Netherlands School of Economics
ECONOMETRIC INSTITUTE

Report 7119

CONSTRUCTING FORMAL GROUPS I.

OVER $Z_{(p)}$ - ALGEBRAS.

by Michiel Hazewinkel

October 11, 1971

Constructing formal groups I. Over $Z_{(p)}$ - algebras*)

Michiel Hazewinkel

0. INTRODUCTION

Let A be an integral domain of characteristic zero, and let K be its quotient field. Let F(X,Y) be a one dimensional formal group over A. Then F is strictly isomorphic to the additive group over K; i.e. there exists a formal power series f(X) with coefficients in K, $f(X) = X + a_2X^2 + \ldots$ such that

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

where f^{-1} is the inverse power series to f; i.e. $f^{-1}(f(X)) = X$. This power series is called the logarithm of F. It is now natural (cf. also Honda [2]) to construct formal groups by taking a power series f and setting $F(X,Y) = f^{-1}(f(X) + f(Y))$. This F(X,Y) is automatically commutative and associative. It "only" remains to find conditions on f which guarantee that all the coefficients of F(X,Y) are in A. It is not difficult to show that if $f(X) = X + a_2X^2 + \ldots$ that then

$$n\,a_n \in A \qquad \text{for all } n \in \mathbb{N} \tag{2}$$

(In fact by differentiating (1) one gets $(\frac{\partial}{\partial X} F)(0,)^{-1} = f'(Y)$ from which (2) follows; cf. also [2] Prop.1)

In the following we shall as in [2] write down some (explicit) power series f to construct a universal formal group for formal groups over $Z_{(p)}$ - algebras. As an application we get necessary and sufficient conditions on f that F be in A [[X,Y]]. No doubt a large part if not all of the results obtained below are contained in some way in the work of Cartier (Cf. [1]).

---

*) Research supported by Z.W.O. (the Netherlands Organization for the Advancement of Pure Research).

1. CONSTRUCTION OF A FORMAL GROUP

We work over the ring $Z[T] = Z[T_1, T_2, \ldots]$ of polynomials in a countably infinite number of indeterminates over the integers.

1.1. The Construction

Choose a prime number p and let f_1 be the power series $f_T(X) = X + a_2X^2 + \ldots$, which is recursively defined by

$$f_T(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} f_T^{(i)}(X^{p^i}) \tag{3}$$

where $f_T^{(i)}$ denotes the power series obtained from f_T by raising each of the indeterminates $T_1, T_2, \ldots$ to the p^i-th power. The condition (3) completely determines the series f_T (recursively). It starts off as

$$f_T(X) = X + \frac{T_1}{p}X^p + \left(\frac{T_1^{1+p}}{p^2} + \frac{T_2}{p}\right)X^{p^2} + \left(\frac{T_1^{1+p+p^2}}{p^3} + \frac{T_1^{p^2}T_2}{p^2} + \frac{T_1T_2^p}{p^2} + \frac{T_3}{p}\right)X^{p^3} + \ldots \tag{4}$$

Let $f_{T(r)}$ stand for $f_{(T_1, T_2, \ldots, T_r, 0, 0, \ldots)}$. Then one easily checks that

$$f_T(X) \equiv f_{T(r)}(X) + \frac{T_{r+1}}{p} X^{p^{r+1}} \qquad \mod(\text{degree } p^{r+1} + 1) \tag{5}$$

Now let $F_T(X,Y)$ be the formal group defined by

$$F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y)) \tag{6}$$

It then follows from (5) that

$$F_{T(r+1)}(X,Y) \equiv F_T(X,Y) \equiv F_{T(r)}(X,Y) + T_{r+1}C_{p^{r+1}}(X,Y) \qquad \mod(\text{degree } p^{r+1} + 1) \tag{7}$$

where

$$C_{p^{r+1}}(X,Y) = p^{-1}((X+Y)^{p^{r+1}} - X^{p^{r+1}} - Y^{p^{r+1}})$$

Remark

Let $f_T(X) = X + a_1X^p + a_2X^{p^2} + \ldots$ then one can of course calculate the generators $T_1, \ldots, T_n, \ldots$ of $Z_{(p)}[T_1, \ldots, T_{n1} \ldots]$ (or $Z_{(p)}[T_1, \ldots, T_n, \ldots]$) from the a_i. This yields a recursion formula for the T_i:

$$
\begin{aligned}
T_1 &= pa_1 \\
T_2 &= pa_2 - T_1^p a_1 \\
T_3 &= pa_3 - T_1^{p^2} a_2 - T_2^p a_1 \\
T_4 &= pa_4 - T_1^{p^3} a_3 - T_2^{p^2} a_2 - T_3^p a_1 \\
&\vdots \\
T_n &= pa_n - \sum_{i=1}^{n-1} T_i^{p^{n-i}} a_{n-i} \\
&\vdots
\end{aligned}
\tag{8}
$$

1.2. Theorem.

All coefficients of $F_T(X,Y)$ are in $Z[T]$.

Proof. In the following we shall work in the ring $Q[T][[X,Y]]$. The expression $G \equiv H \bmod(a, \text{degree } n)$, where $a \in Z$ will mean that $G - H \in a\, Z[T][[X,Y]]$ modulo terms of total degree (in X,Y) greater or equal n. We proceed by induction. Let $F_T(X,Y) = F_1 + F_2 + \dots$, where F_i is homogeneous of degree i (in X,Y). Suppose that

$$F_1, \dots, F_n \in Z[T][X,Y]. \tag{9}$$

It is clear that if $s \geq 2$

$$(F_T(X,Y))^s \equiv (F_1 + \dots + F_n)^s \quad \bmod(\text{degree } n+2) \tag{10}$$

Using this, one shows without difficulty, because $F_1, \dots, F_n \in Z[T][X,Y]$

$$(F_T(X,Y))^{p^{k+\ell}} \equiv (F_T^{(k)}(X^{p^k}, Y^{p^k}))^{p^\ell} \quad \bmod(p^{\ell+1}, \text{degree } n+2) \tag{11}$$

