Journal of Pure and Applied Algebra 9 (1977) 151–161

CONSTRUCTING FORMAL GROUPS II: THE GLOBAL ONE DIMENSIONAL CASE

Michiel HAZEWINKEL

Dept. Math., Econometric Institute, Erasmus University of Rotterdam, 50 Burg. Oudlaan, 3016 Rotterdam, The Netherlands

Communicated by P.J. Freyd
Received 15 May 1975

AMS Subj. Class.: Primary 14L05
formal group   universal formal group

1. Introduction

In this paper we show how to fit together the various (universal) formal groups $F_V(X, Y)$ for $\mathbf{Z}_{(p)}$-algebras of [2], to obtain a global (one dimensional commutative) formal group.

If $f_U(X) \in \mathbf{Z}[U_2, U_3, \dots][[X]]$ is the logarithm of a universal formal group over $\mathbf{Z}[U]$, then it follows from the functional equation lemma [2, Lemma 7.1] that $f_U(X)$ must satisfy

$$(1.1) \qquad f_U(X) - \sum_{i=1}^{\infty} \frac{U_{p^i}}{p} f_U^{(p^i)}(X^{p^i}) \in \mathbf{Z}_{(p)}[U][[X]]$$

for all prime numbers p. So the natural thing to do is to construct the power series $f_U(X)$ according to the recipe (1.1) starting with X. The first thing one writes down is then

$$(1.2) \quad X + \frac{U_2}{2}X^2 + \frac{U_3}{3}X^3 + \left(\frac{U_2U_2^2}{4} + \frac{U_4}{2}\right)X^4 + \frac{U_5}{5}X^5 + \left(\frac{U_3U_2^3}{6} + \frac{U_2U_3^2}{6}\right)X^6 + \dots .$$

However, it now appears that the two prime numbers 2 and 3 interfere with one another. The term $6^{-1}U_3U_2^3$, which has to be there because of condition (1.1) in case $p = 3$, prevents (1.2) from satisfying (1.1) for $p = 2$, and vice versa with respect to the term $6^{-1}U_2U_3^2$. The solution is to insert suitable coefficients. Thus

$$X + \frac{U_2}{2}X^2 + \frac{U_3}{3}X^3 + \left(\frac{U_2U_2^2}{4} + \frac{U_4}{2}\right)X^4 + \frac{U_5}{5}X^5 + \left(\frac{2U_3U_2^3}{3} + \frac{U_2U_3^2}{2} + U_6\right)X^6 + \dots$$

(1.3)

does satisfy (1.1) mod degree 7 for $p = 2, 3$. (To construct a universal formal group it is also necessary to insert U_6X^6 so as to have a free variable available in dimension 6.) So the only problem in constructing a universal formal group is in showing that one can always find suitable coefficients. This readily leads to the following formula for the logarithm $h_U(X)$ of a possible universal formal group:

$$h_U(X) = \sum_{i=1}^{\infty} a_i(U)X^i, \qquad a_1 = 1$$

(1.4) $\quad a_n(U) =$

$$= \sum_{(q_1,\ldots,q_s,d)} \frac{n(q_1,\ldots,q_s,d)}{p_1} \frac{n(q_2,\ldots,q_s,d)}{p_2} \cdots \frac{n(q_s,d)}{p_s} U_{q_1} U_{q_2}^{q_1} \cdots U_{q_s}^{q_1\cdots q_{s-1}} U_d^{q_1\cdots q_s}$$

where q_i is a power of the prime number p_i, $U_1 = 1$, and the sum is over all sequences $(q_1, \ldots, q_s, d)$ with q_i prime powers and $d = 1$ or divisible by at least two different primes, such that $q_1 \ldots q_s d = n$. The coefficients $n(q_1, \ldots, q_s, d)$ can be chosen arbitrarily provided they satisfy the congruences

$$n(q_1,\ldots,q_s,d) \equiv 1 \bmod p_1 \qquad \text{if } p_1 \neq p_2,$$

(1.5)
$$n(q_1,\ldots,q_s,d) \equiv 0 \bmod p_2^r \qquad \text{if } p_1 \neq p_2 = \ldots = p_{r+1} \neq p_{r+2},$$

$$n(q_1,\ldots,q_s,d) \equiv 1 \bmod p \qquad \text{if } p_1 = p_2 = \ldots = p_r \neq p_{r+1}.$$

It turns out that $H_U(X, Y) = h_U^{-1}(h_U(X) + h_U(Y))$ is indeed a universal formal group (over $\mathbf{Z}[U]$). Cf. [3] and [4].

If one chooses the $n(q_1, \ldots, q_s, d)$ in a rather special way (cf. [3] and [4] for details) then one finds reasonable formulae for the U_i in terms of the $a_i(U)$. Now there is another universal formal group viz. the formal group of complex cobordism. Using the formulae for U_i in terms of $a_i(U)$ one then finds polynomial generators for MU(pt) in terms of the (classes of) complex projective spaces. Cf. [3] and [4].

