COMPOSITIO MATHEMATICA

LAWRENCE H. COX

Formal A-modules over p-adic integer rings

Compositio Mathematica, tome 29, nº 3 (1974), p. 287-308

<http://www.numdam.org/item?id=CM_1974__29_3_287_0>

COMPOSITIO MATHEMATICA, Vol. 29, Fasc. 3, 1974, pag. 287-308
Noordhoff International Publishing
Printed in the Netherlands

FORMAL A-MODULES OVER p-ADIC INTEGER RINGS

Lawrence H. Cox [1]

Abstract

Let $B \supseteq A \supseteq \mathbb{Z}_p$ be p-adic integer rings with A finite over $\mathbb{Z}_p$. This paper is an investigation of (one-parameter) formal A-modules F defined over B. After an appropriate definition of the height h of F, the properties of F and of its logarithm $f(x)$ as power-series are studied in relation to B. The (strong) B-isomorphism classes of one-parameter formal A-modules defined over B are completely classified in the unramified case – generalizing a theorem of Honda and resulting in an explicit procedure for constructing all such F. Results of Hill and Lubin are generalized by relating this classification to the set of all Eisenstein polynomials of degree h defined over A. The questions of extendibility and normal form are answered and, assuming non-ramification, the absolute endomorphism ring of F is shown to be integrally closed. Given an arbitrary p-adic integer ring C, a variety of formal A-modules (non-isomorphic, different heights, different A's) are constructed whose absolute endomorphism rings are isomorphic to C.

1. One-parameter formal group laws

1.1. Let p be a fixed prime. $\mathbb{Q}_p$ will denote the p-adic rationals and $\mathbb{Z}_p$ the p-adic integers. Let $L \supset \mathbb{Q}_p$ be a field which is complete in the p-adic topology and let B denote the ring of integers of L (i.e., the integral closure of $\mathbb{Z}_p$ in L). M is the maximal ideal of B, B^* the multiplication group of units of B, $\tau \in M$ a fixed prime element of B and l the residue class field of B.

$\mathbf{X}$ denotes a finite set of variables and $B[[\mathbf{X}]]$ the ring of (formal) power-series in the variables of $\mathbf{X}$ with coefficients in B under ordinary addition and multiplication of power-series. $B[[\mathbf{X}]]_0$ is the sub-ring of $B[[\mathbf{X}]]$ consisting of all power-series in $B[[\mathbf{X}]]$ which have zero constant term. Note that composition of power-series makes sense in $B[[\mathbf{X}]]_0$.

We say that two power-series $R(\mathbf{X})$ and $S(\mathbf{X})$ are *congruent modulo degree n*, written $R(\mathbf{X}) \equiv S(\mathbf{X}) \bmod \deg n$, if the coefficients of $R(\mathbf{X})$ and

[1] This research was supported in part by NSF Grant GP-29082.

$S(\mathbf{X})$ differ only in degrees greater than or equal to n. We say $R(\mathbf{X})$ and $S(\mathbf{X})$ are congruent modulo τ, written $R(\mathbf{X}) \equiv S(\mathbf{X}) \bmod \tau$, if the coefficients of $R(\mathbf{X}) - S(\mathbf{X})$ belong to M.

Given $R(\mathbf{X}) \in B[[\mathbf{X}]]$ we define the *mod deg n part* of $R(\mathbf{X})$ to be that polynomial $R_n(\mathbf{X})$ of degree less than n for which $R_n(\mathbf{X}) \equiv R(\mathbf{X}) \bmod \deg n$.

DEFINITION 1.1.1: A *one-parameter formal group law* $F(X, Y)$ *defined over* B is a (formal) power-series in two variables $F(X, Y) \in B[[X, Y]]_0$ satisfying

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

(ii) $F(F(x, y), z) = F(x, F(y, z))$

for any power-series $x, y, z \in B[[\mathbf{X}]]_0$.

As a direct consequence of (i), we obtain: $F(x, y) \equiv x + y \bmod \deg 2$; and as B contains no nilpotent elements, it results (cf. (6)) that $F(x, y) = F(y, x)$. Also, direct computation yields that for each $x \in B[[\mathbf{X}]]_0$ there exists an $i_F(x) \in B[[\mathbf{X}]]_0$ such that $F(x, i_F(x)) = 0$.

To emphasize the 'group law' nature of $F(X, Y)$ we shall sometimes replace the notation $F(X, Y)$ by $X +_F Y$. Also, as we will deal only with one-parameter formal group laws, we shall henceforth refer to $F(X, Y)$ simply as a *formal group law* (over B).

DEFINITION 1.1.2: Let $R \supset B$ be a ring and let $F(X, Y)$ and $G(X, Y)$ be formal group laws defined over B. An *R-homomorphism* $t(x)$ *from* F *to* G is a power-series in one variable $t(x) \in R[[x]]_0$ for which $t(F(X, Y)) = G(t(X), t(Y))$ (i.e., $t(X +_F Y) = t(X) +_G t(Y)$).

We give $\mathrm{Hom}_R(F, G)$, the set of all R-homomorphisms from F to G, the structure of an Abelian group by defining $s(x) \oplus t(x) = s(x) +_G t(x)$, for any $s(x), t(x) \in \mathrm{Hom}_R(F, G)$. Lubin (cf. (8)) showed that $\mathrm{Hom}_R(F, G)$ is isomorphic to a closed additive subgroup of R via the map $c : \mathrm{Hom}_R(F, G) \to R$ given by $c(t(x)) = t'(0)$, where $t'(x)$ is the (formal) derivative of $t(x)$ with respect to x. In particular, $\mathrm{Hom}_L(F, G) \cong L$ and for $b \in L$ we denote by $[b]_{F,G}(x)$ that element of $\mathrm{Hom}_L(F, G)$ for which $c([b]_{F,G}(x)) = b$.

An *R-isomorphism* $t(x)$ *from* F *to* G is some $t(x) \in \mathrm{Hom}_R(F, G)$ which is invertible as a power-series; and $t(x)$ is the *strong R-isomorphism from* F *to* G if, in addition to the preceding, $t(x)$ also satisfies: $t(x) \equiv x \bmod \deg 2$.

A major result of Lazard (cf. (7)) was that if R is a $\mathbb{Q}$-algebra, then any two formal group laws defined over R are strongly R-isomorphic. This fact allows us to define what will become the keenest tool to be used in our investigation.

DEFINITION 1.1.3: Let $F(X, Y)$ be a formal group law defined over B. The *logarithm* $f(x)$ *of* $F(X, Y)$ is the unique strong L-isomorphism from $F(X, Y)$ to $G_a(X, Y) = X + Y$.

Thus, $f \circ F(X, Y) = f(X) + f(Y)$.

Let $f(x)$ and $g(x)$ be the respective logarithms of the formal group laws $F(X, Y)$ and $G(X, Y)$ defined over B. A straightforward verification yields that for any $b \in L$ the power-series $(g^{-1}bf)(x)$ is an L-homomorphism from F to G with $(g^{-1}bf)(x) \equiv bx \bmod \deg 2$. As $\mathrm{Hom}_L(F, G) \cong L$, then $(g^{-1}bf)(x) = [b]_{F,G}(x)$. In particular, F is strongly B-isomorphic to G if and only if $g^{-1} \circ f(x) \in B[[x]]_0$.

Let $\mathrm{End}\,(F) = \mathrm{Hom}_B(F, F)$ be the set of all B-endomorphisms of F and let $[b]_F(x)$ denote $[b]_{F,F}(x) \in \mathrm{End}\,(F)$. As $\mathrm{End}\,(F)$ already has the structure of an additive Abelian group, taking multiplication in $\mathrm{End}\,(F)$ to be ordinary composition of powerseries, it is easily verified that $\mathrm{End}\,(F)$ is a commutative ring. As $\mathrm{End}\,(F)$ is closed in B (in the p-adic topology induced by the map $c : \mathrm{End}\,(F) \to B$), then $\mathbb{Z}_p \subset \mathrm{End}\,(F) \subset B$. In particular, $\mathrm{End}\,(F)$ is complete.

1.2. Given a formal group law $F(X, Y)$ defined over B and any $[b]_F(x) \in \mathrm{End}\,(F)$, it is clear that $F^*(X, Y)$, the reduction of $F(X, Y)$ to the residue class field l of B, is a formal group law defined over l (i.e., $F^*(x, 0) = x$ and $F^*(F^*(x, y), z) = F^*(x, F^*(y, z))$ for any $x, y, z \in l[[\mathbf{X}]]_0$) and that $[b]_F^*(x)$, the reduction of $[b]_F(x)$ to l, is an l-endomorphism of $F^*(X, Y)$. Lazard (7) proved that $[b]_F^*(x)$ is either zero or is a power-series in x^{p^s} whose first non-zero coefficient occurs in degree p^s, for some integer $s \geqq 0$. He then defined the height of $F(X, Y)$.

