ERASMUS UNIVERSITY ROTTERDAM

ECONOMETRIC INSTITUTE (Dept. Math)

Report 7322/M

CONSTRUCTING FORMAL GROUPS IV: WITT VECTORS AND CARTIER-DIEUDONNE MODULES.

Michiel Hazewinkel

Oct. 31, 1973

CONSTRUCTING FORMAL GROUPS IV : WITT VECTORS AND CARLIER-DIEUDONNE MODULES.

Michiel Hazewinkel*

Contents

1. INTRODUCTION

In this short note we present some complements to the constructions of [3,4,5]. In §3 we first show how the Witt vectors (of length n) associated to a prime p fit into the framework of [3], and then in §4 how the generalized Witt vectors (cf. [1] and [7]) fit into the constructions of [4]. This "requires" a rather special choice of the constants $n(q_1,\dots,q_t,d) \in Z$ which go into the definition of a universal n-dimensional commutative formal group. (Cf. (2.3)).

Choose a prime number p, and let A be a commutative $Z_{(p)}$-algebra. Let G be a commutative n-dimensional formal group over A. A curve in G (cf [2]) is simply an n-column-vector of power series in X over A without constant terms. Curves can be added using the formal group law G(X,Y) and in addition one has operators [a] for $a \in A$, V_n(= Verschiebung) for n = 1,2,... and F_n (= Frobenius) for n = 1,2,... The curves c such that $F_q c = 0$ for all $q \neq p$ constitute a subgroup $C_p(G)$, which is a left-module over a certain noncommutative topological ring $\mathrm{Cart}_{\{p\}}(A)$. (cf. [2], [6] and §5). Every element of $\mathrm{Cart}_{\{p\}}(A)$ can be uniquely written as a sum $\sum_{i,j} V_p^i[c_{ij}]F_p^j$. Now let G(X,Y) be a p-typical group law (over a $Z_{(p)}$-algebra every group law can be brought into p-typical form), and let γ_i be the curve $\gamma_i(X) = (0,\dots,X,0,\dots 0)^t$, X in the i-th place. Then it is easily seen that every element of $C_p(G)$

*) Part of the work for this note was done while the author enjoyed a CNRS grant for a month's stay at the I.H.E.S. in Bures sur Yvette (Winter 1972).

can be written uniquely as a (convergent) sum $\sum_{i=1}^{\infty} \sum_{j=1}^{n} V_p^i[a_{ij}]\gamma_j$.

Cartier's classification theory (local case) says that there is an isomorphism of categories between the category of commutative formal groups over A and the full subcategory of modules of continuous $\text{Cart}_{\{p\}}(A)$-left-modules with this basis property.(Cf. [2] and [6]).

To specify the $\text{Cart}_{\{p\}}(A)$-module structure of $C_p(G)$ it suffices to write $F_p\gamma_i$ as a sum $\sum_{i=1}^{\infty} \sum_{j=1}^{n} V_p^i[a_{i\ell}]\gamma_\ell$. In §5, 6 we do this for the case that G is a formal group obtained by specializing the p-typically universal formal group G_T of [3]. (Cf. (2.2) for its definition; all isomorphism classes of formal groups over $Z_{(p)}$-algebras are obtained in this way).

If G over A is obtained by substituting $t_i(jk)$ voor the $T_i(jk)$ of G_T then the formula for $F_p\gamma_i$ becomes

$$F_p\gamma_i = \sum_{m=o}^{\infty} \sum_{\ell=1}^{n} V_p^m[t_{m+1}(\ell,i)]\gamma_\ell$$

Inversely therefore, given a $\text{Cart}_{\{p\}}(A)$ module M of the right kind, the constructions of [3] provide one with a formal group G such that $C_p(G) = M$.

2. RECAPITULATION

In this section we have collected the results from [3,4,5] which will be needed in the sequel.

(2.1) <u>Local one Dimensional Case.</u>

Choose a prime number p. Let $g_T(X)$ be the power series over $Q[T_1, T_2,\ldots] = Q[T]$ defined by

$$g_T(X) = X + \Sigma \frac{T_i}{p} g_T^{(p^i)}(X^{p^i}) \qquad (2.1.1)$$

where $g_T^{(p^i)}(X)$ is the power series obtained from $g_T(X)$ by replacing the parameters T_j, j = 1, 2,... by $T_j^{p^i}$, j = 1, 2,.... Write

$$(2.1.2)\qquad g_T(X) = \sum_{i=o}^{\infty} a_i X^{p^i}$$

Then we have (cf.[3])

$$(2.1.3)\qquad a_o = 1,\ a_n = \sum_{j_1+\dots+j_k=n} \frac{T_{j_1} T_{j_2}^{p^{j_1}} \dots T_{j_k}^{p^{j_1+\dots+j_{k-1}}}}{p^k}$$

We define

$$(2.1.4)\qquad G_T(X,Y) = g_T^{-1}(g_T(X) + g_T(Y))$$

Then G_T is a formal group over $Z[T_1,T_2,\dots] = Z[T]$, and if A is a commutative (unitary) Z_p-algebra, and if
G is a one dimensional commutative formal group over A, then there exist $t_1, t_2, \dots \in A$ such that G is strictly isomorphic to G_t where G_t is obtained from G_T by substituting t_j for T_j, j = 1, 2, 3, ...

