ECONOMETRIC INSTITUTE

CONSTRUCTING FORMAL GROUPS I: HE LOCAL ONE DIMENSIONAL CASE AND CONSTRUCTING FORMAL GROUPS II: HE GLOBAL ONE DIMENSIONAL CASE

M. HAZEWINKEL

REPRINT SERIES no. 202

se articles appeared in "Journal of Pure and Applied Algebra", 9,(1977).

SMUS UNIVERSITY ROTTERDAM,
BOX 1738, ROTTERDAM, THE NETHERLANDS

Journal of Pure and Applied Algebra 9 (1977) 131–149

CONSTRUCTING FORMAL GROUPS I: THE LOCAL 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 28 April 1975

AMS Subj. Class.: Primary 14L05
formal group — universal formal group
p-typical formal group — universal isomorphism

1. Introduction

This is the first of a series of papers in which we first give fairly explicit formulas for universal commutative formal groups and then proceed to give various applications of these constructions to e.g. complex cobordism and Brown–Peterson cohomology (part III), norm maps (part VII), classification theory via Cartier–Dieudonné modules (part VI) and formal moduli (part V). The following special case may serve to give the flavor of the constructions. If $g(X)$ is a power series over $\mathbf{Z}[V]=\mathbf{Z}[V_1, V_2, \dots]$ then $g^{(n)}(X)$ denotes the power series obtained from $g(X)$ by replacing each V_i with V_i^n, $i=1,2,\dots$. Choose a prime number p and let $f_V(X)$ be the power series defined by the functional equation

$$(1.1)\qquad f_V(X)=X+\sum_{i=1}^{\infty}\frac{V_i}{p}f_V^{(p^i)}(X^{p^i})$$

and let $F_V(X,Y)=f_V^{-1}(f_V(X)+f_V(Y))$. Then $F_V(X,Y)$ is a p-typically universal, one dimensional, commutative formal group over $\mathbf{Z}[V]$. It turns out that "satisfying a function equation like (1.1)" is the essential (and sufficient) condition for integrality of $F_V(X,Y)$. Moreover two logarithms which satisfy functional equations (1.1) "with the same V_i" yield isomorphic formal groups. For a more precise statement, cf. the functional equation Lemma 7.1 below.

Given such a fairly explicit candidate for a universal formal group it becomes possible to use a method of Buhštaber and Novikov [1] to give a direct proof of universality. They used this method for the formal group of complex cobordism.

* Most of the research for this paper was done in 1969/1970 while the author stayed at the Steklov Inst. of Mathematics in Moscow and was supported by ZWO (The Netherlands Organization for the Advancement of Pure Research).

Thus one obtains noticeably shorter proofs of the main theorems concerning universal formal groups and one avoids part of Lazard's difficult comparison lemma. Cf. also Section 5 below.

Now let A be a $\mathbf{Z}_{(p)}$-algebra. One dimensional formal groups over A are classified by left modules of the form $M = E_A/(\mathbf{f} - \sum_{i=1}^{\infty} \mathbf{V}^i[v_i])$ over E_A, where E_A is a certain ring which contains $\mathbf{f}$ (= Frobenius), $\mathbf{V}$ (= Verschiebung) and elements $[a]$, $a \in A$. Cf. [2]. Let $F_v(X, Y)$ be the formal group over A obtained from $F_V(X, Y)$ by substituting v_i for V_i, $i = 1, 2, \ldots$. Then M is the module of p-typical curves of $F_v(X, Y)$. This is possibly the best way to look at these constructions.

In this first part we construct a one dimensional formal group which is universal for one dimensional commutative formal groups over $\mathbf{Z}_{(p)}$-algebras, a p-typically universal one dimensional commutative formal group, and a universal strict isomorphism between p-typical formal groups. Most of the results in this paper have appeared in preprint form in [5]; some of these results have been announced in [6].

For the basic definitions concerning formal groups cf. e.g. [4]. We take the power series point of view. All formal groups in this paper will be commutative one dimensional. All rings will be commutative with unit element. If $F(X, Y)$ is a formal group over a ring A and $\phi : A \to B$ a homomorphism of rings then $F^{\phi}(X, Y)$ denotes the formal group over B obtained from $F(X, Y)$ by applying ϕ to the coefficients of $F(X, Y)$. $\mathbf{Z}$ stands for the integers, $\mathbf{Z}_{(p)}$ for the integers localized at p and $\mathbf{Q}$ for the rational numbers; $\mathbf{N}$ denotes the natural numbers; that is $\mathbf{N} = \{1, 2, 3, \ldots\}$.

2. Constructions, definitions and statement of main results

2.1. Notation. Let A be a ring and let $g_U(X)$ be a power series over $A[U_1, U_2, \ldots]$, i.e. the coefficients of $g_U(X)$ are polynomials in $U_1, U_2, \ldots$ over A. Then $g_U^{(i)}(X)$ denotes the polynomial obtained by replacing each U_j with U_j^i, $j = 1, 2, \ldots$; i.e. $g_U^{(i)}(X)$ is obtained from $g_U(X)$ by applying the A-endomorphism $U_j \mapsto U_j^i$ of $A[U_1, U_2, \ldots]$ to the coefficeints of $g_U(X)$.

2.2. Constructions. Choose a prime number p. The three power series $f_V(X)$, $f_{V,T}(X)$, $f_S(X)$ over respectively $\mathbf{Q}[V_1, V_2, \ldots]$, $\mathbf{Q}[V_1, V_2, \ldots; T_1, T_2, \ldots]$, $\mathbf{Q}[S_2, S_3, \ldots]$ are defined by

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

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

(2.2.3) $$f_S(X) = \sum_{i=1}^{\infty} S_i X^i - \sum_{i=1}^{\infty} S_{p^i} X^{p^i} + \sum_{i=1}^{\infty} \frac{S_{p^i}}{p} f_S^{(p^i)}(X^{p^i}), \quad S_1 = 1.$$

These "functional equations" define the power series $f_V(X)$, $f_{V,T}(X)$ and $f_S(X)$ recursively. For explicit formulae cf. Section 4 below. Now define

(2.2.4) $\quad F_V(X, Y) = f_V^{-1}(f_V(X) + f_V(Y)) \quad$ in $\mathbf{Q}[V][[X, Y]]$

(2.2.5) $\quad F_{V,T}(X, Y) = f_{V,T}^{-1}(f_{V,T}(X) + f_{V,T}(Y)) \quad$ in $\mathbf{Q}[V; T][[X, Y]]$

(2.2.6) $\quad F_S(X, Y) = f_S^{-1}(f_S(X) + f_S(Y)) \quad$ in $\mathbf{Q}[S][[X, Y]]$

where, if $g(X) = a_1X + a_2X^2 + \dots$ is a power series over A with zero constant term and a_1 a unit, $g^{-1}(X)$ denotes the inverse power series i.e. $g^{-1}(g(X)) = g(g^{-1}(X)) = X$.

2.3. Integrality theorem. *The formal power series $F_V(X, Y)$, $F_{V,T}(X, Y)$ and $F_S(X, Y)$ all have integral coefficients.*

I.e. their coefficients are respectively in $\mathbf{Z}[V]$, $\mathbf{Z}[V, T]$ and $\mathbf{Z}[S]$. This is the usual Witt-vector-type miracle.

2.4. Definitions. Let A be a ring and $F(X, Y)$ a (one dimensional commutative) formal group over a ring L. The formal group $F(X, Y)$ will be said to be universal for formal groups over A-algebras if for every formal group $G(X, Y)$ over an A-algebra B there exists a unique homomorphism $\phi : L \to B$ such that $F^{\phi}(X, Y) = G(X, Y)$. Note that if $F(X, Y)$ and $F'(X, Y)$ are two formal groups defined over L and L' respectively which are both universal for formal groups over A-algebras then we need not have $L \simeq L'$. Except when $A = \mathbf{Z}$. But in the case that A is a localisation of $\mathbf{Z}$, e.g. $A = \mathbf{Z}_{(p)}$ we do have that $L \otimes \mathbf{Z}_{(p)}$ and $L' \otimes \mathbf{Z}_{(p)}$ are isomorphic.