Here $F_T^{(k)}$ denotes the formal group, obtained from F_T by raising all of the parameters $T_1, T_2, \dots$ to the p^k-th power; i.e.

$$F_T^{(k)}(X,Y) = (f_T^{(k)})^{-1}\,(f_T^{(k)}(X) + f_T^{(k)}(Y)) \tag{12}$$

The formal group F_T satisfies (by definition)

$$f_T(F_T(X,Y)) = f_T(X) + f_T(Y) \tag{13}$$

and therefore, according to (3)

$$F_T(X,Y) + \sum_{i=1}^{\infty} \frac{T_i}{p} f_T^{(i)}(F_T(X,Y)^{p^i}) = X + Y + \sum_{i=1}^{\infty} \frac{T_i}{p}(f_T^{(i)}(X^{p^i}) + f_T^{(i)}(Y \tag{14}$$

The coefficient of X^{p^j} in $f(X)$ is of the form $p^{-j}u$, $u \in Z[T]$; therefore, using (11), we have that

$$(15)\quad f_T^{(i)}(F_T(X,Y)^{p^i}) \equiv f_T^{(i)}(F_T^{(i)}(X^{p^i}, Y^{p^i})) \qquad \mathrm{mod}(p, \text{degree } n+2)$$

However, (cf. (12)),

$$(16)\quad f_T^{(i)}(F_T^{(i)}(X^{p^i}, Y^{p^i})) = f_T^{(i)}(X^{p^i}) + f_T^{(i)}(Y^{p^i})$$

Combining (15) and (16) and substituting this in (14) we get

$$(17)\quad F_T(X,Y) \equiv X + Y \qquad \mathrm{mod}\ (1, \text{degree } n+2),$$

i.e. F_{n+1} has all its coefficients in $Z[T]$. This completes the induction and the proof.

1.3. A Generalization.

Let g be any formal series in $Z[T][[X]]$ or $Z[T,U][[X]]$ which starts off as $g(X) = X + \ldots$ The U are additional parameters and must also be raised to the power p^i in $f^{(i)}$; let f be the power series

$$(18)\quad f(X) = g(X) + \sum_{i=1}^{\infty} \frac{T_i}{p} f^{(i)}(X^{p^i})$$

and let $F(X,Y) = f^{-1}(f(X) + f(Y))$ as before. Then one proves in the same way as in (1.2) that $F(X,Y)$ has all its coefficients in $Z[T]$ (resp. $Z[$

A good g (for later purposes) is the following

$$(19)\quad g(X) = \sum_{\substack{i=1 \\ (i,p)=1}}^{\infty} U_i X^i + X$$

Substituting U_{p^i} for T_i in (18) for this particular g we get a series $f_U(X)$ such that if $U(r)$ denotes $(U_1, \ldots, U_r, 0, 0, \ldots)$

$$(20)\quad F_{U(r)}(X,Y) \equiv F_U(X,Y) + B_{r+1}(X,Y) \qquad \mathrm{mod}(\text{degree } r+2)$$

if $r+1$ is not a power of p

$$F_{U(r)}(X,Y) \equiv F_U(X,Y) + C_{r+1}(X,Y) \qquad \mathrm{mod}(\text{degree } r+2)$$

if $r+1$ is a power of p

Here $B_{r+1}(X,Y) = (X+Y)^{r+1} - X^{r+1} - Y^{r+1}$, and $C_{r+1}(X,Y) = q^{-1}B_{r+1}(X,Y)$ if $r+1$ is a power of the prime q.

Remark. If $g(X) \in \mathbb{Z}_{(p)}[T]$, then the corresponding $F(X,Y)$ has all its coefficients in $\mathbb{Z}_{(p)}[T]$.

2. UNIVERSALITY PROPERTIES

All formal groups in this section are one dimensional.

It follows almost directly from a fundamental proposition of Lazard on the comparison of two formal groups, that the formal group F constructed in 1.1 is universal for formal groups over $\mathbb{Z}_{(p)}$ - algebras in sofar as a formal group of this special type can be universal; and that the formal group F_U of 1.3 is universal for formal groups over $\mathbb{Z}_{(p)}$ - algebras. Precise definitions are given in 2.3 below.

2.1. Proposition (Lazard).

If F, G are two one dimensional formal groups over a ring A such that $F(X,Y) \equiv G(X,Y) \bmod(\text{degree } n+1)$, then $F(X,Y) \equiv G(X,Y) + a\, C_{n+1}(X,Y) \bmod(\text{degree } n+2)$ for some $a \in A$.

2.2. p- Typical Groups (Cartier).

Let F be a formal group over a ring A. A formal power series c without constant terms is called a curve. We can add two curves by means of the formula

$$(c_1 +^F c_2)(X) = F(c_1(X), c_2(X)) \tag{21}$$

In addition one defines operators

$$\begin{aligned} ([a]c)(X) &= c(aX) && a \in A \\ (V_n c)(X) &= c(X^n) && n = 1, 2, \ldots \\ (F_n c)(X) &= \sum_{i=1}^{n} {}^F c(\xi_n^i X^{1/n}) && n = 1, 2, \ldots \end{aligned} \tag{22}$$

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

A formal group is called p-typical if $F_q c_o = 0$ for all primes $q \neq p$, where c_o is the curve $c_o(X) = X$. If A is a characteristic zero integral domain then this is the same as the requirement that the logarithm of F looks like

$$f(X) = X + a_1 X^p + a_2 X^{p^2} + \ldots$$

cf. Cartier [1].
The group F_T of 1.1 is therefore p-typical.

2.3. Definitions.

If $\rho : B \to A$ is a ring homomorphism, and F is a formal group over B one obtains a formal group $\rho_* F$ by applying ρ to the coefficients of F.

A formal group G over a ring B is called universal if for every formal group F over a ring A., there is a unique homomorphism $\rho: B \to A$ such that $\rho_* G = F$.

