ERASMUS UNIVERSITEIT ROTTERDAM
ECONOMETRISCH INSTITUUT

Report 7519/M

CONSTRUCTING FORMAL GROUPS VI: CARTIER'S THIRD THEOREM AND INVOLVED PAIRS OF FUNCTIONS.

by Michiel Hazewinkel

Part of the work on this paper was done while the author enjoyed the hospitality of the Math. Inst. of the Univ. of Göttingen in November 1975.

Nov. 23rd, 1975 Preliminary

CONSTRUCTING FORMAL GROUPS VI: CARTIER'S THIRD THEOREM AND INVOLVED PAIRS OF FUNCTIONS

by Michiel Hazewinkel

Contents.

1. INTRODUCTION.

Let A be a commutative ring with unit element. We denote with $\underline{Gf}_A$ the category of finite dimensional commutative formal groups over A. To A one associates a certain (in general) noncommutative ring Cart(A) and one then has the curve functor: $G \to \mathcal{C}(G)$, which associates to a finite dimensional formal group G the left Cart(A) module of curves in G. According to theorems 2 and 3 of [3], this functor induces an equivalence of categories of the category of formal groups over A with a certain full subcategory of Cart(A)-modules. Proofs of theorems 2 and 3 can be found in [6], [7]; a different proof of theorem 3 is contained in [1], c.f. also [2]. It is the purpose of the present note to give still another proof of this theorem 3, based on the functional equation techniques which were developped in the earlier parts of this series of papers [4]; at the same time we give the connection between the involved function pair techniques of Ditters [1], [2] and our own functional equation techniques, cf. 2.6 and 2.7 below.

The local case, where A is a $\mathbb{Z}_{(p)}$-algebra and where one replaces Cart(A) with $\mathrm{Cart}_p(A)$, was dealt with in [4] part IV, cf also 2.14 below.

2. THE MODULE OF CURVES OF A FORMAL GROUP.

From now on formal group means finite dimensional commutative formal group over A. We take the naive or power series point of view, i.e. an n-dimensional commutative formal group G is an n-tupel of power series G(X,Y) in 2n-variables $X_1, \ldots, X_n; Y_1, \ldots, Y_n$ such that

$G(X,0) = X$, $G(0,Y) = Y$ and such that $G(X,G(Y,Z)) = G(G(X,Y),Z)$, $G(X,Y) = G(Y,X)$.

2.1. Curves.

A curve in a formal group G is an n-tupel of power series $\gamma(T) = (\gamma^1(T), \ldots, \gamma^n(T))$ in one variable T such that $\gamma^i(0) = 0$, $i = 1, \ldots, n$; i.e. the constant terms are zero.
Two curves can be added by means of the formula $(\gamma +_G \delta)(T) = G(\gamma(T), \delta(T)) = \gamma(T) +_G \delta(T)$. This turns the set of curves in G into an abelian group which is denoted $\mathfrak{C}(G)$.

2.2. The Operators $[a]$, F_n, V_n.

In addition to the group structure on $\mathfrak{C}(G)$ one has a number of operators on $\mathfrak{C}(G)$ which are compatible with the group structure. Viz.:

for every $a \in A$, $([a]\,\gamma)(T) = \gamma(aT)$

for every $n \in \mathbb{N}$, $(V_n\gamma)(T) = \gamma(T^n)$

The definition of the third kind of operator, the frobenius's F_n needs a bit more care; formally one has

$$\text{for every } n \in \mathbb{N},\ F_n\gamma(T) = \gamma(\zeta_n T^{1/n}) +_G \cdots +_G \gamma(\zeta_n^n T^{1/n})$$

where ζ_n is a primitive n-th root of unity. For a more precise definition cf. [4] part IV, or [7].
There are various (obvious) relations among these operators; cf. [3], [6], [7]; cf also 2.11 and 2.12 below.
The operators $[a]$, F_n, V_n are all elements of a certain ring Cart(A). The elements of Cart(A) are expressions $\Sigma V_n[a_{n,m}]F_m$ which are multiplied and added according to certain rules. Cf. [6].