2.5. Theorem. *$F_S(X, Y)$ is universal for formal groups over $\mathbf{Z}_{(p)}$-algebras.*

2.6. Curves. Let $F(X, Y)$ be a formal group over a ring A. A curve over A is a formal power series $\gamma(X)$ over A with constant term equal to zero. Two curves can be added by means of $F(X, Y)$ as follows:

$$(\gamma_1 +_F \gamma_2)(X) := F(\gamma_1 X, \gamma_2 X) =: \gamma_1(X) +_F \gamma_2(X).$$

This turns the set of curves into an abelian group, which is denoted C_F. For every $n \in \mathbf{N}$ we define an operation $\mathbf{f}_n$ on C_F as follows. Choose variables $Z_1, \dots, Z_n$ and let $\gamma(X)$ be a curve. Write down

(2.6.1) $\quad \gamma(Z_1X^{1/n}) +_F \gamma(Z_2X^{1/n}) +_F \dots +_F \gamma(Z_nX^{1/n}) = \beta(Z_1, \dots, Z_n; X).$

This is a power series in $X^{1/n}$ with coefficients in $A[Z_1, \dots, Z_n]$ and because F is commutative and associative the coefficient of $X^{i/n}$ in (2.6.1) is a homogeneous symmetric polynomial in the $Z_1, \dots, Z_n$ of degree i. So we can write

(2.6.2) $\quad \beta(Z_1, \dots, Z_n; X) = \beta'(\sigma_1, \dots, \sigma_n; X)$

where $\sigma_1, \ldots, \sigma_n$ are the elementary symmetric polynomials in the $Z_1, \ldots, Z_n$. Now substitute 0 for $\sigma_1, \ldots, \sigma_{n-1}$ and $(-1)^{n-1}$ for σ_n in $\beta'(\sigma_1, \ldots, \sigma_n; X)$. This results in a power series in X which is denoted $\mathbf{f}_n\gamma(X)$.

If the ring A is such that it makes sense to talk about the n (different) roots of unity over A then one has

$$\mathbf{f}_n\gamma(X) = \gamma(\zeta_n X^{1/n}) +_F \ldots +_F \gamma(\zeta_n^n X^{1/n})$$

where ζ_n is a primitive n-th root of unity.

2.7. Definitions. Choose a prime number p. The formal group $F(X, Y)$ is called p-typical if $\mathbf{f}_q\gamma_0(X) = 0$ for all prime numbers q different from p, where $\gamma_0(X)$ is the curve $\gamma_0(X) = X$.

A p-typical formal group $F(X, Y)$ over a ring L is called universal for p-typical formal groups over $\mathbf{Z}_{(p)}$-algebras or characteristic zero rings if for every p-typical formal group $G(X, Y)$ over A, where A is a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring, there is a unique homomorphism $\varphi : L \to A$ such that $F^\varphi(X, Y) = G(X, Y)$. (A ring A is said to be of characteristic zero if $A \to A \otimes_{\mathbf{Z}} \mathbf{Q}$ is injective.)

2.8. Theorem. *The formal group $F_V(X, Y)$ is p-typical and universal for p-typical formal groups over $\mathbf{Z}_{(p)}$-algebras or characteristic zero rings.*

2.9. Definition. Two formal groups $F(X, Y)$ and $G(X, Y)$ over the same ring A are said to be strictly isomorphic if there is a power series $\alpha(X)$ of the form

$$\alpha(X) = X + \alpha_2 X^2 + \ldots, \qquad a_i \in A$$

such that

$$\alpha(F(X, Y)) = G(\alpha(X), \alpha(Y)).$$

Let $\iota : \mathbf{Z}[V] \to \mathbf{Z}[V, T]$ be the canonical embedding, let $\kappa : \mathbf{Z}[V] \to \mathbf{Z}[S]$ be the injection defined by $V_i \mapsto S_{p^i}$ and let λ denote any of the localization homomorphisms $\mathbf{Z}[V] \to \mathbf{Z}_{(p)}[V]$, $\mathbf{Z}[V, T] \to \mathbf{Z}_{(p)}[V, T]$, $\mathbf{Z}[S] \to \mathbf{Z}_{(p)}[S]$.

2.10. Theorem. *The formal groups $F_V^\kappa(X, Y)$, $F_S(X, Y)$ are strictly isomorphic and the formal groups $F_V^\iota(X, Y)$ and $F_{V,T}(X, Y)$ are strictly isomorphic.*

2.11. Corollary. *Every formal group over a $\mathbf{Z}_{(p)}$-algebra A is strictly isomorphic to a p-typical formal group over A.*

2.12. Theorem. *The triple $(F_V^\iota(X, Y), \alpha_{V,T}(X), F_{V,T}(X, Y))$, where $\alpha_{V,T}(X)$ is the unique strict isomorphism from $F_V^\iota(X, Y)$ to $F_{V,T}(X, Y)$, is universal for triples $(F(X, Y), \alpha(X), G(X, Y))$ consisting of two formal groups and a strict isomorphism between them over a ring A which is a $\mathbf{Z}_{(p)}$-algebra or a ring of characteristic zero.*

3. The integrality theorems

In this section we prove Theorem 2.3.

3.1. Let $f(X)$ be a power series in one variable of the form $f(X) = X + b_2X^2 + \dots$ with coefficients in $\mathbf{Q}[V_1, V_2, \dots; W_1, W_2, \dots]$. Suppose that $f(X)$ satisfies a functional equation of the form

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

with $g(X) \in \mathbf{Z}_{(p)}[V_1, V_2, \dots; W_1, W_2, \dots]$, i.e. $f(X) - \sum_{i=1}^{\infty} p^{-1} V_i f^{(p^i)}(X^{p^i})$ is integral with respect to p.

3.2. Lemma. *Let $f(X) = X + b_2X^2 + \dots$ be as in* 3.1. *Then $p^{v_p(n)} b_n \in \mathbf{Z}_{(p)}[V, W]$, where $v_p(n)$ is the highest integer r such that $p^r \mid n$.*

Proof. Obvious from formula (3.1.1).

3.3. Lemma. *Let $f(X)$ be as in* 3.1 *and let $F(X, Y) = f^{-1}(f(X) + f(Y))$. Then $F(X, Y) \in \mathbf{Z}_{(p)}[V, W][[X, Y]]$.*

Proof. We shall work in $\mathbf{Q}[V, W][[X, Y]]$. The expression

$$G \equiv H \bmod(p^r, \text{degree } n)$$

means that $G - H \in p^r\mathbf{Z}_{(p)}[V, W][[X, Y]]$ modulo terms of total degree $\geq n$ (in X, Y).

Let

$$F(X, Y) = F_1 + F_2 + \dots$$

where F_i is homogeneous of degree i (in X, Y). Then

$$F_1 = X + Y \in \mathbf{Z}_{(p)}[V, W][[X, Y]].$$

Suppose we have already proved that

$$(3.3.1) \qquad F_1, F_2, \dots, F_n \in \mathbf{Z}_{(p)}[V, W][[X, Y]].$$

It is clear that if $s \geq 2$

$$(3.3.2) \qquad (F(X, Y))^s \equiv (F_1 + \dots + F_n)^s \bmod (\text{degree } n + 2).$$

Now if $H(X, Y)$ is in $\mathbf{Z}_{(p)}[V, W][[X, Y]]$ one has that

$$(3.3.3) \qquad H(X, Y)^{p^k} \equiv H^{(p^k)}(X^{p^k}, Y^{p^k}) \bmod(p)$$

and hence

$$(3.3.4) \qquad H(X, Y)^{p^k m} \equiv (H^{(p^k)}(X^{p^k}, Y^{p^k}))^m \bmod(p^{v_p(m)+1}).$$

Combining this with (3.3.1) and (3.3.2) we see that

(3.3.5) $$F(X, Y)^{p^k m} \equiv (F^{(p^k)}(X^{p^k}, Y^{p^k}))^m \bmod(p^{v_p(m)+1}, \text{degree } n+2).$$

Now by definition we have

(3.3.6) $$f(F(X, Y)) = f(X) + f(Y)$$

and therefore according to (3.1.1)

(3.3.7) $$\begin{aligned} g(F(X, Y)) + \sum_{i=1}^{\infty} \frac{V_i}{p} f^{(p^i)}(F(X, Y)^{p^i}) = \\ = g(X) + \sum_{i=1}^{\infty} \frac{V_i}{p} f^{(p^i)}(X^{p^i}) + g(Y) + \sum_{i=1}^{\infty} \frac{V_i}{p} f^{(p^i)}(Y^{p^i}). \end{aligned}$$

