ECONOMETRIC INSTITUTE

CONSTRUCTING FORMAL GROUPS VIII: FORMAL A-MODULES

M. HAZEWINKEL

REPRINT SERIES no. 241

This article appeared in "Compositio Mathematica", Vol. 38 (1979).

ERASMUS UNIVERSITY ROTTERDAM,
P.O. BOX 1738, ROTTERDAM, THE NETHERLANDS

COMPOSITIO MATHEMATICA, Vol. 38, Fasc. 3, 1979, pag. 277–291

CONSTRUCTING FORMAL GROUPS. VIII: FORMAL A-MODULES

Michiel Hazewinkel

1. Introduction

Let $\mathbf{Q}_p$ be the p-adic integers, let K be a finite extension of $\mathbf{Q}_p$ and let A be the ring of integers of K. A formal A-module is, grosso modo, a commutative one dimensional formal group which admits A as a ring of endomorphisms. For a more precise definition cf. 2.1 below. For some results concerning formal A-modules cf. [1], [2] and [6].

It is the purpose of the present note to use the techniques of [3] and [5], cf. also [4], to construct a universal formal A-module, a universal A-typical formal A-module and a universal strict isomorphism of A-typical formal A-modules. For the notion of a A-typical formal A-module, cf. 2.6 below. As corollaries one then obtains a number of the results of [1], [2] and [6].

In particular we thus find a new proof that two formal A-modules over A are (strictly) isomorphic iff their reductions over k, the residue field of K, are (strictly) isomorphic.

As a matter of fact the techniques developed below also work in the characteristic $p > 0$ case. Thus we simultaneously obtain the analogues of some of the results of [1], [2], [6] for the case of formal A-modules where A is the ring of integers of a finite extension of $\mathbf{F}_p((t))$, where $\mathbf{F}_p$ is the field of p-elements.

All formal groups will be commutative and one dimensional; $\mathbf{N}$ denotes the set of natural numbers $\{1, 2, 3, \ldots\}$; $\mathbf{Z}$ stands for the integers, $\mathbf{Z}_p$ for the ring of p-adic integers, $\mathbf{Q}$ for the rational numbers and $\mathbf{Q}_p$ the p-adic numbers.

A will always be the ring of integers of a finite extension of $\mathbf{Q}_p$ or $\mathbf{F}_p((t))$, the field of Laurent series over $\mathbf{F}_p$. The quotient field of A is denoted K, π is a uniformizing element of A and $k = A/\pi A$ is the residue field. We use q to denote the number of elements of k.

0010-437X/79/03/0277-15 $00.20/0

2. Definitions, constructions and statement of main results.

2.1. DEFINITIONS. Let $B \in \mathbf{Alg}_A$, the category of A-algebras. A *formal A-module over B* is a formal group law $F(X, Y)$ over B together with a homomorphism of rings ρ_F: $A \to \mathrm{End}_B(F(X, Y))$ such that $\rho_F(a) \equiv aX$ mod(degree 2) for all $a \in A$. We shall also write $[a](X)$ for $\rho_F(a)$.

If B is torsion free (i.e. $B \to B \otimes_{\mathbf{Z}} \mathbf{Q}$ is injective) and $F(X, Y)$ is a formal group over B, then there is at most one formal A-module structure on $F(X, Y)$, viz $\rho_F(a) = f^{-1}(af(X))$ where $f(X)$ is the logarithm of $F(X, Y)$. On the other hand if $\mathrm{char}(K) = p$, then every formal A-module over $B \in \mathbf{Alg}_A$ is isomorphic to the additive formal group $G_a(X, Y) = X + Y$ over B. In this case all the structure sits in the structural morphism $\rho_F : A \to \mathrm{End}_B(F(X, Y))$.

Let $(F(X, Y), \rho_F)$, $(G(X, Y), \rho_G)$ be two formal A-modules over B. A *homomorphism* of formal A-modules over B, $\alpha(X):(F(X, Y), \rho_F) \to (G(X, Y), \rho_G)$ is a power series $\alpha(X) = b_1X + b_2X^2 + \cdots, b_i \in B$ such that $\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y))$, $\alpha([a]_F(X)) = [a]_G(\alpha(X))$; $\alpha(X)$ is an *isomorphism* if b_1 is a unit and α is a *strict isomorphism* if $b_1 = 1$.

2.2. Let R be a ring, $R[U] = R[U_1, U_2, \ldots]$. If $f(X)$ is a power series over $R[U]$ and $n \in \mathbf{N}$ we denote by $f^{(n)}(X)$ the power series obtained from $f(X)$ by replacing each U_i with U_i^n, $i = 1, 2, \ldots$. Let $A[V]$, $A[V; T]$, $A[S]$ denote respectively the rings $A[V_1, V_2, \ldots]$, $A[V_1, V_2, \ldots; T_1, T_2, \ldots]$, $A[S_2, S_3, \ldots]$. Let p be the residue characteristic of A. The three power series $g_V(X)$, $g_{V,T}(X)$, $g_S(X)$ over respectively $K[V]$, $K[V; T]$ and $K[S]$ are defined by the functional equations

$$g_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{\pi} g_V^{(q^i)}(X^{q^i}) \tag{2.2.1}$$

$$g_{V,T}(X) = X + \sum_{i=1}^{\infty} T_i X^{q^i} + \sum_{i=1}^{\infty} \frac{V_i}{\pi} g_{V,T}^{(q^i)}(X^{q^i}) \tag{2.2.2}$$

$$g_S(X) = X + \sum_{\substack{i=2 \\ i \text{ not a} \\ \text{power of } q}}^{\infty} S_i X^i + \sum_{i=1}^{\infty} \frac{S_{q^i}}{\pi} g_S^{(q^i)}(X^{q^i}) \tag{2.2.3}$$

