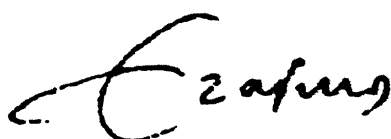


ECONOMETRIC INSTITUTE

CONSTRUCTING FORMAL GROUPS

PARTS IV, V, VI, VII

M. HAZEWINKEL

A handwritten signature in black ink, appearing to read 'Erasmus', is centered on the page.

REPORT 7827/M

CONSTRUCTING FORMAL GROUPS.
IV: MORE DIMENSIONAL FORMAL GROUPS

Michiel Hazewinkel

AMS(MOS): 14L05

Key words and phrases: more dimensional universal commutative formal group, p-typical formal group, curvilinear formal group.

Authors address: Dept. Math., Erasmus Univ. Rotterdam
50, Burg. Oudlaan,
ROTTERDAM, The Netherlands

This preprint contains the final drafts of parts IV - VII of my series of papers "Constructing Formal Groups I - VIII". Parts I, II, III have appeared in the J. pure and applied Algebra 9 (1977) 131-150; *ibid.* 9 (1977), 151-162; *ibid.* 10 (1977), 1-18. Parts IV -VII had been accepted for publication in Adv. Math. However, because of the excessively long publishing delays of Adv. Math., my book Formal Groups and Applications, Acad. Press, 1978, appeared before these papers were actually published. Author and editor therefore decided to remove these papers from the Adv. Math. backlog. Part VIII of the series will appear in Compositio Math.

Michiel Hazewinkel

Constructing Formal Groups IV

1

1. INTRODUCTION.

In this paper we give an explicit construction for the logarithm of more dimensional (commutative) formal groups of various kinds. The procedure is basically the same as in [3], [4]; cf. also the brief indications in [2], part I, II for the more dimensional case. That is, we first construct a suitable candidate for a universal formal group by giving its logarithm in terms of a functional equation, then we prove that the formal group with this logarithm is indeed integral and finally we prove universality of this formal group by a more dimensional extension of the method which Buhštaber and Novikov have used in [1] to prove universality of the formal group of complex cobordism. The one dimensional algebraic version of this trick has already been used in [3], [4].

Thus one avoids Lazard's truly tough (and computational) comparison lemma between more dimensional formal groups. Cf. [7]. This lemma now appears as a corollary.

Thus, starting from nothing, one obtains in 10 pages or so (i) a proof of the existence of a universal n -dimensional formal group, (ii) the structure of the underlying ring and (iii) an explicit description of the logarithm of this formal group, and, if one wishes, the same things for p -typical formal groups.

All formal groups will be commutative. All rings will be commutative with unit element. \mathbb{Z} stands for the integers, $\mathbb{Z}_{(p)}$ for the integers localized at p and \mathbb{Q} for the rational numbers; \mathbb{N} denotes the natural numbers, $\mathbb{N} = \{1, 2, 3, \dots\}$. If $F(X, Y)$ is a formal group over a ring A and $\phi : A \rightarrow B$ a ring homomorphism then $F^\phi(X, Y)$ denotes the formal group obtained from $F(X, Y)$ by applying ϕ to its coefficients.

2. CONSTRUCTIONS AND STATEMENT OF MAIN THEOREMS.

2.1. A multiindex $\underline{n} = (n_1, \dots, n_m)$ is an m -tuple of integers ≥ 0 . Let $|\underline{n}| = n_1 + n_2 + \dots + n_m$. We shall only consider multiindices \underline{n} with $|\underline{n}| \geq 1$. We use $\underline{e}(i)$, $i = 1, \dots, m$ to denote the multiindex $(0, \dots, 0, 1, 0, \dots, 0)$ with 1 in the i -th place. If \underline{n} is a multiindex and $i \in \mathbb{N}$ then $i \underline{n}$ is the multiindex $i \underline{n} = (in_1, \dots, in_m)$. We use \underline{n}

to denote the set of all multiindices \underline{n} with $|\underline{n}| \geq 1$ and

$\underline{n} \neq p^r \underline{e}(i)$ for all $r = 1, 2, \dots; i = 1, \dots, m$ and prime numbers $p \in \underline{\mathbb{N}}$

2.2. If $g(X)$ is a power series over $A[U_1, U_2, \dots]$ and $n \in \underline{\mathbb{N}}$ then $g^{(n)}(X)$ denotes the power series obtained from $g(X)$ by replacing each U_i with U_i^n , $i = 1, 2, \dots$

2.3. Constructions.

Choose $m \in \underline{\mathbb{N}}$. Let $\underline{\mathbb{Z}}[V]$ be short for $\underline{\mathbb{Z}}[V_i(j, k); i = 1, 2, \dots; j, k = 1, \dots, m]$. We write V_i for the matrix $V_i(j, k)$, X for the column vector (X_1, \dots, X_m) and X^n , $n \in \underline{\mathbb{N}}$ for (X_1^n, \dots, X_m^n) . Choose a prime number p . With these notations we define the m -tuple of power series $f_V(X)$ with coefficients in $\underline{\mathbb{D}}[V]$ by

$$(2.3.1) \quad f_V(X) = X + \sum_{i=1}^{\infty} \frac{V_i}{p} f_V^{(p^i)}(X^{p^i})$$

and we define

$$(2.3.2) \quad F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y))$$

where $h^{-1}(X)$ is the inverse m -tuple of power series to $h(X)$; i.e.

$$h^{-1}(h(X)) = X = h(h^{-1}(X)).$$

Let $\underline{\mathbb{Z}}[V; T]$ be short for $\underline{\mathbb{Z}}[V_i(j, k), T_i(j, K); i = 1, 2, \dots; j, k = 1, \dots, m]$.

We define

$$(2.3.3) \quad f_{V, T}(X) = X + \sum_{i=1}^{\infty} T_i X^{p^i} + \sum_{i=1}^{\infty} \frac{V_i}{p} f_{V, T}^{(p^i)}(X^{p^i})$$

and

$$(2.3.4) \quad F_{V, T}(X, Y) = f_{V, T}^{-1}(f_{V, T}(X) + f_{V, T}(Y))$$

For each sequence (q_1, \dots, q_t) of powers of prime numbers, q_i a power of p_i , choose an integer $n(q_1, \dots, q_t)$ such that the following congruences are satisfied

$$(2.3.5) \quad \begin{aligned} n(q_1, \dots, q_t) &\equiv 1 \pmod{p_1^r} \text{ if } p_1 = p_2 = \dots = p_r \neq p_{r+1} \\ n(q_1, \dots, q_t) &\equiv 0 \pmod{p_2^{r-1}} \text{ if } p_1 \neq p_2 = \dots = p_r \neq p_{r+1} \end{aligned}$$

Let $\underline{\mathbb{Z}}[U]$ be short for $\underline{\mathbb{Z}}[U(i,n)]$; \underline{n} a multiindex with $|\underline{n}| \geq 2$, $i = 1, \dots, m$. We also define $U(i, \underline{e}(j)) = 0$ if $i \neq j$ and $U(i, \underline{e}(i)) = 1$. If q is a power of a prime number in $\underline{\mathbb{N}}$, we use U_q to denote the matrix $(U(i, q\underline{e}(j)))_{i,j}$ and if \underline{d} is a multiindex we use $U_{\underline{d}}$ to denote the column vector $(U(1, \underline{d}), \dots, U(m, \underline{d}))$. Finally $X^{\underline{n}} = X_1^{n_1} \dots X_m^{n_m}$ and if a is a vector $aX^{\underline{n}} = (a_1 X^{\underline{n}}, \dots, a_m X^{\underline{n}})$. We now define the column m -vectors $a_{\underline{n}}$ for all multiindices \underline{n} with $|\underline{n}| \geq 1$ as

$$(2.3.6) \quad a_{\underline{n}} = \sum_{(q_1, \dots, q_t, \underline{d})} \frac{n(q_1, \dots, q_t)}{p_1} \frac{n(q_2, \dots, q_t)}{p_2} \dots \frac{n(q_t)}{p_t} U_{q_1} U_{q_2}^{(q_1)} \dots U_{q_t}^{(q_1 \dots q_{t-1})} U_{\underline{d}}^{(q_1 \dots q_t)}$$

where the sum is over all sequences $(q_1, \dots, q_t, \underline{d})$ such that $q_1 \dots q_t \underline{d} = \underline{n}$, $\underline{d} \in \underline{D}$, q_i a power of a prime number p_i . NB $t = 0$ is allowed. We now define

$$(2.3.7) \quad h_U(X) = \sum_{|\underline{n}| \geq 1} a_{\underline{n}} X^{\underline{n}}, \quad H_U(X, Y) = h_U^{-1}(h_U(X) + h_U(Y))$$

and

$$(2.3.8) \quad \bar{h}_U(X) = h_U^\phi(X), \quad \bar{H}_U(X, Y) = H_U^\phi(X, Y)$$

where $\phi: \underline{\mathbb{Z}}[U] \rightarrow \underline{\mathbb{Z}}[U]$ is the homomorphism which takes $U(i, q\underline{e}(j))$ into itself for $i, j = 1, \dots, m$ and prime powers q , and which sends $U(i, \underline{n})$ to zero for all $\underline{n} \in \underline{E}$, $i = 1, \dots, m$, where $\underline{E} = \underline{D} \setminus \{\underline{e}(i) \mid i=1, \dots, m\}$

2.4. Integrality Theorem.

The formal power series $F_V(X, Y)$, $F_{V, T}(X, Y)$, $H_U(X, Y)$ and $\bar{H}_U(X, Y)$ have their coefficients respectively in $\underline{\mathbb{Z}}[V]$, $\underline{\mathbb{Z}}[V; T]$, $\underline{\mathbb{Z}}[U]$ and $\underline{\mathbb{Z}}[U]$.

2.5. Theorem (Universality of $H_U(X, Y)$).

$H_U(X, Y)$ is a universal m -dimensional formal group.

i.e. for every m -dimensional commutative formal group $F(X, Y)$ over a ring A there is unique homomorphism $\phi: \underline{\mathbb{Z}}[U] \rightarrow A$ such that

$$H_U^\phi(X, Y) = F(X, Y).$$

2.6. Theorem.

$H_U(X,Y)$ and $\bar{H}_U(X,Y)$ are strictly isomorphic over $\underline{\mathbb{Z}}[U]$.

2.7. Curves.

Let $F(X,Y)$ be an m -dimensional formal group over a ring A . A curve in $F(X,Y)$ is an m -tuple of power series $\gamma(Z)$ in one indeterminate Z with coefficients in A and zero constant terms. Two curves can be added by means of $F(X,Y)$ as follows $\gamma(Z) +_F \delta(Z) = F(\gamma(Z), \delta(Z))$. Let $n \in \underline{\mathbb{N}}$. One now defines a Frobenius operator $f_{\underline{\mathbb{Z}}_n}$ in exactly the same way as for one dimensional formal groups. I.e. formally we have that

$$(2.7.1) \quad (f_{\underline{\mathbb{Z}}_n} \gamma)(Z) = \gamma(\zeta_n Z^{1/n}) +_F \gamma(\zeta_n^2 Z^{1/n}) +_F \dots +_F \gamma(\zeta_n^n Z^{1/n})$$

where ζ_n is a primitive n -th root of unity. For a more precise definition, cf. [3].

2.8. More Dimensional p-typical Formal Groups.

Choose a prime number p . Let $F(X,Y)$ be a formal group over a ring A . A curve $\gamma(Z)$ is said to be p -typical in F if $(f_{\underline{\mathbb{Z}}_q}^F \gamma)(Z) = 0$ for all prime numbers $q \neq p$. We shall say that the formal group $F(X,Y)$ is p -typical if all curves of the form $\gamma(Z) = (Z^{p^{r_1}-1}, \dots, Z^{p^{r_m}-1})$, $r_i \in \mathbb{N} \cup \{0\}$ are p -typical.

If A is a characteristic zero ring, i.e. $A \rightarrow A \otimes_{\underline{\mathbb{Z}}} \mathbb{Q}$ is injective, and $f(X)$ is a logarithm for $F(X,Y)$ and $f(X)$ is of the form

$$(2.8.1) \quad f(X) = X + \sum_{i=1}^{\infty} \frac{c_i}{p^i} X^{p^i}$$

for certain matrices c_i with coefficients in A , then $F(X,Y)$ is a p -typical formal group, as is easily seen. The converse is also true; this follows from theorem 2.9 below.

2.9. Theorem.

$F_V(X,Y)$ is a universal p -typical formal group (of dimension m) for p -typical formal groups over $\underline{\mathbb{Z}}_{(p)}$ -algebras or characteristic zero rings.

I.e. for every p -typical formal group $G(X,Y)$ over a ring A which is a $\underline{\mathbb{Z}}_{(p)}$ -algebra or a characteristic zero ring there is a unique homomorphism $\phi: \underline{\mathbb{Z}}[V] \rightarrow A$ such that $F_V^\phi(X,Y) = G(X,Y)$.

Let $\kappa: \mathbb{Z}[V] \rightarrow \mathbb{Z}[U]$ be the injective homomorphism defined by $\kappa(V_i(j,k)) = U(j, p^i \underline{e}(k))$, and $\lambda: \mathbb{Z}[U] \rightarrow \mathbb{Z}_{(p)}[U]$ be the localization homomorphism.

2.10. Theorem.

The formal groups $F_V^{\lambda\kappa}(X,Y)$ and $H_U^\lambda(X,Y)$ are strictly isomorphic (over $\mathbb{Z}_{(p)}[U]$).

2.11. Corollary.

Every formal group over a $\mathbb{Z}_{(p)}$ -algebra is isomorphic to a p-typical formal group.

2.12. Theorem.

The formal groups $F_V(X,Y)$ and $F_{V,T}(X,Y)$ are strictly isomorphic over $\mathbb{Z}[V;T]$ and this isomorphism is universal for strict isomorphisms between p-typical formal groups over $\mathbb{Z}_{(p)}$ -algebras or characteristic zero rings.

2.13. Curvilinear Formal Groups.

If $\underline{k}, \underline{\ell}$ are multiindices of length m we define $\underline{k}\underline{\ell} = (k_1\ell_1, \dots, k_m\ell_m)$. Let $\underline{0}$ be the multiindex $\underline{0} = (0, \dots, 0)$. In [7] Lazard defines a formal group $F(X,Y)$ over a ring A to be curvilinear (curviligne) if

$$(2.13.1) \quad \|\underline{k}\|, \|\underline{\ell}\| \geq 1, \underline{k}\underline{\ell} = \underline{0} \Rightarrow a_{\underline{k}, \underline{\ell}}(i) = 0 \text{ for all } i = 1, \dots, m$$

where $F(X,Y) = (F(1)(X,Y), \dots, F(m)(X,Y)$ and $F(i)(X,Y) = X_i + Y_i + \sum a_{\underline{k}, \underline{\ell}}(i) X^{\underline{k}} Y^{\underline{\ell}}$

2.14. Let $\mathbb{Z}[R]$ be short for $\mathbb{Z}[R_i(j,k); i = 2, 3, \dots, j = 1, \dots, m, k = 1, \dots, m]$. Let $\theta: \mathbb{Z}[U] \rightarrow \mathbb{Z}[R]$ be the projection $\theta(U(i, \underline{d})) = 0$ unless \underline{d} is of the form $d\underline{e}(j)$ for some $d \in \mathbb{N}, d \geq 2, j \in \{1, \dots, m\}$, and $\iota(U(i, d\underline{e}(j))) = R_d(i, j)$.

Let $\iota: \mathbb{Z}[R] \rightarrow \mathbb{Z}[U]$ be the injection defined by $\iota(R_d(i, j)) = U(i, d\underline{e}(j))$. We define

$$(2.14.1) \quad h_R(X) = h_U^\theta(X), \quad H_R(X,Y) = H_U^\theta(X,Y)$$

2.15. Theorem.

$H_R(X,Y)$ is a curvilinear m -dimensional formal group over $\mathbb{Z}[R]$ and it is universal for curvilinear m -dimensional formal groups. The formal

groups $H_R^1(X,Y)$ and $H_U(X,Y)$ are strictly isomorphic over $\underline{\mathbb{Z}}[U]$.

2.16. Corollary.

Every formal group over a ring A is strictly isomorphic to a curvilinear formal group over A .

2.17. The formal group $H_R(X,Y)$ is the multidimensional analogue of the one dimensional universal formal group denoted $H_U(X,Y)$ in [4]. There is also a multidimensional curvilinear analogue of the universal one dimensional formal group $F_U(X,Y)$ of [4]. To obtain it choose $c(p,i)$, p a prime number, $i \in \underline{\mathbb{N}} \setminus \{1\}$ as in [4] and determine $n(i_1, \dots, i_s)$ for all sequences (i_1, \dots, i_s) , $i_j \in \underline{\mathbb{N}} \setminus \{1\}$ as in [4]. Let $d(i_1, \dots, i_s) = n(i_1, \dots, i_s)n(i_2, \dots, i_s) \dots n(i_s)v(i_1)^{-1}v(i_2)^{-1} \dots v(i_s)^{-1}$. Now define the matrices $b_i(R)$ as

$$(2.17.1) \quad b_i(R) = \sum_{(i_1, \dots, i_s)} d(i_1, \dots, i_s) R_{i_1}^{(i_1)} R_{i_2}^{(i_1 \dots i_{s-1})} \dots R_{i_s}^{(i_1 \dots i_{s-1})}$$

$$i = 2, 3, \dots$$

where R_k is the matrix $(R_k(j,\ell))_{j\ell}$ and the sum is over all sequences (i_1, \dots, i_s) , $i_j \in \underline{\mathbb{N}} \setminus \{1\}$, $s \geq 1$, such that $i_1, \dots, i_s = i$.

We put

$$(2.17.2) \quad f_R(X) = \sum_{i=1}^{\infty} b_i(R) X^i, \quad b_1(R) = I_m, \text{ the } m \times m \text{ identity matrix}$$

$$(2.17.3) \quad F_R(X,Y) = f_R^{-1}(f_R(X) + f_R(Y))$$

2.18. Theorem.

$F_R(X,Y)$ is an m -dimensional curvilinear formal group over $\underline{\mathbb{Z}}[R]$ and it is universal for m -dimensional curvilinear formal groups. $F_R(X,Y)$ is strictly isomorphic to $H_R(X,Y)$ over $\underline{\mathbb{Z}}[R]$.

2.19. Because the $d(i_1, \dots, i_s)$ in (2.17.1) have been chosen as in [4] we find exactly as in [4] the following formula between the R_i and the $b_i(R)$.

$$(2.19.1) \quad v(n)b_n(R) = R_n + \sum_{\substack{d|n \\ d \neq 1, n}} \rho(n,d)b_{n/d}(R)R_d^{(n/d)}$$

3. PROOF OF THE INTEGRALITY THEOREMS 2.4.

3.1. Let $g_1(X)$ and $g_2(X)$ be m -tuples of power series over $\underline{\mathbb{Z}}(p)[V;W]$ where W is short for an additional set of indeterminates and V is as in 2.3.

Suppose that $g_j(X) = X + \dots$, $j = 1, 2$, has its coefficients in $\underline{\mathbb{Z}}(p)[V;W]$;

$$(3.1.1) \quad f_j(X) = g_j(X) + \sum_{i=1}^{\infty} \frac{v_i}{p^j} (p^i) (X^{p^i})$$

Functional equation lemma.

(i) $F(X,Y) = f_1^{-1}(f_1(X) + f_1(Y))$ has its coefficients in $\underline{\mathbb{Z}}(p)[V;W]$

(ii) There is a $h_1(X)$ with coefficients in $\underline{\mathbb{Z}}(p)[V,W]$ such that $f_1(h_1(X)) = f_2(X)$

(iii) If $h_2(X)$ is of the form $h_2(X) = X + \dots$. Then $f_1(h_2(X))$ satisfies a functional equation of the form 3.1.1.

The proofs of these facts are completely analogous to the proofs of the corresponding lemmas in [3].

3.2. Choose numbers $n(q_1, \dots, q_t)$ for all sequences of powers of prime numbers (q_1, \dots, q_t) such that (2.3.5) is satisfied. Let

$$(3.2.1) \quad d(q_1, \dots, q_t) = \frac{n(q_1, \dots, q_t)}{p_1} \cdot \frac{n(q_2, \dots, q_t)}{p_2} \cdot \dots \cdot \frac{n(q_t)}{p_t}$$

where q_i is a power of the prime number p_i .

Lemma (i) If $p_1 = \dots = p_r \neq p_{r+1}$ then $p_1^r d(q_1, \dots, q_t) \in \underline{\mathbb{Z}}$

(ii) $d(q_1, \dots, q_t) - p_1^{-1} d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}(p_1)$

Proof. We prove (i) by induction. The case $t = 1$ is trivial. If $r = 1$,

Let $p_2 = p_3 = \dots = p_s \neq p_{s+1}$. Then $p_2^{s-1} d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}$ and $n(q_1, \dots, q_t) \equiv 0 \pmod{p_2^{s-1}}$. Therefore $p_1 d(q_1, \dots, q_t) =$

$n(q_1, \dots, q_t) d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}$. Now let $r > 1$, then $p_1^{r-1} d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}$.

Hence $p_1^r d(q_1, \dots, q_t) = n(q_1, \dots, q_t) p_1^{r-1} d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}$.

To prove (ii) we distinguish two cases. If $r = 1$ then $d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}_{(p_1)}$

by (i) and hence $d(q_1, \dots, q_t) - p_1^{-1} d(q_2, \dots, q_t) =$

$p_1^{-1} (n(q_1, \dots, q_t) - 1) d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}_{(p_1)}$, because $n(q_1, q_2, \dots, q_t) \equiv 1 \pmod{p_1}$

if $p_1 \neq p_2$. If $p_1 = p_2 = \dots = p_r \neq p_{r+1}$ with $r > 1$, then

$p_1^{r-1} d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}$ by (i) and hence $d(q_1, \dots, q_t) - p_1^{-1} d(q_2, \dots, q_t) =$
 $p_1^{-1} (n(q_1, \dots, q_t) - 1) d(q_2, \dots, q_t) \in \underline{\mathbb{Z}}_{(p_1)}$ because $n(q_1, \dots, q_t) \equiv 1 \pmod{p_1^r}$
 in this case.

3.3. Lemma.

The formal power series $h_U(X)$ satisfies a functional equation of the form

$$(3.3.1) \quad h_U(X) = g_p(X) + \sum_{i=1}^{\infty} \frac{p^i}{p} h_U^{(p^i)}(X^{p^i})$$

with $g_p(X) = X + \dots \in \underline{\mathbb{Z}}_{(p)}[U][[X]]$ for all prime numbers p .

This follows from (2.3.6) and lemma (3.2) (ii) above.

