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 $F_\nu (X, Y)$ for $\mathbb{Z}_{(p)}$-algebras of [2] to obtain a global (one dimensional commutative) formal group.

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

\[
f_\nu (X) - \sum_{\nu_0} \frac{U_{\nu_0}}{\nu_0} f_\nu^{\nu_0}(X^{\nu_0}) \in \mathbb{Z}[U][[[X]]]
\]

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

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

(1.2)

However, it now appears that the two prime numbers 2 and 3 interfere with one another. The term $6^{-1} U_2 U_3$, which has to be there because of condition (1.1) in case $\nu = 3$, prevents (1.2) from satisfying (1.1) for $\nu = 2$, and vice versa with respect to the term $6^{-1} U_2 U_3$. The solution is to insert suitable coefficients. Thus

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

(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 \( U_\nu X^\nu \) 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:

\[
h_U(X) = \sum_{i=1} a_i(U)X^i, \quad a_1 = 1
\]

\[
a_\nu(U) = \sum_{(q_1, \ldots, q_\nu, d)} \frac{n(q_1, \ldots, q_\nu, d)}{p_1} \cdot \frac{n(q_2, \ldots, q_\nu, d)}{p_2} \cdots \frac{n(q_\nu, d)}{p_\nu} \cdot U_{q_1}U_{q_2}^2 \cdots U_{q_\nu}^{s_{q_\nu}}U_d^{s_d-q_\nu},
\]

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

\[
n(q_1, \ldots, q_\nu, d) \equiv 1 \mod p_i \quad \text{if} \quad p_1 \neq p_i.
\]

\[
n(q_1, \ldots, q_\nu, d) \equiv 0 \mod p_i \quad \text{if} \quad p_1 \neq p_i = \ldots = p_{r-1} \neq p_r,
\]

\[
n(q_1, \ldots, q_\nu, d) \equiv 0 \mod p \quad \text{if} \quad p_1 = p_2 = \ldots = p_r \neq p_{r+1}.
\]

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

If one chooses the \( n(q_1, \ldots, q_\nu, d) \) 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 \( f_U(X) = \sum m_\nu(U)X^\nu \) 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 \( m_\nu(U) \) (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 \( \mathbb{Z}[U] \)) are identical.

As in the local case (cf. [2]) using the approach of Buhštaber and Novikov [1] one
can prove directly that \( F_0(X, Y) \) 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 \((i_1, \ldots, i_s), i_j \in \mathbb{N}\setminus\{1\}\) let \( n(i_1, \ldots, i_s) \) be an integer such that

\[
(2.1.1) \quad n(i_1, \ldots, i_s) = 1 \quad \text{if } s = 1; \\
(2.1.2) \quad n(i_1, \ldots, i_s) \equiv 0 \mod p^{s-1} \quad \text{if } i_1, \ldots, i_s \text{ are powers of } p; \\
(2.1.3) \quad n(i_1, \ldots, i_s) \equiv 1 \mod p' \quad \text{if } i_1, \ldots, i_s \text{ are powers of a prime}
\]

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 \( i_s \) are powers of two different prime numbers.

2.2. Constructions. We now define the power series \( f_0(X), \tilde{f}_0(X), f_{U,T}(X) \) by the following formulae:

\[
(2.2.1) \quad f_0(X) = \sum_{k=1}^\infty m_k(U)X^k, \quad m_k(U) = 1, \\
(2.2.2) \quad \tilde{f}_0(X) = \sum_{k=1}^\infty \tilde{m}_k(U)X^k, \quad \tilde{m}_k(U) = 1, \\
(2.2.3) \quad f_{U,T}(X) = \sum_{k=1}^\infty m_k(U, T)X^k, \quad m_k(U, T) = 1
\]

