



Understanding Counterexamples to Lubin's Conjecture

Andrea Heald

Ghassan Sarkis, Advisor

Michael Orrison, Reader

May, 2007

HARVEY MUDD
COLLEGE

Department of Mathematics

Copyright © 2007 Andrea Heald.

The author grants Harvey Mudd College the nonexclusive right to make this work available for noncommercial, educational purposes, provided that this copyright statement appears on the reproduced materials and notice is given that the copying is by permission of the author. To disseminate otherwise or to republish requires written permission from the author.

Abstract

My thesis deals with finding counterexamples to Lubin's Conjecture. Lubin's Conjecture states that for power series f, g with coefficients in \mathbb{Z}_p , and f invertible and non-torsion, g non-invertible, then if $f \circ g = g \circ f$, f, g are endomorphisms of a formal group over \mathbb{Z}_p . This conjecture connects formal power series over the ring of p -adic integers (\mathbb{Z}_p) to formal groups. In this paper I will explain the properties of Formal Groups, their endomorphisms and logarithms, and will illustrate some properties of power series over the rings \mathbb{Q}_p and \mathbb{Z}_p .

Acknowledgments

I would like to thank my advisor, Professor Sarkis, for all his help on this thesis. I would also like to thank Doug Rizzolo for giving me some help when I was stumped. Finally I would like to thank Professor Orrison and the Harvey Mudd College Math Department for supporting me during my time here.

Contents

Abstract	iii
Acknowledgments	v
1 Introduction	1
2 Power Series Rings and Formal Groups	3
2.1 Power Series Rings	3
2.2 p -adic numbers	5
2.3 Formal Groups	8
3 Properties of Power Series	17
3.1 Power Series Logarithms	17
3.2 Newton Polygons	19
3.3 Lubin's Theorem and Conjecture	20
4 Progress made	23
Bibliography	25

Chapter 1

Introduction

My thesis explores Lubin's conjecture. Lubin's Conjecture states that given two power series f and g in $\mathbb{Z}_p[[x]]$ where f is invertible, and g is non-invertible and non-torsion, if $f \circ g = g \circ f$, then f and g are endomorphisms of a formal group. This conjecture has counterexamples, and I will illustrate some of these. I will also go through the definition and some properties of general power series rings. This leads nicely to the definition of a formal group and a formal group endomorphism. In order to connect general formal groups with formal power series, the concept of a logarithm is introduced. This also leads to the theorem that the endomorphisms of a formal group over \mathbb{Z}_p are commutative.

In general Lubin's conjecture connects formal power series over \mathbb{Z}_p to formal groups over \mathbb{Z}_p . This connection allows for the greater understanding of both, since it allows one to (occasionally) switch a problem in one to a problem in the other.

I made some progress in trying to understand what other conditions are needed for Lubin's conjecture, by examining the logarithm of a power series. I found the coefficients of $\hat{L}^{-1} \circ L$, in an effort to determine when this is in $\mathbb{Z}_p[[x]]$, since that would imply L being the logarithm of a formal group. This then allows one to generate endomorphisms of the formal group f and g .

Chapter 2

Power Series Rings and Formal Groups

2.1 Power Series Rings

The first key to understanding formal groups is understanding power series rings. Let R be a commutative ring.

Definition 1. A power series ring $R[[x_1, x_2, \dots, x_n]]$ is a ring whose elements are formal power series $f(x) = \sum a_i x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}$ where the $a_i \in R$, and the operations are component-wise addition and multiplication.

For example, $1, x, x^2y, 3 + x + 2y$ and $\sum_{i=0}^{\infty} ix^i y^{i+3}$ are all elements of $\mathbb{Z}[[x, y]]$. In other words the elements of $R[[x_1, x_2, \dots, x_n]]$ are just polynomials that can have infinite degree. It is obvious to see that every power series in $R[[x_1, x_2, \dots, x_n]]$ has an additive inverse, since if $f \in R[[x_1, x_2, \dots, x_n]]$ then so is $-f$, and $f + (-f) = 0$ (note $-f$ is defined by replacing every coefficient of f with its additive inverse). (Frolich)

Note also that if $f(x)$ has a multiplicative inverse, $f^{-1}(x)$, then the constant term for f must be a unit in R (if $f = a +$ a summation with no constant term, then $f^{-1} = b +$ a summation with no constant term, since $f * f^{-1} = a * b +$ a product $= 1$, thus $a * b = 1$, and $b = a^{-1}$ and a is a unit in R .) Note also that if the constant term of $f(x)$ is a unit in R we may construct an inverse.

For example if we have $f(x) = 1 + x \in \mathbb{Z}[[x]]$, $g(x) = \sum_{i=0}^{\infty} (-1)^i x^i \in$

4 Power Series Rings and Formal Groups

$\mathbb{Z}[[x]]$, then $f(x) * g(x) = 1$. We can see this by multiplying out

$$\begin{aligned} f(x) * g(x) &= (1+x) \sum_{i=0}^{\infty} (-1)^i x^i \\ &= \sum_{i=0}^{\infty} (-1)^i x^i + \sum_{i=1}^{\infty} (-1)^{i-1} x^i \\ &= 1. \end{aligned}$$

We now prove that in general $f(x) \in R[[x]]$ will have an inverse if the constant term of f is a unit. Let $f(x) = a_0 + \sum_{i=1}^{\infty} a_i x^i$, where $a_0 * a'_0 = 1 \in R$. We know g is of the form $g(x) = a'_0 + \sum_{i=1}^{\infty} a'_i x^i$. To find the a'_i 's we proceed by induction on the degree of x . Assume such a'_i 's exist for $i < n$ such that $f(x) * g(x) \equiv_{x^n} 1$. We have

$$f(x)g(x) \equiv_{x^{n+1}} \left(a_0 + \sum_{i=1}^{n-1} a_i x^i + a_n x^n \right) \left(a'_0 + \sum_{i=1}^{n-1} a'_i x^i + a'_n x^n \right).$$

Reducing and rearranging we get that

$$f(x)g(x) \equiv_{x^{n+1}} \left(a_0 + \sum_{i=1}^{n-1} a_i x^i \right) \left(a'_0 + \sum_{i=1}^{n-1} a'_i x^i \right) + a_0 a'_n x^n + a'_0 a_n x^n,$$

but by the induction hypothesis this implies that $f(x)g(x) \equiv_{x^{n+1}} 1 + cx^n + a_0 a'_n x^n + a'_0 a_n x^n$ for some constant c so if $a'_n = -a'_0(c + a'_0 a_n)$ we have $f(x)g(x) \equiv_{x^{n+1}} 1$, and $f(x)g(x) = 1$. Thus $f(x)$ has a multiplicative inverse.