3.4. Proof of Theorem 2.4 (Integrality Theorems)

By lemma 3.3 and lemma 3.1 (i) we have that $H_U(X, Y)$ is in $\underline{\mathbb{Z}}_{(p)}[U][[X, Y]]$

for all prime numbers p . Hence $H_U(X, Y) \in \underline{\mathbb{Z}}[U][[X, Y]]$. The m -tuple of power series $\bar{H}_U(X, Y)$ is obtained by setting certain $U(i, \underline{d})$ equal to zero in $H_U(X, Y)$, hence also $\bar{H}_U(X, Y) \in \underline{\mathbb{Z}}[U][[X, Y]]$.

The power series $f_V(X)$ and $f_{V, T}(X)$ satisfy by their definition a functional equation of type (3.1.1). Moreover the only denominators occurring in $f_V(X)$ and $f_{V, T}(X)$ are powers of p . Hence $F_V(X, Y)$ and $F_{V, T}(X, Y)$ can only have denominators which are powers of p . Now apply lemma 3.1 (i) again, to conclude that $F_V(X, Y)$ and $F_{V, T}(X, Y)$ are in $\underline{\mathbb{Z}}[V][[X, Y]]$ and $\underline{\mathbb{Z}}[V; T][[X, Y]]$ respectively.

4. A LITTLE BIT OF MULTIDIMENSIONAL BINOMIAL COEFFICIENT ARITHMETIC.

4.1. Let \underline{n} be a multiindex of length m . Recall that $||\underline{n}|| = n_1 + \dots + n_m$, $n_i \in \underline{\mathbb{N}} \cup \{0\}$. We write $\underline{k} \leq \underline{n}$ if $k_i \leq n_i$, $i = 1, \dots, m$ and $\underline{k} < \underline{n}$ if $\underline{k} \leq \underline{n}$ and $||\underline{k}|| < ||\underline{n}||$. If $\underline{k} \leq \underline{n}$ we define

$$(4.1.1) \quad \binom{\underline{n}}{\underline{k}} = \binom{n_1}{k_1} \binom{n_2}{k_2} \dots \binom{n_m}{k_m}$$

We also define $v(\underline{n}) = 1$ unless \underline{n} is of the form $\underline{n} = p^r \underline{e}(j)$ for some $r \in \mathbb{N}$, $j \in \{1, \dots, m\}$, and prime number p , then $v(p^r \underline{e}(j)) = p$. Then one has that

$$(4.1.2) \quad v(\underline{n}) = \text{g. c. d.} \left\{ \binom{\underline{n}}{\underline{k}}; \underline{0} < \underline{k} < \underline{n} \right\}$$

where $\underline{0}$ stands for the multiindex $(0, 0, \dots, 0)$.

This is clear if \underline{n} is of the form $\underline{n} = n \underline{e}(j)$. And if \underline{n} is such that at least two different n_i are > 0 , let i_1 be the smallest number such that $n_{i_1} \neq 0$. Take $\underline{k} = n_{i_1} \underline{e}(i_1)$. Then $\binom{\underline{n}}{\underline{k}} = 1$.

4.2. Let $n \in \mathbb{N}$, $n \geq 2$. Choose $\lambda_{n,1}, \dots, \lambda_{n,n-1}$ such that

$$\lambda_{n,1} \binom{n}{1} + \dots + \lambda_{n,n-1} \binom{n}{n-1} = v(n). \text{ If } \underline{n} \text{ is of the form } \underline{n} = n \underline{e}(j),$$

then if $\underline{0} < \underline{k} < \underline{n}$, $\underline{k} = k \underline{e}(j)$ for some $0 < k < n$. We put $\lambda(\underline{n}, \underline{k}) = \lambda_{n,k}$

for all $\underline{0} < \underline{k} < \underline{n}$ in this case. If \underline{n} is not of the form $\underline{n} = n \underline{e}(j)$, let i_1 be the smallest natural number such that $n_{i_1} \neq 0$. For these \underline{n} we take

$$\lambda(\underline{n}, \underline{k}) = 0 \text{ if } \underline{k} \neq (0, \dots, 0, n_{i_1}, 0, \dots, 0), \underline{0} < \underline{k} < \underline{n} \text{ and } \lambda(\underline{n}, \underline{k}) = 1 \text{ if}$$

$$\underline{k} = (0, 0, \dots, 0, n_{i_1}, 0, \dots, 0). \text{ Then we have of course}$$

$$(4.2.1) \quad \sum_{\underline{0} < \underline{k} < \underline{n}} \lambda(\underline{n}, \underline{k}) \binom{\underline{n}}{\underline{k}} = v(\underline{n})$$

4.3. Lemma.

Let \underline{n} be a multiindex, $|\underline{n}| \geq 2$. For each $\underline{0} < \underline{k} < \underline{n}$ let $X(\underline{k})$ be an indeterminate and let $X(\underline{k}) = X(\underline{n} - \underline{k})$. Then every $X(\underline{k})$ can be written as an integral linear combination of the expressions

$$(4.2.2) \quad \sum_{\underline{0} < \underline{k} < \underline{n}} \lambda(\underline{n}, \underline{k}) X(\underline{k})$$

$$(4.2.3) \quad \binom{\underline{k} + \underline{\ell}}{\underline{\ell}} X(\underline{k} + \underline{\ell}) - \binom{\underline{\ell} + \underline{m}}{\underline{m}} X(\underline{\ell} + \underline{m}) \quad \underline{k} + \underline{\ell} + \underline{m} = \underline{n}, \underline{k}, \underline{\ell}, \underline{m} > \underline{0}$$

where the $\lambda(\underline{n}, \underline{k})$ are as above

Proof. If \underline{n} is of the form $\underline{n} = n \underline{e}(j)$, this is the binomial coefficient lemma of [4] section 4. If \underline{n} is not of the form $n \underline{e}(j)$ let i be the smallest natural number such that $n_i \neq 0$. Then (4.2.2) is equal to $X(n_i \underline{e}(i))$

For all $0 < k < n_i$ take $\underline{k} = k \underline{e}(i)$, $\underline{\ell} = (n_i - k) \underline{e}(i)$, $\underline{m} = \underline{n} - \underline{k} - \underline{\ell}$. Then $X(\underline{k} + \underline{\ell}) = X(n_i \underline{e}(i))$, $X(\underline{\ell} + \underline{m}) = X(\underline{k}) = X(k \underline{e}(i))$ and $\binom{\underline{\ell} + \underline{m}}{\underline{m}} = 1$, so that we have written all $X(k \underline{e}(i))$ with $0 < k < n_i$ as linear combinations of (4.2.2) and (4.2.3). Now let $\underline{j} = (j_1, \dots, j_m)$ be a multiindex with $0 < \underline{j} < \underline{n}$, $0 < j_i \leq n_i$ and $j_i \neq j_i \underline{e}(i)$.

Take $\underline{k} = j_i \underline{e}_i$, $\underline{\ell} = \underline{j} - \underline{k}$, $\underline{m} = \underline{n} - \underline{k} - \underline{\ell}$. Then $\binom{\underline{k} + \underline{\ell}}{\underline{\ell}} = 1$, $X(\underline{k} + \underline{\ell}) = X(\underline{j})$, $X(\underline{\ell} + \underline{m}) = X(\underline{k}) = X(j_i \underline{e}_i)$. So that we can write all $X(\underline{k})$ with $0 < \underline{j} < \underline{n}$ such that $j_i < n_i$ as linear combinations of (4.2.2) and (4.2.3). But if $0 < \underline{j} < \underline{n}$ either \underline{j} or $\underline{n} - \underline{j}$ has its i -th component **greater than 0** and $X(\underline{j}) = X(\underline{n} - \underline{j})$.

q.e.d.

5. PROOF OF THE UNIVERSALITY THEOREMS.

5.1. Let $n \in \mathbb{N}$. We write $h_{U(n)}(X)$ and $H_{U(n)}(X, Y)$ for the m -tuples of formal power series obtained from $h_U(X)$ and $H_U(X, Y)$ by substituting 0 for all $U(i, \underline{d})$ with $||\underline{d}|| > n$. Then we have

$$(5.1.1) \quad h_U(X) \equiv h_{U(n)}(X) + \Gamma_{n+1}(X) \pmod{\text{(total degree } n+2)}$$

where $\Gamma_{n+1}(X)$ is the following m -tuple of homogeneous forms of degree $n + 1$ in X_1, \dots, X_m

$$(5.1.2) \quad \Gamma_{n+1}(X) = \sum_{||\underline{d}||=n+1} v(\underline{d})^{-1} U_{\underline{d}} X^{\underline{d}}$$

where the notation is as in (2.3). This follows immediately from (2.3.6). It follows that we have for $H_U(X, Y)$ that

$$(5.1.3) \quad H_U(X) \equiv H_{U(n)}(X) + \Gamma_{n+1}(X) + \Gamma_{n+1}(Y) - \Gamma_{n+1}(X+Y)$$

mod (total degree $n+2$)

where Γ_{n+1} is as in 5.1.2.

5.2. Let

$$(5.2.1) \quad H_U(X,Y) = (H_U(1)(X,Y), \dots, H_U(m)(X,Y))$$

and write

$$(5.2.2) \quad H_U(i)(X,Y) = X_i + Y_i + \sum_{\substack{||\underline{k}||, ||\underline{\ell}|| \geq 1}} e_{\underline{k}, \underline{\ell}}(i) X^{\underline{k}} Y^{\underline{\ell}}$$

Let for all \underline{d} with $||\underline{d}|| \geq 2$

$$(5.2.3) \quad y(i, \underline{d}) = \sum_{\underline{0} < \underline{k} < \underline{d}} \lambda(\underline{d}, \underline{k}) e_{\underline{k}, \underline{d}-\underline{k}}(i)$$

where the $\lambda(\underline{d}, \underline{k})$ are as in 4.2.

Lemma. The $y(i, \underline{d})$ are a polynomial basis for $\mathbb{Z}[U]$.

I.e. every element of $\mathbb{Z}[U]$ can be written uniquely as a polynomial in the $y(i, \underline{d})$.

This follows from (5.1.3) together with (4.2.1).

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

Let $G(X,Y)$ be a commutative m -dimensional formal group over a ring A . Write $G(X,Y) = (G(i)(X,Y), \dots, G(m)(X,Y))$ and let

$$(5.3.1) \quad G(i)(X,Y) = X_i + Y_i + \sum_{\substack{||\underline{k}||, ||\underline{\ell}|| \geq 1}} a_{\underline{k}, \underline{\ell}}(i) X^{\underline{k}} Y^{\underline{\ell}}$$

Now define the homomorphism $\phi : \mathbb{Z}[U] \rightarrow A$ by the requirement that

$$(5.3.2) \quad \phi(y(i, \underline{d})) = \sum_{\underline{0} < \underline{k} < \underline{d}} \lambda(\underline{d}, \underline{k}) a_{\underline{k}, \underline{d}-\underline{k}}(i)$$

This is a well defined homomorphism because of lemma 5.2. And certainly ϕ is the only possible homomorphism such that $H_U^\phi(X,Y) = G(X,Y)$. It

These few pages explain
~~the~~ pages 12-14 of the
 previous manuscript "Construction
 of formal group \mathbb{F} " (by H. Hazewinkel)

remains, therefore, to prove that $\phi(e_{\underline{k}, \underline{l}}(i)) = a_{\underline{k}, \underline{l}}(i)$ for all $\underline{k}, \underline{l}$ with $||\underline{k}||, ||\underline{l}|| \geq 1$. The case $||\underline{k} + \underline{l}|| = 2$ follows directly from (5.3.2) because both $G(X, Y)$ and $H_U(X, Y)$ are commutative, i.e. $e_{\underline{k}, \underline{l}}(i) = e_{\underline{l}, \underline{k}}(i)$ and $a_{\underline{k}, \underline{l}}(i) = a_{\underline{l}, \underline{k}}(i)$.

Associativity of $H_U(X, Y)$ and $G(X, Y)$ means that the coefficients $e_{\underline{k}, \underline{l}}(i), a_{\underline{k}, \underline{l}}(i)$ must satisfy some universal relations. These are easily seen to be of the form

$$(5.3.3) \quad e_{\underline{k} + \underline{l}, \underline{m}}(i) \binom{\underline{k} + \underline{l}}{\underline{k}} - e_{\underline{k}, \underline{l} + \underline{m}}(i) \binom{\underline{l} + \underline{m}}{\underline{m}} = P_{\underline{k}, \underline{l}, \underline{m}, i}(e_{\underline{s}, \underline{t}})$$

$$a_{\underline{k} + \underline{l}, \underline{m}}(i) \binom{\underline{k} + \underline{l}}{\underline{k}} - a_{\underline{k}, \underline{l} + \underline{m}}(i) \binom{\underline{l} + \underline{m}}{\underline{m}} = P_{\underline{k}, \underline{l}, \underline{m}, i}(a_{\underline{s}, \underline{t}})$$

where the $P_{\underline{k}, \underline{l}, \underline{m}, i}$ are certain universal polynomials in the $e_{\underline{s}, \underline{t}}$ (resp. $a_{\underline{s}, \underline{t}}$) with $||\underline{s} + \underline{t}|| < ||\underline{k} + \underline{l} + \underline{m}||$. Now use induction on $||\underline{k} + \underline{l}||$ and lemma 4.3 to prove that $\phi(e_{\underline{k}, \underline{l}}(i)) = a_{\underline{k}, \underline{l}}(i)$ for all $\underline{k}, \underline{l}, i$.

q.e.d.

5.4. Corollary. (Lazard's comparison lemma, cf [6]).

Let $F(X, Y), G(X, Y)$ be two m -dimensional formal groups over a ring A , and suppose that $F(X, Y) \equiv G(X, Y) \pmod{(\text{total degree } n)}$. Then there is an m -tuple of homogeneous forms Γ of degree n with coefficients in A and a $m \times m$ matrix M with coefficients in A such that

$$(5.4.1) \quad F(X, Y) \equiv G(X, Y) - \Gamma(X) + \Gamma(X+Y) - \Gamma(Y) + M(v(n))^{-1}((X+Y)^n - X^n - Y^n) \pmod{(\text{degree } n+1)}$$

If one adds the restriction that $\Gamma(X)$ may contain no terms of the form aX_1^n , $a \in A$ then the Γ and M in (5.4.1) are unique.

This follows from theorem 2.5 and (5.1.2).

5.5. Proof of theorem 2.9. Let $F(X,Y)$ be a p -typical formal group over A . Then there is a unique homomorphism

$\phi: \underline{\mathbb{Z}}[U] \rightarrow A$ such that $H_U^\phi(X,Y) = F(X,Y)$. We are going to prove that $\phi(U(i, \underline{n})) = 0$ for all multiindices \underline{n} which are not of the form $p^i \underline{e}(j)$.

Suppose we have done this. Then ϕ factors uniquely through

$\underline{\mathbb{Z}}[U] \rightarrow \underline{\mathbb{Z}}[V]$, $U(j, p^i \underline{e}(k)) \mapsto V_i(j,k)$ and $U(i, \underline{d}) \mapsto 0$ for all other (i, \underline{d}) , to give a homomorphism $\psi: \underline{\mathbb{Z}}[V] \rightarrow A$ such that $F_V^\psi(X,Y) = F(X,Y)$.

(This last fact follows immediately from a comparison of $f_V(X)$ with $h_U(X)$). Moreover ψ is certainly unique. For otherwise there would be two homomorphisms $\underline{\mathbb{Z}}[U] \rightarrow A$ (both zero on the $U(i, \underline{d})$ with $\underline{d} \neq p^r \underline{e}(j)$) taking $H_U(X,Y)$ into $F(X,Y)$.

It therefore only remains to prove that $\phi(U(i, \underline{n})) = 0$ if \underline{n} is not of the form $p^r \underline{e}(j)$. To prove this we first do two universal calculations.

5.6. Lemma. Let $n \in \underline{\mathbb{N}}$ and suppose that $v(n) \neq p$. Let $h_n(X)$ and $H_n(X,Y)$ be the power series over $\underline{\mathbb{Q}}[U]$ and $\underline{\mathbb{Z}}[U]$ respectively, obtained by substituting zero for all $U_i(j,k) = U(j, i \underline{e}(k))$ with $i < n$, $v(i) \neq p$, $j, k \in \{1, \dots, m\}$. Then for all prime numbers $q \neq p$ which divide n we have in the group of curves in $H_n(X,Y)$ over $\underline{\mathbb{Z}}[U]$.

$$\sum_{\underline{e}} \delta_i(t) = q^{v(n)} U_{n \underline{e}(i)} t^{n/q} \pmod{(\text{degree } q^{-1}n+1)}$$

where $\delta_i(t)$ is the curve $(0, \dots, 0, t, 0, \dots, 0)$ with the t in the i -th spot.

Proof. It follows immediately from the definition of $h_U(X)$ in 2.3 above that $h_n(\delta_i(t))$ is of the form

$$(5.6.1) \quad h_n(\delta_i(t)) = \sum b_i t^{p^i} + U_{n \underline{e}(i)} t^n$$

because the coefficients of the $X^{\underline{n}}$ for \underline{n} of the form $n \underline{e}(j)$ do not involve any $U(i, \underline{d})$ with $\underline{d} = (d_1, \dots, d_m)$ such that more than one of the d_j is nonzero.

The lemma follows immediately from (5.6.1).

The second universal calculation which we need involves lexicographic degrees.

5.7. Lexicographic degree. Let $\underline{n}, \underline{k}$ be two multiindices of length m .

We shall write $\underline{n} <_{\ell} \underline{k}$ iff $(n_1 < k_1)$ or $(n_1 = k_1 \text{ and } n_2 < k_2)$ or ...

or $(n_1 = k_1, \dots, n_{m-1} = k_{m-1} \text{ and } n_m < k_m)$. Let \underline{n} be a multiindex of length m , and suppose that at least two of the n_j , $j \in \{1, \dots, m\}$ are nonzero. Then there exist $r_1, \dots, r_m \in \mathbb{N}$ such that

- (i) $\bar{n} = n_1 p^{r_1} + \dots + n_m p^{r_m}$ is divisible by a prime number different from p .
- (ii) if $\underline{n} <_{\ell} \underline{k}$ then $\bar{n} < \bar{k} = k_1 p^{r_1} + \dots + k_m p^{r_m}$.

5.8. Lemma. Let $\underline{n} = (n_1, \dots, n_m)$ be a multiindex such that at least two of the n_j are nonzero. Let $h_{\underline{n}}(X)$ and $H_{\underline{n}}(X, Y)$ be the formal power series obtained from $h_U(X)$ and $H_U(X, Y)$ by substituting zero for all $U_i(j, k) = U(j, i_{\underline{n}}(k))$ with $j, k \in \{1, \dots, m\}$ with $v(i) \neq p$ and by also substituting zero for all $U(j, \underline{d})$, $j \in \{1, \dots, m\}$ for which $\underline{d} <_{\ell} \underline{n}$, $v(\underline{d}) \neq p$ and $|\underline{d}| > 1$. Let r_1, \dots, r_m be such that (i) and (ii) of 5.7 hold. Then for all prime numbers q dividing \bar{n} it follows that

$$f_{\underline{n}}(t^{p^{r_1}}, \dots, t^{p^{r_m}}) \equiv q U_{\bar{n}} t^{\bar{n}/q} \pmod{(\text{degree } \bar{n}/q + 1)}$$

Proof. It follows immediately from the definition of $h_U(X)$ in 2.3 above that for $\underline{k} <_{\ell} \underline{n}$ and $v(\underline{k}) \neq p$

$$a_{\underline{k}}(U) \equiv 0 \pmod{(U_i(j, k), U(\ell, \underline{d}) \mid v(i) \neq p, v(\underline{d}) \neq p, \underline{d} <_{\ell} \underline{n}, |\underline{d}| > 1)}$$

It follows also that

$$a_{\underline{n}}(U) \equiv U_{\bar{n}} \pmod{(U_i(j, k), U(\ell, \underline{d}) \mid v(i) \neq p, v(\underline{d}) \neq p, \underline{d} <_{\ell} \underline{n}, |\underline{d}| > 1)}$$

It follows that $h_{\underline{n}}(t^{p^{r_1}}, \dots, t^{p^{r_m}})$ is of the form

$$(5.8.1) \quad h_{\underline{n}}(t^{p^{r_1}}, \dots, t^{p^{r_m}}) = \sum b_i t^{p^i} + U_{\bar{n}} t^{\bar{n}} \pmod{(\text{degree } \bar{n} + 1)}$$

The lemma follows immediately from (5.8.1).

5.9. Proof of theorem 2.9 (conclusion). It is now easy to finish the proof of theorem 2.9. We first show with induction that $\phi(U_{\underline{n}}(j, k)) = 0$ for all \underline{n} for which $v(\underline{n}) \neq p$. Suppose we have shown this for all $\underline{r} < \underline{n}$, for which $v(\underline{r}) \neq p$. If $v(\underline{n}) = p$ the induction step is trivial. If $v(\underline{n}) \neq p$, let q be a prime number $\neq p$ which divides \bar{n} . Let $i \in \{1, \dots, m\}$. Then, by lemma 5.6 (and the functoriality of $f_{\underline{n}}^q$), we have in the group of curves of G over A

$$\underline{f}_{\underline{q}} \delta_i(t) \equiv q\nu(n)^{-1} (U_{\underline{n}\underline{e}(i)}) t^{n/q} \pmod{\text{degree } n/q + 1}$$

Now by hypothesis $\underline{f}_{\underline{q}} \delta_i(t) = 0$; hence $\phi(U_{\underline{n}\underline{e}(i)}) = 0$ because A is a $\underline{\mathbb{Z}}_{(p)}$ -algebra or a characteristic zero ring.

Next we show that also $\phi(U(i, \underline{d})) = 0$ for all $\underline{d} = (d_1, \dots, d_n)$ for which two or more of the d_j are nonzero. Suppose this is not the case. Let \underline{n} be the lexicographically smallest multiindex among these for which $\phi(U_{\underline{d}}) \neq 0$. Choose r_1, \dots, r_m such that (i) and (ii) of 5.7 hold. Let q be a prime number $\neq p$ which divides \bar{n} . Then we have by lemma 5.8

$$\underline{f}_{\underline{q}}(t^{p^{r_1}}, \dots, t^{p^{r_m}}) \equiv q\phi(U_{\underline{n}}) t^{\bar{n}/q} \pmod{\text{degree } \bar{n}/q + 1}$$

But, by hypothesis, $\underline{f}_{\underline{q}}$ of such curves is zero; a contradiction because A is a characteristic zero ring or a $\underline{\mathbb{Z}}_{(p)}$ -algebra. This finishes the proof of theorem 2.9.

6. ISOMORPHISM THEOREMS.

6.1. Proof of Theorems 2.6 and 2.10 and Part of Theorem 2.12.

These theorems are proved in the standard way. The logarithms of $\bar{H}_U(X, Y)$ and $H_U(X, Y)$ both satisfy functional equations of type (3.1.1)

for all prime numbers p (both with U_i instead of V_i). Now apply

part (ii) of the functional equation lemma to conclude that

$$h_U^{-1}(\bar{h}_U(x)) \in \underline{\mathbb{Z}}_{(p)}[U][[X]] \text{ for all prime numbers } p, \text{ hence}$$

$$h_U^{-1}(\bar{h}_U(x)) \in \underline{\mathbb{Z}}[U][[X]].$$

Similarly the logarithms of $F_V(X,Y)$ and $F_{V,T}(X,Y)$ both satisfy functional equations of type (3.1.1) for the fixed prime number p .

