CONSTRUCTING FORMAL GROUPS. VIII:
FORMAL A-MODULES

Michiel Hazewinkel

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.

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 \( F_p((t)) \), where \( F_p \) is the field of \( p \)-elements.

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

\( A \) will always be the ring of integers of a finite extension of \( \mathbb{Q}_p \) or \( F_p((t)) \), the field of Laurent series over \( F_p \). The quotient field of \( A \) is denoted \( K \), \( \pi \) 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 \( k \).
2. Definitions, constructions and statement of main results.

2.1. Definitions. Let \( B \in \text{Alg}_{A} \), 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 \( \rho_{F} : A \to \text{End}_{B}(F(X, Y)) \) such that \( \rho_{F}(a) = aX \mod(\text{degree } 2) \) for all \( a \in A \). We shall also write \([a](X)\) for \( \rho_{F}(a) \).

If \( B \) is torsion free (i.e. \( B \to B \otimes \mathbb{Q} \) 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 \( \text{char}(K) = p \), then every formal \( A \)-module over \( B \in \text{Alg}_{A} \) is isomorphic to the additive formal group \( G_{p}(X, Y) = X + Y \) over \( B \). In this case all the structure sits in the structural morphism \( \rho_{F} : A \to \text{End}_{B}(F(X, Y)) \).

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 \( \alpha(X) = b_{1}X + b_{2}X^{2} + \ldots \), \( b_{i} \in B \) such that \( \alpha(f(X, Y)) = G(\alpha(X), \alpha(Y)) \). \( \alpha([a]_{p}(X)) = [a]_{p}(\alpha(X)) \); \( \alpha(X) \) is an isomorphism if \( b_{1} \) is a unit and \( \alpha \) 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 \( n \in \mathbb{N} \) 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 \( A[V_{1}, V_{2}, \ldots], A[V_{1}, V_{2}, \ldots; T_{1}, T_{2}, \ldots], A[S_{1}, S_{2}, \ldots] \). 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

\[
(2.2.1) \quad g_{v}(X) = X + \sum_{i=1}^{n} \frac{V_{i}}{\pi} g_{v}^{(i)}(X^{i})
\]

\[
(2.2.2) \quad g_{v,T}(X) = X + \sum_{i=1}^{n} T_{i}X^{i} + \sum_{i=1}^{n} \frac{V_{i}}{\pi} g_{v}^{(i)}(X^{i})
\]

\[
(2.2.3) \quad g_{S}(X) = X + \sum_{i=2}^{\infty} S_{i}X^{i} + \sum_{i=1}^{\infty} \frac{S_{i}}{\pi} g_{S}^{(i)}(X^{i})
\]

The first few terms are

\[
(2.2.4) \quad g_{v}(X) = X + \frac{V_{1}}{\pi} X^{2} + \left( \frac{V_{1}^{2}}{\pi^{2}} + \frac{V_{2}}{\pi} \right) X^{2} + \ldots
\]
(2.2.5) \[ g_{v,T}(X) = X + \left( \frac{V_1 + T_1}{\pi} \right) X^2 + \left( \frac{V_1 T_2}{\pi} + \frac{V_2 T_2}{\pi} + T_2 \right) X^3 + \cdots \]

(2.2.6) \[ g_{S}(X) = X + S_1 X^2 + \cdots + S_{q-1} X^{q-1} + \frac{S_2}{\pi} X^q + S_{q+1} X^{q+1} + \cdots \\
+ S_{2q-1} X^{2q-1} + \left( \frac{S_2 S_{q-1}}{\pi} + S_{2q} \right) X^{2q} + \cdots \]

