ERASMUS UNIVERSITY ROTTERDAM

ECONOMETRIC INSTITUTE

Report 7505/M

ON MORE DIMENSIONAL UNIVERSAL FORMAL GROUPS

by Michiel Hazewinkel

April 10th 1975

Preliminary

1. INTRODUCTION.

In this paper we give an explicit construction for the logarithms of more dimensional universal formal groups of various kinds. This has already been done (rather hurriedly) in [2]. There are several reasons to take this up again: (i) the treatment in [2] is rather too sketchy (ii) several new results have turned up, and the third reason (and maybe the most important one) is the following:
Given the construction of a suitable candidate for a universal formal group (e.g. the constructions of [2]), it turns out that one can prove universality directly by a straightforward more dimensional extension of the method which Buhštaber and Novikov have used in [1] to prove the universality of the formal group of complex cobordism and which we have already used twice in [3] and [4]. In particular one avoids Lazard's truly tough (and computational) comparison lemma between more dimensional formal groups. (This lemma can be found in [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, $\mathbb{N} = \{1, 2, 3, \ldots\}$. If $F(X,Y)$ is a formal group over a ring A and $\phi : A \to B$ 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 $\underline{n} = (n_1, \ldots, n_m)$ is an m-tuple of integers ≥ 0. Let $||\underline{n}|| = n_1 + n_2 + \ldots + n_m$. We shall only consider multiindices $\underline{n}$ with $||\underline{n}|| \geq 1$. We use $\underline{e}(i)$, $i = 1, \ldots, m$ to denote the multiindex $(0, \ldots, 0, 1, 0, \ldots, 0)$ 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 $i\underline{n} = (in_1, \ldots, in_m)$. We use $\underline{0}$

to denote the set of all multiindices $\underline{\underline{n}}$ with $||\underline{\underline{n}}|| \geq 1$ and $\underline{\underline{n}} \neq p^r \underline{\underline{e}}(i)$ for all $r = 1,2,\ldots$; $i = 1, \ldots, m$ and prime numbers $p \in \mathbb{N}$

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

2.3. Constructions.

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

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

and we define

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

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

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

and

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

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

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

Let $\mathbb{Z}[U]$ be short for $\mathbb{Z}[U(i,n)$; $\underline{n}$ a multiindex with $||\underline{n}|| \geq 2$, $i = 1, \ldots, m]$. 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 $\mathbb{N}$, 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 $(U(1,\underline{d}), \ldots, U(m,\underline{d}))$. Finally $X^{\underline{n}} = X_1^{n_1} \ldots X_m^{n_m}$ and if a is a vector $aX^{\underline{n}} = (a_1X^{\underline{n}}, \ldots, a_mX^{\underline{n}})$. We now define the column m-vectors $a_{\underline{n}}$ for all multiindices $\underline{n}$ with $||\underline{n}|| \geq 1$ as

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

where the sum is over all sequences $(q_1, \ldots, q_t, \underline{d})$ such that $q_1 \cdot \ldots \cdot q_t \underline{d} = \underline{n}$, $\underline{d} \in \underline{D}$, 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 ϕ: $\mathbb{Z}[U] \to \mathbb{Z}[U]$ is the homomorphism which takes $U(i,q\underline{e}(j))$ into itself for $i,j = 1, \ldots, m$ and prime powers q, and which sends $U(i,\underline{n})$ to zero for all $\underline{n} \in \underline{E}$, $i = 1, \ldots, m$, where $\underline{E} = \underline{D} \setminus \{\underline{e}(i) \mid i=1,\ldots,m\}$

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 $\mathbb{Z}[V]$, $\mathbb{Z}[V;T]$, $\mathbb{Z}[U]$ and $\mathbb{Z}[U]$.

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 ϕ : $\mathbb{Z}[U] \to A$ 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 $\mathbb{Z}[U]$.

