Netherlands School of Economics

ECONOMETRIC INSTITUTE

Report 7201

CONSTRUCTING FORMAL GROUPS. II

OVER $\mathbb{Z}$ - ALGEBRAS

by Michiel Hazewinkel

, 1972

Preliminary and Confidential

CONSTRUCTING FORMAL GROUPS, II
OVER Z - ALGEBRAS

by Michiel Hazewinkel

Contents

1. INTRODUCTION

In [1] we wrote down some explicit power series over $Q[\ldots, T_{p^i}, \ldots]$ which turned out to be the logarithms of a p-typically universal formal group and a formal group universal over $Z_{(p)}$-algebras. Both formal groups are defined over $Z[\ldots, T_{p^i}, \ldots]$. In this note we show how to fit together these formal groups for different p to get a universal formal group (over $Z[T_2, T_3, \ldots]$). If $f(X)$ is the logarithm of this universal group $f(X) = \sum a_i X^i$, then its p-typical part, $X + \sum_{i=1}^{\infty} a_{p^i} X^{p^i}$ is precisely the logarithm of the p-typically universal formal group constructed in [1].

It turns out that there many ways of fitting together the p-typical formal groups. Most of them do not give nice formulas for the T_i in terms of the a_i. One special choice gives inverse formulas comparable to formulas (8) of [1]. In [1] we used these formulas to get generators in dimensions $2(p^n-1)$ of $\Omega^{ev}(pt)$, the complex cobordism ring modulo torsion. Using the universal formal group constructed in section 4 of this note we get a complete set of free generators of $\Omega^{ev}(pt)$ over Z.

Section 2 contains some preliminaries; section three gives the general construction of a universal formal group. In section 4 we discuss a special case with nice properties of the construction of section 3. Section 5 contains the application to complex cobordism theory alluded to above. In section 6 we discuss the more dimensional case which is completely analogical. In section 7 we discuss isomorphisms.

Section 8, finally, is independant of [1] and the rest of this paper. It is elementary (given the existence of universal formal groups and some more results of Lazard) and it would surprise me if it were not already known.

2. PRELIMINARIES.

Let $F(X,Y)$ be a power series over $Z[T_2, T_3, \dots]$ or $Z_{(p)}[T_2, T_3, \dots]$ in X,Y. We denote (cf. also [1]) with $F^{(p^k)}(X,Y)$ the power series obtained from $F(X,Y)$ by replacing the parameters $T_2, T_3, \dots$ with $T_2^{p^k}, T_3^{p^k}, \dots$

2.1. <u>Lemma</u>. Let $F(X,Y) \in Z_{(p)}[T_2, \dots][[X,Y]]$. Then we have

$$\frac{1}{n}(F(X,Y)^{p^k})^n \equiv \frac{1}{n}(F^{(p^k)}(X^{p^k}, Y^{p^k}))^n \bmod p$$

The proof is completely elementary. For $n = p^r$ it is contained in the proof of theorem (1.2) of [1].

Let $f_T(X)$ be a power series in X over $Q[T_2, T_3, \dots]$. The power series $f^{(p^k)}(X)$ is obtained by raising the parameters T_i to the p^k-th power.

2.2. <u>Theorem</u>. Let $f_T(X)$ be a power series in X over $Q[T_2, T_3, \dots]$ such that

$$f_T(X) - \sum \frac{T_{p^i}}{p} f_T^{(p^i)}(X^{p^i}) \in Z_{(p)}[T][[X]] \text{ for all primes } p \tag{2.2.1}$$

Let $F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y))$. Then all coefficients of $F_T(X,Y)$ are in $Z[T]$.

Proof. Fix a prime p for the moment. Then we have

$$f_T(X) = g_p(X) + \sum^T \frac{p^i}{p} f_T^{(p^i)}(X^{p^i})$$

for some power series $g_p(X) \in Z_{(p)}[T][[X]]$. Now repeat the proof of theorem (1.2) of [1] , using lemma (2.1) instead of formula (11) of [1], to show that

$$F(X,Y) \in Z_{(p)}[T][[X,Y]]$$

This must hold for all p, which concludes the proof.

2.3. Remark. Let f(X) be a power series over Q[T] such that

(2.3.1) $$f(X) - \sum^T \frac{p^i}{p} f^{(p^i)}(X^{p^i}) \in Z_{(p)}[T][[X]]$$

and let $u(X) = X + u_2X^2 + \ldots \in Z_{(p)}[T][[X]]$; let $g(X) = f(u(X))$. Then g(X) also satisfies

(2.3.2) $$g(X) - \sum^T \frac{p^i}{p} g^{(p^i)}(X^{p^i}) \in Z_{(p)}[T][[X]]$$

This follows immediately from lemma (3.1) of [1]. Now let G(X,Y) be a universal formal group law over Z[T] and let g(X) be its logarithm. Consider G and g over $Z_{(p)}[T]$. Over $Z_{(p)}[T]$, G(X,Y) must be isomorphic to the universal formal group law constructed in (1.3) of [1]. Combining this with (2.3.2) we see that a universal formal group must have a logarithm which satisfies (2.2.1) for all p.

In view of (2.2) it therefore only remains to construct reasonable power series f_T which satisfy (2.2.1) for all p. This is the subject matter of the next section.

2.4. Remark. If $f_{T,S}(X)$ is a power series over Q[T,S], where the S are additional variables, such that (2.2.1) holds for all p, then also

$$F_{T,S}(X,Y) \in Z[T,S][[X,Y]]$$

where $F_{T,S}(X,Y) = f_{T,S}^{-1}(f_{T,S}(X) + f_{T,S}(Y))$. Same proof.

3. CONSTRUCTION OF A UNIVERSAL FORMAL GROUP.

3.1. The Induction Step.

Suppose we have constructed a power series f_T up to and including degree $s-1$ such that (2.2.1) holds for all primes p mod degree s.