We now define

(2.2.7) \[ G_{v}(X, Y) = g_{v}(g_{v}(X) + g_{v}(Y)) \]
(2.2.8) \[ G_{v,T}(X, Y) = g_{v,T}(g_{v}(X) + g_{v}(Y)) \]
(2.2.9) \[ G_{S}(X, Y) = g_{S}(g_{S}(X) + g_{S}(Y)) \]

where if \( f(X) = X + r_2 X^2 + \cdots \) 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) \[ [a]_{v}(X) = g_{v}(a g_{v}(X)) \]
(2.2.11) \[ [a]_{v,T}(X) = g_{v,T}(a g_{v,T}(X)) \]
(2.2.12) \[ [a]_{S}(X) = g_{S}(a g_{S}(X)) \]

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 \( B \in \text{Alg}_{A} \), 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 \( \phi_{*} \) means: “apply \( \phi \) to the coefficients of the power series involved”.
2.6. A-logarithms

Let \((F(X, Y), \rho_F)\) be a formal A-module over \(B \in \text{Alg}_A\). 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 \(\phi_S g_S(X) = f(X) \in B \otimes_A K[[X]]\) 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 \(f(X) = X \mod(\text{degree 2})\). 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 \(B \in \text{Alg}_A\) is said to be A-typical if it is of the form \(F(X, Y) = \phi_a G_v(X, Y), \rho_v(a) = \phi_a[a]_v(X)\) 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

\[
f(X) = \sum_{n=0}^{\infty} a_n X^n, \quad a_n \in B \otimes_A K, \quad a_0 = 1
\]

Let \(\kappa : A[V] \to A[S]\) be the injective homomorphism defined by \(\kappa(V) = S_v\), and let \(\lambda : A[V] \to A[V, T]\) be the natural inclusion.

2.9. Theorem: (i) The formal A-modules \(G_v(X, Y)\) and \(G_S(X, Y)\) are strictly isomorphic; (ii) The formal A-modules \(G_v(X, Y)\) 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 \(G_v(X, Y)\) to \(G_{V,T}(X, Y)\). i.e. \(\alpha_{V,T}(X) = g_v(g_v(X)).\)

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

\begin{equation}
(2.12.1) \quad g_{SU}(X) = X + \sum_{i \neq q \text{ not power of} q} S_i X^i + \sum_{i} U_i X^i + \sum_{i \neq 1} \frac{S_i}{\pi} g_{SU}(X^i)
\end{equation}

\begin{equation}
(2.12.2) \quad G_{SU}(X, Y) = g_{SU}^{-1}(g_{SU}(X) + g_{SU}(Y))
\end{equation}

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

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

2.14. Theorem: (Lubin [6] in the case 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

\begin{equation}
(3.1.1) \quad g \cdot (X) = \sum_{i \neq q} a_i(V) X^i, \quad a_0(V) = 1
\end{equation}

\begin{equation}
(3.1.2) \quad g \cdot (X) = \sum_{i \neq q} a_i(V, T) X^i, \quad a_0(V, T) = 1
\end{equation}
Then we have

\[ a_i(V) = \sum_{i=1}^{n} a_{i}^{(q_{i}^{(i-1)}, T_{i})} \]

\[ a_i(V) = a_0(V) \frac{V_i}{\pi} + a_1(V) \frac{V_i^2}{\pi} + \cdots + a_{n-1}(V) \frac{V_i^{n-1}}{\pi} \]

(3.1.5) \[ a_i(V, T) = a_i(V) + a_{i-1}(V) T_i^{q_{i}^{(i-1)}} + \cdots + a_0(V) T_{i-1} + a_0(V) T_i \]

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

(3.2.1) \[ Y_{ij} = \pi^{-1}(V_i T_j^{q_{i}^{(j-1)}} - T_i V_j^{q_{j}^{(j-1)}}), \quad Z_{ij} = \pi^{-1}(V_i T_j^{q_{i}^{(j-1)}} - T_i V_j^{q_{j}^{(j-1)}}) \]

