BA

Netherlands School of Economics,

ECONOMETRIC INSTITUTE

Report 7207

# CONSTRUCTING FORMAL GROUPS

## III: Over Z, $Z_{(p)}$ and $Z_p$

by Michiel Hazewinkel

April 2, 1972

Preliminary and Confidential

# CONSTRUCTING FORMAL GROUPS

## III: Over Z, $Z_{(p)}$ and $Z_p$

by Michiel Hazewinkel

## Contents



## 1. INTRODUCTION

The present note merely gives some complements to the constructions of commutative (universal) formal groups in [4], [5]. In [7] Honda has given a method of constructing many formal groups over rings which satisfy a certain hypothesis, e.g. over W(k) where k is a field of characteristic $p > 0$.

In case of W(k) this method gives all isomorphism classes of commutative formal groups; this is not true for ramified extensions of W(k). In section 2 we discuss a link between the constructions of [4], [5] and those of [7].

Let $F_T$ be the formal group over $\mathbf{Z}[T_1, T_2, \ldots]$ constructed in [4] section (1.1). I.e. $F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y))$ where $f_T(X)$ is given by $f_T(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} f_T^{(i)}(X^{p^i})$, where $f_T^{(i)}$ is obtained from $f_T$ by replacing all the parameters $T_1, T_2, \ldots$ by $T_1^{p^i}, T_2^{p^i}, \ldots$

Let $t = (t_1, t_2, \ldots)$ be a sequence of elements of a $Z_{(p)}$-algebra A and let $F_t$ be the formal group over A obtained from $F_T$ by substituting $t_i$ for $T_i$. Every formal group over A is strictly isomorphic to some $F_t$. ([4], theorem (2.6)).

By means of some formulae derived in section 3 we prove in section 4 that for one dimensional formal groups over $Z_{(p)}$ or $Z_p$ the following holds:

let $t = (t_1, t_2, \ldots)$, $t' = (t'_1, t'_2, \ldots)$, $t_i, t'_i \in Z_{(p)}, Z_p$ then $F_t$ and $F_{t'}$ are isomorphic if and only if $t_i = t'_i \bmod p$ $i = 1, 2, \ldots$ As a corollary we get another proof of the fact due to Cartier [1], [3]]and Hill [6], that two formal groups over $Z_p$ are isomorphic if and and only if their reductions are isomorphic. It seems that this result is not generalizable as is shown by two examples given in section 5.

As regards terminology: all formal groups are supposed to be commutative; an n-tuple of power series $f(X) = (f_1(X), \ldots, f_n(X))$ over a ring A in $X = (X_1, \ldots, X_n)$ such that $f(X) \equiv MX$, mod degree 2, where M is an n x n matrix, is said to be an isomorphism between the n-dimensional formal groups $F(X,Y)$ and $G(X,Y)$ over A if $f(F(X,Y)) = G(f(X), f(Y))$; f is said to be a strict isomorphism if $M = I$, the n x n unit matrix.

## 2. THE FORMAL GROUPS OF HONDA [6].

### 2.1. Honda's Construction (One Dimensional case)

Let A be characteristic zero discrete valuation ring of residue characteristic $p > 0$; let $\mathfrak{p}$ be the maximal ideal of A. Assume moreover that the following condition is satisfied

(2.1.1) there exists an endomorphism $\sigma$ of A and a power q of p such that $a^\sigma \equiv a \bmod \mathfrak{p}$ for all $a \in A$.

One can take e.g. $A = W(k)$, the ring of Witt vectors of a field of characteristic p. Then $q = p$ and $\sigma$ is the endomorphism denoted F in [8] , Ch. II, §6, the Frobenius endomorphism.

Let $A_\sigma[[W]]$ be the noncommutative ring of power series in W over A defined by the multiplication rule.

(2.1.2) $$W\, a = a^\sigma W \qquad \text{for } a \in A$$

Let $u \in A_\sigma[[W]]$ be an element of the form $u = \pi - \sum_{\nu=1}^{\infty} c_\nu W^\nu$, where where $\pi$ is a prime element of $\mathfrak{p}$; write $\pi u^{-1} = \sum_{\nu=0}^{\infty} b_\nu W^\nu$, $b_\nu \in Q(A)$, the field of fractions of A. Now let

(2.1.3) $h_c(X) = \sum_{\nu=0}^{\infty} b_\nu X^{q^\nu}$ , $H_c(X,Y) = h_c^{-1}(h_c(X) + h_c(Y))$

where $c = (c_1, c_2, \ldots)$. Then we have

(2.1.4) Theorem (Honda [7])

$H_c(X,Y)$ is a formal group over A

It is not particularly difficult to calculate h(X) from u. One readily finds the recursion relations