Another possible operation on $R[[x]]$ is composition. For $f, g \in R[[x]]$ if f, g have no constant term, $(f \circ g)(x)$ and $(g \circ f)(x)$ are well defined, and we may consider composition to be another type of operation on the elements of $R[[x]]$. Note that if f or g has a constant term things may not work. For example, if $f(x) = \sum_{i=1}^{\infty} x^i$ and $g(x) = 1 + x$, $f(g(x)) = \sum_{i=1}^{\infty} (1+x)^i = \sum_{i=1}^{\infty} 1 + x * (\text{a sum})$, but this has an undefined constant term, thus $f \circ g$ is not an element of $R[[x]]$. Similarly to multiplicative inverses, I claim that if the coefficient for the x term is a unit, then $f(x)$ has a compositional inverse in $R[[x]]$. For example, let $S(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots = \sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!}$,

and let $AS(x) = \sum_{i=0}^{\infty} \frac{(2i)!}{4^i(i!)^2(2i+1)} x^{2i+1}$. I claim $AS(S(x)) = x$.

$$\begin{aligned} AS(S(x)) &= \sum_{i=0}^{\infty} \frac{(2i)!}{4^i(i!)^2(2i+1)} S(x)^{2i+1} \\ &= \sum_{i=0}^{\infty} \frac{(2i)!}{4^i(i!)^2(2i+1)} \left(\sum_{k=0}^{\infty} \frac{(-1)^k x^{2k+1}}{(2k+1)!} \right)^{2i+1} \\ &= x. \end{aligned}$$

(Note that these are the Taylor series for $\sin(x)$ and $\arcsin(x)$, thus we know that $AS(S(x)) = x$. In general Taylor series are power series.)

Let $f(x) = a_1x + \sum_{i=2}^{\infty} a_i x^i$, $g(x) = a'_1 + \sum_{i=2}^{\infty} a'_i x^i$, such that $a_1 * a'_1 = 1$. Proceeding inductively, we have $f(g(x)) \equiv_{x^2} a_1 * a'_1 x = x$. Now assume that for $i < n$, the a'_i 's satisfy $f(g(x)) \equiv_{x^n} x$. Expanding mod x^{n+1} we see

$$\begin{aligned} f(g(x)) &\equiv_{x^{n+1}} \sum_{i=1}^n a_i \left(\sum_{j=1}^{n-1} a'_j x^j + a'_n x^n \right)^i \\ &\equiv_{x^{n+1}} \sum_{i=1}^n a_i \left(\sum_{j=1}^{n-1} a'_j x^j \right)^i + a_1 * a'_n x^n \end{aligned}$$

which by the induction hypothesis reduces to $f(g(x)) \equiv_{x^{n+1}} x + cx^n + a_1 * a'_n x^n$, for some constant c , which implies that for $a'_n = -a'_1 * c$ we have $f(g(x)) \equiv_{x^{n+1}} x$ and there exist a'_i 's such that $f(g(x)) = x$.

2.2 *p*-adic numbers

The ring R for the rest of the thesis will be either \mathbb{Z}_p or \mathbb{Q}_p , the *p*-adic integers or rationals. A *p*-adic integer $x \in \mathbb{Z}_p$, is a number of the form $x = \sum a_i p^i$ where $a_i \in \mathbb{Z}$ and $0 \leq a_i < p$ for some fixed prime p .

Examples in the 3-adics:

- $5 = 2 + 1 * 3$
- $-1 = 2 + 2 * 3 + 2 * 3^2 + 2 * 3^3 + \dots$
This looks odd, but in the *p*-adics $|p^n|_p \rightarrow 0$ as $n \rightarrow \infty$ so this sum converges, and the formula $\sum n * x^i = \frac{n}{1-x}$ gives us that the sum is $\frac{2}{1-3} = -1$.
- $\frac{1}{2} = 2 + 3 + 3^2 + 3^3 + \dots$
It works similarly to the previous summation since $\frac{3}{1-3} - 1 = \frac{1}{2}$.

6 Power Series Rings and Formal Groups

Note that the p -adic valuation $|\cdot|_p$ is defined very differently than the normal absolute value. We know that any number $x \in \mathbb{Z}_p$ may be written as ap^n where p does not divide a , $a \in \mathbb{Z}$ and $n \in \mathbb{Z}^+$. Then $|x|_p = p^{-n}$ (conversely this may also be defined as c^n for a fixed $0 < c < 1$). As stated earlier this does have the property that as $n \rightarrow \infty$, $|p^n| \rightarrow 0$.

\mathbb{Z}_p is a ring, and thus has two operations, addition and multiplication. They are both defined in a natural way. Addition is defined in a pointwise manner, with terms being carried. Examples in the 3-adics:

- $5 + 7 = (2 + 1 * 3) + (1 + 2 * 3) = (1 + 2) + (1 + 2)3 = 3 + (1 + 2)3 = (1 + 1 + 2)3 = (1 + 3)3 = 3 + 3^2$ or 12
- $2 + (-1) = 2 + 2 + 2 * 3 + 2 * 3^2 + \dots = 1 + (1 + 2)3 + 2 * 3^2 + \dots = 1 + (1 + 2)3^2 + 2 * 3^3 + \dots = 1 + (1 + 2) * 3^3 + \dots = 1$ (note that the terms collapse towards p^∞ and thus converge to 0.)
- $\frac{1}{2} + (-1) = 2 + 2 + (1 + 2)3 + (1 + 2)3^2 + \dots = 1 + (1 + 1 + 2)3 + (1 + 2)3^2 + \dots = 1 + 3 + 3^2 + 3^3 + \dots = -\frac{1}{2}$

Multiplication is also defined in the expected way. Examples in the 3-adics:

- $5 * 7 = (2 + 1 * 3)(1 + 2 * 3) = 2 + (4 + 1)3 + 2 * 3^2 = 2 + 2 * 3 + (1 + 2)3^2 = 2 + 2 * 3 + 3^3 = 35$
- $5(-1) = (2 + 3)(2 + 2 * 3 + 2 * 3^2 + \dots) = 2 + 2 + (2 + 4)3 + (2 + 4)3^2 + \dots = 1 + 3 + 2 * 3^2 + 2 * 3^3 + \dots = -5$
- $(-\frac{1}{2})(-1) = (2 + 2 * 3 + 2 * 3^2 + \dots)(1 + 3 + 3^2 + \dots) = 2 + (2 + 2)3 + (2 + 2 + 2)3^2 + (2 * 4)3^3 + \dots = 2 + 3 + 3^2 + 3^3 + 3^4 + \dots = \frac{1}{2}$

In other words, things work in the same manner as the rationals. We can see that in \mathbb{Z}_p any number not divisible by p is a unit, and thus we can get many rational numbers. We can also formulate numbers not in the rationals. I claim that there exists an analog of $\sqrt{2}$ in the 7-adics, i.e. a number $x \in \mathbb{Z}_7$ such that $x^2 = 2$. Let $\sum a_i 7^i = x$, we formulate x term by term (in other words we construct each term by moding out by higher terms). $x^2 \equiv_7 a_0^2 \equiv 2$, which means $a_0 = 3$, then

$$\begin{aligned} x^2 &\equiv_{7^2} (3 + a_1 7)^2 \\ &\equiv_{7^2} 9 + 6a_1 7 \\ &\equiv_{7^2} 2, \end{aligned}$$

or $(6a_1 + 1)7 \equiv_{7^2} 0$ and thus $a_1 = 1$. Continuing

$$\begin{aligned} (3 + 7 + a_2 7)^2 &\equiv_{7^3} 9 + 6 * 7 + (6a_2 + 1)7^2 \\ &= 2 + (6a_2 + 2)7^2, \end{aligned}$$

thus $a_2 = 2$,

$$\begin{aligned} (3 + 7 + 2 * 7^2 + a_3 * 7^3)^2 &\equiv_{7^4} 9 + 6 * 7 + 13 * 7^2 + (6a_3 + 4)7^3 \\ &= 2 + (6a_3 + 6)7^3, \end{aligned}$$

thus $a_3 = 6$. We can see that we can go on in this manner, defining a 7-adic number that squares to 2, since each term is defined only by a linear equation.