Subsequently, Kozma [6], using Witt vectors and a theorem of Cartier, wrote down similar generators for MU(pt). These are different and satisfy a more elegant recursion formula. Translating back one obtains another universal formal group. The formula for its logarithm $f_U(X) = \sum m_n(U)X^n$ is very similar to (1.4) above (cf. (2.2.1) and (2.2.4) below).

This logarithm also satisfies functional equations (1.1), which is the essential property for integrality of the corresponding formal group by the functional equation lemma [2, 7.1].

It is slightly more complicated in terms of the number of different monomials occurring in the $m_i(U)$ (compared to $a_i(U)$) but, I think, superior because of the more elegant recursion relations. The calculations which one has to do to prove that these two different universal formal groups are integral (i.e. defined over $\mathbf{Z}[U]$) are identical.

As in the local case (cf. [2]) using the approach of Buhštaber and Novikov [1] one can prove directly that $F_U(X, Y)$ is universal, without using Lazard's comparison lemma, which now appears as a corollary.

Section 2 below contains the main constructions and results. In Sections 3, 4, 5 we prove the integrality and universality theorems. In Section 7 we show how to choose the coefficients in such a way that nice recursion relations result. In Section 6 we construct a universal strict isomorphism of formal groups.

Some of the applications of this paper and the previous one [2] to complex cobordism and Brown–Peterson cohomology will appear in [5]. Other applications will appear in subsequent papers. Most of the results of this paper have appeared in preprint form in [4]. The conventions of [2] remain in force, in particular all formal groups will be commutative and one dimensional and all rings are commutative and have a unit element.

2. Constructions, definitions and statement of main results

2.1. Choice of coefficients. For each $s \geq 1$ and each sequence $(i_1, \dots, i_s)$, $i_j \in \mathbf{N} \backslash \{1\}$ let $n(i_1, \dots, i_s)$ be an integer such that

(2.1.1) $\quad n(i_1, \dots, i_s) = 1 \quad \text{if } s = 1;$

(2.1.2) $\quad n(i_1, \dots, i_s) \equiv 0 \bmod p^{r-1}$ if $i_2, \dots, i_{r-1}$ are powers of a prime number p and i_1 and i_r are not powers of p;

(2.1.3) $\quad n(i_1, \dots, i_s) \equiv 1 \bmod p^r$ if $i_1, \dots, i_r$ are powers of a prime number p and i_{r+1} is not a power of p.

Note that there are (many) numbers $n(i_1, \dots, i_s)$ satisfying these conditions; $n(i_1, \dots, i_s)$ has to satisfy two different congruences if and only if i_1 and i_2 are powers of two different prime numbers.

2.2. Constructions. We now define the power series $f_U(X)$, $\bar{f}_U(X)$, $f_{U,T}(X)$ by the following formulae:

$$f_U(X) = \sum_{k=1}^{\infty} m_k(U) X^k, \qquad m_1(U) = 1, \tag{2.2.1}$$

$$\bar{f}_U(X) = \sum_{k=1}^{\infty} \bar{m}_k(U) X^k, \qquad \bar{m}_1(U) = 1, \tag{2.2.2}$$

$$f_{U,T}(X) = \sum_{k=1}^{\infty} m_k(U, T) X^k, \qquad m_1(U, T) = 1 \tag{2.2.3}$$

where

$$m_k(U) = \sum_{(i_1, \dots, i_s)} \frac{n(i_1, \dots, i_s)}{\nu(i_1)} \cdot \frac{n(i_2, \dots, i_s)}{\nu(i_2)} \cdots \frac{n(i_s)}{\nu(i_s)} U_{i_1} U_{i_2}^{i_1} \cdots U_{i_s}^{i_1 \cdots i_{s-1}} \tag{2.2.4}$$

where $\nu(i_j) = p$ if i_j is a power of the prime number p and $\nu(i_j) = 1$ if i_j is not a prime power and where the sum is over all sequences $(i_1, \ldots, i_s)$ with $i_j \in \mathbf{N}\backslash\{1\}$ and $s \geq 1$ and $i_1 \ldots i_s = k$. The numbers $n(i_1, \ldots, i_s)$ are such that (2.1.1)–(2.1.3) hold.

$$\bar{m}_k(U) \text{ is obtained from } m_k(U) \text{ by substituting 0 for all } U_d \text{ with } d > 1 \text{ and } d \text{ not a power of a prime number.} \tag{2.2.5}$$

$$m_k(U, T) = \tag{2.2.6}$$

$$= \sum_{(i_1, \ldots, i_s)} \frac{n(i_1, \ldots, i_s)}{\nu(i_1)} \cdot \frac{n(i_2, \ldots, i_s)}{\nu(i_2)} \cdots \frac{n(i_s)}{\nu(i_s)} U_{i_1} U_{i_2}^{i_1} \ldots U_{i_{s-1}}^{i_1 \cdots i_{s-2}} (U_{i_s}^{i_1 \cdots i_{s-1}} + \nu(i_s) T_{i_s}^{i_1 \cdots i_{s-1}}).$$