The first few terms are

$$g_V(X) = X + \frac{V_1}{\pi} X^q + \left(\frac{V_1 V_1^q}{\pi^2} + \frac{V_2}{\pi}\right) X^{q^2} + \cdots \tag{2.2.4}$$

$$(2.2.5)\qquad g_{V,T}(X) = X + \left(\frac{V_1}{\pi} + T_1\right)X^q + \left(\frac{V_1V_1^q}{\pi^2} + \frac{V_1T_1^q}{\pi} + \frac{V_2}{\pi} + T_2\right)X^{q^2} + \cdots$$

$$(2.2.6)\qquad g_S(X) = X + S_2X^2 + \cdots + S_{q-1}X^{q-1} + \frac{S_q}{\pi}X^q + S_{q+1}X^{q+1} + \cdots + S_{2q-1}X^{2q-1} + \left(\frac{S_qS_2^q}{\pi} + S_{2q}\right)X^{q^2} + \cdots$$

We now define

$$(2.2.7)\qquad G_V(X, Y) = g_V^{-1}(g_V(X) + g_V(Y))$$

$$(2.2.8)\qquad G_{V,T}(X, Y) = g_{V,T}^{-1}(g_V(X) + g_V(Y))$$

$$(2.2.9)\qquad G_S(X, Y) = g_S^{-1}(g_S(X) + g_S(Y))$$

where if $f(X) = X + r_2X^2 + \cdots$ is a power series over R, then $f^{-1}(X)$ denotes the inverse power series, i.e. $f^{-1}(f(X)) = X = f(f^{-1}(X))$. And for all $a \in A$ we define

$$(2.2.10)\qquad [a]_V(X) = g_V^{-1}(ag_V(X))$$

$$(2.2.11)\qquad [a]_{V,T}(X) = g_{V,T}^{-1}(ag_{V,T}(X))$$

$$(2.2.12)\qquad [a]_S(X) = g_S^{-1}(ag_S(X))$$

2.3. Integrality Theorems: (i) *The power series $G_V(X, Y)$, $G_{V,T}(X, Y)$ and $G_S(X, Y)$ have their coefficients respectively in $A[V]$, $A[V, T]$, $A[S]$*; (ii) *For all $a \in A$, the power series $[a]_V(X)$, $[a]_{V,T}(X)$, $[a]_S(X)$ have their coefficients respectively in $A[V]$, $A[V, T]$, $A[S]$.*

2.4. Corollary: *$G_V(X, Y)$, $G_{V,T}(X, Y)$ and $G_S(X, Y)$ with the structural homomorphisms $\rho_V(a) = [a]_V(X)$, $\rho_{V,T}(a) = [a]_{V,T}(X)$, $\rho_S = (a) = [a]_S(X)$ are formal A-modules.*

2.5. Universality Theorem: $(G_S(X, Y), \rho_S)$, where $\rho_S(a) = [a]_S(X)$, is a universal formal A-module.

I.e. for every formal A-module $(F(X, Y), \rho_F)$ over $B \in \mathbf{Alg}_A$, there is a unique A-algebra homomorphism $\phi: A[S] \to B$ such that $\phi_*G_S(X, Y) = F(X, Y)$ and $\phi_*[a]_S(X) = \rho_F(a)$ for all $a \in A$. Here ϕ_* means: "apply ϕ to the coefficients of the power series involved".

2.6. *A-logarithms*

Let $(F(X, Y), \rho_F)$ be a formal A-module over $B \in \mathbf{Alg}_A$. Suppose that B is A-torsion free, i.e. that $B \to B \otimes_A K$ is injective. Let $\phi : A[S] \to B$ be the unique homomorphism taking $(G_S(X, Y), \rho_S)$ into $(F(X, Y), \rho_F)$. Then $\phi_* g_S(X) = f(X) \in B \otimes_A K[[X]]$ is a power series such that $F(X, Y) = f^{-1}(f(X) + f(Y))$, $[a](X) = f^{-1}(af(X))$ for all $a \in A$, and such that $f(X) \equiv X$ mod(degree 2). We shall call such a power series an A-logarithm for $(F(X, Y), \rho_F)$. We have just seen that A-logarithms always exist (if B is A-torsion free). They are also unique because there are no nontrivial strict formal A-module automorphisms of the additive formal A-module $G_a(X, Y) = X + Y$, $[a](X) = aX$ over $B \otimes_A K$, as is easily checked.

2.7. *A-typical formal A-modules*

A formal A-module $(F(X, Y), \rho_F)$ over $B \in \mathbf{Alg}_A$ is said to be A-typical if it is of the form $F(X, Y) = \phi_* G_V(X, Y)$, $\rho_F(a) = \phi_*[a]_V(X)$ for some homomorphism $\phi : A[V] \to B$. It is then an immediate consequence of the constructions of $G_S(X, Y)$ and $G_V(X, Y)$ that $(G_V(X, Y), \rho_V)$, $\rho_V(a) = [a]_V(X)$, is a universal A-typical formal A-module (given theorem 2.5).

2.8. THEOREM: *Let B be A-torsion free. Then* $(F(X, Y), \rho_F)$ is an A-typical formal A-module if and only if its A-logarithm $f(X)$ is of the form

$$f(X) = \sum_{i=0}^{\infty} a_i X^{q^i}, \quad a_i \in B \otimes_A K, \quad a_0 = 1$$

Let $\kappa : A[V] \to A[S]$ be the injective homomorphism defined by $\kappa(V_i) = S_{q^i}$, and let $\lambda : A[V] \to A[V, T]$ be the natural inclusion.