Theorem 1. (*Hensel's Lemma*) Let $f(x) = \sum c_i x^i$ be a polynomial with coefficients in \mathbb{Z}_p . Let $0 \leq a_0 < p$ such that $f(a_0) \equiv_p 0$, and $f'(a_0) \not\equiv_p 0$, then there exists $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a \equiv_p a_0$

Proof: We know that for any *p*-adic number a , $a = a_0 + a_1 p + a_2 p^2 + \dots$, (note that the qualification that $a \equiv_p a_0$ means that the first coefficient is in fact a_0 .) I claim we can construct the rest of the coefficients inductively so that for any i , $f(a_0 + a_1 p + \dots + a_i p^i) \equiv_{p^{i+1}} 0$. We have the base case by the assumptions of Hensel's Lemma. Now assume its true for all a_i with $i < n$. Note that

$$\begin{aligned} &f(a_0 + a_1 p + \dots + a_{n-1} p^{n-1} + a_n p^n) \\ &\equiv_{p^{n+1}} f(a_0 + a_1 p + \dots + a_{n-1} p^{n-1}) + f'(a_0 + \dots + a_{n-1} p^{n-1}) a_n p^n \end{aligned}$$

(this is done by expanding the polynomial and reducing.) By the inductive hypothesis $f(a_0 + \dots + a_{n-1} p^{n-1}) \equiv_{p^{n+1}} \alpha p^n$, so we want to find $0 \leq a_n < p$ such that $\alpha p^n \equiv_{p^{n+1}} -f'(a_0 + \dots + a_{n-1} p^{n-1}) a_n p^n$, which reduces to $\alpha \equiv_p -f'(a_0) a_n$. However we know $f'(a_0) \not\equiv_p 0$ and thus has an inverse mod p , so we have $a_n \equiv_p \frac{-\alpha}{f'(a_0)}$, which is well defined. (Frolich 16) Thus we know that if there is a solution to a polynomial mod p , there is a solution in \mathbb{Z}_p .

Similarly to \mathbb{Z}_p , \mathbb{Q}_p is defined by infinite sums. $x \in \mathbb{Q}_p$ is defined by $x = \sum_n^\infty a_i p^i$ with $n \in \mathbb{Z}$ (possibly negative), $a_i \in \mathbb{Q}$ and $0 \leq a_i < p$. Addition and multiplication are defined in the same way, with p powers propagating through. Since this means that any p power now is a unit, we have that every element of \mathbb{Q}_p is a unit (as compared to \mathbb{Z}_p where p powers are not units.) By the definitions we see that $\mathbb{Z}_p \subseteq \mathbb{Q}_p$. We also know that $\mathbb{Q} \subseteq \mathbb{Q}_p$ and by the example of an 7-adic equivalent of $\sqrt{2}$, and Hensel's

Lemma we know that the inclusion is strict. Since \mathbb{Q}_p contains solutions for polynomials that \mathbb{Q} does not, \mathbb{Q}_p is an extension of \mathbb{Q} .

The p -adic metric at first seems a little awkward, however it turns out to be a natural metric on \mathbb{Q} .

Theorem 2. (Ostrowski's Theorem) Any non-trivial norm $\|\cdot\|$ on \mathbb{Q} is equivalent to either $|\cdot|_p$ for some prime p or the euclidean norm.

Proof: Let $\|\cdot\|$ be a norm on \mathbb{Q} . If there exists $n \in \mathbb{Z}$ such that $\|n\| > 1$, then we can prove that $\|\cdot\|$ is equivalent to the euclidean norm $|\cdot|$. Conversely, assume that for all n , $\|n\| \leq 1$. Let p be the smallest positive integer such that $\|p\| < 1$. We know that this number exists since $\|\cdot\|$ is non-trivial. I claim p is prime. Assume not, that there exists $a, b > 1 \in \mathbb{Z}$ such that $ab = p$. This means that $\|a\|\|b\| = \|p\| \leq 1$, but $a, b < p$, thus contradicting the minimality of p . Consider a prime $q \neq p$, and assume $\|q\| < 1$. Then there exists $N, M \in \mathbb{Z}$, such that $\|p\|^N < \frac{1}{2}$ and $\|q\|^M < \frac{1}{2}$. $\gcd(p^N, q^M) = 1$, so there exists $a, b \in \mathbb{Z}$ such that $ap^N + bq^M = 1$ which implies that $\|a\|\|p\|^N + \|b\|\|q\|^M \leq 1$ (by the triangle inequality), however $\|a\|, \|b\| \leq 1$, so

$$\begin{aligned} \|a\|\|p\|^N + \|b\|\|q\|^M &\leq \|p\|^N + \|q\|^M \\ &< \frac{1}{2} + \frac{1}{2} \\ &= 1, \end{aligned}$$

a contradiction. Thus $\|q\| = 1$. This implies that for any $a \in \mathbb{Z}$, with $a = a'p^n$ where $\gcd(a', p) = 1$,

$$\begin{aligned} \|a\| &= \|a'\|\|p^n\| \\ &= \|p^n\| \\ &= \|p\|^n. \end{aligned}$$

This is equivalent to the p -adic metric $|\cdot|_p$.

2.3 Formal Groups

From the background on power series rings we can define a formal group law.

Definition 2. A formal group law is a power series in two variables, $F(x, y)$ such that $F(x, 0) = x$, $F(0, y) = y$ and $F(x, F(y, z)) = F(F(x, y), z)$.

Note that by the first requirement a formal group must be of the form $F(x, y) = x + y + xy(f(x, y))$ for some power series $f(x, y)$. Thus, the simplest formal group is the additive formal group $A(x, y) = x + y$. Another example of a formal group is $F(x, y) = x + y + cxy$ for some constant c . In the case where $c = 1$ this is called the multiplicative formal group. We know that this has the first two requirements of a formal group, but the third requirement is harder to see. Note for the multiplicative formal group

$$\begin{aligned} F(x, F(y, z)) &= x + y + z + cyz + c(x(y + z + cyz)) \\ &= x + y + cxy + z + c((x + y + cxy)z) \\ &= F(F(x, y), z), \end{aligned}$$

as desired. For $c = 1$, this is called the multiplication formal group, since $F(x, y) = x + y + xy = (x + 1)(y + 1) - 1$, which looks somewhat like the multiplication of x and y , with some alterations so it fits the form of a formal group.