Hence $F_V(X,Y)$ and $F_{V,T}(X,Y)$ are strictly isomorphic over $\underline{\mathbb{Z}}_{(p)}[V,T]$. But the only denominators which can occur in $f_V^{-1}(f_{V,T}(X))$ are powers of p . Hence the isomorphism is actually over $\underline{\mathbb{Z}}[V,T]$.

Finally the logarithms of $F_V^{\lambda\kappa}(X,Y)$ and $H_U^\lambda(X,Y)$ also both satisfy functional equations of type (3.1.1) for the (fixed) prime number p (both with U_i instead of V_i). Hence $F_V^{\lambda\kappa}(X,Y)$ and $H_U^\lambda(X,Y)$ are strictly isomorphic over $\underline{\mathbb{Z}}_{(p)}[U]$.

6.2. Lemma.

Let $\gamma(Z)$ and $\delta(Z)$ be two p -typical curves in a formal group $F(X,Y)$ over a ring A , which is either a $\underline{\mathbb{Z}}_{(p)}$ -algebra or a characteristic zero ring. Then if $\gamma(Z) \equiv \delta(Z) \pmod{(\text{degree } p^n)}$, we have $\gamma(Z) \equiv \delta(Z) \pmod{(\text{degree } n+1)}$ unless n is a power of the prime p .

Proof. Let n be not a power of the prime number p . Let $q \neq p$ be a prime number dividing n . There is a unique vector $a \in A$ such that

$$\gamma(Z) \equiv \delta(Z) + Z^n a \pmod{(\text{degree } n+1)}$$

Applying f_q to this we find, because $f_q \gamma(Z) = f_q \delta(Z)$, that $aq = 0$.

As A is a characteristic 0 ring or a $\underline{\mathbb{Z}}_{(p)}$ -algebra it follows that $a = 0$.

6.3. Lemma.

Let $\alpha: F(X,Y) \rightarrow G(X,Y)$ be an isomorphism of formal groups, and let $G(X,Y)$ be a p -typical formal group. Then $\alpha^{-1}(\gamma(Z))$ is a p -typical curve in $F(X,Y)$ for all p -typical curves $\gamma(Z)$ in $G(X,Y)$.

This is immediate because $\alpha(\delta_1(Z)) +_G \alpha(\delta_2(Z)) = \alpha(\delta_1(Z) +_F \delta_2(Z))$.

6.4. Let $\underline{\mathbb{Z}}[U;S]$ be short for $\underline{\mathbb{Z}}[U(i,\underline{d}); S(i,\underline{d}); i = 1, \dots, m, ||\underline{d}|| \geq 2]$.

Let $d(q_1, \dots, q_t) = n(q_1, \dots, q_t)n(q_2, \dots, q_t) \dots n(q_t)p_1^{-1}p_2^{-1} \dots p_t^{-1}$,

where the $n(q_1, \dots, q_t)$ are as in 2.3. Let $U_{\underline{q}}, S_{\underline{q}}$ denote the matrices $(U(i, \underline{q}_{\underline{j}}))_{i,j}, S(i, \underline{q}_{\underline{k}})_{i,j}$.

Let $U(i, \underline{e}(j)) = 0 = S(i, \underline{e}(j))$ if $i \neq j$ and $U(i, \underline{e}(i)) = 1 = S(i, \underline{e}(i))$.

Finally let $U_{\underline{d}}, S_{\underline{d}}$ be the column vectors $(U(1, \underline{d}), \dots, U(m, \underline{d}), (S(1, \underline{d}), \dots, S(m, \underline{d})))$.

We now define for all multiindices $\underline{n}, ||\underline{n}|| \geq 1$

$$(6.4.1) \quad a_{\underline{n}}(U;S) = \sum_{(q_1, \dots, q_t, \underline{d})} d(q_1, \dots, q_t) U_{q_1}^{(q_1)} U_{q_2}^{(q_2)} \dots \\ \sum_{\underline{d} \in \underline{\mathbb{D}}} \dots U_{q_t}^{(q_1, \dots, q_{t-1})} (U_{\underline{d}}^{(q_1, \dots, q_t)} + S_{\underline{d}}^{(q_1, \dots, q_t)})$$

$$+ \sum_{(q_1, \dots, q_t, \underline{d})} d(q_1, \dots, q_t) U_{q_1}^{(q_1)} U_{q_2}^{(q_1 \dots q_{t-2})} \dots U_{q_{t-1}}^{(q_1 \dots q_{t-2})} \\ ||\underline{d}|| = 1$$

$$(U_{q_t}^{(q_1 \dots q_{t-1} + p_t S_{q_t}^{(q_1 \dots q_{t-1})})} U_{\underline{d}}^{(q_1 \dots q_{t-1})})$$

where the sums are over all sequences $(q_1, \dots, q_t, \underline{d})$, $q_i = p_i^{r_i}$, $r_i \in \mathbb{N}$, p_i a prime number, $q_1, \dots, q_t, \underline{d} = n$, $||\underline{d}|| \geq 1$.

(NB $t = 0$ is allowed). Let

$$(6.4.2) \quad h_{U,S}(X) = \sum_{||\underline{n}|| \geq 1} a_{\underline{n}} X^{\underline{n}} \quad H_{U,S}(X,Y) = h_{U,S}^{-1}(h_{U,S}(X) + h_{U,S}(Y))$$

6.5. Proposition.

$H_{U,S}(X,Y)$ is a formal group over $\underline{\mathbb{Z}}[U;S]$ and it is strictly isomorphic over $\underline{\mathbb{Z}}[U,S]$ to the formal group $H_U(X,Y)$ of (2.3.7).

This is proved in the usual way by means of the functional equation

lemma. The strict isomorphism from $H_U(X,Y)$ to $H_{U,S}(X,Y)$ is

$h_{U,S}^{-1}(h_U(X)) = \alpha_{U,S}(X)$. Let $\alpha_{U,S}(n)(X)$ stand for the power series

obtained from $\alpha_U(X)$ by substituting zero for all $S(i, \underline{d})$ with $||\underline{d}|| \geq n$.

Then one has immediately from (6.4.1) that

$$(6.5.1) \quad \alpha_{U,S}(X) \equiv \alpha_{U,S(n)}(X) + \sum_{\|\underline{n}\|=n} S_{\underline{n}} X^{\underline{n}} \pmod{\text{degree } n+1}$$

Using this one proves easily (in the same way as the corresponding theorem is proved in the one dimensional case in [4]):

6.6. Theorem.

The triple $(H_U(X,Y), \alpha_{U,S}(X), H_{U,S}(X,Y))$ is universal for triples consisting of two formal groups and a strict isomorphism between them.

6.7. Proof of theorem 2.12.

That $F_V(X,Y)$ and $F_{V,T}(X,Y)$ are strictly isomorphic has already been shown in 6.1 above. Now let $(F(X,Y), \alpha(X), G(X,Y))$ be a triple of two formal groups and a strict isomorphism over a ring A which is a characteristic zero ring or a $\mathbb{Z}_{(p)}$ -algebra. By theorem 6.6. There is a unique homomorphism $\phi: \mathbb{Z}[U;S] \rightarrow A$ such that $H_U^\phi(X,Y) = F(X,Y)$, $\alpha_{U,S}^\phi(X) = \alpha(X)$ and $H_{U,T}^\phi(X,Y) = G(X,Y)$. We are going to prove that $\phi(U(i,\underline{d})) = 0 = \phi(S(i,\underline{d}))$ for all \underline{d} , $\|\underline{d}\| > 1$ which are not of the form $p^r \underline{e}(j)$, $r \in \mathbb{N}$, $i \in \{1, \dots, m\}$. We already know that $\phi(U(i,\underline{d})) = 0$ for these \underline{d} because of 5.7. (Proof of p -typical universality of $F_V(X,Y)$). Suppose that there is \underline{d} with, $\|\underline{d}\| > 1$, \underline{d} not of the form $p^r \underline{e}(j)$ such that $\phi(S(i,\underline{d})) = a \neq 0$. Choose $r_1, \dots, r_m \in \mathbb{N}$ such that

$$(6.7.1) \quad d_1 p^{r_1} + \dots + d_m p^{r_m} \text{ is not a power of } p$$

$$(6.7.2) \quad d_1 p^{r_1} + \dots + d_m p^{r_m} < e_1 p^{r_1} + \dots + e_m p^{r_m} \text{ if } \underline{d} <_{\ell} \underline{e}$$

Let $\gamma(Z)$ be the curve $\gamma(Z) = (Z^{p^{r_1}}, \dots, Z^{p^{r_m}})$ in $G(X,Y)$. Let $\psi: \mathbb{Z}[V;T] \rightarrow A$ be the composition of $\phi: \mathbb{Z}[U;S] \rightarrow A$ with the canonical embedding $\mathbb{Z}[V;T] \rightarrow \mathbb{Z}[U;S]$. Let $\beta(X) = \alpha_{V,T}^\psi(X)$, where $\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X))$ is the strict isomorphism from $F_V(X,Y)$ to $F_{V,T}(X,Y)$. Then we have two isomorphisms

$$(6.7.3) \quad \begin{array}{ccc} F(X,Y) & \xrightarrow{\alpha(X)} & G(X,Y) \\ F(X,Y) & \xrightarrow{\beta(X)} & F_{V,T}^\psi(X,Y) \end{array}$$

and

$$(6.7.4) \quad \alpha(X) \equiv \beta(X) + aX^{\underline{d}} \pmod{\text{degree} > \underline{d}}$$

By lemma (6.3) the curves $\alpha^{-1}(\gamma(Z))$ and $\beta^{-1}(\gamma(Z))$ are both p -typical in $F(X,Y)$. And from (6.7.4) we see that

$$(6.7.5) \quad \alpha^{-1}\gamma(Z) \equiv \beta^{-1}\gamma(Z) - aZ^{\underline{d}} \pmod{\text{degree } d+1}$$

But this contradicts lemma 6.2 in view of (6.7.1)

q.e.d.

7. CURVILINEAR FORMAL GROUPS.

7.1. Proof of Curvilinearity of $H_R(X,Y)$ and $F_R(X,Y)$

The proofs are identical for these two cases. More generally let A be a characteristic zero ring and let $G(X,Y)$ be a formal group over A with a logarithm of the form

$$(7.1.1) \quad g(X) = X + \sum_{i=2}^{\infty} a_i X^i$$

where the a_i are $m \times m$ matrices with coefficients in $A \otimes_{\mathbb{Z}} \mathbb{Q}$. Then $G(X,Y)$ is a curvilinear formal group. Indeed, write

$$(7.1.2) \quad G(i)(X,Y) = X_i + Y_i + \sum c_{\underline{k},\underline{\ell}}(i) X^{\underline{k}} Y^{\underline{\ell}}$$

Suppose that there are $c_{\underline{k},\underline{\ell}} \neq 0$ with $\underline{k},\underline{\ell} = 0$ and $\|\underline{k}\|, \|\underline{\ell}\| \geq 1$ such that $c_{\underline{k},\underline{\ell}} \neq 0$. Choose a $c_{\underline{k},\underline{\ell}} \neq 0$ with $\|\underline{k}+\underline{\ell}\|$ minimal. Then looking at the coefficient of $X^{\underline{k}} Y^{\underline{\ell}}$ on both sides of

$$g(G(X,Y)) = g(X) + g(Y)$$

we see (7.1.1) that we must have a relation of the form

$$(7.1.3) \quad c_{\underline{k},\underline{\ell}}(i) = \sum b \dots (c_{\underline{k}_{i_1},\underline{\ell}_{i_1}}(j_1))^{r_1} \dots (c_{\underline{k}_{i_s},\underline{\ell}_{i_s}}(j_s))^{r_s}$$

with $j_1 = \dots = j_s$, ^{$(\tau_1, \dots, \tau_s \in \mathbb{N})$} Here the multiindices \underline{k}_i and \underline{l}_i must satisfy
 $1 \leq ||\underline{k}_i + \underline{l}_i|| < ||\underline{k} + \underline{l}||$, $r_1 \underline{k}_{i_1} + \dots + r_s \underline{k}_{i_s} = \underline{k}$, $\tau_1 \underline{l}_{i_1} + \dots + \tau_s \underline{l}_{i_s} = \underline{l}$.

These last two relations imply that $\underline{k}_{i_j} \cdot \underline{l}_{i_j} = 0$ for all $j = 1, \dots, s$, because $\underline{k} \cdot \underline{l} = 0$.

Hence by ^(the) induction ^(hypothesis) $c_{\underline{k}_i \cdot \underline{l}_i} = 0$ unless $\underline{k}_{i_j} = 0$ or $\underline{l}_{i_j} = 0$. Because

$j_1 = \dots = j_s = j$ and $G(j)(X, 0) = X_j$, $G(j)(0, Y) = Y_j$ the products under the sum sign on the right (of 7.1.3) are nonzero if only if for all $t = 1, \dots, s$, $\underline{k}_{i_t} = \underline{e}(j_t) = \underline{e}(j)$ and $\underline{l}_{i_t} = \underline{0}$ or vice versa

but this is impossible because $\underline{k} \cdot \underline{l} = 0$ and $||\underline{k}|| \geq 1$, $||\underline{l}|| \geq 1$.

q.e.d.

7.2. Comparison lemma for curvilinear formal groups.

Let $F(X, Y)$, $G(X, Y)$ be curvilinear formal groups over a ring A , and suppose that $F(X, Y) \equiv G(X, Y) \pmod{\text{degree } n}$. Then there is a unique matrix a with coefficients in A such that

$$F(X, Y) \equiv G(X, Y) + a(v(n))^{-1}((X+Y)^n - X^n - Y^n)$$

This follows directly from the general comparison lemma 5.4.

7.3. Integrality of $F_R(X, Y)$, $H_R(X, Y)$.

This is proved in the usual way by showing that $f_R(X)$, $h_R(X)$ satisfy functional equations of the type (3.1.1) and applying the functional equation lemma.

7.4. Universality of $F_R(X, Y)$ and $H_R(X, Y)$

This follows directly from (7.2) and the formulae for $f_R(X)$ and $h_R(X)$.

7.5. Proof of Theorems 2.15 and 2.18.

Most of this has already been proved in 7.1, 7.3, 7.4 above. It remains to prove the strict isomorphism statements. These are proved in the standard way, i.e. via the functional equation 3.1 (Cf. also 6.1).

8. CONCLUDING REMARKS.

The universal more dimensional formal group $H_U(X,Y)$ constructed here is the analogue of the one dimensional universal formal group $H_U(X,Y)$ of [4]. I do not know of a more dimensional analogue for the one dimensional universal formal group $F_U(X,Y)$ of [4] except the curvilinearly universal formal group $F_R(X,Y)$ constructed above. There are also more dimensional analogues of the p-typically universal one dimensional formal groups $F_S(X,Y)$ of [3]. If one chooses the $n(q_1, \dots, q_t)$ of (2.3) in the special way described in [3] (and [5]) one finds recursion formulae for the $U(i, \underline{d})$ in terms of the $a_{\underline{n}}(U)$ similar to the formulae in [3] and [5].

REFERENCES.

- [1]. Buhštaber, S.P. Novikov. Formal Groups, Power Systems and Adams Operations. Mat. Sbornik 84, 1(1971). Translation: Math. USSR Sbornik 13 (1971), 1, 80-116.
- [2]. M. Hazewinkel, Constructing Formal Groups I, II, III, IV. Reports 7119, 7201, 7207, 7322, Econometric Institute, Erasmus Univ. Rotterdam, 1971, 1972, 1973.
- [3]. M. Hazewinkel, Constructing Formal Groups I: The Local One Dimensional Case (to appear).
- [4]. M. Hazewinkel, Constructing Formal Groups II: The Global One Dimensional Case (to appear).
- [5] M. Hazewinkel, A Universal Formal Group and Complex Cobordism, *Bull. AMS* 81,5 (1975), 930-933.
- [6] M. Lazard, Lois de Groupes et analyseurs. Ann. Ec. Norm. Sup (3), 72 299-400 (1955).
- [7] M. Lazard, Sur les théorèmes fondamentaux des groupes formels commutatifs I, II. Indagationes Mathematicae 35, 4 (1973). 281-300.

CONSTRUCTING FORMAL GROUPS V: THE LUBIN-TATE FORMAL
MODULI THEOREM, THE LAZARD CLASSIFICATION THEOREM FOR
ONE DIMENSIONAL FORMAL GROUPS OVER ALGEBRAICALLY CLOSED
FIELDS, AND THEIR FORMAL A-MODULE ANALOGUES

by Michiel Hazewinkel

Authors address: Dept. Math. Econometric Inst.,
Erasmus University Rotterdam
50, Burg. Oudlaan.
ROTTERDAM, THE NETHERLANDS

AMS(MOS) 1970 classification: 14L05 (primary)

CONSTRUCTING FORMAL GROUPS V.

1. INTRODUCTION.

Let R be a local ring with residue field k and maximal ideal \mathfrak{m} . One way to try to classify formal group (laws) over R is to try to describe all formal group laws over R which reduce modulo \mathfrak{m} to $\Phi(X,Y)$, where $\Phi(X,Y)$ is a pregiven formal group (law) over k . Suppose that $\text{char}(k) = p > 0$, then if R is of characteristic zero one speaks of liftings of $\Phi(X,Y)$ and in case R is of characteristic p also one usually talks about deformations. More precisely one studies liftings (resp. deformations) $F(X,Y)$ over A under the equivalence relation: $F(X,Y) \sim G(X,Y)$ iff there exists an isomorphism $\alpha(X): F(X,Y) \rightarrow G(X,Y)$ over R such that $\alpha(X) \equiv X \pmod{\mathfrak{m}}$. In [10] Lubin and Tate have shown that if k is perfect, if R is complete and Hausdorff in the \mathfrak{m} -adic topology and if $\Phi(X,Y)$ is one dimensional and of height $h < \infty$, then the space of all lifts of $\Phi(X,Y)$ modulo the equivalence relation just described is \mathfrak{m}^{h-1} ; i.e. there are $h-1$ formal moduli. Their methods are cohomological in nature, and involve the calculation of a certain special second cohomology group especially invented for this purpose.

Now in [2] part I we described a universal strict isomorphism between p -typical formal groups $F_V(X,Y) \xrightarrow{\sim} F_{V,T}(X,Y) = F_{\bar{V}}(X,Y)$ over $\mathbb{Z}[V;T]$. The formal group $F_{V,T}(X,Y)$ is also p -typical and hence there exist polynomials \bar{V}_i (in $T_1, \dots, T_i; V_1, \dots, V_i$) such that $F_{V,T}(X,Y) = F_{\bar{V}}(X,Y)$ and the homomorphism $\mathbb{Z}[V] \rightarrow \mathbb{Z}[V,T]$, $V_i \mapsto \bar{V}_i$ describes the most general change of parameters possible within a given strict isomorphism class of formal groups. (This homomorphism $V_i \mapsto \bar{V}_i$ can also be interpreted as the map $\eta_R: BP_*(pt) \rightarrow BP_*(BP)$ of Brown-Peterson cohomology, cf [1], [2] part III, [4] and [8]). In [2] part III we also gave a recursion formula for \bar{V}_i . So if this formula is any good it ought to give (among other things) a reasonably direct (noncohomological) proof of the Lubin-Tate formal moduli theorem. It is one of the purposes of the present work to show that this is indeed the case. There are two bonuses: first one obtains an explicit parametrization of the moduli space \mathfrak{m}^{h-1} and second it turns out that the proof carries over unchanged (except for the occasional replacing of p by q or π) to the case of formal A -modules.

The last section of this note uses the formulas for \bar{V}_i to give a new proof of Lazard's classification theorem for one dimensional formal group laws over algebraically closed fields [9]. Here it is perhaps interesting to note that the congruence formula which makes things work (formula (6.3.2)) translates into the fundamental lemma 1.9 of [7] (sometimes known as the Budweiser lemma) when one interprets $\mathbb{Z}[V] \rightarrow \mathbb{Z}[V;T]$ as $\eta_R: BP_*(pt) \rightarrow BP_*(BP)$.

And, again there is a bonus and one obtains also the corresponding classification result for formal A-modules.

The phrase "formal group" will from now be used as an abbreviation of "one dimensional commutative formal group law". Standard notations: $\mathbb{N} = \{1,2,3,\dots\}$; \mathbb{Z} : the integers, \mathbb{Q} : the rational numbers.

2. RESUME OF SOME FORMULAS OF [2] PARTS I AND III (cf. also [4]).

Let $\mathbb{Z}[V]$, $\mathbb{Z}[V;T]$ be short for $\mathbb{Z}[V_1, V_2, \dots]$, $\mathbb{Z}[V_1, V_2, \dots; T_1, T_2, \dots]$. Let $a_n(V)$, $a_n(V, T)$ be the polynomials in $\mathbb{Q}[V]$, $\mathbb{Q}[V;T]$ defined recursively by

$$(2.1) \quad pa_n(V) = \sum_{i=0}^n a_{n-i}(V) V_i^p, \quad a_0(V) = 1$$

$$(2.2) \quad a_n(V, T) = \sum_{i=0}^n a_i(V) T_{n-i}^p, \quad a_0(V, T) = 1 \text{ and } T_0 = 1$$

and let $f_V(X)$, $f_{V,T}(X)$, $F_V(X, Y)$, $F_{V,T}(X, Y)$, $\alpha_{V,T}(X)$ be the power series

$$(2.3) \quad f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}, \quad f_{V,T}(X) = \sum_{n=0}^{\infty} a_n(V, T) X^{p^n}$$

$$(2.4) \quad F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y)), \quad F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y))$$

$$(2.5) \quad \alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X))$$

Then $F_V(X, Y)$, $F_{V,T}(X, Y)$, $\alpha_{V,T}(X)$ have their coefficients in $\mathbb{Z}[V;T]$, $F_V(X, Y)$ is a universal p-typical formal group and $\alpha_{V,T}(X): F_V(X, Y) \rightarrow F_{V,T}(X, Y)$ is a universal strict isomorphism of p-typical formal groups. The formal group $F_{V,T}(X, Y)$ is also p-typical and hence there are unique polynomials \bar{V}_i in $V_1, \dots, V_i; T_1, \dots, T_i$ with coefficients in \mathbb{Z} such that $F_{V,T}(X, Y) = F_V(X, Y)$ (and $f_V(X) = f_{V,T}(X)$). We have (cf. [2] part III, (5.3.1)).

$$\begin{aligned}
(2.6) \quad \bar{V}_n &= V_n + pT_n + \sum_{k=1}^{n-1} a_{n-k}(V) \{ (V_k^p - \bar{V}_k^p) \} + \\
&+ \sum_{k=1}^{n-1} a_{n-k}(V) \sum_{\substack{i+j=k \\ i,j \geq 1}} (V_i^p T_j^p - T_j^p \bar{V}_i^p) + \\
&+ \sum_{\substack{i+j=n \\ i,j \geq 1}} (V_i T_j^p - T_j \bar{V}_i^p)
\end{aligned}$$

and modulo the ideal generated by the elements $T_i T_j$, $i, j \in \mathbb{N}$ and the elements pT_i , $i = 1, 2, \dots$ we have

$$\begin{aligned}
(2.7) \quad \bar{V}_n &\equiv \sum (-1)^t V_1^{(p-1)^{-1}(p^{s_1+\dots+p^{s_t-t}})} V_{n-s_1}^{p^{s_1-1}} \dots V_{n-s_t}^{p^{s_t-1}} (-T_i V_j^p)^i \\
&+ V_n - T_1 V_{n-1}^p - \dots - T_{n-1} V_1^{p^{n-1}}
\end{aligned}$$

where the sum is over all sequences (s_1, \dots, s_t, i, j) such that $s_k, i, j, t \in \mathbb{N}$, $s_1 + \dots + s_t + i + j = n$.

