ERASMUS UNIVERSITY ROTTERDAM

ECONOMETRIC INSTITUTE

Report 7507/M

CONSTRUCTING FORMAL A-MODULES

by Michiel Hazewinkel

April 17, 1975 Preliminary

1. INTRODUCTION.

Let $\mathbb{Q}_p$ be the p-adic integers, let K be a finite extension of $\mathbb{Q}_p$ 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.

All formal groups will be commutative one dimensional; $\mathbb{N}$ stands for the set the natural numbers $\{1, 2, 3, \ldots\}$; $\mathbb{Z}$ denotes the integers, $\mathbb{Z}_p$ the ring of p-adic integers, $\mathbb{Q}$ denotes the rational numbers and $\mathbb{Q}_p$ the p-adic numbers. A will always be the ring of integers of a finite extension of $\mathbb{Q}_p$, its quotient field will be denoted K, π is a uniformizing element of A and k is the residue field of K, i.e. $k = A/\pi A$. We shall use q to denote the number of elements of k.

2. DEFINITIONS, CONSTRUCTIONS AND STATEMENT OF MAIN RESULTS.

Let $\mathbb{Z}_p$ and A be as above. With B we shall always denote an A-algebra which is a characteristic zero ring i.e. $B \to B \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective.

2.1. <u>Definition</u>.

A formal A-module over B is a (one dimensional commutative) formal group $G(X,Y)$ over B such that for every $a \in A$, there is a power series $[a](X)$ such that $[a](X) \equiv aX$ mod degree 2, and such that

$[a](G(X,Y)) = G([a](X),[a](Y)$, i.e. $[a](X)$ is an endomorphism of $G(X,Y)$. Because B is a characteristic zero ring the series $[a](X)$ is unique.

2.2. Let R be a ring, $\mathbb{R}[U] = \mathbb{R}[U_1,U_2,\dots]$. If $f(X)$ is a power series over $\mathbb{R}[U]$ and $n \in \mathbb{N}$ we denote with $f^{(n)}(X)$ the power series obtained from $f(X)$ by replacing each U_i with U_i^n, $i = 1,2,\dots$.
Let $A[V]$, $A[V;T]$, $A[S]$ denote respectively the rings $A[V_1, V_2,\dots]$, $A[V_1,V_2,\dots; T_1, T_2,\dots]$, $A[S_2,S_3,\dots]$. 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

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

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

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

The first few terms are

$$(2.2.4) \qquad g_V(X) = X + \frac{V_1}{\pi}X^q + \left(\frac{V_1V_1^q}{\pi^2} + \frac{V_2}{\pi}\right)X^{q^2} + \dots$$

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

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

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

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

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

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

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 $G_S(X,Y)$ are formal A-modules

2.5. Universality Theorem.

$G_S(X,Y)$ is a universal formal A-module

I.e. for every formal A-module $F(X,Y)$ over an A-algebra B there is a unique A-algebra homomorphism $\phi : A[S] \to B$ such that $G_S^{\phi}(X,Y) = F(X,Y)$ where $G_S^{\phi}(X,Y)$ is the formal group obtained from $G_S(X,Y)$ by applying ϕ to its coefficients.

2.6. Definition.

Let $F(X,Y)$ be a formal A-module over B. Because B is a characteristic zero ring the logarithm $f(X)$ of $F(X,Y)$ is well defined. We shall say that the formal A-module $F(X,Y)$ is A-typical if its logarithm is of the form

$$f(X) = \sum_{i=0}^{\infty} a_i X^{q^i} \quad , \ a_i \in B \otimes_{\mathbb{Z}} \mathbb{Q} \ , \ a_0 = 1 \tag{2.6.1}$$

2.7. Theorem.

$G_V(X,Y)$ is a universal A-typical formal A-module

2.8. 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.

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

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

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

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 $F(X,Y)$ be a formal A-module over A itself. Let $\rho: A \to k = A/\pi A$ be the natural projection. The formal group $F^\rho(X,Y)$ is called the reduction mod π of $F(X,Y)$.

2.14. Theorem (Lubin [6]).

Two formal A-modules over A are (strictly) isomorphic iff their reductions over k 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. SOME FORMULAE.

