next to last step comes from the induction hypothesis. This completes the induction process, and we have that  $L_j(x) \equiv L_f(x) \pmod{x^{j+1}}$ . Allowing  $j \rightarrow \infty$ , we have that the limit of these logarithms is the logarithm of  $f$ , implying that the limit of the series commutes with  $f$ .  $\square$

Though a new result, the above theorem merely scratches the surface of the possible results in this field. Questions concerning the behavior of the commutant monoid of a series arising from a slight perturbation of its coefficients are still largely unanswered.

We now turn to an analysis of the critical differences that arise between series based on their invertibility under composition.

### 3.5 Invertible and Non-invertible stable series over $\mathcal{O}$ .

To begin, we cite an oft-cited paragraph found originally in [6]:

The study splits naturally into two almost disjoint parts: if a series  $f$  has  $f'(0)$  in the maximal ideal  $\mathcal{M}$ , 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 non-invertible

series. These two studies become no longer disjoint in the case of an invertible series commuting with a non-invertible series.

The purpose of the above paragraph is to introduce why we are interested in invertible series commuting with non-invertible series. One result along these lines, widely used in the field, is a powerful theorem from analysis applied to a  $p$ -adic setting known as the Weierstrass Preparation Theorem, which essentially demonstrates the ability to ‘factor out’ the non-invertible part of any power series.

**Definition 3.18.** *If  $f$  is a power series over  $\mathcal{O}$  such that not all of its coefficients are non-invertible (i.e. at least one coefficient is invertible), then the lowest degree in which an invertible coefficient appears is called the Weierstrass degree of  $f$ , written  $\text{wideg}(f)$ . If all coefficients of  $f$  are in  $\mathcal{M}$ , then we say  $f$  has infinite Weierstrass degree.*

**Theorem 3.19 (Weierstrass Preparation Theorem).** *If  $f$  has finite Weierstrass degree,  $\text{wideg}(f) = \delta < \infty$ , then there is a unique invertible  $u \in \mathfrak{F}_0(\mathcal{O})$  and a unique monic polynomial  $p(x) \in \mathcal{O}[x]$  (called the Weierstrass polynomial of  $f$ ), such that  $f(x) = p(x)u(x)$  and  $\deg(p) = \delta$ .*

A proof of this can be found in [1]. From the proof of this theorem, we also learn that all roots of  $f$ ’s Weierstrass polynomial are found in the algebraic closure of  $\mathcal{M}$ , denoted  $\overline{\mathcal{M}}$ , a subset of  $\overline{\mathcal{O}}$ , defined to be the integral closure of  $\mathcal{O}$ . In addition, we see from the proof that a power series with finite  $\text{wideg}$  can have finitely many roots. These roots will be the focus of the next section.

The Weierstrass degree gives another way of looking at the divide between invertible and non-invertible series: invertible series have  $\text{wideg}(f) = 1$ , whereas non-invertible series have  $\text{wideg}(f) > 1$ . It is in fact this way of looking at it that allows us a close parallel between these series and formal groups; specifically, via their endomorphisms.

We now have the mathematical technology developed to address Lubin’s conjecture.

## 4 Lubin’s Conjecture

We begin with the statement of the conjecture [7]:

**Conjecture 4.1.** *Let  $u, f \in \mathcal{O}[[x]]$  respectively be invertible and non-invertible maps such that:*

1.  $f \circ u = u \circ f$ .
2.  $u(0) = f(0) = 0$ .
3.  $u'(0), f'(0) \notin \{0, \sqrt[k]{1}\}$ , for any  $k \in \mathbb{Z}$ .
4. *Every root of every iterate of  $f$  is simple.*

*Then there exists a formal group  $F(x, y) \in \mathcal{O}[[x, y]]$  such that  $u$  and  $f$  are endomorphisms of  $F$ .*

This conjecture, which attempts to classify when a formal group is lurking in the background behind two commuting functions, is by no means intuitive. It is carefully phrased to include the interesting cases and to disregard the trivial cases and those which go beyond the range of  $p$ -adic analysis. The section will be devoted to motivating each of the numerous hypotheses in the above conjecture. We will then present partial results and support for believing the conjecture's veracity.

## 4.1 The Hypotheses

Perhaps most important of the hypotheses is why we take  $f$  to be invertible,  $u$  to be non-invertible, and require that  $f \circ u = u \circ f$ . This is the crux of what we wish to study. It is rare for two power series to commute, and it is even more unusual that an invertible series commutes with a non-invertible series. This is so because the case of commuting pairs of invertible (resp. non-invertible) are governed by some simple rules that are well understood, as seen in the previous chapter. Lubin's conjecture, therefore, attempts to link (via several other minor assumptions) the phenomenon of  $f$  and  $u$  commuting to a formal group; that both  $f$  and  $u$  are actually endomorphisms of this formal group. We now analyze the necessity and reasonability of the remaining of the conjectures.