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

3.3. LEMMA:

\[ a_n(V, T) = a_n(V) + \sum_{i=1}^{n} a_{i-1}(V, T) \frac{V_i^{q_{i}^{(i-1)}}}{\pi} + \sum_{i=2}^{n} \sum_{j=1}^{n} a_{i-1}(V) Y_{ij}^{(q_{i}^{(i-1)}-1)} + T_n \]

\[ = \sum_{i=1}^{n} a_{i-1}(V, T) \frac{V_i^{q_{i}^{(i-1)}}}{\pi} + \sum_{i=2}^{n} \sum_{j=1}^{n} a_{i-1}(V) Z_{ij}^{(q_{i}^{(i-1)-1})} + T_n \]

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

\[ a_n(V, T) = a_n(V) + \sum_{i=1}^{n} a_{i-1}(V) T_i^{q_{i}^{(i-1)}} \]

\[ = \pi^{-1} V_n + \sum_{i=1}^{n} \pi^{-1} a_{i-1}(V) V_i^{q_{i}^{(i-1)}} + T_n \]

\[ + \sum_{i=1}^{n} \sum_{j=1}^{n} \pi^{-1} a_{i-1}(V) V_i^{q_{i}^{(i-1)}} T_i^{q_{i}^{(i-1)}} \]

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

\[ - \sum_{i=1}^{n} \sum_{j=1}^{n} \pi^{-1} a_{i-1}(V) T_i^{q_{i}^{(i-1)}} V_i^{q_{i}^{(i-1)}} \]

\[ + \sum_{i=1}^{n} \sum_{j=1}^{n} \pi^{-1} a_{i-1}(V) T_i^{q_{i}^{(i-1)}} V_i^{q_{i}^{(i-1)}} \]
\[= T_n + \pi^{-1} V_n + \sum_{i=1}^{n-1} \pi^{-1} a_{n-i}(V, T)V_{\pi^{n-i}}^i + \sum_{i+j \leq n} a_{n-i-j} Y_{\pi^{n-i-j}}\]

\[= T_n + \sum_{i=1}^{n} \pi^{-1} a_{n-i}(V, T)V_{\pi^{n-i}}^i + \sum_{i+j \leq n} a_{n-i-j} Y_{\pi^{n-i-j}}\]

### 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

\[(3.4.1) \quad g_v(x) = g_{v(n)}(X) + V_n \pi X^n \mod (\text{degree } q^n + 1)\]

\[(3.4.2) \quad g_s(x) = g_{s(n)}(X) + \tau(n)S_n X^n \mod (\text{degree } n + 1)\]

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

\[(3.4.3) \quad g_{v,T}(X) = g_{v,T(n)}(X) + T_x X^n \mod (\text{degree } q^n + 1)\]

\[(3.4.4) \quad G_v(X, Y) = G_{v(n)}(X, Y) - V_n \pi^{-1} B_{n}(X, Y) \mod (\text{degree } q^n + 1)\]

\[(3.4.5) \quad G_s(X, Y) = G_{s(n)}(X, Y) - S_n \tau(n) B_n(X, Y) \mod (\text{degree } n + 1)\]

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

\[(3.4.6) \quad g_{s,v}(X) = g_{s,v(n)}(X) + U_{n} X^n \mod (\text{degree } n + 1)\]

### 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 \( P_{r,f}(X_1, X_2) = f(X_i) + f(X_2) \) and \( P_{a,f}(X_1, X_2) = af(X_i), a \in A \).

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

\[(4.1.1) \quad f_r(X) = e_r(X) + \sum_{i=1}^{n} \frac{V_i}{\pi} f_{r,i}(X^i)\]

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

\[
F_{v, e_t}(X_1, X_2) = f_t(P_t(X_1, X_2))
\]

4.2. Function Equation Lemma: (i) The power series \( F_{v, e_t}(X_1, X_2) \) have their coefficients in \( A[V; W] \) for all \( P, e, e_t \); (ii) If \( d(X) \) is a power series with coefficients in \( A[V; W] \) such that \( d(X) = X \mod(\text{degree } 2) \) then \( f_t(d(X)) \) satisfies a functional equation of type (4.1.1).