3.1. Some Formulae.

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

$$(3.1.1)\qquad g_V(X) = \sum_{i=o}^{\infty} a_i(V)X^{q^i}, \quad a_o(V) = 1$$

$$(3.1.2)\qquad g_{V,T}(X) = \sum_{i=o}^{\infty} a_i(V,T)X^{q^i}, \quad a_o(V,T) = 1$$

Then we have

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

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

$$(3.1.5)\qquad a_i(V,T) = a_i(V) + a_{i-1}(V)T_1^{q^{i-1}} + \dots + a_1(V)T_{i-1}^q + a_o(V)T_i$$

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)

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

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

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

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

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

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

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

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

3.4. Some Congruence Formulae.

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

One then has

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

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

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

$$(3.4.3)\qquad G_{V,T}(X) \equiv G_{V,T(n)}(X) + T_n X^{q^n} \mod (\text{degree } q^n+1)$$

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

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

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

And finally

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

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 $P_a f(X_1,X_2) = af(X_1)$, $a \in A$.

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

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

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

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

4.2. <u>Functional Equation Lemma</u>.

(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 $d(X) \equiv X \bmod$ (degree 2) then $f_r(d(X))$ satisfies on a functional equation of type (4.1.1).

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

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

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 $e_r(X) \equiv e_t(X) \equiv X \bmod$ (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 $\in \mathbb{N}$

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

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

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

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

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

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

$$(4.2.4) \qquad F(X_1,X_2)^d \equiv (F_1+\dots+F_n)^d \mod (\text{degree } n+2)$$

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

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

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

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

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

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

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. <u>Proof of Theorem 2.3</u> (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 $C_n(X,Y) = \nu(n)^{-1}Bn(X,Y)$, 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 $F(X,Y) \equiv G(X,Y)$ mod (degree n), there is a unique $b \in B$ such that $F(X,Y) \equiv G(X,Y) + bC_n(X,Y)$.

5.2. Lemma.

Let $F(X,Y)$ and $G(X,Y)$ be formal A-modules, and suppose that $F(X,Y) \equiv G(X,Y)$ mod (degree n), then there is a unique $b \in B \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $F(X,Y) \equiv G(X,Y) + bB_n(X,Y)$, where $b \in B$ if n is not a power of q and $\pi b \in B$ if n is a power of q.
This lemma is standard. Cf. e.g. [2]. For completeness sake we give the easy proof. By 5.1 we know that there is a unique $b \in B \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $F(X,Y) \equiv G(X,Y) + bB_n(X,Y)$. Let $a \in A$. B being a characteristic zero ring we have that $[a]_F(X) \equiv [a]_G(X)$ mod (degree n). Let $c \in B$ be the unique element such that $[a]_F(X) \equiv [a]_G(X) + cX^n$ mod (degree n+1).
We have mod (degree n+1)

$$
\begin{aligned}
[a]_F G(X,Y) &\equiv [a]_F F(X,Y) - abB_n(X,Y) \\
&= F([a]_F(X),[a]_F(Y)) - abB_n(X,Y) \\
&\equiv G([a]_F(X),[a]_F(Y)) - abB_n(X,Y) + bB_n(aX,aY) \\
&\equiv G([a]_G(X),[a]_G(Y)) - abB_n(X,Y) + bB_n(aX,aY) + c(X^n+Y^n) \\
&= [a]_G G(X,Y) - abB_n(X,Y) + ba^nB_n(X,Y) + c(X^n+Y^n) \\
&= [a]_F G(X,Y) - c(X+Y)^n - abB_n(X,Y) + ba^nB_n(X,Y) + c(X^n+Y^n)
\end{aligned}
$$

It follows that $(a-a^n)b \in B$ for all $a \in A$. Now if n is not a power of q, there is a $a \in A$ such that $a - a^n$ is a unit in A, hence $b \in B$ in that case.

Let n be a power of q, suppose that $\pi b \notin B$, then there is an r such that $\pi^r b \in B$ but $\pi^{rn} b \in B$, because $pb \in B$ and $p|\pi^t$ for t large enough. This is a contradiction, hence $\pi b \in B$.

5.3. Proof of Theorem 2.5. (Universality of $G_S(X,Y)$)

This follows immediately from 5.2 above and (3.4.4)

5.4. Proof of Theorem 2.7. (A-typical universality of $G_V(X,Y)$).

Let $F(X,Y)$ be an A-typical formal A-module over B. By the universality of $G_S(X,Y)$, there is a unique A-algebra homomorphism $\phi : A[S] \to B$ such that $G_S^{\phi}(X,Y) = F(X,Y)$. Because $F(X,Y)$ is A-typical (cf. 2.6) it follows from (3.4.1) that we must have $\phi(S_i) = 0$ if i is not a power of q. This proves the theorem.