(2.1.5)
$$b_1 = \frac{c_1}{\pi^\sigma}$$
$$b_2 = \frac{b_1 c_1^\sigma}{\pi^{\sigma^2}} + \frac{c_2}{\pi^{\sigma^2}}$$
$$b_3 = \frac{b_2 c_1^{\sigma^2}}{\pi^{\sigma^3}} + \frac{b_1 c_2^\sigma}{\pi^{\sigma^3}} + \frac{c_3}{\pi^{\sigma^3}}$$
$$\cdots\cdots$$

This looks rather like formula's (8) of [4]. And in fact it is now not difficult to show (reverse the arguments of [4], appendix) that $h_c(X)$ satisfies and is determined by

(2.1.6) $$h_c(X) = X + \sum_{i=1}^{\infty} \frac{c_i}{\pi^{\sigma^i}} h_c^{\sigma^i}(X^{q^i})$$

Practically the same arguments as those of [4] §1 now prove (2.1.4)

2.2. More dimensional Honda formal groups.

Now let the $c_i$ be n x n matrices, let $X = (X_1, \ldots, X_n)$, $X^{q^i} = (X_1^{q^i}, \ldots, X_n^{q^i})$, and let $h_c(X)$ be the n-vector of formal power series in X determined by (2.1.6). Define the n-dimensional formal group $H_c$ by $H_c(X,Y) = h_c^{-1}(h_c(X) + h_c(Y))$. Then (2.1.4) also holds for these more dimensional formal groups.

Honda also considers a stronger condition on A.

(2.2.1) condition (2.1.1) is satisfied with q = p and the valuation of A is unramified.

He proves under this condition.

2.2.2. Theorem (Honda [7]).

If A satisfies (2.2.1) then every formal group over A is isomorphic to an $H_c$.

2.3. Formal Groups over Rings of Witt Vectors.

Let $T_i$, $S_i$ be n x n matrices $T_i = ((T_i)_{j\ell})$, $S_i = ((S_i)_{j\ell})$ $j, \ell = 1, \ldots, n$, in indeterminates $(T_i)_{j\ell}$ $(S_i)_{j\ell}$ . Let $Z_{(p)}[T,S]$ be the ring of polynomials over $Z_{(p)}$ in these indeterminates. We define two n-vectors of power series in $X = (X_1, \ldots, X_n)$.

$$(2.3.1) \quad f_T(X) = X + \sum_{i=1}^{\infty} \frac{T_i}{p} f_T^{(i)}(X^{p^i}), \quad f_{T,S}(X) = X + \sum_{i=1}^{\infty} S_i X^{p^i} + \sum_{i=1}^{\infty} \frac{T_i}{p} f_{T,S}^{(i)}(X^{p^i})$$

where $X^{p^i} = (X_1^{p^i}, \ldots, X_n^{p^i})$ and $f_T^{(i)}$ and $f_{T,S}^{(i)}$ are obtained from $f_T$ and $f_{T,S}$ by replacing the parameters $(T_i)_{j\ell}$ and $(S_i)_{j\ell}$ by their p-th powers. Define

$$(2.3.2) \qquad F_T(X,Y) = f_T^{-1}(f_T(X) + f_T(Y)),$$

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

Then we have: $F_T$ and $F_{T,S}$ are strictly isomorphic formal groups over $Z_{(p)}[T,S]$. (Cf. [4]). Let A be a commutative $Z_{(p)}$-algebra; let $F_t$, $F_{t,s}$ be the formal groups over A obtained from $F_T$ and $F_{T,S}$ by substituting elements $(t_i)_{j\ell}$ and $(s_i)_{j\ell}$ for $(T_i)_{j\ell}$ and $(S_i)_{j\ell}$. We know, that every formal group over A is strictly isomorphic to an $F_t$. Now let A be also an integral domain. An n-dimensional formal group over A will be called p-typical if its logarithm g looks like $g(X) = X + \sum_{i=1}^{\infty} M_i X^{p^i}$ where the $M_i$ are n x n matrices. One also has (cf. [4]): every p-typical formal group over A is equal to some $F_t$.

Given the sequences of matrices t,s let t' be such that $F_{t'} = F_{t,s}$. The formal groups $F_t$ and $F_{t'}$ are strictly isomorphic. Using all this one gets:

(2.3.3) let R be a system of representants of A/pA in the $Z_{(p)}$-algebra A. Then for every n dimensional formal group G over A there exists a sequence of matrices $t = (t_1, t_2, \ldots)$, $(t_i)_{j\ell} \in R$ such that G is strictly isomorphic to $F_t$. (If A is of characteristic zero there exists precisely one such sequence of matrices).

Now let k be a field of characteristic p (or more generally an integral domain of characteristic p). Let A = W(k), and for $\alpha \in k$ let $[\alpha]$ denote the Witt vector $[\alpha] = (\alpha, 0, 0, \ldots)$. Let $\sigma$ be the Frobenius endomorphism of W(k). Let R be the system of representants $R = \{[\alpha] | \alpha \in k\}$ of $A/pA \simeq k$ in A.
The ring A satisfies condition (2.2.1). Also if $t \in R$ then $t^\sigma = t^p$. This gives:

(2.3.4) if $(t_i)_{j\ell} \in R$ for all i = 1, 2, ...; j, = 1, ..., n then

$$H_t(X,Y) = F_t(X,Y)$$

and this combined with (2.3.3) gives a proof of theorem (2.2.2) for rings A = W(k)

(2.3.5) Remark.