3. STATEMENT OF THE FORMAL MODULI THEOREM.

3.1. The setting. Let R be a local ring with residue field k and maximal ideal \mathfrak{m} which is complete and Hausdorff in the \mathfrak{m} -adic topology. Let $\Phi(X, Y)$ be a formal group over k of height $h < \infty$. We assume that k has characteristic $p > 0$ (the other case being absolutely trivial because every formal group over a \mathbb{Q} -algebra is strictly isomorphic to an additive one). Let $F(X, Y)$, $G(X, Y)$ over R be two lifts of $\Phi(X, Y)$. Then we shall say that $F(X, Y)$ and $G(X, Y)$ are $*$ -isomorphic ([10]) if there exists an isomorphism $\alpha(X): F(X, Y) \rightarrow G(X, Y)$ such that $\alpha(X) \equiv X \pmod{\mathfrak{m}}$ and we shall say that $F(X, Y)$ and $G(X, Y)$ are strictly $*$ -isomorphic if there is a $*$ -isomorphism $\alpha(X)$ such that also $\alpha(X) \equiv X \pmod{(\text{degree } 2)}$.

3.2. We can just as well assume that $\Phi(X, Y)$ is p -typical because every formal group over a $\mathbb{Z}_{(p)}$ -algebra is strictly isomorphic to a p -typical one ([2] part I, corollary 2.11). Indeed if $\alpha(X): \Phi(X, Y) \rightarrow \hat{\Phi}(X, Y)$ is a strict isomorphism and $\tilde{\alpha}(X) \in R[[X]]$ is any power series such that

$\tilde{\alpha}(X) \equiv X \pmod{\text{degree } 2}$ and $\tilde{\alpha}(X)$ reduces to $\alpha(X) \pmod{\mathfrak{m}}$ then $\tilde{\alpha}(X)$ sets up a bijective correspondence between lifts of $\Phi(X,Y)$ and lifts of $\hat{\Phi}(X,Y)$ which respects $*$ -isomorphism and strict $*$ -isomorphism.

3.3. Let therefore $\Phi(X,Y)$ be p -typical of height h . Then there are unique elements $v_1, v_2, \dots \in k$ such that $\Phi(X,Y) = F_v(X,Y)$, where $v = (v_1, v_2, \dots)$ and because $\Phi(X,Y)$ is of height h we have $v_1 = v_2 = \dots = v_{h-1} = 0$, $v_h \neq 0$. (This follows from [2] part I, formula (4.4.5); in fact this formula shows that

$$\Phi(X,Y) \equiv X + Y + v_h C_p^h(X,Y) \pmod{\text{degree } p^{h+1}}$$

where $C_p^h(X,Y) = p^{-1}(X^p + Y^p - (X+Y)^p) \in \mathbb{Z}[X,Y]$. Now choose arbitrary

elements $\tilde{v}_i \in R$, $i = h, h+1, \dots$ such that $\phi(\tilde{v}_i) = v_i$ where $\phi: R \rightarrow k$ is the natural projection. For each h -tuple of elements $s = (s_1, \dots, s_h)$, $s_j \in \mathfrak{m}$ let $F_{v(s)}(X,Y)$ be the formal group obtained from $F_v(X,Y)$ by the substitutions

$$V_j \mapsto s_j, \quad j = 1, \dots, h-1$$

$$V_h \mapsto \tilde{v}_h + s_h$$

$$V_i \mapsto \tilde{v}_i, \quad i = h+1, h+2, \dots$$

The formal groups $F_{v(s)}(X,Y)$ are all lifts of $\Phi(X,Y)$ (because the

coefficients of $F_v(X,Y)$ are polynomials with coefficients in \mathbb{Z} in the V_1, V_2, \dots).

3.4. Theorem (Formal moduli theorem). With the notations and assumptions of (3.1) and 3.3 above we have

- (i) For every lift $F(X,Y)$ of $\Phi(X,Y)$ there is a unique h -tuple $s = (s_1, \dots, s_h)$, $s_j \in \mathfrak{m}$ such that $F(X,Y)$ is strictly $*$ -isomorphic to $F_{v(s)}(X,Y)$ (and the $F_{v(s)}(X,Y)$ are all lifts of $\Phi(X,Y)$).
- (ii) For every lift $F(X,Y)$ of $\Phi(X,Y)$ there is a unique h -tuple $s = (s_1, \dots, s_h)$, $s_j \in \mathfrak{m}$ with $s_h = 0$ such that $F(X,Y)$ is $*$ -isomorphic to $F_{v(s)}(X,Y)$.

4. PROOF OF THEOREM 3.4.

4.1. First step. Let $F(X,Y)$ be a formal group over R which lifts $\Phi(X,Y)$. As a first step we show that $F(X,Y)$ is strictly $*$ -isomorphic to a p -typical formal group which lifts $\Phi(X,Y)$. This is almost a triviality.

Indeed let $F_S(X,Y)$ over $\mathbb{Z}[S_2, S_3, \dots]$ be the formal group law of [2] part I formula (2.2.6), (2.2.3) with logarithm $f_S(X)$. This formal group is universal for formal groups over $\mathbb{Z}_{(p)}$ -algebras. Let $\beta_{V,S}(X) = f_V^{-1}(f_S(X))$ where we have identified V_i with S_i , $i = 1, 2, \dots$. Then $\beta_{V,S}(X)$ is a

strict isomorphism $F_S(X,Y) \rightarrow F_V(X,Y)$ over $\mathbb{Z}[S]$ which gives us a functorial way of making formal groups p -typical. Viz. let $G(X,Y)$ be any formal group over B ; let $\phi : \mathbb{Z}[S] \rightarrow B$ such that $G(X,Y) = F_S^\phi(X,Y)$ let $\beta(X) = \beta_{V,S}^\phi(X)$ then $G(X,Y) = \beta \hat{G}(\beta^{-1}(X), \beta^{-1}(Y))$ is p -typical. This method has obviously the property that if $H(X,Y) = G(X,Y)$, $\psi : B \rightarrow C$ then $\hat{H}(X,Y) = \hat{G}^\psi(X,Y)$. (by the uniqueness part of the universality property of $F_S(X,Y)$). Also $G(X,Y)$ is p -typical if and only if $\phi(S_i) = 0$ for all i which are not a power of p ([2] part I, proof of theorem 2.8 in section 6.6) and because $f_S(X) \equiv f_V(X) \pmod{S_i}$; i not a power of p) we also have $\hat{G}(X,Y) = G(X,Y)$ if $G(X,Y)$ is p -typical, because then $\beta(X) = X$.

Now let $F(X,Y)$ over R be a lift of $\Phi(X,Y)$, then by functoriality $\hat{F}(X,Y)$ lifts $\hat{\Phi}(X,Y)$ and by the remark just made the isomorphism $F(X,Y) \rightarrow \hat{F}(X,Y)$ reduces to $X \pmod{\mathfrak{m}}$ if $\Phi(X,Y)$ is p -typical, i.e. $F(X,Y) \rightarrow \hat{F}(X,Y)$ is a strict $*$ -isomorphism.

4.2. Second step. Now let $F(X,Y)$ over R be a p -typical lift of $\Phi(X,Y)$. Then $F(X,Y) = F_w(X,Y)$ for a certain sequence of elements $w = (w_1, w_2, \dots)$ of R . Because $F_w(X,Y)$ and $F_{\tilde{v}(0)}(X,Y)$ both reduce to $\Phi(X,Y) \pmod{\mathfrak{m}}$ we have that

$$(4.2.1) \quad \begin{aligned} w_1, \dots, w_{h-1} &\in \mathfrak{m} \\ w_i &\equiv \tilde{v}_i \pmod{\mathfrak{m}}, \quad i = h, h+1, \dots \end{aligned}$$

Inductively we are now going to construct sequences of elements of R

$$v(n) = (v_1(n), v_2(n), \dots)$$

and power series $\beta_n(X) \in R[[X]]$ such that

(4.2.2) $\beta_n(X): F_{v(n)}(X,Y) \rightarrow F_{v(n+1)}(X,Y)$ is a strict isomorphism

(4.2.3) $\beta_n(X) \equiv X \pmod{\mathfrak{m}^n}$

(4.2.4) $v(1) = w; v_i(n) \equiv \tilde{v}_i \pmod{\mathfrak{m}^n}$ for $i = h+1, h+2, \dots$

(4.2.5) $v_i(n) \equiv v_i(n+1) \pmod{\mathfrak{m}^n}$ for $i = 1, \dots, h$

First assume that $h > 1$. Suppose we have already found $v_i(n)$ and $\beta_{n-1}(X)$ (one takes $\beta_0(X) = X$). Now define elements $t_i(n)$ with induction with respect to i by means of the formula

$$(4.2.6) \quad t_i(n) = v_h(n)^{-p^i} (v_{i+h}(n) - \tilde{v}_{i+h} - t_1(n)v_{i+h-1}(n)^p - \dots - t_{i-1}(n)v_{h+1}(n)^{p^{i-1}})$$

(a formula which is clearly suggested by formula (2.7) above). Note that this is welldefined because $v_h(n) \equiv v_h(1) \pmod{\mathfrak{m}}$ so that $v_h(n)$ is invertible because $v_h(1)$ is invertible. Induction with respect to i gives us

$$t_i(n) \in \mathfrak{m}^n, i = 1, 2, \dots$$

Now let $t(n) = (t_1(n), t_2(n), \dots)$ and let

$$\beta_n(X) = \alpha_{v(n), t(n)}(X), v_i(n+1) = \bar{v}_i(v(n), t(n))$$

Then because $\bar{v}_n \equiv v_n \pmod{(T_1, \dots, T_n)}$, cf e.g. (2.7), and $\alpha_{v, T}(X) \equiv X \pmod{(T_1, T_2, \dots)}$ (because $f_{v, T}(X) \equiv f_v(X) \pmod{(T_1, T_2, \dots)}$ we have

$$\beta_n(X) \equiv X \pmod{\mathfrak{m}^n}$$

$$v_i(n+1) \equiv v_i(n) \pmod{\mathfrak{m}^n}, i = 1, 2, \dots$$

which takes care of (4.2.3) and (4.2.5) and also of (4.2.2) because $\alpha_{v(n), t(n)}(X)$ is a strict isomorphism $F_{v(n)}(X,Y) \rightarrow F_{v(n), t(n)}(X,Y)$. It remains to check that (4.2.4) holds (with $n+1$ instead of n) which

follows from (4.2.6) combined with (2.7) because $v_1(n)t_j(n) \in \mathfrak{m}^{n+1}$ as $h > 1$

In the case that $h = 1$ one cannot neglect the sum term in (2.7), but this does not matter precisely because $h = 1$. One proceeds in the same way except that formula (4.2.6) is replaced by

$$(4.2.7) \quad \begin{aligned} t_i(n) &= v_1(n)^{-p^i} (v_{i+1}(n) - \tilde{v}_{i+1} - t_1(n)v_i(n)^p - \dots - t_{i-1}(n)v_2(n)^{p^{i-1}}) + \\ &+ v_1(n)^{-p^i} (\sum (-1)^t v_1(n)^{(p-1)^{-1} (p^{s_1 + \dots + p^{s_t} - t)} v_{i+1-s_1}^{p^{s_1-1}}(n) \dots \dots \\ &\cdot v_{i+1-s_1}^{p^{s_t-1}} \dots v_t^{p^{s_t}}(n) (-t_j v_l^{p^j}(n))). \end{aligned}$$

Now consider the composed isomorphisms

$$F(X, Y) = F_w(X, Y) \rightarrow F_{v(2)}(X, Y) \rightarrow \dots \rightarrow F_{v(n)}(X, Y)$$

Because of (4.2.3) and the completeness of R these converge to an isomorphism

$$F(X, Y) \xrightarrow{\sim} F_{v(\infty)}(X, Y)$$

and because of (4.2.4) we have that $v_i(\infty) \equiv \tilde{v}_i \pmod{\mathfrak{m}^n}$ for all n if $i > h$ and hence because R is Hausdorff $v_i(\infty) = \tilde{v}_i$. This proves (together with step 1) that every lift of $\Phi(X, Y)$ is strictly $*$ -isomorphic to a formal group of the form $F_{\tilde{v}(s)}(X, Y)$.

4.3. Third step.

To finish the proof of part (i) of the theorem it only remains to prove that two formal groups $F_{\tilde{v}(s)}(X, Y)$ and $F_{\tilde{v}(s')}(X, Y)$ are strictly $*$ -isomorphic if and only if they are equal (i.e. $s=s'$). So suppose that $F_{\tilde{v}(s)}(X, Y)$ and $F_{\tilde{v}(s')}(X, Y)$ are strictly $*$ -isomorphic. By the universality of the isomorphism $\alpha_{V, T}(X)$ ([2] part I, theorem 2.12) this means that there are $t_1, t_2, \dots \in R$ such that the isomorphism is equal to

$$\alpha_{\tilde{v}(s),t}(X) = \alpha(X)$$

Now $\alpha_{V,T}(X) \equiv X + T_n X^{p^n} \pmod{(T_1, \dots, T_{n-1}; \text{degree } p^{n+1})}$. So as $\alpha(X)$ is a $*$ -isomorphism we must have $t_i \in \mathfrak{m}$ for all $i \in \mathbb{N}$. Now suppose that $\alpha(X) \neq X$ and let $n, r \in \mathbb{N}$ be such that

$$(4.3.1) \quad \begin{aligned} t_i &\in \mathfrak{m}^{r+1}, \quad i = 1, \dots, n-1; \quad t_n \in \mathfrak{m}^r \setminus \mathfrak{m}^{r+1}; \\ t_j &\in \mathfrak{m}^r \quad \text{for } j = n+1, n+2, \dots \end{aligned}$$

We have that \tilde{v}_{n+h} , the $(n+h)$ -th element of $\tilde{v}(s')$ is equal to $\bar{V}_{n+h}(\tilde{v}(s), t)$ for all $n \in \mathbb{N}$, and formula (2.7) combined with (4.3.1) gives

$$\bar{V}_{n+h}(\tilde{v}(s), t) \equiv \tilde{v}_{n+h} - t_n v_h^{p^n} \pmod{\mathfrak{m}^{r+1}}$$

which is a contradiction, so that indeed $\alpha(X) = X$. This concludes the proof of part (i) of theorem 3.4.

4.4. Proof of the second part of theorem 3.4. To prove the second part of theorem 3.4 we need to use more general isomorphisms than the strict isomorphisms $\alpha_{v,t}(X)$. The isomorphism $\gamma(X) = (1+T_0)^{-1}X$ applied to $F_{V,T}(X,Y) = F_{\tilde{V}}(X,Y)$ changes $F_V(X,Y)$ to a p -typical formal group law $\hat{F}_V(X,Y)$ with \hat{V}_n equal to

$$(4.4.1) \quad \hat{V}_n = (1+T_0)^{p^n - 1} \bar{V}_n$$

(simply because the logarithm of $(1+T_0)^{-1}F_V((1+T_0)X, (1+T_0)Y)$ is $(1+T_0)^{-1}f_V((1+T_0)X)$). Now let I_0 be the ideal generated by all elements $T_i T_j$, $i, j = 0, 1, 2, \dots$ and all elements pT_i , $i = 0, 1, 2, \dots$. Then we find

$$(4.4.2) \quad \hat{V}_n \equiv \bar{V}_n - T_0 V_n \pmod{I_0}$$

Of course for all this to make sense we must be working over a ring with T_0 in it and such that moreover $(1+T_0)^{-1}$ exists.

One takes e.g. the ring $\mathbb{Z}[[T_0]][[V;T]]$. The proof of the second part of theorem 3.4 now proceeds exactly as the proof of the first part; i.e.

we construct sequences of elements $\hat{v}(n) = (\hat{v}_1(n), \hat{v}_2(n), \dots)$, $\hat{v}(1) = w$, $\hat{v}_i(n+1) = \hat{V}_i(\hat{v}(n), \hat{t}(n))$ where now $\hat{t}(n) = (\hat{t}_0(n), \hat{t}_1(n), \dots)$ and power series $\hat{\beta}_n(X) = \hat{\alpha}_{\hat{v}(n), \hat{t}(n)}$ where $\hat{\alpha}_{V, T} = (1+T)_0^{-1} \alpha_{V, T}(X)$, such that

$$(4.4.3) \quad \hat{\beta}_n(X): F_{\hat{v}(n)}(X, Y) \rightarrow F_{\hat{v}(n+1)}(X, Y) \text{ is an isomorphism}$$

$$(4.4.4) \quad \hat{\beta}_n(X) \equiv X \pmod{\mathfrak{m}^n}$$

$$(4.4.5) \quad \hat{v}(1) = w; \hat{v}_i(n) \equiv \tilde{v}_i \pmod{\mathfrak{m}^n} \text{ for } i = h, h+1, \dots$$

$$(4.4.6) \quad \hat{v}_i(n) \equiv \hat{v}_i(n+1) \pmod{\mathfrak{m}^n} \text{ for } i = 1, \dots, h-1$$

(Note the three small changes with respect to (4.2.2) - (4.2.5). The formulae for the $\hat{t}_i(n)$ are

$$\hat{t}_0(n) = \hat{v}_h(n)^{-1}(\hat{v}_h(n) - \tilde{v}_h(n)), \hat{t}_i(n) = t_i(n) - \hat{t}_0(n)\hat{v}_h(n), i = 1, 2, \dots$$

where the $t_i(n)$ are as in (4.2.6) (resp. 4.2.7) if $h > 1$ (resp. $h=1$)
The remainder of the proof is exactly as before.

5. FORMAL MODULI FOR FORMAL A-MODULES.

5.1. Formal A-modules.

Let A be a ring. A formal A -module over an A -algebra R is a formal group $F(X, Y)$ over R together with a ring homomorphism $\rho_F: A \rightarrow \text{End}_R(F)$, such that $\rho_F(a)(X) \equiv aX \pmod{(\text{degree } 2)}$.

A homomorphism of formal A -modules over R is a homomorphism $\alpha(X): F(X, Y) \rightarrow G(X, Y)$ of formal groups over R such that

$$\begin{array}{ccc} F & \xrightarrow{\alpha} & G \\ \downarrow \rho_F(a) & & \downarrow \rho_G(a) \\ F & \xrightarrow{\alpha} & G \end{array}$$

commutes for all $a \in A$. (If R is of characteristic zero this condition is automatically fulfilled, but if R is of characteristic $p > 0$ there are in general many homomorphisms of formal groups which are not homomorphisms of formal A -modules).

5.2. From now on suppose that A is a discrete valuation ring with residue field k of q elements, $q = p^r$, $p = \text{char}(k) > 0$. The ring A itself maybe of characteristic p or 0 . (The hypothesis " k is finite" is no great restriction; if k is infinite all formal A -modules are isomorphic to $\hat{G}(X, Y) = X + Y$ with the obvious formal A -module structure (cf. [6])).

Choose a uniformizing element π of A . We define (almost exactly as in section 2 above)

$$(5.2.1) \quad \pi a_n^A(V) = \sum_{i=0}^n a_{n-i}^A(V) V_i^{q^{n-i}}, \quad a_0^A(V) = 1$$

$$(5.2.2) \quad a_n^A(V, T) = \sum_{i=0}^n a_i^A(V) T_{n-i}^{q^i}, \quad a_0^A(V, T) = 1$$

$$(5.2.3) \quad f_V^A(X) = \sum_{n=0}^{\infty} a_n^A(V) X^{q^n}, \quad f_{V, T}^A(X) = \sum_{n=0}^{\infty} a_n^A(V, T) X^{q^n}$$

$$(5.2.4) \quad F_V^A(X, Y) = (f_V^A)^{-1}(f_V^A(X) + f_V^A(Y)), \quad \rho_V^A(a) = (f_V^A)^{-1}(af_V^A(X))$$

$$(5.2.5) \quad f_{V, T}^A(X, Y) = (f_{V, T}^A)^{-1}(f_{V, T}^A(X) + f_{V, T}^A(Y)),$$

$$\rho_{V, T}^A(a) = (f_{V, T}^A)^{-1}(af_{V, T}^A(X))$$

$$(5.2.6) \quad \alpha_{V, T}^A(X) = (f_{V, T}^A)^{-1}(f_V^A(X)).$$

Then $(F_V^A(X, Y), \rho_V^A)$ and $(F_{V, T}^A(X, Y), \rho_{V, T}^A(X))$ are " A -typical" formal A -modules over $A[V]$ and $A[V, T]$ and they are strictly isomorphic (as formal A -modules) via $\alpha_{V, T}^A(X)$. The integrality statements on which these assertions rest are proved in [2] part VIII. Moreover there exists a universal formal A -module $F_S^A(X, Y)$ over $A[S_2, S_3, \dots]$ which is strictly isomorphic to $F_V^A(X, Y)$ (where we identify V_i with S_i) and this isomorphism gives us a functorial way of making q formal A -modules A -typical (compare the first step of the proof of theorem 3.4 above; i.e. section 4.1). Finally the isomorphism $\alpha_{V, T}^A(X)$ is universal for strict isomorphisms between A -typical formal A -modules over A -algebras R . These statements are also proved in [2] part VIII, albeit under some extra (totally unnecessary) hypotheses.

A less restrictive treatment will be found in [5], chapter IV, sections 21.4, 21.5 and 21.7.

We have now all the ingredients to state and prove the analogue for formal A-modules of theorem 3.4 except the notion of height.