A p-typical G over a ring B is called p-typically universal if for every p-typical formal group F over a ring A there is a unique homomorphism $\rho: B \to A$ such that $\rho_* G = F$.

We add the qualification "over $Z_{(p)}$-algebras" in the definitions if these statements (only) hold for formal groups F over a $Z_{(p)}$-algebra.

2.4. Theorem.

The formal group F_U of 1.3 is universal over $Z_{(p)}$-algebras

2.5. Theorem.

The formal group F_T of 1.1 is p-typically universal over $Z_{(p)}$-algebras

2.6. Theorem.

Every formal group G over a $Z_{(p)}$-algebra A is strictly isomorphic to a formal group F_t where $t = (t_1, t_2, \ldots)$ is a sequence of elements of A.
("Strict" means that the isomorphism is given by a power series of the form $X + a_2 X^2 + \ldots$, $a_i \in A$.

2.7. The proof of 2.4. is standard. One uses Lazard's result 2.1 and the fact that all primes $q \neq p$ are invertible in a $Z_{(p)}$-algebra A. To prove 2.5 we need a lemma.

2.8. Lemma.

Let F and G be two p-typical formal groups over a $Z_{(p)}$-algebra A; and suppose that

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

then

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

Proof. Suppose this is not true, and let m be the smallest integer such that $F(X,Y) \not\equiv G(X,Y)$ mod(degree m+1), then $p^r+1 \leq m \leq p^{r+1}-1$. Then

$$F(X,Y) \equiv G(X,Y) + a\, B_m(X,Y) \qquad \text{mod(degree } m+1) \tag{23}$$

for some a A. Now let q be any prime different from p which divides m. Let $F^2(X_1, X_2) = F(X_1, X_2)$, $F^3(X_1, X_2, X_3) = F(X_1, F^2(X_2, X_3)$ and so on; and similarly for G. One then checks easily that

$$F^q(X_1, \ldots, X_q) \equiv G^q(X_1, \ldots, X_q) + a((X_1 + \ldots + X_q)^m - X_1^m - \ldots - X_q^m) \tag{24}$$

$$\text{mod(degree } m+1)$$

Now (cf. (22)), $(F_q c_o)^F(X) = F^q(\xi_q X^{1/q}, \xi_q^2 X^{1/q}, \ldots, \xi_q^q X^{1/q})$, and similarly for G. (The superscript F indicates that the operator F_q of 2.2 is to be taken with respect to the formal group F). Therefore by (24) the coefficients of $X^{m/q}$ in $(F_q c_o)^F(X)$ and $(F_q c_o)^G(X)$ differ by -aq. On the other hand $(F_q c_o)^F = 0 = (F_q c_o)^G$ because F and G are p-typical. Therefore, as q is invertible in A, a = 0 which contradicts our assumption.

q.e.d.

Remark. This lemma is just about completely trivial if A is an integral domain of characteristic zero, because we can then use the logarithm.

2.9. Proof of 2.5.

Let G be a p-typical formal group over a $Z_{(p)}$-algebra A. Suppose we have already found elements $t_1, \ldots, t_r \in A$ such that

$$G(X,Y) \equiv F_{(t_1, t_2, \ldots, t_r, 0,0, \ldots)}(X,Y) \qquad \text{mod(degree } p^r+1)$$

Then because both these formal groups are p-typical

$$F_{(t_1, t_2, \ldots, t_r,0,0, \ldots)}(X,Y) \equiv G(X,Y) \quad \text{mod(degree } p^{r+1})$$

By (2.1) and (5) there is now a unique a $t_{r+1} \in A$ such that

$$F_{(t_1, t_2, \ldots, t_{r+1}, 0,0, \ldots)}(X,Y) \equiv G(X,Y) \quad \text{mod(degree } p^{r+1}+1)$$

2.10. Proof of 2.6.

Let G be a formal group over A. We proceed by induction. Suppose that we have already found $t_1, \ldots, t_r \in A$ and a strict isomorphism given by a power series φ_n over A such that $\phi_n : F_{t(r)} \to G$ defines an isomorphism mod(degree n+1), where $t(r) = (t_1, \ldots, t_r, 0, \ldots)$, and $p^r \leq n < p^{r+1}$. I.e.

$$(25) \qquad F_{t(r)}(X,Y) \equiv \phi_n^{-1} G(\phi_n(X), \phi_n(Y)) \qquad \text{mod(degree } n+1)$$

It now follows from 2.1 that

$$(26) \quad F_{t(r)}(X,Y) \equiv \phi_n^{-1} G(\phi_n(X), \phi_n(Y)) + a\, C_{n+1}(X,Y) \quad \text{mod(degree } n+2)$$

for some $a \in A$. We distinguish three cases

(i) $n+1 < p^{r+1}$ is not a power of a prime. Then $\phi_{n+1}(X) = \phi_n(X) + a\, X^{n+1}$ defines an isomorphism mod(degree n+2) between $F_{t(r)}$ and G.

(ii) $n+1 < p^{r+1}$ is a power of a prime $q \neq p$. Then q is invertible in A and $\phi_{n+1}(X) = \phi_n(X) + q^{-1} a\, X^{n+1}$ defines an isomorphism mod(degree n+2) between $F_{t(r)}$ and G.

(iii) $n+1 = p^{r+1}$. Let $t_{r+1} = a$. Then ϕ_n defines an isomorphism between $F_{t(r+1)}$ and G.

q.e.d.

Remark.

The elements $t_1, t_2, \ldots$ are not uniquely determined by G. They also depend on the choice of ϕ. Cf. also sections (3.4), (3.5).

2.11. Corollary.

Every formal group over $Z_{(p)}$-algebra is isomorphic to a p-typical one.

Remark.

Cartier [1] gives a canonical transformation for rendering a given group law typical. Cf. also 3.3 and 3.2.