By (3.3.5) and Lemma 3.2 we see that

(3.3.8) $$f^{(p^i)}(F(X, Y)^{p^i}) \equiv f^{(p^i)}(F^{(p^i)}(X^{p^i}, Y^{p^i})) \bmod(p, \text{degree } n+2).$$

It follows from (3.3.6) that

(3.3.9) $$f^{(p^i)}(F^{(p^i)}(X, Y)) = f^{(p^i)}(X) + f^{(p^i)}(Y).$$

Using (3.3.8) and (3.3.9) in (3.3.7) we conclude that

(3.3.10) $$g(F(X, Y)) \equiv g(X) + g(Y) \bmod(1, \text{degree } n+2).$$

And it follows that F_{n+1} is also in $\mathbf{Z}_{(p)}[V, W][[X, Y]]$ because $g(X)$ is of the form $g(X) = X + \ldots$. □

3.4. Proof of the integrality Theorem 2.3. It is now easy to prove 2.3. Indeed, it is obvious from the defining equations (2.2.1), (2.2.2), (2.2.3) that the only denominators which occur in $f_V(X)$, $f_{V,T}(X)$ and $f_S(X)$ are powers of p. Hence the only denominators which occur in $f_V^{-1}(X)$, $f_{V,T}^{-1}(X)$, $f_S^{-1}(X)$ and $F_V(X, Y)$, $F_{V,T}(X, Y)$, $F_S(X, Y)$ are powers of p. It now suffices to apply Lemma 3.3.

4. Some formulae

For various reasons it is useful to have some explicit formulae and congruences available.

4.1. Formulae for f_V, $f_{V,T}$ and f_S. The "functional equations" (2.2.1), (2.2.2) and (2.2.3) define the power series f_V, $f_{V,T}$ and f_S recursively. Writing

(4.1.1) $$f_V(X) = \sum_{i=0}^{\infty} a_i(V)X^{p^i}, \qquad f_{V,T}(X) = \sum_{i=0}^{\infty} a_i(V, T)X^{p^i},$$
$$f_S(X) = \sum_{i=1}^{\infty} b_i(S)X^i$$

it is not difficult to prove that the following formulae hold:

(4.1.2) $$a_n(V) = \sum_{i_1+\ldots+i_r=n} \frac{V_{i_1} V_{i_2}^{p^{i_1}} \ldots V_{i_r}^{p^{i_1+\ldots+i_{r-1}}}}{p^r}, \qquad a_0(V) = 1$$

where the sum is over all sequences $(i_1, \ldots, i_r)$, $i_j \in \mathbf{N} = \{1, 2, 3, \ldots\}$, $r \geq 1$, such that $i_1 + \ldots + i_r = n$;

(4.1.3) $$a_n(V, T) = \sum_{i_1+\ldots+i_r=n} \frac{V_{i_1} V_{i_2}^{p^{i_1}} \ldots V_{i_r}^{p^{i_1+\ldots+i_{r-1}}}}{p^r} + \sum_{i_1+\ldots+i_r=n} \frac{V_{i_1} V_{i_2}^{p^{i_1}} \ldots V_{i_{r-1}}^{p^{i_1+\ldots+i_{r-2}}}}{p^{r-1}} T_{i_r}^{p^{i_1+\ldots+i_{r-1}}},$$

$$a_0(V, T) = 1,$$

(4.1.4) $$b_n(S) = \sum_{(q_1,\ldots,q_r,d)} \frac{S_{q_1} S_{q_2}^{q_1} \ldots S_{q_r}^{q_1\cdots q_{r-1}}}{p^r} S_d^{q_1\cdots q_r}, \qquad S_1 = 1, \quad b_1(S) = 1$$

where the sum is over all sequences $(q_1, \ldots, q_r, d)$ such that q_i is a power of p, $q_i = p^{r_i}$, $r_i \in \mathbf{N}$; $r \geq 0$; $d \in \mathbf{N}$ and not a power of p and $q_1 \ldots q_r d = n$. Note that $d = 1$ is allowed and also $r = 0$.

4.2. Examples. The first few $a_n(V)$, $a_n(V, T)$, $b_n(S)$ look as follows:

(4.2.1) $$a_0(V) = 1, \qquad a_1(V) = \frac{V_1}{p}, \qquad a_2(V) = \frac{V_1 V_1^p}{p^2} + \frac{V_2}{p},$$

$$a_3(V) = \frac{V_1 V_1^p V_1^{p^2}}{p^3} + \frac{V_1 V_2^p}{p^2} + \frac{V_2 V_1^{p^2}}{p^2} + \frac{V_3}{p};$$

$$a_0(V, T) = 1, \quad a_1(V, T) = \frac{V_1}{p} + T_1, \quad a_2(V, T) = \frac{V_1 V_1^p}{p^2} + \frac{V_1 T_1^p}{p} + \frac{V_2}{p} + T_2,$$

(4.2.2) $$a_3(V, T) = \frac{V_1 V_1^p V_1^{p^2}}{p^3} + \frac{V_1 V_1^p T_1^{p^2}}{p^2} + \frac{V_1 V_2^p}{p^2} + \frac{V_2 T_1^{p^2}}{p} + \frac{V_2 V_1^{p^2}}{p^2} + \frac{V_2 T_1^{p^2}}{p} + \frac{V_3}{p} + T_3.$$

Taking $p = 3$, the first few $b_n(S)$ are equal to

$$b_1(S) = 1, \quad b_2(S) = S_2, \quad b_3(S) = \frac{S_3}{3}, \quad b_4(S) = S_4, \quad b_5(S) = S_5,$$

(4.2.3) $$b_6(S) = \frac{S_3 S_2^3}{3} + S_6, \qquad b_9(S) = \frac{S_3 S_3^3}{9} + \frac{S_9}{3},$$

$$b_{18}(S) = \frac{S_3 S_3^3 S_2^9}{9} + \frac{S_9 S_2^9}{3} + \frac{S_3 S_6^3}{3} + S_{18}.$$

4.3. Relations between the $a_n(V)$, $a_n(V, T)$ and $b_n(S)$. The following formulae between the $a_n(V)$, $a_n(V, T)$ and $b_n(S)$ follow directly from the formulae in 4.1:

$$a_n(V) = a_{n-1}(V)\frac{V_1^{p^{n-1}}}{p} + \dots + a_1(V)\frac{V_{n-1}^p}{p} + \frac{V_n}{p}, \tag{4.3.1}$$

$$a_n(V, T) = a_n(V) + a_{n-1}(V)T_1^{p^{n-1}} + \dots + a_1(V)T_{n-1}^p + T_n. \tag{4.3.2}$$

Let us write $a_n(S)$ for the polynomial obtained from $a_n(V)$ by substituting S_{p^i} for V_i, $i = 1, 2, \dots$. Then if $n = p^r m$, $(m, p) = 1$ we have

$$\begin{aligned} &b_n(S) = a_r(S)S_m^{p^r} + a_{r-1}(S)S_{pm}^{p^{r-1}} + \dots + a_1 S^p_{p^{r-1}m} + S_{p^r m} \quad \text{if } m > 1 \\ &b_{p^r}(S) = a_r(S). \end{aligned} \tag{4.3.3}$$

4.4. Congruence formulae. For each $n \geqslant 2$ let $B_n(X, Y)$ be the polynomial

$$B_n(X, Y) = (X + Y)^n - X^n - Y^n. \tag{4.4.1}$$

Let $V(n)$, $n \geqslant 0$ be short for $V(n) = (V_1, V_2, \dots, V_n, 0, 0, 0, \dots)$ and $S(n)$, $n \geqslant 1$ for $S(n) = (S_2, \dots, S_n, 0, 0, \dots)$. Then one has directly from 4.1:

$$\begin{aligned} &F_S(X, Y) \equiv F_{S(n-1)}(X, Y) - S_n B_n(X, Y) \bmod(\text{degree } n + 1) \\ &\qquad\qquad \text{if } n \text{ not a power of } p, \\ &F_S(X, Y) \equiv F_{S(n-1)}(X, Y) - S_n(p^{-1}B_n(X, Y)) \bmod(\text{degree } n + 1) \\ &\qquad\qquad \text{if } n \text{ is a power of } p; \end{aligned} \tag{4.4.2}$$

$$F_V(X, Y) \equiv F_{V(n-1)}(X, Y) - V_n(p^{-1}B_{p^n}(X, Y)) \bmod(\text{degree } p^n + 1). \tag{4.4.3}$$