5.3. A height of formal A-modules. Let $F(X,Y)$ be an A-typical formal A-module over a field ℓ (where A is as above in 5.2); i.e. $F(X,Y) = F_V^A(X,Y)$ for a suitable sequence $v = (v_1, v_2, \dots)$ of elements of ℓ . We define $A\text{-height}(F_V^A(X,Y)) = \text{index of first } v_i \neq 0$. For arbitrary formal A-modules over ℓ there is a strictly isomorphic A-typical formal A-module $\hat{F}(X,Y)$ over ℓ and we define $A\text{-height}(F(X,Y)) = A\text{-height}(\hat{F}(X,Y))$. This is welldefined. From the structure of $f_V^A(X)$ one sees that if $v_1 = \dots = v_{h-1} = 0$ then $\rho_V^A(\pi)(X) \equiv v_h X^{q^h} \pmod{\text{degree } q^{h+1}}$, which gives us an alternative definition of A-height. If A is the ring of integers of a finite extension K of \mathbb{Q}_p and $[K:\mathbb{Q}_p] = n$, then $A\text{-height}(F(X,Y)) = h^{-1}$ height $(F(X,Y))$ which is also clear because in that case

$$[p]_F(X) = \rho_V^A(p)(X) = \rho_V^A(\pi^e)(X) \quad \rho_V^A(u)(X) \equiv v_h^e u X^{q^{he}}$$

$\pmod{\text{degree } q^{eh+1}}$ if $p = \pi^e u$, u a unit in A. (If A is of characteristic $p > 0$ then $F(X,Y)$ always has infinite height as a formal group, but may very well have finite height as a formal A-module).

We now state the analogue for formal A-modules of part (ii) of theorem 3.4.

5.4. Theorem. (Formal moduli for formal A-module). Let $\Phi(X,Y)$ be an A-typical formal A-module over a field ℓ (as ℓ must be an A-algebra ℓ is an extension field of k). Let R be a local A-algebra with residue field ℓ and maximal ideal \mathfrak{m} which is complete and Hausdorff in the \mathfrak{m} -adic topology.

Let $\Phi(X,Y)$ be of A-height $h < \infty$ and let $v_1 = \dots = v_{h-1} = 0, 0 \neq v_h, v_{h+1}, \dots \in \ell$ be such that $\Phi(X,Y) = F_V^A(X,Y)$ and choose elements $\tilde{v}_h, \tilde{v}_{h+1}, \dots \in R$ which are lifts of v_h, v_{h+1}, \dots . For each $h-1$ tuple $s = (s_1, \dots, s_{h-1})$ of elements of \mathfrak{m} let $F_{\tilde{v}(s)}^A(X,Y)$

be the formal A-module over R obtained by substituting s_i for V_i , $i = 1, \dots, h-1$ and \tilde{v}_j for V_j , $j = h, h+1, \dots$ in $F_V^A(X,Y)$. Then every lift $F(X,Y)$ over R of $\Phi(X,Y)$ is *-isomorphic (as formal A-modules) to exactly one of the $F_{\tilde{v}(s)}^A(X,Y)$ (and the $F_{\tilde{v}(s)}^A(X,Y)$ are all lifts of $\Phi(X,Y)$).

5.5. On the proof of theorem 5.4. By and large one obtains a proof of theorem 5.4 by copying the proof of theorem 3.4 while observing the following transcribing rule "p's in exponents become q's and p's on line or in denominators become π 's".

There is one small difference: the somewhat obnoxious sum term in the analogue of formula (2.7) disappears. (This term can be nonzero mod $(T_i T_j, T_i, i, j \in \mathbb{N})$ only if $p = q$ and A is unramified; i.e. this term contributes something only in the case that $F(X, Y)$ is a formal A -module over nothing larger than \mathbb{Z}_p). So the proof actually simplifies somewhat.

6. LAZARD'S CLASSIFICATION THEOREM AND ITS FORMAL A-MODULE ANALOGUE

The classification theorem alluded to in the title of this section is:

6.1. Theorem. ([]). Let K be a separably closed field of characteristic $p > 0$. Then the one dimensional formal groups over K are classified by their heights.

6.2. Start of the proof. Let $F_h(X, Y)$ over K be the formal group obtained by substituting $V_i = 0$ for $i \neq h$, $V_h = 1$ in the universal p -typical formal group law $F_V(X, Y)$. This gives a formal group law of height h over K for each $h \in \mathbb{N}$, and these are (by the definition of height) pairwise nonisomorphic and also nonisomorphic to the additive formal group $\hat{G}_a(A, Y)$ over K .

Now assume that $F(X, Y)$ has infinite height; as $F(X, Y)$ is strictly isomorphic to a p -typical formal group we can assume that $F(X, Y) = F_V(X, Y)$ for a suitable sequence of elements $v = (v_1, v_2, \dots)$ in K . The height of $F_V(X, Y)$ is equal to the first index i such that $v_i \neq 0$, hence $v_i = 0$ all i as $F_V(X, Y)$ has infinite height, hence $F_V(X, Y) = \hat{G}_a(X, Y)$.

So it only remains to show that a formal group of height $h < \infty$ over K is isomorphic to $F_h(X, Y)$. To prove this we use two congruence formulas for the polynomials \bar{v}_n in $V_1, \dots, V_n; T_1, \dots, T_n$.

6.3. Lemma. Fix $h \in \mathbb{N}$, then we have for every $n \in \mathbb{N}$

$$(6.3.1) \quad \bar{v}_n \equiv V_n \pmod{(V_1, \dots, V_{n-1}, p)}$$

$$(6.3.2) \quad \bar{v}_{n+h} \equiv V_{n+h} - T_n V_h^p + V_h T_n^p \pmod{(V_1, \dots, V_{h-1}, V_{h+1}, \dots, V_{n+h-1}; T_1, \dots, T_{n-1}, p)}$$

6.4. Remark. Formula (6.3.2) translates into the Budweiser lemma if one interpretes $V_i \mapsto \bar{V}_i$ as the right unit homomorphism

$\eta_R: BP_*(pt) \rightarrow BP_*(BP)$ of the Hopf algebra of homology operations of Brown-Peterson cohomology. Cf. [7] lemma 1,9 and [4], [2] part III.

6.5. Proof of lemma 6.3. We work in $\mathbb{Q}[V;T]$. First of all we have directly from the defining formulas (2.1)

$$(6.5.1) \quad a_i(V) \equiv 0 \pmod{(V_1, \dots, V_{n-1})} \text{ if } i < n, \quad a_n(V) \equiv p^{-1}V_n \pmod{(V_1, \dots, V_{n-1})}$$

which by (2.2) gives us that

$$(6.5.2) \quad a_i(V,T) \equiv T_i \pmod{(V_1, \dots, V_{n-1})} \text{ if } i < n,$$

$$a_n(V) \equiv p^{-1}V_n + T_n \pmod{(V_1, \dots, V_{n-1})}$$

and as by the definition of the \bar{V}_i we have

$$(6.5.3) \quad pa_n(V,T) = a_{n-1}(V,T)\bar{V}_1^{p^{n-1}} + \dots + a_1(V,T)\bar{V}_{n-1}^p + \bar{V}_n$$

we see that (6.3.1) follows immediately from (6.5.1), (6.5.2) (and (6.5.3)).

To prove (6.3.2) we use formula (2.6) above. We proceed by induction on n (keeping h fixed). The case $n = 0$ is taken care of by (6.3.1).

By induction hypothesis we therefore have

$$(6.5.4) \text{ if } i < n+h \text{ then } \bar{V}_i \equiv V_i \pmod{(V_1, \dots, V_{h-1}, V_{h+1}, \dots, V_{n+h-1}, T_1, \dots, T_{n-1}, p)}$$

Let \mathfrak{a} be the ideal $(V_1, \dots, V_{h-1}, V_{h+1}, \dots, V_{n+h-1}, T_1, \dots, T_{n-1})$ in $\mathbb{Z}[V,T]$.

We now deal with the various terms appearing in formula (2.6) separately.

- (a) The terms $V_i T_j^p$, $i, j \geq 1$, $i + j = n + h$. These are all zero mod \mathfrak{a} unless $i = h$ (and hence $j=n$) which gives us a term $V_h T_n^{p^h}$
- (b) The terms $T_j \bar{V}_i^{p^j}$, $i, j \geq 1$, $i + j = n + h$. These are zero mod (\mathfrak{a}, p) unless $j = h$, $i = n$ which gives a term $-T_n \bar{V}_h^{p^h}$. (Here (6.5.4) is used).

Let $\bar{\mathfrak{a}}$ be the ideal $\mathfrak{a}\mathbb{Q}[V;T] \subset \mathbb{Q}[V;T]$. We shall use the notation $b(V,T) \equiv 0 \pmod{(\bar{\mathfrak{a}}, p)}$ to mean that $b(V,T) \in \bar{\mathfrak{a}} + p\mathbb{Z}[V,T]$.

(c) The terms $a_{n-k}(V)(V_k^p - \bar{V}_k^p)$, $k = 1, \dots, n-1$. By the induction hypothesis (6.5.4) we have that $V_k \equiv \bar{V}_k \pmod{(\sigma, p)}$ for these k and hence $V_k^p \equiv \bar{V}_k^p \pmod{(\sigma, p)}$ which implies that the terms under consideration are $\equiv 0 \pmod{(\bar{\sigma}, p)}$ because $p^{n-k} a_{n-k}(V) \in \mathbb{Z}[V; T]$.

(d) The terms $a_{n-k}(V) V_i^p T_j^p$, $k = 1, \dots, n-1, i + j = k, i, j \geq 1$.

There are all zero mod $\bar{\sigma}$ because for these i and j either $V_i \in \sigma$ or $T_j \in \sigma$.

(e) The terms $a_{n-k}(V) T_j^p V_i^p$, $k = 1, \dots, n-1, i + j = k, i, j \geq 1$.

For these i and j we have $T_j \in \sigma$ unless $j \geq n$ which means that $i < h$ so that $V_i \equiv 0 \pmod{(\sigma, p)}$ and $V_i^{p^{n-i}} \equiv 0 \pmod{(\sigma, p^{n-k+1})}$ so that all these terms are zero mod $(\bar{\sigma}, p)$.

Putting all this together we find

$$V_{n+h} \equiv V_{n+h} + V_h T_n^p - T_n V_h^p \pmod{(\bar{\sigma}, p)}$$

which by sublemma 6.6 below means that (6.3.2) holds.

6.6. Sublemma. Let $b(V, T) \in \mathbb{Z}[V, T]$ and suppose that $b(V, T) \in \bar{\sigma} + p\mathbb{Z}[V, T]$.

Proof. Write $b(V, T)$ as a sum of monomials $b(V, T) = \sum c_{\underline{n}, \underline{m}} V^{\underline{n}} T^{\underline{m}}$. Then

$b(V, T) \in \bar{\sigma} + p\mathbb{Z}[V, T]$ means that for all $\underline{n}, \underline{m}$ at least one of the following hold

(i) $c_{\underline{n}, \underline{m}} \equiv 0 \pmod{p}$,

(ii) $V_i | V^{\underline{n}}$ for some $i \in \{1, \dots, h-1, h+1, \dots, h+n-1\}$,

(iii) $T_j | T^{\underline{m}}$ for some $j \in \{1, 2, \dots, n-1\}$. And this in turn implies that

$b(V, T) \in \bar{\sigma} + p\mathbb{Z}[V; T]$ because the $c_{\underline{n}, \underline{m}}$ are integral.

6.7. Proof of theorem 6.1 (conclusion).

We must show that if $F(X, Y) = F_v(X, Y)$, $v = (v_1, v_2, \dots)$, $v_1 = \dots = v_{h-1} = 0$, $v_h \neq 0$ then $F(X, Y)$ is isomorphic to $F_h(X, Y)$. We are now going to construct sequences of elements $v(n) = (v_1(n), v_2(n), \dots)$ of elements of K with $v(1) = v$ and power series $\beta_n(X)$ such that

$$(6.7.1) \quad v_i(n) = 0 \text{ for } i = 1, \dots, h-1, \dots, h+n-1; v_h(n) \neq 0$$

(6.7.2) $\beta_n(X)$ is a strict isomorphism $F_{v(n)}(X,Y) \rightarrow F_{v(n+1)}(X,Y)$

(6.7.3) $\beta_n(X) \equiv X \pmod{\text{degree } p^n}$

Suppose we have already found $v_i(n)$, $i = 1, 2, \dots$ for a certain $n \in \mathbb{N}$. (Take $v(1)=v$). Take $t_i(n) = 0$ for $i = 1, \dots, n-1, n+1, n+2, \dots$ and choose $t_n(n)$ such that

$$(6.7.4) \quad v_{n+h}(n) - t_n(n)v_h(n)^{p^n} + v_h(n)t_n(n)^{p^h} = 0$$

(such a $t_n(n)$ exists in K because K is separably closed and $v_h(n) \neq 0$). Now let

$$v_i(n+1) = V_i(v(n), t(n)), \quad \beta_n(X) = \alpha_{v(n), t(n)}(X)$$

then (6.7.2) and (6.7.3) are clear because $\alpha_{V, T}(X) \equiv X \pmod{(T_1, \dots, T_{n-1}, \text{degree } p^n)}$ and (6.7.1) (with $n+1$ instead of n) follows from (6.7.4) and (6.3.2). Now consider the composed isomorphisms

$$F_v(X,Y) \rightarrow F_{v(2)}(X,Y) \rightarrow \dots \rightarrow F_{v(n)}(X,Y)$$

These converge to an isomorphism $\beta(X): F_v(X,Y) \rightarrow F_{v(\infty)}(X,Y)$ because of (6.7.3) and because of (6.7.1) we have that $v_i(\infty) = 0$ for $i \neq h$ and $v_h(\infty) \neq 0$. Now let $\gamma(X) = a^{-1}X$ where a is a (p^h-1) -th root of $v_h(\infty)$. Then $\gamma(X)$ is an isomorphism $F_{v(\infty)}(X,Y) \rightarrow F_h(X,Y)$, which concludes the proof of theorem 6.1.

The formal A -module analogue of theorem 6.1 is

6.8. Theorem. Let A be a discrete valuation field with residue field of q elements and let K be a separably closed extension field of k . Then the formal A -modules over K are classified by their A -height.

The proof of this theorem is obtained from the proof given above for Lazard's theorem by the transcribing rule mentioned in 5.5 above. For

example (6.3.2) becomes $V_{n+h} \equiv V_{n+h} - T_n V_h^q + V_h T_n^q \pmod{(V_1, \dots, V_{h-1}, V_{h+1}, \dots, V_{n+h-1}, T_1, \dots, T_{n-1}, \pi)}$ where π is a uniformizing element of A .

REFERENCES.

1. J.F. Adams, Stable Homotopy and Generalised Homology, Univ. of Chicago Pr., 1974.
2. M. Hazewinkel, Constructing Formal Groups I-VIII (I,II,III to appear J. Pure and Applied Algebra; IV to appear Adv. Math; VIII submitted Compositio Math; available in preprint form as reports 7119, 7201, 7207, 7322, 7505, 7507, 7514, 7519, Econometric Inst., Erasmus Univ. Rotterdam, 1971-1975).
3. M. Hazewinkel, A Universal Formal Group and Complex Cobordism. Bull. Amer. Math. Soc. 81 (1975), 930-933.
4. M. Hazewinkel, A Universal Isomorphism of p-typical Formal Groups and Operations in Brown-Peterson Cohomology, Indagationes Math. 38 (1976), 195-199.
5. M. Hazewinkel, Formal Groups and Applications; in preparation.
6. M. Hazewinkel, On Universal Formal A-Modules; in preparation.
7. D.C. Johnson, W.S. Wilson, BP-Operations and Morava's extraordinary K-theories, Math. Z. 144 (1975), 55-75.
8. P. Landweber, $BP_*(BP)$ and Typical Formal Groups, Osaka J. Math. 12 (1975), 357-363.
9. M. Lazard, Sur les Groupes de Lie Formels à un Paramètre, Bull. Soc. Math. de France 83(1955), 251-274.
10. J. Lubin, J. Tate, Formal Moduli for One Parameter Formal Lie Groups, Bull. Soc. Math. de France 94 (1966), 49-60.

CONSTRUCTING FORMAL GROUPS VI: CARTIER'S THIRD
THEOREM *)

Michiel Hazewinkel

Author's address: Math. Dept., Econometric Inst.,
Erasmus Univ. Rotterdam,
50, Burg. Oudlaan,
Rotterdam, The Netherlands

AMS(MOS) 1970 classification: 14L05

*) Part of the work for this paper was done in November 1975,
while the author enjoyed the hospitality of the Math. Inst.
of Georg August University, Göttingen.

ABSTRACT.

Let $\underline{\text{Gf}}_A$ be the category of finite dimensional commutative formal groups over a ring A . To A one associates a certain, in general noncommutative, ring $\text{Cart}(A)$. One then defines a functor $G \rightarrow \hat{\mathbb{C}}(G)$ which assigns to a formal group law G its group of curves which is a module over $\text{Cart}(A)$. Theorems 2 and 3 of [1] now say that $G \rightarrow \hat{\mathbb{C}}(G)$ is an equivalence of categories of $\underline{\text{Gf}}_A$ with a certain full subcategory of $\text{Cart}(A)$ -modules. In this paper we give a new proof of theorem 3 of [1], Cartier's third theorem, which asserts that every $\text{Cart}(A)$ -module of a certain type comes from a formal group law over A . This proof is based on the constructions of part IV of this series of papers [3].

1. INTRODUCTION AND STATEMENT OF THE THEOREM.

From now on formal group means finite dimensional formal group law over A . We take the naive or power series point of view; i.e. an m -dimensional formal group over A is simply an m -tuple of power series $G(X,Y)$ in $2m$ variables $X_1, \dots, X_m; Y_1, \dots, Y_m$ such that $G(X,0) = X, G(0,Y) = Y, G(X,G(Y,Z)) = G(G(X,Y),Z), G(X,Y) = G(Y,X)$.

1.1. Curves. A curve (over A) in a formal group G over A is an m -tuple of power series $\gamma(t) = (\gamma_1(t), \dots, \gamma_m(t))$ in one variable t , such that $\gamma(0) = 0$. Two curves $\gamma(t), \delta(t)$ can be added by means of the formula $\gamma(t) +_G \delta(t) = G(\gamma(t), \delta(t))$. This turns the set of all curves into an abelian group $\mathcal{C}(G)$. We use $\mathcal{C}^n(G)$ to denote the subgroup of all curves $\gamma(t)$ such that $\gamma(t) \equiv 0 \pmod{t^n}, n = 1, 2, \dots$. This defines a filtration $\mathcal{C}(G) = \mathcal{C}^1(G) \supset \mathcal{C}^2(G) \supset \dots$ and $\mathcal{C}(G)$ is complete in the topology defined by this filtration.

1.2. The Operators. $\langle a \rangle, \underline{V}_n, \underline{f}_n$. In addition to the topological group structure on $\mathcal{C}(G)$ one has a number of operators which are compatible with this structure. Viz.:

$$\begin{aligned} \text{for all } a \in A, \quad \langle a \rangle \gamma(t) &= \gamma(at) \\ \text{for all } n = 1, 2, \dots, \quad \underline{V}_n \gamma(t) &= \gamma(t^n) \end{aligned}$$

The definition of the third kind of operator, the Frobenius operators \underline{f}_n , needs a bit more care. Formally one has

$$\text{for all } n = 1, 2, \dots, \quad \underline{f}_n \gamma(t) = \gamma(\zeta_n t^{1/n}) +_G \dots +_G \gamma(\zeta_n^n t^{1/n})$$

where ζ_n is a primitive n -th root of unity. For a more precise definition cf. [3] part IV or [5]. There are various relations among these operators. They are

$$\begin{aligned} \langle a \rangle \langle b \rangle &= \langle ab \rangle, \quad \langle 1 \rangle = \underline{V}_1 = \underline{f}_1 = \text{identity operator}, \\ \underline{V}_\tau \underline{V}_n &= \underline{V}_{\tau n}, \quad \underline{f}_\tau \underline{f}_n = \underline{f}_{\tau n}, \\ \langle a \rangle \underline{V}_\tau &= \underline{V}_\tau \langle a^\tau \rangle, \quad \underline{f}_\tau \langle a \rangle = \langle a^\tau \rangle \underline{f}_\tau \end{aligned}$$

$$(1.3) \quad \text{if } (n, \tau) = 1, \text{ then } \underline{f}_\tau \underline{V}_n = \underline{V}_n \underline{f}_\tau,$$

$$\begin{aligned} \underline{f}_n \underline{V}_n &= n, \text{ i.e. } \underline{f}_n \underline{V}_n \gamma(t) = \gamma(t) +_G \gamma(t) +_G \dots +_G \gamma(t) \quad (n \text{ factors}), \\ \langle a+b \rangle &= \sum_{n=1}^{\infty} \underline{V}_n r_n(a, b) \underline{f}_n, \end{aligned}$$

where the $r_n(Z_1, Z_2)$ are the polynomials with coefficients in \mathbb{Z} defined by

$$(1.4) \quad r_n(Z_1, Z_2) = \sum_{d|n} dr_d(Z_1, Z_2)^{n/d}$$

1.5. A \underline{V} -basis for $\mathbb{C}(G)$. Let $\delta_i(t)$ denote the curve $(0, \dots, 0, t, 0, \dots, 0)$ in G , where t is in the i -th spot. It immediately follows from $F(X, Y) \equiv X + Y \pmod{\text{degree } 2}$ that every curve in G can be uniquely written as a convergent sum

$$(1.6) \quad \gamma = \sum_{i=1}^n \sum_{k=1}^{\infty} \underline{V}_k \langle a_{ik} \rangle \delta_i$$

It follows, cf. (1.3) and also section 2 below, that we know the structure of $\mathbb{C}(G)$ as a topological group with operators $\langle a \rangle$, $\underline{f}_n, \underline{V}_n$ if we know all the expressions

$$(1.7) \quad \underline{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V}_s \langle c(n, s)_{ji} \rangle \delta_j$$

The "structure coefficients" $c(n, s)_{ji}$, $n, s \in \mathbb{N}$, $i, j \in \{1, \dots, m\}$ are far from independent. They satisfy certain relations which come from

$$\underline{f}_n \underline{f}_r = \underline{f}_{nr}$$

1.8. Reduced Cart(A)-modules. If $\mathbb{C}(G)$ is the module of curves of a formal group G , then $\mathbb{C}(G)$ has the following properties

- (i) There are subgroups \mathbb{C}^n , closed under the operators $\langle a \rangle$, \underline{V}_r ; \mathbb{C} is complete in the topology defined by the \mathbb{C}^n and \mathbb{C}^n is the smallest closed subgroup of \mathbb{C} which contains all the $\underline{V}_r \mathbb{C}$ with $r \geq n$.
- (ii) The operators $\langle a \rangle$, \underline{f}_n , \underline{V}_n are all continuous and satisfy the relations (1.3).
- (iii) There are elements $\delta_1, \dots, \delta_m \in \mathbb{C}$ such that every element $\gamma \in \mathbb{C}$ can be uniquely written as a convergent sum

$$\gamma = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V}_s \langle a_{js} \rangle \delta_j$$

In general we shall call a topological abelian group \mathbb{C} with operators $\langle a \rangle$, $\underline{V}_n, \underline{f}_n$ such that (i), (ii), (iii) hold a reduced Cart(A)-module. (Here Cart(A) stands for the set of all formal expressions $\sum \underline{f}_i \langle a_{ij} \rangle \underline{V}_j$, with for every j only finitely many i such that $a_{ij} \neq 0$. These expressions can be added and multiplied by means of the calculation rules (1.3) to form a (topological) ring of operators, cf. [4]).