where

\[
(2.2.4) \quad m_k(U) = \sum_{(i_1, \ldots, i_k) \neq \emptyset} n(i_1, \ldots, i_k) \cdot \frac{n(i_2, \ldots, i_k)}{\nu(i_2)} \cdot \frac{n(i_3, \ldots, i_k)}{\nu(i_3)} \cdots \frac{n(i_k)}{\nu(i_k)} U_{i_1}U_{i_2}U_{i_3} \cdots U_{i_k}.
\]
where \( \nu(i) = p \) if \( i \) is a power of the prime number \( p \) and \( \nu(i) = 1 \) if \( i \) is not a prime power and where the sum is over all sequences \((i_1, \ldots, i_s)\) with \( i_j \in \mathbb{N}\setminus\{1\} \) and \( s \geq 1 \) and \( i_1 \cdots i_s = k \). The numbers \( n(i_1, \ldots, i_s) \) are such that (2.1.1)-(2.1.3) hold.

\[
\bar{m}_s(U) \text{ is obtained from } m_s(U) \text{ by substituting } 0 \text{ for all } U_d
\]

with \( d > 1 \) and \( d \) not a power of a prime number.

\[
m_s(U, T) = \frac{\prod n(i_1, \ldots, i_s)}{\nu(i)} \cdots \frac{n(i_1, \ldots, i_s)}{\nu(i)} \cdots \frac{n(i_1)}{\nu(i)} \cdot U_i U_{i_2} \cdots U_{i_{s-1}}^{-1} \cdot \left(U_{i_s}^{(i_1-1)} + \nu(i_1) T_{i_1} \cdots i_s^{-1} \cdot \right).
\]

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

\[
\begin{align*}
F_U(X, Y) &= f_U(f_U(X) + f_{U, \tau}(Y)), \\
\bar{F}_U(X, Y) &= \bar{f}_U(\bar{f}_U(X) + \bar{f}_U(Y)), \\
F_{U, \tau}(X, Y) &= f_{U, \tau}(f_U(X) + f_{U, \tau}(Y)).
\end{align*}
\]

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

I.e. these power series are formal groups over \( \mathbb{Z}\{U\} \) and \( \mathbb{Z}\{U, T\} \).

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 \( \phi : \mathbb{Z}\{U\} \to A \) such that \( F_U(X, Y) = G(X, Y) \).

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

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

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

2.6. Universal isomorphism theorem. The triple \((F_U(X, Y), \alpha_{U, \tau}(X), F_{U, \tau}(X, Y))\) 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 \( \phi : \mathbb{Z}\{U, V\} \to A \) such that \( F_U(X, Y) = F(X, Y) \), \( \alpha_{U, \tau}(X) = \alpha(X) \) and \( F_{U, \tau}(X, Y) = G(X, Y) \).
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) \[ f_U(X) = X + \nu(n)^{-1}U_0X^s \mod(U_2, \ldots, U_{n-1}, \text{ degree } n+1), \]

(3.1.2) \[ f_{U,T}(X) = f_U(X) + T_0X^s \mod(T_2, \ldots, T_{n-1}, \text{ degree } n+1), \]

(3.1.3) \[ \alpha_{U,T}(X) = X - T_0X^s \mod(T_2, \ldots, T_{n-1}, \text{ degree } n+1), \]

(3.1.4) \[ f_U(X, Y) = X + Y - U_n(\nu(n)^{-1}B_n(X, Y)) \mod(U_2, \ldots, U_{n-1}, \text{ degree } n+1) \]

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) \[ f_U(X) = f_{U(n)}(X) + \nu(n + 1)^{-1}U_{n+1}X^{s+1} \mod(\text{degree } n+2), \]

(3.1.6) \[ f_{U,T}(X) = f_{U,T(n)}(X) + T_{n+1}X^{s+1} \mod(\text{degree } n+2), \]

(3.1.7) \[ \alpha_{U,T}(X) = \alpha_{U,T(n)}(X) - T_{n+1}X^{s+1} \mod(\text{degree } n+2), \]

(3.1.8) \[ F_U(X, Y) = F_{U(n)}(X, Y) - U_{n+1}(\nu(n + 1)^{-1}B_{n+1}(X, Y)) \mod(\text{degree } n+2). \]