The power series $f_U(X)$ and $\bar{f}_U(X)$ are over $\mathbf{Q}[U_2, U_3, \ldots] = \mathbf{Q}[U]$ and $f_{U,T}(X)$ is a power series with its coefficients in $\mathbf{Q}[U_2, U_3, \ldots; T_2, T_3, \ldots]$. We now define

$$F_U(X, Y) = f_U^{-1}(f_U(X) + f_U(Y)), \qquad \bar{F}_U(X, Y) = \bar{f}_U^{-1}(\bar{f}_U(X) + \bar{f}_U(Y)),$$
$$F_{U,T}(X, Y) = f_{U,T}^{-1}(f_{U,T}(X) + f_{U,T}(Y)). \tag{2.2.7}$$

2.3. Integrality theorem. *The power series $F_U(X, Y)$, $\bar{F}_U(X, Y)$ and $F_{U,T}(X, Y)$ have their coefficients respectively in $\mathbf{Z}[U]$, $\mathbf{Z}[U]$, $\mathbf{Z}[U, T]$.*

I.e. these power series are formal groups over $\mathbf{Z}[U]$ and $\mathbf{Z}[U, T]$.

2.4. Universality theorem. *The formal group $F_U(X, Y)$ is universal.*

I.e. for every ring A and every (one dimensional commutative) formal group $G(X, Y)$ over A there is a unique homomorphism $\phi : \mathbf{Z}[U] \to A$ such that $F_U^{\phi}(X, Y) = G(X, Y)$.

2.5. Isomorphism theorems. (i) *The formal groups $F_U(X, Y)$ and $\bar{F}_U(X, Y)$ are strictly isomorphic (over $\mathbf{Z}[U]$).*

(ii) *The formal groups $F_U(X, Y)$ and $F_{U,T}(X, Y)$ are strictly isomorphic (over $\mathbf{Z}[U, T]$, where $\mathbf{Z}[U]$ is seen as a subring of $\mathbf{Z}[U, T]$).*

Let $\alpha_{U,T}(X)$ be the unique strict isomorphism between $F_U(X, Y)$ and $F_{U,T}(X, Y)$, i.e. $\alpha_{U,T}(X) = f_{U,T}^{-1}(f_U(X))$.

2.6. Universal isomorphism theorem. *The triple $(F_U(X, Y), \alpha_{U,T}(X), F_{U,T}(X, Y))$ is universal for formal groups and a strict isomorphism between them.*

I.e. for every ring A and every triple $(F(X, Y), \alpha(X), G(X, Y))$ consisting of two formal groups $F(X, Y)$, $G(X, Y)$ and a strict isomorphism $\alpha(X)$ from $F(X, Y)$ to $G(X, Y)$ there is unique homomorphism $\phi : \mathbf{Z}[U, V] \to A$ such that $F_U^{\phi}(X, Y) = F(X, Y)$, $\alpha_{U,T}^{\phi}(X) = \alpha(X)$ and $F_{U,T}^{\phi}(X, Y) = G(X, Y)$.

3. Some congruences and lemmas

This section contains some technical results on the f_U, $f_{U,T}$ and $n(i_1,\dots,i_s)$ which will be needed in the sequel.

3.1. Some congruences. Directly from the definitions (2.2.1)–(2.2.7) one sees that

(3.1.1) $f_U(X)\equiv X+\nu(n)^{-1}U_nX^n \bmod(U_2,\dots,U_{n-1},\text{ degree } n+1)$,

(3.1.2) $f_{U,T}(X)\equiv f_U(X)+T_nX^n \bmod(T_2,\dots,T_{n-1},\text{ degree } n+1)$,

(3.1.3) $\alpha_{U,T}(X)\equiv X-T_nX^n \bmod(T_2,\dots,T_{n-1},\text{ degree } n+1)$,

(3.1.4) $f_U(X,Y)\equiv X+Y-U_n(\nu(n)^{-1}B_n(X,Y)) \bmod(U_2,\dots,U_{n-1},\text{ degree } n+1)$

where $B_n(X,Y)=(X+Y)^n-X^n-Y^n$. (If n is a power of a prime number q, then $B_n(X,Y)$ is divisible by $q=\nu(n)$.)

More precisely one has the following. Let $U(n)$ be short for $(U_2,U_3,\dots,U_n,0,0,\dots)$ and let $f_{U(n)}(X)$, $F_{U(n)}(X,Y)$ be the formal power series obtained from $f_U(X)$ and $F_U(X,Y)$ by substituting zero for $U_{n+1},U_{n+2},\dots$. Then one has (immediately from (2.2.1)–(2.2.7)):

(3.1.5) $f_U(X)\equiv f_{U(n)}(X)+\nu(n+1)^{-1}U_{n+1}X^{n+1} \bmod(\text{degree } n+2)$,

(3.1.6) $f_{U,T}(X)\equiv f_{U,T(n)}(X)+T_{n+1}X^{n+1} \bmod(\text{degree } n+2)$,

(3.1.7) $\alpha_{U,T}(X)\equiv \alpha_{U,T(n)}(X)-T_{n+1}X^{n+1} \bmod(\text{degree } n+2)$,

(3.1.8) $F_U(X,Y)\equiv F_{U(n)}(X,Y)-U_{n+1}(\nu(n+1)^{-1}B_{n+1}(X,Y)) \bmod(\text{degree } n+2)$.