Let p be a prime dividing s, and let q be a power of p which divides s. Then according to (2.2.1) there must be a term

$$(3.1.1)\qquad \frac{T_q}{p} a_d^{(q)}, \; d = q^{-1}s, \; a_d \text{ de coefficient of } X^d$$

in the coefficient of X^s. The coefficient a_d looks like $d^{-1}c_d$, $c_d \in Z[T]$, which can be written as a sum

$$(3.1.2)\qquad a_d = \sum_{q'|d} \frac{c_{d,q'}}{q'}, \; q' \text{ a power of a prime.}$$

Substituting this in (3.1.1) we find a contribution

$$(3.1.3)\qquad \sum_{q'|d} \frac{T_q}{p} \frac{c^{(q)}_{d,q'}}{q'}$$

to a_s. We get such a contribution for every prime power q dividing s. We find therefore that a_n must contain

$$(3.1.4)\qquad \sum_{q|n} \sum_{q'|d} \frac{T_q}{p} \frac{c^{(q)}_{d,q'}}{q'}, \quad d = q^{-1}n, \; q, \; q' \text{ prime powers.}$$

If we use (3.1.4) to define a_s, (2.2.1) is in general not satisfied. This can be repaired by adding to each summand $p^{-1}(q')^{-1}.T_q.c^{(q)}_{d,q'}$, a term of the form $m(q,q')\, p^{-1}(q')^{-1}\, T_q\, c^{(q)}_{d,q'}$, where $m(q,q') \in Z$ is such that

$$(3.1.5)\qquad 1 + m(q,q') \equiv \begin{cases} 1 \bmod p \\ 0 \bmod q' \end{cases} \quad \text{if } (q,q') = 1$$

$$(3.1.6)\qquad 1 + m(q,q') \equiv 1 \bmod pq' \quad \text{if } (q,q') = p^s$$

Let $n(q,q') = 1 + m(q,q')$, and define

$$(3.1.7)\qquad a_s = \sum_{q|n} \sum_{q'|d} \frac{T_q}{p} \frac{c^{(q)}_{d,q'}}{q'} n(q,q') + \alpha_s T_s$$

where $\alpha_s = 1$ if s is not a power of a prime and $\alpha_s = 0$ otherwise.

We maintain that $f_T(X) = X + a_2X^2 + \ldots + a_sX^s$ then satisfies (2.2.1) for all p mod. degree $s + 1$.

Indeed, fixe a prime p_o, then we must show that

$$(3.1.8)\qquad a_s - \sum_{p_o|q|s} \frac{T_q}{p_o} a^{(q)}_{q^{-1}s} \in Z_{(p_o)}[T\ ]$$

The sum (3.1.8) is equal to

$$\sum_{p_o|q}\ \sum_{p_o|q'} \frac{n(q,q')-1}{p_o q'} T_q\, c^{(q)}_{d,q'} + \sum_{p_o|q,\,p_o\nmid q'} \frac{n(q,q')-1}{p_o q'} T_q\, c^{(q)}_{d,q'}$$

(3.1.9)

$$+ \sum_{p_o\nmid q,\,p_o|q'} \frac{n(q,q')}{pq'} T_q\, c^{(q)}_{d,q'} + \sum_{p_o\nmid q,\,p_o\nmid q'} \frac{n(q,q')}{pq'} T_q\, c^{(q)}_{d,q'} + \alpha_n T_n$$

(where $d = q^{-1}s$; q a power of p in the third and fourth terms). The first term of (3.1.9) is in $Z_{(p_o)}[T]$ because of (3.1.6); the second term of (3.1.9) is in $Z_{(p_o)}[T]$ because $(q')^{-1} \in Z_{(p_o)}$ and (3.1.5); the third term because $p^{-1} \in Z_{(p_o)}$ and (3.1.5) and the fourth term because p^{-1}, $(q')^{-1} \in Z_{(p_o)}$; finally: $\alpha_n T_n \in Z[T]$.

Note that we can choose for the $n(q,q')$ any numbers in Z which have properties (3.1.5), (3.1.6); in particular we can, if we wish, let $n(q,q')$ depend not only on q,q' but also on s and on the way in which the term $c_{d,q'}$ arose.

3.2. Ordered Factorizations.

An ordered factorization of $s \in N$ is a sequence of numbers $(q_1, q_2, \ldots, q_t, d)$ where the q_i are powers of primes and $d \in N$ is not a power of a prime (but $d = 1$ is possible). Example: the different ordered factorizations of $s = 12$ are

(2, 2, 3, 1), (4, 3, 1), (2, 3, 2, 1), (3, 2, 2, 1), (3, 4, 1), (2, 6), (12).

3.3. Lemma. If we use the procedure of (3.1) to construct f_T, then the monomials in T occurring in a_s are of the form

$$T_{q_1} T_{q_2}^{q_1} T_{q_3}^{q_1 q_2} \cdots T_{q_t}^{q_1 q_2 \cdots q_{t-1}} T_d^{q_1 q_2 \cdots q_t}$$

where $T_1 = 1$ and $(q_1, q_2, \ldots, q_t, d)$ is an ordered factorization of s.

Proof. By induction; elementary.

3.4. A Formula for a_s

For every ordered factorization $(p_1^{k_1}, \ldots, p_t^{k_t}, d)$ of s let $n(p_1^{k_1}, \ldots, p_t^{k_t}, d)$ be a number $\in Z$ such that

$$(3.4.1) \quad n(p_1^{k_1}, p_2^{k_2}, \ldots, p_t^{k_t}, d) \equiv \begin{cases} 1 \bmod p_1 & \text{if } p_1 \neq p_2 \quad (t \geq 2) \\ 0 \bmod p_2^r & \text{if } p_1 \neq p_2 = \ldots = p_{r+1} \neq p_{r+2} \quad (t \geq 2) \\ 1 \bmod p_1^r & \text{if } p_1 = p_2 = \ldots = p_r \neq p_{r+1} \quad (t \geq 1) \end{cases}$$

We define a_s by the formula

$$(3.4.2) \quad a_s = \sum_{(p_1^{k_1}, \ldots, p_t^{k_t}, d)} \frac{n(q_1, \ldots, q_t, d)}{p_1} \frac{n(q_2, \ldots, q_t, d)}{p_2} \cdot \ldots \cdot \frac{n(q_t, d)}{p_t} T_{q_1} T_{q_2}^{q_1} \cdots T_{q_t}^{q_1 \cdots q_{t-1}} T_d^{q_1 \cdots q_t}$$

where $q_i = p_i^{k_i}$, and $(p_1^{k_1}, \ldots, p_t^{k_t}, d)$ runs through all ordered factorizations of s; as above we set $T_1 = 1$.