Also from the definition, for any formal group F we can construct a power series $i(x)$, such that $F(x, i(x)) = 0$. I claim that for the additive formal group $i(x) = -x$, since if $F(x, y) = x + y$, then $F(x, -x) = x - x = 0$ as desired. For the multiplicative formal group I claim $i(x) = \sum_{i=1}^{\infty} (-1)^i x^i$, i.e. if $F(x, y) = x + y + xy$ then

$$F(x, i(x)) = x + \sum (-1)^i x^i + x \sum (-1)^i x^i = 0.$$

We can easily see this cancels for the first few terms ($F(x, i(x)) = x - x + x^2 - x^2 \dots$), thus in full we may prove it by induction. Note first that $F(x, i(x)) \equiv_{x^2} x - x = 0$. Assume $F(x, i(x)) \equiv_{x^n} 0$, then

$$F(x, i(x)) \equiv_{x^{n+1}} (-1)^n x^n + (-1)^{n-1} x^n = 0,$$

thus $F(x, i(x)) = 0$.

In general we may prove that for any formal group there exists a power series $i(x)$ such that $F(x, i(x)) = 0$. Since every formal group starts off as $x + y + \dots$, we know that $i(x) = -x + \sum_{j=2}^{\infty} a'_j x^j$. Inductively, assume that for $j < n$, there are a'_j 's that satisfy $F(x, i(x)) \equiv_{x^n} 0$, and let $i_n(x) = \sum_{i=1}^n a'_i x^i$. Consider now

$$F(x, i_n(x) + a'_n x^n) \equiv_{x^{n+1}} x + i_n(x) + a'_n x^n + x(g(x)),$$

for some power series $g(x)$, but note that since we're dealing mod x^{n+1} there will be no a'_n 's in $g(x)$, thus

$$x + i_n(x) + xg(x) \equiv_{x^n} F(x, i_n(x)) \equiv_{x^n} 0$$

(by the induction hypothesis). Thus we have

$$F(x, i_n(x) + a'_n x^n) \equiv_{x^{n+1}} c * x^n + a'_n x^n$$

and for $a'_n = -c$ we have

$$F(x, i_n(x) + a'_n x^n) = F(x, i_{n+1}(x)) \equiv_{x^{n+1}} 0$$

and there exists $i(x)$ such that $F(x, i(x)) = 0$.

Although a formal group is not a group because it does not have elements, $F(x, y)$ acts like a group operation $x +_F y$ (it has associativity, identity and inverses). Thinking this way, we can develop the idea of a homomorphism f of formal groups. In groups, homomorphism map one group to another, similarly for formal groups we want to map $x +_F y$ to $x +_G y$ in some sense.

Definition 3. *Given F, G are formal groups, a power series $f(x)$ is a homomorphism if $f(F(x, y)) = G(f(x), f(y))$*

In other words, $f(x +_F y) = f(x) +_G f(y)$, which looks like a normal group homomorphism. Similarly an endomorphism is a power series $f(x)$ such that $f(F(x, y)) = F(f(x), f(y))$. Thus in some sense an endomorphism is a mapping from a formal group to itself, as desired.

If one examines the set of endomorphisms of a formal group F with coefficients in R , $\text{End}_R(F)$, we can see that it forms a ring with operations $F(f(x), g(x)) = f +_F g$ and composition. Note

$$\begin{aligned} f(g +_F h) &= f(F(g(x), h(x))) \\ &= F(f(g(x)), f(h(x))) \\ &= f(g) +_F f(h), \end{aligned}$$

so the operations are distributive. From the definition of formal group we have an additive inverse for the function x , i.e. there exists an $i(x)$ such that $x +_F i(x) = 0$. We now apply f to both sides. $f(0) = 0$ by construction, thus we have

$$\begin{aligned} f(F(x, i(x))) &= F(f(x), f(i(x))) \\ &= f +_F f \circ i = 0 \end{aligned}$$

and f has an inverse under F addition. $\text{Hom}_R(F, G)$, the set of homomorphisms from F to G , is also a ring with operations composition and G addition. We can also see that if $f \in \text{Hom}_R(F, G)$ has a compositional inverse

f^{-1} , then $f^{-1} \in \text{Hom}_R(G, F)$. By simple manipulations we have that

$$\begin{aligned} f^{-1}(G(x, y)) &= f^{-1}(G(f(f^{-1}(x)), f(f^{-1}(y)))) \\ &= f^{-1}(f(F(f^{-1}(x), f^{-1}(y)))) \\ &= F(f^{-1}(x), f^{-1}(y)) \end{aligned}$$

as desired. $\text{End}_R(F)$, the set of endomorphism of F , is also a ring with the same operations with the same properties. Note that in this case, $f \in \text{End}_R(F)$ implies $f^{-1} \in \text{End}_R(F)$, and the ring is closed under compositional inverses.

For example $f(x) = 2x + x^2$ is an endomorphism of $F(x, y) = x + y + xy$ since

$$\begin{aligned} f(F(x, y)) &= 2(x + y + xy) + (x + y + xy)^2 \\ &= 2x + 2y + 2xy + x^2 + y^2 + 2xy + 2x^2y + 2xy^2 + x^2y^2 \\ &= 2x + x^2 + 2y + y^2 + (2x + x^2)(2y + y^2) \\ &= f(x) + f(y) + f(x)f(y) \\ &= F(f(x), f(y)). \end{aligned}$$

We also have $g(x) = 3x + 3x^2 + x^3$ is an endomorphism of $F(x, y)$. Thus since composition is an operation on $\text{End}_R(F)$, $f(g(x))$ should be another endomorphism. $f(g(x)) = 6x + 15x^2 + 20x^3 + 15x^4 + 6x^5 + x^6$, and if we plug it in, we discover that $F(f(g(x)), f(g(y))) = f(g(F(x, y)))$. Note also that $g(f(x)) = f(g(x))$, and I will prove later that this is true for all endomorphisms of a formal group (with coefficients in the p -adics), which is important to Lubin's Conjecture. To add f and g , we use F addition, i.e. $f +_F g = F(f(x), g(x)) = 5x + 4x^2 + x^3 + (2x + x^2)(3x + 3x^2 + x^3) = 5x + 10x^2 + 10x^3 + 5x^4 + x^5$. Note that this is the unique homomorphism which begins with $5x$, and in general a homomorphism of $F(x, y)$ may be uniquely defined by its first term.

An example of a homomorphism is $f(x) = x + \frac{x^2}{2}$ which maps $F(x, y) = x + y + xy$ to $G(x, y) = x + y + 2xy$, since

$$\begin{aligned} f(F(x, y)) &= x + y + xy + \frac{x^2}{2} + \frac{y^2}{2} + xy + x^2y + xy^2 + \frac{x^2y^2}{2} \\ &= x + \frac{x^2}{2} + y + \frac{y^2}{2} + 2(x + \frac{x^2}{2})(y + \frac{y^2}{2}) \\ &= f(x) + f(y) + 2f(x)f(y) \\ &= G(f(x), f(y)). \end{aligned}$$

We now define a special type of homomorphism, the logarithm. The natural logarithm has the property $\log(xy) = \log(x) + \log(y)$, and the formal group logarithm is defined to have this same property.

Definition 4. A logarithm $L(x)$ is a homomorphism from a formal group $F(x, y)$ to the additive formal group $A(x, y)$, i.e. $L(F(x, y)) = L(x) + L(y)$.

In other words, $L(x +_F y) = L(x) + L(y)$.

Example 1. Let $L(x) = \sum (-1)^{i-1} \frac{x^i}{i}$. I claim $L(x)$ is a logarithm of the multiplicative formal group.