Proof: Write \( F(X_1, X_2) \) for \( F_{v, e_t}(X_1, X_2) \). (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 \( e_0(X) = e_t(X) = X \mod(\text{degree } 2) \). Let \( a(X_1, X_2) \) be any power series with coefficients in \( A[V; W] \). Then we have for all \( i, j \in \mathbb{N} \)

\[
(a(X_1, X_2))^q^{i+j} = (a(q^{i+j}(X_1^q, X_2^{q^j}))^q \mod(p^{i+j})
\]

This follows immediately from the fact that \( a^q = a \mod p \) for all \( a \in A \) and \( p \in \pi A \). Write

\[
f_t(X) = \sum_{r=1}^n b_r(r)X^i, \quad b_1(r) = 1
\]

Then we have, if \( q^f|n \) but \( q^{f+1} \nmid n \), that

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

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 \( d \geq 2 \)

\[
F(X_1, X_2)^d = (F_1 + \cdots + F_n)^d \mod(\text{degree } n + 2)
\]

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

\[
f_t^{q^f}(F(X_1, X_2)^d) = f_t^{q^f}(F^{q^f}(X_1^{q^f}, X_2^{q^f})) \mod(\pi, \text{degree } n + 2)
\]
Now from (4.1.2) it follows that for all $i \in \mathbb{N}$

\[(4.2.6) \quad f_i^{(q)}(F^{(q)}(X_1, X_2)) = Pf_i^{(q)}(X_1, X_2).\]

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

\[
f_i(F(X_1, X_2)) = e_i(F(X_1, X_2) + \sum_{i=1}^{\infty} \pi^{-1} V f_i^{(q)}(F^{(q)}(X_1, X_2))
\]

\[
= e_i(F(X_1, X_2) + \sum_{i=1}^{\infty} \pi^{-1} V f_i^{(q)}(F^{(q)}(X_1^q, X_2^q))
\]

\[
= e_i(F(X_1, X_2) + \sum_{i=1}^{\infty} \pi^{-1} V Pf_i^{(q)}(X_1^q, X_2^q)
\]

\[
= e_i(F(X_1, X_2) + \left(P \sum_{i=1}^{\infty} \pi^{-1} V f_i^{(q)}\right)(X_1, X_2)
\]

\[
= e_i(F(X_1, X_2)) + Pf_i(X_1, X_2) - Pe_i(X_1, X_2),
\]

where all congruences are mod(1, degree $n + 2$). But $f_i(F(X_1, X_2)) = Pf_i(X_1, X_2)$. And hence $e_i(F(X_1, X_2) - (Pe_i)(X_1, X_2) = 0$ 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 $d(X) \equiv X \mod(\text{degree } 2)$. Then we have because of (4.2.1) and (4.2.2)

\[
g_i(X) = f_i(d(X)) = \sum_{i=1}^{\infty} \pi^{-1} V f_i^{(q)}(d(X)^q)
\]

\[
= \sum_{i=1}^{\infty} \pi^{-1} V f_i^{(q)}(d^{(q)}(X^q))
\]

\[
= \sum_{i=1}^{\infty} \pi^{-1} V g_i^{(q)}(X^q)
\]

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 $V_1 = S_a$).

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 $F(X, Y) \equiv G(X, Y) \mod(\text{degree } n)$, there is a unique $b \in B$ such that $F(X, Y) = G(X, Y) + bC_n(X, Y) \mod(\text{degree } n + 1)$.