2.3. A V-basis for $\mathfrak{C}(G)$.

Let $\gamma_i(T)$ denote the curve $(0,\ldots,0,T,0,\ldots,0)$ in G, where the T is the i-th spot. Then it is immediately clear that every curve in G can be uniquely written as a sum

$$\delta = \sum_{i=1}^{n} \sum_{k=1}^{\infty} V_k[a_{ik}]\gamma_i$$

It follows that we know the Cart(A) module structure of (G) if we know the expressions

$$F_p\gamma_i = \sum_{j,r} V_r[c(p,r,j,i)]\gamma_j$$

for all prime numbers p. (Because $F_nF_m = F_{nm}$ for all $n,m \in \mathbb{N}$, $F_1 = \mathrm{id}$).
The elements $c(p,r,j,i) \in A$ cannot be chosen arbitrarily. They have to satisfy certain relations.

2.4. <u>On the Relations between the Structure Constants c(p,r,j,i)</u>.

To find out what the relations between the c(p,r,j,i) are suppose for the moment that A is a characteristic zero ring, i.e. that $A \to A \otimes \mathbb{Q}$ is injective. Then the formal group G has a logarithm $g(x) = (g_1(X), \ldots, g_n(X))$ i.e. $G(X,Y) = g^{-1}(g(X) + g(Y))$.
Suppose that

$$g_i(\gamma_j(T)) = \sum_{r=1}^{\infty} a_{ij,r}T^r$$

By the definition of F_p, cf. 2.2 above, we then have

$$g(F_p(\gamma_i(T)) = g(\gamma_i(\zeta_p T^{1/p})) + \ldots + g(\gamma_i(\zeta_p^p T^{1/p}))$$

And the ℓ-th component of this is therefore eqũal to

$$(2.4.1) \qquad \sum_{s=1}^{p} \sum_{r=1}^{\infty} a_{\ell,i,r}\zeta_p^s X^{r/p} = p \sum_{m=1}^{\infty} a_{\ell,i,pm}T^m$$

On the other hand we have that

$$g(\Sigma^G V_r[c(p,r,j,i)]\gamma_j(T)) = \sum_{j,r} g(\gamma_j(c(p,r,j,i)T^r))$$

and the ℓ-th component of this is equal to

$$(2.4.2) \qquad \sum_{j,r,s} a_{\ell,j,s}c(p,r,j,i)^s T^{rs}$$

Comparing c oefficients in (2.4.1) and (2.4.2) we see that

$$(2.4.3) \qquad p\, a_{\ell,i,pm} = \sum_{rs=m,j} a_{\ell,j,s}c(p,r,j,i)^s$$

Let $a(m)$ denote the $n \times n$ matrix $a(m)_{i,j} = a_{i,j,m}$, and let $c(p,r)$ be the $n \times n$ matrix $c(p,r)_{ij} = c(p,r,i,j)$. We use $c(p,r)^{(k)}$ to denote the matrix with (i,j)-th element $(c(p,r)_{ij})^k$. Then (2.4.3) says

$$(2.4.4) \qquad p\, a(pm) = \sum_{r|m} a_{m/r} c(p,r)^{(m/r)}$$

and writing $b(m) = ma(m)$ we obtain

$$(2.4.5) \qquad b(pm) = \sum_{r|m} rb(m/r)c(p,r)^{(m/r)}, \quad b(1) = I_n$$

Now let A be a ring, which is not necessarily of characteristic zero. Then there is a formal group G' over a characteristic zero ring A' and a homomorphism $\pi: A' \to A$ such that $G'^{\pi} = G$, and hence also $\pi(c'(p,r,j,i)) = c(p,r,j,i)$. Because $ma'(m) \in A'$ we obtain also in the case of a non characteristic zero ring A, that there exists a function b with values in the $n \times n$ matrices with coefficients in A such that (2.4.5) holds.

2.5. Involved Function Pairs.

Let $\mathfrak{M}(n,A)$ denote the set of $n \times n$ matrices with coefficients in A, and let P denote the set of prime numbers. An involved function pair is a couple of functions (b,c), $b : \mathbb{N} \to \mathfrak{M}(n,A)$ $c: P \times \mathbb{N} \to \mathfrak{M}(n,A)$ such that (2.4.5) holds for every $p \in P$ and $m \in \mathbb{N}$. We have just shown that an formal group G gives rise to a pair of involved functions (b,c). Inversely we shall show that every pair of involved functions (b,c) comes from a formal group.

Let $C(p,m)_{ij}$ and $B(r)_{ij}$ be indeterminates for $i,j = 1, \ldots, n$; $r = 2,3,\ldots$; $m = 1,2,\ldots$; $p \in P$.