Writing $F_S(X, Y) = F_S(1) + F_S(2) + \dots$, $F_V(X, Y) = F_V(1) + F_V(2) + \dots$ where $F_S(i)$ and $F_V(i)$ are homogeneous of degree i (in X, Y) we have in particular for $n \geqslant 2$:

$$\begin{aligned} &F_S(n) \equiv -S_n B_n(X, Y) \bmod(S_2, \dots, S_{n-1}) \quad \text{if } n \text{ is not a power of } p, \\ &F_S(n) \equiv -S_n(p^{-1}B_n(X,Y)) \bmod(S_2, \dots, S_{n-1}) \quad \text{if } n \text{ is a power of } p; \end{aligned} \tag{4.4.4}$$

and if r is the smallest integer such that $p^r \geqslant n$

$$\begin{aligned} &F_V(n) \equiv 0 \bmod(V_1, \dots, V_{r-1}) \quad \text{if } n \text{ is not a power ot } p, \\ &F_V(n) \equiv -V_r(p^{-1}B_n(X, Y)) \bmod(V_1, \dots, V_{r-1}) \quad \text{if } n = p^r. \end{aligned} \tag{4.4.5}$$

5. A bit of binomial coefficient arithmetic

To prove the universality of various formal groups we shall have occasion to use the following bit of binomial coefficient arithmetic several times in this series of papers. There is nothing new about it. It is simply a restatement of Lazard's fundamental lemma for $R = \mathbf{Z}$. Cf. Fröhlich [4] p. 60. The proof is practically identical with the proof given by Fröhlich loc. cit. on pages 64, 65 for the cases $R = \mathbf{Q}$, R a field of characteristic $p > 0$.

Let $n \in \mathbf{N}$, $n \geqslant 2$. We define $\nu(n) = p$ if $n = p^r$, $r \in \mathbf{N}$, p a prime number and $\nu(n) = 1$ if n is not a prime power. Consider the binomial coefficients $\binom{n}{1}, \ldots, \binom{n}{n-1}$. Their greatest common divisor is $\nu(n)$. Hence there exist $\lambda_i \in \mathbf{Z}$ such that $\lambda_1\binom{n}{1} + \ldots + \lambda_{n-1}\binom{n}{n-1} = \nu(n)$.

5.1. Lemma. *Let $X_1, \ldots, X_{n-1}$ be indeterminates, $X_i = X_{n-i}$, $i = 1, \ldots, n-1$. Let $\lambda_1, \ldots, \lambda_{n-1}$ be integers such that $\lambda_1\binom{n}{1} + \ldots + \lambda_{n-1}\binom{n}{n-1} = \nu(n)$. Then every X_i can be written as an integral linear combination of the expressions*

(5.1.1) $\qquad \lambda_1 X_1 + \ldots + \lambda_{n-1} X_{n-1},$

(5.1.2) $\qquad \binom{i+j}{i} X_{i+j} - \binom{k+j}{j} X_{k+j}, \qquad i, j, k \geqslant 1, \qquad i + j + k = n.$

Proof. To prove this it suffices to show: (i) every X_i can be written as a rational linear combination of the expressions (5.1.1) and (5.1.2) and (ii) for every prime number p, X_i can be written modulo p as a linear combination of the expressions (5.1.1) and (5.1.2).

5.2. The rational case. Take $i = 1$; $j = 1, \ldots, n-2$; $k = n-2, \ldots, 2, 1$ in (5.1.2) to obtain the following matrix of coefficients (using $X_i = X_{n-i}$):

$$A = \begin{pmatrix} \lambda_1 & \lambda_2 & \lambda_3 & \ldots & \lambda_{n-1} \\ -\binom{n-1}{1} & \binom{2}{1} & 0 & \ldots & 0 \\ -\binom{n-1}{2} & 0 & \binom{3}{1} & \ldots & \vdots \\ \vdots & \vdots & \ldots & \ldots & 0 \\ -\binom{n-1}{n-2} & 0 & \ldots & 0 & \binom{n-1}{1} \end{pmatrix}.$$

One finds

$$\det(A) = \sum_{i=1}^{n-1} \frac{(n-1)!}{n} \binom{n}{i} \lambda_i = \frac{(n-1)!}{n} \nu(n),$$

which takes care of the rational case.

5.3. The mod p **case with** $n = p$ **or** $(n, p) = 1$. If $n = p$ or $(n, p) = 1$, then for every $i = 1, \ldots, n-1$ we have $(i, p) = 1$ or $(n - i, p) = 1$. For each $i = 1, \ldots, n-1$ let $a(i) \in \{i, n-i\}$ be such that $(a(i), p) = 1$. Using $X_i = X_{n-i}$ we can assume that $\lambda_i = 0$ if $i \neq a(i)$. We take $a(1) = 1$. Now consider the matrix of coefficients

$$A' = \begin{pmatrix} \lambda_1 & \lambda_{a(2)} & \lambda_{a(3)} & \dots & \lambda_{a(m)} \\ -\binom{n-1}{a(2)-1} & \binom{a(2)}{1} & 0 & \dots & 0 \\ -\binom{n-1}{a(3)-1} & 0 & \binom{a(3)}{1} & \dots & \vdots \\ \vdots & \vdots & \dots & \dots & 0 \\ -\binom{n-1}{a(m)-1} & 0 & \dots & 0 & \binom{a(m)}{1} \end{pmatrix}$$

where $m = \frac{1}{2}n$ if $(n, 2) = 2$ and $m = \frac{1}{2}(n-1)$ if $(n, 2) = 1$. We have

$$\det A' = \sum_{i=1}^{m} \frac{a(1)\dots a(m)}{n} \binom{n}{a(i)} \lambda_{a(i)}$$

$$= \frac{1}{n}\left(\prod_{i=1}^{m} a(i)\right) \sum_{i=1}^{m} \binom{n}{a(i)} \lambda_{a(i)} = \left(\prod_{i=1}^{m} a(i)\right) \frac{\nu(n)}{n}$$

because $\lambda_i = 0$ if $i \notin \{a(1), \dots, a(m)\}$.

We see that $\det(A') \not\equiv 0 \bmod p$ because $(a(i), p) = 1$ and either $\nu(n) = n$ or $(n, p) = 1$. This takes care of this case.

Note that for this proof to work we only need to know that $\Sigma \lambda_i \binom{n}{i} \equiv 1 \bmod p$ in case $(n, p) = 1$ and $\Sigma \lambda_i \binom{n}{i} \equiv p \bmod p^2$ if $n = p$.

5.4. The mod p **case with** $n = pm$ **and** $m > 1$. Let $n = pm$ and $m > 1$.

Taking $j = 1$ in (5.1.2) and using $X_{k+j} = X_i$ we find the expressions

$$-(pm - i)X_i + (i+1)X_{i+1}. \tag{5.4.1}$$

Taking $i = pl$ and $i + 1 = pl$ we see that mod p we can write the X_{pi-1} and X_{pi+1} as integral linear combinations of the expressions (5.1.2). And then taking $i = pi+1, \dots, pi+p-2$ and $i = pi-1, \dots, pi-p+2$ in (5.4.1) we see that modulo p all X_i with $(i, p) = 1$ can be written as linear combinations of the expressions (5.1.2).

To obtain the X_{pi}, $i = 1, \dots, m$ we use induction. The induction hypothesis is: if $\lambda_1, \dots, \lambda_{n-1}$ are such that $\Sigma \lambda_i \binom{n}{i} \equiv \nu(n) \bmod p$ if $\nu(n) \neq p$ and $\Sigma \lambda_i \binom{n}{i} \equiv p \bmod p^2$ if $\nu(n) = p$ then each X_i can be written modulo p as a linear combination of the expressions (5.1.1) and (5.1.2). The induction starts because of 5.3.