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

\begin{align*}
(5.2.1) \quad & \phi_{\nu n}(G_s(X, Y)) = F(X, Y) \mod(\text{degree } n) \\
(5.2.2) \quad & \phi_{\nu n}[a]_s(X) = [a]_\rho(X) \mod(\text{degree } n)
\end{align*}

and that $\phi_n$ 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 $m, m_n, a \in A$, in $B$ such that

\begin{align*}
(5.2.3) \quad & \phi_{\nu n}G_s(X, Y) = F(X, Y) + mC_n(X, Y) \mod(\text{degree } n + 1) \\
(5.2.4) \quad & \phi_{\nu n}[a]_s(X) = [a]_\rho(X) + m_nX^n \mod(\text{degree } n + 1)
\end{align*}

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

\begin{align*}
(5.2.5) \quad & (a^n - a)m = \nu(n)m_n \\
(5.2.6) \quad & m_{a + b} - m_a - m_b = C_n(a, b)m \\
(5.2.7) \quad & am_b + b^n m_a = m_{ab}
\end{align*}

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 $\phi_n$ on $A[S]_n$ and which is such that $\phi_{n+1}(S_n) = \tau(n)^{-1}$. 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)

\begin{align*}
(5.2.8) \quad & [a]_s(X) = [a]_{S_n}X^n - \tau(n)(a^n - a)S_nX^n \mod(\text{degree } n + 1).
\end{align*}
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 \( \phi_n \) on \( A[S]_n \) and which takes \( S_a \) to \((y - y^n)^{-1}m_a \). Now (5.2.7) implies that for all \( a \in A \)

\[(y - y^n)m_a = (a - a^n)m_a\]

Hence \( \phi_{n+1}(a - a^n)S_a = m_a \) 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

\[(\phi_{n+1})(-S_a\tau(n)B_a(X, Y)) = (y^n - y)^{-1}m_aB_a(X, Y) = mC_a(X, Y)\]

Finally let \( n \) be a power of \( q \). In this case there is a unique homomorphism \( \phi_{n} : A[S]_{n} \to B \) which agrees with \( \phi_n \) on \( A[S]_n \) and which takes \( S_a \) into \((1 - \pi^{n-1})^{-1}m_a \). Of course this is the only possible choice for \( \phi_{n+1} \) 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 \((a^n - a)\hat{m} = \nu(n)\hat{m}_a, \hat{m}_{a+b} - \hat{m}_a - \hat{m}_b = C_a(a, b)\hat{m}_a, \hat{m}_a + b^n\hat{m}_a = \hat{m}_{ab} \) for all \( a, b \in A \). This module is free on one generator \( \hat{m}_a \). 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 \( \hat{m}_a \). These multiples turn out to be

\[\hat{m}_a = \pi^{-1}(a^n - a)(\pi^{n-1} - 1)^{-1}\hat{m}_a, \quad \hat{m} = \pi^{-1}\nu(n)(\pi^{n-1} - 1)^{-1}\hat{m}_a\]

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

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

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

\[\phi_{n+1}(\pi^{-1}(a^n - a)S_a) = m_a, \quad \phi_{n+1}(-S_a\pi^{-1}\nu(n)) = m\]

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
\[(5.3.1) \quad (a^n - a)m = \nu(n)m_a \quad \text{for all } a \in A\]
\[(5.3.2) \quad m_{a+b} - m_a - m_b = C_n(a, b)m \quad \text{for all } a, b \in A\]
\[(5.3.3) \quad a m_b + b^n m_a = m_{ab} \quad \text{for all } a, b \in A\]

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

Proof: Let \(\bar{X} = X/A_m\). For each \(x \in X\) we denote with \(\bar{x}\) its image in \(\bar{X}\). Then because \((\pi - \pi^a)m_a = (a - a^n)m_a\) and because \(1 - \pi^{n-1}\) is a unit in \(A\) we have that \(\pi m_a = 0\) in \(\bar{X}\). Further \((\pi^n - \pi)m = \nu(n)m_a\) so that also \(\pi m = 0\) in \(\bar{X}\). This proves that \(\bar{X}\) is a \(k\)-module. Now \(b^n = b \mod \pi\) (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 \(C(\bar{a}^s) = n\bar{a}^{n-1}C(\bar{a}) = 0\). But \(\bar{a}^s = \bar{a}\). Hence \(C(\bar{a}) = \bar{m}_a = 0\) for all \(a \in A\).