The result derived above on the one hand extents (2.2.2) a bit and on the other hand does not cover all of (2.2.2). This last fact can be repaired to a large extent as follows. Let t,s be two series of matrices in W(k); let $t'' = (t''_1, t''_2, \ldots)$ be defined by

$$(p + t''_1W + t''_2W^2 + \ldots) = (1 + s_1W + s_2W^2 + \ldots)(p + t_1W + t_2W^2 + \ldots)$$

The formal groups $H_{t''}$ and $H_t$ are then strictly isomorphic (Honda [7]). Now let A be a subring of W(k) which is invariant under $\sigma$ and contains a full set of representatives of k = W(k)/pW(k), then every Honda formal group over W(k) is strictly isomorphic (over W(k) to one defined over A. Thus we also get a proof of (2.2.2) for such subrings of rings W(k).

3. A FORMULA.

As in (2.3) let the n-vectors of power series $f_T(X)$ and $f_{T,S}(X)$ in $X = (X_1, \ldots, X_n)$ be defined by

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

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

(3.2) $$f_T(X) = \sum_{i=o}^{\infty} A_i^*(T) X^{p^i},$$

$$f_{T,S}(X) = \sum_{i=o}^{\infty} A_i(T,S) X^{p^i}$$

where the $A_i^*(T)$ and $A_i(T,S)$ are n x n matrices, $A_o^*(T) = A_o(T,S) = I$, and $X^{p^i}$ is the columnvector consisting of the $X_j^{p^i}$, $j = 1, \ldots, n$

Then we have (cf. [4] appendix)

(3.3) $$A_m^*(T) = \sum_{i=1}^{m} A_{m-i}^*(T) \frac{T_i^{(m-i)}}{p}$$

(3.4) $$A_m(T,S) = A_m^*(T) + \sum_{i=1}^{m} A_{m-i}^*(T) S_i^{(m-i)}$$

where $T_i^{(o)} = T_i$ are $T_i^{(r)}$ (resp. $S_i^{(r)}$) is the n x n matrix $(((T_i)_{j\ell})^{p^r})$ (resp. $(((S_i)_{j\ell})^{p^r})$).

We define

(3.5) $$Z_{ij}(T,S) = \frac{T_i S_j^{(i)} - S_i T_j^{(i)}}{p} \quad \text{and} \quad Z_{ij}^{(r)}(T,S) = \frac{T_i^{(r)} S_j^{(i+r)} - S_i^{(r)} T_j^{(i+r)}}{p}$$

Then we have

3.6. <u>Proposition</u>.

$$A_m(T,S) = \sum_{i=1}^{m} A_{m-i}(T,S) \frac{T_i^{(m-i)}}{p} + \sum_{i,j \geq 1, i+j \leq m} A_{m-i-j}^*(T) Z_{ij}^{(m-i-j)}(T,S) + S_m$$

Proof. Using (3.3) and (3.4) one finds

$$A_m(T,S) = A^*_m(T) + \sum_{i=1}^{m} A^*_{m-i}(T)S_i^{(m-i)}$$

$$= \sum_{i=1}^{m-1} A^*_{m-i}(T)\frac{T_i^{(m-i)}}{p} + \frac{T_m}{p} + \sum_{i=1}^{m-1}\sum_{j=1}^{m-i} A^*_{m-i-j}(T)\frac{T_j^{(m-i-j)}}{p} S_i^{(m-i)} + S_m$$

$$= \sum_{i=1}^{m-1} A_{m-i}(T,S)\frac{T_i^{(m-i)}}{p} - \sum_{i=1}^{m-1}\sum_{j=1}^{m-i} A^*_{m-i-j}(T)\, S_j^{(m-i-j)}\, \frac{T_i^{(m-i)}}{p}$$

$$+ \sum_{i=1}^{m-1}\sum_{j=1}^{m-i} A^*_{m-i-j}(T)\frac{T_j^{(m-i-j)}}{p} S_i^{(m-i)} + \frac{T_m}{p} + S_m$$

$$= \sum_{i=1}^{m-1} A_{m-i}(T,S)\frac{T_i^{(m-i)}}{p} + \sum_{i,j\geq 1,\, i+j\leq m} A^*_{m-i-j}(T)\, Z_{ij}^{(m-i-j)}(T,S) + \frac{T_m}{p} + S_m$$

$$= \sum_{i=1}^{m} A_{m-i}(T,S)\frac{T_i^{(m-i)}}{p} + \sum_{i,j\geq 1,\, i+j\leq m} A^*_{m-i-j}(T) Z_{ij}^{(m-i-j)}(T,S) + S_m$$

## 4. FORMAL GROUPS OVER $Z_{(p)}$, $Z_p$ and $Z$.

### 4.1. p-Typical Groups.

Let A be a Z-algebra. A more dimensional formal group G over A is called p-typical if it is of the form $G = F_t$ for some sequence of matrices $t = (t_1, t_2, \ldots)$ with coefficients in A. This agrees in the one dimensional case with the definition used in [4] and elsewhere. Every formal group over a $Z_{(p)}$-algebra is isomorphic to a p-typical one. Simply because the universal formal group of [5] is isomorphic (over $Z_{(p)}[T,S]$) to $F_T$.