3.2. For each sequence $(i_1,\dots,i_s)$, $i_j\in\mathbf{N}\backslash\{1\}$ let

(3.2.1) $$d(i_1,\dots,i_s)=\frac{n(i_1,\dots,i_s)}{\nu(i_1)}\cdots\frac{n(i_s)}{\nu(i_s)}=\frac{n(i_1,\dots,i_s)}{\nu(i_1)}d(i_2,\dots,i_s)$$

where the $n(i_1,\dots,i_s)$ satisfy the conditions of 2.1.

3.3. Lemma. (i) *If* $1\neq\nu(i_1)=\nu(i_2)=\dots=\nu(i_r)\neq\nu(i_{r+1})$, $r\leq s$, *then* $p^rd(i_1,\dots,i_s)\in\mathbf{Z}$ *where* $p=\nu(i_1)=\dots=\nu(i_r)$. *(If* $r=s$ *then* $\nu(i_r)\neq\nu(i_{r+1})$ *is taken to be automatically fulfilled.)*

(ii) *If* $\nu(i_1)=1$ *then* $d(i_1,\dots,i_s)\in\mathbf{Z}$.

Proof. We prove both parts of the lemma simultaneously by induction on s. The case $s=1$ is trivial. If $s>1$ we distinguish four cases.

Case (1): $\nu(i_1)=1=\nu(i_2)$. Then $d(i_2,\dots,i_s)\in\mathbf{Z}$ and hence $d(i_1,\dots,i_s)=\nu(i_s)^{-1}n(i_1,i_2,\dots,i_s)d(i_2,\dots,i_s)\in\mathbf{Z}$.

Case (2): $\nu(i_1)=1\neq\nu(i_2)=p$. Let $\nu(i_2)=\dots=\nu(i_t)\neq\nu(i_{t+1})$. Then by induction $p^{t-1}d(i_2,\dots,i_s)\in\mathbf{Z}$ and hence $d(i_1,\dots,i_s)=\nu(i_1)^{-1}n(i_1,i_2,\dots,i_s)d(i_2,\dots,i_s)\in\mathbf{Z}$ because $n(i_1,i_2,\dots,i_s)\equiv 0 \bmod p^{t-1}$ by (2.1.2) in this case.

Case (3): $1 \neq \nu(i_1) = \nu(i_2)$. Then $p^{r-1}d(i_2, \ldots, i_s) \in \mathbf{Z}$ and hence

$$p^r d(i_1, \ldots, i_s) = \nu(i_1)^{-1} n(i_1, i_2, \ldots, i_s) p^r d(i_2, \ldots, i_s)$$
$$= n(i_1, \ldots, i_s) p^{r-1} d(i_2, \ldots, i_s) \in \mathbf{Z}.$$

Case (4): $1 \neq \nu(i_1) \neq \nu(i_2) \neq 1$. Let $q = \nu(i_2) = \ldots = \nu(i_t) \neq (i_{t+1})$. Then by induction $q^{t-1}d(i_2, \ldots, i_s) \in \mathbf{Z}$ and hence $pd(i_1, \ldots, i_s) = n(i_1, \ldots, i_s) d(i_2, \ldots, i_s) \in \mathbf{Z}$ because by (2.1.2) $n(i_1, i_2, \ldots, i_s) \equiv 0 \bmod q^{t-1}$ in this case. □

3.4. Lemma. *Let $1 \neq \nu(i_1) = p$, then $d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$.*

Proof. We distinguish three cases

Case (1): $\nu(i_2) = 1$. Then $d(i_2, \ldots, i_s) \in \mathbf{Z}$ by Lemma 3.3 and hence

$$d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) = p^{-1}(n(i_1, \ldots, i_s) - 1) d(i_2, \ldots, i_s) \in \mathbf{Z}$$

because $n(i_1, \ldots, i_s) \equiv 1 \bmod p$ in this case by (2.1.3).

Case (2): $1 \neq \nu(i_2) = q \neq p$. Then $d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$ by Lemma 3.3 and $d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) \in \mathbf{Z}_{(p)}$ as in case (1).