Let Y, Z be indeterminates. We have

$$(Y^p + Z^p)^m \equiv (Y + Z)^{pm} \bmod p, \quad (Y^p + Z^p)^{p^r} \equiv (Y + Z)^{p^{r+1}} \bmod p^2.$$

It follows that

$$\binom{n}{pi} = \binom{pm}{pi} \equiv \binom{m}{i} \bmod p, \binom{p^{r+1}}{pi} \equiv \binom{p^r}{i} \bmod p^2 \qquad \text{if } r \geq 1,$$

$$\binom{n}{i} = \binom{pm}{i} \equiv 0 \bmod p \text{ if } (i, p) = 1, \binom{p^{r+1}}{i} \equiv 0 \bmod p^2 \quad \text{if } r \geq 1 \text{ and } (p, i) = 1.$$

Hence

$$\nu(n) = \sum_{i=1}^{n-1} \lambda_i \binom{n}{i} \equiv \sum_{i=1}^{m-1} \lambda_{ip} \binom{m}{i} \bmod p \quad \text{if } n \text{ is not a power of } p,$$

$$p = \sum_{i=1}^{n-1} \lambda_i \binom{n}{i} \equiv \sum_{i=1}^{m-1} \lambda_{ip} \binom{m}{i} \bmod p^2 \quad \text{if } n = p^{r+2},\ r \geq 1.$$

By induction it follows that we can write the X_{pi} modulo p as linear combinations of the expressions (5.1.2) with $p \mid i$, $p \mid j$, $p \mid k$ and the expression $\nu(m)\nu(n)^{-1}(\lambda_p X_p + \ldots + \lambda_{n-p} X_{n-p})$ (resp. $(\lambda_p X_p + \ldots + \lambda_{n-p} X_{n-p})$) if $\nu(n) \neq p$ (resp. $\nu(n) = p$). This concludes the proof because $\nu(n) \not\equiv 0 \bmod p$ if $\nu(n) \neq p$ and because we have already shown that the X_i with $(i, p) = 1$ can modulo p be written as linear combinations of the (5.1.2).

6. The universality theorems

We are now in a position to prove some universality theorems. The proof of Theorem 2.5 follows the proof given in [1] by Buhštaber and Novikov slightly adapted from the topological case to our algebraic setting. In both cases one has a good candidate for being a universal formal group and in both cases one knows enough about this formal group to be able to dispense with practially all of Lazard's difficult comparison lemma (wich now appears as a corollary) except for the bit of binomial coefficient arithmetic which was discussed in Section 5. We first need a lemma.

6.1. For each $n \in \mathbf{N}$ choose $\lambda_{i,n} \in \mathbf{Z}$, $i = 1, \ldots, n-1$ such that

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

Now let

(6.1.2) $$F_S(X, Y) = X + Y + \sum_{i,j \geq 1} e_{ij} X^i Y^j, \qquad e_{i,j} \in \mathbf{Z}[S]$$

and let

(6.1.3) $$y_n = \sum_{i=1}^{n-1} \lambda_{i,n} e_{i,n-i}, \qquad n = 2, 3, \ldots .$$

Lemma. *The y_n are a set of polynomial generators for $\mathbf{Z}_{(p)}[S_2, S_3, \ldots]$.*

I.e. every element of $\mathbf{Z}_{(p)}[S_2, S_3, \ldots]$ can be written uniquely as a polynomial in the y_n, $n \geq 2$ with coefficients in $\mathbf{Z}_{(p)}$.

Proof. Immediate from (4.4.4).

6.2. Proof of Theorem 2.5. (Universality of $F_S(X, Y)$ for formal groups over $\mathbf{Z}_{(p)}$-algebras.) Let A be a $\mathbf{Z}_{(p)}$-algebra and let

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

be a formal group over A. Let $\lambda_{i,n}$ and y_n be as in 6.1. Now define

(6.2.2) $$\phi : \mathbf{Z}_{(p)}[S] \to A, \qquad \phi(y_n) = \sum_{i=1}^{n-1} \lambda_{i,n}a_{i,n-i}.$$

This is a well defined homomorphism because of Lemma 6.1. It is also certainly the only possible homomorphism such that $F^\phi(X, Y) = G(X, Y)$, because such a homomorphism must take $e_{i,j}$ into $a_{i,j}$. This takes care of uniqueness. So it remains to prove that $\phi(e_{i,j}) = a_{i,j}$ for all $i, j \geq 1$. We have $\phi(e_{1,1}) = a_{1,1}$ because $y_1 = e_{1,1}$. So with induction we can assume that $\phi(e_{i,j}) = a_{i,j}$ for $i + j < n$.

Commutativity and associativity of G and F_S mean that certain universal relations must hold between the coefficients $a_{i,j}$, $e_{i,j}$. These are of the form

$$a_{i,n-i} = a_{n-i,i}, \qquad e_{i,n-i} = e_{n-i,i}, \qquad i = 1, \ldots, n-1$$

(6.2.3) $$\binom{i+j}{i} a_{i+j,k} - \binom{j+k}{j} a_{j+k,i} = P_{ijk}(a_{m,l}), \qquad i, j, k \geq 1,\ i + j + k = n$$

$$\binom{i+j}{i} e_{i+j,k} - \binom{j+k}{j} e_{j+k,i} = P_{ijk}(e_{m,l}), \qquad i, j, k \geq 1,\ i + j + k = n$$

where P_{ijk} is a polynomial in the $a_{m,l}$ (resp. $e_{m,l}$) with $m + l < n$. Now apply Lemma 5.1 to conclude that $\phi(e_{i+j,k}) = a_{i+j,k}$ for all $i, j, k \geq 1$, $i + j + k = n$.

We have now proved that $F_S^\wedge(X, Y)$ over $\mathbf{Z}_{(p)}[S]$ is universal for formal groups over $\mathbf{Z}_{(p)}$-algebra. It follows that $F_S(X, Y)$ over $\mathbf{Z}[S]$ is also universal because there is a one–one correspondence between homomorphisms $\mathbf{Z}_{(p)}[S] \to A$ and homomorphisms $\mathbf{Z}[S] \to A$ if A is a $\mathbf{Z}_{(p)}$-algebra. ☐

6.3. Corollary. *Let $F(X, Y)$ and $G(X, Y)$ be two formal groups over a $\mathbf{Z}_{(p)}$-algebra A such that $F(X, Y) \equiv G(X, Y)$* mod(degree n). *Then there is an $a \in A$ such that*

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

This is Lazard's comparison lemma. (Cf. [10].) Of course it holds for all rings A, not just for $\mathbf{Z}_{(p)}$-algebras. To prove it for all rings A in the way we have done it for $\mathbf{Z}_{(p)}$-algebras requires first the construction of a (globally) universal formal group. This will be done in part II of this series of papers [8].

6.4. p-typical formal groups. Let A be a characteristic zero ring. We define this as a ring A such that $n \in \mathbf{Z}$, $a \in A$ and $na = 0$ implies $n = 0$ or $a = 0$. The natural homomorphism $A \to A \otimes_{\mathbf{Z}} \mathbf{Q}$ is then injective. Let $F(X, Y)$ be a formal group over A and let $f(X) = X + b_2X^2 + \ldots$ be a power series with coefficients in $A \otimes_{\mathbf{Z}} \mathbf{Q}$ such that $F(X, Y)=f^{-1}(f(X)+f(Y))$. Then $F(X, Y)$ is p-typical iff $f(X)$ is of the form $f(X)=X+b_pX^p+b_{p^2}X^{p^2}+\dots$. Indeed we have

$$f(\mathbf{f}_q\gamma_0(X))=f(Z_1X^{1/q})+f(Z_2X^{1/q})+\dots+f(Z_qX^{1/q})$$

from which the result readily follows.

6.5. To prove Theorem 2.8 (p-typical universality of $F_V(X, Y)$) we need a lemma.

Lemma. *Let $F(X, Y)$ be two p-typical formal groups over a ring A which is of characteristic zero or a $Z_{(p)}$-algebra. Suppose that*

(6.5.1) $\qquad F(X, Y)\equiv G(X, Y)\ \mathrm{mod}(\text{degree } p^r+1), \qquad r\geq 0$

then

(6.5.2) $\qquad F(X, Y)\equiv G(X, Y)\ \mathrm{mod}(\text{degree } p^{r+1})$.

To prove this lemma for all rings A we need the comparison lemma for all rings A, which we have not yet proved. So the proof of this lemma and also of Theorem 2.8 which depends on this lemma still has a gap. This gap will be filled in [8].