2.9. THEOREM: (i) *The formal A-modules* $G_V^\kappa(X, Y)$ *and* $G_S(X, Y)$ *are strictly isomorphic*; (ii) *The formal A-modules* $G_V^\lambda(X, Y)$ and $G_{V,T}(X, Y)$ *are strictly isomorphic.*

2.10. COROLLARY: *Every formal A-module is isomorphic to an A-typical one.*

2.11. Let $\alpha_{V,T}(X)$ be the (unique) strict isomorphism from $G_V^\lambda(X, Y)$ to $G_{V,T}(X, Y)$. I.e. $\alpha_{V,T}(X) = g_{V,T}^{-1}(g_V(X))$.

2.12. THEOREM: *The triple* $(G_V(X, Y), \alpha_{V,T}(X), G_{V,T}(X, Y))$ *is universal for triples consisting of two A-typical formal A-modules* *and a strict isomorphism between them over A-algebras B which are A-torsion free.*

There is also a triple $(G_S(X, Y), \alpha_{S,U}(X), G_{S,U}(X, Y))$ which is universal for triples of two formal A-modules and a strict isomorphism between them. The formal A-module $G_{S,U}(X, Y)$ over $A[S; U]$ is defined as follows

$$g_{S,U}(X) = X + \sum_{\substack{i\geq 2\\ i \text{ not power}\\ \text{of } q}} S_i X^i + \sum_{i=2}^{\infty} U_i X^i + \sum_{i=1}^{\infty} \frac{S_{q^i}}{\pi} g_{S,U}^{(q^i)}(X^{q^i}) \tag{2.12.1}$$

$$G_{S,U}(X, Y) = g_{S,U}^{-1}(g_{S,U}(X) + g_{S,U}(Y)) \tag{2.12.2}$$

The strict isomorphism between $G_{S,U}(X, Y)$ and $G_{S,U}(X, Y)$ is $\alpha_{S,U}(X) = g_{S,U}^{-1}(g_S(X))$.

2.13. Let $(F(X, Y), \rho_F)$ be a formal A-module over A itself. Let $\omega : A \to k = A/\pi A$ be the natural projection. The formal A-module $(\omega_* F(X, Y), \omega_* \rho_F)$ is called the reduction mod π of $F(X, Y)$. We also write $(F^*(X, Y), \rho_F^*)$ for $(\omega_* F(X, Y), \omega_* \rho_F)$.

2.14. THEOREM: (Lubin [6] in the case $\text{char}(K) = 0$): *Two formal A-modules over A are (strictly) isomorphic if and only if their reductions over A are (strictly) isomorphic.*

2.15. REMARK: If the two formal A-modules over A are both A-typical then they are (strictly) isomorphic if and only if their reductions are equal.

3. Formulae

3.1. *Some formulae*

The following formulae are all proved rather easily, directly from the definitions in 2.2. Write

$$g_V(X) = \sum_{i=0}^{\infty} a_i(V) X^{q^i}, \quad a_0(V) = 1 \tag{3.1.1}$$

$$g_{V,T}(X) = \sum_{i=0}^{\infty} a_i(V, T) X^{q^i}, \quad a_0(V, T) = 1 \tag{3.1.2}$$

Then we have

$$(3.1.3)\qquad a_i(V)=\sum_{i_1+\cdots+i_r=i}\frac{V_{i_1}V_{i_2}^{q^{i_1}}\cdots V_{i_r}^{q^{i_1+\cdots+i_{r-1}}}}{\pi^r}$$

$$(3.1.4)\qquad a_i(V)=a_0(V)\frac{V_i}{\pi}+a_1(V)\frac{V_{i-1}^q}{\pi}+\cdots+a_{i-1}(V)\frac{V_1^{q^{i-1}}}{\pi}$$

$$(3.1.5)\quad a_i(V,T)=a_i(V)+a_{i-1}(V)T_1^{q^{i-1}}+\cdots+a_1(V)T_{i-1}^q+a_0(V)T_i$$

3.2. We define for all $i,j\geq 1$.

$$(3.2.1)\qquad Y_{ij}=\pi^{-1}(V_iT_j^{q^i}-T_iV_j^{q^i}),\quad Z_{ij}=\pi^{-1}(V_iT_j^{p^i}-T_jV_i^{p^j})$$

The symbols $Y_{ij}^{(q^r)}$, $Z_{ij}^{(q^r)}$ then have the usual meaning, i.e. $Y_{ij}^{(q^r)}=\pi^{-1}(V_i^{q^r}T_j^{q^{r+i}}-T_i^{q^r}V_j^{q^{r+i}})$

3.3. Lemma:

$$a_n(V,T)=\sum_{i=1}^n a_{n-i}(V,T)\frac{V_i^{q^{n-i}}}{\pi}+\sum_{i,j\geq 1,i+j\leq n}a_{n-i-j}(V)Y_{ij}^{(q^{n-i-j})}+T_n$$

$$=\sum_{i=1}^n a_{n-i}(V,T)\frac{V_i^{q^{n-i}}}{\pi}+\sum_{i,j\geq 1,i+j\leq n}a_{n-i-j}(V)Z_{ij}^{(q^{n-i-j})}+T_n$$

Proof: That the two expressions on the right are equal is obvious from the definitions of $Z_{i,j}$ and Y_{ij} (because $Z_{ij}+Z_{ji}=Y_{ij}+Y_{ji}$). We have according to (3.1.4) and (3.1.5)

$$a_n(V,T)=a_n(V)+\sum_{i=1}^n a_{n-i}(V)T_i^{q^{n-i}}$$

$$=\pi^{-1}V_n+\sum_{i=1}^{n-1}\pi^{-1}a_{n-i}(V)V_i^{q^{n-i}}+T_n$$

$$+\sum_{i=1}^{n-1}\sum_{j=1}^{n-i}\pi^{-1}a_{n-i-j}(V)V_j^{q^{n-i-j}}T_i^{q^{n-i}}$$

$$=\pi^{-1}V_n+T_n+\sum_{i=1}^{n-1}\pi^{-1}a_{n-i}(V,T)V_i^{q^{n-i}}$$

$$-\sum_{i=1}^{n-1}\sum_{j=1}^{n-i}\pi^{-1}a_{n-i-j}(V)T_j^{q^{n-i-j}}V_i^{q^{n-i}}$$