Case (3): $\nu(i_2) = p$. Let $\nu(i_2) = \nu(i_3) = \ldots = \nu(i_r) \neq \nu(i_{r+1})$. Then $p^{r-1}d(i_2, \ldots, i_s) \in \mathbf{Z}$ and hence

$$d(i_1, \ldots, i_s) - p^{-1}d(i_2, \ldots, i_s) = p^{-1}(n(i_1, \ldots, i_s) - 1) d(i_2, \ldots, i_s) \in \mathbf{Z}$$

because according to (2.1.3) $n(i_1, \ldots, i_s) \equiv 1 \bmod p^r$ in this case. □

4. Proof of the integrality theorems

4.1. For each $k \geq 2$, let c_k be an element of $\mathbf{Z}[U; T]$ and for each $i \in \mathbf{N}$ let $c_k^{(i)}$ be the polynomial obtained from c_k by replacing each U_j and T_l by their i-th powers U_j^i and T_l^i. We define

(4.1.1) $$g(X) = \sum_{i=1}^{\infty} e_i X^i, \qquad e_1 = 1,$$

(4.1.2) $$e_i = \sum_{(i_1, \ldots, i_s)} d(i_1, \ldots, i_s) U_{i_1} U_{i_2}^{i_1} \ldots U_{i_{s-1}}^{i_1 \cdots i_{s-2}} \cdot (U_{i_s}^{i_1 \cdots i_{s-1}} + \nu(i_s) c_{i_s}^{(i_1 \cdots i_{s-1})})$$

where the sum is over all $(i_1, \ldots, i_s)$ such that $i_1 \ldots i_s = i$, $i_j \in \mathbf{N} \backslash \{1\}$, and $d(i_1, \ldots, i_s)$ is as in (3.2)

4.2. Lemma. *For all prime numbers p we have that*

(4.2.1) $$g(X) - \sum_{k=1}^{\infty} \frac{U_{p^k}}{p} g^{(p^k)}(X^{p^k}) \in \mathbf{Z}_{(p)}[U; T][[X]].$$

Proof. Consider the coefficient of X^n in (4.2.1). If $(p, n) = 1$ this coefficient is equal to e_n and is in $\mathbf{Z}_{(p)}[U; T]$ by Lemma 3.3. Now suppose $(p, n) > 1$ and let $n = p^r i$, $(p, i) = 1$. The coefficient of X^n in (4.2.1) is then equal to

(4.2.2) $$e_{p^r i} - \frac{U_p}{p} e^{(p)}_{p^{r-1} i} - \ldots - \frac{U_{p^r}}{p} e^{(p^r)}_{i}.$$

For the terms of $e_{p^r i}$ with $\nu(i_1) \neq p$ we have that $d(i_1, \ldots, i_s) \in \mathbf{Z}_{(p)}$. It remains to deal with the terms with $i_1 = p, p^2, \ldots, p^r$. We have, if $i > 1$ or $t < r$,

$$\sum_{i_1 = p^t} d(i_1, \ldots, i_s) U_{i_1} \ldots U_{i_{s-1}}^{i_1 \ldots i_{s-2}} (U_{i_s}^{i_1 \ldots i_{s-1}} + \nu(i_s) c_{i_s}^{(i_1 \ldots i_{s-1})})$$

$$= \sum_{i_1 = p^t} \frac{U_{p^t}}{p} n(i_1, \ldots, i_s) d(i_2, \ldots, i_s) U_{i_2}^{i_1} \ldots U_{i_{s-1}}^{i_1 \ldots i_{s-2}} (U_{i_s}^{i_1 \ldots i_{s-1}} + \nu(i_s) c_{i_s}^{(i_1 \ldots i_{s-1})}).$$

And because of Lemma 3.4 we see that the part of $e_{p^r i}$ with $i_1 = p^t$ minus $p^{-1} U_{p^t} e^{(p^t)}_{p^{r-t} i}$ is in $\mathbf{Z}_{(p)}[U, T]$ if $i > 1$ or $t < r$.

And if $i = 1$, $t = r$ we have that the part of $e_{p^r i}$ with $i_1 = p^t$ is equal to $p^{-1} U_{p^r} + c_{p^r} = p^{-1} U_{p^r} e_1^{(p^r)} + c_{p^r}$ and $c_{p^r} \in \mathbf{Z}[U; T]$. So we see that (4.2.2) is in $\mathbf{Z}_{(p)}[U; T]$. □

4.3. Proof of the integrality theorem 2.3 (parts (i) and (iii)). Taking $c_k = 0$ for all $k \geq 2$ we get $g(X) = f_U(X)$. Hence f_U satisfies a functional equation (4.2.1), and we can apply [2, 3.3] to conclude that $F_U(X, Y) \in \mathbf{Z}_{(p)}[U][[X]]$ for all prime numbers p, hence $F_U(X, Y) \in \mathbf{Z}[U][[X, Y]]$.

Taking $c_k = T_k$, $k = 2, 3, \ldots$ we find $g(U) = f_{U,T}(X)$ and the same argument gives that $F_{U,T}(X, Y) \in \mathbf{Z}[U; T][[X, Y]]$.

4.4. Proof of the integrality theorem 2.3 (part (ii)). $\bar{F}_U(X, Y)$ is obtained from $F_U(X, Y)$ by substituting 0 for all U_d with d not a power of a prime number. So $\bar{F}_U(X, Y)$ is integral because $F_U(X, Y)$ is integral. (One can also show that $\bar{f}_U(X)$ satisfies a functional equation of type (4.2.1) for all p.)