3.5. Theorem.

Define $f_T(X)$ as

(3.5.1) $$f_T(X) = \sum_{s=1}^{\infty} a_s X^s$$

where a_s is given by formula (3.4.2). Then $f_T(X)$ satisfies (2.2.1) for all p. Let $F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y))$, then $F_T(X,Y)$ is a universal formal group.

Proof. The product

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

where q_i is a power of p_i is of the form

$$\frac{c}{p_1^r}$$

with $c \in Z$, if $p_1 = p_2 = \ldots = p_r \neq p_{r+1}$. This follows immediately from (3.4.1) by induction. It follows from this and (3.3) that the a_s are related to each other in the manner discussed in (3.1). The power series $f_T(X)$ therefore satisfies (2.2.1). Theorem (2.2) then shows that all coefficients of $F_T(X,Y)$ are in Z[T]. Finally writing $F_{T(s)}$ for $F_{(T_1,T_2,\ldots,T_s,0,0,\ldots)}$ we have

(3.5.2) $$F_T(X,Y) \equiv F_{T(s)}(X,Y) + \beta(s+1)T_{s+1} \quad \text{mod degree } s+2$$

where $\beta(s+1) = 1$ if s + 1 is not a power of a prime and $\beta(s+1) = \frac{1}{p}$ if s + 1 is a power of p. This follows immediately from (3.4.1). The relation (3.5.2) implies that F_T is a universal formal group, [2].

3.6. Examples.

The different ordered factorizations of 12 are

(2,2,3,1), (4,3,1), (3,2,2,1), (2,3,2,1), (3,4,1), (2,6), (12)

Let $n(2, q_1, q_2, \ldots, q_t, d) = n(q_1, \ldots, q_t)$, $t \geq 2$, $n(q,d) = 1$

$n(2,2,3) = 1$, $n(2,3) = 3$, $n(4,3) = 3$, $n(3,2,2) = 4$, $n(2,2) = 1$, $n(2,3,2) = 3$, $n(3,2) = 4$, $n(3,4) = 4$. Then we find for a_{12}

$$a_{12} = \tfrac{1}{4}T_2T_2^2T_3^4 + \tfrac{1}{2}T_4T_3^4 + \tfrac{1}{3}T_3T_2^3T_2^6 + T_2T_3^2T_2^6 + \tfrac{2}{3}T_3T_4^3 + \tfrac{1}{2}T_2T_6^2 + T_{12}$$

The ordered factorizations of 6 are

(2,3,1), (3,2,1), (6)

Using the same n's we find for a_6

$$a_6 = \tfrac{1}{2}T_2T_3^2 + \tfrac{2}{3}T_3T_2^3 + T_6$$

4. INVERSE FORMULAE.

The formula (3.4.2) permits us of course to write T_s in terms of the $a_d^{(q)}$, $d|s$ and the $T_{s'}$, $s'|s$, $s' < s$. In anology with formula (8) of [1] however, we would like to find a formula for T_s in terms of the a_d and the $T_{s'}$, where d and s' divide s.

Note that this is not possible with the choices for the $n(q_1, q_2, \ldots, q_t, d)$ which we used in (3.6). (A redefinition of n(3,2,2) as n(3,2,2) = 16 remedies this).

4.1. Some Special $n(q_1, q_2, \ldots, q_t.d)$

We define inductively

$$b(p_1^{k_1}, \ldots, p_t^{k_t}, d) = b(p_1, \ldots, p_t)$$

(4.1.1) $$b(p_i) = 1,\ b(d) = 1$$

$$b(p_1, \ldots, p_t) = \prod_{p\in J} c(p,p_t)\, b(p_1, \ldots, p_{t-1}),$$

where $J = \{p_1, \ldots, p_t\}$ and

$c(p,p') = 1$ if $p = p'$

(4.1.2) $c(p,p') \equiv 1$ mod p if $p \neq p'$

$c(p,p') \equiv 0$ mod p' if $p \neq p'$

(One can e.g. take $c(p,p') = (p')^{p-1}$, if $p' \neq p$).

Note that the factor $c(p,p_t)$ occurs precisely once in $\prod_{p\in J} c(p,p_t)$ if $p \in J$.

Now define $n(q_1, \ldots, q_t, d)$ by the formula

$$(4.1.3) \quad n(q_1, \ldots, q_t, d) = \frac{b(q_1, \ldots, q_t, d)}{b(q_2, \ldots, q_t, d)}, \quad n(d) = 1$$

4.2. Lemma.

The $n(q_1, \ldots, q_t, d)$ as defined by (4.1.3) satisfy the conditions (3.4.1).

Proof. One checks directly that $n(p_1^{t_1}, d) = 1$, $n(p_1^{t_1}, p_2^{t_2}) = n(p_1, p_2) =$

$= c(p_1,p_2)$; further $n(q_1, \ldots, q_t, d) = n(p_1, \ldots, p_t)$ if q_i is a power of p_i. By induction we get from (4.1.1) that

$$(4.2.1) \quad b(p_1, \ldots, p_t) = \prod_{p\in J_t} c(p,p_t) \ldots \prod_{p\in J_2} c(p,p_2), \; J_i = \{p_1, \ldots, p_i\}$$

Let $I_t = \{p_2, \ldots, p_t\}$, $I_i = \{p_2, \ldots, p_i\}$, $i = 2, \ldots, t$. The numbers

$$\prod_{p\in J_i} c(p,p_i) \quad \text{and} \quad \prod_{p\in I_i} c(p,p_i)$$

are either equal or differ by a factor $c(p_1,p_i)$ depending on whether p_1 is in I_i or not. It follows that

$$(4.2.2) \qquad n(p_1, \ldots, p_t) = \prod_{p_1\notin I_i} c(p_1,p_i),$$

The first congruence of (3.4.1) follows immediately from this. Moreover if $p_1 = p_2$ then $p_1 \in I_i$ for all $i = 2, \ldots, t$ so that

$$(4.2.3) \qquad n(p_1,p_2, \ldots, p_t) = 1 \quad \text{if } p_1 = p_2$$

Finally, suppose that $p_1 \neq p_2 = p_3 = \ldots = p_{r+1}$. Then for $i = 2, \ldots, r+1$ we have $p_i = p_2$ and $I_i = \{p_2\}$, $p_1 \notin I_i$, so that $n(p_1,p_2, \ldots, p_t)$ contains r factors $c(p_1,p_2)$ which proves the second congruence of (3.4.1).

q.e.d.