A set of elements such that (iii) holds is called a \underline{V} -basis.

1.9. Cartier's third theorem. Let \mathbb{C} be a reduced $\text{Cart}(A)$ -module with \underline{V} -basis $\delta_1, \dots, \delta_m$. There there exists an m -dimensional formal group law G over A such that $\mathbb{C}(G) \cong \mathbb{C}$ as $\text{Cart}(A)$ -modules with δ_i corresponding to the i -th element $\delta_i(t)$ of the canonical \underline{V} -basis of $\mathbb{C}(G)$ described in 1.5.

¶ This is theorem 3 of [1]. Cartier never published his proofs of the theorems of [1]. Proofs can be found in [5]; these are outlined in [4]. In [2] there is a proof of Cartier's third theorem for the case that A is torsion free. This proof breaks down if A has additive torsion.

The remainder of this paper mainly concerns still another proof of Cartier's third theorem based on the constructions of the earlier parts of these series of papers. This proof also provides a link between these constructions and the "intertwined function pair" considerations of [2].

2. CONSTRUCTION OF A UNIVERSAL CURVE MODULE.

Choose $m \in \mathbb{N}$ and choose a set of elements $\delta_1, \dots, \delta_m$. Let $\tilde{\mathcal{L}}_{\mathbb{C}}$ be the ring $\tilde{\mathcal{L}}_{\mathbb{C}} = \mathbb{Z} [C(n,r)_{i,j} | r \in \mathbb{N}, n \in \mathbb{N} \setminus \{1\}, i, j \in \{1, \dots, m\}]$ of polynomials in the indeterminates $C(n,r)_{i,j}$. For convenience we also introduce $C(1,1)_{i,j} = 0$ if $i \neq j$, $C(1,1)_{i,i} = 1$, $C(1,r)_{i,j} = 0$ for all $r \in \mathbb{N} \setminus \{1\}$, $i, j \in \{1, \dots, m\}$.

Now consider the set \mathbb{M} of all formal expressions

$$(2.1) \quad \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V}_s \langle a_{s,j} \rangle \delta_j \quad a_{s,j} \in \tilde{\mathcal{L}}_{\mathbb{C}}$$

We now introduce the defining relations

$$(2.2) \quad \underline{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V}_s \langle C(n,s)_{ji} \rangle \delta_j$$

for all $n \in \mathbb{N}$. One can now use the calculation rules (1.3) with the exception of the rule $\underline{f}_n \underline{f}_r = \underline{f}_{nr}$, and the defining relations (2.2) to add expressions of the form (2.1) and to define \underline{f}_r of such an expression, $r \in \mathbb{N}$.

To do this we start by showing how to rewrite any sum of the form

$$(2.3) \quad \sum_{s=1}^{\infty} \sum_{j=1}^m \sum_t \underline{V}_s \langle a_{s,j,t} \rangle \delta_j \quad a_{s,j,t} \in \tilde{\mathcal{L}}_{\mathbb{C}}$$

in the form (2.1). Here for each $s \in \mathbb{N}$, $j \in \{1, \dots, m\}$ the index t runs over some finite index set which may depend on s and j .

For each $n \in \mathbb{N}$, let $\lambda(n)$ be the number of prime factors of n , i.e. $\lambda(1) = 0$ and if $n = p_1^{r_1} p_2^{r_2} \dots p_t^{r_t}$, p_i a prime number, $r_i \in \mathbb{N}$, then $\lambda(n) = r_1 + \dots + r_t$. One now proceeds as follows

$$\begin{aligned} \sum_{s,j,t} \prod_{s} \langle a_{s,j,t} \rangle^{\delta_j} &= \sum_{j,t} \langle a_{1,j,t} \rangle^{\delta_j} \sum_{\underline{s} \geq 2} \prod_{j,t} \prod_{s} \langle a_{s,j,t} \rangle^{\delta_j} \\ &= \sum_j \sum_{i=1}^{\infty} \prod_{i,j} \langle b_{i,j} \rangle^{\delta_j} + \sum_{\underline{s} \geq 2} \prod_{j,t} \prod_{s} \langle a_{s,j,t} \rangle^{\delta_j} \end{aligned}$$

where $b_{i,j} = r_i(a_{1,j,1}, a_{1,j,2}, \dots)$ with r_1, r_2, \dots the polynomials in k variables defined by

$$(2.4) \quad Z_1^n + \dots + Z_k^n = \sum_{d|n} dr_d(Z_1, \dots, Z_k)^{n/d}, \quad n = 1, 2, \dots$$

(Cf. (1.4); of course k may depend on j). Now use (2.2) to rewrite (2.3) further as

$$\begin{aligned} &\sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_j \sum_{i \geq 2} \prod_{i,j} \langle b_{i,j} \rangle^{\delta_j} \sum_{\ell,k} \prod_{\ell} \langle C(i,\ell)_{kj} \rangle^{\delta_k} \\ &+ \sum_{\underline{s} \geq 2} \prod_{j,t} \prod_{s} \langle a_{s,j,t} \rangle^{\delta_j} = \sum_j \langle b_{1,j} \rangle^{\delta_j} \\ &+ \sum_{j,k} \sum_{i \geq 2} \sum_{\ell} \prod_{i,\ell} \langle b_{i,j}^{\ell} C(i,\ell)_{kj} \rangle^{\delta_k} + \sum_{\underline{s} \geq 2} \prod_{j,t} \prod_{s} \langle a_{s,j,t} \rangle^{\delta_j} \\ &= \sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_{\lambda(s) \geq 1} \sum_j \sum_t \prod_{s} \langle b'_{s,j,t} \rangle^{\delta_j} \end{aligned}$$

for certain well determined $b'_{s,j,t} \in \mathbb{L}_C$. And of course the summation set for t for a given s, j will now in general be different than the one in (2.3). For each $s \in \mathbb{N}$ with $\lambda(s) \geq 1$ (i.e. $s \geq 2$) write $s = p_s s'$ where p_s is the first prime number dividing s . We find an expression

$$(2.5) \quad \sum_j \langle b_{1,j} \rangle^{\delta_j} + \sum_{\lambda(r)=1} \prod_{s,j,t} \prod_{r} \langle a'_{r,s,j,t} \rangle^{\delta_j}$$

where now the summation set for t may also depend on r . Now repeat the

procedure given above for each of the interior sums

$$\sum_{s,j,t} V_{=s} \langle a'_{r,s,j,t} \rangle \delta_j$$

to obtain an expression

$$\sum_j \langle b_{1,j} \rangle \delta_j + \sum_{\lambda(r)=1} V_{=r} \sum_j \langle b_{r,1,j} \rangle \delta_j + \sum_{\lambda(r)=2} V_{=r} \sum_{s,j,t} V_{=s} \langle a''_{r,s,j,t} \rangle \delta_j$$

Now apply the same procedure to the interior sums in the third summand, ..., etc., ... After k steps we thus obtain algorithmically the coefficients $x_{s,j}$ in

$$(2.6.) \quad \sum_{s,j,t} V_{=s} \langle a_{s,j,t} \rangle \delta_j = \sum_{s,j} V_{=s} \langle x_{s,j} \rangle \delta_j$$

for all s with $\lambda(s) \leq k-1$.

We now proceed to define $f_{=n}$ of an expression (2.1). Write

$$(2.7) \quad \begin{aligned} f_{=n}(\sum_{s,j} V_{=s} \langle a_{s,j} \rangle \delta_j) &= \sum_{s,j} dV_{=s/d} f_{=n/d} \langle a_{s,j} \rangle \delta_j \\ &= \sum_{s,j} dV_{=s/d} \langle a_{s,j}^{n/d} \rangle f_{=n/d} \delta_j \\ &= \sum_{s,j,r,k} dV_{=s/d} \langle a_{s,j}^{n/d} \rangle V_{=r} \langle C(n/d,r)_{k,j} \rangle \delta_k \\ &= \sum_{s,j,r,k} dV_{=rs/d} \langle a_{s,j}^{rn/d} \rangle C(n/d,r)_{k,j} \delta_k \end{aligned}$$

where $d = (s,n)$. This is a sum of the type (2.3), which then is put into the form (2.1) by the algorithmic procedure outlined above.

To complete this picture we also define

$$\begin{aligned} V_{=r}(\sum_{s,j} V_{=s} \langle a_{s,j} \rangle \delta_j) &= \sum_{s,j} V_{=rs} \langle a_{s,j} \rangle \delta_j \\ \langle \otimes \rangle (\sum_{s,j} V_{=s} \langle a_{s,j} \rangle \delta_j) &= \sum_{s,j} V_{=s} \langle a_{s,j}^{\otimes} \rangle \delta_j \end{aligned}$$

("see also addition")

We have now defined a topological abelian (M) with operators $\langle \otimes \rangle$, $V_{=n}$, $f_{=n}$ for all $a \in \mathcal{L}_C$, $n \in \mathbb{N}$. (The topology is the obvious one). Note that (M) is definitely not a $\text{Cart}(\mathcal{L}_C)$ module. For one thing it is not at

all clear that \underline{f}_n is additive and obviously $\underline{f}_{n+m} = \underline{f}_{nm}$ does not hold in general. Before discussing the relations one must introduce to make a variant of (M) a Cart(L_C) module over some quotient ring L_C of \tilde{L}_C we note a homogeneity property. First make \tilde{L}_C into a graded ring by giving $C(n,r)_{i,j}$ degree $nr - 1$ for all $n,r \in \mathbb{N}$, $i,j \in \{1, \dots, m\}$. We then have

2.8. Lemma. Suppose that in the sum (2.3) each $a_{s,j,t}$ is homogeneous of degree $ks - 1$ for some $k \in \mathbb{N}$ independent of s,j,t . Then the $x_{s,j}$ in (2.6) are homogeneous of degree $ks - 1$.

Proof. To prove this by induction it suffices to show that under the hypothesis stated the $b_{1,j}$ and $a'_{r,s,j,t}$ of (2.5) are respectively of degree $k - 1$ and $krs - 1$ respectively. Now $b_{1,j} = a_{1,j,1} + a_{1,j,2} + \dots$ which is homogeneous of degree $k - 1$. As to the $a'_{r,s,j,t}$, they are of two types, viz. 1^o) $a'_{r,s,j,t} = a_{rs,j,t}$ which by hypothesis is homogeneous of degree $krs - 1$, and 2^o) $a'_{r,s,j,t} = b_{i,j}^{C(i,\ell)}_{k,j}$, with $i\ell = rs$. Now from (2.4) we see that $r_i(Z_1, \dots, Z_k)$ is homogeneous of degree i (if each Z_i is given degree 1) so that $b_{i,j} = r_i(a_{1,j,1}, a_{1,j,2}, \dots)$ is homogeneous of degree $i(k-1)$. It follows that $a'_{r,s,j,t} = b_{i,j}^{C(i,\ell)}_{k,j}$ is homogeneous of degree $\ell i(k-1) + i\ell - 1 = \ell ik - 1 = krs - 1$. This proves the lemma.

2.9. Corollary. Let $\underline{f}_{n=\ell} \delta_i = \underline{f}_n \left(\sum_{s,j} v_{s,j} \langle C(\ell,s)_{j,i} \rangle \delta_j \right) = \sum_{s,j} v_{s,j} \langle y_{n,\ell,s,j,i} \rangle \delta_j$ where the $y_{n,\ell,s,j,i}$ are calculated as in (2.7). Then $y_{n,\ell,s,j,i}$ is homogeneous of degree $n\ell s - 1$.

Proof. In this particular case of (2.7) we have $a_{s,j} = C(\ell,s)_{j,i}$. Thus $a_{s,j}^{rn/d} C(n/d,r)_{k,j}$ is homogeneous of degree $d^{-1}rn(\ell s - 1) + d^{-1}nr - 1 = d^{-1}rn\ell s - 1 = (d^{-1}rs)n\ell - 1$ and the corollary follows by lemma 2.8.

2.10. Lemma. If $\ell > 1$ then $y_{n,\ell,t,i,j} \equiv nC(\ell,nt)_{i,j} \pmod{\text{(decomposables)}}$ (Here (decomposables) stands for the ideal of \tilde{L}_C generated by all products of the form $C(n,r)_{i,j} C(s,t)_{k,\ell}$ with $n,s \in \mathbb{N} \setminus \{1\}$, $r,t \in \mathbb{N}$, $i,j,k,\ell \in \{1, \dots, m\}$).

Proof. From (2.7) we have

$$\sum_{t,j} v_{t,j} \langle y_{n,\ell,t,j,i} \rangle \delta_j = \sum_{s,r,j,k} v_{rs/d} \langle C(\ell,s)_{j,i}^{nr/d} C(n/d,r)_{k,j} \rangle \delta_k$$

where $d = (s, n)$ in the sum on the right. Choose a fixed $t \in \mathbb{N}$. By the rewriting procedure discussed in the beginning of this section a summand in the sum on the right can contribute to $y_{n, \ell, t, j, i}$ iff $d^{-1}rs \leq t$. Moreover, if this contribution is to be nonzero modulo decomposables we must in addition have $d = nr$, $d^{-1}n = 1$, $r = 1$, $k = j$ (because $\ell > 1$). It follows that s is a multiple of n and $s \leq tn$ so that the only contributions to $y_{n, \ell, t, j, i}$, which are possibly nonzero modulo decomposables, come from

$$\sum_{a=1}^t \sum_{n < C(\ell, an)} \langle C(\ell, an) \rangle_{j, i} \delta_j$$

However $n \langle C(\ell, an) \rangle_{j, i} = \langle nC(\ell, an) \rangle_{j, i} +$ (terms which are zero modulo decomposables). The lemma follows.

2.11 Remark. By definition one has $y_{1, n, s, j, i} = y_{n, 1, s, j, i} = C(n, s)_{j, i}$ so that lemma 2.10 does not hold for $\ell = 1$.

3. THE UNIVERSAL RING L_C .

Let L_C be the quotient ring of \hat{L}_C obtained by factoring out the ideal generated by the homogeneous polynomials

$$(3.1) \quad C(n\ell, t)_{j, i} - y_{n, \ell, t, j, i}, \quad n, \ell, t \in \mathbb{N}, \quad i, j \in \{1, \dots, m\}$$

3.2. Theorem. $L_C \cong \mathbb{Z} [T(n)_{i, j} \mid n = 2, 3, \dots; i, j \in \{1, \dots, m\}]$ as a graded ring, with $\text{degree}(T(n)_{i, j}) = n - 1$.

Proof. The ring L_C is graded because the polynomials (3.1) are homogeneous by corollary 2.8. Let $L_C^{(t)}$ be its homogeneous summand of degree $t - 1$ and let $M^{(t)}$ be the submodule of $L_C^{(t)}$ generated by the decomposables. Then $L_C^{(t)}/M^{(t)}$ is generated (as an abelian group) by the $C(s, r)$ with $sr = t$. Now by lemma 2.10 and the defining relations (cf. (3.1)) we see that modulo decomposables

$$C(rs, t)_{i, j} \equiv rC(s, rt)_{i, j}$$

for all $i, j \in \{1, \dots, m\}$, $s \in \mathbb{N} \setminus \{1\}$, $r \in \mathbb{N}$. It follows that if s is not a prime number, $s \neq 1$, and p is a prime number dividing s , then

$$(3.3) \quad C(s, r)_{i, j} \equiv p^{-1} s C(p, p^{-1} sr)_{i, j}$$

It readily follows that $L_C^{(t)}/M^{(t)}$ is the abelian group generated by the $C(p, p^{-1}t)_{i,j}$, where p runs through all prime divisors of t , subject to the relations

$$(3.4) \quad qC(p, p^{-1}t)_{i,j} \equiv pC(q, q^{-1}t)_{i,j}$$

for all prime number divisors p and q of t . If t is a power of a prime number p , $t = p^r$, this means that $L_C^{(t)}/M^{(t)}$ is a free abelian group of rank m^2 generated by the classes of the $T(t)_{i,j} = C(p, p^{-1}t)_{i,j}$. If t is not a power of a prime number let $P(t)$ be the set of prime numbers dividing t . Choose $\mu(p) \in \mathbb{Z}$ such that

$$(3.5) \quad \sum_{p \in P(t)} p\mu(p) = 1$$

Let

$$T(t)_{i,j} = \sum_{p \in P(t)} \mu(p)C(p, p^{-1}t)_{i,j}$$

It then follows from (3.3) and (3.4) that $L_C^{(t)}/M^{(t)}$ is the free abelian group of rank m^2 generated by the classes of the $T(t)_{i,j}$. This proves the theorem.

3.6. Remark. (Construction of a "universal $\text{Cart}(L_C)$ -module" (continued))

Let \mathbb{C}_C be the set of all expressions $\sum_{s,j} \underline{v}_s \langle a_{s,j} \rangle \delta_j$ with $a_{s,j} \in L_C$. Now

calculate sums and $\underline{f}_r \gamma$, $\langle a \rangle \gamma$, $\underline{v}_r \gamma$ for $\gamma \in \mathbb{C}_C$ as in section 2. Then \mathbb{C}_C is in fact a $\text{Cart}(L_C)$ module. One has of course $\underline{f}_{n=l} \delta_i = \underline{f}_{nl} \delta_i$ by the relations defining L_C . And, using this, one can now prove directly that the $\langle a \rangle$, \underline{f}_n , \underline{v}_n are additive and that all the relations (1.3) hold. This also follows from the isomorphism result below, cf. remark 4.7.

4. PROOF OF CARTIER'S THIRD THEOREM.

Let $F(X,Y)$ be any m -dimensional formal group law over a ring A . Let $\delta_1(t), \dots, \delta_m(t)$ be the standard \underline{v} -basis for $\mathbb{C}(F)$. Then we have unique expressions, cf. (1.7),

$$\underline{f}_n \delta_i(t) = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{v}_s \langle c(n,s)_{j,i} \rangle \gamma_j(t)$$

Now define $\tilde{\eta}: \tilde{L}_C \rightarrow A$ by $\tilde{\eta}(C(n,s)_{i,j}) = c(n,s)_{i,j}$.

Because $f_{\underline{n}=\ell} f_{\underline{n}=\ell} \gamma_i(t) = f_{\underline{n}=\ell} \gamma_i(t)$ in $\widehat{C}(F)$ for all m, ℓ, i it follows that

$$\tilde{\eta}(y_{n,\ell,s,j,i}) = c(n,\ell,s)_{j,i}$$

for all $s, \ell, n \in \mathbb{N}$, $i, j \in \{1, \dots, m\}$. Therefore $\tilde{\eta}$ induces a homomorphism of rings $\eta_C: L_C \rightarrow A$. We can in particular apply this to the case $F(X, Y) = F_R(X, Y)$, the universal curvilinear m -dimensional formal group law over $\mathbb{Z}[R] = \mathbb{Z}[R_n(i, j) | n \in \mathbb{N} \setminus \{1\}, i, j \in \{1, \dots, m\}]$ of [3], part IV. This gives us a homomorphism.

$$(4.1) \quad \eta_C: L_C \rightarrow \mathbb{Z}[R]$$

4.2. Theorem. The homomorphism η_C of (4.1) is an isomorphism of graded rings.

Proof. Let $f_R(X)$, the logarithm of $F_R(X, Y)$, be equal to $f_R(X) = \sum_{n=1}^{\infty} b_n(R) X^n$. Recall that

$$(4.3) \quad b_n(R) = \sum_{(i_1, \dots, i_s)} d(i_1, \dots, i_s) R_{i_1}^{(i_1)} R_{i_2}^{(i_1 \dots i_{s-1})} \dots R_{i_s}^{(i_1 \dots i_{s-1})},$$

$$b_1(R) = I_m$$

where R_k is the matrix $(R_k(j, \ell))_{j, \ell}$ and the sum is over all sequences (i_1, \dots, i_s) , $i_j \in \mathbb{N} \setminus \{1\}$, $s \geq 1$, $i_1 i_2 \dots i_s = n$. Here the $d(i_1, \dots, i_s)$ are certain well-determined coefficients, and $R_i^{(j)}$ is the matrix obtained from R_i by raising each of its entries to the power j . Cf. [3], part IV, section 2. Then $b_n(R)$ is homogeneous of degree $n - 1$ if $R_k(j, \ell)$ is given degree $k - 1$. Let $\delta_1(t), \dots, \delta_m(t)$ be the standard \underline{V} -basis for $\widehat{C}(F_R)$ and let

$$(4.4) \quad f_{\underline{p}} \delta_i(t) = \sum_{s, j} v_s \langle c(p, s)_{j,i} \rangle \delta_j(t)$$

Now $f_R(\gamma(t) +_{F_R} \delta(t)) = f_R(\gamma(t)) + f_R(\delta(t))$ (ordinary coefficientwise sum), by the definition of logarithm. It follows that $f_R(f_{\underline{p}} \gamma(t)) = \sum_{i=1}^{\infty} p_i \gamma_i(t)$

if $f_R(\gamma(t)) = \sum z_i t^i$, $z_i \in \mathbb{Q}[R]^m$. Applying f_R to (4.4) it follows that

$$(4.5) \quad p b_{pn}(R) = \sum_{d|n} b_{n/d}(R) c(p,d)^{n/d}$$

(This formula provides the link with the "intertwined function pair" considerations of [2]).

With induction it follows from (4.5) that the $c(p,s) \in \mathbb{Z}[R]$ are homogeneous of degree $ps - 1$ (, that is to say the entries of these ~~max~~ matrices are homogeneous of degree $ps-1$). Now $b_{pn}(R) \equiv p^{-1} R_{pn}$ modulo decomposables if n is a power of p and $b_{pn}(R) \equiv R_{pn}$ modulo decomposables if n is not a power of a prime number, cf (4.3) and use that $d(i_1) = p^{-1}$ if i_1 is a power of a prime number p and $d(i_1) = 1$ if i_1 is not a power of a prime number, cf. [3], part IV, section 2.

It follows that η_C satisfies

$$\eta_C(C(p, p^{r-1})_{ij}) \equiv R_{p^r}(i,j) \pmod{\text{decomposables}}$$

$$\eta_C(C(p,s)_{i,j}) \equiv p R_{ps}(i,j) \pmod{\text{decomposables}}$$

if s is not a power of p . Hence $\eta_C(T_{p^r}(i,j)) \equiv R_{p^r}(i,j) \pmod{\text{decomposables}}$,

and if s is not a power of a prime number

$$\eta_C(T_s(i,j)) = \eta_C\left(\sum_{p \in P(s)} \mu(p) C(p, p^{-1}s)_{ij}\right) \equiv \sum_{p \in P(s)} \mu(p) p R_s(i,j) = E_s(i,j)$$

modulo(decomposables). Here $P(s)$ and the $\mu(p)$ are as in (3.5). It follows that η_C is indeed an isomorphism (homogeneous of degree zero).