5. Proof of the universality theorem 2.4

This proof is completely analogous to the proof of universality of $F_S(X, Y)$ in [2].

5.1. For each $n \in \mathbf{N} \backslash \{1\}$ we have that g.c.d. $(\binom{n}{1}, \ldots, \binom{n}{n-1}) = \nu(n)$. Choose $\lambda_{n,i} \in \mathbf{Z}$ such that

(5.1.1) $$\lambda_{n,1} \binom{n}{1} + \ldots + \lambda_{n,n-1} \binom{n}{n-1} = \nu(n).$$

Write

(5.1.2) $$F_U(X, Y) = X + Y + \sum_{i,j \geq 1} e_{ij} X^i Y^j$$

and define

(5.1.3) $$y_n = \sum_{i=1}^{n-1} \lambda_{n,i} e_{i,n-i}.$$

5.2. Lemma. *The y_n, $n = 2, 3, \ldots$ are a polynomial basis for $\mathbf{Z}[U] = \mathbf{Z}[U_2, U_3, \ldots]$.*

I.e. every element of $\mathbf{Z}[U]$ can be uniquely written as a polynomial in the y_n with coefficients in $\mathbf{Z}$.

Proof. This follows directly from (3.1.4).

5.3. Proof of the universality theorem. Let A be a ring and $G(X, Y)$ a formal group over A. Write

(5.3.1) $$G(X, Y) = X + Y + \sum_{i,j \geq 1} a_{ij} X^i Y^j.$$

Now define $\phi : \mathbf{Z}[U] \to A$ by the requirement $\phi(y_n) = \sum_{i=1}^{n-1} \lambda_{n,i} a_{i,n-i}$. This is a well defined homomorphism because of Lemma 5.2. Further if ψ is a homomorphism $\mathbf{Z}[U] \to A$ such that $F_U^{\psi}(X, Y) = G(X, Y)$ then we have $\psi(e_{ij}) = a_{ij}$ and hence $\psi(y_n) = \phi(y_n)$. This takes care of uniqueness. One now proves that $\phi(e_{ij}) = a_{ij}$ exactly as in [2, 6.2]. □

5.4. Corollary (Lazard's comparison lemma). *Let A be a ring and $F(X, Y)$ and $G(X, Y)$ two formal groups over A. Suppose that*

(5.4.1) $$F(X, Y) \equiv G(X, Y) \bmod(\text{degree } n).$$

Then there is a (unique) $a \in A$ such that

(5.4.2) $$F(X, Y) \equiv G(X, Y) + a(\nu(n)^{-1} B_n(X, Y)) \bmod(\text{degree } n + 1).$$

This follows directly from Theorem 2.4 and (3.1.5).

This corollary completes the proofs of Theorem 2.8 and its corollaries in [2].

6. Isomorphism theorems

6.1. Proof of Theorem 2.5. Let $F(X, Y)$ and $G(X, Y)$ be two formal groups over $\mathbf{Z}[U; T]$ with logarithms $f(X)$, $g(X) \in \mathbf{Q}[U; T][[X]]$; i.e. $F(X, Y) = f^{-1}(f(X) + f(Y))$, $G(X, Y) = g^{-1}(g(X) + g(Y))$. The formal groups $F(X, Y)$ and $G(X, Y)$ are strictly isomorphic if and only if $g^{-1}(f(X)) \in \mathbf{Z}[U; T][[X]]$ and this is the case if and only if $g^{-1}(f(X)) \in \mathbf{Z}_{(p)}[T; U][[X]]$ for all prime numbers p.

The power series $f_U(X)$, $\bar{f}_U(X)$, $f_{U,T}(X)$ all satisfy functional equations (4.2.1). Hence it suffices to apply the functional equation lemma [2, 7.1] to prove Theorem 2.5.

6.2. Proof of Theorem 2.6 (universality of the triple $(F_U(X, Y), \alpha_{U,T}(X), F_{U,T}(X, Y))$). Let $F(X, Y)$ and $G(X, Y)$ be two formal groups over a ring A and $\alpha(X)$ an isomorphism from $F(X, Y)$ to $G(X, Y)$. Because of universality of $F_U(X, Y)$, there is a unique homomorphism $\psi: \mathbf{Z}[U] \to A$ such that $F_U^{\psi}(X, Y) = F(X, Y)$. Suppose we have already found a homomorphism $\phi_n : \mathbf{Z}[U, T] \to A$ such that

(6.2.1) $\quad F_U^{\phi_n}(X, Y) = F(X, Y)$, i.e. ϕ_n is equal to ψ on $\mathbf{Z}[U] \subset \mathbf{Z}[U; T]$,

(6.2.2) $\quad \alpha_{U,T}^{\phi_n}(X) \equiv \alpha(X) \bmod(\text{degree } n)$

and suppose that ϕ_n is unique on the subring $\mathbf{Z}[U; T_2, \ldots, T_{n-1}]$ of $\mathbf{Z}[U; T]$. There is a unique $a \in A$ such that

(6.2.3) $\quad \alpha_{U,T}^{\phi_n}(X) \equiv \alpha(X) + aX^n \bmod(\text{degree } n + 1)$.