Remark. The formula (4.2.2) can be rephrased as

$$
\begin{aligned}
&n(p_1,p_2,\ldots,p_t) = c(p_1,p_2)\ \ldots\ c(p_1,p_t) && \text{if } p_i \neq p_1,\ i = 2,\ldots,t,\\
(4.2.4)\quad &n(p_1,p_2,\ldots,p_t) = 1 && \text{if } p_1 = p_2\\
&n(p_1,p_2,\ldots,p_t) = n(p_1,\ldots,p_r) && \text{if } p_i \neq p_1,\ i = 2,\ldots,r,\\
& && p_{r+1} = p_1
\end{aligned}
$$

Let a_s' be the element of $Q[T]$ obtained (from (3.4.2)) by setting $T_d = 0$ for all $d \neq 1$ which are not a power of a prime. Let $NP = \{n \in N \mid n \neq 1,$ n not a power of a prime $\}$. We have

$$
(4.2.5)\quad a_s' = \sum_{(p_1^{k_1},\ldots,p_t^{k_t},1)} \frac{n(q_1,\ldots,q_t,1)}{p_1} \cdot \ldots \cdot \frac{n(q_t,1)}{p_t}\, T_{q_1} T_{q_2}^{q_1} \ldots T_{q_t}^{q_1\ldots q_{t-1}}
$$

4.3. <u>Proposition</u>.

Let the $n(q_1,\ldots,q_t,d)$ be defined by (4.1.3). Then we have

$$
(4.3.1)\qquad a_s = \sum_{\substack{d|s\\ d\neq 1}} \frac{m(s,d)}{\mu(d)}\, a'_{s/d}\, T_d^{s/d}
$$

where $m(s,d) = 1$ if $d \in NP$, $m(s,p^t) = \prod_{p'\in J} c(p',p)$, where J is the set of primes occurring in s; and $\mu(d) = 1$ if $d \in NP$, $\mu(p^t) = p$. Further we have

$$
(4.3.2)\qquad a_s' = a_s - \sum_{\substack{d|s,\, d\in NP\\ d\neq 1}} a'_{s/d}\, T_d^{s/d}
$$

Proof. Both these formulas are proved by looking at the formula (3.4.2) for a_s. Take a fixed d, and consider all ordered factorizations $(p_1^{k_1},\ldots,p_t^{k_t},d)$ of s. First suppose that d is not a power of a prime, $d \neq 1$. The part of a_s consisting of terms involving T_d is then

$$(4.3.3)\quad \sum_{(p_1^{k_1},\dots,p_t^{k_t},1)} \frac{n(q_1,q_2,\dots,q_t,d)}{p_1}\cdot\ldots\cdot\frac{n(q_t,d)}{p_t} T_{q_1} T_{q_2}^{q_1}\cdots T_{q_t}^{q_1\cdots q_{t-1}} \cdot T_d^{q_1\cdots q_t}$$

where the sum is over all ordered factorizations of s/d ending in 1. Combining this with (4.1.3) and (4.1.1) proves formula (4.3.2). Cf. (4.2.5). Now let d = q be a power of a prime, and consider the coefficient of $T_q^{s/q}$ in a_s. This is equal to

$$(4.3.4)\quad \sum_{(q_1,\dots,q_t,q,1)} \frac{n(q_1,\dots,q_t,q,1)}{p_1}\cdot\ldots\cdot\frac{n(q_t,q,1)}{p_t}\cdot\frac{n(q,t)}{p}\,.\, T_{q_1}\cdots T_{q_t}^{q_1\cdots q_t}$$

where the sum is over all factorizations ending in (...,q,1), and these correspond bijectively to all factorizations ending in 1 of $q^{-1}s$.

According to (4.1.3) and the first two formulas of (4.1.1) we have

$$(4.3.5)\qquad n(q_1,\dots,q_t,q,1).\ \ldots\ .\ n(q_t,q,1).n(q,1) = b(p_1,\dots,p_t,p)$$

and using the third formula of (4.1.1) and again (4.1.3) and the first two formulas of (4.1.1) we see that

$$(4.3.6)\quad n(q_1,\dots,q_t,q,1).\ \ldots\ .\ n(q_t,q,1).n(q,1) = $$

$$= m(s,q)\, n(q_1,\dots,q_t,1)\ \ldots\ n(q_t,1)$$

This in combination with (4.3.4) and the argument used to establish (4.3.2) proves (4.3.1).

4.4. <u>Remark</u>. The formulae (4.3.1) and (4.3.2) permit one to write T_s as an expression in the T_d, $d < s$, $d|s$ and the a_d, $d|s$. This is the reason why this section is headed "inverse formulae".

5. GENERATORS FOR THE COMPLEX COBORDISM RING.

Let $\Omega^{ev}(pt)$ denote the complex cobordism ring modulo torsion. It is freely generated by countably many generators over Z. There is also a canonically defined formal group over it. Cf. [3]. The logarithm of this formal group law is equal to

$$\ell(X) = \sum_{n=0}^{\infty} \frac{P_n}{n+1} X^{n+1} \tag{5.1}$$

where $P_n \in \Omega^{-2n}(pt)$ is the cobordism class of CP^n. Cf [3]. Quillen [3] has shown that this formal group law is universal. It is therefore isomorphic to the formal group law constructed above, in particular to the one which uses the $n(q_1, \ldots, q_t, d)$ defined and used in section 4. We can therefore use proposition (4.3) to find a set of generators for the complex cobordism ring

5.2. <u>Theorem</u>.