Let $L' = \mathbb{Z}[\ldots, C(p,m)_{i,j},\ldots; \ldots,B(r)_{ij},\ldots]$ and let $\mathfrak{a}$ be the ideal of L' generated by the relations

$$B(pm) = \sum_{r|m} rB(m/r)C(p,r)^{m/r}$$

Let $L = L'/\mathfrak{a}$. Then there is an obvious one-one correspondence between pairs of involved functions and homomorphisms $L \to A$.

2.6. The Universal Curvilinear n-dimensional Formal Group.

For each $i,j = 1,2,\ldots,n$; $r = 2,3,\ldots$ let $R_r(i,j)$ be an indeterminate. We write $\mathbb{Z}[R]$ for $\mathbb{Z}[\ldots,R_r(i,j),\ldots]$. Then there is defined over $\mathbb{Z}[R]$ a curvilinear formal group $H_R(X,Y)$ which is universal for n-dimensional commutative curvilinear formal groups, cf. [5] and also 3.2 below.
According to 2.4 and 2.5 above this formal group gives rise to homomorphism

$$\vartheta : L \to \mathbb{Z}[R] \tag{2.6.1}$$

2.7. Theorem.

Every pair of involved functions comes from a formal group. More precisely the homomorphism ϑ is an isomorphism and if $\phi: L \to A$ defines a pair of involved functions, then $F_R^{\phi\vartheta^{-1}}(X,Y)$ is a formal group over A which gives rise to the pair of involved functions determined by $\phi: L \to A$.

The proof of this theorem will be given in section 3 below. The notion of an involved pair of functions is due to Ditters [1], [2] and another proof (via the dual category)(of the first part) of this theorem can be found in [1], [2].

2.8. Addendum.

If $n = 1$ and A is a characteristic zero ring, then the $b(r)$ determine the logarithm of the corresponding formal group and we get a 1 - 1 correspondence between one dimensional formal groups and one dimensional pairs of involved functions. This is still true for arbitrary A.
If $n > 1$, then there is more than one formal group giving rise to the same pair of involved functions, but there is a unique curvilinear formal group corresponding to each pair of involved functions.

2.9. Reduced Cart(A)-modules.

If $\mathfrak{C}(G)$ is the module of curves of a formal group G, then, cf. also above, it is clear that $\mathfrak{C}(G)$ has the following properties:

1^o There are subgroups C_n, closed under the operators $[a]$, V_m.
(C_n is the subgroup of all curves $\gamma(T) = (\gamma^1(T), \ldots, \gamma^n(T))$ such that $\gamma^i(T) \equiv 0 \bmod T^n$ for all i)

2^o The subgroups C_n define a topology on $\mathfrak{C}(G)$; $\mathfrak{C}(G)$ is complete for this topology and C_n is the smallest closed subgroup of $\mathfrak{C}(G)$ such that $V_m\mathfrak{C}(G) \subset C_n$ for all $m \geq n$.

3^o There are elements $\gamma_1, \ldots, \gamma_n \in \mathfrak{C}(G)$ such that every element γ in $\mathfrak{C}(G)$ can be uniquely written as a convergent sum

$$\gamma = \sum_{r=1}^{\infty} \sum_{j=1}^{n} V_r[a_{r_j}]\gamma_j$$

Such a set of elements is called a V-basis for $\mathfrak{C}(G)$.

4^o The operators F_m, $V_r[a]$ are all continuous.

In general we shall call a Cart(A)-module which enjoys the four properties listed above a <u>reduced</u> Cart(A)-module. Thus we have seen that formal groups give rise to reduced Cart(A)-modules.

2.10. <u>Reduced Cart(A)-modules and Involved Pairs of Functions</u>.

Let C be a reduced Cart(A)-module. Let $\gamma_1, \gamma_2, \ldots, \gamma_n$ be a V-basis for C. Then for every $m \in \mathbb{N}$ we have an expression.

$$\text{(2.10.1)} \qquad F_m\gamma_i = \sum_{r=1}^{\infty} \sum_{j=1}^{n} V_r[c(m,r,j,i)]\gamma_j$$

Now define

$$\text{(2.10.2)} \qquad c(p,r)_{ij} = c(p,r,i,j) \ , \ p \in P; \ r \in \mathbb{N}; \ i,j = 1, \ldots, n$$

$$\text{(2.10.3)} \qquad b(m)_{ij} = c(m,1,i,j) \ , \ m \in \mathbb{N}; \ i,j = 1, \ldots, n$$

Then we claim that the pair of functions $c(p,r)$, $b(m)$ defined by (2.10.1) - (2.10.3) is an involved pair of functions. To prove this we need a lemma.