3.2. For each sequence \((i_1, \ldots, i_s), i_j \in \mathbb{N} \setminus \{1\}\) let

(3.2.1) \[ \nu(i_1, \ldots, i_s) = \nu(i_1) \cdots \nu(i_s) = \nu(i_1) \cdots \nu(i_1) \text{ d}(i_1, \ldots, i_s) \]

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

3.3. Lemma. (i) If \( 1 \neq \nu(i_1) = \nu(i_2) = \ldots = \nu(i_r) \neq \nu(i_{s-r}) \), \( r \leq s \), then \( p^{r-1}d(i_1, \ldots, i_s) \in \mathbb{Z} \) where \( p = \nu(i_1) = \ldots = \nu(i_r) \). (If \( r = s \) then \( \nu(i_1) \neq \nu(i_{s-r}) \) is taken to be automatically fulfilled.)

(ii) If \( \nu(i_1) = 1 \) then \( d(i_1, \ldots, i_s) \in \mathbb{Z} \).

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

Case (2): \( \nu(i_1) = 1 \neq \nu(i_2) = p \). Let \( \nu(i_2) = \ldots = \nu(i_r) \neq \nu(i_{s-r}) \). Then by induction \( p^{-1}d(i_1, \ldots, i_s) \in \mathbb{Z} \) and hence \( d(i_1, \ldots, i_s) = \nu(i_1)^{-1}n(i_1, i_2, \ldots, i_s) \in \mathbb{Z} \) because \( n(i_1, i_2, \ldots, i_s) \equiv 0 \mod p^{-1} \) by (2.1.2) in this case.
Case (3): \(1 \neq \nu(i_i) = \nu(i_i)\). Then \(p^{-1}d(i_1, \ldots, i_i) \in \mathbb{Z}\) and hence
\[
p^{-1}d(i_1, \ldots, i_i) = \nu(i_i)^{-1}n(i_1, \ldots, i_i)p^{-1}d(i_1, \ldots, i_i)
= n(i_1, \ldots, i_i)p^{-1}d(i_2, \ldots, i_i) \in \mathbb{Z}.
\]

Case (4): \(1 \neq \nu(i_i) \neq \nu(i_1) \neq 1\). Let \(q = \nu(i_1) = \ldots = \nu(i_i) \neq (i_1, \ldots, i_i)\). Then by induction \(q^{-1}d(i_1, \ldots, i_i) \in \mathbb{Z}\) and hence \(pd(i_1, \ldots, i_i) = n(i_1, \ldots, i_i)d(i_2, \ldots, i_i) \in \mathbb{Z}\) because by (2.1.2) \(n(i_1, i_2, \ldots, i_i) = 0 \mod q^{-1}\) in this case.

\[\square\]

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

Proof. We distinguish three cases

Case (1): \(\nu(i_i) = 1\). Then \(d(i_1, \ldots, i_i) \in \mathbb{Z}\) by Lemma 3.3 and hence
\[
d(i_1, \ldots, i_i) - p^{-1}d(i_2, \ldots, i_i) = p^{-1}(n(i_1, \ldots, i_i) - 1)d(i_2, \ldots, i_i) \in \mathbb{Z}
\]
because \(n(i_1, \ldots, i_i) = 1 \mod p\) in this case by (2.1.3).

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

Case (3): \(\nu(i_i) = p\). Let \(\nu(i_i) = \nu(i_1) = \ldots = \nu(i_i) \neq \nu(i_1, \ldots, i_i)\). Then \(p^{-1}d(i_1, \ldots, i_i) \in \mathbb{Z}\) and hence
\[
d(i_1, \ldots, i_i) - p^{-1}d(i_2, \ldots, i_i) = p^{-1}(n(i_1, \ldots, i_i) - 1)d(i_2, \ldots, i_i) \in \mathbb{Z}
\]
because according to (2.1.3) \(n(i_1, \ldots, i_i) = 1 \mod p\) in this case.

\[\square\]