Let, for the moment, A be a characteristic zero $Z_{(p)}$ integral domain. Let G be a formal group over A with logarithm g. Replacing the coefficients of all monomials $X^s = X_1^{s_1}, \ldots, X_n^{s_n}$ with zero for all s which are not of the form $(0, \ldots, 0, p^r, 0, \ldots, 0)$ gives a vector of power series f which is the logarithm of a formal group F over A which is isomorphic (over A) to G.

As in the one dimensional case cf [2] this isomorphism can also be described in terms of the formal group G.

Let $c(X)$, $c'(X)$ be n-vectors of power series in $X = (X_1, \dots, X_n)$ with coefficients in A without constant terms. Let G be an n-dimensional formal group over A. One defines

(4.1.1) $$(c +_G c')(X) = G(c(X), c'(X))$$

and for each $i = 1, \dots, n$ and $m \in N$ we define operators $V_m(i)$, $F_m(i)$ as

(4.1.2) $$(V_m(i)c)(X) = c(0, \dots, X_i^m, 0, \dots, 0)$$

(4.1.3) $$(F_m(i)c)(X) = c(0, \dots, \zeta_m X_i^{1/m}, 0, \dots, 0) + {}_G\, c(0, \dots, 0, \zeta_m^2 X_i^{1/m}, 0, \dots, 0) +_G \dots + c(0, \dots, 0, \zeta_m^m X_i^{1/m}, 0, \dots, 0)$$

Now let $c^o(X)$ be the n-vector of power series $c^o(X) = (X_1, \dots, X_n)$. Define

(4.1.4) $$c_G = \sum_{\substack{i=1,2,\dots,n \\ (m,p)=1}} \frac{\mu(m)}{m} V_m(i) F_m(i) c^o$$

Then $c_G(X)$ is the isomorphism between G and the p-typical formal group F. This also works over $Z_{(p)}$-algebras A which are not an integral domain.

4.2. Isomorphisms of p-typical Groups.

Below we shall need the following isomorphism result of [4].

4.2.1. Proposition.

Let A be an integral domain, $F_t$ the formal group obtained from $F_T$ by substituting $(t_i)_{j\ell}$ for $(T_i)_{j\ell}$, $(t_i)_{j\ell} \in A$. Let G be another p-typical formal group over A. Then G is strictly isomorphic to $F_t$ if and only if there are n x n matrices $s_i$, $i = 1, \dots, n$ with coefficients in A such that $G(X,Y) = F_{t.s}(X,Y)$, where $F_{t.s}$ is the formal group obtained from $F_{T,S}$ by substituting $(t_i)_{j\ell}$ and $(s_i)_{j\ell}$ for $(T_i)_{j\ell}$ and $(S_i)_{j\ell}$ .

4.2.2. Remarks.

1. For a proof cf [4] or (better) [5].

2. The most important step of the proof of (4.2.1) is to show that $F_{T,S}$ and $F_T$ are isomorphic over $Z_{(p)}[T,S]$ (or $Z[T,S]$). Another proof of this rests on the following lemma.

Lemma. In the expansion of $(X + uX^{p^i})^{p^s}$ there occur no other p-power powers of X then $X^{p^s}$ and $X^{p^{i+s}}$. (N.B. this is not true if there occur more than two terms inside the brackets). Let $f_{T,S}(X)$ and $f_T(X)$ be the logarithms of $F_{T,S}$ and $F_T$. We now indicate in the one-dimensional case how to obtain $f_{T,S}(X)$ from $f_T(X)$ by successive substitutions. First substitute $X + S_1X^p$ for X and render the resulting power series p-typical; the resulting coefficients are (if $f_T(X) = \sum_{i=1}^{\infty} a_iX^{p^i}$)

$$1,\ a_1 + S_1,\ a_2 + a_1S_1^p,\ a_3 + a_2S_1^{p^2},\ a_4 + a_3S_1^{p^3},\ a_5 + a_4S_1^{p^4},\ \ldots$$

Now substitute $X + S_2X^{p^2}$ and render the resulting power series p-typical again. We obtain

$$1,\ a_1 + S_1,\ a_2 + a_1S_1^p + S_2,\ a_3 + a_2S_1^{p^2} + a_1S_2^p,\ a_4 + a_3S_1^{p^3} + a_2S_2^{p^2} + a_1S_1^pS_2^{p^2},\ \ldots$$

