BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 4, July 1973

FORMAL A-MODULES[1]

BY LAWRENCE COX

Communicated by M. Artin, December 26, 1972

1. **Introduction.** In this announcement, we present results obtained in an investigation of *one-parameter formal A-modules* defined over a p-adic integer ring B. The formal modules were introduced into the literature by Lubin and Tate in [**6**] wherein the formal modules of height one and their endomorphisms were used to describe the maximal Abelian extension and the Artin symbol of an arbitrary local field. Since then, they have gone virtually unnoticed, except for [**5**]. Aside from adding enrichment to the theory of formal groups in general, it is believed that a study of the formal modules will bear fruit in the form of applications to number theory, in the spirit of [**6**]. I wish to acknowledge my gratitude to Professor Jonathan Lubin for his insights and suggestions in the development and presentation of this work.

2. **Formal groups and modules.** Throughout this paper, Z_p will denote the ring of p-adic integers; A and B will be fixed (integrally closed) complete p-adic integer rings with $Z_p \subseteq A \subseteq B$. Let k be the residue class field of A and assume that k contains q elements. A (one-parameter) *formal group law* $F(X, Y)$ defined over B is a formal power series $F(X, Y) \in B[[X, Y]]$ for which (i) $F(X, 0) = X$, and (ii) $F(F(X, Y), Z) = F(X, F(Y, Z))$. As B contains no nilpotent elements, it results that (iii) $F(X, Y) = F(Y, X)$. If $G(X, Y)$ is another formal group law defined over B, then a *B-homomorphism* $t(x)$ *from F to G* is a power series $t(x) \in B[[X]]$ without constant term such that $t(F(X, Y)) = G(t(X), t(Y))$. If $t(x)$ is invertible as a power series, we say $t(x)$ is a *B-isomorphism*; and if $t(x) \equiv x \bmod \deg 2$, we say $t(x)$ is a *strong B-isomorphism*. It results (cf. [**4**]) that under F-addition and composition of power series, End(F), the set of all B-endomorphisms of $F(X, Y)$, becomes a complete topological ring for which $Z_p \subseteq \text{End}(F) \subseteq B$.

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

Let L and K be the fields of fractions of A and B, respectively, let B^* denote the multiplicative group of units of B, and let π be a fixed prime element of A. It results that $[p]_F(x)^*$, the reduction of $[p]_F(x)$ to the residue class field of B, is either equal to the zero power series or else is a power series in x^{p^H} whose first nonzero coefficient occurs in degree p^H, for

AMS (*MOS*) *subject classifications* (1970). Primary 14L05; Secondary 14G20.

[1] This research was supported by NSF Grant No. GP-29082 (A2).

some positive integer H. In the latter case, the *formal group height* of $F(X, Y)$ is defined to be H; otherwise, we say F is of infinite height (cf. [**3**]). We first prove that if $F(X, Y)$ is a formal A-module of finite (formal group) height H defined over B, then $[\pi]_F(x)^*$ is a power series in x^{q^h} whose first nonzero coefficient occurs in degree q^h, where $h = H/n$ and $n = [L:Q_p]$. Accordingly, we define the *A-module height* (henceforth simply the *height*) of $F(X, Y)$ to be h in this case, and infinity otherwise. It results that much information about $F(X, Y)$ can be related in terms of the height of F.

One of the most important results of Lazard [**3**] was that, given a formal group law $F(X, Y)$ defined over a Q-algebra R, there exists a unique strong R-isomorphism $f(x)$ from $F(X, Y)$ to the additive group law $X + Y$. In our setting, $R = K$ and we call $f(x)$ the *logarithm* of $F(X, Y)$. Our approach in this investigation was to obtain various results concerning $f(x)$ and its relationship to the height h of F and to bring this information to bear upon questions relating to $F(X, Y)$. In particular, under the assumption that K is unramified over L, we obtain a complete classification of the strong B-isomorphism classes of formal A-modules $F(X, Y)$ of finite height h defined over B. Moreover, in so doing, we obtain an explicit means of constructing *all* one-parameter formal A-modules defined over B.