2.11. <u>Lemma</u>.

Let C be a reduced Cart(A)-module and fix $m \in \mathbb{N}$. Then we have that $F_mV_r\gamma \equiv 0 \bmod C_2$ unless $r|m$ and then $F_mV_r\gamma \equiv [r]F_{m/r}\gamma \bmod C_2$.

Proof. We shall use the following relations which hold in Cart(A).

$F_mV_r = V_rF_m$ if $(r,m) = 1$, $V_1 = F_1 = id_{Cart(A)} = [1]$

$F_mF_r = F_rF_m = F_{rm}$, $V_mV_r = V_rV_m = V_{rm}$ for all $r, m \in \mathbb{N}$ (2.11.1)

$F_mV_m = m\, id_{Cart(A)}$, i.e. $F_mV_m\gamma = \gamma + \ldots + \gamma$ (m times)

$[a] + [b] = \sum_{n=1}^{\infty} V_n s_n(a,b) F_n$, where the $s_n(a,b)$ are certain polynomials in a and b and $s_1(a,b) = a + b$

Now let $d = (r,m)$ and suppose that $d < r$. Then we have

$$F_mV_r\gamma = F_{m/d}F_dV_dV_{r/d}\gamma = dF_{m/d}V_{r/d}\gamma = dV_{r/d}F_{m/d}\gamma \equiv 0 \mod C_2$$

because $r/d > 1$.

Now let $r|m$, then we have

$$F_mV_r\gamma = F_{m/r}F_rV_r\gamma = rF_{m/r}\gamma \equiv [r]F_{m/r}\gamma \mod C_2$$

2.12. Proof that (2.10.1)-(2.10.3) define an Involved Pair of Functions.

We shall need two more of the relations that hold in Cart(A); viz.

$$(2.12.1) \qquad \begin{aligned} [a][b] &= [ab] \\ F_m[c] &= [c^m]F_m \end{aligned}$$

Now if C is a reduced Cart(A) module then it follows from the third property listed in 2.9 above that C/C_2 is a free A-module of rank n with as basis the classes mod C_2 of the V-basis $\gamma_1, \ldots, \gamma_n$. And by (2.10.3) we know that the b(m) are determined by the $F_m\gamma_i$ mod C_2.

We have

$$(2.12.2) \qquad F_mF_p\gamma_i = F_{mp}\gamma_i \equiv \sum_{k=1}^{n} b(mp)_{k,i}\gamma_k$$

On the other hand

$$
\begin{aligned}
F_m F_p \gamma_i &= F_m\Big(\sum_{r=1}^{\infty}\sum_{j=1}^{n} V_r[c(p,r,j,i)]\gamma_j\Big) \\
&= \sum_{r=1}^{\infty}\sum_{j=1}^{n} F_m V_r[c(p,r,j,i)]\gamma_j \\
&\equiv \sum_{r|m}\sum_{j=1}^{n} [r]F_{m/r}[c(p,r,j,i)]\gamma_j \\
&= \sum_{r|m}\sum_{j=1}^{n} [rc(p,r,j,i)^{m/r}]F_{m/r}\gamma_j \\
&\equiv \sum_{r|m}\sum_{j=1}^{n} [rc(p,r,j,i)^{m/r}]\sum_{k=1}^{n} b(m/r)_{k,j}\gamma_k \\
&\equiv \sum_{k=1}^{n}\Big(\sum_{r|m}\sum_{j=1}^{n} [rc(p,r,j,i)^{m/r}b(m/r)_{k,j}]\Big)\gamma_k
\end{aligned}
$$

where all congruences are modulo C_2. A comparison of the result of this calculation with (2.12.2) now gives that the $c(p,r)$ and $b(m)$ do indeed constitute a pair of involved functions.

2.13. Theorem (Cartier's Third Theorem).

For every reduced Cart(A)-module C there is a formal group G over A such that $\mathfrak{C}(G) \simeq C$ (as Cart(A)-modules).

This follows from theorem 2.7 and the results above 2.9 - 2.12.