To prove this we proceed inductively on the degree. It is obvious that

$$\begin{aligned} L(F(x, y)) &\equiv_{x^i y^j, i+j=2} x + y \\ &\equiv_{x^i y^j, i+j=2} L(x) + L(y) \end{aligned}$$

(since the first term of $L(x)$ is x). We now assume that for degree less than n ,

$$L(F(x, y)) \equiv_{x^i y^j, i+j=n} L(x) + L(y).$$

Substituting we get

$$L(x + y + xy) \equiv_{x^i y^j, i+j=n+1} \sum_{i=1}^{n-1} (-1)^{i-1} \frac{(x + y + xy)^i}{i} + (-1)^{n-1} \frac{(x + y + xy)^n}{n}.$$

Note that the first term is of the form

$$L(x) + L(y) + \sum i + j = n + 1 a_{ij} x^i y^j$$

for some a_{ij} . Also since the a_{ij} 's come from expansions powers of polynomials we can see that

$$a_{ij} = (-1)^{n-2} * \binom{n}{i} \binom{n-i}{k} / n.$$

When we examine this we note that these are the negative cross terms of appropriate degree in the $(x + y + xy)^n$ sum. Thus we get

$$\begin{aligned} L(F(x, y)) &\equiv_{x^i y^j, i+j=n+1} L(x) + L(y) + \sum_{i+j=n+1} a_{ij} x^i y^j - \sum_{i+j=n+1} a_{ij} x^i y^j \\ &= L(x) + L(y) \end{aligned}$$

showing that $L(F(x, y)) = L(x) + L(y)$.

From this we can see that even though the coefficients of $F(x, y)$ are in \mathbb{Z}_p , the coefficients of $L(x)$ are instead in \mathbb{Q}_p .

In general we know a logarithm is of the form $L(x) = \sum b_i x^i$ for $b_i \in \mathbb{Q}_p$, and since all formal groups begin $F(x, y) = x + y + \dots$, we have $L(F(x, y)) = b_1(x + y) + \dots = b_1 x + b_1 y$ which implies that the constant connected to the x term doesn't matter, and thus we may assume it is $b_1 = 1$ i.e. $L(x) = x + \dots$

The derivative of the logarithm is nice, even though $L(x) \in \mathbb{Q}_p[[x]]$ rather than $\mathbb{Z}_p[[x]]$.

Theorem 3. *If $L(x)$ is the logarithm of a formal group, then $\frac{d}{dx}L(x) \in \mathbb{Z}_p$.*

The previous example of the logarithm of the multiplicative obviously has this property.

Proof: By definition $L(F(x, y)) = L(x) + L(y)$, so by taking the partial with respect to x of each side we obtain $F'(x, y)L'(F(x, y)) = L'(x)$. Substituting $x = 0$, we have $F'(0, y)L'(y) = L'(0)$. From the definition of a formal group we have $F'(0, y) = 1 + \sum_{i=1}^{\infty} a_i y^i$, for $a_i \in \mathbb{Z}_p$, we also know that $L'(0) = 1$, thus $L'(y) = \frac{1}{1 + \sum_{i=1}^{\infty} a_i y^i}$.

We now proceed by induction. L is a power series so $L'(y) = \sum b_i y^i$ for some b_i , and $F'(0, y)L'(y) = L'(0)$ implies that $(1 + a_1 y)(1 + b_1 y) \equiv_{y^2} 1$, and therefore $a_1 = -b_1$, and $b_1 \in \mathbb{Z}_p$. Now assume $b_1, \dots, b_{n-1} \in \mathbb{Z}_p$, such that

$$\left(1 + \sum_{i=1}^n a_i y^i\right) \left(1 + \sum_{i=1}^{n-1} b_i y^i + b_n y^n\right) \equiv_{y^{n+1}} 1.$$

Solving for b_n we obtain that

$$b_n y^n \equiv_{y^{n+1}} \left(1 + \sum_{i=1}^n a_i y^i\right) \left(1 + \sum_{i=1}^{n-1} b_i y^i\right).$$

However, the coefficients on the right side are all in \mathbb{Z}_p by the induction hypothesis, and therefore $b_n \in \mathbb{Z}_p$ and all the coefficients of $L'(x)$ are in \mathbb{Z}_p .

The logarithm also has a nice connection to the endomorphisms of a formal group.

Theorem 4. *Given an endomorphism $f(x)$ of $F(x, y)$ and a logarithm $L(x)$ of F , then $L(f(x)) = f'(0)L(x)$.*

Proof: We know $L(x)$ is a homomorphism from $F(x, y)$ to $A(x, y)$ ($= x + y$). We also know that since $L(x) \equiv_{x^2} x$ there exists a compositional inverse $L^{-1}(x)$, which we showed earlier is a homomorphism from $A(x, y)$ to $F(x, y)$. I claim that $L \circ f \circ L^{-1}$ is an endomorphism of $A(x, y)$. Just following definitions, we get

$$\begin{aligned} L(f(L^{-1}(A(x, y)))) &= L(f(F(L^{-1}(x), L^{-1}(y)))) \\ &= L(F(f(L^{-1}(x)), f(L^{-1}(y)))) \\ &= A(L(f(L^{-1}(x))), L(f(L^{-1}(y)))) \end{aligned}$$

as desired. Now I claim that any endomorphism g of $A(x, y)$ is of the form $g(x) = ax$ for some $a \in \mathbb{Q}_p$. We take a generic endomorphism $g(x) = \sum a_i x^i$. g being a homomorphism of $A(x, y)$ implies that $g(x + y) = g(x) + g(y)$ and

$$\sum a_i (x + y)^i = \sum a_i x^i + \sum a_i y^i.$$

However, we know that since we are in a ring of characteristic 0, for $i > 1$ $(x + y)^i$ will have terms with xy , which we cannot have. Thus $a_i = 0$ for $i > 1$ and $g(x) = a_1 x$, we can also see that $g'(0) = a_1$. Thus we have that $L(f(L^{-1}(x))) = ax$.

$$\frac{d}{dx} L(f(L^{-1}(x))) = \left(\frac{d}{dx} L^{-1}(x) \right) f'(L^{-1}(x)) L'(f(L^{-1}(x)))$$

which at 0 is $f'(0)L'(0) = f'(0)$. Thus $L(f(L^{-1}(x))) = f'(0)x$ and when we substitute $L(x)$ for x we get $L(f(x)) = f'(0)L(x)$.

Note that given a logarithm we can generate the formal group by $F(x, y) = L^{-1}(L(x) + L(y))$ where L^{-1} denotes the compositional inverse (by the properties of power series, since $L(x)$ has a unit x coefficient, $L^{-1}(x)$ exists). There is a useful theorem that involves formulations of that type. First we must define a special recurrence relation of a power series. Let $S \subset R$ be rings, and I be an ideal of S , ϕ a ring homomorphism, p a prime, $q = p^k$, $r_i \in R$. Given a power series $g(x) = \sum_{i=1}^{\infty} a_i x^i$, $a_i \in A$, we construct $f_g(x)$ by

$$f_g(x) = g(x) + \sum_{i=1}^{\infty} r_i \phi_*^i f_g(x^{q^i}),$$

where $\phi_*^i f_g(x)$ is obtained by applying ϕ^i to each coefficient of $f_g(x)$. Note that logarithms are of the form of this recurrence.