4. Proof of the integrality theorems

4.1. For each \(k \geq 2\), let \(c_k\) be an element of \(\mathbb{Z}[U; T]\) and for each \(i \in \mathbb{N}\) let \(c_i\) be the polynomial obtained from \(c_k\) by replacing each \(U_i\) and \(T_i\) by their \(i\)-th powers \(U_i^i\) and \(T_i^i\). We define
\[
(4.1.1) \quad g(X) = \sum_{i=1}^{k} e_iX_i^i, \quad e_i = 1,
\]
(4.1.2) \[
e_i = \sum_{(i, \ldots, i_i)} d(i_1, \ldots, i_i)U_1U_1^{i_1} \cdots U_kU_k^{i_k} + (U_1^{i_1} \cdots U_k^{i_k} + \nu(i_i)c_i^{i_1 \cdots i_k})
\]
where the sum is over all \((i_1, \ldots, i_k)\) such that \(i_1, \ldots, i_k = i, i_i \in \mathbb{N} \setminus \{1\}\), and \(d(i_1, \ldots, i_k)\) is as in (3.2)

4.2. Lemma. For all prime numbers \(p\) we have that
\[
(4.2.1) \quad g(X) - \sum_{k=1}^{\infty} \frac{U_k}{p} \left(\frac{g^{p^k}(X^{p^k})}{p^k}\right) \in \mathbb{Z}_{(p)}[U; T][[X]].
\]

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 \(\mathbb{Z}_{(p)}[U; T]\) by Lemma 3.3. Now suppose \((p, n) > 1\) and let \(n = p^i\), \((p, i) = 1\). The coefficient of \(X^n\) in (4.2.1) is then equal to
\[ e_{\nu' \cdot \frac{U_p}{p}} = \frac{U_p}{p} e_{p^{\nu(i_1)} - \ldots - \frac{U_p}{p} e_{p^{\nu(i)}}}. \]

For the terms of \( e_{\nu(i)} \) with \( \nu(i) \neq p \) we have that \( d(i, \ldots, i) \in \mathbb{Z}_{(p)} \). It remains to deal with the terms with \( i_1 = p, p^2, \ldots, p' \). We have, if \( i > 1 \) or \( t < r \),

\[
\sum_{i_1 = p'} d(i_1, \ldots, i) U_{i_1} \ldots U_{i_r} \cdot \frac{U_p}{p} e_{p^{\nu(i)}} = \sum_{i_1 = p'} \frac{U_p}{p} n(i_1, \ldots, i) U_{i_1} \ldots U_{i_r} \cdot \frac{U_p}{p} e_{p^{\nu(i)}} + \nu(i) c_{(i)}^{(i)}.
\]

And because of Lemma 3.4 we see that the part of \( e_{\nu(i)} \) with \( i_1 = p' \) minus \( p^{-1} U_p e_{p^{\nu(i)}} \) is in \( \mathbb{Z}_{(p)} U, T \) if \( i > 1 \) or \( t < r \).

And if \( i = 1, t = r \) we have that the part of \( e_{\nu(i)} \) with \( i_1 = p' \) is equal to \( p^{-1} U_p + c_{p'} = p^{-1} U_p e^{p^{\nu(i)}} + c_{p'} \) and \( c_{p'} \in \mathbb{Z}[U; T] \). So we see that (4.2.2) is in \( \mathbb{Z}_{(p)} U; T \).

4.3. Proof of the integrality theorem 2.3 (parts (i) and (iii)). Taking \( c_k = 0 \) for all \( k > 2 \) we get \( g(X) = f_{t_1}(X) \). Hence \( f_{t_1} \) satisfies a functional equation (4.2.1), and we can apply [2, 3.3] to conclude that \( F_U(X, Y) \in \mathbb{Z}_{(p)} U[[X]] \) for all prime numbers \( p \), hence \( F_U(X, Y) \in \mathbb{Z}[U][[X, Y]] \).

Taking \( c_k = T_k \), \( k = 2, 3, \ldots \) we find \( g(U) = f_{U, -1}(X) \) and the same argument gives that \( F_{U, -1}(X, Y) \in \mathbb{Z}[U; T][[X, Y]] \).