2.14. The Local Case.

In this subsection A is a $\mathbb{Z}_{(p)}$-algebra. In this case one defines a much smaller ring $\mathrm{Cart}_p(A)$ of which the elements are expressions $\Sigma\, V_p^r[a_{rs}]F_p^s$. A curve $\gamma \in \mathfrak{C}(G)$ in a formal group G is called p-typical if $F_q\gamma = 0$ for all prime numbers $q \neq p$. These curves form a subgroup of $\mathfrak{C}(G)$ which is denoted $\mathfrak{C}_p(G)$ and $\mathfrak{C}_p(G)$ is a $\mathrm{Cart}_p(A)$ module. A reduced $\mathrm{Cart}_p(A)$-module is described by a set of n-relations (where n is the number of elements in a V-basis)

$$F_p\gamma_i = \sum_{r=1}^{\infty}\sum_{j=1}^{n} V_r[c(r,j,i)]\gamma_j$$

and one can choose the c(r,j,i) arbitrarily. Given a set of c(r,j,i), it is easy to write down a p-typical n-dimensional formal group such that its module of p-typical curves is described by (2.14.1). This is done in [4] part IV.

3. PROOF OF THEOREM 2.7

The basic idea of the proof is to use relations (2.4.5) to write $a(m) := m^{-1}b(m)$ in such a way that the series $\Sigma a(m)X^m$, where X^m is short for the columnvector $(X_1^m, \ldots, X_n^m)$, is seen to satisfy the functional equation of [5], section 3.1. This of course makes sense only when the c(p,1) and b(m) have their coefficients in a characteristic zero ring.

3.1. Solutions of the Involved Function Equations in Characteristic Zero.

Let A be a characteristic zero ring; i.e. $A \to A \otimes \mathbb{Q}$ is injective. Let ϕ: $L \to A$ be a homomorphism and let $b(m)_{ij}$ and $c(p,r)_{ij}$ be the images of $B(m)_{ij}$, $C(p,r)_{ij} \in L$. Define the matrix a(m) as $a(m) = m^{-1}b(m)$. Choose a prime number p and choose an ordening of the prime numbers $p_1, p_2, p_3, \ldots$ such that $p = p_1$. Choose $m \in \mathbb{N}$, $m > 1$ and write $m = p_1^{r_1} \cdots p_t^{r_t}$ with $r_1, \ldots, r_{t-1} \geq 0$ and $r_t \geq 1$. Then we have

$$a(m) = \Sigma \frac{c(p_1,d(1,1))^{(e(1,1))} \cdots\cdots c(p_1,d(1,s_1))^{(e(1,s_1))}}{p_1^{s_1}} \cdot \cdots \tag{3.1.1}$$

$$\cdot \frac{c(p_t,d(t,1))^{(e(t,1))} \cdot \cdots \cdot c(p_t,d(t,s_t))^{(e(t,s_t))}}{p_t^{s_t}}$$

where the sum is over all sequences

$$(p_1,d(1,1)), \ldots, (p_1,d(1,s_1)); \ldots ; (p_t,d(t,1)), \ldots, (p_t,d(t,s_t))$$

such that

1^o $p_1 d(1,1) \cdot \ldots \cdot p_1 d(1,s_1) \cdot \ldots \cdot p_t d(t,1) \cdot \ldots \cdot p_t d(t,s_t) = m$

2^o $s_1, \ldots, s_{t-1} \geq 0,\ s_t \geq 1$

3^o $d(i,j)$ involves only prime numbers $p_1, \ldots, p_i$,
and the exponents $e(i,j)$ are given by the formula

4^o $e(i,j) = p_1 d(1,1) \cdot \ldots \cdot p_1 d(1,s_1) \cdot \ldots \cdot p_i d(i,1) \cdot \ldots \cdot p_i d(i,j-1)$.