The following inductively defined elements, $s = 2, 3, \ldots$, constitute a set of free generators over Z of the complex cobordism ring $\Omega^{ev}(pt)$.

$$t_s = \mu(s)\frac{P_{s-1}}{s} - \mu(s)\sum_{dd_1=s,\, d_1\neq 1,s} \frac{m(s,d_1)}{\mu(d_1)}\frac{P_{d-1}}{d} t_{d_1}^{d} + \ldots$$

$$+ \mu(s)\sum_{\substack{dd_2d_1=s,\, d_2\in NP\\ d_1\neq 1,s}} \frac{m(s,d_1)}{\mu(d_1)}\frac{P_{d-1}}{d} t_{d_2}^{d}\, t_{d_1}^{dd_2} + \ldots$$

$$+ (-1)^i\mu(s)\sum_{\substack{dd_i\cdots d_2d_1=s\\ d_i,\ldots,d_2\in NP,\, d_1\neq 1,s}} \frac{m(s,d_1)}{\mu(d_1)}\frac{P_{d-1}}{d} t_{d_i}^{d}\, t_{d_{i-1}}^{dd_i} \cdots t_{d_1}^{dd_i\cdots d_2}$$

. . . .

(We take $P_0 = 1$)

<u>Proof</u>. This follows immediately from proposition (4.3). Use formula (4.3.1) and then eleminate the $a'_{s/d}$ inductively by means of (4. 3.2).

(If d is a prime power $a_d = a'_d$). Note that $\mu(s)\mu(d_1)^{-1}m(s,d_1)$ is always an integer.

5.3. Some Examples.

We take $c(3,2) = 4$, $c(2,3) = 3$. Using (5.2) one then easily calculates

$$t_2 = P_1$$
$$t_3 = P_2$$
$$t_4 = \tfrac{1}{2}P_3 - \tfrac{1}{2}P_1^3$$
$$t_6 = \frac{P_5}{6} - \frac{2P_2P_1^3}{3} - \frac{P_1P_2^2}{2}$$
$$t_9 = \frac{P_8}{3} - \frac{P_2^4}{3}$$
$$t_{18} = \frac{P_{17}}{18} - \frac{2P_8P_1^9}{9} - \frac{P_5P_2^6}{6} - \frac{P_2}{3}\left(\frac{P_5}{6} - \frac{2P_2P_1^3}{3} - \frac{P_1P_2^2}{2}\right)^3 + \left(\frac{P_5}{6} - \frac{2P_2P_1^3}{3} - \frac{P_1P_2^2}{2}\right)P_2^6$$

6. MORE DIMENSIONAL UNIVERSAL FORMAL GROUPS.

In this section we study higher dimensional formal groups. All formal groups considered will be commutative. To get a universal n-dimensional formal group, we work over the ring $Q[\ldots,T_q(i,j),\ldots\ ;\ \ldots,\ S_d(i),\ldots]$ where the $T_q(i,j)$ and $S_d(i)$ are indeterminates, one for each prime power q and $1 \leq i,\ j \leq n$; and one for each $1 \leq i \leq n$ and multiindex $d = (d_1, \ldots, d_n)$, $d_i \geq 0$, $d \neq (0,0,\ldots,0)$ which is not of the form $p^r e_j$ where $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$, the 1 in the j-th place, $j = 1, \ldots, n$; p prime; $r = 0, 1, 2, \ldots$. Let T_q denote the n x n matrix $(T_q(i,j))$ and S_d the column vector

$$S_d = \begin{pmatrix} S_d(1) \\ \cdot \\ \cdot \\ \cdot \\ S_d(n) \end{pmatrix}$$

If d is a multiindex $d = (d_1, \ldots, d_n)$ then X^d denotes $X^d = X_1^{d_1} \ldots X_n^{d_n}$. Our first result is completely analogeous to theorem (2.2).

6.1. Theorem.

Let $f(X)$ be an n-dimensional column vector of power series in the n-variables $X_1, \ldots, X_n$ over $Q[\ldots, T_q(i,j), \ldots; \ldots, S_d(i), \ldots]$ such that

$$(6.1.1) \qquad f(X) - X - \sum_{i=1}^{\infty} \frac{T_p^i}{p} f^{(p^i)}(X^{p^i}) \in Z_{(p)}[T,S]$$

for all primes p. (Here X is the column vector of the $X_1, \ldots, X_n$ and X^{p^i} is short for the column vector of the $X_1^{p^i}, \ldots, X_n^{p^i}$; $f^{(p^i)}$ denotes (as usual) the power series obtained from f by raising all the parameters $T_q(i,j)$, $S_d(i)$ to the power p^i). Let $F(X,Y) = f^{-1}(f(X) + f(Y))$, then all the coefficients of $F(X,Y)$ are in $Z[\ldots, T_q(i,j), \ldots; \ldots, S_d(i), \ldots]$]

Proof. Same proof as of theorem (2.2).

As in the one dimensional case it remains to construct power series such that (6.1.1) holds for all primes p. We also know that there exist such power series.. This is exactly the same problem as we encountered in sections 3,4. We recall and introduce some notation.

6.2. Ordered Factorizations, etc.

Let s be a multiindex $s = (s_1, \ldots, s_n)$. We write NPM for the set of all multiindices which are not of the form $p^r e_j$, $j = 1, \ldots, n$; p prime; $r = 1, 2, \ldots$, (Note that we start with $r = 1$ here).
An ordered factorization of $s = (s_1, \ldots, s_n)$ is a sequence

$$(q_1, \ldots, q_t, d)$$

where q_i is a prime power and $d = (d_1, \ldots, d_n)$ is a multiindex which is in NPM such that $q_1, \ldots, q_t d_i = s_i$.

We also introduce the symbols $S_{e_j}(i)$ as $S_{e_j}(i) = \delta_{ij}$, where δ_{ij} is the Kronecker index; S_{e_j} is the column vector of the $S_{e_j}(i)$.