DEFINITION 1.2.1: Let $F(X, Y)$ be a formal group law defined over B. If $[p]_F^*(x) = 0$, we say the *height* of $F(X, Y)$ is infinite. If not, we say $F(X, Y)$ is of *finite formal group height* H, where H is that positive integer such that the first nonzero coefficient of $[p]_F^*(x)$ occurs in degree p^H.

Note that the 'additive' group law $G_a(X, Y) = X + Y$ is of infinite height, whereas the 'multiplicative' group law $X + Y + XY$ is of height one.

The importance of this definition is reflected in the following facts:

(1) Over an algebraically closed field of characteristic $p \neq 0$, two formal group laws are isomorphic if and only if they are of the same formal group height (cf. (7)).

(2) If $F(X, Y)$ and $G(X, Y)$ are formal group laws defined over B which are of unequal heights, then $\mathrm{Hom}_R(F, G) = (0)$ for any domain $R \supset B$ (cf. (8)).

(3) *Honda's Theorem*: Assume L is unramified over $\mathbb{Q}_p$. The set of all

strong B-isomorphism classes of one-parameter formal group laws of finite height H defined over B corresponds bijectively to the set $M^{H-1} \times B^*$ (cf. (5)).

One of the major results of this paper is to generalize Honda's Theorem. It results that this generalization is to be found within the category of formal A-modules defined over B.

2. One-parameter formal A-modules

2.1. Let $K \subset L$ be a local field with ring of integers A. Let π be a fixed prime element of A, let k denote the residue class field of A and let the cardinality of k be $q = p^d$. Assume that $[K : \mathbb{Q}_p] = m$ and that the ramification index of K equals e, so that $de = m$.

DEFINITION 2.1.1: A one-parameter formal group law $F(X, Y)$ defined over B is a *one-parameter formal A-module* defined over B if for each $a \in A$ there is a B-endomorphism $[a]_F(x)$ of $F(X, Y)$ such that $[a]_F(x) \equiv ax \bmod \deg 2$.

REMARKS: Evidently, $[a]_F(x) = (f^{-1} a f)(x)$, where $f(x)$ is the logarithm of $F(X, Y)$; and any formal group law over B may be viewed as a formal $\mathbb{Z}_p$-module. As we are concerned only with the one-parameter case, we shall simply refer to $F(X, Y)$ as a *formal A-module* defined over B.

PROPOSITION 2.1.1: *Let $F(X, Y)$ be a formal A-module defined over B which is of finite formal group height H. Then $[\pi]_F^*(x)$, the reduction to l of $[\pi]_F(x)$, is a power-series in x^{q^h} whose first non-zero coefficient occurs in degree q^h, where $h = H/m$. Moreover, h is an integer.*

PROOF: As π^e and p are associate in A, then $([\pi]_F(x))^e = [\pi^e]_F(x)$ and $[p]_F(x)$ are associate in End (F). Thus, the first non-zero coefficient of $[\pi^e]_F^*(x)$ occurs in degree p^H. Therefore, the first non-zero coefficient of $[\pi]_F^*(x)$ occurs in degree $(p^H)^{1/e} = p^{H/e} = p^{mh/e} = p^{deh/e} = q^h$.

Lubin (9) showed that h is an integer. Q.E.D.

Consistent with Proposition 2.1.1 and our desire to relate information about formal A-modules in terms of A, we make the following definition.

DEFINITION 2.1.2: Let $F(X, Y)$ be a formal A-module defined over B. If $F(X, Y)$ is of finite formal group height H, then we define the *formal A-module height h* (henceforth, simply the *height*) of $F(X, Y)$ to be $h = H/m$. Otherwise, we say $F(X, Y)$ is of *infinite height*.

2.2. Let $F(X, Y)$ be a formal A-module defined over B and let

$$f(x) = \sum_{n=1}^{\infty} a_n x^n$$

be its logarithm. In this section, we prove certain technical facts about $f(x)$ which also serve to illustrate the interplay between the formal A-modules and the ring A.

PROPOSITION 2.2.1:
(i) $f(\pi x) \equiv 0 \bmod \pi$ *and*
(ii) $f^{-1}(\pi x) \equiv 0 \bmod \pi$
and hence $y \equiv 0 \bmod \pi$ *if and only if* $f(y) \equiv 0 \bmod \pi$, *for all* $y \in B[[X]]_0$.

PROOF (i): As $f(\pi x) \equiv 0 \bmod \deg 2, \bmod \pi$ we may assume inductively that $f(\pi x) \equiv 0 \bmod \deg n, \bmod \pi$. Thus

$$\pi^{n-1} f(x) \equiv \pi^{n-1} a_n x^n \bmod \deg (n+1), \bmod \pi. \tag{2.1}$$

Composing both sides of congruence (2.1) with $[\pi]_F(x) = (f^{-1}\pi f)(x)$ yields: $\pi^n f(x) \equiv \pi^{2n-1} a_n x^n \bmod \deg (n+1), \bmod \pi$. As $\pi^n f(x) \equiv \pi^n a_n x^n \bmod \deg (n+1), \bmod \pi$ by assumption, then $\pi^n a_n \equiv \pi^{2n-1} a_n \bmod \pi$. Therefore $\pi^n a_n \equiv 0 \bmod \pi$. Thus $f(\pi x) \equiv 0 \bmod \deg (n+1), \bmod \pi$, and the result is established by induction.

PROOF OF (ii): Let $f^{-1}(x) = \sum_{n=1}^{\infty} b_n x^n$ and assume by induction that

$$f^{-1}(\pi x) \equiv 0 \bmod \deg n, \bmod \pi$$

i.e.

$$f^{-1}(\pi x) \equiv \pi^n b_n x^n \bmod \deg (n+1), \bmod \pi$$

as

$$[\pi]_F(x) \circ f^{-1}(\pi x) \equiv \pi f^{-1}(\pi x) \bmod \deg (n+1), \bmod \pi$$

i.e.

$$(f^{-1}\pi f)(x) \circ f^{-1}(\pi x) \equiv \pi f^{-1}(\pi x) \bmod \deg (n+1), \bmod \pi$$

i.e.

$$f^{-1}(\pi^2 x) \equiv \pi f^{-1}(\pi x) \bmod \deg (n+1), \bmod \pi$$

then

$$\pi^{2n} b_n x^n \equiv \pi^{n+1} b_n x^n \bmod \pi$$

and hence $\pi^n b_n \in B$.

A glance ahead to Proposition 2.2.2 assures that

$$f \circ f^{-1}(\pi x) \equiv f(\pi^n b_n x^n) \bmod \deg (n+1), \bmod \pi$$

i.e.

$$\pi x \equiv \pi^n b_n x^n \bmod \pi$$

implying $\pi^n b_n \equiv 0 \bmod \pi$.

So,

$$f^{-1}(\pi x) \equiv 0 \bmod \deg (n+1), \bmod \pi$$

and the result is established by induction. Q.E.D.

The next two results exhibit the relationship between the arithmetic in the ring A and the power-series $F(X, Y)$ and $f(x)$, respectively. Let $t, y, z, w \in B[[\mathbf{X}]]_0$.

PROPOSITION 2.2.2: *$t \equiv y \bmod \pi$ if and only if there exists some $z \in B[[\mathbf{X}]]_0$ such that $t = y +_F \pi z$.*

PROOF: Assume $t = y + \pi w$ for some $w \in B[[\mathbf{X}]]_0$. Then

$$t -_F y = F(t, i_F(y)) = F(t, i_F(t - \pi w)).$$

As $i_F(t - \pi w) \equiv i_F(t) \bmod \pi$, then

$$t -_F y \equiv F(t, i_F(t)) \equiv 0 \bmod \pi$$

(i.e., $t -_F y = \pi z$ for some $z \in B[[\mathbf{X}]]_0$) and hence $t = y +_F \pi z$. The converse is trivial. Q.E.D.

PROPOSITION 2.2.3: *$t \equiv y \bmod \pi$ if and only if $f(t) \equiv f(y) \bmod \pi$.*

PROOF: $t = y + \pi w$ for some $w \in B[[\mathbf{X}]]_0$ if and only if $t = F(y, \pi z)$ for some $z \in B[[\mathbf{X}]]_0$ if and only if $f(t) = f(F(y, \pi z)) = f(y) + f(\pi z) \equiv f(y) \bmod \pi$. Q.E.D.