With induction one finds from (5.3.2) that
\[(5.3.4) \quad m_{a_1 \cdots a_p} - m_{a_1} - \cdots - m_{a_p} = C_{a_1, \ldots, a_p}(a_1, \ldots, a_p)m\]
where \(C_{a_1, \ldots, a_p}(Z_1, \ldots, Z_p) = p^{-1}((Z_1 + \cdots + Z_p)^n - Z_1 + \cdots - Z_p)\). 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 \(m_a\). Now define \(X \to A\) by \(m_a \mapsto \pi^{-1}(a^n - a)\), \(m \mapsto \pi^{-1}p\mbox{. This is well defined and surjective. Hence } X = A\).

5.4. Proof of Theorem 2.8: First, \((G_t(X, Y), \rho_t)\) has the \(A\)-logarithm \(g_t(X)\) and hence satisfies the \(A\)-logarithm condition of theorem 2.8. The \(A\)-logarithm of \((\phi_a G_t(X, Y), \phi_a \rho_t)\) is \(\phi_a g_t(X)\), 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 \(\phi_a G_t(X, Y) = F(X, Y), \phi_a \rho_t = \rho_F\). Then, as \(B\) is \(A\)-torsion free, \(\phi_a g_t(X) = f(X)\) because \(A\)-logarithms are unique. From the definition of \(G_t(X, Y)\) (cf. (3.4.1), (3.4.2)) we see that \(\phi(S) = 0\) unless \(i\) is a power of \(q\). Hence \(\phi\) factorizes through \(A[S] \to A[V]\), \(S_i \mapsto 0\) if \(i\) is not a power of \(q\), \(S_q \mapsto V_a\), and, comparing \(g_t(X)\) and \(g_t(X)\), we see that \(\psi_a g_t(X) = f(X)\), where \(\psi\) is the \(A\)-homomorphism \(A[V] \to B\) induced by \(\phi\). 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: \( (G_\delta(X, Y), \alpha_{SU}(X), G_{SU}(X, Y)) \): 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 \( G_\delta(X, Y) \) is universal there is a unique homomorphism \( \phi : A[S] \to B \) such that \( \phi \circ G_\delta(X, Y) = F(X, Y), \phi \circ \alpha_{SU}(X) = \rho_F \). Now \( \alpha_{SU}(X) = g_{SU}^{-1}(g_\delta(X)) \), hence we have by (3.4.6)

\[
(6.2.1) \quad \alpha_{SU}(X) = \alpha_{SU/\alpha}(X) - U_i X^i \mod(\text{degree } n + 1)
\]

It follows from this that there is a unique extension \( \psi : A[S, U] \to B \) such that \( \psi \circ \alpha_{SU}(X) = \beta(X) \), and then \( \psi \circ G_{SU}(X, Y) = G(X, Y), \psi \circ \alpha_{SU} = \rho_G \) 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 \( (G_\delta(X, Y), \alpha_{SU}(X), G_{SU}(X, Y)) \) there is a unique \( A \)-algebra homomorphism \( \psi : A[S, U] \to B \) such that

\[
\psi \circ G_\delta(X, Y) = F(X, Y), \quad \psi \circ \alpha_{SU} = \rho_F \quad \text{and} \quad \psi \circ \alpha_{SU}(X) = \beta(X).
\]

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 \( \Sigma c_i X^i \). 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 \( \phi, \phi^f \) be the unique homomorphisms \( A[V] \to A \) such that

\[
\phi \circ G_\delta(X, Y) = F(X, Y), \quad \phi \circ \alpha_{SU} = \rho_F, \\
\phi^f \circ G_\delta(X, Y) = G(X, Y), \quad \phi^f \circ \alpha_{SU} = \rho_G.
\]
Let $v_i = \phi(V_i)$, $v'_i = \phi'(V_i)$. Because $F^*(X, Y) = G^*(X, Y)$, $\rho^x = \rho^x$, we must have

\[(6.4.1) \quad v_i \equiv v'_i \mod \pi A, \quad i = 1, 2, \ldots \]

(by the uniqueness part of the universality of $(F, \rho, \rho_V)$).