For every ordered factorization $(q_1, \ldots, q_t, d)$ of a multiindex s we define $n(q_1, \ldots, q_t, d) = n(q_1, \ldots, q_t) = n(p_1, \ldots, p_t)$ = the number defined in section 4. Now let the column vector a_s, s a multiindex, be defined by

$$(6.2.1)\quad a_s = \sum_{(q_1,\ldots,q_t,d)} \frac{n(q_1,\ldots,q_t,d)}{p_1} \cdot \ldots \cdot \frac{n(q_t,d)}{p_t} \cdot T_{q_1} T_{q_2}^{(q_1)} \ldots T_{q_t}^{(q_1\ldots q_{t-1})} S_d^{(q_1\ldots q_t)}$$

where $(q_1, \ldots, q_t, d)$ runs through all ordered factorizations of s; $T_q^{(n)}$ is the matrix $(T_q^n(i,j))$ and $S_d^{(n)}$ is the column vector consisting of the $S_d^n(i)$.

6.3. Theorem.

Let f(X) be the n-dimensional vector of power series defined by

$$f(X) = \sum_s a_s X_1^{s_1} \ldots X_n^{s_n}$$

where s runs through all multiindices $s = (s_1, \ldots, s_n)$, $s_i \geq 0$, $s \neq (0, 0, \ldots, 0)$. Let

$$F(X,Y) = f^{-1}(f(X) + f(Y))$$

Then we have

(i) f(X) satisfies (6.1.1) for all primes p.

(ii) The coefficients of F(X,Y) are in $Z[\ldots, T_q(i,j),\ldots; S_d(i),\ldots]$

(iii) F(X,Y) is a universal commutative n-dimensional formal group.

Proof. (i) follows directly from the definition of a_s and the properties of $n(q_1, \ldots, q_t, d)$, cf. section 3. (ii) follows from (i) in virtue of theorem 1.1. As to (iii), this follows from (ii) because we have enough free parameters. More precisely one uses the result of Lazard cited as proposition (4.1) in [1].

q.e.d.

6.4. Remark. As in the one dimensional case one has formulae like those of proposition (4.3.) which can be used to write the $T_q(i,j)$ and $S_d(i)$ inductively in terms of the a_s.

7. ISOMORPHISMS.

In sections 3, 4 we constructed certain power series $f_T(X)$

over $Q[T_2, T_3, \ldots]$ such that

$$f_T(X) - \Sigma \frac{T_{p^i}}{p} f_T^{(p^i)}(X^{p^i}) \in Z_{(p)}[T][[X]]$$

for all primes p. In a certain sense the construction used there is the only one possible.

7.1. Lemma. Let $f_{T,S}(X) \in Q[T_2, T_3, \ldots; S_2, S_3, \ldots][[X]]$ be a power series such that

(7.1.1) $$f_{T,S}(X) - \Sigma \frac{T_{p^i}}{p} f_T^{(p^i)}(X^{p^i}) \in Z_{(p)}[T,S][[X]]$$

for all p. Then if a_n denotes the coefficient of X^n we have

(7.1.2) $$a_n = \sum_{q|s} \sum_{q'|d} \frac{T_q}{p} \frac{c_{d,q'}}{q'} \cdot n(q,q') + b_n(S,T)$$

where $d = q^{-1}n$, $a_d = \Sigma(q')^{-1}c_{d,q'}$, $c_{d,q'} \in Z[T,S][[X]]$, $b_n \in Z[T,S][[X]]$ and $n(q,q')$ any numbers such that $n(q,q') \equiv 1 \bmod p$, $n(q,q') \equiv 0 \bmod q'$ if $(q,q') = 1$ and $n(q,q') \equiv 1 \bmod pq'$ if $(q,q') = p^s$.

Proof. It follows immediately from (7.1.1) that a_n must be of the form given by (7.1.2). Assume for the moment that there are no monomials in S,T which occur both in $b_n(S,T)$ and in the double sum part of a_n. It then immediately follows from(7.1.1) that $b_n(S,T) \in Z[T,S][[X]]$. Necessary and sufficient for (7.1.1) to hold is then that the expression (3.1.9) be in $Z_{(p_o)}[S,T]$ for every p_o (with $\alpha_n T_n$ left out). First let $(q,q') = p^s$. The necessary and sufficient condition on $n(q,q')$ is that $(pq')^{-1}\{n(q,q')-1\}c_{d,q'} \in Z_{(p)}[S,T]$. Any $n(q,q') \equiv 1 \bmod pq'$ works. It may of course happen that $c_{d,q'}$ contains a few factors p so that a $\bar{n}(q,q') \equiv 1$ modulo a smaller power of p than the exponent of pq' also works. The difference $\{n(q,q') - \bar{n}(q,q')\}(pq')^{-1}c_{d,q'}$ is then in $Z[S,T]$ and can be absorbed in $b_n(S,T)$. Now let $(q,q') = 1$. The necessary and sufficient conditions on $n(q,q')$ are (cf. (3.1.9)).

$$(pq')^{-1}(n(q,q') - 1)c^{(q)}_{d,q'} \in Z_{(p)}[S,T]$$

$$(pq')^{-1}(n(q,q')c^{(q)}_{d,q'} \in Z_{(p')}[S,T]$$

Any $n(q,q')$ such that $n(q,q') \equiv 1 \bmod p$ and $n(q,q') \equiv 0 \bmod q'$ works. It may of course happen that $c^{(q)}_{d,q'}$ is divisible by say $p^a p'^b$, which case we must have $\bar{n}(q,q') \equiv 1 \bmod p^{1-a}$, $\bar{n}(q,q') \equiv 0 \bmod p'^{-b}q'$. The difference $(pq')^{-1}\{n(q,q') - \bar{n}(q,q')\}c^{(q)}_{d,q'}$ is in $Z[S,T]$ and can be absorbed into $b_n(S,T)$.

q.e.d

7.2. <u>Corollary</u>.