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 $n \in \mathbb{N}$. One now defines a Frobenius operator $\underset{\sim}{f}_n$ in exactly the same way as for one dimensional formal groups. I.e. formally we have that

$$(2.7.1) \qquad (\underset{\sim}{f}_n\gamma)(Z) = \gamma(\zeta_n Z^{1/n}) +_F \gamma(\zeta_n^2 Z^{1/n}) +_F \ldots +_F \gamma(\zeta_n^n Z^{1/n})$$

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 $(\underset{\sim}{f}_q^F\gamma)(Z) = 0$ 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 $\gamma(Z) = (Z^{p^{r_1}},\ldots,Z^{p^{r_m}})$, $r_i \in \mathbb{N} \cup \{0\}$ are p-typical.

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

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

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 p-typical universal formal group (of dimension m).

I.e. for every p-typical formal group $G(X,Y)$ over a ring A there is a unique homomorphism $\phi\colon \mathbb{Z}[V] \to A$ such that $F_V^{\phi}(X,Y) = G(X,Y)$

Let κ: $\mathbb{Z}[V] \to \mathbb{Z}[U]$ be the injective homomorphism defined by $\kappa(T_i(j,k)) = U(j,p^i\underline{e}(k))$, and $\lambda : \mathbb{Z}[U] \to \mathbb{Z}_{(p)}[U]$ 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 $\underline{k}\underline{\ell} = (k_1\ell_1, \ldots, k_m\ell_m)$. Let $\underline{0}$ be the multiindex $\underline{0} = (0,\ldots,0)$. In [7] Lazard defines a formal group $F(X,Y)$ over a ring A to be curvilinear (curviligne) if

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

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

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

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

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

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 $\mathbb{Z}[U]$.

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, $i \in \mathbb{N} \setminus \{1\}$ as in [4] and determine $n(i_1, \ldots, i_s)$ for all sequences $(i_1, \ldots, i_s)$, $i_j \in \mathbb{N} \setminus \{1\}$ as in [4]. Let $d(i_1,\ldots,i_s) = n(i_1, \ldots,i_s)n(i_n,\ldots,i_s) \ldots n(i_s)\nu(i_1)^{-1}\nu(i_2)^{-1} \ldots \nu(i_s)^{-1}$. Now define the matrices $b_i(R)$ as

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

$$i = 2, 3, \ldots$$

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

We put

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

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

2.18. Theorem.

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

2.19. Because the $d(i_1,\ldots,i_s)$ 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 $b_i(R)$.

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

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 $\mathbb{Z}_{(p)}[V;W]$ where W is short for an additional set of indeterminates and V is as in 2.3.

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

$$(3.1.1)\qquad f_j(X) = g_j(X) + \sum_{i=1}^{\infty} \frac{V_i}{p} f_j(p^i)(X^{p^i})$$

Functional equation lemma.

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

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

(iii) If $h_2(X)$ is of the form $h_2(X) = X + \ldots$ 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 $n(q_1, \ldots, q_t)$ for all sequences of powers of prime numbers $(q_1, \ldots, q_t)$ such that (2.3.5) is satisfied. Let

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

where q_i is a power of the prime number p_i.

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

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

Proof. We prove (i) by induction. The case $t = 1$ is trivial. If $r = 1$, let $p_2 = p_3 = \ldots = p_s \neq p_{s+1}$. Then $p_2^{s-1}d(q_2,\ldots,q_t) \in \mathbb{Z}$ and $n(q_1,\ldots,q_t) \equiv 0 \bmod p_2^{s-1}$. Therefore $p_1 d(q_1,\ldots,q_t) = n(q_1,\ldots,q_t)d(q_2,\ldots,q_t) \in \mathbb{Z}$. Now let $r > 1$, then $p_1^{r-1}d(q_2,\ldots,q_t) \in \mathbb{Z}$.

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

To prove (ii) we distinguish two cases. If $r = 1$ then $d(q_2,\ldots,q_t) \in \mathbb{Z}_{(p_1)}$ by (i) and hence $d(q_1,\ldots,q_t) - p_1^{-1}d(q_2,\ldots,q_t) = p_1^{-1}(n(q_1,\ldots,q_t)-1)d(q_2,\ldots,q_t) \in \mathbb{Z}_{(p_1)}$, because $n(q_1,q_2,\ldots,q_t) \equiv 1 \bmod p_1$ if $p_1 \neq p_2$. If $p_1 = p_2 = \ldots = p_r \neq p_{r+1}$ with $r > 1$.

