TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 286, Number 2, December 1984

FINITE SUBGROUPS OF FORMAL A-MODULES OVER $\mathfrak{p}$-ADIC INTEGER RINGS

BY
TETSUO NAKAMURA

ABSTRACT. Let $B \supset A$ be $\mathfrak{p}$-adic integer rings such that A/Z_p is finite and B/A is unramified. Generalizing a result of Fontaine on finite commutative p-group schemes, we show that galois homomorphisms of finite subgroups of one-dimensional formal A-modules over B are given by power series.

Introduction. Let K be a finite extension of the rational p-adic number field Q_p, and A the integer ring of K. Let L be a complete unramified extension of K, B the ring of integers of L, and $\mathfrak{p}$ the maximal ideal of B. We write $\bar{\mathfrak{p}}$ for the maximal ideal of the integer ring of the algebraic closure $\bar{L}$ of L. Let F denote an n-dimensional formal A-module defined over B of finite A-height. Then F induces an A-module structure on $\bar{\mathfrak{p}}^n$, which we denote by $F(\bar{\mathfrak{p}})$; it is an $A[\mathfrak{G}]$-module, where $\mathfrak{G} = \mathrm{Gal}(\bar{L}/L)$. Let P be a finite sub-$A[\mathfrak{G}]$-module of $F(\bar{\mathfrak{p}})$ (henceforth, simply of F). In this paper, we attach to P a couple $ML(P)$ of modules over a noncommutative power series ring. Let G be another formal A-module over B of finite A-height and Q be a finite sub-$A[\mathfrak{G}]$-module of G. Then we describe the $A[\mathfrak{G}]$-homomorphisms from P to Q by morphisms from $ML(Q)$ to $ML(P)$ (Theorem 1). If $A = Z_p$ (the p-adic integer ring), this result follows from Fontaine [**4**], but our proof depends rather on Tate modules of formal groups. Furthermore, if F and G are one-dimensional, we can show that every $A[\mathfrak{G}]$-homomorphism from P to Q is of the form $g^{-1} \circ cf$ for some $c \in B$, where f and g are the logarithms of F and G, respectively (Theorem 3). In [**8**], Lubin has obtained a rather weaker version of this result.

In the following, let K, A, L, B, $\mathfrak{p}$, $\bar{\mathfrak{p}}$ and $\mathfrak{G}$ be as above. We write π for a fixed prime element of A and q for the cadinality of the residue field of A. Let σ denote the Frobenius automorphism of L/K. We write $E = B_\sigma[[T]]$ for the ring of noncommutative power series ring over B in a variable T with respect to the multiplication rule: $Tb = b^\sigma T$ for all $b \in B$. Call $F^A(B)$ the category of finite-dimensional formal A-modules over B of finite A-height.

I would like to thank the referee for calling my attention to Lubin [**8**].

1. Homomorphisms of finite subgroups of formal A-modules. We write $T(F)$ for the Tate module of a formal A-module F. $T(F)$ is an $A[\mathfrak{G}]$-module, A-free of rank h (= A-height of F). Let DH' be the category defined in Decauwert [**2**]. Let $M(F)$ and $L(F)$ be as in [**2**]; $M(F)$ is an E-module, B-free of rank h and

Received by the editors February 15, 1983.
1980 *Mathematics Subject Classification*. Primary 14L05.
Key words and phrases. Formal module (group), Tate module, special element, logarithm of formal group.

$L(F)$ is a sub-B-module of $M(F)$. The functor $ML(F) = (M(F), L(F))$ induces an antiequivalence between $F^A(B)$ and DH' [**2**, Théorème 2].

Let $\alpha\colon F \to G$ be a morphism in $F^A(B)$. We also write α for the homomorphism $T(F) \to T(G)$ induced by α. We write $\tilde{\alpha}$ for the morphism $ML(G) \to ML(F)$ induced by α.