Let $f_T(X)$ be the power series $f_T(X) = \Sigma\, a_s X^s$, where a_s is given by (3.4.2). Substitute $X + S_2X^2 + \ldots$ for X in $f_T(X)$ and let the resulting series be $g(X) = \Sigma d_s X^s$.
Then we have

$$d_s = \sum_{(q_1,\ldots,q_t,d)} \frac{n(q_1,\ldots,q_t,d)}{p_1} \cdots \frac{n(q_t,d)}{p_t} T_{q_1} T_{q_2}^{q_1} \cdots T_{q_t}^{q_1\cdots q_{t-1}} \cdot \left(T_d^{q_1\cdots q_t} + b_d^{(q_1\cdots q_t)}(S,T)\right)$$

(7.2.1)

$$+ \sum_{(q_1,\ldots,q_t,1)} \frac{n(q_1,\ldots,q_t,1)}{p_1} \cdots \frac{n(q_t,1)}{p_t} T_{q_1} \cdots T_{q_{t-1}}^{q_1\cdots q_{t-2}} p_t \cdot b_{q_t}^{(q_1,\ldots,q_{t-1})}(S,T)$$

<u>Proof</u>. This follows from (7.1) because $g(X)$ satisfies (7.1.1) if $f_T(X)$ satisfies (7.1.1). Cf. [1] (3.1) and (3.2).

7.3. <u>Corollary</u>.

Let $b_d(S,T)$ be any polynomial in S,T; $d = 2, 3, \ldots$. Let $g_{T,S}(X) = \Sigma\, d_s X^s$ be the power series given by (7.2.1). The formal groups $F_T(X,Y)$ and $G_{T,S}(X,Y)$ are then isomorphic over $Z[T,S]$.

<u>Proof</u>. Suppose we have proved this already mod degree n for all series of polynomials $b_d(S,T)$. Let φ be the power series over $Z[T,S]$

establishing the isomorphism mod n. The power series $f(\phi(X))$ and $g(X)$ both have coefficients of the form (7.2.1) and they coincide mod degree n. It follows that their polynomials ($b'_d(S,T)$ and $b_d(S,T)$ resp.) coincide for $d < n$. It follows that we can find a $u(S,T) \in Z[S,T]$ such that $f(\phi(X) + u(S,T)X^n)$ and $g(X)$ coincide mod degree $n + 1$.

q.e.d.

Now let $h_{S,T}(X)$ be the power series $h_{S,T}(X) = \Sigma\, b_s X^s$, b_s given by (7.2.1) with $b_d(S,T) = S_d$. Let $t = (t_2, \ldots, t_n, \ldots)$, $s = (s_2, s_3, \ldots)$ be two sequences of elements from a characteristic zero ring A. Let $h_{t,s}(X)$ and $f_t(X)$ be the power series obtained from $h_{T,S}(X)$ and $f_T(X)$ by substituting t_i and s_i for T_i and S_i. Let $H_{t,s}(X,Y)$ and $F_t(X,Y)$ be the formal groups belonging to $h_{t,s}(X)$ and $f_t(X)$.

7.4. Corollary.

The formal groups $H_{t,s}(X,Y)$ and $F_t(X,Y)$ are isomorphic. Inversely, if A is a characteristic zero ring and $H(X,Y)$ is isomorphic over A to $F_t(X,Y)$ then there exist $(s_2, s_3, \ldots)$ such that the logarithm of $H(X,Y)$ is equal to $h_{t,s}(X)$.

Proof. The first part follows from (7.3). As to the second part, suppose we have already found $s_2, \ldots, s_{n-1}$ such that

$$h(X) \equiv h_{t,s}(X) \text{ mod degree } n$$

The formal groups $H(X,Y)$ and $H_{t,s}(X,Y)$ are isomorphic and congruent mod degree n. It follows that there exists an s_n such that

$$h(X) \equiv h_{t,s}(X) \text{ mod degree } n + 1$$

7.5. Remarks.

1. Corollary (7.4) can of course be used as a criterium for testing whether two formal groups over a characteristic zero ring are isomorphic.
2. Similar results can be obtained for more dimensional formal groups.

8. A LOCAL GLOBAL RESULT.

Let K be an algebraic number field, A denotes its ring of integers. If $\mathfrak{p}$ is a prime ideal, $A_{(\mathfrak{p})}$ is the localization of A at $\mathfrak{p}$, and $A_{\mathfrak{p}}$ is the completion of $A_{(\mathfrak{p})}$. We shall view $A_{(\mathfrak{p})}$ as a subring of K; $v_{\mathfrak{p}}$ is the valuation on $A_{\mathfrak{p}}$ and K belonging to the prime ideal $\mathfrak{p}$.

8.1. Lemma.

Let the prime p decompose as $p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_n^{e_n}$ in A. For every prime $\mathfrak{p}$ dividing p let there be given a number $a_{\mathfrak{p}} \in A_{\mathfrak{p}}$. Then there exists an $a \in A$ such that $a - a_{\mathfrak{p}} \in pA_{\mathfrak{p}}$ for all the primes $\mathfrak{p}$ dividing p.

Proof. First we show that for every $\mathfrak{p}_i$ there is a $b_{\mathfrak{p}_i} \in A_{\mathfrak{p}_i}$ such that $a_{\mathfrak{p}_i} + pb_{\mathfrak{p}_i} \in \bigcap_{i=1}^{n} A_{(\mathfrak{p}_i)}$. We can in any case assume that $a_{\mathfrak{p}_i} \in A_{(\mathfrak{p}_i)}$ for $i = 1, \ldots, n$. Let $\pi_1, \ldots, \pi_n$ be elements of A such that $v_{\mathfrak{p}_i}(\pi_j) = \delta_{ij}, i, j = 1, \ldots, n$. Then we can write

$$a_{\mathfrak{p}_i} = \frac{c_{\mathfrak{p}_i}}{\pi_1^{t_1} \cdots \pi_{i-1}^{t_{i-1}} \pi_{i+1}^{t_{i+1}} \cdots \pi_n^{t_n}}, \quad c_{\mathfrak{p}_i} \in B = \bigcap_{i=1}^{n} A_{(\mathfrak{p}_i)}$$

Let $b_{\mathfrak{p}_i}$ be of the form $b_{\mathfrak{p}_i} = (\pi_1^{t_1+e_1} \cdots \pi_{i-1}^{t_{i-1}+e_{i-1}} \pi_{i+1}^{t_{i+1}+e_{i+1}} \cdots \pi_n^{t_n+e_n})^{-1} d_{\mathfrak{p}_i}$, $d_{\mathfrak{p}_i} \in B$.