2.3. Lazard was the first to study the formal power-series properties of formal group laws and, in so doing, defined

$$B_n(X, Y) = (X + Y)^n - X^n - Y^n \qquad (n \geqq 2)$$

and

$$C_n(X, Y) = \begin{cases} B_n(X, Y) & \text{if } n \text{ is not a power of some prime} \\ \dfrac{1}{s} B_n(X, Y) & \text{if } n \text{ is a power of the prime } s \end{cases}$$

and showed that $C_n(X, Y)$ is a primitive polynomial over $\mathbb{Z}$. Then, by a series of difficult computations, he proved the following result (Lemma 3 of (7)).

THEOREM 2.3.1: *The R be a ring with unity which contains no nilpotent elements. If $F(X, Y)$ and $G(X, Y)$ are formal group laws defined over R*

for which $F(X, Y) \equiv G(X, Y) \bmod \deg n$, *then there exists* $c \in R$ *such that*

$$F(X, Y) \equiv G(X, Y) + cC_n(X, Y) \bmod \deg (n+1).$$

In particular, if $R = B$ then Theorem 2.3.1 yields

$$F(X, Y) \equiv G(X, Y) + bB_n(X, Y) \bmod \deg (n+1),$$

where

$$\left\{ \begin{array}{ll} b \in B & \text{if } n \text{ is not a power of } p \\ pb \in B & \text{if } n \text{ is a power of } p \end{array} \right\}.$$

Assuming a formal A-module structure, we obtain a sharper result.

THEOREM 2.3.2: *Let* $F(X, Y)$ *and* $G(X, Y)$ *be formal* A*-modules defined over* B *for which* $F(X, Y) \equiv G(X, Y) \bmod \deg n$. *Then*

$$F(X, Y) \equiv G(X, Y) + bB_n(X, Y) \bmod \deg (n+1),$$

where

$$\left\{ \begin{array}{ll} b \in B & \textit{if } n \textit{ is not a power of } q \\ \pi b \in B & \textit{if } n \textit{ is a power of } q \end{array} \right\}$$

PROOF: By induction, the case $n = 1$ being trivial. Assume the theorem is true for all $k < n$, where, by virtue of Theorem 2.3.1, we may assume that n is a power of p. Thus, by Theorem 2.3.1, there exists $b \in L$ with $pb \in B$ such that

$$F(X, Y) \equiv G(X, Y) + bB_n(X, Y) \bmod \deg (n+1).$$

If $b \in B$, we are done. If not, let t be the integer for which $\tau^t b \in B^*$. As $\phi_n(x) = x - bx^n$ behaves mod deg $(n+1)$ as an L-isomorphism from F to G, then for each $a \in A$ we have $\phi_n \circ [a]_F(x) \equiv [a]_G \circ \phi_n(x) \bmod \deg (n+1)$. Collecting terms, we obtain

$$([a]_G(x) - [a]_F(x)) \equiv b(a - a^n)x^n \bmod \deg (n+1). \tag{2.2}$$

As the left-hand side of congruence (2.2) is B-integral, then substituting $a = \pi$ yields that $\pi b \in B$. Multiplying (2.2) by τ^t and considering the result mod τ yields $a \equiv a^n \bmod \tau$, for all $a \in A$. Therefore, $(q-1)$ must divide $(n-1)$. As n and q are powers of p, this can happen only if n is a power of q. Q.E.D.

2.4. We now completely classify formal A-modules of *infinite* height over B.

THEOREM 2.4.1: *Let* $F(X, Y)$ *be a formal* A*-module defined over* B *and let* $f(x)$ *be its logarithm.* $F(X, Y)$ *is of infinite height if and only if* $\pi^{e'} f(x) \equiv 0 \bmod \pi$, *where* e' *is the ramification index of* L *over* K.

PROOF: The theorem is demonstrated by the equivalence of the following statements:

$$\pi^{e'} f(x) \equiv 0 \bmod \pi$$

$$[\pi^{e'}]_F(x) = (f^{-1}\pi^{e'} f) \equiv 0 \bmod \pi$$

$$[\pi]_F(x) \equiv 0 \bmod \tau. \qquad \text{Q.E.D.}$$

Thus, if L is unramified over K, there is a unique (strong) B-isomorphism class of one-parameter formal A-modules of infinite height defined over B.

3. Isomorphism classes of formal A-modules

3.1. Throughout this section we will *assume that L is unramified over K*. We parametrize the set $S(B, h)$ of strong B-isomorphism classes of one-parameter formal A-modules $F(X, Y)$ of finite height h defined over B by the set $M^{h-1} \times B^*$. This result is a generalization of Honda's Theorem and the approach adopted and many of the results employed are due to Honda. In particular, following Honda, we cast our problem in the setting of the ring $B_\sigma[[T]]$ and rely heavily upon the results of Honda's investigation of the arithmetic in this ring. The approach is constructive so that our work results in a straightforward computational means of constructing *all* oneparameter formal A-modules defined over B (in the unramified case). We then specialize to the case $A = B$ and obtain an alternate parametrization of the strong isomorphism classes – this time in terms of Eisenstein polynomials, thereby generalizing a result of Hill. We then compute explicit formulae which relate these two systems of parameters.

3.2. As L is unramified over K, let $\sigma \in \mathrm{Gal}(L/K)$ denote the Frobenius (i.e., the unique K-automorphism of L for which $b^\sigma \equiv b^q \bmod \pi$ for all $b \in B$). Define $L_\sigma[[T]]$ to be the ring of non-commutative power-series over L in the variable T with respect to the multiplication rule: $Tb = b^\sigma T$ for all $b \in L$. Let $B_\sigma[[T]]$ be the sub-ring of $L_\sigma[[T]]$ consisting of all power-series of this type which have coefficients in B. Let $L_\sigma[[T]]$ operate on $L[[x]]_0$ as follows: for $u(T) = \sum_{m=0}^{\infty} c_m T^m \in L_\sigma[[T]]$ and $r(x) \in L[[x]]_0$, define $u * r(x) = \sum_{m=0}^{\infty} c_m r^{\sigma^m}(x^{q^m})$ where $r^\sigma(x)$ is the power-series obtained from $r(x)$ by applying σ to each of the coefficients of $r(x)$. Then clearly $u * (v * r(x)) = (uv) * r(x)$ for any $v(T) \in L_\sigma[[T]]$.

DEFINITION 3.2.1: $u(T) \in B_\sigma[[T]]$ is *special* if $u(T) \equiv \pi \bmod \deg 1$.

DEFINITION 3.2.2: Let $u(T) \in B_\sigma[[T]]$ be special and let $P \in B^*$. Then

$r(x) \in L[[x]]_0$ is of *type* $(P; u)$ if

(1) $r(x) \equiv Px \bmod \deg 2$ and

(2) $u * r(x) \equiv 0 \bmod \pi$.

If $r(x) \equiv x \bmod \deg 2$ and if (2) holds we simply say r *is of type* u.

It is the relationship between special elements $u(T) \in B_\sigma[[T]]$ and logarithms $f(x)$ of formal A-modules $F(X, Y)$ defined over B which we shall develop. To this end, we present the following brief exposition of the results of Honda's investigation of the arithmetic of the ring $B_\sigma[[T]]$. The reader is referred to Sections 2 and 3 of (5) for the complete presentation.

LEMMA 3.2.1 (Integrality Lemma): *Let* $r(x) \in L[[x]]_0$ *be of type* $(P; u)$ *and let* $v(T) \in B_\sigma[[T]]$. *Let* $\psi(\mathbf{X}) \in L[[\mathbf{X}]]_0$. *If the coefficients of* $\psi(\mathbf{X})$ *of total degree* $< N$ *belong to* B *for* $N \geqq 2$, *then* $v * (r \circ \psi(\mathbf{X})) \equiv (v * r) \circ \psi(\mathbf{X})$ mod deg $(N+1)$, mod π.

This is Lemma 2.3 of (5), proved by direct computation. Its importance cannot be overstated, as evidenced by the following (Lemma 2.4 of (5)).

LEMMA 3.2.2: *If* $r(x)$, $s(x) \in L[[x]]_0$ *are of types* $(P; u)$ *and* $(Q; u)$, *respectively, then* $s^{-1} \circ r(x) \in B[[x]]_0$.