3. **Isomorphism classes.** Throughout this section, we assume that K is unramified over L. We make use of the results of Honda (cf. [**2**]) on the so-called "Hilbert power series". The set-up is as follows: Let σ denote the Frobenius L-automorphism of K (i.e. the unique L-automorphism of K for which $b^\sigma \equiv b^q \bmod \pi$ for all $b \in B$). Let $B_\sigma[[T]]$ denote the noncommutative (Hilbert) power series ring defined over B with respect to the multiplication rule: $Tb = b^\sigma T$ for all $b \in B$. Let $B_\sigma[[T]]$ operate on $K[[x]]_0$, the subring of $K[[x]]$ consisting of all power series $r(x)$ with zero constant term, via $u(T) * r(x) = \sum_{m=0}^{\infty} C_m r^{\sigma^m}(x^{q^m})$ for $u(T) = \sum_{m=0}^{\infty} C_m T^m \in B_\sigma[[T]]$ and where $r^\sigma(x)$ is the power series obtained from $r(x)$ by applying σ to each of the coefficients of $r(x)$. Call an element $u(T)$ of $B_\sigma[[T]]$ *special* if $u(T) \equiv \pi \bmod \deg 1$. If $r(x) \in K[[x]]_0$ with $r(x) \equiv x \bmod \deg 2$, we say $r(x)$ *is of type u* if $u(T) * r(x) \equiv 0 \bmod \pi$. We then prove that for each formal A-module $F(X, Y)$ defined over B there exists a special element $u(T)$ such that the logarithm $f(x)$ of $F(X, Y)$ is of type u. This fact, together with some theorems of Honda regarding the structure of $B_\sigma[[T]]$ and an integrality lemma (Lemma 2.3 of [**2**]), enables us to prove

THEOREM 1. *Assume K is unramified over L. Then, there is a one-to-one correspondence between the strong B-isomorphism classes of formal A-*

modules $F(X, Y)$ of finite height h defined over B and special elements $u(T)$ in $B_\sigma[[T]]$ of the form $u(T) = b_0 + b_1T + \cdots + b_hT^h$ with $\pi = b_0, b_1, \ldots, b_{h-1} \equiv 0 \bmod \pi$ while $b_h \in B^*$. Moreover, if $F(X, Y)$ and $u(T)$, $G(X, Y)$ and $v(T)$ so correspond, then $F(X, Y)$ is B-isomorphic to $G(X, Y)$ if and only if there exists some $b \in B^*$ such that $vb = bu$.

For the case of formal Z_p-modules defined over an unramified extension B of Z_p, the preceding theorem is precisely Proposition 3.5 of [**2**].

Similar techniques yield the following result concerning $\mathrm{Hom}(F, G)$, the set of all B-homomorphisms from the formal A-module $F(X, Y)$ to the formal A-module $G(X, Y)$:

COROLLARY. *Assume K is unramified over L. Let $F(X, Y)$ and $u(T)$, $G(X, Y)$ and $v(T)$ correspond as in the statement of Theorem 1. Then, $\mathrm{Hom}(F, G)$ is isomorphic as an A-module to the set of all $b \in B$ for which $vb = bu$.*

Perhaps of even greater interest than Theorem 1 itself is the following construction: Given any special element $u(T)$ as in Theorem 1, letting $w(T)$ denote the reciprocal of $u(T)$ in $K_\sigma[[T]]$, application of the techniques of Honda [**2**] yields that $f(x) = (\pi w(T)) * (x)$ is the logarithm of a formal group law $F(X, Y) = f^{-1}(f(X) + f(Y))$ of formal group height over B equal to hn. Moreover, further analysis yields that $F(X, Y)$ is actually a formal A-module (of height h) defined over B. Thus, we have discovered an explicit means of constructing *all* one-parameter formal A-modules defined over B.

When $A = B$, an alternative description of the strong isomorphism classes was obtained.

PROPOSITION. *Let $F(X, Y)$ be a formal A-module of finite height h defined over A and let $u(T) = b_0 + b_1T + \cdots + b_hT^h$ be the special element corresponding to $F(X, Y)$ as per Theorem 1. Then the minimal polynomial over A of the Frobenius endomorphism x^q of the reduction of $F(X, Y)$ to k is $P(X) = c_0 + c_1X + \cdots + X^h$, where $c_i = b_h^{-1}b_i$ for all $i = 0, 1, \ldots, h-1$.*

This generalizes a result of W. Hill [**1**] who parametrized the strong isomorphism class of $F(X, Y)$ by $P(X)$ for the case of formal group laws $F(X, Y)$ defined over Z_p. In addition, the Proposition exhibits explicitly the relationship between Hill's parameters and those of Honda and gives an interpretation of the special elements as liftings of analytic equations satisfied in k by the Frobenius.

We conjecture that the Proposition is true in greater generality: If K is unramified over L, then the coefficients of the minimal polynomial over B of the Frobenius endomorphism of the reduction of $F(X, Y)$ to the residue class field of B form a system of parameters for the (strong) isomorphism class over B of $F(X, Y)$.

4. **The structure theorems and constructions.** In this section, we ask and answer certain natural questions about power series $F(X, Y)$ which are formal A-modules and note the structural differences between $F(X, Y)$ and arbitrary formal group laws over B. Unless otherwise stated, we no longer assume that K is unramified over L.