where a product $p_1 d(k,1) \cdot \ldots \cdot p_1 d(k,s_k)$ is to be interpreted as 1 if $s_k = 0$. (Asimilar convention holds in the formula for a(m)).
For example

$$a(p_1 p_2^2) = \frac{c(p_1,1)}{p_1} \frac{c(p_2,1)^{(p_1)} c(p_2,1)^{(p_1 p_2)}}{p_2^2} + \frac{c(p_2,p_1) c(p_2,1)^{(p_2 p_1)}}{p_2^2} + $$

$$+ \frac{c(p_1,1)}{p_1} \frac{c(p_2,p_2)^{(p_1)}}{p_2} + \frac{c(p_2,1) c(p_2,p_1)^{(p_2)}}{p_2^2} + \frac{c(p_2,p_2 p_1)}{p_2}$$

where the various sequences and exponents are

$(p_1,1),\ (p_2,1),\ (p_2,1)$	$1,\ p_1,\ p_1 p_2$
$(p_1,1)(p_2,p_2)$	$1,\ p_1$
$(p_2,1)(p_2,p_1)$	$1,\ p_2$
$(p_2,p_1)(p_2,1)$	$1,\ p_1 p_2$
$(p_2,p_2 p_1)$	1

Formula (3.1.1) is not difficult to prove. One simply writes

$a(m) = a(rp_t)$, with $r = mp_t^{-1}$ and

$$a(m) = m^{-1} b(m) = m^{-1} \sum_{d|r} d\ b(r/d) c(p_t,d)^{(r/d)} =$$

$$= \sum_{d|r} a(r/d) \frac{c(p_t,d)^{(r/d)}}{p_t}$$

And now one uses induction on the a(r/d).

3.2. Curvilinear Formal Groups.

If $\underline{\underline{k}}$ and $\underline{\underline{\ell}}$ are multiindices of length n we define

$\underline{\underline{k}}\underline{\underline{\ell}} = (k_1\ell_1,\dots,k_n\ell_n)$, $|\underline{\underline{k}}| = k_1 + \dots + k_n$, and $\underline{\underline{0}} = (0,0,\dots,0)$.
An n-dimensional formal group $G(X,Y)$,
$G_j(X,Y) = X_j + Y_j + \sum_{|\underline{\underline{\ell}}|,|\underline{\underline{k}}|>1} a_{\underline{\underline{k}},\underline{\underline{\ell}}}(j)X^{\underline{\underline{k}}}Y^{\underline{\underline{\ell}}}$ is said to be <u>curvilinear</u>
([6]) if the following holds

$$(3.2.1)\qquad |\underline{\underline{k}}|,\ |\underline{\underline{\ell}}| \geq 1 \text{ and } \underline{\underline{k}}\underline{\underline{\ell}} = \underline{\underline{0}} \Rightarrow a_{\underline{\underline{k}},\underline{\underline{\ell}}}(j) = 0 \text{ for } j = 1, \dots, n$$

If $G(X,Y)$ is a formal group over a characteristic zero ring and $g(X)$ is its logarithm, then $G(X,Y)$ is curvilinear iff $g(X)$ is of the form

$$(3.2.2)\qquad g(X) = \sum_{m=1}^{\infty} a(m)X^m, \qquad a(1) = I_n$$

for certain matrices $a(m)$, where X^m is short for the column vector $(X_1^m, \dots, X_n^m)$.
Every formal group over a ring A is isomorphic to a curvilinear one, and there exists a universal curvilinear formal group defined over $\mathbb{Z}[R] = \mathbb{Z}[\dots,R(m)_{i,j},\dots;\ m = 2,3,\dots;i,j = 1,\dots,n]$ which we shall denote $H_R(X,Y)$.
For all these facts cf. [5].

3.3. <u>Local Variants of</u> L.

Choose a prime number p and choose an ordering $p_1, p_2, p_3,\dots$ of the prime numbers with $p = p_1$. For each pair (p_i,d), such that d involves only the primes $p_1, \dots, p_i$ take n^2 indeterminates $C(p_i,d)_{k\ell}$, $k,\ell = 1, \dots, n$. Let $L(\underline{<})$ be the ring $\mathbb{Z}[\dots, C(p_i,d)_{k,\ell},\dots]$. There is a natural inclusion.

$$(3.3.1)\qquad L(\underline{<}) \hookrightarrow L'$$

and hence a natural map

$$(3.3.2)\qquad L(\underline{<}) \to L' \to L = L'/\mathfrak{a}$$

For each $m \in \mathbb{N}$, $m \geq 2$, define the matrix $A(m)$ with coefficients in $L(\leq) \otimes Q$ by formula (3.1.1), replacing all small c's with the matrices of indeterminates $C(p_i,d)$. Define in addition $Q(m)$ as the sum of those terms of $A(m)$ for which $s_1 = 0$.
For example

$$(3.3.3.) \qquad Q(p_1p_2^2) = \frac{C(p_2,1)C(p_2,p_1)^{(p_2)}}{p_2^2} + \frac{C(p_2,p_1)C(p_2,1)^{(p_2p_1)}}{p_2^2} + \frac{C(p_2,p_2p_1)}{p_2}$$