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

3.3. Lemma.

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

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

with $g_p(X) = X + \ldots \quad \mathbb{Z}_{(p)}[U][[X]]$ 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 $\mathbb{Z}_{(p)}[U][[X,Y]]$ for all prime number p. Hence $H_U(X,Y)$ in $\mathbb{Z}[U][[X,Y]]$. 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 $\mathbb{Z}[U][[X,Y]]$.

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 $\mathbb{Z}[V][[X,Y]]$ and $\mathbb{Z}[V;T][[X,Y]]$ respectively.

4. A LITTLE BIT OF MULTIDIMENSIONAL BINOMIAL COEFFICIENT ARITHMETIC.

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

$$(\underline{\underline{n}}) = \binom{n_1}{k_1}\binom{n_2}{k_2} \dots \binom{n_m}{k_m} \tag{1.1}$$

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

$$\nu(\underline{\underline{n}}) = \text{g.c.d.}\ \{(\underline{\underline{n}}); \underline{\underline{0}} < \underline{\underline{k}} < \underline{\underline{n}}\} \tag{1.2}$$

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

2. Let $n \in \mathbb{N}$, $n \geq 2$. Choose $\lambda_{n,1}, \dots, \lambda_{n,n-1}$ such that $\lambda_{n,1}\binom{n}{1} + \dots + \lambda_{n,n-1}\binom{n}{n-1} = \nu(n)$. If $\underline{\underline{n}}$ is of the form $n = n\,\underline{\underline{e}}(j)$, en if $\underline{\underline{0}} < \underline{\underline{k}} < \underline{\underline{n}}$, $\underline{\underline{k}} = k\,\underline{\underline{e}}(j)$ for some $0 < k < n$. We put $\lambda(\underline{\underline{n}},\underline{\underline{k}}) = \lambda_{n,k}$ r all $\underline{\underline{0}} < \underline{\underline{k}} < \underline{\underline{n}}$ in this case. If n is not of the form $n\,\underline{\underline{e}}(j)$, let i_1 the smallest natural number such that $n_{i_1} \neq 0$. For these n we take

$\underline{\underline{n}},\underline{\underline{k}}) = 0$ if $\underline{\underline{k}} \neq (0,\dots,0,n_{i_1},0,\dots,0)$, $\underline{\underline{0}} < \underline{\underline{k}} < \underline{\underline{n}}$ and $\lambda(\underline{\underline{n}},\underline{\underline{k}}) = 1$ if $= (0,0,\dots,0,n_{i_1},0,\dots,0)$. Then we have of course

$$\sum_{\underline{\underline{0}}<\underline{\underline{k}}<\underline{\underline{n}}} \lambda(\underline{\underline{n}},\underline{\underline{k}})(\underline{\underline{n}}) = \nu(\underline{\underline{n}}) \tag{2.1}$$

3. Lemma.

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

$$\sum_{\underline{\underline{0}}<\underline{\underline{k}}<\underline{\underline{n}}} \lambda(\underline{\underline{n}},\underline{\underline{k}})X(\underline{\underline{k}}) \tag{2.2}$$

$$(\underline{\underline{k}+\underline{\ell}})X(\underline{\underline{k}}+\underline{\ell}) - (\underline{\underline{\ell}+\underline{m}})X(\underline{\ell}+\underline{m}) \qquad \underline{\underline{k}} + \underline{\ell} + \underline{m} = \underline{\underline{n}},\ \underline{\underline{k}},\underline{\ell},\ \underline{m} > \underline{\underline{0}} \tag{2.3}$$

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 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 $\underline{j} = (j_1, \ldots, j_m)$ be a multiindex with $\underline{0} < \underline{j} < \underline{n}$ and $j_i < n_i$.