PROOF: Let $h(x) = (u^{-1}\pi) * (x)$. As $s^{-1} \circ r(x) = (h^{-1} \circ s(x))^{-1} \circ (h^{-1} \circ r(x))$, it suffices to verify the lemma for $s(x) = h(x)$. As $h^{-1} \circ r(x)$ is B-integral mod deg 2, assume inductively that it is B-integral mod deg N, for $N \geqq 2$. Then

$$\begin{aligned} \pi(h^{-1} \circ r(x)) &= (u * h) \circ (h^{-1} \circ r(x)) \\ &\equiv u * (h \circ h^{-1} \circ r(x)) \bmod \deg (N+1), \bmod \pi \\ &= u * r(x) \equiv 0 \bmod \pi. \end{aligned}$$

Thus, the N^{th} degree coefficient of $h^{-1} \circ r(x)$ is B-integral also and the lemma is therefore proved by induction. Q.E.D.

Honda then proceeds to relate elements $v(T) \in B_\sigma[[T]]$ and $r(x) \in L[[x]]_0$ for which $v * r(x) \equiv 0 \bmod \pi$.

LEMMA 3.2.3: *Let* $u(T) \in B_\sigma[[T]]$ *be special. Then* $r(x) \in L[[x]]_0$ *is of type* $(P; u)$ *if and only if* $r(x) = ((u^{-1}\pi) * (x)) \circ \psi(x)$ *for some* $\psi(x) \in B[[x]]_0$ *with* $\psi(x) \equiv Px \bmod \deg 2$.

Dually,

LEMMA 3.2.4: *Let* $r(x) \in L[[x]]_0$ *be of type* $(P; u)$ *and let* $v(T) \in B_\sigma[[T]]$.

Then $v * r(x) \equiv 0 \bmod \pi$ *if and only if there exists some* $t(T) \in B_\sigma[[T]]$ *such that* $v(T) = t(T) \cdot u(T)$.

The preceding lemmas are, respectively Propositions 2.5 and 2.6 of (5), both proved by means of the Integrality Lemma. Together they establish a correspondence between left-associate classes $(u(T))$ of special elements $u(T)$ of $B_\sigma[[T]]$ and 'B-right-associate' classes of certain power-series $r(x) = (u^{-1}\pi) * (x)$ in $L[[x]]_0$. To produce a canonical left-associate class representative for $(u(T))$, Honda proves (Lemma 3.4 of (5)).

LEMMA 3.2.5 (Weierstrass Preparation Theorem for $B_\sigma[[T]]$): *Let* $u(T) = \pi + \sum_{m=1}^{\infty} c_m T^m$ *be a special element of* $B_\sigma[[T]]$. *If each* c_m *belongs to* M, *then there is a unit* $t(T) \in B_\sigma[[T]]$ *such that* $tu = \pi$. *If* $c_1, \cdots, c_{h-1} \in M$ *while* $c_h \in B^*$, *then there is a unit* $t(T) \in B_\sigma[[T]]$ *such that* $t(T) \cdot u(T) = \pi + \sum_{m=1}^{h} b_m T^m$, *where* $b_1, \cdots, b_{h-1} \in M$ *while* $b_h \in B^*$.

3.3. We now set out to classify the strong B-isomorphism classes of one-parameter formal A-modules defined over B in terms of the set of left-associate classes of special elements $u(T) \in B_\sigma[[T]]$. We first relate the special elements to logarithms $f(x)$ of formal A-modules $F(X, Y)$ defined over B.

PROPOSITION 3.3.1: *Assume* L *is unramified over* K. *Let* $F(X, Y)$ *be a formal* A*-module defined over* B *and let* $f(x)$ *be its logarithm. Then there is a special element* $u(T) \in B_\sigma[[T]]$ *such that* f *is of type* u.

PROOF: Given $f(x)$, we shall construct $u(T)$ inductively. As $\pi * f(x) \equiv 0 \bmod \deg (q^0 + 1), \bmod \pi$, then we inductively assume that we have found $\pi = c_0, c_1, \cdots, c_m \in B$ such that

$$(c_0 + c_1 T + \cdots + c_m T^m) * f(x) \equiv 0 \bmod \deg (q^m + 1), \bmod \pi.$$

Say

$$(3.1) \qquad (c_0 + c_1 T + \cdots + c_m T^m) * f(x) \equiv \sum_{\lambda = \lambda'}^{\infty} b_\lambda x^\lambda \bmod \pi$$

where $\lambda' = \inf \{\lambda : b_\lambda \not\equiv 0 \bmod \pi\}$ and $q^m < \lambda' \leqq q^{m+1}$.

As $(F(X, Y))^{q^j} \equiv F^{\sigma^j}(X^{q^j}, Y^{q^j}) \bmod \pi$, composing both sides of congruence (3.1) with $F(X, Y)$ and applying Proposition 2.2.3, we obtain

$$\sum_{\lambda = \lambda'}^{\infty} b_\lambda (X^\lambda + Y^\lambda) \equiv \sum_{\lambda = \lambda'}^{\infty} b_\lambda (F(X, Y))^\lambda \bmod \pi.$$

Comparing terms of degree λ' in this congruence yields that

$$b_{\lambda'}(X^{\lambda'} + Y^{\lambda'}) \equiv b_{\lambda'}(X + Y)^{\lambda'} \bmod \pi,$$

and thus λ' is a power of p.

Composing both sides of congruence (3.1) with $[a]_F(x)$ for an arbitrary $a \in A$ yields

$$\pi f \circ [a]_F(x) + c_1 f^{\sigma}([a]_F(x))^q + \cdots + c_m f^{\sigma^m}([a]_F(x))^{q^m} \equiv \sum_{\lambda=\lambda'}^{\infty} b_\lambda([a]_F(x))^\lambda \bmod \pi.$$

As $([a]_F(x))^{q^j} \equiv [a]_F^{q^j}(x^{q^j}) \bmod \pi$, and as $f \circ [a]_F(x) = af(x)$, application of Proposition 2.2.3 to the above congruence yields:

$$a \sum_{\lambda=\lambda'}^{\infty} b_\lambda x^\lambda \equiv \sum_{\lambda=\lambda'}^{\infty} b_\lambda([a]_F(x))^\lambda \bmod \pi \qquad \text{for all } a \in A.$$

Comparing terms of degree λ' in this congruence yields

$$ab_{\lambda'} \equiv a^{\lambda'} b_{\lambda'} \bmod \pi \qquad \text{for all } a \in A. \tag{3.2}$$

In particular, for $a = \pi$ congruence (3.2) implies that $\pi b_{\lambda'} \equiv 0 \bmod \pi$ (i.e., $b_{\lambda'} \in B^*$). Thus, congrence (3.2) reduces to: $a \equiv a^{\lambda'} \bmod \pi$ for all $a \in A$. So, $(q-1) | (\lambda'-1)$. But the only powers λ' of p for which this is true are the powers of q. Thus, λ' is a power of q. As $q^{m+1} \geqq \lambda' > q^m$ by hypothesis, we may take $c_{m+1} = -b_{\lambda'}$ and obtain

$$(\pi + c_1 T + \cdots + c_m T^m + c_{m+1} T^{m+1}) * f(x) \equiv 0 \bmod \deg (q^{m+1}+1), \bmod \pi.$$

The proposition is, therefore, proved by induction. Q.E.D.

On the other hand, special elements give rise to logarithms of formal A-modules.

PROPOSITION 3.3.2: *Assume L is unramified over K. Let*

$$u(T) = \pi + b_1 T + \cdots + b_h T^h$$

with $b_1, \cdots, b_{h-1} \in M$ while $b_h \in B^*$. Define $f(x) = (u^{-1}\pi) * (x)$ and $F(X, Y) = f^{-1}(f(X) + f(Y))$. Then $F(X, Y)$ is a formal A-module of finite height h defined over B and $f(x)$ is its logarithm.

PROOF: Clearly $F(X, Y)$ is a formal group law. It is equally obvious that $f(x)$ is the logarithm of $F(X, Y)$. Note that f is of type u. We first prove that $F(X, Y)$ is defined over B. As $F(X, Y) \equiv X + Y \bmod \deg 2$, assume by induction that the coefficients of $F(X, Y)$ in degrees $< N$ belong to B for $N \geqq 2$. By Lemma 3.2.1,

$$\pi F(X, Y) = ((uu^{-1}\pi) * (x))F(X, Y) = (u * ((u^{-1}\pi) * (x))) \circ F(X, Y)$$
$$\equiv u * (((u^{-1}\pi) * (x)) \circ F(X, Y)) \bmod \deg (N+1), \bmod \pi$$
$$\equiv u * (f \circ F(X, Y)) = u * (f(X) + f(Y)) \equiv 0 \bmod \pi.$$

Thus, the N^{th} degree coefficients of $F(X, Y)$ belong to B also, and so $F(X, Y)$ is defined over B.