4.6. Proof of Cartier's third theorem. Let \mathbb{C} be a reduced Cart(A) module, i.e. \mathbb{C} is a topological abelian group such that the properties of 1.8 hold. Let $\delta_1, \dots, \delta_m$ be a \underline{V} -basis for \mathbb{C} . Then every $\underline{f}_n \delta_i$ can be uniquely written as a convergent sum (cf. (1.7)),

$$\underline{f}_n \delta_i = \sum_{s=1}^{\infty} \sum_{j=1}^m \underline{V}_s \langle c(n,s)_{j,i} \rangle \delta_j \quad c(n,s)_{j,i} \in A$$

Now define $\tilde{\eta}: \tilde{\mathcal{L}}_C \rightarrow A$ by $\tilde{\eta}(C(n,s)_{j,i}) = c(n,s)_{j,i}$. Because $\underline{f}_n \underline{f}_\ell = \underline{f}_{n\ell}$

in \mathbb{C} we have that

$$\tilde{h}(C(n^{\ell}, s)_{j,i}) = \tilde{h}(y_{n,\ell,s,j,i})$$

for all n, ℓ, s, j, i so that \tilde{h} factorizes through L_C to define a homomorphism $\eta: L_C \rightarrow A$. Now let $\phi: \mathbb{Z}[R] \rightarrow A$ be equal to $\phi = \eta\eta_C^{-1}$, where η_C is the isomorphism of theorem 4.2. Then $F(X, Y) = \phi_* F_R(X, Y)$ is a formal group law over A such that $\mathcal{C}(F) \cong \mathbb{C}$ as a topological group with operators. The isomorphism is given by $\delta_i(t) \mapsto \delta_i$, where $\delta_1(t), \dots, \delta_m(t)$ is the standard \underline{V} -basis of $\mathcal{C}(F)$.

4.7. Remark. The module \mathcal{C}_C of 3.6 above is the module of curves of the formal group law $(\eta_C^{-1})_* F_R(X, Y)$ over L_C .

5. THE LOCAL CASE.

Choose a prime number p and suppose that A is a $\mathbb{Z}_{(p)}$ -algebra. Then the formal groups G over A can be classified by a much smaller group of curves $\mathcal{C}_p(G) \subset \mathcal{C}(G)$, with a much simpler ring of operators. In detail $\mathcal{C}_p(G) = \{\gamma(t) \in \mathcal{C}(G) \mid \underline{f}_q \gamma(t) = 0 \text{ for all prime numbers } q \neq p\}$. The operators on $\mathcal{C}_p(G)$ are the $\underline{v}_p, \underline{f}_p^i$ and $\langle a \rangle$, $a \in A, i \in \mathbb{N} \cup \{0\}$. The topological group of p -typical curves $\mathcal{C}_p(G)$ has filtration subgroups $\mathcal{C}_p^{(n)}(G) = \mathcal{C}_p(G) \cap \mathcal{C}^{p^n}(G)$ and is complete in the topology defined by this filtration. One shows that the topological groups with operators thus obtained satisfy

(i) $\mathcal{C}_p(G)$ is a complete Hausdorff topological group with operators $\underline{v}_p^i, \underline{f}_p^i, \langle a \rangle$ which satisfy analogous relations (1.3) obtained by setting

$\underline{v}_n = 0 = \underline{f}_k$ for all $k, n \in \mathbb{N}$ which are not a power of p .

(ii) The topology of $\mathcal{C}_p(G)$ is defined by the subgroups $\mathcal{C}_p^{(n)}(G) = \underline{v}_p^n \mathcal{C}_p(G)$

(iii) There are elements $\delta_i(t), i = 1, \dots, m \in \mathcal{C}_p(G)$ such that every curve $\gamma(t) \in \mathcal{C}_p(G)$ can be written as a unique convergent sum

$$\gamma = \sum_{n=0}^{\infty} \sum_{j=1}^m \underline{v}_p^n \langle a_{n,i} \rangle \delta_i$$

(To prove (iii) one uses Corollary (2.11) of [3] part IV to reduce to the case that G is a p -typical formal group and in that case the standard basis curves $\delta_i(t) = (0, \dots, 0, t, 0, \dots, 0)$ are p -typical and satisfy (iii)).

Inversely, the local version of Cartier's third theorem says that every filtered topological group $\mathcal{C} \supset \mathcal{C}^1 \supset \mathcal{C}^2 \supset \dots$ with operators $\underline{v}_p, \underline{f}_p^i, \langle a \rangle$ such that (i), (ii), and (iii) hold comes from a formal group over A .

The proof of this is a triviality, given the construction of the m -dimensional p -typical universal formal group $F_V(X,Y)$ of [3], part IV. Let $\delta_i(t)$ be the i -th standard curve over $\mathbb{Z}[V] = \mathbb{Z}[V_n(i,j) | n \in \mathbb{N}, i, j, \in \{1, \dots, m\}]$ in $\mathbb{C}(F_V)$. Then one calculates as in section 4 above

$$(5.1) \quad \mathbb{f}_p \delta_i(t) = \sum_{n=0}^{\infty} \sum_{j=1}^m y^n \langle V_{n+1}(j,i) \rangle \delta_j(t)$$

where one uses that the logarithm $f_V(X)$ of $F_V(X,Y)$ satisfies

$$f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}$$

$$p a_n(V) = a_{n-1}(V) V_1^{(p^{n-1})} + \dots + a_1(V) V_{n-1}^{(p)} + V_n$$

on the two sides use the same

cf. [3], parts II and IV. (Apply $f_V(X)$ to both sides of (5.1) and ascertain that the results

Now let \mathbb{C} be any topological group with operators $\mathbb{f}_p, \mathbb{V}_p, \langle a \rangle, a \in A$ such that (i) - (iii) hold. Choose $\delta_1, \dots, \delta_m$ such that (iii) holds and let

$$(5.2) \quad \mathbb{f}_p \delta_i = \sum_{n=0}^{\infty} \sum_{j=1}^m y^n \langle a_{n,j,i} \rangle \delta_j$$

Define $\phi: \mathbb{Z}[V] \rightarrow A$ by $\phi(V_{n+1}(j,i)) = a_{n,j,i}$. Then $\phi_* F_V(X,Y)$ is a formal group law over A such that $\mathbb{C}_p(\phi_* F_V) \cong \mathbb{C}$ as topological groups with operators. The isomorphism is given by $\delta_i(t) \mapsto \delta_i$, where $\delta_i(t)$ is the curve $(0, \dots, 0, t, 0, \dots, 0)$ in $\mathbb{C}_p(\phi_* F_V)$. This follows from (5.2) as compared to (5.1).

REFERENCES.

1. P. Cartier, Modules associés à un groupe formel commutatif. Courbes typiques, C.R. Acad. Sci. Paris 265(1967), A 129-132.
2. E. Ditters, Cours de groupes formels, Lect. Notes, Orsay, 1975
3. M. Hazewinkel, Constructing Formal Groups I - VIII, I: J. Pure and Applied Algebra 9(1977), 131-150; II: *ibid* 9(1977), 151-162; III: *ibid.* 10(1977), 1 - 18 ; IV-VII: Adv. Math., to appear; VIII: Compositio Math., submitted.
4. M. Lazard, Sur les théorèmes fondamentaux des groupes formels commutatifs, Indagationes Math. 35, 4 (1973), 281-300, Errata et Addenda, *ibid* 36, 2 (1974), 122-124.
5. M. Lazard, Commutative Formal Groups, Springer, 1975, Lect. Notes Math. 443.

REMARKS FOR THE TYPESETTER.

- double black underline: boldface (except for the standard boldface symbols \mathbb{Z} , \mathbb{N} , \mathbb{Q} , which are typed in as shown; besides these three only f and V occur boldface).
- encircled in black: script (Only C and M occur as script letters)
- greek letters have been typed in, the only ones occurring are λ , μ , γ , δ , ϕ , η .
- no fraktur letters occur.
- The typed script l which occurs is an ordinary latin lower case "el" (Use l as the typescript to distinguish from 1 ("one"))

Constructing Formal Groups

VII: isomorphisms and examples

by

Michiel Hazewinkel

Authors address:

Dept. Math., Econometric Inst.
Erasmus Univ. Rotterdam
50, Burg. Oudlaan
ROTTERDAM, The Netherlands

AMS (MOS) 1970 classification: primary 14L05.

1. Introduction

The first result of this paper says that we know an m -dimensional formal group over a characteristic zero ring A (i.e. $A \rightarrow A \otimes_{\mathbb{Z}} \mathbb{Q}$ is injective) if we know it over each $A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ and inversely that one can specify these "local" formal groups arbitrarily (up to isomorphism). If A is the ring of integers of a finite extension K of \mathbb{Q} (or a ring of \mathcal{V} -integers) then there is a refinement where the place of the $A \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$ is taken by $A_{\mathcal{V}}$, the rings of integers of the local completions $K_{\mathcal{V}}$ of K for each nonarchimedean valuation \mathcal{V} of K .

These results are useful e.g. to construct a formal group law over a global ring of integers A which over each localization $A_{\mathcal{V}}$ is isomorphic to a (twisted) Lubin-Tate formal group law. Cf. [4] and [2], chapter IV, sections 25.8 and 25.9.

Now let $F(X,Y)$ and $G(X,Y)$ be two one dimensional formal groups over \mathbb{Z}_p (or $\mathbb{Z}_{(p)}$ or any ring in between), then a result due to Honda and Hill ([5],[6]) says that $F(X,Y)$ and $G(X,Y)$ are isomorphic over \mathbb{Z}_p if and only if their reductions mod p are isomorphic over $\mathbb{Z}/(p)$. In section 4 below we give a new proof of this result based on the universal isomorphism $\alpha_{\mathcal{V},T}(X)$ of [1], part I, and the formulas which were also useful in [1], part III, cf. also [4], for the study of BP cohomology operations. (The relevant formulas are recalled in section 3 below). There is a bonus: the same proof works to give the corresponding result for formal A -modules where A is a discrete valuation ring with finite

residue field both in the case that A is of characteristic zero (where the result is due to Lubin [7]) and the case that A is of characteristic $p > 0$ (cf. [1] part VIII, [2] chapter IV, section 22.2).

Finally section 5 below gives two counter examples in dimensions 1 and 2 respectively which are designed to show that these reduction-isomorphism results do not easily generalize.

2. Local-global results

2.1. We shall use rather freely some notations and results from the earlier papers of this series, especially from [1] part IV. In particular $H_U(X, Y)$ over $\underline{\underline{Z}}[U] = \underline{\underline{Z}}[\dots, U(i, \underline{n}), \dots]$ is the m -dimensional universal formal group law constructed in [1] part IV, section 2.3.; $F_V(X, Y)$ over $\underline{\underline{Z}}[V]$ is the universal p -typical m -dimensional formal group constructed in the same place, and $\alpha_{V, T}(X): F_V(X, Y) \longrightarrow F_{V, T}(X, Y)$ is the universal isomorphism between p -typical formal group laws of [1], part IV theorem 2.12.

The local-global results of the title of this section are now

2.2 Theorem. Let A be a characteristic zero ring.

- (i) If $F(X,Y)$ and $G(X,Y)$ are two formal group laws over A then they are strictly isomorphic over A if and only if they are strictly isomorphic over $A \otimes \mathbb{Z}_{(p)}$ for all prime numbers p .
- (ii) Suppose we have given for every prime number p an m -dimensional formal group $F_{(p)}(X,Y)$ over $A \otimes \mathbb{Z}_{(p)}$. Then there exist an m -dimensional formal group law $F(X,Y)$ over A which is strictly isomorphic over $A \otimes \mathbb{Z}_{(p)}$ to $F_{(p)}(X,Y)$ for every prime number p .

2.3 , Theorem. Let A be the ring of integers of a number field K . For each nonarchimedean valuation v let A_v be the ring of integers of the local completion K_v of K .

- (i) If $F(X,Y)$ and $G(X,Y)$ are two formal group laws over A then they are strictly isomorphic over A if and only if they are strictly isomorphic over A_v for all nonarchimedean valuations v of K .
- (ii) Suppose we have given for every nonarchimedean valuation v an m -dimensional formal group law $F_{(v)}(X,Y)$ over A_v . Then there exists an m -dimensional formal group law $F(X,Y)$ over A which is strictly isomorphic to $F_{(v)}(X,Y)$ over A_v for all nonarchimedean valuations v .

2.4 . Proof of theorem 2.2.

- (i) The m -dimensional formal group laws $F(X,Y)$ and $G(X,Y)$ are strictly isomorphic if and only if the power series $g^{-1}(f(X))$ has its coefficients in A , where $f(X)$ and $g(X)$ are the logarithms of $F(X,Y)$, $G(X,Y)$. This is the case if and only if $g^{-1}(f(X)) \in A \otimes \mathbb{Z}_{(p)}[[X]]$ for all prime numbers p because A is of characteristic zero.

$\mathbb{Z}_{(p)}$ - algebra

(ii) Because $A \otimes \mathbb{Z}_{(p)}$ is a $\mathbb{Z}_{(p)}$ - algebra we can assume that all the $F_{(p)}(X,Y)$ are p -typical formal group laws. Let $v_p = (v_{1p}, v_{2p}, \dots)$ be a sequence of $m \times m$ matrices such that $F_{(p)}(X,Y) = F_{v_p}(X,Y)$, where $F_{v_p}(X,Y)$ is the formal group law obtained from the universal p -typical formal group law $F_V(X,Y)$ over $\mathbb{Z}[V]$ by substituting v_{ip} for V_i , $i \in \mathbb{N}$.

Up to strict isomorphism we can assume that the matrices $v_{i,p}$ have their coefficients in A and not just in $A \otimes \mathbb{Z}_{(p)}$. Indeed suppose that i is the smallest natural number such that $v_{i,p} \notin A^{m \times m}$. Then there exists a $t_i \in A \otimes \mathbb{Z}_{(p)}^{m \times m}$ and a $\bar{v}_{i,p} \in A^{m \times m}$ such that $\bar{v}_{i,p} = v_{i,p} + pt_i$.

(Let $v_{i,p} = n^{-1}(\hat{v}_{i,p})$, $(n,p) = 1$, $\hat{v}_{i,p} \in A^{m \times m}$, take $r, s \in \mathbb{Z}$ such that $ps + rn = 1$; take $\bar{v}_{i,p} = r\hat{v}_{i,p}$, $t_i = -n^{-1}s\hat{v}_{i,p}$).

Applying the isomorphism $\alpha_{v_p, t_p}(X)$ to $F_{v_p}(X,Y)$ with $t_p = (t_{p,1}, t_{p,2}, \dots)$, $t_{p,j} = 0$ if $i \neq j$, $t_{p,i} = t_i$ we find an isomorphic formal group law $F_{\bar{v}}(X,Y)$ with $\bar{v}_j = v_{p,j}$ for $j < i$, $\bar{v}_i = \bar{v}_{p,i}$.

Now let $H_U(X,Y)$ be the universal m -dimensional formal group law over $\mathbb{Z}[U]$. Substitute $U_{p^i} = v_{p,i}$ for all prime number powers p^i and $U(i, \underline{n}) = 0$ for all \underline{n} not of the form $p^i \underline{e}(j)$. Let $F(X,Y)$ be the formal group law over A thus obtained. Then $F(X,Y)$ is strictly isomorphic to $F_{v_p}(X,Y)$ over $A \otimes \mathbb{Z}_{(p)}$ because for each prime number p $H_U(X,Y)$ is strictly isomorphic to $F_V(X,Y)$ over $\mathbb{Z}_{(p)}[U]$ if one identifies V_i with U_{p^i} , $i = 1, 2, \dots$ (cf [1], part IV, theorem 2.10)

25. Remark.

Part (ii) of theorem 2.2 (also holds) if A is not necessarily of characteristic zero; in fact this hypothesis was not used in the proof of part (ii) given above,

To prove theorem 2.3 we need the strong approximation theorem of algebraic number theory. For the convenience of the reader we state it here explicitly in the form in which we shall use it.

2.6. Strong approximation theorem. Let \mathcal{V} be a finite set of nonarchimedean valuation on a number field K with ring of integers A and for each $v \in \mathcal{V}$ let a_v be an element of K_v , the completion of K with respect to v . For each $v \in \mathcal{V}$ choose an $r_v \in \mathbb{N}$. Then there exists an $a \in K$ such that $v(a - a_v) \geq r_v$ for all $v \in \mathcal{V}$ and $v(a) \geq 0$ for all $v \notin \mathcal{V}$. (Note that if $a_v \in A_v$, the ring of integers of K_v , for all $v \in \mathcal{V}$ then $a \in A$).

2.7. Proof of theorem 2.3 .

(i) trivial, as part (i) of 2.4.

(ii) As in 2.4 we can assume that the $F_{(v)}(X, Y)$ are all p -typical formal group laws. We are going to obtain $F(X, Y)$ by substituting inductively suitable values for the $U(i, \underline{n})$ in the universal formal group law $H_U(X, Y)$ over $\mathbb{Z}[U]$. Suppose we have already found elements $a(i, \underline{n}) \in A$ for $|\underline{n}| \leq n$ and power series $\alpha_{(v)}(X)$ such that mod (degree n)

$$(2.7.1) \quad F_{(n)}(X, Y) - \alpha_{(v), n}^{-1}(F_{(v)}(\alpha_{(v), n}(X), \alpha_{(v), n}(Y))) \equiv 0$$

where $F_{(n)}(X, Y)$ is the formal group law obtained by substituting $a(i, \underline{n})$ for $U(i, \underline{n})$ for $|\underline{n}| < n$ and $U(i, \underline{n}) = 0$ for $|\underline{n}| \geq n$.

By the comparison lemma ([1], part IV, cor. 5.4) there exist m -tuples of homogeneous forms $\Gamma_{(v)}(X)$ and an $m \times m$ matrices $M_{(v)}$ such that the differences (2.7.1) are mod (degree $n+1$) equal to

$$\Gamma_{(v)}(X) + \Gamma_{(v)}(Y) - \Gamma_{(v)}(X+Y) + M_{(v)}(v(n)^{-1}(X^n + Y^n - (X+Y)^n))$$

If n is not a power of a prime number, then $v(n) = 1$, take

$a(i, \underline{n}) = 0$ for all \underline{n} with $|\underline{n}| = n$ and let $\alpha_{(v), n+1}(X) =$

$\alpha_{(v), n}(X) + \Gamma_{(v)}(X) + M_{(v)}X^n$. Then (2.7.1) holds with $n+1$ instead of n . Now suppose that $n = p^r$ for a prime number p and $r \in \mathbb{N}$. Then $v(n) = p$. Let \mathcal{V} be the set of all valuations v "dividing" p (i.e. for which $v(p) > 0$). By the strong approximation theorem 2.6 there

exists a matrix a with coefficients in A such that $a \equiv M_{(v)} \pmod{pA_v}$ for all $v \in \mathcal{V}$. Let $N_{(v)} = p^{-1}(M_{(v)} - a)$. Now we take

$$a_{(i, n_{\underline{e}}(j))} = a_{ij} \text{ for } i = 1, \dots, m; j = 1, \dots, m$$

and

$$\alpha_{(v), n+1}(X) = \alpha_{(v), n}(X) + \Gamma_{(v)}(X) + N_{(v)}X^n \text{ for } v \in \mathcal{V}$$

$$\alpha_{(v), n+1}(X) = \alpha_{(v), n}(X) + \Gamma_{(v)}(X) + p^{-1}M_{(v)}X^n + aX^n \text{ for } v \notin \mathcal{V}$$

then (171) holds with $n + 1$ instead of n for all v . To see this use e.g. formula (23b) of [1], part IV. By induction this completes the proof.

3. The more dimensional isomorphism formula.

3.1. Let $F_V(X,Y)$ be the universal p -typical m -dimensional formal group law of [1] part IV and $\alpha_{V,T}(X): F_V(X,Y) \longrightarrow F_{V,T}(X,Y)$ be the universal isomorphism of [1], part IV, theorem 2.12. Let the logarithms of $F_V(X,Y)$, $F_{V,T}(X,Y)$ be respectively.

$$(3.1.1.) \quad f_V(X) = \sum_{n=0}^{\infty} a_n(V) X^{p^n}, \quad f_{V,T}(X) = \sum_{n=0}^{\infty} a_n(V,T) X^{p^n}$$

In [1] part III we derived a most usefull little formula for $a_n(V,T)$ for the one dimensional case ($m=1$), which was also rather important in [1] part V. Argueing exactly as in [1] part III, proposition 5.2 we find the following more dimensional version of this formula.

$$(3.1.2.) \quad \begin{aligned} p a_n(V,T) &= p T_n + \sum_{i=1}^n a_{n-i}(V,T) V_i^{\{p^{n-i}\}} + \\ &+ \sum_{k=2}^n \sum_{\substack{i+j=k \\ i,j \geq 1}} a_{n-k}(V) [V_i^{\{p^{n-k}\}} T_j^{\{p^{n-j}\}} - T_j^{\{p^{n-k}\}} V_i^{\{p^{n-i}\}}] \end{aligned}$$

where $M^{\{q\}}$ is the matrix obtained from a matrix M by raising each of the entries of M to the q -th power.

The formal group law $F_{V,T}(X,Y)$ is p -typical, hence there are unique polynomials $V_i \in \underline{\mathbb{Z}}[V;T]$ such that $F_{V,T}(X,Y) = F_{\bar{V}}(X,Y)$. These polynomials \bar{V}_i then satisfy

$$(3.1.3.) \quad pa_n(V,T) = a_{n-1}(V,T)\bar{V}_1^{\{p^{n-1}\}} + \dots + a_1(V,T)\bar{V}_{n-1}^{\{p\}} + \bar{V}_n$$

by the more dimensional version of formula (4.3.1) of [1] part I, which is proved in exactly the same way starting from the functional equation of $f_V(X)$ i.e.

$$f_V(X) = X + \sum_{i=1}^{\infty} p^{-i} V_i f_V^{\{p^i\}}(X^{p^i})$$

By combining formulas (3.1.2.) and (3.1.3.) one obtains a formula for T_n in terms of $a_i(V,T)$, $a_i(V)$, T_i , V_i and \bar{V}_i with $i < n$ which turns out to be usable. Cf. sections 4,5 below.

4. The \mathbb{Z}_p - $\mathbb{Z}/(p)$ theorem.

The theorem is

4.1. Theorem ([5],[6]) . Let $F(X,Y)$ and $G(X,Y)$ be two one dimensional formal groups over \mathbb{Z}_p (or $\mathbb{Z}/(p)$ or any ring in between). Then $F(X,Y)$ and $G(X,Y)$ are strictly isomorphic over \mathbb{Z}_p (or $\mathbb{Z}/(p)$ or ...) if and only if their reductions modulo p are isomorphic over $\mathbb{Z}/(p)$.