Now substitute $X - S_1S_2^pX^{p^3}$ (assuming p is odd) and render p-typical again. We obtain

$$1,\ a_1 + S_1,\ a_2 + a_1S_1^p + S_2,\ a_3 + a_2S_1^{p^2} + a_1S_2^p,$$
$$a_4 + a_3S_1^{p^3} + a_2S_2^{p^2} - S_1S_1^pS_2^{p^2},\ \ldots.$$

Now substitute $X + S_3X^{p^3}$ and render p-typical. We find

$$1,\ a_1 + S_1,\ a_2 + a_1S_1^p + S_2,\ a_3 + a_2S_1^{p^2} + a_1S_2^p + S_3,$$
$$a_4 + a_3S_1^{p^3} + a_2S_2^{p^2} + a_1S_3^p + S_1S_3^p - S_1S_1^pS_2^{p^2},\ \ldots$$

In two steps one now gets rid of $S_1S_3^p$ and $-S_1S_1^pS_2^{p^2}$ in the coefficient of $X^{p^4}$, and then $S_4$ is introduced, continuing in this way we "finally" get $f_{T,S}(X)$.

The rest of the proof of (4.2.1) goes as follows. Let G be isomorphic to $F_t$, suppose we have already found $s_1, \dots, s_r$ such that G and $F_{t,s}$ coincide mod deg $p^r + 1$, then both being p-typical they coincide mod $p^{r+1}$.
They are also isomorphic (because $F_t$ and $F_{t,s}$ are isomorphic). The isomorphism must look like $X + aX^{p^{r+1}}$ mod degree $p^{r+1}+1$, a an n x n matrix over A. Choosing $s_{n+1} = a$ we see that

$G \equiv F_{t,s}$ mod degree $p^{r+1} + 1$.

From now on in section 4 we shall consider only one dimensional formal groups over $Z$, $Z_{(p)}$, $Z_p$ (and other rings A for which $a^p \equiv a$ mod p).

4.3. Proposition.

Let A be a characteristic zero integral domain in which $a^p \equiv a$ mod p holds. The one dimensional p-typical formal groups $F_t$ and $F_{t'}$ are then strictly isomorphic if and only if $t_i \equiv t_i'$ mod p. $i = 1, 2, \dots$

Proof. Let $f_t$ and $f_{t'}$ be the logarithms of $F_t$ and $F_{t'}$. We write

$$(4.3.1) \qquad f_t(X) = \sum_{i=o}^{\infty} a_i^* X^{p^i} \qquad f_{t'}(X) = \sum_{i=o}^{\infty} a_i X^{p^i}$$

First assume that $F_t$ and $F_{t'}$ are strictly isomorphic. Then there are $s_1, s_2, \dots, s_i \in A$ such that $f_{t'}(X) = f_{t,s}(X)$. Let $z_{ij}^{(m)} = Z_{ij}^{(m)}(t,s)$ (cf. (3.5)). Using (3.6) we find

$$(4.3.2) \qquad a_m = \sum_{i=1}^{m-1} a_{m-i} \cdot \frac{t_i^{p^{m-i}}}{p} + \sum_{i,j\geq 1, i+j\leq m} a^*_{m-i-j} z_{ij}^{(m-i-j)} + \frac{t_m}{p} + s_m$$

and on the other hand (cf. (3.3)).

$$(4.3.3) \qquad a_m = \sum_{i=1}^{m-1} a_{m-i} \frac{t_i'^{p^{m-i}}}{p} + \frac{t_m'}{p}$$

Taking $m = 1$ gives $t_1 \equiv t_1'$ mod p. Now because $a^p \equiv a$ mod p we have $pz_{ij} \equiv 0$ mod p ($pz_{ij} = t_i s_j^{p^i} - s_i t_j^{p^i}$) and $pz_{ij}^{(\ell)} = t_i^{p^\ell} s_j^{p^{i+\ell}} - s_i^{p^\ell} t_j^{p^{i+\ell}} \equiv 0$ mod $p^{\ell+1}$. It follows that $a^*_{m-i-j} z_{ij}^{(m-i-j)} \equiv 0$ mod 1 for all i,j.

Now suppose $t_i \equiv t_i'$ for $i = 1, \ldots, m-1$, then $t_i^{p^{m-i}} \equiv t_i'^{p^{m-i}}$ mod $p^{m-i+1}$; using this and (4.3.3) and (4.3.2) we find that $t_m \equiv t_m'$ mod p.

Now suppose $t_i \equiv t_i'$ mod p for all $i = 1, 2, \ldots$ To prove $F_t$ and $F_{t'}$ isomorphic we must show that we can find $s_1, s_2, \ldots \in A$ such that $f_{t'} = f_{t,s}$. Take $s_1 = \frac{t_1'-t_1}{p}$. Suppose we have already found $s_1, \ldots, s_{m-1}$. The element $s_m$ is then determined by (4.3.2) and we must show that it is in A. This follows from $a^*_{m-i-j} z_{ij}^{(m-i-j)} \equiv 0$ mod 1 and $p^{-1} a_{m-i}(t_i^{p^{m-i}} - t_i'^{p^{m-i}}) \equiv 0$ mod 1, $i = 1, \ldots, m$ q.e.d.