Theorem 5. (*The Functional Equation Lemma*) Let $g(x) = \sum_{i=1}^{\infty} a_i x^i$, $\bar{g}(x) = \sum_{i=1}^{\infty} \bar{a}_i x^i$, $a_i, \bar{a}_i \in S$, and b_1 be invertible in S then,

- i) The coefficients of $F(x, y) = f_g^{-1}(f_g(x) + f_g(y))$ are in S
- ii) The coefficients of $f_g^{-1}(f_{\bar{g}}(x))$ are in S
- iii) If the coefficients of $h(x) = \sum_{i=1}^{\infty} b_i x^i$ are in S then there exists a power series $\hat{h}(x) = \sum_{i=1}^{\infty} \hat{b}_i x^i$ with $\hat{b}_i \in S$ such that $f_g(h(x)) = f_{\hat{h}}(x)$.

For a relevant example take $R = \mathbb{Q}_p$, $S = \mathbb{Z}_p$, $r_1 = \frac{1}{p}$ and $r_i = 0$ for $i > 1$. Let $g(x) = x$ and $\bar{g}(x) = \sum_{(n,p)=1} n^{-1} (-1)^{n+1} x^n$, let $H(x) = f_g(X)$, and $l(x) = f_{\bar{g}}(x)$. If $\exp(x) = \sum_{n=0}^{\infty} (n!)^{-1} x^n$, then we can see that $\exp(H(x))$ has coefficients in the p -adic integers (Hazewinkel 9). Another example in the p -adic's is

$$f_g(x) = L(x) = \sum a_i x^i,$$

and

$$f_{\bar{g}}(x) = \hat{L}(x) = \sum a_{p^i} x^{p^i}.$$

For these power series we can see that if $L(x)$ is the logarithm of a formal group, then we will have $\hat{L}^{-1}(L(x)) \in \mathbb{Z}_p[[x]]$.

The height of a power series is obtained in the following manner. Let $f(x) \in \mathbb{Z}_p[[x]]$, then there is a natural mapping from this to $\bar{f}(x) \in \mathbb{Z}_p[[x]]/(p\mathbb{Z}) \cong \mathbb{Z}[[x]]/p\mathbb{Z}$. If the first (non-zero) term of $\bar{f}(x)$ is $a_h x^h$ then the height of the power series is h . Let $f(x)$ be an endomorphism of a formal group, then we can show that the height of $f(x)$ is a p -power.

Chapter 3

Properties of Power Series

3.1 Power Series Logarithms

Similarly to formal group logarithms, we can define logarithms for power series. First we observe that if $L(x)$ is a logarithm for a formal group $F(x, y)$ with endomorphism $f(x)$, then $L(f(x)) = f'(0)L(x)$. For example if $F(x, y) = x + y + xy$ then $L(x) = \sum (-1)^{i-1} \frac{x^i}{i}$. We know $f(x) = 2x + x^2$, and from this may compute:

$$\begin{aligned} L(f(x)) &= \sum (-1)^{i-1} \frac{(2x + x^2)^i}{i} \\ &= \sum (-1)^{i-1} \frac{x^i (2 + x)^i}{i} \\ &= \sum (-1)^{i-1} \frac{x^i \sum_{k=0}^i \binom{i}{k} x^{i-k} 2^k}{i} \\ &= 2 \sum (-1)^{i-1} \frac{x^i \sum_{k=0}^i \binom{i}{k} x^{i-k} 2^{k-1}}{i} \\ &= 2 \sum (-1)^{i-1} \frac{x^i}{i} \\ &= 2L(x) \\ &= f'(0)L(x). \end{aligned}$$

For a general power series $f(x) \in \mathbb{Z}_p[[x]]$, we can use this property to define the logarithm of $f(x)$.

Definition 5. Let $f(x)$ be a power series. A power series $L(x)$ is a logarithm if $L(f(x)) = f'(0)L(x)$.

We can prove that if $f(x)$ is an endomorphism of a formal group F , then if $L(x)$ is a logarithm of $f(x)$ it is also a logarithm of $F(x, y)$. For example if we take $f(x) = 2x + x^2$, then when we try to find an $L(x)$ such that $L(f(x)) = f'(0)L(x)$ we get that $L(x)$ is the logarithm of $F(x, y) = x + y + xy$. (Let $L(x) = \sum a_i x^i$, $L(f(x)) \equiv_{x^2} 2a_1 x \equiv_{x^2} f'(0)L(x)$ and $a_1 = 1$, $L(f(x)) \equiv_{x^3} 2x + x^2 + 4a_2 x^2 \equiv_{x^3} 2x + 2a_2 x^2$ and $a_2 = -\frac{1}{2}$, and so on as desired.)

This correspondence means that logarithms provide a bridge between power series and the endomorphisms of formal groups, i.e. we know that if the logarithm of a power series is the logarithm of a formal group, then the power series is an endomorphism of that formal group.

We now look for further connections between the power series logarithm and the formal group logarithm. We know that formal group logarithms have the property that $\frac{d}{dx}L(x) \in \mathbb{Z}_p[[x]]$, and we would like it if power series logarithms had that same property. For example take the power series $f(x) = (p+1)x + px^3$. We can construct the logarithm of $f(x)$ term by term. $L(x) = x + \sum_{i=1}^{\infty} b_i x^i$, $(p+1)x + b_2(p+1)^2 x^2 \equiv_{x^3} (p+1)x + (p+1)b_2 x^2$, and thus $b_2 = 0$. $(p+1)x + x^3 + b_3(p+1)^3 x^3 \equiv_{x^4} (p+1)x + (p+1)b_3 x^3$ and $b_3 = \frac{-1}{(p+1)(p+2)}$, continuing on in similar manner we get $b_4 = 0$ and $b_5 = \frac{3}{(p^2+2*p+2)(p+2)^2}$. Note that all of these terms are in \mathbb{Z}_p , as long as $p \neq 2$, since p does not divide the denominator.

Theorem 6. *If $L(x)$ is the logarithm of a power series $f(x) = \sum a_i x^i \in \mathbb{Z}[[x]]$, with $f'(x) \in p\mathbb{Z}_p[[x]]$ then $\frac{d}{dx}L(x) \in \mathbb{Z}_p[[x]]$.*

Proof: We proceed by induction on the degree. We know that $\frac{d}{dx}L(x)$ is of the form $L'(x) = 1 + \sum_{i=2}^{\infty} b_i x^i$. We also know that since $L(f(x)) = f'(0)L(x)$, $f'(x)L'(f(x)) = f'(0)L'(x)$. Base case: Substituting in we can see that

$$(a_1 + 2a_2x)(1 + b_2(a_1x)) \equiv_{x^2} a_1(1 + b_2x)$$

which implies that $b_2 = \frac{2a_2}{a_1 - a_1^2} = \frac{a_2}{a_1(1-a_1)}$. Note that since $f'(x) \in p\mathbb{Z}_p[[x]]$, we have that $p|2a_2$, and since $a_1(1-a_1)$ has at most one factor of p , $b_2 \in \mathbb{Z}_p$. Assume that for $i < n$, $b_i \in \mathbb{Z}_p$, then we have that

$$\left(\sum_{i=1}^n ia_i x^{i-1}\right)\left(1 + \sum_{i=2}^n b_i \left(\sum_{i=1}^n a_i x^i\right)^{i-1}\right) \equiv_{x^n} a_1 \left(1 + \sum_{i=1}^n b_i x^{i-1}\right).$$