LEMMA 1. *Let F, G and H be objects of $F^A(B)$. Let $\alpha\colon F \to H$ and $\beta\colon H \to G$ be homomorphisms over B. Then $0 \to T(F) \xrightarrow{\alpha} T(H) \xrightarrow{\beta} T(G) \to 0$ is exact if and only if $0 \to ML(G) \xrightarrow{\tilde{\beta}} ML(H) \xrightarrow{\tilde{\alpha}} ML(F) \to 0$ is exact.*

SKETCH OF PROOF. For a morphism s in DH', we see that $\operatorname{Ker} s$ and $\operatorname{Im} s$ are in DH'. The "if" part follows easily from this. By Fontaine [**5**, Chapter V, §2] we can express $ML(F)$ by means of special elements. Choosing an appropriate special element of H, we can prove the "only if" part (cf. also Honda [**6**]).

Now let $F \in F^A(B)$, and let P be a finite sub-$A[\mathfrak{G}]$-module of F. Denote by S the superlattice of $T(F)$ in $T(F) \otimes_A K$ such that $S/T(F) \cong P$. Then by Waterhouse [**10**, Theorem 1.3] there exists an isogeny $\nu\colon F \to F'$ defined over B such that $S = \nu^{-1}T(F')$. As S is an $A[\mathfrak{G}]$-module, we see that $F' \in F^A(B)$. Define $ML(P) = (M(P), L(P))$, where $M(P) = M(F)/\tilde{\nu}M(F')$ and $L(P) = L(F)/\tilde{\nu}L(F')$. Then $M(P)$ is an E-module and $L(P)$ is a sub-B-module of $M(P)$. Let M, M' be left E-modules and N, N' be sub-B-modules of M and M', respectively. By $\operatorname{Hom}_E((M, N), (M', N'))$ we denote the set of E-linear maps $\delta\colon M \to M'$ such that $\delta(N) \subset N'$. Then clearly P determines $ML(P)$ up to an E-isomorphism.

THEOREM 1. *Let $F, G \in F^A(B)$. Let P and Q be finite sub-$A[\mathfrak{G}]$-modules of F and G, respectively. Then $\operatorname{Hom}_{A[\mathfrak{G}]}(P, Q)$ is A-isomorphic to*

$$\operatorname{Hom}_E(ML(Q), ML(P)).$$

SKETCH OF PROOF. We refer to the method used in Oort [**9**]. Let $\alpha\colon F \to F'$ and $\beta\colon G \to G'$ be isogenies over B such that $\operatorname{Ker}\alpha = P$ and $\ker\beta = Q$. Write $T_1 = T(F)$, $T_2 = T(G)$, $M_1 = ML(F)$ and $M_2 = ML(G)$; let T_1', T_2', M_1', M_2' be similarly defined for F' and G'. We note that $P \cong T_1'/\alpha(T_1)$ and $Q \cong T_2'/\beta(T_2)$. Let $\eta \in \operatorname{Hom}_{A[\mathfrak{G}]}(P, Q)$ and $\Gamma(\eta)$ be the superlattice of $\alpha(T_1) \times \beta(T_2)$ in $T_1' \times T_2'$ such that $\Gamma(\eta)/\alpha(T_1) \times \beta(T_2)$ is the graph of η. We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc}
0 \to T_2 & \xrightarrow{i} & T_1 \times T_2 & \xrightarrow{j} & T_1 & \to & 0 \\
\| & & \downarrow \varepsilon & & \downarrow \alpha & & \\
0 \to T_2 & \to & \Gamma(\eta) & \to & T_1' & \to & 0 \\
\downarrow \beta & & \downarrow & & \| & & \\
0 \to T_2' & \xrightarrow{i'} & T_1' \times T_2' & \xrightarrow{j'} & T_1' & \to & 0
\end{array}$$

where i, i' are the canonical injections, j, j' the canonical projections and ε the composite map $T_1 \times T_2 \xrightarrow{\alpha\times\beta} \alpha(T_1) \times \beta(T_2) \hookrightarrow \Gamma$. Then the functor ML gives the following commutative diagram, whose rows are exact by Lemma 1:

$$\begin{array}{ccccccccc} 0 & \to & M_1' & \to & M_1' \times M_2' & \to & M_2' & \to & 0 \\ & & \| & & \downarrow & & \downarrow \tilde{\beta} & & \\ 0 & \to & M_1' & \to & ML(H) & \to & M_2 & \to & 0 \\ & & \downarrow \tilde{\alpha} & & \downarrow & & \| & & \\ 0 & \to & M_1 & \to & M_1 \times M_2 & \to & M_2 & \to & 0 \end{array}$$

where $H \in F^A(B)$ is such that $T(H) \cong \Gamma(\eta)$ (cf. [**10**]). By the above diagram we have a morphism $ML(Q) = M_2/\tilde{\beta}M_2' \to ML(P) = M_1/\tilde{\alpha}M_1'$, which does not depend on the choice of H; we denote it by $\theta(\eta)$. By construction we see easily that $\theta\colon \mathrm{Hom}_{A[\mathfrak{G}]}(P,Q) \to \mathrm{Hom}_E(ML(Q), ML(P))$ is a bijection. Let $\eta_1, \eta_2 \in \mathrm{Hom}_{A[\mathfrak{G}]}(P,Q)$. As the exact sequence $0 \to T_2 \to \Gamma(\eta_1+\eta_2) \to T_1' \to 0$ is the Baer sum of the extensions $0 \to T_2 \to \Gamma(\eta_i) - T_1' \to 0$ $(i = 1,2)$, we see that θ is a homomorphism using the functor ML. Clearly θ is an A-isomorphism.

2. One-dimensional formal A-modules. Let v be the valuation of $\overline{L}$ which is normalized so that $v(\pi) = 1$. Here we assume that all formal A-modules are one-dimensional. Let $u = \pi + \sum_{\nu=1}^{\infty} b_\nu T^\nu$ be a special element in E. We write $(u^{-1}\pi)^*(x)$ for the element $f(x)$ of $L[[x]]$ such that $f(0) = 0$ and $\pi x = \pi f(x) + \sum_{\nu=1}^{\infty} b_\nu f^{\sigma^\nu}(x^{q^\nu})$. Then $F(x,y) = f^{-1}(f(x)+f(y))$ is a formal A-module over B. This shows that the strong isomorphism classes of formal A-modules over B, of A-height h, correspond bijectively to the special elements of the form $\pi + \sum_{\nu=1}^{h} b_\nu T^\nu$, where $b_1, \ldots, b_{h-1} \in \mathfrak{p}$ but b_h is a unit of B (cf. Cox [**1**]). Let F be a formal A-module of A-height h defined over B. We write $\Lambda_{F,m} = \mathrm{Ker}[\pi^m]_F = \{x \in \overline{\mathfrak{p}} \mid [\pi^m]_F(x) = 0\}$ for $m \geq 0$, which is a finite subgroup of order q^{hm} in $F(\overline{\mathfrak{p}})$.

THEOREM 2. *Let $u_1 = \pi + \sum_{i=1}^{h} b_i T^i$ and $u_2 = \pi + \sum_{i=1}^{h} c_i T^i$ be special elements of E such that $b_i, c_i \in \mathfrak{p}$ $(1 \leq i \leq h-1)$ and b_h, c_h are units of B. Let $f_1(x) = (u_1^{-1}\pi)^*(x) = \sum_{n=0}^{\infty} a_n x^{q^n}$, $f_2(x) = (u_2^{-1}\pi)^*(x) = \sum_{n=0}^{\infty} a_n' x^{q^n}$ and $\psi = f_2^{-1} \circ f_1$. Let m be an integer such that $u_1 \equiv u_2 \bmod \mathfrak{p}^m$ but $u_1 \not\equiv u_2 \bmod \mathfrak{p}^{m+1}$. Put $w_i = (b_i - c_i)/\pi^m$ for $1 \leq i \leq h$ and let e $(1 \leq e \leq h)$ be such that $w_i \in \mathfrak{p}$ for $1 \leq i \leq e-1$ and w_e is a unit. Then the convergence domain of ψ contains $\{x \in \overline{\mathfrak{p}} \mid v(x) > q^{-e} r^{-m+1}(r-1)^{-1}\}$, where $r = q^h$.*