3. ISOMORPHISMS

The groups F_U of 1.3 and F_T of 1.1 are isomorphic over $Z_{(p)}[T]$ according to theorem 2.6. There is,however, an isomorphism between them over Z[T], which can be indicated fairly precisely. To see this we need some lemmas.

3.1. Lemma.

Let $u(X) = X + u_2X^2 + \ldots$ be a power series over Z[T] (or $Z_{(p)}[T]$). Let $b_n = c_n p^{-j}$, $c_n \in Z[T]$ (or $Z_{(p)}[T]$), where $n = p^i k$, with $(k,p) = 1$. Then we have

$$b_n(u(X)^{p^i})^n \equiv b_n(u^{(i)}(X^{p^i}))^n \qquad \text{mod } p.$$

where $u^{(i)}$ is the power series obtained from u by raising all the parameters $T_1, T_2, \ldots$ to the power p^i.

Proof.

$$p^{-j}c_n(u(X)^{p^i})^n = p^{-j}c_n(u^{(i)}(X^{p^i}) + p(\ \ldots))^{p^j k} =$$

$$= p^{-j}c_n(u^{(i)}(X^{p^i})^{p^j} + p^{j+1}(\ldots))^k = p^{-j}c_n(u^{(i)}(X^{p^i}))^n + p(\ldots).$$

3.2. Lemma.

Let $f(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} f^{(i)}(X^{p^i}) + f_o(X)$, $g(X) = X +$

$+ \sum_{i=1}^{\infty} \frac{T_i}{p} g^{(i)}(X^{p^i}) + g_o(X)$, where $f_o(X)$, $g_o(X) \in Z[T,U][[X]]$

(resp. $Z_{(p)}[T,U][[X]]$ and $f_o(X)$, $g_o(X) \equiv 0$ mod(degree 2). Then there exists a power series $u(X) \in Z[T,U][[X]]$ (resp. $Z_{(p)}[T,U][[X]]$ such that $u(X) = X$ mod(degree 2) and $f(u(X)) = g(X)$.

Proof.

Suppose $f(X) \equiv g(X)$ mod degree r. Let a_r, a_r^o, b_r, b_r^o be the coefficients of X^r in $f(X)$, $f_o(X)$, $g(X)$, $g_o(X)$ respectively. Then

$$a_r = \sum_{p^i j = r} \frac{T_i}{p} a_j^{(i)} + a_r^o$$

$$b_r = \sum_{p^i j = r} \frac{T_i}{p} b_j^{(i)} + b_r^o$$

It follows that $u_r = b_r - a_r = b_r^o - a_r^o$ is in $Z[T,U]$ (resp. $Z_{(p)}[T,U]$ Now substitute $u(X) = X + u_r X^r$ for X in $f(X)$. Then

$$f'(X) = f(u(X)) \equiv g(X) \text{ mod(degree } r+1)$$

To complete the proof it remains to show that $f'(X)$ is of the same general shape as $f(X)$ (with a different $f'_o(X)$ of course). This follows from 3.1.

q.e.d.

A corollary of 3.1 is that the logarithm of any universal formal group law satisfies an identity of the type $f(X) = X + f_o(X) + \sum_{i=1}^{\infty} \frac{T_i}{p} f^{(i)}(X^{p^i})$. By means of 3.2, and 3.1 over an integral domain A which is (not necessarily a $Z_{(p)}$-algebra) one sees that a formal group over A is isomorphic over A to a p-typical one iff it comes from F_U.

3.3. Corollary.

The logarithm f of a formal group F over $Z_{(p)}$-algebra A, which is an integral domain, satisfies an identity

$$f(X) = X + f_o(X) + \sum_{i=1}^{\infty} \frac{t_i}{p} f^{(i)}(X^{p^i}) \tag{27}$$

where $f_o(X) \in A[[X]]$ is $\equiv 0$ mod(degree 2), and $t_i \in A$. This is a necessary and sufficient condition for F(X,Y) to be in A[[X,Y]]. To determine therefore whether a given power series $f(X) = X + a_2X^2 + \ldots$ gives rise to a formal group over A. One first sets $f_o(X) = a_2X^2 + \ldots + a_{p-1}X^{p-1}$; $p\,a_p$ is in A; one takes $t_1 = a_p p$.

then (27) is satisfied nod(degree p + 1). (One can also take $t_1 = a_p + ps_1, s_1 \in A$ and correct $f_o^1(X)$ with a term $-s_1X^p$). Let

$$g_1(X) = X + a_2X^2 + \ldots + a_{p-1}X^{p-1} + \frac{t_1}{p} g_1^{(1)}(X^p) \tag{28}$$

Then $f(X) - g_1(X)$ must be of the form (if F is to be in A[[X,Y]])

$$c_{p+1}X^{p+1} + \ldots + c_{p^2-1}X^{p^2-1} + \frac{d_2}{p}X^{p^2} \quad \text{mod(degree } p^2 + 1)$$

with $c_{p+1}, \ldots, c_{p^2-1}, d_2 \in A$, this determines $f_o(X)$ mod(degree $p^2 + 1$) and $t_2 = d_2$ (Again we can also take $t_2 = d_2 + ps_2$ and correct

$f_o^2(X)$ which is the polynomial of consisting of the terms of degree $\leq p^2$ of $f_o(X)$ with a term $- s_2X^{p^2}$.

Now let

$$g_2(X) = X + f_o^2(X) + \sum_{i=1}^{2} \frac{t_i}{p} g_2^{(i)}(X^{p^i}) \tag{29}$$

Then $f(X) - g_2(X)$ must be of the form (if F is to be in A[[X,Y]])

$$c_{p^2+1} X^{p^2+1} + \ldots + c_{p^3-1} X^{p^3-1} + \frac{d_3}{p} X^{p^3} \quad \text{mod(degree } p^3 + 1)$$

with $c_{p^2+1}, \ldots, c_{p^3-1}, d_3 \in A$. This determines $f_o(X)$ mod(degree $p^3 + 1$) and t_3 (with again the same indeterminacy); etc ....etc ....