Proof of the lemma. We use induction. Suppose we have already proved that $F(X, Y)\equiv G(X, Y)\ \mathrm{mod}(\text{degree } m)$, $p^{r+1}>m\geq p^r+1$. Then by the comparison lemma we have

(6.5.3) $\qquad F(X, Y)\equiv G(X, Y)+a(\nu(m)^{-1}B_m(X, Y))\ \mathrm{mod}(\text{degree } m+1)$

for a certain $a\in A$. Let q be a prime number different from p which divides m. It follows directly from (6.5.3) that

$$\begin{aligned}&\gamma_0(Z_1X^{1/q})+_F\dots+_F\gamma_0(Z_qX^{1/q})\\ (6.5.4)\qquad &\equiv\gamma_0(Z_1X^{1/q})+_G\dots+_G\gamma_0(Z_qX^{1/q})\\ &\quad+a(\nu(m)^{-1}[(Z_1X^{1/q}+\dots+Z_qX^{1/q})^m-Z_1^mX^{m/q}-\dots-Z_q^mX^{m/q}])\end{aligned}$$

where the congruence is mod(degree $m+1$). Now if $\tau_n=Z_1^n+\dots+Z_q^n$ and σ_i is the i-th elementary symmetric function in the Z_i we have

$$\begin{aligned}&\tau_m=\sigma_1\tau_{m-1}-\sigma_2\tau_{m-2}+\dots+(-1)^{q-1}\sigma_q\tau_{m-q}\quad \text{if } m>q\\ (6.5.5)\qquad &\\ &\tau_q=\sigma_1\tau_{q-1}-\sigma_2\tau_{q-2}+\dots+(-1)^{q-1}\sigma_q q.\end{aligned}$$

It follows from (6.5.4) and (6.5.5) that

(6.5.6) $\qquad \mathbf{f}_q^F\gamma_0(X)\equiv\mathbf{f}^G\gamma_0(Y)+(\nu(m)^{-1}q)aX^{m/q}\ \mathrm{mod}(\text{degree } m+1)$.

On the other hand because $F(X, Y)$ and $G(X, Y)$ are p-typical we know that $\mathbf{f}_q^F\gamma_0(X)=\mathbf{f}_q^G\gamma_0(X)=0$. Therefore

(6.5.7) $\qquad (\nu(m)^{-1}q)a=0$

for all prime numbers q different from p dividing m. If m is a power of q then (6.5.7) says that $a = 0$ and if m is not a power of a prime different from p then $\nu(m) = 1$ and there is a prime number $q_1 \neq p$ such that $q_1 a = 0$. It follows that $a = 0$ because A is a $Z_{(p)}$-algebra or of characteristic zero. □

6.6. Proof of Theorem 2.8 (p-typical universality of $F_V(X, Y)$). First of all $F_V(X, Y)$ is a p-typical formal group, because of 6.4. Now let $G(X, Y)$ be a p-typical formal group over a ring A. Suppose we have already constructed $\phi_r : \mathbf{Z}[V] \to A$, $r \geq 0$ such that

$$F_V^{\phi_r}(X, Y) \equiv G(X, Y) \bmod(\text{degree } p^r + 1) \tag{6.6.1}$$

(the case $r = 0$ is trivial, take $\phi_0(V_i) = 0$, $i = 1, 2, \ldots$) and suppose we have proved that such a ϕ_r is uniquely determined on the subring $\mathbf{Z}[V_1, \ldots, V_r]$ of $\mathbf{Z}[V]$ by (6.6.1). Because $F_V^{\phi_r}(X, Y)$ and $G(X, Y)$ are both p-typical formal groups it follows from (6.6.1) and the comparison Lemma 6.3 that

$$F_V^{\phi_r}(X, Y) \equiv G(X, Y) + a(p^{-1}B_{p^{r+1}}(X, Y)) \bmod(\text{degree } p^{r+1} + 1) \tag{6.6.2}$$

for a certain $a \in A$. Now define ϕ_{r+1} as follows, $\phi_{r+1}(V_i) = \phi_r(V_i)$ for $i \leq r$, $\phi_{r+1}(V_{r+1}) = -a$, $\phi_{r+1}(V_i) = 0$ if $i > r + 1$. Then because of (4.4.3) we have

$$F_V^{\phi_{r+1}}(X, Y) \equiv G(X, Y) \bmod(\text{degree } p^{r+1} + 1) \tag{6.6.3}$$

and it is also clear that ϕ_{r+1} is uniquely determined on $\mathbf{Z}[V_1, \ldots, V_{r+1}]$ by (6.6.3). □

7. Isomorphisms

In this section we first want to prove Theorem 2.10. Now to prove that the formal groups $F_V^{\lambda\kappa}(X, Y)$ and $F_S^{\lambda}(X, Y)$ and that the formal groups $F_V^{\lambda\iota}(X, Y)$ and $F_{V,T}^{\lambda}$ are strictly isomorphic can be done in the standard way by constructing the isomorphism step by step using the comparison lemma to calculate the next coefficient at each stage. Here λ is the appropriate localization map $A \to A \otimes_{\mathbf{Z}} \mathbf{Z}_{(p)}$.

It then follows that $F_V^{\kappa}(X, Y)$ and $F_S(X, Y)$, and $F_V^{\iota}(X, Y)$ and $F_{V,T}(X, Y)$, are also isomorphic.

Another proof uses what I like to call the functional equation lemma (cf. 7.1 below). This proof gives directly that the pairs of formal groups $F_V^{\kappa}(X, Y)$ and $F_S(X, Y)$, and $F_V^{\iota}(X, Y)$ and $F_{V,T}(X, Y)$ are isomorphic. Later we shall also find this lemma useful or at least suggestive in the construction of a global universal formal group (cf. [8]).

7.1. Functional equation lemma. (i) Let $f_i(X)$, $i = 1, 2$ be a power series over $\mathbf{Q}[V; W]$ of the form $f_i(X) = X + \ldots$ such that

$$f_i(X) = g_i(X) + \sum_{n=1}^{\infty} \frac{V_n}{p} f_i^{(p^n)}(X^{p^n}), \qquad i = 1, 2 \tag{7.1.1}$$

with $g_1(X) \in \mathbf{Z}[V; W][[X]]$ and $g_2(X) \in \mathbf{Z}_{(p)}[V; W][[X]]$. Let $h_1(X)$ and $h_2(X)$ be power series of the form $h_i(X) = X + \ldots$ over $\mathbf{Z}[V; W]$, respectively $\mathbf{Z}_{(p)}[V; W]$, and let $\bar{f}_i(X) = f_i(h_i(X))$. Then one has

$$(7.1.2) \qquad \bar{f}_i(X) = \bar{g}_i(X) + \sum_{n=1}^{\infty} \frac{V_n}{p} \bar{f}_i^{(p^n)}(X^{p^n}), \qquad i = 1, 2$$

with $\bar{g}_1(X) \in \mathbf{Z}[V; W][[X]]$ and $\bar{g}_2(X) \in \mathbf{Z}_{(p)}[V; W][[X]]$.

(ii) Inversely, suppose we have power series $f_i(X)$, $\bar{f}_i(X)$, $i = 1, 2$ of the form $f_i(X) = X + \ldots$, $\bar{f}_i(X) = X + \ldots$ such that (7.1.2) and (7.1.1) hold with $g_1(X)$, $\bar{g}_1(X) \in \mathbf{Z}[V; W][[X]]$ and $g_2(X)$, $\bar{g}_2(X) \in \mathbf{Z}_{(p)}[V; W][[X]]$ then there exist power series $h_1(X)$ (resp. $h_2(X)$) of the form $h_i(X) = X + \ldots$ with coefficients in $\mathbf{Z}[V; W]$ (resp. $\mathbf{Z}_{(p)}[V; W]$) such that $\bar{f}_i(X) = f_i(h_i(X))$.

In other words, if a power series $f(X)$ satisfies a functional equation of type (7.1.1) then all power series obtained by a strict substitution satisfy the same kind of functional equation, and inversely if two power series both satisfy a functional equation of type (7.1.1) then they are strict substitutes of one another.

N.B. It is not true in general that $\bar{g}_i(X) = g_i(h_i(X))$.

7.2. Proof of part (i) of the functional equation lemma. It is obvious that the only denominators occurring in $f_1(X)$ and $\bar{f}_1(X)$ are powers of p. Therefore the only denominators occurring in

$$\bar{f}_1(X) - \sum_{n=1}^{\infty} \frac{V_n}{p} \bar{f}_1^{(p^n)}(X^{p^n})$$

are powers of p. It suffices therefore to prove (7.1.2) for the case $i = 2$.