We set $A(1) = Q(1) = I_n$ and define

$$(3.3.4) \qquad q(X) = \sum_{m=1}^{\infty} Q(m)X^m \qquad g_{\leq}(X) = \sum_{m=1}^{\infty} A(m)X^m$$

where X^m is short for the column vector $(X_1^m,\ldots,X_n^m)$.
Then $g_{\leq}(X)$ satisfies the following functional equation

$$(3.3.5) \qquad g_{\leq}(X) = q(X) + \sum_{i=1}^{\infty} \frac{C(p,p^{i-1})}{p} g_{\leq}^{(p^i)}(X^{p^i})$$

Let

$$(3.3.6) \qquad G_{\leq}(X,Y) = g_{\leq}^{-1}(g_{\leq}(X) + g_{\leq}(Y))$$

then it follows from the functional equation lemma ([5] 3.1) that $G_{\leq}(X,Y)$ is a formal group over $L(\leq)_{(p)}$. It is a curvilinear formal group by 3.2 above.

3.4. Proof of Theorem 2.7 in the Characteristic Zero Case.

Let A be a characteristic zero ring and $c(p,d)$, $b(m)$ an involved pair of functions with coefficients in A. We define

$$(3.4.1) \qquad g(X) = \sum_{m=1}^{\infty} m^{-1}b(m)X^m, \quad G(X,Y) = g^{-1}(g(X) + g(Y))$$

Then because of (3.1.1) $G(X,Y)$ is obtained from $G_{\leq}(X,Y)$ by specializing the $C(p_i,d)_{k\ell}$ to the $c(p_i,d)_{k\ell}$. It follows that $G(X,Y)$ has its coefficients in $A \otimes \mathbb{Z}_{(p)}$. But we have a formula (3.1.1) for every ordering of the primes. Hence $G(X,Y)$ is defined over A (and is a curvilinear formal group) Further because A is of characteristic zero the $b(m)$ determine the $c(p,r)$, cf. equation (2.4.5). It now follows from the calculations of 2.4 above that the involved function pair associated to $G(X,Y)$ is precisely the pair we started out with. This concludes the proof of theorem 2.7 in the case of characteristic zero rings.

3.5. L has no Additive Torsion.

We are now going to show that L has no additive torsion. Let $\mathbb{Z}[R]$ be the ring of the 3.2 above and $H_R(X,Y)$ the universal curvilinear n-dimensional formal group over $\mathbb{Z}[R]$. This formal group gives rise to homomorphism $\vartheta: L \to \mathbb{Z}[R]$. Take an ordening $p_1, p_2, \ldots$ of the prime numbers. The formal group $G_{\leq}(X,Y)$ over $L(\leq)_{(p)}$ is curvilinear, hence there is a unique homomorphism $\phi_{(p)} : \mathbb{Z}[R]_{(p)} \to L(\leq)_{(p)}$ such that $H_R^{\phi_{(p)}}(X,Y) = G_{\leq}(X,Y)$, and the composition $\phi_{(p)}\vartheta$ is the homomorphism $L \to L(\leq)_{(p)}$ which gives the pair of involved functions of the formal group $G_{\leq}(X,Y)$. Finally we have the natural map induced by the inclusion

$$L(\leq) \to L' \to L'/\mathfrak{a} = L$$

Consider the composed map

$$L(\leq)_{(p)} \xrightarrow{\iota_{(p)}} L_{(p)} \xrightarrow{\vartheta_{(p)}} \mathbb{Z}[R]_{(p)} \xrightarrow{\phi_{(p)}} L(\leq)_{(p)}$$

By the very construction of $G_{\leq}(X,Y)$ (and the fact that $L(\leq)_{(p)}$ is of characteristic zero) it follows that $\phi_{(p)}\vartheta_{(p)}\iota_{(p)} = \text{id}$.