N.B. Applying an isomorphism $X + s_iX^{p^i}$ does not change the form of f(X) according to 3.1., and changing $f_o(X)$ by a term $s_iX^{p^i}$ comes from an isomorphism according to 3.2. This is why one can change t_i to $t_i + ps_i$; in the test described above.

3.4. Corollary.

If $f(X) = X + a_2X^2 + \ldots$ is the logarithm of a formal group over a characteristic zero integral domain A over $Z_{(p)}$. Then $f_{(p)}(X) = X + a_pX^p + a_{p^2}X^{p^2} + \ldots$ is the logarithm of an isomorphic p-typical formal group.

3.5. This procedure for rendering a given group law p-typical is in fact the same as that of Cartier [1]. Let c_o be the curve $c_o(X) = X$ and let $c_F = \sum_{(n,p)=1}^{F} \frac{\mu(n)}{n} V_n F_n c_o$, where all sums and operators are in the (filtered) groups of curves. Cf. (2.2); $\mu(n)$ is the Möbi s function. Then according to [1]

$$c_F^{-1} F(c_F(X), c_F(Y))$$

is a p-typical formal group. Because $F(X,Y) = f^{-1}(f(X) + f(Y))$ the logarithm of this p-typical formal group is $fc_F(X)$, which is

$$f(c_F(X)) = \sum_{(n,p)=1} \frac{\mu(n)}{n}\{f(\xi_n X) + \ldots + f(\xi_n^n X) \qquad \text{(ordinary sum)}$$

because $f\,(n \cdot^F c)(X) = f^{-1}(n f(c(X))$ and $(c_1 +^F c_2)(X) = f^{-1}(fc_1(X) + fc_2(X))$

If $f = X + a_2X^2 + \ldots$, then $f(\xi_n X) + \ldots + f(\xi_n^n X) = n(a_n X^n + a_{2n}X^{2n} + \ldots)$

The coefficient of X^m in $f(c_F(X))$ is therefore equal to

$$\sum_{\substack{\ell \mid m \\ (\ell,p)=1}} \mu(\ell) a_{\frac{m}{\ell}} = \begin{cases} 0 \text{ if } m \text{ is not a power of } p \\ a_m \text{ if } m \text{ is a power of } p \end{cases}$$

We have, if $m = p^r m'$, $(p,m') = 1$, $\sum_{\substack{\ell \mid m \\ (\ell,p)=1}} \mu(\ell) = \sum_{\ell \mid m'} \mu(\ell)$ and this is zero if $m' \neq 1$ and 1 if $m' = 1$)

(3.6) Suppose F_t and $F_{t'}$ are two p-typical formal groups over an integral domain A, obtained from F_T by substituting two different sequences $t = (t_1, t_2, \ldots)$, $t' = (t'_1, \ldots)$. We ask ourselves when they are isomorphic. We know from (3.1) and (3.2) that it is necessary and sufficient for this that $f_{t'}(X)$ is of the form

$$(30) \qquad f_{t'}(X) = s(X) + \sum_{i=1}^{\infty} \frac{t_i}{p} f_{t'}^{(i)}(X)$$

with $s(X) = X + \ldots \in A[[X]]$. Because $f_{t'}(X)$ is p-typical we must have that $s(X)$ is of the form

$$(31) \qquad s(X) = X + s_1X^p + s_2X^{p^2} + \ldots.$$

An easy calculation now shows that if $f(X) = X + a_1X^p + \ldots$ and $f'(X) = X + b_1X^p + \ldots$, it follows from (30) and (31) that

(32)
$$\begin{aligned} b_1 &= a_1 + s_1 \\ b_2 &= a_2 + s_2 + a_1 s_1^p \\ b_3 &= a_3 + s_3 + a_1 s_2^p + a_2 s_1^{p^2} \\ b_4 &= a_4 + s_4 + a_1 s_3^p + a_2 s_2^{p^2} + a_3 s_1^{p^3} \\ &\cdots \end{aligned}$$

Necessary and sufficient conditions for F_t and $F_{t'}$ to be isomorphic over A are therefore that

(33)
$$\begin{aligned} b_1 - a_1 &= s_1 \in A \\ b_2 - a_1 s_1^p - a_2 &= s_2 \in A \\ b_3 - a_1 s_2^p - a_2 s_1^{p^2} - a_3 &= s_3 \in A \\ b_4 - a_1 s_3^p - a_2 s_2^{p^2} - a_3 s_1^{p^3} - a_4 &= s_4 \in A \\ &\cdots \end{aligned}$$

4. HIGHER DIMENSIONAL COMMUTATIVE FORMAL GROUPS

Concerning higher dimensional commutative formal groups over a ring A, Lazard [4] proved

4.1. Proposition.

If $F(X,Y) \equiv G(X,Y)$ mod degree r, then $F(X,Y) \equiv G(X,Y) + \Delta(X,Y)$ mod degree r+1, with $\Delta(X,Y)$ of the form $\Gamma(X) - \Gamma(X+Y) + \Gamma(Y)$ for some form of degree r over A if r is not a power of a prime, and if $r = q^j$, then there is a form of degree r, Γ, and an $n \times n$ matrix D (with coefficients in A) such that

$$\Delta(X,Y) = \Gamma(X) - \Gamma(X+Y) + \Gamma(Y) + D C_{q^i}(X,Y)$$

where
$$C_{q^i}(X,Y) = (C_{q^i}(X_1,Y_1), \ldots, C_{q^i}(X_n,Y_n))$$

4.2. Construction.

Let f_T be an n-dimensional (column)vector of power series in the n-variables $X^t = (X_1, X_2, \ldots, X_n)$ over $\mathbb{Q}[T]$ such that

$$f_T(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} f_T(p^i)(X^{p^i}) \tag{34}$$

where now T_i is an n x n matrix of parameters

$$T_i = \begin{pmatrix} (T_i)_{1,1} & \cdots & (T_i)_{1n} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ (T_i)_{n1} & \cdots & (T_i)_{nn} \end{pmatrix}$$

and X^{p^i} is short for

$$X^{p^i} = \begin{pmatrix} X_1^{p^i} \\ \cdot \\ \cdot \\ \cdot \\ X_n^{p^i} \end{pmatrix}$$

We define the commulative n-dimensional formal group F_T by

$$F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y)) \tag{35}$$

Theorem. All coefficients of $F_T(X,Y)$ are in $\mathbb{Z}[T]$.
Same proof as of theorem 1.2.