Given $a \in A$, as $[a]_F(x) \equiv ax \bmod \deg 2$, then assume inductively that all coefficients of $[a]_F(x)$ in degrees $< N$ belong to B for $N \geqq 2$.

Applying Lemma 3.2.1 and realizing that A is contained in the center of $B_\sigma[[T]]$, we observe

$$\begin{aligned}
\pi[a]_F(x) &= ((uu^{-1}\pi) * (x)) \circ [a]_F(x) = (u * ((u^{-1}\pi) * (x))) \circ [a]_F(x) \\
&\equiv u * (((u^{-1}\pi) * (x)) \circ [a]_F(x)) \bmod \deg (N+1), \bmod \pi \\
&= u * (f \circ [a]_F(x)) = u * (af(x)) = (ua) * f(x) \\
&= (au) * f(x) = a * (u * f(x)) \\
&\equiv 0 \bmod \pi.
\end{aligned}$$

So, the N^{th} degree coefficient of $[a]_F(x)$ belongs to B also. Therefore, $F(X, Y)$ is a formal A-module defined over B.

It remains to show that the height of $F(X, Y)$ equals h. By Lemmas 3.2.2 and 3.2.4, it suffices to prove that the formal A-module obtained from

$$\begin{aligned}
u'(T) &= (1+\pi^{-1}b_1 T+\pi^{-1}b_2 T^2+\cdots+\pi^{-1}b_{h-1} T^{h-1})^{-1}u(T) \\
&\equiv \pi+b_h T^h \bmod \deg (h+1)
\end{aligned}$$

is of height h. Call this formal A-module $F(X, Y)$ and its logarithm $f(x)$ also. As $f(x) = ((u')^{-1}\pi) * (x)$, then $f(x) \equiv x - \pi^{-1}b_h x^{q^h} \bmod \deg (q^h+1)$. Thus $[\pi]_F(x) \equiv \pi x - b_h x^{q^h} \bmod \deg (q^h+1)$, and thus the height of $F(X, Y)$ equals h. Q.E.D.

Therefore, to (the logarithm of) each formal A-module $F(X, Y)$ of finite height defined over B there corresponds a left-associate class of special elements of $B_\sigma[[T]]$; and the height of $F(X, Y)$ equals the minimal degree of a representative $u(T)$ of this left-associate class. Any formal A-module $G(X, Y)$ defined over B which is strongly B-isomorphic to $F(X, Y)$ clearly has the same left-associate class corresponding to it as does $F(X, Y)$. Conversely, if $F(X, Y)$ and $G(X, Y)$ are formal A-modules of finite height h defined over B which both have the left-associate class of some special $u(T)$ corresponding to them, then their respective logarithms $f(x)$ and $g(x)$ are of type u and hence $F(X, Y)$ and $G(X, Y)$ are strongly B-isomorphic by Lemma 3.2.2. So, we have proved

THEOREM 3.3.1: *Assume L is unramified over K. There is a one-to-one correspondence between the set $S(B, h)$ of strong B-isomorphism classes of one-parameter formal A-modules of finite height h defined over B and*

special elements $u(T) \in B_\sigma[[T]]$ *of the form:* $u(T) = \pi + b_1 T + \cdots + b_h T^h$, *where* $b_1, \cdots, b_{h-1} \in M$ *while* $b_h \in B^*$.

3.4. *Construction.* Given $(b_1, \cdots, b_h) \in M^{h-1} \times B^*$, form the special element $u(T) = \pi + b_1 T + \cdots + b_h T^h$ and the power-series $f(x) = (u^{-1}\pi) * (x)$. Then $f(x)$ is the logarithm of the height h formal A-module $F(X, Y) = f^{-1}(f(X) + f(Y))$ defined over B. Moreover, a formal A-module $G(X, Y)$ defined over B is strongly B-isomorphic to $F(X, Y)$ if and only if its logarithm $g(x)$ is of the form: $g(x) = f(x) \circ \psi(x)$ where $\psi(x) \in B[[x]]_0$ and $\psi(x) \equiv x \bmod \deg 2$. We thus have an explicit means of constructing *all* one-parameter formal A-modules of height h defined over B.

3.5. Carrying our techniques a little further, we prove

THEOREM 3.5.1: *Assume L is unramified over K. Let $F(X, Y)$ and $G(X, Y)$ be formal A-modules of finite height h defined over B and let their logarithms be of types u and v, respectively. Then, as A-modules,* $\mathrm{Hom}_B(F, G) \cong \{c \in B : vc = cu\}$.

PROOF: For $c \in B$, consider $[c]_{F,G} = (g^{-1} c f)(x)$. By Lemma 3.2.3, we may assume $f(x) = (u^{-1}\pi) * (x)$ and $g(x) = (v^{-1}\pi) * (x)$.

Assume $vc = cu$. As $[c]_{F,G}(x) \equiv cx \bmod \deg 2$, assume by induction that the coefficients of $[c]_{F,G}(x)$ in degrees $< N$ belong to B for $N \geqq 2$. Using Lemma 3.2.1,

$$\begin{aligned}
\pi[c]_{F,G}(x) &= ((vv^{-1}\pi) * (x)) \circ [c]_{F,G}(x) \\
&= (v * ((v^{-1}\pi) * (x))) \circ [c]_{F,G}(x) \\
&\equiv v * (((v^{-1}\pi) * (x)) \circ [c]_{F,G}(x)) \bmod \deg (N+1), \bmod \pi \\
&= v * (g \circ [c]_{F,G}(x)) \\
&= v * (cf(x)) = (vc) * f(x) = (cu) * f(x) \equiv 0 \bmod \pi.
\end{aligned}$$

Thus, the N^{th} degree coefficient of $[c]_{F,G}(x)$ belongs to B also and hence $[c]_{F,G}(x) \in \mathrm{Hom}_B(F, G)$ by induction.

Conversely, if $[c]_{F,G}(c) \in B[[x]]_0$, then there exists $\psi(x) \in B[[x]]_0$ such that $(g^{-1} c f)(x) = \psi(x)$ and so $cf(x) = g \circ \psi(x)$. Hence,

$$(vc) * f(x) = v * (cf(x)) \equiv 0 \bmod \pi.$$

Therefore, by Lemma 3.2.4, there exists $t(T) \in B_\sigma[[T]]$ such that $vc = tu$. By Theorem 3.3.1, we may assume both $u(T)$ and $v(T)$ are 'polynomials' of degree h. Therefore, $t = c$.

That the map $[c]_{F,G}(x) \leftrightarrow c$ is an A-module homomorphism is a simple verification. Q.E.D.

3.6. *Strong Isomorphism and Eisenstein Polynomials.* In (9), Lubin investigated one-parameter formal A-modules defined over A and proved that two formal A-modules defined over A whose reductions to the residue class field k of A are k-isomorphic must be A-isomorphic. In (3), Hill proved that there exists a one-to-one correspondence between the set of strong $\mathbb{Z}_p$-isomorphism classes of one-parameter formal group laws of finite height h defined over $\mathbb{Z}_p$ and the set of Eisenstein polynomials of degree h defined over $\mathbb{Z}_p$. In this section, we prove a result which generalizes both these theorems. Moreover, we perform some calculations which enable us to interpret our result in terms of Theorem 3.3.1.

Note that for a formal A-module $F(X, Y)$ defined over A, we have that $A \cong \mathrm{End}\,(F)$, in which addition is $+_F$ and multiplication is composition of power-series.