The proof of this theorem is in several steps. Let A be \mathbb{Z}_p , $\mathbb{Z}/(p)$ or any ring in between.

4.2. Proposition. Let $v = (v_1, v_2, \dots)$, $\hat{v} = (\hat{v}_1, \hat{v}_2, \dots)$ be two sequences of elements of A . Then the one dimensional formal groups $F_v(X,Y)$ and $F_{\hat{v}}(X,Y)$ are isomorphic over A if and only if $v_i \equiv \hat{v}_i \pmod{p}$ for all $i \in \mathbb{N}$ and then they are strictly isomorphic.

Proof. First suppose that $v_i \equiv \hat{v}_i \pmod{p}$ for all $i \in \mathbb{N}$. Put

$$(4.2.1.) \quad t_n = p^{-1} \sum_{i=1}^n \hat{a}_{n-i} (\hat{v}_i^p - v_i^p) + \sum_{k=2}^n \sum_{i+j=k} a_{n-k} (v_i^{n-k} t_j^p - t_j^{n-k} v_i^p)$$

where $\hat{a}_\ell = a_\ell(\hat{v})$ and $a_\ell = a_\ell(v)$ are the coefficients of the logarithms of $F_{\hat{v}}(X,Y)$ and $F_v(X,Y)$ respectively.

This determines t_n inductively. And by (3.1.2.), (3.1.3.) we have that

$\bar{V}_n(v,t) = \hat{v}_n$ so that $\alpha_{v,t}(X)$ will be a strict isomorphism over A of

$F_v(X,Y) \longrightarrow F_{\hat{v}}(X,Y) = F_{v,t}(X,Y)$ provided we can show that the t_i are

in A (and not just in $A \otimes \mathbb{Q}$). But $v_i \equiv \hat{v}_i \pmod{p}$ and assuming with induction that $t_1, \dots, t_{n-1} \in A$ we have also $v_i t_j^p \equiv t_j v_i^p \pmod{p}$. It follows that

$$\hat{v}_i^p \equiv v_i^p \pmod{(p^{n-i+1})}, \quad v_i^p t_j^p \equiv t_j^p v_i^p \pmod{(p^{n-k+1})}$$

so that indeed $t_n \in A$ because $p^{n-k} a_{n-k} \in A$, $p^{n-i} \hat{a}_{n-i} \in A$. Inversely suppose that $\alpha(X): F_v(X,Y) \longrightarrow F_{\hat{v}}(X,Y)$ is an isomorphism over A . We can write $\alpha(X) = \beta(X) \circ \gamma(X)$ where $\beta(X)$ is a strict isomorphism and $\gamma(X) = uX$ for some invertible element u of A . Let $G(X,Y)$ be equal to $uF_v(u^{-1}X, u^{-1}Y)$. Then the logarithm of $G(X,Y)$ is equal to $u \log_v(u^{-1}X)$ so that $G(X,Y) = F_{\tilde{v}}(X,Y)$ with \tilde{v}_i equal to

$$\tilde{v}_i = u^{-(p^i-1)} v_i$$

(This follows immediately from formula (4.1.2.) of [1] part I for $a_n(V)$).

Now $u^{-(p^i-1)} \equiv 1 \pmod{p}$. So it suffices to show that $\tilde{v}_i \equiv \hat{v}_i \pmod{p}$.

I.e. we are reduced to the case that $\alpha(X)$ is a strict isomorphism. But then by the universality of the strict isomorphism $\alpha_{V,T}(X)$ there are $t_1, t_2, \dots \in A$ such that $V_n(v, t) = \hat{v}_n$, i.e. there are $t_1, t_2, \dots \in A$ such that (4.2.1.) holds. And this shows inductively that $\hat{v}_n \equiv v_n \pmod{p}$ (Take $i=n$ in the first sum of (4.2.1.) to isolate the term $p^{-1}(\hat{v}_n - v_n)$).

4.3. Proof of theorem 4.1. Let $F(X,Y)$, $G(X,Y)$ be two formal groups over A such that their reductions $\bar{F}(X,Y)$, $\bar{G}(X,Y)$ are isomorphic over $\underline{\mathbb{Z}}/(p)$. Let $\alpha(X)$ be any lift of this isomorphism and let $H(X,Y) = \alpha^{-1}G(\alpha X, \alpha Y)$. Then $H(X,Y)$ reduces to $\bar{F}(X,Y)$ modulo p and we must show that $F(X,Y)$ and $H(X,Y)$ are isomorphic, i.e. we are reduced to the case that $\bar{F}(X,Y) = \bar{G}(X,Y)$. Let $F_S(X,Y)$ be the one dimensional formal group law over $\underline{\mathbb{Z}}/(p)[S]$ which is

universal for one dimensional formal group laws over $\underline{\mathbb{Z}}_{(p)}$ -algebras (Cf. [1] part I, theorem 2.5). Let $s = (s_2, s_3, \dots)$, $\hat{s} = (\hat{s}_2, \hat{s}_3, \dots)$ be such that $F(X,Y) = F_s(X,Y)$, $G(X,Y) = F_{\hat{s}}(X,Y)$. Then by the uniqueness part of the universality property of $F_s(X,Y)$ we have $\bar{F}(X,Y) = \bar{G}(X,Y)$ if and only if $s_i \equiv \hat{s}_i \pmod{p}$. Now by [1] part I, theorem 2.10, $F_s(X,Y)$ and $F_{\hat{s}}(X,Y)$ are strictly isomorphic to the p -typical formal group laws $F_v(X,Y)$, $F_{\hat{v}}(X,Y)$ with $v_i = s_i/p^i$, $\hat{v}_i = \hat{s}_i/p^i$. Hence $v_i \equiv \hat{v}_i \pmod{p}$ so that $F_v(X,Y)$ and $F_{\hat{v}}(X,Y)$ are strictly isomorphic by proposition 4.2. This proves that $F(X,Y)$ and $G(X,Y)$ are isomorphic over A if their reductions are isomorphic. So it only remains to show that this implies that $F(X,Y)$ and $G(X,Y)$ are also strictly isomorphic. Both $F(X,Y)$, $G(X,Y)$ are strictly isomorphic to p -typical formal groups so we can assume that they are p -typical. Then an isomorphism $\alpha(X)$ again decomposes into a strict one and one of the form $\gamma(X) = uX$, $u \in A^*$. So it only remains to show that if $H(X,Y) = uF_v(u^{-1}X, u^{-1}Y)$ for some $u \in A^*$ then $H(X,Y)$ and $F_v(X,Y)$ are strictly isomorphic. As before we then have $H(X,Y) = F_{\tilde{v}}(X,Y)$ with $\tilde{v}_i = u^{-(p^i-1)}v_i$ so that $\tilde{v}_i \equiv v_i \pmod{p}$ and another application of proposition 4.2. shows that $H(X,Y)$ and $F_v(X,Y)$ are indeed strictly isomorphic. This concludes the proof of the theorem.

4.4. Corollary. Two p -typical formal group laws over $\underline{\mathbb{Z}}/(p)$ are isomorphic if and only if they are identical. (NB this does not mean that all isomorphisms are equal to the identity).

Proof. Let $\bar{\alpha}(X): \bar{F}(X,Y) \longrightarrow \bar{G}(X,Y)$ be an isomorphism. Let $F(X,Y), G(X,Y)$ be two p -typical lifts of $\bar{F}(X,Y), \bar{G}(X,Y)$. Then $F(X,Y)$ and $G(X,Y)$ are (strictly) isomorphic by theorem 4.1. which by proposition 4.2. implies that their reductions are equal.

5. Two examples.

We conclude with two counter examples to imaginable generalizations of theorem 4.1.

5.1. Example. Let $W_{3^\infty}(\mathbb{F}_9) = \mathbb{Z}_3[i]$, $i^2 = -1$ be the ring of integers of the unramified extension of degree 2 of \mathbb{Q}_3 . Consider the sequences of elements $v = (0, i, 0, 0, \dots)$ and $\bar{v} = (3i, i, 0, 0, \dots)$, ^(and) consider the ^{one dimensional} formal group laws $F_v(X, Y)$, $F_{\bar{v}}(X, Y)$ over $\mathbb{Z}_3[i]$. The reductions mod 3 of these formal group laws over \mathbb{F}_9 are equal. We show that $F_v(X, Y)$ and $F_{\bar{v}}(X, Y)$ are not isomorphic over $\mathbb{Z}_3[i]$.

Indeed suppose that $\alpha(X) = uX + u_2X^2 + \dots$ were an isomorphism. As usual we break up $\alpha(X)$ into a composite.

$$F_v(X, Y) \xrightarrow{\beta(X)} G(X, Y) \xrightarrow{\gamma(X)} F_{\bar{v}}(X, Y)$$

where $\beta(X) = uX$ and $\gamma(X)$ is a strict isomorphism. Then $G(X, Y) = u F_{\bar{v}}(u^{-1}X, u^{-1}Y)$. so that $\log_G(X) = u \log_{F_{\bar{v}}}(u^{-1}X)$ which means that $G(X, Y) = F_{\bar{v}}(X, Y)$ with

$\hat{v} = (0, u^{-8}i, 0, 0, \dots)$. Now $\gamma(X)$ is a strict isomorphism between p-typical formal group laws. By the universality of the strict isomorphism $\alpha_{V, \Gamma}(X)$ this means that there must be elements t_1, t_2, \dots in $\underline{\mathbb{Z}}[i]$ such that $f_{\bar{v}}(X) = f_{\hat{v}, t}(X)$. According to (3.1.2) and (3.1.3) above this means that we must have

$$\frac{\bar{v}_1}{3} = \frac{\hat{v}_1}{3} + t_1$$

i.e. $t_1 = i$, and (looking at the coefficients of X^{27})

$$\begin{aligned} \frac{\bar{v}_3}{3} + \bar{a}_1 \frac{\bar{v}_2^3}{3} + \bar{a}_2 \frac{\bar{v}_1^9}{3} &= \frac{\hat{v}_3}{3} + \bar{a}_1 \frac{\hat{v}_2^3}{3} + \bar{a}_2 \frac{\hat{v}_1^9}{3} + \frac{\hat{v}_1}{3} \left(\frac{\hat{v}_1^3 t_1^9 - t_1^3 \hat{v}_1^9}{3} \right) \\ &+ \frac{\hat{v}_1 t_2^3 - t_2 \hat{v}_1^9}{3} + \frac{\hat{v}_2 t_1^9 - t_1 \hat{v}_2^3}{3} + t_3 \end{aligned}$$

where $f_{\bar{v}}(X) = \sum_{i=0}^{\infty} \bar{a}_i X^{3^i}$. Substituting the known values of $\bar{v}_1, \bar{v}_2, \bar{v}_3, \dots$, $\hat{v}_1, \hat{v}_2, \dots$, i.e. $\bar{v}_1 = 3i$, $\hat{v}_1 = 0$, $\bar{v}_2 = i$, $\hat{v}_2 = u^{-8}i$, $\bar{v}_3 = \hat{v}_3 = 0$ we find that we must have

$$(5.1.1) \quad \bar{a}_1 \frac{\bar{v}_2^3}{3} + \bar{a}_2 \frac{\bar{v}_1^9}{3} = \bar{a}_1 \frac{\hat{v}_2^3}{3} + \frac{\hat{v}_2 t_1^9 - t_1 \hat{v}_2^3}{3} + t_3$$

Now $\bar{a}_1 = \frac{1}{3} \bar{v}_1 = i$, and $\hat{v}_2 = u^{-8}i \equiv i = \bar{v}_2 \pmod{3}$ so that $\bar{a}_1 \frac{\bar{v}_2^3}{3} \equiv \bar{a}_1 \frac{\hat{v}_2^3}{3} \pmod{(\underline{\mathbb{Z}}_3[i])}$. Further $\bar{v}_1^9 = (3i)^9 \equiv 0 \pmod{(3^3 \underline{\mathbb{Z}}_3[i])}$ so that $\frac{\bar{v}_1^9}{3} \equiv 0 \pmod{(\underline{\mathbb{Z}}_3[i])}$. Hence it follows from (5.1.1) that we must have

$$(5.1.2) \quad \hat{v}_2 t_1^9 - t_1 \hat{v}_2^3 \equiv 0 \pmod{(3^3 \underline{\mathbb{Z}}_3[i])}$$

However $t_1=i$ and $\hat{v}_2=u^{-8}i \equiv i \pmod{3}$ which contradicts (5.1.2).

5.2. Example. Now let $F_v(X,Y)$ over $\underline{\mathbb{Z}}[V]$ be the two dimensional universal p-typical formal group, cf. [1], part IV. Consider the two sequences of 2x2 matrices

$$v = \left(\begin{pmatrix} 10 \\ 00 \end{pmatrix}, \begin{pmatrix} 00 \\ 01 \end{pmatrix}, \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \dots \right)$$

$$\bar{v} = \left(\begin{pmatrix} 1p \\ p0 \end{pmatrix}, \begin{pmatrix} 00 \\ 01 \end{pmatrix}, \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \begin{pmatrix} 00 \\ 00 \end{pmatrix}, \dots \right)$$

and let $F_v(X,Y)$ and $F_{\bar{v}}(X,Y)$ be the formal group laws over $\underline{\mathbb{Z}}$ which are obtained by substituting $v_i(j,k)$ and $\bar{v}_i(j,k)$ for $V_i(j,k)$ in $F_v(X,Y)$, $i=1,2,\dots$; $j,k=1,2$. Then $\bar{F}_v(X,Y) = \bar{F}_{\bar{v}}(X,Y)$ over $\underline{\mathbb{F}}_p$. We show that $F_v(X,Y)$ and $F_{\bar{v}}(X,Y)$ are not isomorphic over $\underline{\mathbb{Z}}_p$. Note that $F_v(X,Y)$ and $F_{\bar{v}}(X,Y)$ are both of height 3, hence in particular of finite height.

Suppose that $\alpha(X) : F_v(X,Y) \longrightarrow F_{\bar{v}}(X,Y)$ is an isomorphism. As usual we decompose $\alpha(X)$ into an isomorphism $\beta(X)=u^{-1}X : F_v(X,Y) \longrightarrow G(X,Y)$ and a strict isomorphism $\gamma(X) : G(X,Y) \longrightarrow F_{\bar{v}}(X,Y)$. Here u is invertible (over $\underline{\mathbb{Z}}_p$) 2x2 matrix. The logarithm of $G(X,Y)$ is equal to

$$\text{Log}_G(X) = u^{-1} f_v(uX)$$

As a rule $G(X,Y)$ is not a p-typical formal group law. However, by [1], part IV theorem 2.10 $G(X,Y)$ is strictly isomorphic to a p-typical formal group law whose logarithm is obtained from $\text{log}_G(X)$ by simply striking out all terms in $\text{log}_G(X)$ which shouldn't be there for a p-typical formal group law. This means that $G(X,Y)$ is strictly isomorphic to the p-typical formal group law $\hat{G}(X,Y)$ with logarithm

$$(5.2.1) \quad \log_{\hat{G}}(X) = X + u^{-1} a_1(v) u^{\{p\}} X^p + u^{-1} a_2(v) u^{\{p^2\}} X^{p^2} + \dots$$

where $f_v(X) = \sum_{i=1}^{\infty} a_i(v) X^{p^i}$ and $u^{\{p^i\}}$ is the matrix obtained from u by raising each of its entries to the power p^i and where, as usual X^{p^i} denotes the columnvector $(X_1^{p^i}, X_2^{p^i})$.

Composing the strict isomorphism $\hat{G}(X,Y) \longrightarrow G(X,Y)$ with the strict isomorphism $\gamma(X): G(X,Y) \longrightarrow F_{\underline{v}}(X,Y)$ we find a strict isomorphism $\delta(X): \hat{G}(X,Y) \longleftarrow F_{\underline{v}}(X,Y)$. By the universality of the strict isomorphism $\alpha_{\underline{v},\underline{T}}(X)$ (2 dimensional case ; cf. [1], part IV) this means that these must be 2×2 matrices t_1, t_2, \dots with coefficients in $\mathbb{Z}_{\underline{p}}$ such that

$$(5.2.2) \quad f_{\hat{v},t}(X) = f_{\underline{v}}(X)$$

where $\hat{v} = (\hat{v}_1, \hat{v}_2, \dots)$ is a sequence of matrices such that $F_{\hat{v}}(X,Y) = \hat{G}(X,Y)$.

(Such a sequence of matrices exists because $\hat{G}(X,Y)$ is p -typical). From

(5.2.1) we see that

$$\frac{\hat{v}_1}{p} = u^{-1} a_1(v) u^{\{p\}} = u^{-1} \frac{v_1}{p} u^{\{p\}}$$

(5.2.3)

$$\frac{\hat{v}_1 \hat{v}_1^{\{p\}}}{p^2} + \frac{\hat{v}_2}{p} = u^{-1} a_2(v) u^{\{p^2\}}$$

and (5.2.2) gives us that (cf formulas (3.1.2), (3.1.3) above

$$\frac{\hat{v}_1}{p} + t_1 = \frac{\bar{v}_1}{p}$$

(5.2.4)

$$a_1(\bar{v}) \frac{\bar{v}_1^{[p]}}{p} + \frac{\bar{v}_2}{p} = t_2 + a_1(\bar{v}) \frac{\hat{v}_1^{[p]}}{p} + \frac{\hat{v}_2}{p} + \frac{\hat{v}_1 t_1^{[p]} - t_1 \hat{v}_1^{[p]}}{p}$$

Suppose that $u = \begin{pmatrix} b & c \\ d & e \end{pmatrix}$. Now $u^{[p]} \equiv u \pmod p$ and by (5.2.4) $\hat{v}_1 \equiv \bar{v}_1 \pmod p$. Using this in (5.2.3) we find that u must satisfy.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b & c \\ d & e \end{pmatrix} \equiv \begin{pmatrix} b & c \\ d & e \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod p$$

This gives us

$$c \equiv d \equiv 0 \pmod p$$

so that u is of the form

$$u = \begin{pmatrix} b & py \\ pz & e \end{pmatrix}$$

Substituting this in (5.2.3) gives that modulo (p^2)

$$\hat{v}_1 = \det(u)^{-1} \begin{pmatrix} e & -py \\ -pz & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} b^p & p^p y^p \\ p^p z^p & e^p \end{pmatrix} \equiv \begin{pmatrix} b^{p-1} & 0 \\ -pze^{-1} b^{p-1} & 0 \end{pmatrix}$$

which gives mod p^2 for $p\hat{v}_2$ by (5.2.3) using $p^2 a_2(v) = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$,

$$p\hat{v}_2 \equiv \det(u)^{-1} \begin{pmatrix} e & -py \\ -pz & b \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} b^{p^2} & p^{p^2} y^{p^2} \\ p^{p^2} z^{p^2} & e^{p^2} \end{pmatrix} = \begin{pmatrix} b^{p^2-1} & 0 \\ -p^2 e^{-1} z b^{p^2-1} & 0 \end{pmatrix}$$

$$\equiv (eb)^{-1} \begin{pmatrix} e - py & \\ -pz & b \end{pmatrix} \begin{pmatrix} b^{p^2} & 0 \\ 0 & pe^{p^2} \end{pmatrix} = \begin{pmatrix} b^{p^2-1} & 0 \\ -pe^{-1}zb^{p^2-1} & 0 \end{pmatrix}$$

$$\equiv \begin{pmatrix} 0 & 0 \\ 0 & pe^{p^2-1} \end{pmatrix}$$

so that we find

$$\hat{v}_2 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p}, \quad \hat{v}_1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod{p}$$

This means that

$$(5.2.5) \quad \hat{v}_2 \equiv \bar{v}_2 \pmod{p}, \quad \hat{v}_1 \equiv \bar{v}_1 \pmod{p}$$

and hence

$$(5.2.6) \quad -\hat{v}_1^{[p]} \equiv \bar{v}_1^{[p]} \pmod{p^2}$$

Using (5.2.5) and (5.2.6) in the second line of (5.2.4) we must have

$$(5.2.7) \quad \hat{v}_1 t_1^{[p]} - t_1 \hat{v}_1^{[p]} \equiv 0 \pmod{p}$$

$$\text{But } t_1 = p^{-1}(\bar{v}_1 - \hat{v}_1) = p^{-1} \begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix} = p^{-1} \begin{pmatrix} 1 + p\hat{y} & 0 \\ p\hat{z} & 0 \end{pmatrix} = \begin{pmatrix} -\hat{y} & 1 \\ 1 - \hat{z} & 0 \end{pmatrix}$$

where $\hat{z}, \hat{y} \in \mathbb{Z}_p$ are such that $b^{p-1} = 1 + p\hat{y}$, $-pzc^{-1}b^{p-1} = p\hat{z}$,

so that modulo p

$$\hat{v}_1 t_1^{[p]} \equiv \hat{v}_1 t_1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} -\hat{y} & 1 \\ 1-\hat{z} & 0 \end{pmatrix} \equiv \begin{pmatrix} -\hat{y} & 1 \\ 0 & 0 \end{pmatrix} \pmod{p}$$

$$t_1 \hat{v}_1^{[p]} \equiv t_1 \hat{v}_1 \equiv \begin{pmatrix} -\hat{y} & 1 \\ 1-\hat{z} & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \equiv \begin{pmatrix} -\hat{y} & 0 \\ 1-\hat{z} & 0 \end{pmatrix} \pmod{p}$$

which is a contradiction with (5.2.7). This proves that the two 2-dimensional formal group laws $F_v(X, Y)$, $F_{-v}(X, Y)$ over $\underline{\mathbb{Z}}_p$ are not isomorphic.

References

1. M. Hazewinkel, Constructing formal groups I-VIII (I,II,III to appear J. pure and applied algebra; IV to appear Adv. Math; V, VI, VII submitted Adv. Math; VIII submitted Compositio Math. all available in preprint form as reports 7119, 7201, 7207, 7322, 7505, 7507, 7514, 7519. Econometric Inst., Erasmus Univ. Rotterdam, 1971-1975)
2. M. Hazewinkel, Formal groups and applications, in preparation.
3. M. Hazewinkel, Twisted Lubin-Tate formal group laws, ramified Witt vectors and Artin-Hasse exponential mappings(submitted Bull. AMS)
4. M. Hazewinkel, A universal isomorphism of p -typical formal groups and operations in Brown-Peterson cohomology, *Indagationes Math.* 38, 3(1976), 195-199.
5. W. Hill, Formal groups and zeta-functions of elliptic curves, *Inv. Math.* 12(1971), 321-326.
6. T. Honda, Formal groups and zetafunctions, *Osaka J. Math.* 5 (1968), 199-213.
7. J. Lubin, Formal A -modules defined over A , *Symp. Math. INDAM 1968/1969*, vol. 3, Acad. Press 1970, 241-245.