4.3. Universal n-dimensional formal groups.

Exactly as in 1.3 we can take instead of X in formula (34) a power series g(X) with coefficients in a suitable ring of polynomials over Z (or $Z_{(p)}$). By taking a good g(X) (cf. 4.1) we get a formal group which is universal for commulative n-dimensional formal groups over $Z_{(p)}$-algebras (the analogue of Th. 2.4). The analogues of 2.5 and 2.6 also hold. Same kind of proof, using 4.1 instead of 2.1.

5. ADDITIONAL REMARKS AND COMMENTS.

5.1. Honda's Groups

Let K be a finite extension of Q_p; n the degree of the residue field extension and π a uniformizing element of K. In [2] Honda defines a series of one dimensional formal groups by means of the logarithmic series

$$f(X) = X + \frac{X^{p^{an}}}{\pi} + \frac{X^{p^{2an}}}{\pi^2} + \dots \tag{36}$$

where $a \in \mathbb{N}$ is arbitrary.

This series (36) satisfies the relation

$$f(X) = X + \pi^{-1} f(X^{p^{an}}) \tag{37}$$

One can now prove in almost exactly the same way as in §1 that the formal group

$$F(X,Y) = f^{-1}(f(X) + f(Y)) \tag{38}$$

has all its coefficients in A_K, the ring of integers of K.

An endomorphism u(X) of the formal group (38) is necessarily of the form

$$u(X) = f^{-1}(uf(X))$$

where u is integral over A_K. Using the relation $f(u(X)) = u\, f(X)$ one can apply similar arguments as those of §1 to the determination of the (absolute) endomorphism ring of F.

5.2. Height.

Let F_T be the one dimensional formal group defined in §1. Let

A be the ring of integers of some finite extension of $\mathbb{Q}_p$; let $(t_1, t_2, \ldots)$ be a sequence of elements of A. Let h be the smallest number such that $t_h \in A^* = U(A)$, let $h = \infty$ if such a t_h does not exist. Then height $(F_t) = h$.

5.3. Formal moduli.

Let R be a complete noetherian local ring with maximal ideal m such that $R/m \simeq k$, a field of characteristic $p > 0$. Let Φ be a formal group over k such that $\bar{\Phi}(X,Y) = X + Y + C_q(X,Y) \bmod(\text{degree } q+1)$ (Any formal group law over k is isomorphic to one of these). Then there is a lift F of $\bar{\Phi}$ of the form

$$F(0, \ldots, 0, a_n, a_{n+1}, \ldots)$$

where $q = p^n$, and a_n reduces to a mod m. Now consider the formal group law

$$F(T_1, \ldots, T_{n-1}, a_n, a_{n+1}, \ldots) \tag{39}$$

over $R[T_1, \ldots, T_{n-1}]$. This formal group law satisfies the conditions of Proposition 1.1 of [5]. It then follows from [5] that (39) gives an (explicit) parametrization of the *-isomorphism classes of lifts of $\bar{\Phi}$. (*-isomorphism = strict isomorphism).

5.4. Application to complex cobordism theory.

The formal group law F_U of 1.3 is universal for formal groups over $Z_{(p)}$-algebras (cf.2.4). If

$$f(X) = X + a_2X^2 + a_3X^3 + \ldots.$$

is its logarithm, then we can calculate the generators $U_1,U_2,\ldots$ of $Z_{(p)}[U_1,U_2,\ldots]$ from the $a_2,a_3,\ldots$. Cf. also formula (8) of 1.1 remark. Writing T_i for U_{p^i} this gives the following recursion formula:

$$\begin{aligned} T_1 &= p\, a_p \\ T_2 &= p\, a_{p^2} - T_1{}^p a_p \\ T_3 &= p\, a_{p^3} - T_1{}^{p^2} a_{p^2} - T_2{}^p a_p \qquad (40) \\ &\ldots \\ T_n &= p\, a_{p^n} - \sum_{i=1}^{n-1} T_i{}^{p^{n-i}} a_{p^{n-i}} \end{aligned}$$

If k is not a power of p, then k is of the form p^sr, where $(p,r) = 1$. For these U_k one finds recusively

$$\begin{aligned} U_r &= a_r \\ U_{pr} &= a_{pr} - a_pU_r{}^p \\ U_{p^2r} &= a_{p^2r} - a_{p^2}U_r{}^{p^2} - a_pU_{pr}{}^p \\ &\ldots\ldots \\ U_{p^sr} &= a_{p^sr} - \sum_{i=0}^{s-1} a_{p^{s-i}}U_{p^ir}{}^{p^{s-i}} \end{aligned}$$

The formal group law of complex cobordism theory is universal over Z (cf. Quillen [6]) and hence also universal over $Z_{(p)}$. Its logarithm is equal to

$$X + \frac{P_1}{2} X^2 + \ldots + \frac{P_n}{n+1} X^{n+1} + \ldots$$

where P_n is the class of $\mathbb{C}P^n$ in $\Omega^{-2n}(pt)$. Two universal group laws are isomorphic. Therefore, writing $a_{n+1} = (n+1)^{-1}P_n$, a free set of generators for the algebra $\Omega^{ev}(pt) \otimes Z_{(p)}$ over $Z_{(p)}$ is given by the formulas (40) and (41) above.