Further let $g_{T,S}(X)$ over Q[T,S] be defined by

$$(2.1.5)\qquad g_{T,S}(X) = X + \sum_{i=1}^{\infty} S_i X^{p^i} + \sum_{i=1}^{\infty} \frac{T_i}{p} g_{T,S}^{(p^i)}(X^{p^i})$$

Then one has (cf[3,5]):

$$(2.1.6)\qquad g_{T,S}(X) = X + \sum_{j_1,\dots,j_k \in N} \frac{T_{j_1} T_{j_2}^{p^{j_1}} \dots T_{j_k}^{p^{j_1+\dots+j_{k-1}}}}{p^k} X^{p^{j_1+\dots+j_k}}$$

$$+ \sum_{j_1,\dots,j_k \in N} \frac{T_{j_1} T_{j_2}^{p^{j_1}} \dots T_{j_{k-1}}^{p^{j_1+\dots+j_{k-2}}} S_{j_k}^{p^{j_1+\dots+j_{k-1}}}}{p^{k-1}} X^{p^{j_1+\dots+j_k}}$$

Let

$$(2.1.7)\qquad G_{T,S}(X,Y) = g_{T,S}^{-1}(g_{T,S}(X) + g_{T,S}(Y))$$

then $G_{T,S}$ is a formal group over Z[T,S], and is isomorphic to G_T. Moreover if A is an integral domain then G_t and $G_{t'}$ are strictly isomorphic over A if and only if there exists a sequence $s = (s_1,s_2,\dots)$ of elements of A such that $G_{t,s}(X,Y) = G_{t'}(X,Y)$ (or $g_{t,s}(X) = g_{t'}(X)$).

2.2. Local more Dimensional Case.

Again choose a prime number p, and let $T_i = (T_i(jk))_{jk}$ be an $n \times n$ matrix of indeterminates for each $i = 1, 2, \ldots$. We define the column n-vector of power series $g_T(X_1,\ldots,X_n)$ over $Q[\ldots, T_i(jk),\ldots]$ by

$$(2.2.1) \qquad g_T(X_1,\ldots,X_n) = (X_1,\ldots,X_n)^t + \sum_{i=1}^{\infty} \frac{T_i}{p} g_T^{(p^i)}(X_1^{p^i},\ldots,X_n^{p^i})$$

where $(X_1,\ldots,X_n)^t$ is the column vector of the X_i and $g_T^{(p^i)}(X_1,\ldots,X_n)$ is obtained from $g_T(X_1,\ldots,X_n)$ by replacing all $T_m(jk)$ by their p^i-th powers ($m = 1,2,\ldots$; $j = 1,\ldots,n$; $k = 1,\ldots,n$).

Writing

$$(2.2.2) \qquad g_T(X_1,\ldots,X_n) = \sum_{i=o}^{\infty} a_i(X_1^{p^i},\ldots,X_n^{p^i})^t$$

where now a_i is an $n \times n$ matrix one has (cf. [3])

$$(2.2.3) \qquad a_o = I_n, \quad a_i = \sum_{j_1+\ldots+j_k=i} \frac{T_{j_1} T_{j_2}^{(p^{j_1})} \cdots T_{j_k}^{(p^{j_1+\ldots+j_{k-1}})}}{p^k}$$

where $T_n^{(p^\ell)}$ is the matrix $((T_n(jk))^{p^\ell})_{jk}$. Now define

$$(2.2.4) \quad G_T(X_1,\ldots,X_n;\ Y_1,\ldots,Y_n) = g_T^{-1}(g_T(X_1,\ldots,X_n) + g_T(Y_1,\ldots,Y_n))$$

then G_T is an $n \times n$ formal group over $Z[\ldots, T_i(jk),\ldots]$, and if A is a commutative ring with unit element such that every prime number $q \neq p$ is invertible in A then every n-dimensional formal group over A is isomorphic to a G_t, obtained from G_T by substituting suitable $t_i(jk)$ for $T_i(jk)$.

2.3. Global more Dimensional Case.

Let e_j be the n-multiindex $e_j = (0,\ldots,0,1,0,\ldots,0)$, the 1 in the j-th place.