4.4. Proof of the integrality theorem 2.3 (part (ii)). \( \tilde{F}_U(X, Y) \) is obtained from \( F_U(X, Y) \) by substituting \( 0 \) for all \( U_\lambda \) with \( \lambda \) not a power of a prime number. So \( \tilde{F}_U(X, Y) \) is integral because \( F_U(X, Y) \) is integral. (One can also show that \( f_U(X) \) 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 \( F_0(X, Y) \) in [2].

5.1. For each \( n \in \mathbb{N}\setminus\{1\} \) we have that g.c.d. \((\ell_1, \ldots, \ell_n)) = \nu(n). \) Choose \( \lambda_{n, i} \in \mathbb{Z} \) such that

\[
\lambda_{n, 1} \left( \binom{n}{1} \right) + \ldots + \lambda_{n, n-1} \left( \binom{n}{n-1} \right) = \nu(n).
\]

Write

\[
F_{U_0}(X, Y) = X + Y + \sum_{i \not\equiv 1} e_{i} X^i Y^i
\]

and define
(5.1.3) \[ y_n = \sum_{i=1}^N \lambda_n, e_{i,n} \ldots. \]

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

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

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) \[ G(X, Y) = X + Y + \sum_{i,j=1} a_{ij}X^iY^j. \]

Now define \( \phi : \mathbb{Z}[U] \rightarrow A \) by the requirement \( \phi(y_n) = \sum_{i=1}^{\infty} \lambda_n, a_{i,n} \ldots. \) This is a well defined homomorphism because of Lemma 5.2. Further if \( \psi \) is a homomorphism \( \mathbb{Z}[U] \rightarrow A \) such that \( F^\psi(X, Y) = G(X, Y) \) then we have \( \psi(e_n) = a_n \) and hence \( \psi(y_n) = \phi(y_n) \). This takes care of uniqueness. One now proves that \( \phi(e_n) = a_n \) exactly as in [2, 6.2]. \( \square \)

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) \[ F(X, Y) = G(X, Y) \mod (\text{degree } n). \]

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

(5.4.2) \[ F(X, Y) = G(X, Y) + a(n(\nu(n))^{-1}B_n(X, Y)) \mod (\text{degree } n + 1). \]

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 \( \mathbb{Z}[U; T] \) with logarithms \( f(X), g(X) \in \mathbb{Q}[U; T][[X]] \); 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 \( g^{-1}(f(X)) \in \mathbb{Z}[U; T][[X]] \) and this is the case if and only if \( f^{-1}(f(X)) \in \mathbb{Z}[U; T][[X]] \) for all prime numbers \( p \).

The power series \( f_{i,t}(X), f_{i,t}(X), f_{u,r}(X) \) 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 \(\psi: \mathbb{Z}[U] \rightarrow A\) such that \(F^\psi(X, Y) = F(X, Y)\). Suppose we have already found a homomorphism \(\phi_n: \mathbb{Z}[U, T] \rightarrow A\) such that

\begin{align}
(6.2.1) \quad F^\psi(X, Y) &= F(X, Y), \quad \text{i.e. } \phi_n \text{ is equal to } \psi \text{ on } \mathbb{Z}[U] \subset \mathbb{Z}[U; T], \\
(6.2.2) \quad \alpha^\psi_{U,T}(X) &= \alpha(X) \mod \text{(degree } n) \tag{6.2.2}
\end{align}

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

\begin{align}
(6.2.3) \quad \alpha^\psi_{U,T}(X) &= \alpha(X) + aX^n \mod \text{(degree } n + 1). \tag{6.2.3}
\end{align}