For the proof of Theorem 2 we need the following

LEMMA 2. *Assume the same hypothesis as in Theorem 2, and put $A_n = a_n - a_n'$. Then we have $v(A_n) \geq (m-1) - [(n-e)/h]$ for $n \geq 0$, where $[\alpha]$ denotes the largest integer not exceeding α.*

PROOF. We proceed by induction on n. First we note that $v(a_t') \geq -[t/h]$ by [**1**, Proposition 4.1.1]. By the definition of f_1 and f_2 we can show that

$$A_n = -\sum_{i=1}^{h} \pi^{-1} b_i A_{n-i}^{\sigma^i} - \pi^{m-1} \sum_{i=1}^{h} w_i a_{n-i}'^{\sigma^i}.$$

Then it is clear that $v(A_n) \geq m$ for $0 \leq n \leq e$. Hence we may assume that the assertion of our lemma holds for n' with $n' < n = h(j-1) + e + k$, where $0 \leq k < h$

and $j \geq 1$. We have $v(\pi^{-1}b_i A_{n-i}) \geq m-1-[(n-i-e)/h] \geq m-j$ for $1 \leq i \leq h-1$ and $v(\pi^{-1}b_h A_{n-h}) \geq m-j$. Noting $e+k<2h$, we have

$$v(\pi^{m-1}w_i a_{n-i}'^{\sigma^i}) \geq m-1-[(n-h)/h] = m-j-[(e+k-h)/h] \geq m-j.$$

Therefore $v(A_n) \geq m-j = (m-1)-[(n-e)/h]$. This completes our proof by induction.

PROOF OF THEOREM 2. We can write $\psi(x) = \sum_{n=0}^{\infty} \alpha_n x^{n(q-1)+1}$ with $\alpha_n \in L$ by Lubin [7, p. 475]. Let ξ be an element of $\bar{\mathfrak{p}}$ such that $\xi^{q^e r^{m-1}(r-1)} = \pi$. Put $\beta_n = \alpha_n \xi^{n(q-1)+1}$. By induction on n we shall show that $v(\beta_n) \geq 1/(r-1)$. Let R be the set whose points are sequences $\mathfrak{n} = (n_0, n_1, n_2, \ldots)$, where n_i are nonnegative integers for all i and $n_i = 0$ for almost all i. For $\mathfrak{n} \in R$, define $|\mathfrak{n}| = \sum_{k=0}^{\infty} n_k$, $\mathfrak{n}^* = \sum_{k=0}^{\infty} kn_k$ and $C(\mathfrak{n}) = |\mathfrak{n}|!/(\prod_{k=0}^{\infty}(n_k!))$. They are rational integers. We define an element $\alpha^{\mathfrak{n}}$ of L to be $\prod_{k=0}^{\infty} \alpha_k^{n_k}$. Put $Q_s = (q^s-1)/(q-1)$. Let t be an integer such that $Q_t < N+1 \leq Q_{t+1}$. On comparing the coefficients of $x^{(N+1)(q-1)+1}$, we get by the equation $f_2(\psi(x)) = f_1(x)$ that

$$(*) \qquad \alpha_{N+1} + \sum_{k=1}^{t} a_k' \left(\sum_k C(\mathfrak{n})\alpha^{\mathfrak{n}} \right) = \begin{cases} 0 & \text{if } N+1 < Q_{t+1}, \\ A_{t+1} & \text{if } N+1 = Q_{t+1}, \end{cases}$$

where the sum $\sum_k$ is taken over all $\mathfrak{n} \in R$ such that $|\mathfrak{n}| = q^k$ and $\mathfrak{n}^* = N+1-Q_k$. We have easily by Lemma 2 that $v(A_1) \geq m-1$ if $e=1$ and $v(A_1) \geq m$ if $e>1$. Then

$$v(\beta_1) = v(\xi^q \alpha_1) \geq q^{1-e}r^{1-m}(r-1)^{-1} + v(A_1) \geq 1/(r-1).$$