6. PROOFS OF THE ISOMORPHISM THEOREMS.

6.1. Proof of Theorem 2.9.

Apply the functional equation lemma.

6.2. Proof of the Universality 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 $G_S^{\phi}(X,Y) = F(X,Y)$. Now $\alpha_{S,U}(X) = g_{S,U}^{-1}(g_S(X))$, hence we have by (3.4.6),

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

It follows from this that there is a unique extension $\psi : A[S,T] \to B$ such that $\alpha_{S,U}^{\psi}(X) = \beta(X)$. And then $G_{S,U}^{\psi}(X,Y) = G(X,Y)$ 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 $G_S^{\psi}(X,Y) = F(X,Y)$ and $\alpha_{S,U}^{\psi}(X) = \beta(X)$. 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 distroy 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 $G_V^\phi(X,Y) = F(X,Y)$, $G_V^\phi(X,Y) = G(X,Y)$. Let $v_i = \phi(V_i)$, $v_i' = \phi'(V_i)$. Because $F^*(X,Y) = G^*(X,Y)$ we must have

$$(6.4.1) \qquad v_i \equiv v_i' \quad \bmod \pi\ ,\ i = 1, 2, \ldots$$

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 $A \otimes_{\mathbb{Z}} \mathbb{Q}$ 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

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

Now

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

So that t_n is determined by the recursion formula

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

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

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

Hence

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

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 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 $v_1 \equiv v_1' \mod \pi$. Assuming that $v_i \equiv v_i' \mod \pi$, $i = 1, \ldots, n-1$, 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 $v_1' = u^{q-1}v_1, \ldots, v_n' = u^{q^n-1}v_n$, and it follows that $v_i' \equiv v_i \mod \pi$, 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 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 $F_V^{\phi_h}(X,Y)$ is a formal A-module of formal A-module height h and with absolute endomorphism ring equal to A.

REFERENCES.

[1]. L. Cox, Formal A-Modules. Bull. Amer. Math. Soc. 79, 4 (1973, 690-694.

[2]. L. Cox, Formal A-Modules over p-adic Integer Rings. Preprint, Brown University 1973.

[3]. M. Hazewinkel, Constructing Formal Groups I, II, III, IV. Reports 7119, 7201, 7207, 7322 of the Econometric Institute, Erasmus Univ. Rotterdam, 1971, 1972, 1973.

[4]. M. Hazewinkel, A Universal Formal Group and Complex Cobordism. Bull. Amer. Math. Soc. (to appear).

[5]. M. Hazewinkel, Constructing Formal Groups I: The Local One Dimensional Case (to appear).

[6]. J. Lubin, Formal A-modules defined over A. Symposia Mathematica INDAM 3, 1970, 241-245.

SYMBOLS USED.

Latin lower case   k,q,a,f,i,n,p,g,r,t,e,d,j,b,c,z,u,h,

Latin upper case   K,A,B,G,R,U,X,Y,V,T,S,F,Z,W,P,E,N,D,

Latin lower case bold face

Latin upper case bold face $\mathbb{Q}$(rational numbers, $\mathbb{N}$(natural numbers, $\mathbb{Z}$ (integers)

Latin lower case as sub- or superscript p,n,i,q,r,j,a,t,e,l,d,h

Latin upper case a sub- or superscript V,T,S,U,P,F,G,

Latin upper case bold face as sub- or superscript $\mathbb{Z}$

Greek lower case $\pi,\phi,\kappa,\lambda,\alpha,\rho,\tau,\nu,\beta,\psi$,

Greek upper case

Greek lower case as sub- or superscript $\phi,\kappa,\lambda,\rho,\psi$,

Numerals   0,1,2,3,4,5,6

Numerals as sub- or superscript 0,1,2

Special symbol as sub- or superscript $\infty,=,+,-,(,),\geq,\leq$,

Special symbols $/,[,],=,\otimes,\rightarrow,\in,(,),\equiv,\Sigma,+,-,\geq,\leq,\{,\},|,\nmid$,

Groups of letters occurring in formulas   mod, degree