$$+\sum_{i=1}^{n-1}\sum_{j=1}^{n-i}\pi^{-1}a_{n-i-j}(V)V_j^{q^{n-i-j}}T_i^{q^{n-i}}$$

$$= T_n + \pi^{-1} V_n + \sum_{i=1}^{n-1} \pi^{-1} a_{n-i}(V, T) V_i^{q^{n-i}}$$

$$+ \sum_{i,j \geq 1, i+j \leq n} a_{n-i-j} Y_{ij}^{(q^{n-i-j})}$$

$$= T_n + \sum_{i=1}^{n} \pi^{-1} a_{n-i}(V, T) V_i^{q^{n-i}} + \sum_{i,j \geq 1, i+j \leq n} a_{n-i-j} Y_{ij}^{(q^{n-i-j})}$$

3.4. *Some congruence formulae*

Let $n \in \mathbb{N}$; we write $g_{V(n)}(X), G_{V(n)}(X, Y), \ldots$ for the power series obtained from $g_V(X), G_V(X, Y), \ldots$ by substituting 0 for all V_i with $i \geq n$.

One then has

(3.4.1) $$g_V(x) \equiv g_{V(n)}(X) + \frac{V_n}{\pi} X^{q^n} \bmod(\text{degree } q^n + 1)$$

(3.4.2) $$g_S(X) \equiv g_{S(n)}(X) + \tau(n) S_n X^n \bmod(\text{degree } n + 1)$$

where $\tau(n) = 1$ if n is not a power of q and $\tau(n) = \pi^{-1}$ if n is a power of q. Further

(3.4.3) $$g_{V,T}(X) \equiv g_{V,T(n)}(X) + T_n X^{q_n} \bmod(\text{degree } q^n + 1)$$

(3.4.4) $$G_V(X, Y) \equiv G_{V(n)}(X, Y) - V_n \pi^{-1} B_{q^n}(X, Y) \bmod(\text{degree } q^n + 1)$$

(3.4.5) $$G_S(X, Y) \equiv G_{S(n)}(X, Y) - S_n \tau(n) B_n(X, Y) \bmod(\text{degree } n + 1)$$

where $B_i(X, Y) = (X + Y)^i - X^i - Y^i$, and finally

(3.4.6) $$g_{S,U}(X) \equiv g_{S,U(n)}(X) + U_n X^n \bmod(\text{degree } n + 1)$$

4. The functional equation lemma

Let $A[V; W] = A[V_1, V_2, \ldots; W_1, W_2, \ldots]$. If $f(X)$ is a power series with coefficients in $K[V; W]$ we write $P_{1,2} f(X_1, X_2) = f(X_1) + f(X_2)$ and $P_a f(X_1, X_2) = a f(X_1)$, $a \in A$.

4.1. Let $e_r(X)$, $r = 1, 2$ be two power series with coefficients in $A[V, W]$ such that $e_r(X) \equiv X \bmod(\text{degree } 2)$. Define

(4.1.1) $$f_r(X) = e_r(X) + \sum_{i=1}^{\infty} \frac{V_i}{\pi} f_r^{(q^i)}(X^{q^i})$$

And for each operator P, where $P = P_{1,2}$ or $P = P_a$, $a \in A$ and r,

$t \in \{1, 2\}$ we define

$$F^{P}_{V,e_r,e_t}(X_1, X_2) = f_r^{-1}(Pf_t(X_1, X_2)) \tag{4.1.2}$$

4.2. Functional Equation Lemma: (i) *The power series* $F^{P}_{V,e_r,e_t}(X_1, X_2)$ *have their coefficients in* $A[V; W]$ *for all* P, e_r, e_t; (ii) *If* $d(X)$ *is a power series with coefficients in* $A[V; W]$ *such that* $d(X) \equiv X$ mod(degree 2) *then* $f_r(d(X))$ *satisfies a functional equation of type* (4.1.1).

Proof: Write $F(X_1, X_2)$ for $F^{P}_{V,e_r,e_t}(X_1, X_2)$. (If $P \neq P_{1,2}$, X_2 does not occur). Write

$$F(X_1, X_2) = F_1 + F_2 + \cdots$$

where F_i is homogeneous of degree i. We are going to prove by induction that all the F_i have their coefficients in A[V; W]. This is obvious for F_1 because $e_r(X) \equiv e_t(X) \equiv X$ mod(degree 2). Let $a(X_1, X_2)$ be any power series with coefficients in $A[V; W]$. Then we have for all $i, j \in \mathbb{N}$

$$(a(X_1, X_2))^{q^{i+j}} \equiv (a^{(q^i)}(X_1^{q^i}, X_2^{q^i}))^{q^j} \bmod(\pi^{j+1}) \tag{4.2.1}$$

This follows imnediately from the fact that $a^q \equiv a \bmod \pi$ for all $a \in A$ and $p \in \pi A$. Write

$$f_r(X) = \sum_{i=1}^{\infty} b_i(r)X^i, \quad b_1(r) = 1 \tag{4.2.2}$$

Then we have, if $q^{\ell}|n$ but $q^{\ell+1} \nmid n$, that

$$b_n(r)\pi^{\ell} \in A[V; W] \tag{4.2.3}$$

This is obvious from the defining equation (4.1.1). Now suppose we have shown that $F_1, \ldots, F_n$ have their coefficients in $A[V; W]$, $n \geq 1$. We have for all $d \geq 2$.

$$F(X_1, X_2)^d \equiv (F_1 + \cdots + F_n)^d \bmod(\text{degree } n + 2) \tag{4.2.4}$$