THEOREM 3.6.1: *The set $S(A, h)$ of strong A-isomorphism classes of one-parameter formal A-modules of finite height h defined over A corresponds bijectively to the set of all Eisenstein polynomials of degree h defined over A. Specifically, if $F(X, Y)$ is a formal A-module of height h defined over A whose strong A-isomorphism class is represented by $(b_1, \cdots, b_h) \in M_A^{h-1} \times A^*$ as per Theorem* 3.3.1, *then the minimal polynomial $P(Z)$ over $A \cong \mathrm{End}\,(F)$ of the Frobenius formal A-module endomorphism $\xi(x) = x^q$ of the reduction of $F(X, Y)$ to the residue class field k of A is given by*

$$P(Z) = Z^h + (b_h)^{-1} b_{h-1} Z^{h-1} + \cdots + (b_h)^{-1} b_1 Z + (b_h)^{-1} \pi.$$

Conversely, given an Eisenstein polynomial

$$P(Z) = Z^h + c_{h-1} Z^{h-1} + \cdots + c_0$$

defined over A, the formal A-module $F(X, Y)$ defined over A which corresponds to the tuple

$$\left(\frac{c_1 \pi}{c_0}, \frac{c_2 \pi}{c_0}, \cdots, \frac{c_{h-1} \pi}{c_0}, \frac{\pi}{c_0} \right) \in M^{h-1} \times A^*$$

as per Theorem 3.3.1 *has $P(Z)$ as the minimal polynomial over $A \cong \mathrm{End}\,(F)$ of the Frobenious A-module endomorphism of the reduction of $F(X, Y)$ to k.*

PROOF: The theorem is proved by observing that the following statements are equivalent:

$$\begin{aligned}
(\pi + b_1 T + \cdots + b_h T^h) * f(x) &\equiv 0 \bmod \pi \\
\pi f(x) + b_1 f(x^q) + \cdots + b_h f(x^{q^h}) &\equiv 0 \bmod \pi \\
b_h^{-1} \pi f(x) + b_h^{-1} b_1 f(x^q) + \cdots + f(x^{q^h}) &\equiv 0 \bmod \pi \\
f \circ [b_h^{-1} \pi]_F(x) + f \circ [b_h^{-1} b_1]_F(x^q) + \cdots + f \circ [1]_F(x^{q^h}) &\equiv 0 \bmod \pi \\
f \circ ([b_h^{-1} \pi]_F(x) +_F [b_h^{-1} b_1]_F(x^q) +_F \cdots +_F [1]_F(x^{q^h})) &\equiv 0 \bmod \pi
\end{aligned}$$

which, by Proposition 2.2.3, is equivalent to:

$$[b_h^{-1}\pi]_F(x)+_F[b_h^{-1}b_1]_F(x^q)+_F\cdots+_F[1]_F(x^{q^h}) \equiv \bmod \pi$$

which holds if and only if $\xi(x) = x^q$ satisfies the Eisenstein polynomial equation: $P(Z) = Z^h + b_h^{-1}b_{h-1}Z^{h-1} + \cdots + b_h^{-1}b_1 Z + b_h^{-1}\pi$ defined over $A \cong \mathrm{End}\,(F)$ (in which addition is $+_F$ and multiplication is composition of power-series). Q.E.D.

So, for the case $A = B$, we see that the special elements are lifting to A of (analytic) equations satisfied in k by the Frobenius.

COROLLARY: *Two formal A-modules defined over A whose reductions to the residue class field k of A are k-isomorphic must be A-isomorphic.*

PROOF: Let $\psi^*(x)$ be any k-isomorphism from F^* to G^*. Lifting $\psi^*(x)$ in any manner to a power-series $\psi(x) \in B[[x]]_0$, we have that $F(X, Y)$ and $G_1(X, Y) = \psi^{-1} \circ G(\psi(X), \psi(Y))$ have the same reduction to k and hence the same minimal polynomial for the Frobenius. So, F and G_1 are strongly A-isomorphic. Thus, F and G are A-isomorphic. Q.E.D.

4. Structure theorems

4.1. In this section, under the assumption that L is unramified over K, we undertake a detailed investigation of formal A-modules $F(X,Y)$ defined over B and their logarithms $f(x)$. We prove specific results which serve not only as valuable computational tools but which also underscore the differences between formal A-modules and arbitrary formal group laws defined over B.

We first prove that the Newton polygon of $f(x)$ is 'logarithmic'.

PROPOSITION 4.1.1: *Assume L is unramified over K. Let $F(X, Y)$ be a formal A-module of finite height h defined over B and let $f(x) = \sum_{n=1}^{\infty} a_n x^n$ be its logarithm. Then*

$$\left\{\begin{array}{ll} a_n \in B & \text{if } n \text{ is not a multiple of } q^h \\ \pi^r a_n \in B & \text{if } n \text{ is a multiple of } q^h \text{ and } q^{hr} \leqq n < q^{h(r+1)} \\ \pi^r a_n \in B^* & \text{if } n = q^{hr} \end{array}\right\}$$

PROOF: Let $(b_1, \cdots, b_h) \in M^{h-1} \times B^*$ be such that

$$\pi f(x) + b_1 f^{\sigma}(x^q) + \cdots + b_h f^{\sigma^h}(x^{q^h}) \equiv 0 \bmod \pi. \tag{4.1}$$

If n is not a multiple of q, congruence (4.1) yields that $\pi a_n \equiv 0 \bmod \pi$ and so $a_n \in B$. If n is a multiple of q but is not a multiple of q^2, then $\pi a_n + b_1 a_{n/q}^{\sigma} \equiv 0 \bmod \pi$ and as $a_{n/q} \in B$ by the preceding sentence, then $a_n \in B$. Similarly, for all multiples n of $q^2, q^3, \cdots, q^{h-1}$ which are not multiples of q^h we have $a_n \in B$.

For $n = q^h$, congruence (4.1) yields that $\pi a_{q^h} + b_1 a_{q^{h-1}}^{\sigma} + \cdots + b_h \equiv 0 \bmod \pi$, and hence $\pi a_{q^h} \in B^*$.

We proceed by induction on multiples n of q^h. Assume that, whenever $n' < n$ and n' is a multiple of q^h, we have

$$\begin{Bmatrix} \pi^{r'} a_{n'} \in B & \text{for } q^{hr'} \leqq n' < q^{h(r'+1)} \\ \pi^{r'} a_{n'} \in B^* & \text{for } n' = q^{hr'} \end{Bmatrix}$$

Let $n = sq^h$ and assume $q^{hr} \leqq n < q^{h(r+1)}$. Collecting terms of degree n from congruence (4.1), we obtain

$$\pi a_n + b_1 a_{sq^{h-1}}^{\sigma} + \cdots + b_h a_s^{\sigma^h} \equiv 0 \bmod \pi. \tag{4.2}$$

The inductive hypothesis implies that

$$\pi^{r-1} b_j a_{sq^{h-j}}^{\sigma} \in B \qquad 1 \leqq j \leqq h.$$

Multiplying congruence (4.2) by π^{r-1}, we obtain $\pi^r a_n \in B$. Moreover, if $n = q^{hr}$, congruence (4.2) yields that

$$\pi^r a_n \equiv -\pi^{r-1} b_h a_s^{\sigma^h} \bmod \pi.$$

Since $s = q^{h(r-1)}$, then $\pi^r a_n \in B^*$ as asserted. Q.E.D.

COROLLARY: $\pi^r f(x) \equiv 0 \bmod \deg q^{hr}, \bmod \pi$.

REMARK: The converse of Proposition 4.1.1 is *not* true. If $p \neq 2$ and

$$f(x) \equiv x - \frac{1}{\pi} x^q - \frac{1}{\pi^2} x^{q^2} \bmod \deg (q^2+1)$$

then there does not exist a special element $u(T) = \sum_{m=0}^{\infty} b_m T^m$ in $B_\sigma[[T]]$ for which $u * f(x) \equiv 0 \bmod \pi$, as direct computation shows that $\pi b_2 \equiv 2 \bmod \pi$ and, since $p \neq 2$, this implies $\pi b_2 \in B^*$.

4.2. The next theorem illustrates the uniformity of structure present in the unramified case.

THEOREM 4.2.1: *Assume L is unramified over K. Let $F(X, Y)$ be a formal A-module of finite height h defined over B. Then there exists $b \in L$ with $\pi b \in B^*$ such that $F(X, Y)$ is strongly B-isomorphic to a formal A-module $H(X, Y)$ of the form*:

$$H(X, Y) \equiv X + Y + bB_{q^h}(X, Y) \bmod \deg (q^h+1).$$

We say such an $H(X, Y)$ is in normal form.

PROOF: Let $f(x) = \sum_{n=1}^{\infty} a_n x^n$ be the logarithm of $F(X, Y)$.

As $a_n \in B$ for $1 \leqq n < q^h$ and as $\pi a_{q^h} \in B^*$ by Proposition 4.1.1, we may construct $\psi(x) \in B[[x]]_0$ *such that*

$$h(x) = f \circ \psi(x) \equiv x - bx^{q^h} \bmod \deg (q^h+1),$$

for some $b \in L$ with $\pi b \in B^*$.Then, $H(X, Y) = h^{-1}(h(X)+h(Y))$ is the desired formal A-module defined over B. Q.E.D.

4.3. *Extendibility.* Lazard (7) showed that any power-series $R(X, Y)$ which is an abelian $(n-1)$-bud defined over B i.e., which satisfies

(1) $R(X, Y) = R(Y, X) \in B[[X, Y]]_0$
(2) $R(X, Y) \equiv X + Y \bmod \deg 2$
(3) $R(R(X, Y), Z) \equiv R(X, R(Y, Z)) \bmod \deg n$

is *extendible* to a formal group law $F(X, Y)$ defined over B, i.e., there exists a formal group law $F(X, Y)$ defined over B for which $F(X, Y) \equiv R(X, Y) \bmod \deg n$.