We give $B(m)_{ij}$ weight $m - 1$ and $C(p,r)_{ij}$ weight $pr - 1$. All the relations generating $\mathfrak{a}$ are then homogeneous and L becomes a graded ring. We give $R(m)_{ij}$ weight $m - 1$. The homomorphisms ϑ and $\phi_{(p)}$ are then homogeneous of degree 0. It is not difficult to calculate $\phi_{(p)}(R(m)_{ij})$ modulo all elements of weight $< m-1$. Indeed $\phi_{(p)}$ must take the logarithm of $H_R(X,Y)$ into the logarithm of $G_{\leq}(X,Y)$.
A comparision of these logarithms then gives

$$\phi_{(p)}(R(m)_{ij}) \equiv p_t^{-1}\nu(m)C(p_t, p_t^{-1}m)_{ij}$$

where $m = p_1^{r_1} \cdots p_t^{r_t}$, $r_t \geq 1$, and where $\nu(m) = 1$ if m is not a power of a prime and $\nu(p_i^k) = p_i$. It follows that the induced morphisms

$$gr_{m-1}(\mathbb{Z}[R]_{(p)}) \to gr_{m-1}(L(\leq)_p)$$

are isomorphisms, and hence that $\phi_{(p)}$ is an isomorphism. It follows that $\vartheta_{(p)}$ is surjective. This can of course be done for all orderings of the primes. I.e. we have that $\vartheta: L \to \mathbb{Z}[R]$ is a homogeneous of degree 0 such that $\vartheta_{(p)}$ is surjective for all prime numbers p. But $\mathbb{Z}[R]$ has no torsion. An easy argument (using the abelian groups L/(ideal generated by expressions of weight $\geq$ m)) now shows that L has no additive torsion, and that ϑ is surjective.
Caveat: there is no homomorphism $\phi: \mathbb{Z}[R] \to L$ of which $\phi_{(p)}$ is the localization in p.

3.6. End of the Proof of Theorem 2.7.

There are now various ways to prove that ϑ is an isomorphism. One way is to remark that because L is of characteristic zero it follows that $L \otimes \mathbb{Q}$ is generated by the $B(m)_{ij}$, cf. the relations (2.4.5). It is then not difficult to calculate $\vartheta_{\mathbb{Q}}B(m)_{ij}$ modulo elements of weight < m-1, because $\vartheta_{\mathbb{Q}}(B(m)_{ij})$ = coefficient of X_j^m in the i-th component of $h_R(X)$, the logarithm of $H_R(X,Y)$. We find therefore cf. [5].

$$\vartheta_{\mathbb{Q}}B(m)_{ij} \equiv \nu(m)^{-1}R(m)_{ij}$$

and it follows that $\vartheta_{\mathbb{Q}}$ is injective and hence ϑ itself also, as L has no additive torsion.
Another way to prove that ϑ is an isomorphism is to apply 3.4 to the pair of involved functions given by the classes of the $C(p,d)_{ij}$ and $B(m)_{ij}$ in L. This gives a formal group over L which is curvilinear and hence a homomorphism $\psi: \mathbb{Z}[R] \to L$ because of the universality of $H_R(X,Y)$. A little reflexion then shows that $\psi\vartheta$= id because ψ must take the logarithm of $H_R(X,Y)$ into the logarithm of the formal group over L and that last logarithm is determined by the classes of the $B(m)_{ij}$.
This concludes the proof of theorem 2.7.

REFERENCES.

1. B. Ditters. Cours des Groupes Formels. Lecture Notes, Orsay 1975.
2. B. Ditters. Formale Gruppen, die Vermutungen von Atkin-Swinnerton Dyer und Verzweigte Witt Vektoren. Lecture Notes, Göttingen, 1975.
3. P. Cartier. Modules associés à un Groupe Formel Commutatif. Courbes Typiques. C.R. Acad. Sci. Paris 265 (1967), A129-132.
4. M. Hazewinkel. Constructing Formal Groups I, II, III, IV, V. Reports 7119, 7201, 7207, 7322, 7514, Econometric Inst., Erasmus University Rotterdam, 1971, 1972, 1973, 1975.
5. M. Hazewinkel. On More Dimensional Formal Groups. Report 7505, Econometric Inst., Erasmus Univ. Rotterdam, 1975.
6. M. Lazard. Sur les Théorèmes Fondamentaux des Groupes Formels Commutatifs. Indagationes Math. 35, 4 (1973), 281-300, Errata et Addenda, Ibid. 36, 2(1974), 122-124.
7. M. Lazard. Commutative Formal Groups. Springer, 1975, Lecture Notes in Math. 443.