Now define \(\phi_{n+1}\) by \(\phi_{n+1}(U_i) = \psi(U_i); \quad \phi_{n+1}(T_i) = \phi_n(T_i), \quad i = 1, \ldots, n - 1; \quad \phi_{n+1}(T_n) = -a; \quad \phi_{n+1}(T_{n+1}) = 0, \quad i \geq n + 1\). Then (6.2.1) and (6.2.2) hold with \(n\) replaced by \(n + 1\) and \(\phi_{n+1}\) is unique on \(\mathbb{Z}[U; T_2, \ldots, T_n]\), 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 \(\mathbb{Z}[U; T]\) 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 \(n(i_1, \ldots, i_r)\)

In this section we define special \(n(i_1, \ldots, i_r)\), 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 \(i \in \mathbb{N} \setminus \{1\}\) let \(c(p, i)\) be an integer such that

\begin{align}
(7.1.1) \quad c(p, i) &= 1 \quad \text{if } \nu(i) = 1 \\
&= \begin{cases} 1 \mod p & \text{if } \nu(i) = q \neq p. \\ 0 \mod q & \end{cases}
\end{align}

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

\begin{align}
(7.1.2) \quad b(i_1, \ldots, i_r) &= \prod_{i_1, \ldots, i_r} c(p, i) b(i_1, \ldots, i_r) \quad \text{if } s \geq 2
\end{align}
where the product is over all prime numbers $p$ which divide $i_1 \ldots i_s$. (The factor $c(p, i)$ occurs only once, irrespective of how high a power of $p$ divides $i_1 \ldots i_s$.)

Finally we define

$$n(i_1, \ldots, i_s) = \frac{b(i_1, \ldots, i_s)}{b(i_1, \ldots, i_s)} \quad \text{if } s \geq 2, \text{ and } n(i) = 1.$$  

(7.1.3)

7.2. It follows directly from (7.1.2) that

$$b(i_1, \ldots, i_s) = \prod_{p \mid i_1 \ldots i_s} c(p, i) \prod_{p \mid i_1 \ldots i_{s-1}} c(p, i) \prod_{p \mid i_1} c(p, i)$$

and hence that

$$n(i_1, \ldots, i_s) = \prod_{p \mid i_1 \ldots i_s} c(p, i) \prod_{p \mid i_1 \ldots i_{s-1}} c(p, i) \prod_{p \mid i_1} c(p, i).$$

(7.2.2)

7.3. Lemma. The $n(i_1, \ldots, i_s)$ defined by (7.3.1) satisfy conditions (2.1.1)-(2.1.3).

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

Next let $d(i_1, \ldots, i_s)$ be as in 3.2, i.e.

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

(7.4.1)

then we have by (7.1.3)

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

(7.4.2)

Note that this number depends only on the product $i_1 \ldots i_s$. We define for all $n, d \in \mathbb{N} \setminus \{1\}$

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

(7.4.3)

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
\[ m_n(U) = \sum d(i_1, \ldots, i_l) U_{i_1} U_{i_2} \ldots U_{i_{n-l}} \]
\[ = \sum_{i=1}^{\mu(n)} \frac{\mu(i_1, \ldots, i_l)}{\nu(i_1, \ldots, i_l)} d(i_1, \ldots, i_{n-l}) U_{i_1} U_{i_2} \ldots U_{i_{n-l}} + \frac{1}{\nu(n)} U_n \]
\[ = \sum_{d \nmid n, (d,n)=1} \frac{\mu(n, d)}{\nu(d)} m_{n/d}(U) U_d^{n/d} + \mu(n)^{-1} U_n. \]

So that we find

\[ (7.5.1) \quad \nu(n)m_n(U) = U_n + \sum_{d \nmid n, (d,n)=1} \frac{\mu(n, d)\nu(n)}{\nu(d)} m_{n/d}(U) U_d^{n/d}. \]

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 \( q(n, d) \) 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 \( H_U(X, Y) = h_U(h_U(X) + h_U(Y)) \) where \( h_U(X) \) is the power series defined in (1.4). Then one has (i) \( H_U(X, Y) \) has its coefficients in \( \mathbb{Z}[U] \); (ii) the formal groups \( H_U(X, Y) \) and \( F_U(X, Y) \) are strictly isomorphic over \( \mathbb{Z}[U] \); (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