We answer the question of extendibility for formal A-modules. Let $n \geqq 2$ be a fixed integer.

Let $R(X, Y)$ be an abelian $(n-1)$-bud defined over B, and let $r(x)$ be any solution of the congruence $r \circ R(X, Y) \equiv r(X)+r(Y) \bmod \deg n$, for which $r(x) \equiv x \bmod \deg 2$.

Fixing $r(x)$, define, for each $a \in A$, $[a]_R(x) = (r^{-1}ar)(x)$. (Note that the mod deg n part of $[a]_R(x)$ is independent of the choice of $r(x)$).

DEFINITION 4.3.1: Let $R(X, Y)$ be an abelian $(n-1)$-bud defined over B. If the coefficients of $[a]_R(x)$ in degree $< n$ belong to B for each $a \in A$, we say $R(X, Y)$ *behaves* mod deg n *like a formal A-module defined over B.*

For each integer $s > 2$, define $B[[X, Y]]_s$ to be the subring of $B[[X, Y]]_0$ consisting of all power-series in $B[[X, Y]]_0$ which have their non-zero coefficients only in degrees congruent to 1 modulo $(s-1)$. Let τ denote a fixed prime element of B.

THEOREM 4.3.1: *Let $R(X, Y) \in B[[X, Y]]_0$ behave* mod deg n *like a formal A-module defined over B. Then there exists a formal A-module $F(X, Y)$ defined over B such that*

$$F(X, Y) \equiv R(X, Y) \bmod \deg n.$$

PROOF: It suffices to construct an $\bar{R}(X, Y) \in B[[X, Y]]_0$ which agrees with $R(X, Y)$ mod deg n and which behaves mod deg $(n+1)$ like a formal A-module defined over B, for then the existence of a formal A-module $F(X, Y)$ of the desired type is guaranteed by induction.

Extend the mod deg n part of $R(X, Y)$ in any way to a formal group law (also called $R(X, Y)$) defined over B. Let $w \in A$ be a primitive $(q-1)^{st}$ root of unity.

Then the mod deg n part $\psi_n(x)$ of any solution $\psi(x)$ of the equation $[w]_R(x) \circ \psi(x) = \psi(wx)$ for which $\psi(x) \equiv x \bmod \deg 2$, behaves *mod deg n*

like a B-isomorphism of $R(X, Y)$ (see Lemma 4.1.2 of (8)). Thus, $\psi^{-1} \circ R(\psi(X), \psi(Y)) \in L[[X, Y]]_q$ is a formal group law defined over L whose mod deg n part $S_1(X, Y)$ behaves mod deg n like a formal A-module defined over B. Extend $S_1(X, Y)$ in any way to a formal group law $S(X, Y) \in B[[X, Y]]_q$ and let $s(x)$ denote the logarithm of $S(X, Y)$. Then $[w]_S(x) = wx$.

It now suffices to find a form $\Gamma(X, Y)$ of degree n with coefficients in B such that the mod deg $(n+1)$ part $T_1(X, Y)$ of $S(X, Y)+\Gamma(X, Y)$ behaves mod deg $(n+1)$ like a formal A-module defined over B, because then the mod deg $(n+1)$ part of $\psi_n \circ T_1(\psi_n^{-1}(X), \psi_n^{-1}(Y))$ will serve as the desired extension $\bar{R}(X, Y)$ of $R(X, Y)$.

Let c denote the coefficient of the n^{th} degree term of $[\pi]_S(x)$. As $S(X, Y) \in B[[X, Y]]_q$ then $[\pi]_S(x) \in L[[x]]_q$ and hence $(q-1) | (n-1)$. If $c \in B$, then the mod deg $(n+1)$ part of $S(X, Y)$ is already the desired extension of $S_1(X, Y)$. Assume $c \notin B$, let $p = a\pi^e$ with $a \in A^*$. As a can be written as a sum of products of powers of w and π, then $[a]_S(x)$ is B-integral *mod deg n*. Moreover, its n^{th} degree coefficient a^1 can be no worse than c (i.e., $(a^1/c) \in B$). As $[p]_S(x)$ is B-integral, then direct computation yields that the n^{th} degree coefficient of $[a]_S(x) \circ ([\pi]_S(e))^e$ is of the form: $a^1(\pi^{ne}) + ac\pi^{e-1}(1+\pi b)+b'$, where $b, b' \in B$. Thus, $\pi^{e-1}c \in B$. As,

$$\tau[\pi]_S(x) \equiv \tau c x^n \bmod \deg (n+1), \bmod \tau$$

by hypothesis, then composing both sides of this congruence with $S(X, Y)$ yields:

$$\tau c(X+Y)^n \equiv \tau c(X^n + Y^n) \bmod \tau$$

(i.e., $\tau c B_n(X, Y) \equiv 0 \bmod \tau$). Therefore, n is a power of p. As $(q-1) | (n-1)$, then n is a power of q. Thus, the mod deg $(n+1)$ part $T_1(X, Y)$ of

$$S(X, Y) + \frac{c}{\pi - \pi^n} B_n(X, Y)$$

belongs to $B[[X, Y]]_q$.

Complete $T_1(X, Y)$ to a formal group law $T(X, Y) \in B[[X, Y]]_q$. Let $t(x)$ be the logarithm of $T(X, Y)$. Then

$$t(x) \equiv s(x) - \frac{c}{\pi - \pi^n} x^n \bmod \deg (n+1),$$

and hence

$$[\pi]_T(x) \equiv [\pi]_S(x) + \left(\frac{c}{\pi - \pi^n}\right)(\pi^n - \pi)x^n \bmod \deg (n+1).$$

Therefore, the mod deg $(n+1)$ part of $[\pi]_T(x)$ belongs to $B[[x]]_q$ and so $T_1(X, Y)$ is the desired extension of $S_1(X, Y)$. Q.E.D.

Notice that the preceding theorem provides an explicit, step-by-step procedure for extending $R(X, Y)$.

5. The absolute endomorphism ring

5.1. DEFINITION 5.1.1: Let $F(X, Y)$ be a formal group law of finite height defined over B. The absolute endomorphism ring $\mathrm{END}(F)$ of $F(X, Y)$ is the ring whose underlying set is the union of all $\mathrm{End}_C(F)$ over all rings of integers $C \supseteq B$.

If $F(X, Y)$ is of finite formal group height H, Lubin (8) showed that $\mathrm{END}(F)$ is contained in the ring of integers of the compositum of all field extensions of $\mathbb{Q}_p$ of degree dividing H. In particular, the degree of the fraction field of $\mathrm{END}(F)$ over $\mathbb{Q}_p$ divides H. More recently, Waterhouse (11) proved that $\mathrm{END}(F)$ is contained in the ring of integers of an unramified extension of L. The following proposition is, therefore, a simple restatement of the work of Waterhouse and Lubin.

PROPOSITION 5.1.1: *Let $F(X, Y)$ be a formal A-module of finite height h defined over B. Then $END(F)$ is contained in the ring of integers of the unramified extension L_h of L of degree h. Also, the degree of the fraction field of $END(F)$* over K *divides h.*

5.2. In this section, we investigate the relationship between the various possible $\mathrm{END}(F)$'s and arbitrary p-adic integer rings.

The following result on the structure of certain non-integral endomorphisms is certainly not best possible, but is well-suited to our needs.

LEMMA 5.2.1: *Assume L is unramified over K. Let $F(X, Y)$ be a formal A-module of finite height h defined over B and let c be a unit in the ring of integers C in an unramified extension of L. Assume that*

$$[c]_F(x) = \sum_{k=1}^{\infty} c_k x^k$$

is not *C-integral and that c_n is the first non-integral coefficient of $[c]_F(x)$. Then $n \geqq q^h$, and the coefficients of $[c]_F(x)$ satisfy*

$$\pi^{r+1} c_{n+r} \in C \qquad \text{for all } r \geqq 0.$$

PROOF: As the logarithm $f(x)$ of $F(X, Y)$ is B-integral mod deg q^h by Proposition 4.1.1, then so too is $[c]_F(x)$. Thus, $n \geqq q^h$. We proceed by induction on r. For $r = 0$, collecting terms of degree n on both sides of the equation

$$\pi[c]_F \circ [\pi]_F(x) = \pi[\pi]_F \circ [c]_F(x)$$

and reducing mod π, we obtain: $\pi^{n+1} c_n \equiv \pi^2 c_n \bmod \pi$. Thus, $\pi c_n \in C$.