It now follows from (4.2.4), (4.2.3) and (4.2.1) that

$$f_r^{(q^i)}(F(X_1, X_2)^{q^i}) \equiv f_r^{(q^i)}(F^{(q^i)}(X_1^{q^i}, X_2^{q^i})) \bmod(\pi, \text{degree } n + 2) \tag{4.2.5}$$

Now from (4.1.2) it follows that for all $i \in \mathbb{N}$

(4.2.6) $$f_r^{(q^i)}(F^{(q^i)}(X_1, X_2)) = Pf_t^{(q^i)}(X_1, X_2).$$

Using (4.2.5), (4.2.6) and (4.1.1) we now see that

$$\begin{aligned}
f_r(F(X_1, X_2)) &= e_r(F(X_1, X_2) + \sum_{i=1} \pi^{-1} V_i f_r^{(q^i)}(F(X_1, X_2)^{q^i}) \\
&\equiv e_r(F(X_1, X_2) + \sum_{i=1}^{\infty} \pi^{-1} V_i f_r^{(q^i)}(F^{(q^i)}(X_1^{q^i}, X_2^{q^i})) \\
&= e_r(F(X_1, X_2) + \sum_{i=1}^{\infty} \pi^{-1} V_i P f_t^{(q^i)}(X_1^{q^i}, X_2^{q^i}) \\
&= e_r(F(X_1, X_2)) + \left(P \sum_{i=1}^{\infty} \pi^{-1} V_i f_t^{(q^i)}\right)(X_1, X_2) \\
&= e_r(F(X_1, X_2)) + Pf_t(X_1, X_2) - Pe_t(X_1, X_2),
\end{aligned}$$

where all congruences are mod(1, degree $n+2$). But $f_r(F(X_1, X_2)) = Pf_t(X_1, X_2)$. And hence $e_r(F(X_1, X_2) - (Pe_t)(X_1, X_2) \equiv 0$ mod(1, degree $n+2$), which implies that F_{n+1} has its coefficients in $A[V, W]$. This proves the first part of the functional equation lemma. Now let $d(X)$ be a power series with coefficients in $A[V, W]$ such that $d(X) \equiv X$ mod(degree 2). Then we have because of (4.2.1) and (4.2.2)

$$\begin{aligned}
g_r(X) = f_r(d(X)) &= \sum_{i=1}^{\infty} \pi^{-1} V_i f_r^{(q^i)}(d(X)^{q^i}) \\
&\equiv \sum_{i=1}^{\infty} \pi^{-1} V_i f_r^{(q^i)}(d^{(q^i)}(X^{q^i})) \\
&= \sum_{i=1}^{\infty} \pi^{-1} V_i g_r^{(q^i)}(X^{q^i})
\end{aligned}$$

where the congruences are mod(1). This proves the second part.

4.3. Proof of Theorem 2.3 (and corollary 2.4): *Apply the functional equation lemma part (i). (For $G_S(X, Y)$ and $[a]_S(X)$ take $V_i = S_{q^i}$).*

5. Proof of the universality theorems

We first recall the usual comparison lemma for formal groups (cf. e.g. [3]).

For each $n \in \mathbb{N}$, define $B_n(X, Y) = ((X+Y)^n - X^n - Y^n))$ and $C_n(X, Y) = \nu(n)^{-1} B_n(X, Y)$, where $\nu(n) = 1$ if n is not a power of a prime number, and $\nu(p^r) = p$, $r \in \mathbb{N}$, if p is a prime number.

5.1. If $F(X, Y)$, $G(X, Y)$ are formal groups over a ring B, and $F(X, Y) \equiv G(X, Y) \bmod(\text{degree } n)$, there is a unique $b \in B$ such that $F(X, Y) \equiv G(X, Y) + bC_n(X, Y) \bmod(\text{degree } n+1)$.

5.2. PROOF OF THE UNIVERSALITY THEOREM 2.5: *Let $(F(X, Y), \rho_F)$ be a formal A-module over B. Let $A[S]_n$ be the subalgebra $A[S_2, \ldots, S_{n-1}]$ of $A[S]$. Suppose we have shown that there exists a homomorphism $\phi_n : A[S]_n \to B$ such that*

$$\phi_{n*}(G_S(X, Y)) \equiv F(X, Y) \bmod(\text{degree } n) \tag{5.2.1}$$

$$\phi_{n*}[a]_S(X) \equiv [a]_F(X) \bmod(\text{degree } n) \tag{5.2.2}$$

and that ϕ_n is uniquely determined on $A[S]_n$ by this condition. This holds obviously for $n = 2$ so that the induction starts.

Now, according to the comparison lemma 5.1 above there exist unique elements m, m_a, $a \in A$, in B such that

$$\phi_{n*} G_S(X, Y) \equiv F(X, Y) + mC_n(X, Y) \bmod(\text{degree } n+1) \tag{5.2.3}$$

$$\phi_{n*}[a]_s(X) \equiv [a]_F(X) + m_a X^n \bmod(\text{degree } n+1) \tag{5.2.4}$$

From the fact that $a \mapsto [a]_S(X)$ and $a \mapsto [a]_F(X)$ are ring homomorphisms one now obtains easily the following relations between the m and m_a

$$(a^n - a)m = \nu(n) m_a \tag{5.2.5}$$

$$m_{a+b} - m_a - m_b = C_n(a, b)m \tag{5.2.6}$$

$$am_b + b^n m_a = m_{ab} \tag{5.2.7}$$

If n is not a power of $p = \text{char}(k)$, then $\nu(n)$ is a unit. Let $\phi_{n+1} : A[S]_{n+1} \to B$ be the unique homomorphism, which agrees with ϕ_n on $A[S]_n$ and which is such that $\phi_{n+1}(S_n) = m\nu(n)^{-1}$. Then obviously (5.2.1) holds with n replaced by $n+1$, and (5.2.2) holds with n replaced by $n+1$ because of (5.2.5) and because (3.4.2) implies that (with the obvious notations)

(5.2.8) $[a]_S(X) \equiv [a]_{S(n)}(X) - \tau(n)(a^n - a)S_n X^n \bmod(\text{degree } n+1)$.