If we can find $t_i \in A$ such that $a_n(v, t) = a_n(v')$ for all $n$ then $\alpha_n(X)$ will be the desired isomorphism. Let us write $z'^{(x^{x^{-1}})}_n$ for the element of $A \otimes_\mathbb{Z} \mathcal{O}$ obtained by substituting $v_i$ for $V_i$ and $t_i$ for $T_i$ in $Z'^{x^{x^{-1}}}_n$. Then the problem is to find $t_n, i = 1, 2, \ldots$ such that

\[(6.4.2) \quad a_n(v') = \sum_{i=1}^n \pi^{-1} a_{n-i}(v') v'^{x^{x^{-1}}} + \sum_{i,j \geq 1, ij \leq n} a_{n-i-j}(v) z'^{(x^{x^{-1}})}_n + t_n \]

Now

\[(6.4.3) \quad a_n(v') = \sum_{i=1}^n \pi^{-1} a_{n-i}(v') v'^{x^{x^{-1}}} \]

So that $t_n$ is determined by the recursion formula

\[(6.4.4) \quad t_n = \sum_{i=1}^n a_{n-i}(v') \pi^{-1}(v'^{x^{x^{-1}}}_i - v'^{x^{x^{-1}}}_i) - \sum_{i,j \geq 1, ij \leq n} a_{n-i-j}(v) z'^{(x^{x^{-1}})}_n \]

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

\[(6.4.5) \quad \pi^{x^{-1}} a_{n-i}(v') \in A, \quad z'^{(x^{x^{-1}})}_n = \pi^{-1}(v'^{x^{x^{-1}}}_i - t_i v'^{x^{x^{-1}}}_i), \quad v_i \equiv v'_i \mod \pi \]

Hence

\[(6.4.6) \quad v'^{x^{x^{-1}}} = v'^{x^{x^{-1}}} \mod \pi^{x^{-1}}, \quad z'^{(x^{x^{-1}})}_n \equiv 0 \mod \pi^{x^{x^{-1}}-i} \]

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 $v_n, v'_n, t_i \in A$ 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 $v_n = v'_n$. Finally, let $F(X, Y)$ be an $A$-typical
formal $A$-module, $F(X, Y) = G_e(X, Y)$, $v_1, v_2, \ldots \in A$, and let $u \in A$ be an invertible element of $A$. If $f(X) = \sum a_i X^{u_i}$ is the logarithm of $F(X, Y)$, then the logarithm of $F'(X, Y) = u^{-1} F(uX, uY)$ is equal to $\sum a_i u^{u_i - 1} X^{u_i}$, so that $F'(X, Y) = G_e(X, Y)$ with $v'_1 = u^{u_1 - 1} v_1$, $\ldots$, $v'_n = u^{u_n - 1} v_n$, and it follows that $v'_i = v_i \mod \pi$, 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 $\text{END}(F)$, 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 $((\phi_h)_* F_r(X, Y), (\phi_h)_* \rho_Y)$ is a formal $A$-module of formal $A$-module height $h$ and with absolute endomorphism ring equal to $A$.

(If $\text{char}(K) = p$ 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 $[\pi]_p(X)$ for $(F(X, Y), \rho_Y)$ a formal $A$-module over $B$. If $[\pi]_p(X) \equiv 0 \mod(m)$, then one shows that the first monomial of $[\pi]_p(X)$ which is not $\equiv 0 \mod(m)$ is necessarily of the form $aX^h$. Then $A$-height $(F(X, Y), \rho_Y) = h$. If $\text{char}(K) = 0$ this agrees with the usual definition $A$-height $= [K:Q_\pi]^{1/2}$ Height).

REFERENCES