Precisely as in the proof of Lemma 3.3 we have that

$$h_2(X)^{p^n} \equiv h_2^{(p^n)}(X^{p^n}) \bmod(p)$$

and

$$f_2^{(p^n)}(h_2(X)^{p^n}) \equiv f_2^{(p^n)}(h_2^{(p^n)}(X^{p^n})) \bmod(p).$$

It follows that we have mod 1 that

$$\bar{f}_2(X) = f_2(h_2(X)) = g_2(h_2(X)) + \sum_{n=1}^{\infty} \frac{V_n}{p} f_2^{(p^n)}(h_2(X)^{p^n})$$

$$\equiv \sum_{n=1}^{\infty} \frac{V_n}{p} f_2^{(p^n)}(h_2^{(p^n)}(X^{p^n})) = \sum_{n=1}^{\infty} \frac{V_n}{p} \bar{f}_2^{(p^n)}(X^{p^n}).$$

7.3. Proof of part (ii) of the functional equation lemma. If there exits a $h_1(X)$ such that $\bar{f}_1(X) = f_1(h_1(X))$ then it is equal to $f_1^{-1}(\bar{f}_1(X))$. So because the only denominators occurring in $f_1(X)$ and $\bar{f}_1(X)$ are powers of p, it suffices to prove the case $i = 2$. Let $h_2(X) = f_2^{-1}(\bar{f}_2(X))$. Write $h_2(X) = X + b_2X^2 + \ldots$ and suppose we have already proved that $b_i \in \mathbf{Z}_{(p)}[V, W]$ for $i \leq n$. Exactly as in Lemma 3.3 one now shows that

$$f_2^{(p^n)}(h_2(X)^{p^n}) \equiv f_2^{(p^n)}(h_2^{(p^n)}(X^{p^n})) \operatorname{mod}(p, \text{degree } n+2).$$

It follows that we have mod (1, degree $n+2$)

$$g_2(h_2(X)) = f_2(h_2(X)) - \sum \frac{V_n}{p} f_2^{(p^n)}(h_2(X)^{p^n})$$

$$\equiv f_2(h_2(X)) - \sum \frac{V_n}{p} f_2^{(p^n)}(h_2^{(p^n)}(X^{p^n}))$$

$$= \bar{f}_2(X) - \sum \frac{V_n}{p} \bar{f}_2^{(p^n)}(X^{p^n}) = \bar{g}_2(X) \equiv 0$$

which shows that b_{n+1} is integral because $g_2(X)$ is of the form $g_2(X) = X + \dots$. □

7.4. Proof of Theorem 2.10. Apply part (ii) of the functional equation lemma to $f_S(X)$ and $f_V^\kappa(X)$, and $f_{V,T}(X)$ and $f_V^\iota(X)$.

7.5. Corollary. *Every formal group over $\mathbf{Z}_{(p)}$-algebra A is strictly isomorphic to a p-typical formal group over A.*

This follows directly from the isomorphism between $F_S(X, Y)$ and $F_V^\kappa(X, Y)$ and the universality of $F_S(X, Y)$ for formal groups over $\mathbf{Z}_{(p)}$-algebras. This is a universal way of making formal groups p-typical and it agrees with Cartier's formula for making formal groups p-typical (cf. [2]). This last fact is easily checked by calculating what Cartier's formula does to (the logarithm $f_S(X)$ of) $F_S(X, Y)$.

7.6. To prove Theorem 2.12 we first need a lemma similar to Lemma 6.5.

Lemma. *Let $F(X, Y)$ be a formal group over A, where A is a $\mathbf{Z}_{(p)}$-algebra or a charcteristic zero ring and let $\gamma(X)$, $\delta(X)$ be two p-typical curves for F over A. Suppose that*

(7.6.1) $\quad \gamma(X) \equiv \delta(X) \operatorname{mod}(\text{degree } p^n + 1)$

then

(7.6.2) $\quad \gamma(X) \equiv \delta(X) \operatorname{mod}(\text{degree } p^{n+1})$.

Remark. This lemma is not true for arbitrary rings A.

Proof of the lemma. We use induction. Suppose we have shown that $\gamma(X) \equiv \delta(X) \operatorname{mod}(\text{degree } m)$ where $p^{n+1} > m \geq p^n + 1$. Let q be a prime number dividing m different from p. We have $\gamma(X) \equiv \delta(X) + aX^m \operatorname{mod}(\text{degree } m+1)$ for a certain $a \in A$. It follows that $(\mathbf{f}_q\gamma)(X) \equiv (\mathbf{f}_q\delta)(X) + qaX^{m/q} \operatorname{mod}(\text{degree } (m/q)+1)$. But

$\gamma(X)$ and $\delta(X)$ are both p-typical, therefore $qa = 0$ from which it follows that $a = 0$ because A is a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring.

7.7. Proof of Theorem 2.12. (Universality of the triple $(F_V^{\cdot}(X, Y),\ \alpha_{V,T}(X),\ F_{V,T}(X, Y))$ for triples over $\mathbf{Z}_{(p)}$-algebras or characteristic zero rings.)

Let A be a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring and let $F(X, Y)$ and $G(X, Y)$ be two p-typical groups over A and $\alpha(X)$ a strict isomorphism from $F(X, Y)$ to $G(X, Y)$. Because $F_V(X, Y)$ is universal for p-typical formal groups there is a unique homomorphism $\psi : \mathbf{Z}[V] \to A$ such that $F_V^{\psi}(X, Y) = F(X, Y)$. Suppose we have already found a homomorphism $\phi_n : \mathbf{Z}[V; T] \to A$ such that

(7.7.1) $F_V^{\phi_n}(X, Y) = F(X, Y)$, i.e. ϕ_n extends ψ,

(7.7.2) $\alpha_{V,T}^{\phi_n}(X) \equiv \beta(X) \bmod \text{degree } (p^n + 1)$

and suppose we have proved that ϕ_n is unique on $\mathbf{Z}[V; T_1, \ldots, T_n] \subset \mathbf{Z}[V; T]$. Write $\alpha_n(X)$ for $\alpha_{V,T}^{\phi_n}(X)$. Now quite generally if $\beta(X)$ is a strict isomorphism from a formal group $H_1(X, Y)$ to a formal group $H_2(X, Y)$, i.e. if $\beta(H_1(X, Y)) = H_2(\beta(X), \beta(Y))$ and if $H_2(X, Y)$ is a p-typical formal group, then $\beta^{-1}(X)$ is a p-typical curve for $H_1(X, Y)$. (Very easy to check.)

Now $\beta(X)$ is a strict isomorphism from $F(X, Y)$ to $G(X, Y)$ and $\alpha_n(X)$ is a strict isomorphism from $F(X, Y)$ to $F_{V,T}^{\phi_n}(X)$, because of (7.7.1). Both $G(X, Y)$ and $F_{V,T}^{\phi_n}(X, Y)$ are p-typical formal groups. Therefore we have that

(7.7.3) $\beta^{-1}(X)$ and $\alpha_n^{-1}(X)$ are p-typical for $F(X, Y)$.

Using (7.7.2), (7.7.3) and Lemma 7.6 we see that

(7.7.4) $\alpha_{V,T}^{\phi_n}(X) \equiv \beta(X) + aX^{p^{n+1}} \bmod(\text{degree } p^{n+1} + 1)$

for a certain unique $a \in A$.

Now from (4.3.2) e.g. we see that

(7.7.5) $f_{V,T}(X) \equiv f_V(X) + T_{n+1}X^{p^{n+1}} \bmod(T_1, \ldots, T_n, \text{degree } p^{n+1} + 1)$.

It follows that we have for $\alpha_{V,T}(X) = f_{V,T}^{-1}(f_V(X))$ that

(7.7.6) $\alpha_{V,T}(X) \equiv X - T_{n+1}X^{p^{n+1}} \bmod(T_1, \ldots, T_n, \text{degree } p^{n+1} + 1)$.

Now define $\phi_{n+1} : \mathbf{Z}[V; T] \to A$ by $\phi_{n+1} = \phi_n$ on $\mathbf{Z}[V; T_1, \ldots, T_n]$, $\phi_{n+1}(T_{n+1}) = -a$, $\phi_{n+1}(T_i) = 0$, $i > n + 1$. Then ϕ_{n+1} satisfies (7.7.1) and (7.7.2) with n replaced by $n + 1$ and ϕ_{n+1} is unique on $\mathbf{Z}[V; T_1, \ldots, T_{n+1}]$. Both, because of (7.7.6) and (7.7.4). □

7.8. Remark. The triple $(F_V^{\cdot}(X, Y), \alpha_{V,T}(X), F_{V,T}(X, Y))$ is not universal for triples over arbitrary rings. The easiest counter example is probably the following. Take $A = \mathbf{Z}/(q)$ (q a prime number). Choose a prime number $p > q$. Let $F(X, Y) = X + Y$, $\alpha(X) = X + X^q$, $G(X, Y) = X + Y$. Both $F(X, Y)$ and $G(X, Y)$ are p-typical and $\alpha(X)$ is a strict isomorphism (over $\mathbf{Z}/(q)$!).