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 $\underline{0} < \underline{j} < \underline{n}$ such that $j_i < n_i$ as linear combinations of (4.2.2) and (4.2.3). But if $\underline{0} < \underline{j} < \underline{n}$ either $\underline{j}$ or $\underline{n} - \underline{j}$ has its i-th component smaller than n_i 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

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

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

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

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

$$(5.2.1)\qquad H_U(X,Y) = (H_U(1)(X,Y), \ldots, H_U(m)(X,Y))$$

and write

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

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

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

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 we 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 $G(X,Y) = (G(i)(X,Y), \ldots, G(m)(X,Y))$ and let

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

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

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

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

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

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

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

(5.3.3)

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

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

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 $F(X,Y) \equiv G(X,Y)$ mod (total degree n). Then there is an m-tuple of homogeneous forms Γ of degree n with coefficients in A and a m x m matrix M with coefficients in A such that

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

If one adds the restriction that $\Gamma(X)$ may contain no terms of the form aX_i^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. Give each $U(i,\underline{d})$ lexicographic degree $\underline{d}$.

Let $\underline{d} <_\ell \underline{n}$ stand for $\underline{d}$ is lexicographically smaller than $\underline{n}$, and let ℓdegree be short for lexicographic degree. Let $h_{U(\underline{n})}(X)$ and $H_{U(\underline{n})}(X)$

be obtained from $h_U(X)$ and $H_U(X)$ by substituting zero for all $U(i,\underline{\underline{d}})$ with $\underline{\underline{d}} \geq_\ell \underline{\underline{n}}$. Then one has from (2.3.6) that

$$(5.5.1) \qquad h_U(X) \equiv h_{U(\underline{\underline{n}})}(X) + \nu(\underline{\underline{n}})^{-1} U_{\underline{\underline{n}}} X^{\underline{\underline{n}}} \bmod (\text{ℓdegree} >_\ell \underline{\underline{n}})$$

and hence

$$(5.5.2) \qquad H_U(X,Y) \equiv H_{U(\underline{\underline{n}})}(X,Y) - U_{\underline{\underline{n}}}(\nu(\underline{\underline{n}})^{-1}((X+Y)^{\underline{\underline{n}}} - X^{\underline{\underline{n}}} - Y^{\underline{\underline{n}}}))$$

5.6. Lexicographic Comparison Lemma.

Let $F(X,Y)$, $G(X,Y)$ be two m-dimensional formal groups over a ring A, and suppose that $F(X,Y) \equiv G(X,Y) \bmod (\text{ℓdegree } n)$, then there is a unique vector $a = (a(1),\ldots,a(m))$, $a(i) \in A$ such that $F(X,Y) \equiv G(X,Y) - a(\nu(\underline{\underline{n}})^{-1}((X+Y)^{\underline{\underline{n}}} - X^{\underline{\underline{n}}} - Y^{\underline{\underline{n}}})) \bmod (\text{ℓdegree} >_\ell \underline{\underline{n}})$.

This follows immediately from (5.5.2) and theorem 2.5.

5.7. Proof of Theorem 2.9.

Let $F(X,Y)$ be p-typical m-dimensional formal group over a ring A.

There is a unique homomorphism $\phi : \mathbb{Z}[U] \to A$ such that $H_U^{\phi}(X,Y) = F(X,Y)$. We are going to prove that $\phi(U(i,\underline{\underline{d}}))$ is zero for all multiindices $\underline{\underline{d}}$ not of the form $p^i \underline{\underline{e}}(j)$. Suppose this is not true. Let $\underline{\underline{d}}$ be the lexicographically smallest multiindex for which $\phi(U(i,\underline{\underline{d}})) \neq 0$ for some $i \in \{1,\ldots,m\}$. Let $\psi = \phi \circ \kappa$ where κ is the natural inclusion $\mathbb{Z}[V] \to \mathbb{Z}[U]$, cf. just above 2.10 above. Let $G(X,Y) = F_V^{\psi}(X,Y)$. Then

$$(5.7.1) \qquad F(X,Y) \equiv G(X,Y) - a(\nu(\underline{\underline{d}})^{-1}((X+Y)^{\underline{\underline{d}}} - A^{\underline{\underline{d}}} - Y^{\underline{\underline{d}}})) \bmod (\text{ℓdegree} >_\ell \underline{\underline{d}})$$

where $a(i) = \phi(U(i,\underline{\underline{d}}))$.