Therefore by induction hypothesis we assume that $v(\beta_n) \geq 1/(r-1)$ for $1 \leq n \leq N$. For $\mathfrak{n} = (n_0, n_1, n_2, \ldots) \in R$ with $|\mathfrak{n}| = q^k$ $(k \geq 1)$ and $\mathfrak{n}^* = N+1-Q_k$, let

$$D_{k,\mathfrak{n}}^{N+1} = \xi^{(N+1)(q-1)+1} a_k' C(\mathfrak{n})\alpha^{\mathfrak{n}} = a_k' C(\mathfrak{n})\xi^{n_0} \prod_{k=1}^{\infty} \beta_k^{n_k}.$$

Now let $g(x) = r^x(r-1)^{-1} - x$; it is clear that $g(n) \geq 1/(r-1)$ for all integers n and $g(n) = 1/(r-1)$ if and only if $n=0$ or $n=1$. Now if $n_0 = 0$, then

$$v(D_{k,\mathfrak{n}}^{N+1}) \geq v(a_k') + v(C(\mathfrak{n})) + q^k/(r-1) \geq g([k/h]) \geq 1/(r-1).$$

If $n_0 \neq 0$, then $0 < n_0 < q^k$. Writing $q = p^j$, $n_0 = q^s d$ with $q \nmid d$ and $d = p^{j'} d_1$ with $(p, d_1) = 1$, we easily get

$$\operatorname{ord}_p({}_{q^k}C_{n_0}) = j(k-s) - j' \geq k-s.$$

Clearly ${}_{q^k}C_{n_0}$ is a divisor of $C(\mathfrak{n})$ and $q^s \leq q^k - n_0$. Therefore

$$\begin{aligned} v(D_{k,\mathfrak{n}}^{N+1}) &\geq v(a_k') + v(C(\mathfrak{n})) + nq^{-e}r^{1-m}(r-1)^{-1} + (q^k - n_0)(r-1)^{-1} \\ &> -[k/h] + (k-s) + q^s(r-1)^{-1} \geq g([s/h]) \geq (r-1)^{-1}. \end{aligned}$$

Let us now assume $N+1 = Q_{t+1}$. Then, by Lemma 2, we have

$$v(\xi^{(N+1)(q-1)+1} A_{t+1}) \geq g(-(m-1) + [(t+1-e)/h]) \geq (r-1)^{-1}.$$

In view of $(*)$, we have thus established that $v(\beta_{N+1}) \geq 1/(r-1)$; therefore $v(\beta_n) \geq 1/(r-1)$ for all $n \geq 1$. As $\psi(x) = \sum_{n=0}^{\infty} \beta_n (x/\xi)^{n(q-1)+1}$, the proof is completed.

REMARK. By further computations we can show that $v(\beta_{Q_{hs+e}}) = 1/(r-1)$ for $s \geq m$. Therefore the convergence domain of ψ is $\{x \in \bar{\mathfrak{p}} | v(x) > q^{-e}r^{1-m}(r-1)^{-1}\}$.

COROLLARY. *Assumptions and notation being as in Theorem 2, let* $F_i(x,y) = f_i^{-1}(f_i(x)+f_i(y))$ $(i = 1,2)$. *Then* ψ *defines an* $A[\mathfrak{G}]$*-isomorphism* $\Lambda_{F_1,m} \to \Lambda_{F_2,m}$.

As $v(x) \geq r^{1-m}(r-1)^{-1}$ for $x \in A_{F_1,m}$, this is clear.

THEOREM 3. *Let* F *and* G *be one-dimensional formal* A*-modules of the same* A*-height* h *defined over* B *and* f, g *be the logarithms of* F, G, *respectively. Then every element of* $\mathrm{Hom}_{A[\mathfrak{G}]}(\Lambda_{F,m}, \Lambda_{G,m})$ *is of the form* $g^{-1} \circ cf$ *for some* $c \in B$. *If* f *and* g *are of type* $u_1 = \pi + \sum_{i=1}^{h} b_i T^i$ *and* $u_2 = \pi + \sum_{i=1}^{h} c_i T^i$, *respectively (cf.* [**1**, *p.* 295]), *then* $g^{-1} \circ cf \in \mathrm{Hom}_{A[\mathfrak{G}]}(\Lambda_{F,m}, \Lambda_{G,m})$ *for* $c \in B$ *if and only if* $u_2 c \equiv c u_1 \bmod \mathfrak{p}^m$.