7.9. Let $v = (v_1, v_2, \dots)$ be a sequence of elements of a ring A. We write $F_v(X, Y)$ for the formal group $F_V^\phi(X, Y)$ where $\phi : \mathbf{Z}[V] \to A$ is the homomorphism which takes V_i into v_i, $i = 1, 2, \dots$. Every p-typical formal group over A is equal to an $F_v(X, Y)$ according to Theorem 2.8.

Corollary 1. *Let A be a $\mathbf{Z}_{(p)}$-algebra or a characteristic zero ring. The formal groups $F_v(X, Y)$, $F_{v'}(X, Y)$ are strictly isomorphic iff there exist $t_1, t_2, \dots \in A$ such that $F_{v'}(X, Y) = F_{v,t}(X, Y)$.*

Corollary 2. *Let A be a characteristic zero ring. The formal groups $F_v(X, Y)$ and $F_{v'}(X, Y)$ are strictly isomorphic iff there exist $t_1, t_2, \dots \in A$ such that*

$$a_1(v') - a_1(v) = t_1 \in A \subset A \otimes_{\mathbf{Z}} \mathbf{Q},$$

$$a_2(v') - a_1(v)t_1^p - a_2(v) = t_2 \in A,$$

$$a_3(v') - a_1(v)t_2^p - a_2(v)t_1^{p^2} - a_3(v) = t_3 \in A,$$

$$\dots\dots$$

where $a_i(v)$ (resp. $a_i(v')$) is the element of $A \otimes_{\mathbf{Z}} \mathbf{Q}$ obtained by substituting $v_1, v_2, \dots$ (resp. $v_1', v_2', \dots$) for $V_1, V_2, \dots$ in the polynomials $a_i(V)$. The $t_1, t_2, \dots$ are unique if they exist.

This follows from (4.3.2) and Theorem 2.12. The $t_1, t_2, \dots$ in Corollary 1 above need not be unique.

8. Concluding remarks

In Honda [9] the reader will find a construction for formal groups very similar to the constructions carried out here. The integrality proof is also similar. (They were found indepently however.) In Ditters [3] still other constructions can be found of similar flavour. Both Honda and Ditters work with power series $f(X) = \sum a_i X^i$ for which the a_i satisfy relations like (4.3.1) rather than with power series which satisfy a functional equation like (3.1.1). It may be of interest to remark that $f_V(X)$ seems to be the only power series which satisfies a relation like (4.3.1) *and* a functional equation like (3.1.1).

The p-typical formal groups $F_V(X, Y)$ for various p can be fitted together to yield a (global) universal (one dimensional commutative) formal group $F_U(X, Y)$. There are also more dimensional versions of $F_V(X, Y)$ and $F_U(X, Y)$. Cf. [5] and [8].

The explicit formulae (4.3.1) relating the coefficients of $f_V(X)$ and a similar formula concerning $f_U(X)$, the logarithm of the global universal formal group, can be used to find generators for the coefficient ring $\mathrm{BP}_*(pt)$ of Brown–Peterson cohomology and the coefficient ring $\mathrm{MU}_*(pt)$ of complex cobordism cohomology. Cf. [5] and [6].

:rences

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

P. Cartier, Modules associés à un Groupe Formel Commutatif, Courbes Typiques, C. R. Acad. Sci. Paris 265 (1967) A 129–132.

E.J. Ditters, Groupes Formels à un Paramètre sur **Z** et $\mathbf{Z}_p$, C.R. Acad. Sci. Paris 275 (1972) 251–254.

A. Fröhlich, Formal Groups, Lecture Notes in Mathematics 74 (Springer, 1968).

M. Hazewinkel, Constructing Formal Groups I, II, III, IV, Reports 7119, 7201, 7207, 7322, of the Econometric Institute, Erasmus Univ. Rotterdam (1971, 1972, 1973).

M. Hazewinkel, A universal formal group and complex cobordism, Bull. Amer. Math. Soc. 81, 5 (1975) 930–933.

M. Hazewinkel, A universal isomorphism for p-typical formal groups and operations in Brown–Peterson cohomology, Indagationes Math. 38, 3 (1976) 195–199.

M. Hazewinkel, Constructing formal groups II: the global one dimensional case, J. Pure Appl. Algebra 9 (1977) 151–161.

T. Honda, On the Theory of Commutative Formal Groups, J. Math. Soc. Japan 22, 2 (1970) 213–246.

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

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 $f_U(X) \in \mathbf{Z}[U_2, U_3, \ldots][[X]]$ 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

$$(1.2) \quad X + \frac{U_2}{2} X^2 + \frac{U_3}{3} X^3 + \left(\frac{U_2 U_2^2}{4} + \frac{U_4}{2}\right) X^4 + \frac{U_5}{5} X^5 + \left(\frac{U_3 U_2^3}{6} + \frac{U_2 U_3^2}{6}\right) X^6 + \ldots$$

However, it now appears that the two prime numbers 2 and 3 interfere with one another. The term $6^{-1} U_3 U_2^3$, 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 $6^{-1} U_2 U_3^2$. The solution is to insert suitable coefficients. Thus

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

(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) $$a_n(U) = $$

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

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

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

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

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

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 $n(q_1,\dots,q_s,d)$ 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. [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 $(i_1, \ldots, i_s)$, $i_j \in \mathbf{N} \setminus \{1\}$ let $n(i_1, \ldots, i_s)$ be an integer such that

(2.1.1) $\quad n(i_1, \ldots, i_s) = 1 \quad$ if $s = 1$;

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

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

Note that there are (many) numbers $n(i_1, \ldots, i_s)$ satisfying these conditions; $n(i_1, \ldots, i_s)$ 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

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

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 $i_j \in \mathbf{N}\setminus\{1\}$ 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.

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

(2.2.6) $m_k(U, T) =$

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

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

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

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 $n(i_1, \ldots, i_s)$ 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) $$f_U(X) \equiv X + \nu(n)^{-1} U_n X^n \bmod (U_2, \ldots, U_{n-1}, \text{degree } n+1),$$

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

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

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

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 $(U_2, U_3, \ldots, U_n, 0, 0, \ldots)$ 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 $U_{n+1}, U_{n+2}, \ldots$. 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 $(i_1, \ldots, i_s)$, $i_j \in \mathbf{N} \backslash \{1\}$ let

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

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

3.3. Lemma. (i) *If* $1 \neq \nu(i_1) = \nu(i_2) = \ldots = \nu(i_r) \neq \nu(i_{r+1})$, $r \leqslant s$, *then* $p^r d(i_1, \ldots, i_s) \in \mathbf{Z}$ *where* $p = \nu(i_1) = \ldots = \nu(i_r)$. *(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* $d(i_1, \ldots, i_s) \in \mathbf{Z}$.

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

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

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

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

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

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

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 $t < r$,

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

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

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 $p^{-1} U_{p^r} + c_{p^r} = p^{-1} U_{p^r} e^{(p^r)}_1 + c_{p^r}$ 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

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

Write

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

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

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

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

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

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

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 $i \in \mathbf{N} \setminus \{1\}$ let $c(p, i)$ be an integer such that

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

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

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

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 $i \in \mathbf{N} \setminus \{1\}$. 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 $n, d \in \mathbf{N} \setminus \{1\}$

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

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

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

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

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

we find

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

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

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

ural more dimensional generalization of $H_U(X,Y)$ is discussed in [4]

es

Buhštaber, S.P. Novikov, Formal Groups, Power Systems and Adams Operations, Mat. c 84 (1971) 81–118.

zewinkel, Constructing Formal Groups I: The Local One Dimensional Case, J. Pure Appl. a 9 (1977) 131–149.

:ewinkel, A Universal Formal Group and Complex Cobordism, Bull. Amer. Math. Soc. 81, 5 930–933.

:ewinkel, Constructing Formal Groups I, II, III, IV, V, Reports 7119, 7201, 7207, 7322, 7505 Econometric Institute, Erasmus University Rotterdam (1971, 1972, 1973, 1975).

zewinkel, Constructing Formal Groups III: Applications to Complex Cobordism and -Peterson Cohomology, J. Pure Appl. Algebra, to be published.

na, Witt Vectors and Complex Cobordism, Topology 13, 4 (1974) 389–394.