Now define ϕ_{n+1} by $\phi_{n+1}(U_i) = \psi(U_i)$; $\phi_{n+1}(T_i) = \phi_n(T_i)$, $i = 1, \ldots, n-1$; $\phi_{n+1}(T_n) = -a$; $\phi_{n+1}(T_i) = 0$, $i \geq n+1$. Then (6.2.1) and (6.2.2) hold with n replaced by $n+1$ and ϕ_{n+1} is unique on $\mathbf{Z}[U; T_2, \ldots, T_n]$, both because of (3.1.7).

6.3. Remark. The arguments of 6.1 show that if $g(X)$ is any of the power series defined by (4.1.1) and (4.1.2) and $G(X, Y) = g^{-1}(g(X) + g(Y))$, then $G(X, Y)$ is a formal group over $\mathbf{Z}[U; T]$ (by 4.2 and 4.3) and $G(X, Y)$ is strictly isomorphic to $F_{U,T}(X, Y)$.

7. A special choice for the $n(i_1, \ldots, i_s)$

In this section we define special $n(i_1, \ldots, i_s)$, which are such that there are reasonable formulas for the U_i in terms of the $m_i(U)$.

7.1. For each prime number p and each $i \in \mathbf{N}\backslash\{1\}$ let $c(p, i)$ be an integer such that

(7.1.1)
$$c(p, i) = 1 \quad \text{if } \nu(i) = 1$$
$$c(p, p^r) = 1$$
$$c(p, i) \equiv \begin{cases} 1 & \bmod p \\ 0 & \bmod q \end{cases} \quad \text{if } \nu(i) = q \neq p.$$

We now define $b(i_1, \ldots, i_s)$ for all sequences $(i_1, \ldots, i_s)$ with $i_j \in \mathbf{N}\backslash\{1\}$ by the recursion formula

(7.1.2)
$$b(i) = \prod_{p \mid i} c(p, i),$$
$$b(i_1, \ldots, i_s) = \prod_{p \mid i_1 \ldots i_s} c(p, i_s) b(i_1, \ldots, i_{s-1}) \quad \text{if } s \geq 2$$

where the product is over all prime numbers p which divide $i_1 \dots i_s$. (The factor $c(p, i_s)$ occurs only once, irrespective of how high a power of p divides $i_1 \dots i_s$.)

Finally we define

$$(7.1.3) \qquad n(i_1, \dots, i_s) = \frac{b(i_1, \dots, i_s)}{b(i_2, \dots, i_s)} \qquad \text{if } s \geq 2, \text{ and } n(i) = 1.$$

7.2. It follows directly from (7.1.2) that

$$(7.2.1) \qquad b(i_1, \dots, i_s) = \prod_{p \mid i_1 \dots i_s} c(p, i_s) \prod_{p \mid i_1 \dots i_{s-1}} c(p, i_{s-1}) \dots \prod_{p \mid i_1 i_2} c(p, i_2) \prod_{p \mid i_1} c(p, i_1)$$

and hence that

$$(7.2.2) \qquad n(i_1, \dots, i_s) = \prod_{\substack{p \mid i_1 \\ p \nmid i_2 \dots i_s}} c(p, i_s) \prod_{\substack{p \mid i_1 \\ p \nmid i_2 \dots i_{s-1}}} c(p, i_{s-1}) \dots \prod_{\substack{p \mid i_1 \\ p \nmid i_2}} c(p, i_2) \prod_{p \mid i_1} c(p, i_1).$$

7.3. Lemma. *The* $n(i_1, \dots, i_s)$ *defined by* (7.3.1) *satisfy conditions* (2.1.1)–(2.1.3).

Proof. (2.1.1) is satisfied by definition. Suppose that $1 \neq p = \nu(i_1) = \dots = \nu(i_r) \neq \nu(i_{r+1})$. First let $r \geq 2$. The only prime number dividing i_1 is p, and p also divides $i_2, i_2 i_3, \dots, i_2 \dots i_{s-1}$. Therefore $n(i_1, \dots, i_s) = 1$ in this case. Now let $r = 1$. The only prime dividing i_1 is p and $c(p, i) \equiv 1 \bmod p$ for all $i \in \mathbf{N} \backslash \{1\}$. It now follows from (7.2.2) that $n(i_1, \dots, i_s) \equiv 1 \bmod p$. This proves (2.1.3). Now let $\nu(i_1) \neq p = \nu(i_2) = \dots = \nu(i_r) \neq \nu(i_{r+1})$. Then there is a prime number q which divides i_1 but does not divide $i_2, i_2 i_3, \dots, i_2 \dots i_r$. It now follows from (7.2.2) that $n(i_1, \dots, i_s)$ contains the factor $c(q, i_2) c(q, i_3) \dots c(q, i_r)$. But $c(q, i_t) \equiv 0 \bmod p$, because $\nu(i_t) = p \neq 1$ for $t = 2, \dots, r$. This proves (2.1.2).