The formulas (40) give the generators of $\Omega T^*(pt)$, where ΩT^* is the generalized cohomology theory associated to the Brown Peterson spectrum as obtained from MUQ_p by the Quillen splitting [6].

5. .Remark. In this paper we have constructed some universal formal groups for formal groups over $Z_{(p)}$-algebras (F_U), where p was chosen in advance. This formal group F_U is not universal for commutative formal groups over Z-algebras (i.e. commulative rings with identity element). In a subsequent paper we shall show how to fit the formal groups F_U for each prime p together to get a truly universal formal group (i.e. over Z-algebras).

REFERENCES

[1]. Cartier, P, Modules associés à un groupe formal commutatif Courbes typiques, C.R. Acad. Sci. Paris 265 (1967), 129-132

[2]. Honda, T, Formal groups and zeta functions, Osaka J. Math. 5 (1968, 199-213.

[3]. Lazard, M, Sur les groupes de Lie formels à un paramètre, Bull. Soc. Math. France 83 (1955), 251-274.

[4]. Lazard, M, Lois de groupes et analyseurs, Ann. Sci. Ec. Norm. Sup. (3) 72 (1955), 299-400.

[5]. Lubin, J and Tate, J, Formal moduli for one-parameter formal Lie groups, Bull. Soc. Math. France 94 (1966), 49-60.

[6]. Quillen, D, On the formal group laws of unoriented and complex cobordism theory, Bull. Am. Math. Soc. 75 (1969), 1293-1298.

Michiel Hazewinkel
Nederlandse Economische Hogeschool
Burg. Oudlaan 50
3016 Rotterdam
The Netherlands

BA

Netherlands School of Economics

ECONOMETRIC INSTITUTE

Report 7119 (continued)

Appendix to : Constructing Formal Groups I.

Michiel Hazewinkel

October 15, 1971

Appendix to : Constructing Formal Groups I

In [ ] the formulas (8), (32), (40) and (41) were stated without proof.

Formulas (8), (40), (41) follow from the

A.1. Proposition

Let $f(X)$ be the power series over $Q[U_2, U_3, \ldots; T_1, T_2, \ldots]$ defined by

$$f(X) = g(X) + \sum_{i=1}^{\infty} \frac{T_i}{p} f^{(i)}(X^{p^i}) \tag{1}$$

where $g(X) = X + \sum_{\substack{i \geq 2 \\ (i,p)=1}} U_i X^i$ and $f^{(i)}$ is obtained from f by raising all of the parameters $T_1, T_2, \ldots, U_2, U_3, \ldots$ to the p^i-the power. Then if a_n is the coëfficient of X^n in $f(X)$ we have:

$$\begin{aligned} T_1 &= p\, a_p \\ T_2 &= p\, a_{p^2} - T_1^p a_p \\ T_3 &= p\, a_{p^3} - T_1^{p^2} a_{p^2} - T_2^p a_p \\ &\vdots \\ T_n &= p\, a_{p^n} - T_1^{p^{n-1}} a_{p^{n-1}} - \ldots - T_{n-1}^p a_p \end{aligned} \tag{2}$$

and if $u\, i = p^k s$, $(s,p) = 1$, we have for U_i

$$\begin{aligned} U_s &= a_s \\ U_{ps} &= a_{ps} - a_p U_s^p \\ U_{p^2 s} &= a_{p^2 s} - a_{p^2} U_s^{p^2} - a_p U_{sp}^p \\ &\vdots \\ U_{p^k s} &= a_{p^k s} - a_{p^k} U_s^{p^k} - a_{p^{k-1}} U_{ps}^{p^{k-1}} - \ldots - a_p U_{p^{k-1} s}^p \end{aligned} \tag{3}$$

(p is some fixed prime number).

To prove this we need some lemmas.

A.2. Lemma

Let $f(X)$ and a_n be as before. Then for $n \geq 1$

$$a_{p^n} = \Sigma \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}}}{p^r} \tag{4}$$

where the sum is taken over all $j_k \in N \cup \{0\}$, $i_k \in N$, $k = 1, \ldots, r$, $r \leq n$ such that

$$0 \leq j_1 < \ldots < j_r$$
$$p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^n - 1 \tag{5}$$

and, if $s > 1$, $(p,s) = 1$

$$a_{p^n s} = \Sigma \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}}}{p^r} U_{p^\ell s}^{p^{j_o}} \tag{6}$$

where the sum is taken over all ℓ, $j_k \in N \cup \{0\}$, $k = 0, 1, \ldots, r$; $i_k \in N$, $k = 1, \ldots, r$ such that

$$\ell + j_o = n, \; 0 \leq j_1 < j_2 < \ldots < j_r$$
$$p^{j_o}(p^\ell s - 1) + p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^n s - 1 \tag{7}$$

Proof. We use induction. Assume therefore that (4) holds for all $m < n$. It follows from (5) that $j_1 = 0$, $i_1 \leq n$, and that $i_1 \leq j_2 < \ldots < j_r$. Therefore

$$\Sigma \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}}}{p^r} = \sum_{i_1=1}^{n} \frac{T_{i_1}}{p} \Sigma \frac{(T_{i_2}^{p^{i_1}})^{p^{j_2 - i_1}} \cdots (T_{i_r}^{p^{i_1}})^{p^{j_2 - i_1}}}{p^{r-1}}$$

where $p^{j_2}(p^{i_2} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^n - p^{i_1}$ and hence

$$p^{j_2 - i_1}(p^{i_2} - 1) + \ldots + p^{j_r - i_1}(p^{i_r} - 1) = p^{n - i_1} - 1$$

$$0 \leq j_2 - i_1 < j_3 - i_1 < \ldots < j_r - i_1$$

and it follows by the induction hypothesis that

$$\sum \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}}}{p^r} = \sum_{i=1}^{n} \frac{T_i}{p} a_{p^{n-i}}^{(i)}$$

where $a_k^{(i)}$ is obtained from a_k by replacing the parameters $T_1, \ldots, T_n, \ldots$ by $T_1^{p^i}, \ldots, T_n^{p^i}, \ldots$. But according to (1) one has

$$a_{p^n} = \sum_{i=1}^{n} \frac{T_i}{p} a_{p^{n-i}}^{(i)}$$

which proves formula (4).