4.4. <u>Corollary</u>.

The formal groups $F_t$ and $F_{t'}$, over A are isomorphic if and only if $t_i \equiv t_i'$ mod p.

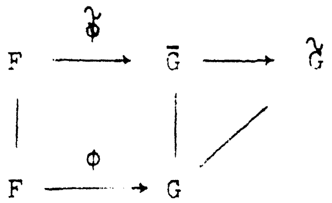
<u>Proof</u>. We need only prove that if $F_t$ and $F_{t'}$ are isomorphic then $t_i \equiv t_i'$. Let $\phi(X) = uX + u_2X^2 + \ldots$, u a unit of A, be the isomorphism. $\phi(X)$ can we written as $\phi = \psi \circ \chi$ where $\chi(X) = uX$ and $\psi$ is a strict isomorphism between $G(X,Y) = u^{-1}F_t(uX,uY)$ and $F_{t'}(X,Y)$. The logarithm of G is $g(X) = u^{-1}f_t(uX)$. It follows that $g(X) = f_{t''}(X)$ where $t_i'' = u^{p^i-1}t_i$, and as $u^{p^i-1} \equiv 1$ mod p, we find $t_i'' \equiv t_i$ mod p. Also $t_i'' \equiv t_i'$ mod p according to (4.3). Therefore $t_i \equiv t_i'$ mod p.

4.5. <u>Corollary</u>.

Two p-typical formal groups over $Z/(p)$ are (strictly) isomorphic if and only if they are identical.

Proof. Let $F, G$ be two p-typical formal groups over $Z/(p)$. Let $\tilde{F}$ be a formal group over $Z_p$ which lifts $F$. Let $\phi$ be an isomorphism between $F, G$ and let $\tilde{\phi}$ be any power series over $Z_p$ without constant term which lifts $\phi$. Define

$\bar{G}(X,Y) = \tilde{\phi}^{-1}\tilde{F}(\tilde{\phi}X, \tilde{\phi}Y)$. Now render $\bar{G}$ p-typical using (4.1.4). Let $\tilde{G}$ be the result. Then $\tilde{G}$ also reduces to $G$ (because $G$ is already p-typical).



Let $\tilde{F} = F_t$, $\tilde{G} = F_{t'}$. Then $t_i \equiv t_i'$. It follows that $F = G$. Cf. lemma below. (N.B. $\phi$ need not be the identity).

q.e.d.

4.6. Lemma.

Let A be a characteristic zero $Z_{(p)}$-integral domain. The reductions mod p of $F_t$ and $F_{t'}$ are identical iff $t_i \equiv t_i'$, $i = 1, 2, \ldots$

Proof. The coefficients of $F_T(X,Y)$ are polynomials in $T_1, T_2, \ldots$; and

$F_{(T_1, \ldots, T_r, 0, 0, \ldots)}(X,Y)$ and $F_T(X,Y)$ differ by

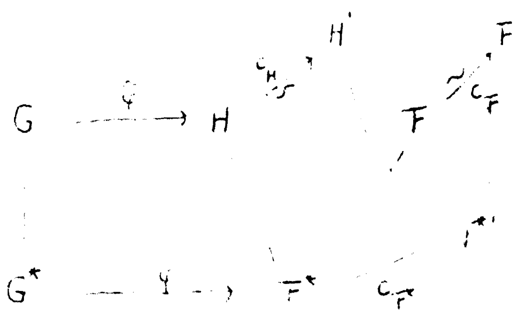
$\frac{T_r}{p}[(X + Y)^{p^r} - X^{p^r} - Y^{p^r}]$ mod degree $p^r + 1$.

Remark. This lemma does not hold for the groups $H_T(X,Y)$ discussed in section 2.

4.7. Corollary (Cartier [1], Hill [6])

Two formal groups over $Z_{(p)}$ or $Z_p$ (or any ring in between) are isomorphic iff their reductions mod p are isomorphic.

Proof. Let the reductions $F^*$ and $G^*$ of $F$ and $G$ be isomorphic. Let $F' = c_F^{-1}(F(c_F(X), c_F(Y)))$, where $c_F$ is as in (4.1.4). Then $F'$ is p-typical. The reduction of $c_F$ mod p is $c_{F^*}$. (This follows from (4.1.4)).




Let $\phi(X)$ be the isomorphism between $G^*$ and $F^*$, let $\tilde{\phi}(X) = uX + u_2X^2 + \ldots$, u a unit be any lift of $\phi(X)$. Let $H(X,Y) = \tilde{\phi}^{-1}G(\tilde{\phi}(X), \tilde{\phi}(Y))$. Then H reduces to $F^*$. It follows that the reduction of $c_H$ is $c_{F^*}$. Let $H'(X,Y) = c_H^{-1}H(c_H(X), c_H(Y))$. The formal groups H' and F' are both p-typical and have the same reduction. It follows that they are isomorphic ((4.6), (4.3)). And as $\tilde{\phi}$, $c_H$ and $c_F$ are isomorphisms, F and G are also isomorphic.