First suppose that $\underline{\underline{d}}$ is not of the form $d\,\underline{\underline{e}}(j)$. Then, because at least two d_i are different from zero we can find $r_1, \ldots, r_m \in \mathbb{N}$ such that

$$(5.7.2) \qquad d_1 p^{r_1} + \ldots + d_m p^{r_m} \text{ is divisible by two primes different from } p$$

$$(5.7.3) \qquad d_1 p^{r_1} + \ldots + d_m p^{r_m} < e_1 p^{r_1} + \ldots + e_m p^{r_m} \text{ if } \underline{\underline{d}} <_\ell \underline{\underline{e}}$$

(To see to it that (5.7.3) holds it suffices to take $r_1, \ldots, r_m$

such that $p^{r_{m-1}} > p^{r_m}d_m$, $p^{r_{m-2}} > p^{r_m}d_m + p^{r_{m-1}}d_{m-1}$, ... , $p^{r_1} > p^{r_m}d_m + \ldots + p^{r_2}d_2$).

Let $q \neq p$ be a prime number dividing $d_1p^{r_1} + \ldots + d_mp^{r_m} = d'$ and let $\gamma(Z)$ be the curve $\gamma(Z) = (Z^{p^{r_1}},\ldots,Z^{p^{r_m}})$. Then, writing Y for $Z^{1/q}$, we obtain from (5.7.1) and (5.7.3).

$$(5.7.4) \qquad (\underset{\equiv q}{f}{}^F\gamma)(Y) \equiv (\underset{\equiv q}{f}{}^G\gamma)(Y) + aqZ^{d'} \mod (\text{degree} > d')$$

But the formal group $F_V(X,Y)$ is p-typical, hence $G(X,Y) = F_V^{\psi}(X,Y)$ is p-typical and F(X,Y) was supposed to be p-typical. Therefore (5.7.4) gives that aq = 0. There are at least two different primes $q \neq p$ dividing d and it follows that the vector a is equal to 0. Next suppose that $\underline{\underline{d}}$ is of the form $d\,\underline{\underline{e}}(j)$. Let q be a prime number dividing d different from p. (Such a prime number q exists because $\underline{\underline{d}} \neq p^r\underline{\underline{e}}(j)$, j = 1, ..., m, r = 0,1,2,...).
Because d is not a power of p we can find $r_1, \ldots, r_m$ such that (5.7.3) holds and such that $d' = d_1p^{r_1}+\ldots+d_mp^{r_n}$ is divisible by a prime $\neq p$. Let $\gamma(Z) = (Z^{p^{r_1}},\ldots,Z^{p^{r_m}})$; we obtain again

$$(5.7.5) \qquad \underset{\equiv q}{f}{}^F\gamma(Y) \equiv \underset{\equiv q}{f}{}^G\gamma(Y) + a(\nu(d)^{-1}qZ^{d'})$$

If d is a power of q. Then because $\underset{\equiv q}{f}{}^F\gamma(Y) = 0 = \underset{\equiv q}{f}{}^G\gamma(Y)$ we get a = 0, and if d is not a prime power there are two different primes $\neq p$ dividing d'. Hence a = 0 also in that case. This proves the existence of a $\chi : \mathbb{Z}[V] \to A$ such that $F_V^{\chi}(X,Y) = F(X,Y)$. The homomorphism χ is also unique, for otherwise there would be two different homomorphisms $\phi : \mathbb{Z}[U] \to A$ (both zero on the $\underline{\underline{U}}(i,\underline{\underline{d}})$ with $\underline{\underline{d}} \neq p^r\underline{\underline{e}}(j)$ such that $H_U^{\phi}(X,Y) = F(X,Y)$. This proves the theorem.

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_{p^i} instead of V_i). Now apply part (ii) of the functional equation lemma to conclude that $h_U^{-1}(\bar{h}_U(X)) \in \mathbb{Z}_{(p)}[U][[X]]$ for all prime numbers p, hence $h_U^{-1}(\bar{h}_U(X)) \in \mathbb{Z}[U][[X]]$.