To prove (6) one proceeds similarly. If $\ell = n$, $j_o = 0$ and $r = 0$. If $\ell < n$, $j_1 = 0$ and the rest of the proof is completely analogous.

A.3. Lemma

Let $p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^n - 1$, with $i_1, \ldots, i_r \geq 1$ and $0 \leq j_1 < j_2 < \ldots < j_r$. Then $j_r = i_r = n$.

Proof. By induction on r. The case r = 1 is trivial. Suppose therefore that r > 1. It follows from the asymptions that $j_1 = 0$, and therefore

$$p^{j_2}(p^{i_2} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^n - p^{i_1}$$

It follows from this that $j_2 = i_1$, because $0 < j_2 < \ldots < j_n$, and $i_1 < n$. Therefore we find

$$(p^{i_2} - 1) + p^{j_3 - i_1}(p^{i_3} - 1) + \ldots + p^{j_r - i_1}(p^{i_r} - 1) = p^{n - i_1} - 1$$

By the induction hypothesis we now have $(j_r - i_1) + i_r = n - i_1$ and hence $j_r + i_r = 1$.

q.e.d.

A.4. Proof of proposition A.1.

According to lemma A.3 we have that $i_r + j_r = n$ in formula (4).

It follows that

$$a_{p^n} = \sum_{i=1}^{n} \frac{T_i^{p^{n-i}}}{p} \sum \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_{r-1}}^{p^{j_{r-1}}}}{p^{r-i}}$$

where, because $i_r + j_r = n$

$$p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_{r-1}}(p^{i_{r-1}} - 1) = p^{j_r} - 1 = p^{n-i} - 1$$

Therefore

$$a_{p^n} = \sum_{i=1}^{n} \frac{T_i^{p^{n-i}}}{p} a_{p^{n-i}}, \quad a_1 = 1$$

from which (2) follows.

According to (7) we have that

$$p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_r}(p^{i_r} - 1) = p^{j_o} - 1$$

for the $j_1 < \ldots < j_r$ occurring in (6). It follows that

$$a_{p^n s} = U_{p^n s} + \sum_{i=1}^{n} a_{p^i} U^{p^i}_{p^{n-i} s}$$

from which (3) follows

To prove formula (Jl) we need another lemma.

A.5. Lemma

Let $f(X) \in Q[s_1, s_2, \ldots, T_1, T_2, \ldots]$ be defined by the formula

$$f(X) = X + \sum_{i=1}^{\infty} s_i X^{p^i} + \sum_{i=1}^{\infty} \frac{T_i}{p} f^{(i)}(X^{p^i})$$

Then if

$$f(X) = X + b_1 X^p + b_2 X^{p^2} + \ldots$$

we have

$$b_n = \sum \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}}}{p^r} + \sum \frac{T_{i_1}^{p^{j_1}} \cdots T_{i_r}^{p^{j_r}} S_{i_o}^{p^{j_o}}}{p^r}$$

where the first sum is taken over all $j_k \in N \cup \{0\}$, $i_k \in N$, $r \in N$ such that $j_1 < j_2 < \ldots < j_r$ and $p^{j_1}(p^{i_1}-1) + \ldots + p^{j_r}(p^{i_r}-1) = p^n - 1$; and the second sum is taken over all $j_k \in N \cup \{0\}$, $r \in N \cup \{0\}$, $i_k \in N$ such that $i_o + j_o = n$, $j_1 < j_2 < \ldots < j_r$, $p^{j_1}(p^{i_1} - 1) + \ldots + p^{j_r}(p^{i_r}-1) + p^{j_o}(p^{i_o} - 1) = p^n - 1$.

Proof. Similar to the proof of Lemma A.2.

A.6. Corollary.

Let $f(X)$ be as above, and let $g(X) = X + a_1 X^p + \ldots$ be defined by

$$g(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} g^{(i)}(X^{p^i})$$

then we have

$$b_1 = a_1 + S_1$$

$$b_2 = a_2 + a_1 S_1^p + S_2$$

$$b_3 = a_3 + a_2 S_1^{p^2} + a_1 S_2^p + S_3$$

$$b_n = a_n + a_{n-1} S_1^{p^{n-1}} + \ldots + a_1 S_{n-1}^p + S_n$$

Proof. Exactly as in A.4, starting from A.5 instead of A.2.
Note that this proves formula (3) of [1].

A.7. Remark

Let now X be a vector and let $f(X)$ be the n-dimensional power series defined by

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

where now the T_i are n x n matrices of parameters as in [1] (§4).

(If $X^T = (X_1, \ldots, X_n)$, then $(X^{p^i})^T = (X_1^{p^i}, \ldots, X_n^{p^i})$;

$..^T$ denotes transposition as usual)

Then f(X) is of the form

$$f(X) = + a_1 X^p + a_2 X^{p^2} + \ldots$$

where now the a_i are n x n matrices. Then if we write $T_i^{(p^k)}$ for the matrix T_i with all its entries raised to the power p^k, one has

$$T_1 = p\, a_1$$

$$T_2 = p\, a_2 - a_1 T_1^{(p)}$$

$$T_3 = p\, a_3 - a_2 T_1^{(p^2)} - a_1 T_2^{(p)}$$

$$T_n = p\, a_n - a_{n-1} T_1^{(p^{n-1})} - \ldots - a_1 T_{n-1}^{(p)}$$

This is proved in the same way as A.1. One also has analogues for the second part of A.2. and for A.6., which gives multi-dimensional analogues for the formulas (8), (32), (40) and (41) of [1].

Reference

1. M. Hazewinkel, Constructing formal groups I. Over $Z_{(p)}$-algebras. Report of the Econometric Institute, Netherlands School of Economics, no. 7119 (1971).