The problem is then to choose $d_{\mathfrak{p}_i}$ such that

$$c_{\mathfrak{p}_i} + \pi_i^{e_i} d_{\mathfrak{p}_i} \equiv 0 \bmod \prod_{j \neq i} \pi_j^{t_j+e_j}$$

which can be done because the π_i are prime to each other. We can therefore assume that the $a_{\mathfrak{p}}$ are all in B. Now for each i let $e_{\mathfrak{p}_i}$ be of the form $e_{\mathfrak{p}_i} = \prod_{j \neq i} \pi_j^{-e_j} f_{\mathfrak{p}_i}$ (with $f_{\mathfrak{p}_i} \in B$). Then $a_{\mathfrak{p}_i} + pe_{\mathfrak{p}_i}$ is of the form $a_{\mathfrak{p}_i} + \pi_i^{e_i} f_{\mathfrak{p}_i}$

And the next problem is therefore to find an $a' \in B$ such that $a' \equiv a_{\mathfrak{p}_i}$

mod $\pi_i^{e_i}$ which can be done by the Chinese remainder theorem.

We have now found an $a' \in B$ which satisfies the requirements of the lemma. It now suffices to show that there is an $b \in B$ such that $a = a' + pb$ is in A. Let $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ be the prime ideals of A such that $v_{\mathfrak{q}_j}(a') < 0$. Choose elements ρ_j of A such that $v_{\mathfrak{q}_j}(\rho_j) = \delta_{ij}$, $v_{\mathfrak{q}_i}(\rho_i) = 0$. Then we can write

$$a' = \frac{c'}{\rho_1^{r_1} \dots \rho_m^{r_m}}$$

with $c' \in A$.

let b' be of the form $b' = \rho_1^{-r_1} \dots \rho_m^{-r_m} d'$, $d' \in A$. The problem is then to find a $d' \in A$ such that $c' + pd' \equiv 0 \mod \rho_1^{r_1} \dots \rho_m^{r_m}$ which can be done because p and $\prod_i \rho_i^{r_i}$ are prime to each other.

8.2. <u>Proposition</u>.

Let F and G be two formal groups over A. Then F and G are isomorphic over A if and only if they are isomorphic over all $A_{\mathfrak{p}}$.

<u>Proof</u>. The isomorphism between F and G, if it exists, is equal to $g^{-1}(f(X))$, where f,g are the logarithms of F and G. The coefficients of $g^{-1}(f(X))$ are in A iff they are in $A_{\mathfrak{p}}$ for all $\mathfrak{p}$

8.3. <u>Proposition</u>.

Suppose we have a formal group $F_{\mathfrak{p}}$ over $A_{\mathfrak{p}}$ for all prime divisors $\mathfrak{p}$ of A. Then there exists a formal group F over A such that F is isomorphic to $F_{\mathfrak{p}}$ for all $\mathfrak{p}$ over $A_{\mathfrak{p}}$

<u>Proof</u>. Suppose we have already constructed F up to and including degree n . If n + 1 is not a prime power F and $F_{\mathfrak{p}}$ are also isomorphic mod degree n + 2, for all $\mathfrak{p}$, and we can extend F to degree n + 1 arbitrarily. Now suppose that n + 1 is a power of the prime p. For each prime $\mathfrak{p}$ dividing p, let $\phi_{\mathfrak{p}}$ be a power series over $A_{\mathfrak{p}}$ establishing the isomorphism between F and $F_{\mathfrak{p}}$ mod degree n + 1

and let $F'_{\mathfrak{p}}(X,Y) = \phi_{\mathfrak{p}}^{-1} F(\phi_{\mathfrak{p}}(X), \phi_{\mathfrak{p}}(Y))$ and let $f'_{\mathfrak{p}}(X)$ be the logarithm of $F'_{\mathfrak{p}}$. Let $f_T(X)$ be the power series over Z[T] given by (3.4.2) and $t = (t_2, \ldots, t_n)$, be such that $f_t(X) \equiv f(X)$ mod degree n + 1 where f is the logarithm of F. For each $\mathfrak{p}$ dividing p let $t(p) = (t_2(\mathfrak{p}), \ldots)$ be such that $f_{t(\mathfrak{p})}(X) = f'_{\mathfrak{p}}(X)$ then $t_i(\mathfrak{p}) \equiv t_i$ for i = 2, ..., n
Now choose $t_{n+1} \in A$ such that

$$t_{n+1} - t_{n+1}(\mathfrak{p}) \in pA_{\mathfrak{p}} \text{ for all } \mathfrak{p}.$$

Every formal group $F_s(X,Y)$ with $s_i = t_i$ for $i < n + 1$, s_i arbitrary for $i > n + 1$ is then isomorphic to $F_{\mathfrak{p}}(X,Y)$ modulo degree n + 2, for all primes $\mathfrak{p}$ dividing p. As to the primes $\mathfrak{q}$ not dividing p, $F_s(X,Y)$ and $F_{\mathfrak{q}}(X,Y)$ are isomorphic mod degree n + 2 if they are isomorphic mod degree n + 1 because $\mathfrak{q}$ is prime to n + 1.

REFERENCES.

[1]. Hazewinkel, M (1971), Constructing Formal Groups, I: Over $Z_{(p)}$-algebras. Report of the Econometric Institute, Netherlands School of Economics, nr. 7119.

[2]. Lazard, M. (1955), Sur les Groupes de Lie Formels à un Paramètre Bull. Soc. Math. France 83, 251-274.

[3]. Quillen, D. (1969), On the Formal Group Laws of Unoriented and Complex Cobordism Theory. Bull. Am. Math. Soc. 75, 1293-1298.

Michiel Hazewinkel
Netherlands School of Economics
Burg. Oudlaan 50,
3016 Rotterdam.
The Netherlands