PROOF. As $M(F) \cong E/Eu_1$ and $M(\Lambda_{F,m}) \cong E/(Eu_1 + E\pi^m)$, we get easily by Theorem 1 that

$$\mathrm{Hom}_{A[\mathfrak{G}]}(\Lambda_{F,m}, \Lambda_{G,m}) \cong \{c \in B \mid u_2 c \equiv c u_1 \bmod \mathfrak{p}^m\}/\mathfrak{p}^m.$$

Let $c \in B$ be such that $u_2 c \equiv c u_1 \bmod \mathfrak{p}^m$. We assume $v(c) = s \leq m$ and write $c = b\pi^s$ with a unit b in B. Let $u' = bu_1 b^{-1}$. Then u' is special and $u' \equiv u_2 \bmod \mathfrak{p}^{m-s}$. Let $f_1(x) = (u'^{-1}\pi)^*(x)$ and $F_1(x,y) = f_1^{-1}(f_1(x) + f_1(y))$. Then $g^{-1} \circ cf = (g^{-1} \circ f_1)[\pi^s]_{F_1} \circ (f_1^{-1} \circ bf)$, where $f_1^{-1} \circ bf \colon F \to F_1$ is an isomorphism. By the Corollary above, $g^{-1} \circ cf$ defines an element $\eta(c)$ of $\mathrm{Hom}_{A[\mathfrak{G}]}(\Lambda_{F,m}, \Lambda_{G,m})$; clearly $\eta(c) = \eta(c')$ if and only if $c \equiv c' \bmod \mathfrak{p}^m$. Our assertion is now obvious.

REMARK. For a formal A-module F over B of finite A-height h, we have the results which are completely analogous to those in Fontaine [**3**]. Let $\rho\colon \mathfrak{G} \to \mathrm{Aut}_A(T(F))$ $(\cong \mathrm{GL}_h(A))$ be the π-adic representation attached to F. Then by [**3**] we have

(1) $\rho(\mathfrak{G}) \supset A^\times$. Therefore $\mathfrak{G}$-endomorphisms of $\Lambda_{F,m}$ are $A[\mathfrak{G}]$-endomorphisms.

(2) For $h = 1$ or 2, applying our Theorem 3 we can determine the closed subgroup $\rho(\mathfrak{G})$ of $\mathrm{GL}_h(A)$ (up to an isomorphism) by the special element of F.

REFERENCES

1. L. H. Cox, *Formal A-modules over p-adic integer rings*, Compositio Math. **29** (1974), 287–308.
2. J.-M. Decauwert, *Classification des A-modules formels*, C. R. Acad. Sci. Paris **282** (1976), 1413–1416.
3. J.-M. Fontaine, *Points d'ordre fini d'un groupe formel sur une extension non ramifiée de* Z_p, Bull. Soc. Math. France **37** (1974), 75–79.
4. ——, *Groupes finis commutatifs sur les vectuers de Witt*, C. R. Acad. Sci. Paris **280** (1975), 1423–1425.
5. ——, *Groupes p-divisibles sur les corps locaux*, Astérisque 47–48, Soc. Math. de France, 1977.
6. T. Honda, *On the theory of commutative formal groups*, J. Math. Soc. Japan **22** (1970), 213–246.
7. J. Lubin, *One parameter formal Lie groups over* $\mathfrak{p}$*-adic integer rings*, Ann. of Math. (2) **80** (1964), 464–484.
8. ——, *Galois endomorphisms of the torsion subgroup of certain formal groups*, Proc. Amer. Math. Soc. **20** (1969), 229–331.
9. F. Oort, *Dieudonné modules of finite local group schemes*, Nederl. Akad. Wetensch. Proc. Ser. A **77** (1974), 284–292.
10. W. Waterhouse, *On p-divisible groups over complete valuation rings*, Ann. of Math. (2) **95** (1972), 55–65.

DEPARTMENT OF MATHEMATICS, COLLEGE OF GENERAL EDUCATION, TÔHOKU UNIVERSITY, KAWAUCHI, SENDAI 980, JAPAN