### 4.1.1 $u(0) = f(0) = 0$

A simple test case will reveal the necessity of this assumption. If we allow a constant term in the expansions of our power series  $u$  and  $f$ , then a situation like the following example will arise.

**Example 4.2.** *Let  $f(x) = 2 + x$  and  $g(x) = 1 + x + x^2 + x^3 + \dots$ . Then*

$$(g \circ f)(x) = 1 + (2 + x) + (2 + x)^2 + (2 + x)^3 + \dots,$$

*whose constant term will clearly be infinite.*

To avoid this situation, the above assumption is necessary.

### 4.1.2 $u'(0)$ and $f'(0)$ not a root of unity

An attempt to solve for coefficients of a commuting power series invariably leads to terms where the  $k$ -th coefficient has a factor of  $(a_n^k - 1)$  in the denominator[6]. Consequently, if we allow any of the coefficients  $a_n$  to be roots of unity, we allow the possibility of power series with undefined or infinite coefficients in our commutant monoids. As this is clearly undesirable, this restriction is necessary.

According to Li [4], in addition, the restriction is important from a dynamical sense as well. According to Li, it is important to know that periodic points of period  $p^n m$  are also periodic points of period  $p^n$ . Li shows that this result does not necessarily hold if we do not include the above restriction.

### 4.1.3 $u'(0)$ and $f'(0)$ non-zero

There are several reasons to include this restriction. Hensel's lemma, for example, also includes this hypothesis, suggesting that functions satisfying this hypothesis play a different role in  $p$ -adic number theory. Another reason is that we wish to ignore some of the undesirable properties exhibited by functions such as  $f(x) = x^n$  (for  $n > 1$ ) under composition. For example  $f(x) = x^n$  commutes with every  $x^m$ , clearly violating our isomorphism between a function's commutant monoid and the coefficients of that field. Consequently, this restriction is a necessary part of the definition of a stable series.

### 4.1.4 Every root of every iterate of $f$ is simple.

This assumption is included to rule out the only known example of an instance with two commuting power series (one invertible, one non-invertible) that are not endomorphisms of a formal group. Specifically, Li [3] defines the *condensation* of a commuting family, a power series that commutes with the elements of a commuting family, yet are not endomorphisms of a formal group.

Thus, the hypothesis that every root of  $f$  is simple is a necessary one. It is interesting to note, however, that the only known counterexamples without this hypothesis arise from these formal group condensations, suggesting perhaps an even deeper relation than Lubin's conjecture stipulates.

**Definition 4.3.** *From now on, we will refer to a pair of power series satisfying the hypotheses of Conjecture 5.1.1 as a stable commuting pair.*

Lubin's conjecture thus states that if  $u$  and  $f$  are a stable commuting pair, then there exists a formal group  $F$  such that  $u$  and  $f$  are endomorphisms of  $F$ .

## 4.2 Support for the Conjecture

Some preliminary results offer the conjecture credibility, if not a proof. In this section, we catalogue some of the known results from the theory of commuting functions relating the topics at hand, in an attempt to persuade the reader that the conjecture is plausible, perhaps even probable. We begin with Lubin's main theorem in [6], the seminal work in the field.

### 4.2.1 Lubin's Main Theorem

Recall that  $\mathcal{O}$  is a finite algebraic extension of  $\mathbb{Q}_p$ .

**Theorem 4.4.** *Let  $u, f$  be a stable commuting pair over  $\mathcal{O}$  and let  $f$  have finite wideg  $\delta$ . Then either some iterate of  $u$  is the identity, or  $\delta = p^d$  for some  $d > 0$ .*

Thus, with the same conditions as Lubin's conjecture, we have either the somewhat trivial case of  $u$  being a *torsion series* (in that some iterate of  $u$  is the identity function), or that the wideg of  $f$  is a power of  $p$ , as known to be the case for endomorphisms of formal groups. So we now have that non-trivial stable commuting pairs share a property with endomorphisms of formal groups, providing support for the conjecture.

### 4.2.2 Sarkis' Result

Sarkis answers in his PhD thesis that the conjecture is true if it is true for formal groups over the residue field  $k$ . The theorem involves the notion of the *height* of a formal group.