If $F(X, Y)$ and $G(X, Y)$ are two formal group laws defined over B for which $F(X, Y) \equiv G(X, Y) \bmod \deg n$ for some n, the work of Lazard [**3**] yields that: $F(X, Y) \equiv G(X, Y) + bB_n(X, Y) \bmod \deg(n + 1)$, where $B_n(X, Y) = (X + Y)^n - (X^n + Y^n)$ and where $b \in K$ satisfies: $b \in B$ if n is not a power of p; and $pb \in B$ if n is a power of p. If we assume that F and G are formal A-modules defined over B, then the conditions on $b \in K$ become more restrictive.

THEOREM 2. *With notation and assumptions as above, $b \in B$ if n is not a power of q; and $\pi b \in B$ if n is a power of q. Moreover, if $F(X, Y)$ is of finite height h and if we further assume that K is unramified over L, then $F(X, Y)$ is strongly B-isomorphic to a formal A-module $H(X, Y)$ for which $H(X, Y) \equiv X + Y + cB_{q^h}(X, Y) \bmod \deg(q^h + 1)$ and where $c \notin B$ but $\pi c \in B$.*

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

The proof of Theorem 2 is rather computational and relies upon an analysis of the structure of the logarithm $f(x)$ of $F(X, Y)$.

Another important question in the study of formal group laws is that of the extendibility of an arbitrary polynomial $R(X, Y)$ of degree $(n - 1)$ to a formal group law $F(X, Y)$ defined over B: Given $R(X, Y)$, does there exist a formal group law $F(X, Y)$ such that $F(X, Y) \equiv R(X, Y) \bmod \deg n$? Lazard [**3**] showed that the answer is affirmative if $R(X, Y)$ is *associative* mod deg n, i.e., $R(R(X, Y), Z) \equiv R(X, R(Y, Z)) \bmod \deg n$. If $R(X, Y)$ is a power series with coefficients in B which is associative mod deg n, then it makes sense to speak of solutions $[a]_R(x)$ of the congruences $[a]_R(R(X, Y)) \equiv R([a]_R(X), [a]_R(Y)) \bmod \deg n$ for $a \in A$ which satisfy $[a]_R(x) \equiv ax \bmod \deg 2$. If, for each $a \in A$, there exists one such solution $[a]_R(x)$ which has its coefficients in degrees less than n ın B, and if $R(X, Y)$ is associative mod deg n, then we say that $R(X, Y)$ *behaves as a formal A-module defined over B* mod deg n. By a reduction to the case when $R(X, Y)$ has all of its nonzero coefficients only in degrees congruent to 1 modulo $(q - 1)$ and by a suitable choice of the nth degree coefficient of $[\pi]_R(x)$, we obtain:

THEOREM 3. *Let $R(X, Y) \in B[[X, Y]]$ behave as a formal A-module defined over B* mod deg n. *Then there exists a formal A-module $F(X, Y)$*

defined over B such that: $F(X, Y) \equiv R(X, Y) \bmod \deg n$.

The final result deals with the *absolute* endomorphism ring of a formal A-module $F(X, Y)$. Following Lubin [**4**], we define the *absolute endomorphism ring* END(F) of $F(X, Y)$ to be the ring consisting of all endomorphisms of $F(X, Y)$ which are defined over the ring of integers of some finite extension of K. Then END(F) is contained in the ring of integers of the field M, where M is the compositum of all field extensions of L of degree dividing h (cf. [**4**]). We then construct formal A-modules defined over A whose absolute endomorphism rings are minimal:

THEOREM 4. *For every positive integer h, there exists a formal A-module* $F(X, Y)$ *defined over A for which* (i) *the height of F equals h and* (ii) END(F) $= A$.

Detailed proofs and related results will appear elsewhere.

REFERENCES

1. W. Hill, *Formal groups and zeta functions of elliptic curves*, Invent. Math. **12** (1971), 321–336.

2. T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246. MR **41** #212.

3. M. Lazard, *Sur les groupes de Lie formels a un parametre*, Bull. Math. France **83** (1955), 251–274. MR **17**, 508.

4. J. Lubin, *One-parameter formal Lie groups over p-adic integer rings*, Ann. of Math. (2) **80** (1964), 464–484. MR **29** #5827.

5. ———, *Formal A-modules defined over A*, Symposia Matematica (INDAM, Rome, 1968/69) **3** (1970), 241–245. MR **42** #260.

6. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387. MR **30** #3094.

DEPARTMENT OF MATHEMATICS, BROWN UNIVERSITY, PROVIDENCE, RHODE ISLAND 02912