Now let $n = p^r$, but n not a power of q, the number of elements of k. Then there is an $y \in A$ such that $(y - y^n)$ is a unit in A. Let $\phi_{n+1}: A[S]_{n+1} \to B$ be the unique homomorphism which agrees with ϕ_n on $A[S_n$ and which takes S_n to $(y - y^n)^{-1}m_y$. Now (5.2.7) implies that for all $a \in A$

$$(y - y^n)m_a = (a - a^n)m_y$$

Hence $\phi_{n+1}(a - a^n)S_n = m_a$ for all a so that (5.2.2) holds with n replaced with $n + 1$. Finally, again because $(y - y^n)$ is a unit, we find

$$(\phi_{n+1})_*(-S_n\tau(n)B_n(X, Y)) = (y^n - y)^{-1}m_yB_n(X, Y) = mC_n(X, Y)$$

Finally let n be a power of q. In this case there is a unique homomorphism $\phi_{n+1}: A[S]_{n+1} \to B$ which agrees with ϕ_n on $A[S]_n$ and which takes S_n into $(1 - \pi^{n-1})^{-1}m_\pi$. Of course this is the only possible choice for ϕ_{n+1} because of (5.2.8).

Now consider the A-module generated by symbols $\hat{m}, \hat{m}_a$, $a \in A$ subject to the relations $(a^n - a)\hat{m} = \nu(n)\hat{m}_a$, $\hat{m}_{a+b} - \hat{m}_a - \hat{m}_b = C_n(a, b)\hat{m}$, $a\hat{m}_b + b^n\hat{m}_a = \hat{m}_{ab}$, for all $a, b \in A$. This module is free on one generator $\hat{m}_\pi$. This will be proved in 5.3 below. It follows that all the $\hat{m}_a$ and $\hat{m}$ can be written as multiples of $\hat{m}_\pi$. These multiples turn out to be

$$\hat{m}_a = \pi^{-1}(a^n - a)(\pi^{n-1} - 1)^{-1}\hat{m}_\pi, \quad \hat{m} = \pi^{-1}\nu(n)(\pi^{n-1} - 1)^{-1}.$$

simply because if one takes an arbitrary element $\hat{m}_\pi$ and one defines $\hat{m}_a$, $\hat{m}$ as above, then all the required relations are satisfied. It follows in particular that

$$m_a = \pi^{-1}(a^n - a)(\pi^{n-1} - 1)^{-1}m_\pi, \quad m = \pi^{-1}\nu(n)(\pi^{n-1} - 1)^{-1}m_\pi$$

where m, m_a, $a \in A$ are as in (5.2.3), (5.2.4) above. Hence

$$\phi_{n+1}(\pi^{-1}(a - a^n)S_n) = m_a, \quad \phi_{n+1}(-S_n\pi^{-1}\nu(n)) = m$$

so that, by (5.2.8) and (3.45), (5.2.1) and (5.2.2) hold with n replaced by $n + 1$. This completes the induction step and (hence) the proof of theorem 2.5.

5.3. Lemma: *Let X be the A-module generated by symbols m, m_a for all $a \in A$ subject to the relations*

$$(5.3.1)\qquad (a^n - a)m = \nu(n)m_a \quad \text{for all } a \in A$$

$$(5.3.2)\qquad m_{a+b} - m_a - m_b = C_n(a, b)m \quad \text{for all } a, b \in A$$

$$(5.3.3)\qquad am_b + b^n m_a = m_{ab} \quad \text{for all } a, b \in A$$

Suppose moreover that n is a power of q. Then X is a free A-module of rank 1, with generator m_π.

PROOF: Let $\bar{X} = X/Am_\pi$. For each $x \in X$ we denote with $\bar{x}$ its image in $\bar{X}$. Then because $(\pi - \pi^n)m_a = (a - a^n)m_\pi$ and because $1 - \pi^{n-1}$ is a unit in A we have that $\pi\bar{m}_a = 0$ in $\bar{X}$. Further $(\pi^n - \pi)m = \nu(n)m_\pi$ so that also $\pi\bar{m} = 0$ in $\bar{X}$. This proves that $\bar{X}$ is a k-module. Now $b^n \equiv b \bmod \pi$ (as n is a power of q). Hence $\bar{m}_{ab} = a\bar{m}_b + b\bar{m}_a$ in $\bar{X}$ proving that the map $C: k \to \bar{X}$, defined by $\bar{a} \mapsto \bar{m}_a$ is well defined and satisfies $C(\bar{a}\bar{b}) = \bar{a}C(\bar{b}) + \bar{b}C(\bar{a})$. In particular $C(\bar{a}^n) = n\bar{a}^{n-1}C(\bar{a}) = 0$. But $\bar{a}^n = \bar{a}$. Hence $C(\bar{a}) = \bar{m}_a = 0$ for all $a \in A$.

With induction one finds from (5.3.2) that

$$(5.3.4)\qquad m_{a_1+\cdots+a_p} - m_{a_1} - \cdots - m_{a_p} = C_{n,p}(a_1, \ldots, a_p)m$$

where $C_{n,p}(Z_1, \ldots, Z_p) = p^{-1}((Z_1 + \cdots + Z_p)^n - Z_1^n - \cdots - Z_p^n)$. Taking $a_1 = \cdots = a_p = 1$ we find that $m_p - pm_1 = (p^{n-1} - 1)m$, and hence $\bar{m} = 0$ because $1 - p^{n-1}$ is a unit of A. This proves that $\bar{X}$ is zero so that X is generated by m_π. Now define $X \to A$ by $m_a \mapsto \pi^{-1}(a^n - a)$, $m \mapsto \pi^{-1}$p. This is well defined and surjective. Hence $X \simeq A$.