Assume the lemma holds for $0 \leqq j < r$. In like fashion to the preceding argument, consider the equation

$$\pi^{r+1}[c]_F \circ [\pi]_F(x) = \pi^{r+1}[\pi]_F \circ [c]_F(x). \tag{5.1}$$

As $n \geqq q^h$, then

$$\pi^{r+1}[\pi]_F \circ (cx + \cdots + c_{n+r-1}x^{n+r-1}) \equiv 0 \bmod \deg (n+r+1), \bmod \pi.$$

Also, as $\pi^{r+1}[c]_F \circ [\pi]_F(x) \equiv 0 \bmod \deg (n+r)$, mod π, then considering equation (5.1) mod deg $(n+r+1)$, mod π we obtain

$$\pi^{n+2r+1}c_{n+r}x^{n+r} \equiv \pi^{r+2}c_{n+r}x^{n+r} \bmod \pi.$$

Thus $\pi^{r+1}c_{n+r} \in C$ as asserted. Q.E.D.

Weaker forms of the following theorem exist, but I know of none which is proved directly from power-series considerations. (Note that a non-power-series proof follows from Theorem 3.5.1).

THEOREM 5.2.1: *Assume L is unramified over K. Let $F(X, Y)$ be a formal A-module of finite height h defined over B. Then $\mathrm{END}(F)$ is integrally closed in its field of fractions.*

PROOF: As fract$(\mathrm{END}(F))$ is contained in the unramified extension K_h of K of degree h by Proposition 5.1.1, then it suffices to prove: if c is any unit in the ring of integers C of K_h for which $[c]_F(x) \notin \mathrm{END}(F)$, then $[c\pi]_F(x) \notin \mathrm{END}(F)$ (for then $\mathrm{END}(F)$ will be a complete discrete valuation ring, and hence integrally closed).

Let $[c]_F(x) = \sum_{k=1}^{\infty} c_k x^k$ and $[\pi]_F(x) = \sum_{k=1}^{\infty} b_k x^k$. As L is unramified over K, Theorem 4.2.1 allows us to assume that $F(X, Y)$ is linear mod deg q^h. Therefore, $[c]_F(x)$ and $[\pi]_F(x)$ are linear mod deg q^h also.

Assume that the first non-integral coefficient of $[c]_F(x)$ occurs in degree n. We will show that the coefficient d_{nq^h} of the $(nq^h)^{\text{th}}$ term of $[c]_F \circ [\pi]_F(x) = [c\pi]_F(x)$ is non-integral. Computation yields

$$\begin{aligned} d_{nq^h} = {} & c_n(b_{q^h})^n + c_{n+q^h-1}(b_{q^h})^{n-1}\pi^{q^h} + c_{n+2(q^h-1)}(b_{q^h})^{n-2}\pi^{2q^h} + \cdots \\ & + c_{n+j(q^h-1)}(b_{q^h})^{n-j}\pi^{jq^h} + \cdots + c_{nq^h}\pi^{nq^h} \\ & + (\text{assorted } C\text{-integral terms involving the } c_i \text{ for } 1 \leqq i < n). \end{aligned}$$

Application of Lemma 5.2.1 yields that $c_{n+j(q^h-1)}(b_{q^h})^{n-j}\pi^{jq^h}$ is C-integral for $1 \leqq j \leqq n$. As $b_{q^h} \in B^*$, then $c_n(b_{q^h})^n$ is *not* C-integral and hence neither is d_{nq^h}. Therefore, $[c\pi]_F(x) \notin \mathrm{END}(F)$ and so $\mathrm{END}(F)$ is integrally closed. Q.E.D.

On the other hand, every p-adic integer ring C is an $\mathrm{END}(F)$ for a variety of non-isomorphic F's.

THEOREM 5.2.2: *Let K_s be the unramified extension of K of degree s and let C denote the ring of integers of K_S. Then for each integer $r > 0$ there exists a formal A-module $F_r(X, Y)$* defined over A *for which*

(i) *the A-module height of F_r equals rs*
(ii) *$END(F_r) \cong C$.*

PROOF: Given $r > 0$, as

$$R(X, Y) = X + Y + \frac{1}{\pi} B_{q^{rs}}(X, Y)$$

behaves mod deg $(q^{rs}+1)$ like a formal A-module defined over A, extend $R(X, Y)$ to a formal A-module $F_r(X, Y) \in B[[X, Y]]_{q^s}$ for which

(i) $R(X, Y) \equiv F_r(X, Y)$ mod deg $(q^{rs}+1)$ and
(ii) the $(q^{(r+1)s})^{\text{th}}$ degree form of $F_r(X, Y)$ equals

$$\frac{1}{\pi} B_{q^{(r+1)s}}(X, Y).$$

Let $f(x)$ denote the logarithm of $F_r(X, Y)$. Then

$$f(x) \equiv x - \frac{1}{\pi} x^{q^{rs}} \text{ mod deg } (q^{rs}+1)$$

and hence

$$[\pi]_{F_r}(x) \equiv (\pi^{q^{rs-1}} - 1)x^{q^{rs}} \text{ mod deg } (q^{rs}+1), \text{ mod } \pi.$$

Therefore, the height of F_r equals *rs*.

As $F_r(X, Y) \equiv R(X, Y)$ mod deg $(q^{rs}+1)$, then END(F_r) is integrally closed by Theorem 5.2.1.

As, for each primitive $(q^s-1)^{st}$ root of unity $w \in C$, we have that $[w]_{F_r}(x) = wx$, then END(F_r) contains all roots of unity in C. If $[w']_{F_r}(x) \in$ END(F_r) for some primitive $(q^{s'}-1)^{st}$ root of unity w' and some multiple s' of s, then $F_r(X, Y)$ would be $A[w']$-isomorphic to a formal A-module $F'_r(X, Y) \in A[w'][[X, Y]]_{q^{s'}}$. But, the simultaneous presence of the $B_{q^{rs}}$ and $B_{q^{(r+1)s}}$ terms in $F_r(X, Y)$ makes this impossible unless $s' = s$. So, the only roots of unity in END(F_r) are those in C. Therefore, as END(F_r) is unramified over A, then END$(F_r) \cong C$.

Q.E.D.

COROLLARY: *For every positive integer h there exists a formal A-module $F_h(X, Y)$* defined over A *such that*

(i) *the height of F_h equals h and*
(ii) *$END(F_h) \cong A$.*

Comment

Theorems of the preceding type should bear fruit in the form of applications to number theory. Perhaps the non-Abelian extensions of K can be obtained and classified from finite height formal A-modules just as the Abelian extensions of K were constructed from the height one formal A-modules over A (cf. (10)). This would involve knowledge of $END(F)$, the construction of which (in the unramified case) follows from Theorem 3.3.1.

REFERENCES

[1] L. Cox: Formal A-Modules. *Bull. Amer. Math. Soc., 79* (1973) 620–624.
[2] A. Frohlich: Formal Groups. *Lecture Notes in Math. 74*. Springer-Verlag, New York, 1968.
[3] W. Hill: Formal Groups and Zeta-Functions of Elliptic Curves. *Inv. Math., 12* (1971) 321–336.
[4] T. Honda: Formal Groups and Zeta-Functions. *Osaka Jour. Math., 5* (1968) 199–213.
[5] T. Honda: On the Theory of Commutative Formal Groups. *Journ. Math. Soc. Japan, 22* (1970) 213–246.
[6] M. Lazard: La Non-Existence des Groupes de Lie Formels Non-Abéliens à un Paramètre. *C. R. Acad. Sci. Paris, 239* (1954) 942–945.
[7] M. Lazard: Sur les groupes de Lie Formels à un Paramètre. *Bull. Soc. Math. France, 83* (1955) 251–274.
[8] J. Lubin: One-Parameter Formal Lie Groups over p-adic Integer Rings. *Annals Math., 80* (1964) 464–484.
[9] J. Lubin: Formal A-Modules Defined over A. Instituto Nazionale di Alta Matematica. *Symposia Mathematica 3* (1970) 241–245.
[10] J. Lubin and J. Tate: Formal Complex Multiplication in Local Fields. *Annals of Math.*, 81 (1965) 380–387.
[11] W. Waterhouse: On p-divisible Groups over Complete Valuation Rings. *Annals of Math., 95* (1972) 55–65.

(Oblatum 7–V–1974)

Brown University
Providence, R.I. 02912

Current Address:
Statistical Research Division
Census Bureau
Suitland, Maryland, USA.