Similary 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 $\mathbb{Z}_{(p)}[V,T]$. 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 $\mathbb{Z}[V,T]$.
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_{p^i} instead of V_i). Hence $F_V^{\lambda\kappa}(X,Y)$ and $H_U^{\lambda}(X,Y)$ are strictly isomorphic over $\mathbb{Z}_{(p)}[U]$.

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 $\mathbb{Z}_{(p)}$-algebra or a characteristic zero ring. Then if $\gamma(Z) \equiv \delta(Z)$ mod (degree $p^r n$), we have $\gamma(Z) \equiv \delta(Z)$ mod (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

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

Applying $\underline{f}_q$ to this we find, because $\underline{f}_q\gamma(Z) = \underline{f}_q\delta(Z)$, that $aq = 0$.

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

6.3. Lemma.

Let $\alpha: F(X,Y) \to G(X,Y)$ 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 $\mathbb{Z}[U;S]$ be short for $\mathbb{Z}[U(i,\underline{\underline{d}}); S(i,\underline{\underline{d}}); i = 1, \ldots, m, ||\underline{\underline{d}}|| \geq 2]$.
Let $d(q_1,\ldots,q_t) = n(q_1,\ldots,q_t)n(q_2,\ldots,q_t)\ldots n(q_t)p_1^{-1}p_2^{-1}\ldots p_t^{-1}$,
where the $n(q_1,\ldots,q_t)$ are as in 2.3. Let U_q, S_q denote the matrices $(U(i,q\underline{\underline{e}}(j))_{i,j}$, $S(i,q\underline{\underline{e}}(k))_{i,j}$.
Let $U(i,\underline{\underline{e}}(j)) = 0 = S(i,\underline{\underline{e}}(j))$ if $i \neq j$ and $U(i,\underline{\underline{e}}(i)) = 1 = S(i,\underline{\underline{e}}(i))$.
Finally let $U_{\underline{\underline{d}}}$, $S_{\underline{\underline{d}}}$ be the column vectors $(U(1,\underline{\underline{d}}), \ldots, U(m,\underline{\underline{d}}))$, $(S(1,\underline{\underline{d}}), \ldots, S(m,\underline{\underline{d}}))$.
We now define for all multiindices $\underline{\underline{n}}$, $||\underline{\underline{n}}|| \geq 1$

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

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

where the sums are over all sequences $(q_1,\ldots,q_t,\underline{\underline{d}})$, $q_i = p_i^{r_i}$, $r_i \in \mathbb{N}$, p_i a prime number, $q_1, \ldots, q_t\underline{\underline{d}} = n$, $||\underline{\underline{d}}|| \geq 1$.
(NB $t = 0$ is allowed). Let

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

6.5. Proposition.

$H_{U,S}(X,Y)$ is a formal group over $\mathbb{Z}[U;S]$ and it is strictly isomorphic over $\mathbb{Z}[U,S]$ 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 $\alpha_{U,S}(X)$ by substituting zero for all $S(i,\underline{\underline{d}})$ with $||\underline{\underline{d}}|| \geq n$.

Then one has immediately from (6.4.1) that

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

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 $\phi: \mathbb{Z}[U;S] \to A$ 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 $p^r\underline{e}(j)$, $r \in \mathbb{N}$, $i \in \{1,\ldots, m\}$. 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 $r_1, \ldots, r_m \in \mathbb{N}$ such that

$$d_1 p^{r_1} + \ldots + d_m p^{r_m} \text{ is not a power of } p \tag{6.7.1}$$

$$d_1 p^{r_1} + \ldots + d_m p^{r_m} < e_1 p^{r_1} + \ldots + e_m p^{r_m} \text{ if } \underline{d} <_{\ell} \underline{e} \tag{6.7.2}$$

Let $\gamma(Z)$ be the curve $\gamma(Z) = (Z^{p^{r_1}}, \ldots, Z^{p^{r_m}})$ in $G(X,Y)$. Let $\psi : \mathbb{Z}[V;T] \to A$ be the composition of $\phi: \mathbb{Z}[U;S] \to A$ with the canonical embedding $\mathbb{Z}[V;T] \to \mathbb{Z}[U;S]$. 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

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

and

$$(6.7.4) \qquad \alpha(X) \equiv \beta(X) + aX^{\underline{\underline{d}}} \mod(\text{ degree } >_{\underline{\underline{\ell}}} \underline{\underline{d}})$$