Extracting the b_n terms we get

$$a_1^n b_n x^{n-1} - a_1 b_n x^{n-1} = b_n (a_1^n - a_1) x^{n-1} \equiv_{x^n} a_1 \left(1 + \sum_{i=1}^{n-1} b_i x^{i-1}\right) - \left(\sum_{i=1}^n i a_i x^{i-1}\right) \left(1 + \sum_{i=2}^{n-1} b_i \left(\sum_{i=1}^n a_i x^i\right)^{i-1}\right)$$

. Note that by the induction hypothesis all the b_i 's of the left side are in \mathbb{Z}_p , and when expanded each b_i is multiplied by an ia_i which is divisible by p . We are then dividing through by a factor that has at most one p power and everything cancels. Thus $b_n \in \mathbb{Z}_p$ and $\frac{d}{dx}L(x) \in \mathbb{Z}_p[[x]]$ as desired.

Thus we have that the derivative of the logarithm is in $\mathbb{Z}_p[[x]]$. Note also if $a_1 = p$, and the a_i 's all divide p , the derivative of the logarithm will also be in $\mathbb{Z}_p[[x]]$. (The proof is very similar.) Thus we now have two types of power series whose logarithms behave somewhat like the logarithms of formal groups.

We can make another connection between power series and the endomorphisms of formal groups.

Theorem 7. *If two power series $f(x), g(x)$ have the same logarithm $L(x)$, then $f(g(x)) = g(f(x))$.*

Note that this will be true of any two endomorphisms of the same formal group.

Proof: $\frac{d}{dx}f(g(x)) = g'(x)f'(g(x))$ which at 0 is $g'(0)f'(0)$, which is also the derivative of $g(f(x))$ evaluated at 0. Also note that $L(x)$ is a logarithm of $f(g(x))$ and $g(f(x))$ since $L(f(g(x))) = f'(g(0))L(g(x)) = f'(0)g'(0)L(x)$ as desired (we can also see $L(g(f(x))) = g'(0)f'(0)L(x)$). Thus

$$\begin{aligned} f(g(x)) &= L^{-1}(f'(0)g'(0)L(x)) \\ &= L^{-1}(g'(0)f'(0)L(x)) \\ &= g(f(x)) \end{aligned}$$

and thus composition commutes when f and g have the same logarithm.

3.2 Newton Polygons

A useful tool in the analysis of power series is the Newton polygon. First we define ord_p . $\text{ord}_p a$ is defined as the highest p power that is a factor of a (i.e. if $a = \frac{b}{c}p^\lambda$ where p does not divide b or c , then $\text{ord}_p a = \lambda$). Given a power series $f(x) = 1 + \sum_{i=1}^{\infty} a_i x^i$ with coefficients in \mathbb{Q}_p , a Newton polygon is obtained as follows. A point is put at $(0,0)$, then

$(1, \text{ord}_p a_1), \dots, (i, \text{ord}_p a_i)$, and so on. Then the polygon is drawn by rotating a line segment placed vertically at $(0,0)$ until it hits another point. The next is obtained from rotation from that point and so on.

For example if $f(x) = 1 + px + p^4x^2$ we have a Newton Polygon connecting points $(0,0)$ to $(1,1)$ to $(2,4)$ (since in this case the power series is finite, it has only 3 points.)

Another example is if $f(x) = 1 + \sum_{i=1}^{\infty} \frac{x^i}{i+1}$ (i.e. $L(x)/x$ for the logarithm of the multiplicative formal group), then we have points for the polygon at $(0,0), (1,0), \dots, (p-1, -1), \dots, (2p-1, -1), \dots, (p^2-1, -2), \dots$ which gives us a Newton Polygon with lines connecting $(0,0)$ to $(p-1, -1)$ to $(p^2-1, -2)$ and so on.

Conversely if $f(x) = 1 + \sum_{i=1}^{\infty} \frac{x^{p^i}}{p^i}$ (i.e. $1 + \hat{L}(x)$), then we have points for the Newton Polygon at $(0,0), (1, -1), (2, -2), \dots$ and the Newton polygon is just the line $y = -x$.

From the Newton polygon we can obtain information about the zeros of the power series. The slope of each segment corresponds to the p -adic order of the root (the highest power of p that appears) and the length determines the multiplicity. Thus for the example of $f(x) = L(x)/x$, we see that there are $p-1$ roots of p -adic order $1/(p-1)$, p^2-p roots of order $1/(p^2-p)$, p^3-p^2 roots of order $1/(p^3-p^2)$, and in general p^i-p^{i-1} roots of order $1/(p^i-p^{i-1})$. These roots are in fact $1-\zeta$ where ζ is a p^i th root of unity. Note that these are roots of the polynomial, and they have the necessary order.

As well, the least upper bound of the slopes of the Newton polygon determines the radius of convergence. (If the least upper bound is λ the radius of convergence is p^λ .) Thus for $f(x) = L(x)/x$ since we have a least upper bound of the slopes of $1/(p-1)$, the radius of convergence is $p^{1/(p-1)}$. Similarly, for $f(x) = 1 + \hat{L}(x)$ we have that the least upper bound of slopes is -1 and thus the radius of convergence is p^{-1} . The Newton polygon is obviously a useful tool in analyzing the behavior of power series (Koblitz).

3.3 Lubin's Theorem and Conjecture

Lubin found that for power series f, g such that $f \circ g = g \circ f$, where f is invertible, non-torsion, and g is non-invertible, then f and g have height of a p -power. However, any endomorphism of a formal group also has a p -power height. As well, all endomorphisms of the same formal group commute with one another, since they have the same logarithm. Thus it is

natural to guess that such power series f, g will always be endomorphisms of formal groups. However, this is not the case.

Notice that we may use an invertible power series $L(x)$ to construct commuting power series $f(x)$ and $g(x)$ by defining $f(x) = L^{-1}(cL(x))$, $g(x) = L^{-1}(dL(x))$ with constants c, d . The constants will be the first terms in the power series. The first term is

$$\begin{aligned} f'(0) &= \left(\frac{d}{dx} L^{-1}(cL(x)) \right) \Big|_0 \\ &= cL'(0) \left(\frac{d}{dx} L^{-1}(cL(0)) \right) \\ &= c. \end{aligned}$$

This implies $L(f(x)) = f'(0)L(x)$, and $L(x)$ is a logarithm of $f(x)$.