5.4. PROOF OF THEOREM 2.8: *First*, $(G_V(X, Y), \rho_V)$ has the A-logarithm $g_V(X)$ and hence satisfies the A-logarithm condition of theorem 2.8. The A-logarithm of $(\phi_* G_V(X, Y), \phi_* \rho_V)$ is $\phi_* g_V(X)$, which also satisfies the condition of theorem 2.8. Inversely, let $(F(X, Y), \rho_F)$ have an A-logarithm of the type indicated. Let $\phi: A[S] \to B$ be such that $\phi_* G_S(X, Y) = F(X, Y)$, $\phi_* \rho_S = \rho_F$. Then, as B is A-torsion free, $\phi_* g_S(X) = f(X)$ because A-logarithms are unique. From the definition of $G_S(X, Y)$ (cf. (3.4.1), (3.4.2)) we see that $\phi(S_i) = 0$ unless i is a power of q. Hence ϕ factorizes through $A[S] \to A[V]$, $S_i \mapsto 0$ if i is not a power of q, $S_{q_i} \mapsto V_i$, and, comparing $g_V(X)$ and $g_S(X)$, we see that $\psi_* g_V(X) = f(X)$, where ψ is the A-homomorphism $A[V] \to B$ induced by ϕ. q.e.d.

6. Proofs of the isomorphism theorems

6.1. PROOF OF THEOREM 2.9: *Apply the functional equation lemma.*

6.2. PROOF OF THE UNIVERSITY OF THE TRIPLE: $(G_S(X, Y), \alpha_{S,U}(X), G_{S,U}(X, Y))$: *Let* $F(X, Y)$, $G(X, Y)$ be two formal A-modules over B and let $\beta(X)$ be a strict isomorphism from $F(X, Y)$ to $G(X, Y)$. Because $G_S(X, Y)$ is universal there is a unique homomorphism $\phi: A[S] \to B$ such that $\phi_* G_S(X, Y) = F(X, Y)$, $\phi_* \rho_S = \rho_F$. Now $\alpha_{S,U}(X) = g_{S,U}^{-1}(g_S(X))$, hence we have by (3.4.6)

$$\alpha_{S,U}(X) \equiv \alpha_{S,U(n)}(X) - U_n X^n \bmod(\text{degree } n+1) \tag{6.2.1}$$

It follows from this that there is a unique extension $\psi: A[S, U] \to B$ such that $\psi_* \alpha_{S,U}(X) = \beta(X)$, and then $\psi_* G_{S,U}(X, Y) = G(X, Y)$, $\psi_* \rho_{S,U} = \rho_G$, automatically.

6.3. PROOF OF THEOREM 2.12: Let $F(X, Y)$, $G(X, Y)$ be two A-typical formal A-modules over B, and let $\beta(X)$ be a strict isomorphism from $F(X, Y)$ to $G(X, Y)$. Let $f(X)$, $g(X)$ be the logarithms of $F(X, Y)$ and $G(X, Y)$. Then $g(\beta(X)) = f(X)$. Because of the universality of the triple $(G_S(X, Y), \alpha_{S,U}(X), G_{S,U}(X, Y))$ there is a unique A-algebra homomorphism $\psi: A[S, U] \to B$ such that

$$\psi_* G_S(X, Y) = F(X, Y), \quad \psi_* \rho_S = \rho_F \quad \text{and} \quad \psi_* \alpha_{S,U}(X) = \beta(X).$$

Because $F(X, Y)$ is A-typical we know that $\psi(S_i) = 0$ if i is not a power of q. Because $F(X, Y)$ and $G(X, Y)$ are A-typical we know that $f(X)$ and $g(X)$ are of the form $\Sigma\, c_i X^{q^i}$. But $g(\beta(X)) = f(X)$. It now follows from (6.2.1) that we must have $\psi(U_i) = 0$ if i is not a power of q. This proves the theorem.

6.4. PROOF OF THEOREM 2.14: It suffices to prove the theorem for the case of strict isomorphisms. Let $F(X, Y)$, $G(X, Y)$ be two formal A-modules over A and suppose that $F^*(X, Y)$ and $G^*(X, Y)$ are strictly isomorphic. By taking any strict lift of the strict isomorphism we can assume that $F^*(X, Y) = G^*(X, Y)$. Finally by Theorem 2.9 (i) and its corollary 2.10 we can make $F(X, Y)$ and $G(X, Y)$ both A-typical and this does not destroy the equality $F^*(X, Y) = G^*(X, Y)$ because the theorem gives us a universal way of making an A-module A-typical. So we are reduced to the situation: $F(X, Y)$, $G(X, Y)$ are A-typical formal A-modules over A and $F^*(X, Y) = G^*(X, Y)$. Let ϕ, ϕ' be the unique homomorphisms $A[V] \to A$ such that

$$\phi_* G_V(X, Y) = F(X, Y), \quad \phi_* \rho_V = \rho_F,$$
$$\phi'_* G_V(X, Y) = G(X, Y), \quad \phi'_* \rho_V = \rho_G.$$

Let $v_i = \phi(V_i)$, $v'_i = \phi'(V_i)$. Because $F^*(X, Y) = G^*(X, Y)$, $\rho_F^* = \rho_G^*$ we must have

$$v_i \equiv v'_i \bmod \pi A, \quad i = 1, 2, \ldots \tag{6.4.1}$$

(by the uniqueness part of the universality of $(F_V(X, Y), \rho_V)$).