4.8. Remark. If $F^*$ and $G^*$ are strictly isomorphic then F and G are strictly isomorphic. (Take $\tilde{\phi}(X) = X + u_2X^2 + \ldots$).

4.9. Corollary.

Two formal groups over Z are isomorphic if they are isomorphic mod p for all primes p.

## 5. TWO COUNTEREXAMPLES.

The results of (4.3) - (4.9) do not seem to be generalizable. More precisely: let k be a field of characteristic p which is not equal to Z/(p). Then there are one dimensional p-typical formal groups over W(k) with the same reduction which are not isomorphic. Cf. (5.1) below. The corollary (4.5) is also false over k (also for strict isomorphisms).

Finally two more dimensional formal groups over $Z_{(p)}$ or $Z_p$ with the same reductions need not be isomorphic. Cf. (5.2).

5.1. Example.

Let $F_9 = k$, the field of 9 elements; $W(k) \simeq Z_3(i)$, where $i^2 = -1$. Let $t_1 = 0$, $t_2 = i$, $t_3 = 0$, $t_4 = 0, \ldots, t_n = 0, \ldots$;

$t_1' = 3i$, $t_2' = i$, $t_3' = 0, \ldots, t_n' = 0, \ldots$

Consider the formal groups $F_t$ and $F_{t'}$ over $Z_3(i)$.

(i) The formal groups $F_t$ and $F_{t'}$ are not strictly isomorphic over $Z_3(i)$. Indeed, if they were there would be elements $s_1, s_2, \ldots \in Z_3(i)$ such that $F_{t'} = F_{t,s}$ or, equivalently, $f_{t'} = f_{t,s}$. Then we must have $s_1 = i$. Looking at the coefficients of $X^{27}$ we see that there must be an $s_2, s_3 \in Z_3(i)$ such that (cf. (4.3)).

$$(5.1.1)\quad \frac{t_3'}{p} + a_1\frac{(t_2')^p}{p} + a_2\frac{(t_1')^{p^2}}{p} = \frac{t_3}{p} + a_1\frac{t_2^p}{p} + a_2\frac{t_1^{p^2}}{p^2} + \frac{t_1}{p}\,\frac{t_1^p s_1^{p^2} - s_1^p t_1^{p^2}}{p} + \frac{t_1 s_2^p - s_2 t_1^{p^2}}{p} + \frac{t_2 s_1^{p^2} - s_1 t_2^p}{p} + s_3$$

where $p = 3$, $f_{t'}(X) = \sum_{i=0}^{\infty} a_i X^{p^i}$, $a_0 = 1$. Because $t_1 = 0$ and $t_i' \equiv t_i \bmod p$, this implies that

$t_2 s_1^{p^2} - s_1 t_2^p \equiv 0 \bmod p$ which is not the case.

(ii) The formal groups $F_t$ and $F_{t'}$ are not isomorphic over $Z_3(i)$. Every isomorphism $\phi(X) = uX + u_2X^2 + \ldots$, $u$ a unit of $Z_3(i)$ can be decomposed as $\phi = \psi \circ \chi$ where $\chi(X) = uX$ and $\psi(X) = X + \ldots$ is a strict isomorphism. Let $G(X,Y) = \chi^{-1}F(\chi X, \chi Y)$. The logarithm of $G$ is $f_{t''}(X)$, where $t_1'' = 0$, $t_2'' = u^{p^2-1}t_2$, $t_3'' = 0, \ldots, t_n'' = 0, \ldots$ The groups $G(X,Y)$ are strictly isomorphic. There must therefore be $s_1, s_2, \ldots \in Z_3(i)$ such that $f_{t'',s}(X) = f_{t'}(X)$. This gives $s_1 = i$. As above (5.1.1) must hold (with $t_i$ replaced by $t_i''$). Now $u^{p^2-1} \equiv 1 \bmod p$ because the residue field has $p^2$ elements. It follows that $t_2'' \equiv t_2 \bmod p$, and therefore we must have $t_2'' s_1^{p^2} - s_1 t_2''^p \equiv 0 \bmod p$, which is not the case because $t_2'' \equiv i \bmod p$ and $s_1 = i$.

5.2. Example.

We work over $Z_p$ or $Z_{(p)}$. Let the matrices $t_i$, $t_i'$ be given by

$$t_1 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \; t_2 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \; t_3 = 0, \ldots, t_n = 0, \ldots$$

$$t_1' = \begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix}, \; t_2' = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \; t_3 = 0, \ldots, t_n = 0, \ldots$$

We consider the 2-dimensional formal groups $F_t$ and $F_{t'}$ over $Z_{(p)}$ or $Z_p$.