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

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

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

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

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

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

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

$$(7.1.3) \qquad c_{\underline{\underline{k}},\underline{\underline{\ell}}}(i) = \Sigma\, b \cdots (c_{\underline{\underline{k}}_{i_1},\underline{\underline{\ell}}_{i_1}}(j_1))^{r_1} \cdot \ldots \cdot (c_{\underline{\underline{k}}_{i_s},\underline{\underline{\ell}}_{i_s}}(j_s))^{r_s}$$

with $j_1 = \ldots = j_s$. Here the multiindices $\underline{\underline{k}}_{i_j}$ and $\underline{\underline{\ell}}_{i_j}$ must satisfy

$$1 \leq ||\underline{\underline{k}}_{i_j} + \underline{\underline{\ell}}_{i_j}|| < ||\underline{\underline{k}} + \underline{\underline{\ell}}||, \; r_1\underline{\underline{k}}_{i_1} + \ldots + r_s\underline{\underline{k}}_{i_s} = r_1\underline{\underline{\ell}}_{i_1} + \ldots + r_s\underline{\underline{\ell}}_{i_s}.$$

These last two relations imply that $\underline{\underline{k}}_{i_j}.\underline{\underline{\ell}}_{i_j} = 0$ for all $j = 1, \ldots, s$.

Hence by induction $c_{\underline{\underline{k}}_{i_j} \bullet \underline{\underline{\ell}}_{i_j}} = 0$ unless $\underline{\underline{k}}_{i_j} = 0$ or $\underline{\underline{\ell}}_{i_j} = 0$. Because $j_1 = \ldots = j_s = j$ 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 $t = 1, \ldots, s, \underline{\underline{k}}_{i_t} = \underline{\underline{e}}(j_t) = \underline{\underline{e}}(j)$ and $\underline{\underline{\ell}}_{i_t} = \underline{\underline{0}}$ or vice versa

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

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 $F(X,Y) \equiv G(X,Y)$ mod degree n. Then there is a unique matrix a with coefficients in A such that

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

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 $n(q_1, \ldots, q_t)$ of (2.3) in the special way described in [3] (and [5]) one finds recursion formulae for the $U(i,\underline{\underline{d}})$ in terms of the $a_{\underline{\underline{n}}}(U)$ 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 (to appear).

[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.

LIST OF SYMBOLS.

Latin lower case p,n,m,i,r,g,j,k,h,q,a,c,ℓ,d,s,y

Latin upper case X,Y,F,A,B,U,V,T,H,Z,G,R,I,W,S

Latin lower case boldface n,e,d,f,k,ℓ,m,j,s,t

Latin upper case boldface $\mathbb{Z}$ (integers), $\mathbb{N}$(natural numbers), $\mathbb{Q}$(rational numbers), D, E

Latin lower case as sub- or superscript p,m,r,n,i,t,q,j,s,k,ℓ

Latin upper case as sub- or superscript V,T,U,F,R,G,S

Latin script as sub or superscript ℓ (only in the combination of symbols $>_{\ell}$)

Latin lower case boldface as sub or superscript d,n,k,ℓ,m,s,t

Latin upper case boldface as sub or superscript $\mathbb{Z}$

Greek lower case $\phi,\gamma,\zeta,\kappa,\lambda,\vartheta,\iota,\nu,\rho,\psi,\chi,\delta,\alpha,\beta,$

Greek upper case Γ

Greek lower case as sub or superscript $\phi,\lambda,\kappa,\vartheta,\iota,\psi,\chi$

Numerals 0,1,2,3,4,5,6,7

Numerals as sub or superscript 1,2

Numerals boldface 0

Numerals bold face subscript 0

Special symbols $\{,\},(,),\rightarrow,\geq,\|,=,+,\in,\Sigma,\neq,[,],\cup,\otimes,\times,|,/,>,\equiv,\leq,<,\circ$

Special symbols as sub or superscript $(,),\|,=,\infty,-,+,\geq,\|,/,|,\neq,<,$

Conventions boldface: double straight black underline (usually typed)