If we can find $t_i \in A$ such that $a_n(v, t) = a_n(v')$ for all n then $\alpha_{v,t}(X)$ will be the desired isomorphism. Let us write $z_{ij}^{(q^{n-i-j})}$ for the element of $A \otimes_Z \mathbf{Q}$ obtained by substituting v_i for V_i and t_j for T_j in $Z_{ij}^{(q^{n-i-j})}$. Then the problem is to find t_i, $i = 1, 2, \ldots$ such that

$$a_n(v') = \sum_{i=1}^{n} \pi^{-1} a_{n-i}(v') v_i^{q^{n-i}} + \sum_{i,j \geq 1, i+j \leq n} a_{n-i-j}(v) z_{ij}^{(q^{n-i-j})} + t_n \tag{6.4.2}$$

Now

$$a_n(v') = \sum_{i=1}^{n} \pi^{-1} a_{n-i}(v') v_i'^{q^{n-i}} \tag{6.4.3}$$

So that t_n is determined by the recursion formula

$$t_n = \sum_{i=1}^{n} a_{n-i}(v') \pi^{-1} (v_i'^{q^{n-i}} - v_i^{q^{n-i}}) - \sum_{i,j \geq 1, i+j \leq n} a_{n-i-j}(v) z_{ij}^{(q^{n-i-j})} \tag{6.4.4}$$

And what we have left to prove is that these t_n are elements of A (and not just elements of K). However,

$$\pi^{n-i} a_{n-i}(v') \in A, \quad z_{ij} = \pi^{-1}(v_i t_j^{q^i} - t_j v_i^{q^j}), \quad v_i \equiv v'_i \bmod \pi \tag{6.4.5}$$

Hence

$$v_i'^{q^{n-i}} \equiv v_i^{q^{n-i}} \bmod \pi^{n-i+1}, \quad z_{ij}^{(q^{n-i-j})} \equiv 0 \bmod \pi^{n-i-j} \tag{6.4.6}$$

and it follows recursively that the t_n are integral. This proves the theorem.

6.5. Proof of Remark 2.15. If $F(X, Y)$ and $G(X, Y)$ are A-typical formal A-modules over A, which are strictly isomorphic then $F^*(X, Y) = G^*(X, Y)$. Indeed, because $F(X, Y)$, $G(X, Y)$ are strictly isomorphic A-typical formal A-modules we have that there exist unique v_i, v'_i, $t_i \in A$ such that (6.4.2), (6.4.3) and hence (6.4.4) hold. Taking $n = 1$ we see that $v_1 \equiv v'_1 \bmod \pi$. Assuming that $v_i \equiv v'_i \bmod \pi$, $i = 1, \ldots, n-1$, it follows from (6.4.4) that $v_n \equiv v'_n$. Finally, let $F(X, Y)$ be an A-typical formal A-module, $F(X, Y) = G_v(X, Y)$, $v_1, v_2, \ldots \in A$, and let $u \in A$ be an invertible element of A. If $f(X) = \Sigma a_i X^{q^i}$ is the logarithm of $F(X, Y)$, then the logarithm of $F'(X, Y) = u^{-1}F(uX, uY)$ is equal to $\Sigma a_i u^{q^i-1} X^{q^i}$, so that $F'(X, Y) = G_{v'}(X, Y)$ with $v_1' = u^{q-1}v_1, \ldots, v_n' = u^{q^n-1}v_n, \ldots$ and it follows that $v_i' \equiv v_i \bmod \pi$, i.e. $F'^*(X, Y) = F^*(X, Y)$.

7. Concluding remarks

Several of the results in [1], [2] and [6] follow readily from the theorems proved above. For example the following. Let $F(X, Y)$ be a formal A-module; define $\mathrm{END}(F)$, the absolute endomorphism ring of F, to be the ring of all endomorphisms of F defined over some finite extension of K. Let $\phi_h : A[V] \to A$ be any homomorphism such that $\phi_h(V_i) = 0$, $i = 1, \ldots, h-1$, $\phi_h(V_h) \in A^*$, the units of A and $\phi_h(V_{h+1}) \neq 0$. Then $((\phi_h)_* F_V(X, Y), (\phi_h)_* \rho_V)$ is a formal A-module of formal A-module height h and with absolute endomorphism ring equal to A.

(If $\mathrm{char}(K) = p$ then formal A-module height is defined as follows. Let B be the ring of integers of a finite extension of K; let m be the maximal ideal of B. Consider $[\pi]_F(X)$ for $(F(X, Y), \rho_F)$ a formal A-module over B. If $[\pi]_F(X) \equiv 0 \bmod (m)$, then one shows that the first monomial of $[\pi]_F(X)$ which is not $\equiv 0 \bmod (m)$ is necessarily of the form aX^{q^h}. Then A-height $(F(X, Y), \rho_F) = h$. If $\mathrm{char}(K) = 0$ this agrees with the usual definition A-height $= [\mathrm{K} : \mathbf{Q}_p]^{-1}$ Height).

REFERENCES

[1] L. COX: Formal A-modules. *Bull. Amer. Math. Soc. 79*, 4 (1973) 690–6994.

[2] L. COX: Formal A-modules over $\mathfrak{p}$-adic integer rings, *Compositio Math. 29* (1974) 287–308.

[3] M. HAZEWINKEL: Constructing Formal Groups I–VII; I: *Journal of Pure and Applied Algebra 9* (1977), 131–149; II: ibid. 151–161; III: ibid, *10* (1977) 1–18; IV–VII: *Adv. Math.*, to appear.

' M. HAZEWINKEL: A Universal Formal Group and Complex Cobordism. *Bull. Amer. Math. Soc. 81* (1975) 930–933.

[5] M. HAZEWINKEL: A Universal Isomorphism for p-typical Formal Groups and Operations in Brown-Peterson Cohomology. *Indagationes Math. 38* (1976) 195–199.

[6] J. LUBIN: Formal A-modules defined over A. *Symposia Mat. INDAM 3* (1970) 241–245.

(Oblatum 30–VIII–1976 & 14–X–1977)

Erasmus University
Econometric Institute
Burg. Oud-laan 50, Rotterdam
The Netherlands