7.4. Let $d(i_1, \dots, i_s)$ be as in 3.2, i.e.

$$(7.4.1) \qquad d(i_1, \dots, i_s) = \frac{n(i_1, \dots, i_s)}{\nu(i_1)} \cdot \dots \cdot \frac{n(i_s)}{\nu(i_s)}$$

then we have by (7.1.3)

$$(7.4.2) \qquad \frac{d(i_1, \dots, i_s)}{d(i_1, \dots, i_{s-1})} = \frac{1}{\nu(i_s)} \prod_{p \mid i_1 \dots i_s} c(p, i_s) \quad \text{for } s \geq 2.$$

Note that this number depends only on the product $i_1 \dots i_s$ and i_s. We define for all $n, d \in \mathbf{N} \backslash \{1\}$

$$(7.4.3) \qquad \mu(n, d) = \prod_{p \mid n} c(p, d).$$

7.5. A Recursion formula for the U_n in terms of the $m_n(U)$

We have according to (2.2.4) and (7.4.1) that

$$m_n(U) = \sum d(i_1, \dots, i_s) U_{i_1} U_{i_2}^{i_1} \dots U_{i_s}^{i_1 \cdots i_{s-1}}$$

$$= \sum_{s \geq 2} \frac{\mu(i_1 \dots i_s, i_s)}{\nu(i_s)} (d(i_1, \dots, i_{s-1}) U_{i_1} \dots U_{i_{s-1}}^{i_1 \cdots i_{s-2}}) U_{i_s}^{i_1 \cdots i_{s-1}} + \frac{1}{\nu(n)} U_n$$

$$= \sum_{\substack{d \mid n \\ d \neq 1, n}} \frac{\mu(n, d)}{\nu(d)} m_{n/d}(U) U_d^{n/d} + \mu(n)^{-1} U_n.$$

So that we find

$$\nu(n) m_n(U) = U_n + \sum_{\substack{d \mid n \\ d \neq 1, n}} \frac{\mu(n, d)\nu(n)}{\nu(d)} m_{n/d}(U) U_d^{n/d}. \tag{7.5.1}$$

Note that the factor $\nu(d)^{-1}\nu(n)\mu(n, d)$ is always integral. Indeed, this factor is certainly integral if $\nu(d) = 1$ and if $\nu(d) = p = \nu(n)$. And if $\nu(d) = p \neq \nu(n)$ there is a prime number $q \neq p$ dividing n so that $\mu(n, d)$ contains a factor $c(q, d)$ which is congruent to zero mod p by (7.1.1). Note also that $\nu(d)^{-1}\nu(n)\mu(n, d) = 1$ if $\nu(n) \neq 1$ (and $d \mid n$) and that $\nu(d)^{-1}\nu(n)\mu(n, d) = 1$ if $\nu(d) = 1$ (and hence also $\nu(n) = 1$). So the only factors $\nu(d)^{-1}\mu(n, d)\nu(n)$ different from 1 occurring in (7.5.1) have $\nu(n) = 1$ and $\nu(d) \neq 1$. Cf. also [6].

7.6. Remark. Let $H_U(X, Y) = h_U^{-1}(h_U(X) + h_U(Y))$ where $h_U(X)$ is the power series defined in (1.4). Then one has (i) $H_U(X, Y)$ has its coefficients in $\mathbf{Z}[U]$; (ii) the formal groups $H_U(X, Y)$ and $F_U(X, Y)$ are strictly isomorphic over $\mathbf{Z}[U]$; (iii) $H_U(X, Y)$ is a universal formal group. These things are proved in exactly the same way as the corresponding statements for $F_U(X, Y)$.

A natural more dimensional generalization of $H_U(X, Y)$ is discussed in [4] part V.

References

[1] V.M. Buhštaber, S.P. Novikov, Formal Groups, Power Systems and Adams Operations, Mat. Sbornik 84 (1971) 81–118.

[2] M. Hazewinkel, Constructing Formal Groups I: The Local One Dimensional Case, J. Pure Appl. Algebra 9 (1977) 131–149.

[3] M. Hazewinkel, A Universal Formal Group and Complex Cobordism, Bull. Amer. Math. Soc. 81, 5 (1975) 930–933.

[4] M. Hazewinkel, Constructing Formal Groups I, II, III, IV, V, Reports 7119, 7201, 7207, 7322, 7505 of the Econometric Institute, Erasmus University Rotterdam (1971, 1972, 1973, 1975).

[5] M. Hazewinkel, Constructing Formal Groups III: Applications to Complex Cobordism and Brown–Peterson Cohomology, J. Pure Appl. Algebra, to be published.

[6] J. Kozma, Witt Vectors and Complex Cobordism, Topology 13, 4 (1974) 389–394.