We may use this fact to construct counterexamples to Lubin's conjecture. For example let $L(x) = x + \frac{x^p}{p}$. We may then define $f(x) = L^{-1}((1 + p^2)L(x))$ and $g(x) = L^{-1}(p^2L(x))$. We can see that f is invertible, non-torsion and g is non-invertible (since that invertibility is defined by the first term). I also claim that $f, g \in \mathbb{Z}_p$. Proof that $f \in \mathbb{Z}_p$: We know that f is of the form $f(x) = \sum a_i x^i$. We proceed by induction on the degree. Since $L(f(x)) = (1 + p^2)L(x)$ implies that $a_1 x \equiv_{x^2} (1 + p^2)x$, $a_1 = 1 + p^2 \in \mathbb{Z}_p$. Now assume that $a_i \in \mathbb{Z}_p$ for $i < n$. We can see that

$$\sum_{i=1}^n a_i x^i + \frac{(\sum_{i=1}^n a_i x^i)^p}{p} \equiv_{x^{n+1}} (1 + p^2) \left(x + \frac{x^p}{p} \right)$$

we can then rewrite the equation so we have

$$a_n x^n \equiv_{x^{n+1}} (1 + p^2) \left(x + \frac{x^p}{p} \right) - \sum_{i=1}^{n-1} a_i x^i - \frac{(\sum_{i=1}^n a_i x^i)^p}{p}$$

but the binomial expansion means that each term will be divisible by p , and $a_n \in \mathbb{Z}_p$, and $f(x) \in \mathbb{Z}_p[[x]]$. Similarly we may prove $g(x) \in \mathbb{Z}_p[[x]]$.

However, I claim that $L(x)$ is not a logarithm of a formal group, and therefore f and g cannot be endomorphisms of a formal group.

Proof that $L(x)$ is not a logarithm of a formal group: Assume that $L(x)$ is the logarithm of a formal group $F(x, y)$. We may construct an endomorphism $[n](x) = x +_F \dots +_F x$ (n -times). Note that

$$\begin{aligned} [n](F(x, y)) &= (x +_F y) +_F \dots +_F (x +_F y) \\ &= (x +_F \dots +_F x) +_F (y +_F \dots +_F y) \\ &= F([n](x), [n](y)) \end{aligned}$$

and $[n](x)$ is an endomorphism. We know that $[n](x)$ has an infinite number of 0's. Since $L(x)$ is a logarithm of $F(x, y)$, we must have that $L([n](x)) = nL(x)$ (the first term of $[n](x)$ is obviously nx). This means that if $[n](a) = 0$, then $nL(a) = L([n](a)) = L(0) = 0$, and a is also a 0 of $L(x)$. The Newton polygon of $L(x)/x$ is a finite line between $(0, 0)$ and $(p, -1)$, implying that $L(x)$ only has p zeros, but $[n](x)$ has an infinite number of zeros, thus $L(x)$ is not a logarithm of $F(x, y)$ for any formal group.

Note that this counterexample to Lubin's conjecture rests on the fact that $L(x)$ (and therefore f and g) had a finite number of zeros. Thus one may add the qualification that the power series f and g must have an infinite number of zeros. However even adding this qualification there are still counterexamples, many of them connected to certain properties of the p -power terms of $L(x)$. (Sarkis)

Chapter 4

Progress made

There are a few observations to be made about logarithms. The first is that for a logarithm $L(x)$ of a power series $f(x)$, such that $f'(x) \in p\mathbb{Z}_p[[x]]$, $\frac{d}{dx}L(x) \in \mathbb{Z}_p[[x]]$. This allows one to make an observation about the coefficients of $\hat{L}^{-1} \circ L$.

This observation is something that I proved. Given the logarithm $L(x) = \sum \frac{a_i}{i} x^i$ (from above we know it takes that form with $a_i \in \mathbb{Z}_p$), we define $\hat{L}(x)$ to be $\sum a_{pi} x^{p^i}$. Given this it can be shown that $\hat{L}^{-1} \circ L \in \mathbb{Z}_p[[x]]$ implies $a_{np} \equiv_p a_n a_p$ for $n < p$. Thus we can construct logarithms with the appropriate properties up to the p^2 term. We want $\hat{L}^{-1} \circ L \in \mathbb{Z}_p[[x]]$, since this would imply (by the functional equation lemma) that $f(x)$ is an endomorphism of a formal group.

Generalizing this observation we have an expression for the coefficients of the logarithm. Let $L(x) = \sum_{i=1}^{\infty} \frac{b_i}{i} x^i$ be a logarithm of a function. We know already that $b_i \in \mathbb{Z}_p$. Let $\hat{L} = \sum_{i=0}^{\infty} \frac{b_{p^i}}{p^i} x^{p^i}$, for the same b_i 's. Consider $\hat{L}^{-1} \circ L$. Define $f(x) = \sum_{i=1}^{\infty} a_i x^i$ such that $f(x) = \hat{L}^{-1}(L(x))$, implying that $\hat{L}(f(x)) = L(x)$ or $L(x) - \hat{L}(f(x)) = 0$. Since this is by construction a polynomial, we know that the n -th coefficient of this polynomial is

$$\frac{1}{n!} \frac{d^n}{dx^n} (L(x) - \hat{L}(f(x)))$$

evaluated at 0. Expanding this out we see that

$$\frac{1}{n!} (L^{(n)}(x) - \sum_{i=1}^n K_i \hat{L}^{(i)}(x))$$

evaluated at 0, where

$$K_i = \sum_{k_1 + \dots + k_i = n} \frac{n!}{\alpha k_1! k_2! \dots k_i!} f^{(k_1)}(x) f^{(k_2)}(x) \dots f^{(k_i)}(x)$$

where if $k_1 = k_2 = \dots = k_j$, and $k_{j+1} = \dots = k_l$ etc, $\alpha = j!(l-j)!\dots$. Note evaluating this at 0 gives us

$$K_i = \sum_{k_1 + \dots + k_i = n} \frac{n!}{\alpha k_1! k_2! \dots k_i!} k_1! a_{k_1} k_2! a_{k_2} \dots k_i! a_{k_i} = \sum_{k_1 + \dots + k_i = n} \frac{n!}{\alpha}$$

Note that since

$$\hat{L}(x) = \sum \frac{b_{p^i}}{p^i} x^{p^i}$$

when we evaluate this at 0, we get

$$\frac{1}{n!} (n! \frac{b_n}{n} - (b_1 * a_1 + p! * K_p * a_p + \dots)) = \frac{b_n}{n} - a_n - p! K_p * (b_p / p) - \dots = 0.$$

This implies that

$$a_n = \frac{b_n}{n} - (p-1)! K_p * b_p - (p^2-1)! K_{p^2} b_{p^2} - \dots,$$

and thus we have a way of expressing the coefficients of $\hat{L}^{-1} \circ L$.

This expression for the coefficients of $\hat{L}^{-1} \circ L$ should help in an effort to determine under what conditions $L(x)$ is a formal group logarithm, and from that what conditions are needed on f and g , so that f and g are endomorphisms of a formal group. Hopefully this will lead to qualifications that need to be added to Lubin's conjecture so that it is true.

Bibliography

- [1] A. Frolich, *Formal Groups*, Springer-Verlag, Berlin, 1968.
- [2] Michiel Hazewinkel, *Formal Groups and Applications*, Academic Press, New York, 1978.
- [3] Neal Koblitz, *p -adic Numbers, p -adic Analysis, and Zeta-Functions* Springer-Verlag, Berlin 1984.
- [4] Ghassan Sarkis, conversations during Fall '06 and Spring '07 semesters.