**Definition 4.5.** *Let  $F$  be a formal group over  $R$ . Then the height of  $F$ , denoted  $ht(F)$  is defined by*

$$ht(F) = \log_p(\text{widedeg}([p]_F)).$$

**Remark 4.6.** *This is the typical real-valued logarithm base  $p$ , not a new  $p$ -adic logarithm function. As widegs of endomorphisms of formal groups are powers of  $p$ , these heights will always be integers.*

**Theorem 4.7 (Sarkis' Theorem).** *Let  $u$  and  $f$  be a stable commuting pair over  $\mathcal{O}$ , and let  $v$  be the image of  $u$  in  $k = \mathcal{O}/\mathcal{M}$ . Then if  $v$  and  $w$  are an endomorphism of a formal group  $F$ , over  $k$ , and if  $ht(F) > 1$ , then  $f$  and  $u$  are endomorphisms of a formal group over  $\mathcal{O}$ .*

This is one of several results provided by Sarkis concerning the relation between results over  $k$  and results over  $\mathcal{O}$ . In general, Sarkis [8] is concerned with providing results over formal groups of positive characteristic.

### 4.2.3 Li's Result

Although much of Lubin's conjecture is unproven, a student of his, Hua-Chieh Li, has proven a substantial leap toward the final goal using Galois theory. Li's theorem gives the following partial result to Lubin's conjecture [5]:

**Definition 4.8.** *If  $f$  is a series over  $R[[x]]$ , denote  $f(f(x))$  by  $f^{\circ 2}(x)$  and in general, denote the  $n$ -fold iteration of  $f$  by  $f^{\circ n}(x)$ , for any  $n \in \mathbb{N}$ . This can be extrapolated to negative  $n$  for invertible series, where  $f^{\circ -n} = (f^{-1})^{\circ n}$ .*

**Theorem 4.9 (Li's Theorem).** *If  $u$  and  $f$  are a stable commuting pair over  $\mathcal{O}$  and  $\overline{\mathcal{O}}[[x]]$  is Galois over  $\overline{\mathcal{O}}[[f^{\circ n}(x)]]$  for all  $n \in \mathbb{N}$ , then there exists a formal group  $F$  such that  $u$  and  $f$  are endomorphisms of  $F$ .*

The proof makes extensive use of Newton polygons, logarithms of series and, in general, most of the results we have presented in this paper. The basic idea of the proof is to show that for any  $n \in \mathbb{Z}$ , the ring extension  $\mathcal{O}[[x]] \supset \overline{\mathcal{O}}[[f^{\circ n}(x)]]$  is Galois, with Galois group isomorphic to the set of roots of  $\{f^{\circ n}\}_{n \in \mathbb{Z}_p}$ . The interested reader can find the proof in [5].

The parallels between this theorem and Lubin's conjecture are quickly seen. Li has proven Lubin's conjecture with the added hypothesis that  $\overline{\mathcal{O}}[[x]]$  is Galois over  $\overline{\mathcal{O}}[[f^{\circ n}(x)]]$  for all  $n \in \mathbb{N}$ . It is important to note that the extra Galois hypothesis is not terrible restrictive. For example, Li shows that the Galois hypothesis implies Lubin's hypothesis that all roots of  $f$  be simple, so that we are not requiring too much different or extra with the Galois hypothesis.

## 5 Conclusion

Lubin's conjecture remains unproven, though tremendous progress has been made toward it since the founding of the field in the 1960s. The question of what other set of requirements will ensure a formal group behind two commuting power series has been answered, but this has not been refined to a minimal set, as Lubin's conjecture might.

Though attempts are made at a direct proof of Lubin's conjecture, most of the current work in the area concerns developing the theory to a greater extent. Li has written several papers concerning the theory of periodic points in  $p$ -adic dynamics ([2], for example), which have arisen in his attempts to prove the conjecture. On a different path, Sarkis [8] has attempted to relate formal groups over  $k$ , where we can take advantage of the field's positive characteristic, to formal groups over  $\mathcal{O}$ .

## References

- [1] F. P. Gouvêa.  *$p$ -adic Numbers: an Introduction*. Springer Universitext, second edition, 2000.
- [2] H.-C. Li.  $p$ -adic periodic points and sen's theorem. *Journal of Number Theory*, 56:309–318, 1994.
- [3] H.-C. Li. Isogenies between dynamics of formal groups. *J. Number Theory*, 62(2), 284–297 1996.
- [4] H.-C. Li.  $p$ -adic dynamics and formal groups. *Compositio Math.*, 1(104):41–54, 1996.
- [5] H.-C. Li. When is a  $p$ -adic power series an endomorphism of a formal group? *Proc. Amer. Math. Soc.*, 124(8):2325–2329, 1996.
- [6] J. Lubin. Nonarchimedean dynamical systems. *Compositio Mathematica*, 94:321–346, 1994.
- [7] J. Lubin. Dynamics of the  $p$ -adic open disc. Talk given at a Claremont Colleges Colloquium, 2001.
- [8] G. Y. Sarkis. *Formal Groups and  $p$ -adic Dynamical Systems*. PhD thesis, Brown University, 1997.
- [9] J. P. Silverman. *The Arithmetic of Elliptic Curves*. Number 106 in Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.
- [10] N. Strickland. Formal groups.