(i) The formal groups $F_t$ and $F_{t'}$ are not strictly isomorphic over $Z_p$. If they were strictly isomorphic there must be matrices $s_1, s_2, \ldots$ such that $F_{t'} = F_{t,s}$. We find $s_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and comparing the coefficients of $X^{p^2}$ in $f_{t'}(X)$ and $f_{t,s}(X)$ we see that

$$p^{-2}\begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} + s_2 + p^{-1}\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\} =$$

$$= p^{-2}\begin{pmatrix} 1 & p \\ p & 0 \end{pmatrix}\begin{pmatrix} 1 & p^p \\ p^p & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

for a certain $s_2$ with coefficients in $Z_p$. Contradiction.

(ii) The formal groups $F_t$ and $F_{t'}$ are not isomorphic over $Z_p$.

Every isomorphism is of the form $uX + \ldots$ where $u$ is an invertivle $2 \times 2$ matrix. Decompose $\phi$ as $\psi \circ \chi$ where $\chi(X) = uX$ and $\psi$ is a strict isomorphism. Let $G(X,Y) = u^{-1}F_t(uX,uY)$ The logarithm of $G$ is then $g(X) = u^{-1}f_t(uX)$. $G$ is not a p-typical group in general. Rendering $G$ p-typical gives a formal group $G'$ with logarithm $g'(X) = X + u^{-1}a_1^*u^{(1)}X^p + u^{-1}a_2^*u^{(2)}X^{p^2} + \ldots$ if $f_t(X) = X + a_1^*X^p + a_2^*X^{p^2} + \ldots$ where $u^{(i)}$ is the matrix $u^{(i)} = (u_{j\ell}^{p^i})$. The formal groups $G'$ and $F_{t'}$ are strictly isomorphic. This means that we must have

(5.2.1) $$u^{-1}a_1^*u^{(1)} \equiv a_1 \mod 1$$

if $f_{t'}(X) = X + a_1X^p + a_2X^{p^2} + \ldots$ Let $u = \begin{pmatrix} b & c \\ d & e \end{pmatrix}$, because $u^{(1)} \equiv u \mod p$

we see that we must have

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} b & c \\ d & e \end{pmatrix} \equiv \begin{pmatrix} b & c \\ d & e \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \mod p$$

This gives $c \equiv d \equiv 0 \mod p$. Let $g'(X) = f_{t''}(X)$. We calculate $t''_1$, $t''_2$. This gives

$$t''_1 \equiv \det(u)\begin{pmatrix} eb^p & 0 \\ -pd'b^p & 0 \end{pmatrix} \mod p^2, \quad \text{where } pd' = d$$

Therefore

$$t''_1 \equiv \begin{pmatrix} 1+py & 0 \\ pz & 0 \end{pmatrix} \mod p^2 \qquad y,\ z \in Z_p$$

$$t''_2 \equiv \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \mod p$$

There must be matrices $s_1$, $s_2$ such that

$$a_1 \frac{t_1''^{(1)}}{p} + \frac{t''_2}{p} + \frac{t''_1 s_1^{(1)} - s_1 t_1''^{(1)}}{p} + s_2 = a_1 \frac{t_1'^{(1)}}{p} + \frac{t'_2}{p}$$

Because $t''_1 \equiv t'_1 \mod p$ and $t''_2 \equiv t_2 \mod p$, this implies

(5.2.2) $$t''_1 s_1^{(1)} - s_1 t_1''^{(1)} \equiv 0 \mod p$$

Now

$$s_1 = \begin{pmatrix} 0 & 1 \\ 1-z & 0 \end{pmatrix},\ t''_1 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \mod p$$

which contradicts (5.2.2)

REFERENCES.


[1]. Cartier, P (1971), Groupes Formels, Fonctions automorphes et Fonctions zeta des Courbes Elliptiques. Actes du Congrès International des Mathématiciens, Nice 1970. Tome 2, 291-299 Gauthier Villars.

[2]. Cartier, P (1967), Modules Associés à un Groupe Formel Commutatif. Courbes Typiques. C.R. Acad. Sc. Paris 265, Serie A, 129-132.

[3]. Cartier, P. (1971), Relèvement des Groupes Formels Commutatifs. Séminaire Bourbaki, exposé 359 (Lecture notes in Mathematics 179, Springer.)

[4]. Hazewinkel, M., Constructing Formal Groups I : over $Z_{(p)}$-algebras. Report 7119 and 7119 (appendix) of the Econometric Institute, Netherlands School of Economics, Rotterdam.

[5]. Hazewinkel, M., Constructing Formal Groups. II: over Z-algebras. Report 7201 of the Econometric Institute, Netherlands School of Economics, Rotterdam.

[6]. Hill, W.L., (1971), Formal Groups and Zeta-Functions of Elliptic Curves. Inv. Math. 12, 321-336.

[7]. Honda, T. (1970), On the Theory of Commutative Formal Groups. J. Math. Soc. Japan 22, 213-245.

[8]. Serre, J.P. (1962), Corps Locaux. Hermann.

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