We define

$$(2.3.1) \ \Upsilon = \{d = (d_1,\ldots,d_n) \mid d_i \in \mathbb{N} \cup \{0\},\ d \neq (0,\ldots,0), d \neq p^r e_j \text{ for all prime numbers } p,\ j = 1,\ldots,n \text{ and } r = 1,2,\ldots\}$$

For each $d \in \Upsilon$, $d \neq e_j$; $j = 1,\dots,n$ let S_d be the column vector of indeterminates $S_d = (S_d(1),\dots,S_d(n))^t$ and let $S_{e_j} = e_j^t = (0,\dots,0,1,0,\dots 0)^t$ for $j = 1,\dots,n$; further let T_q be the n x n matrix of indeterminates $(T_q(jk))_{jk}$ for all prime powers q.

Let $s = (s_1,\dots,s_n)$, $s_i \in N \cup \{0\}$ be any multiindex. An <u>ordered factorization</u> of s is a sequence $(q_1,\dots,q_t,d)$ where q_i is a prime power and d is a multiindex from Υ such that $q_1 \cdot \dots q_t d = s$. We now define for each multiindex s the columnvector a_s by the formula

$$(2.3.2) \qquad a_s = \sum_{(q_1,\dots,q_t,d)} \frac{n(q_1,\dots,q_t,d)}{p_1} \cdot \dots \cdot \frac{n(q_t,d)}{p_t} \cdot T_{q_1} \cdot T_{q_2}^{(q_1)} \dots T_{q_t}^{(q_1 \dots q_{t-1})} S_d^{(q_1 \dots q_t)}$$

where the sum is over all ordered factorizations of s; p_i is a prime number such that q_i is a power of p_i; $T_q^{(r)}$ is the matrix $(T_q(jk)^r)_{jk}$ and $S_d^{(q)}$ is the column vector of entries $S_d(i)^q$. The $n(q_1,\dots,q_t,d)$ are any set of integers satisfying the conditions:

$$(2.3.3) \qquad \begin{array}{l} \text{if } p_1 \neq p_2 = \dots = p_r \neq p_{r+1} \text{ then } n(q_1,\dots,q_t,d) \equiv 1 \bmod p_1 \\ \text{and } n(q_1,\dots,q_t,d) \equiv 0 \bmod p_2^{r-1} \\ \text{if } p_1 = \dots = p_r \neq p_{r+1} \text{ then } n(q_1,\dots,q_t,d) \equiv 1 \bmod p_1^r \end{array}$$

(If $r = t$, take p_{r+1} = any prime number $\neq p_r$)

(Such integers exist). Now let $g(X_1,\dots,X_n)$ be the column-n-vector of power series defined by

$$(2.3.4) \qquad g(X_1,\dots,X_n) = \sum_s a_s X_1^{s_1} \dots X_n^{s_n}$$

where s runs through the multiindices $s = (s_1,\dots,s_n)$, $s_i \in N \cup \{0\}$, $s \neq (0,\dots,0)$.

We define

$$(2.3.5) \qquad G(X_1,\dots,X_n; Y_1,\dots,Y_n) = g^{-1}(g(X_1,\dots,X_n) + g(Y_1,\dots,Y_n))$$

then G is a universal n dimensional commutative formal group over $Z[\ldots, T_q(jk),\ldots; \ldots, S_d(i),\ldots]$

3. WITT VECTORS ASSOCIATED TO A PRIME p.

The formal group of Witt vectors of length n associated to a prime p is a p-typical formal group over any commutative ring with unit element A. There for it must be isomorphic to some formal group G_t, $t_i(jk) \in A$ where G_T is the formal group of (2.2). (In fact because this Witt formal group is p-typical it must be equal to some such G_t).

3.1. Witt Vectors.

Choose a prime number p. The Witt polynomials are then

$$\Phi_1(X_1) = X_1$$

(3.1.1) $$\Phi_2(X_1,X_2) = pX_2 + X_1^p$$

$$\vdots$$

$$\Phi_n(X_1,X_2,\ldots,X_n) = p^{n-1}X_n + p^{n-2}X_{n-1}^p + \ldots + pX_2^{p^{n-2}} + X_1^{p^{n-1}}$$

The polynomials $S_i(X_1,\ldots,X_i; Y_1,\ldots,Y_i)$, $i = 1,2,\ldots,n$ defined by

(3.1.2) $$\Phi_i(S_1,\ldots,S_i) = \Phi_i(X_1,\ldots,X_i) + \Phi_i(Y_1,\ldots,Y_i)$$

have coefficients in Z, and define a formal group of dimension n over any commutative ring with unit element A.

3.2. Specification.

Let $t_i(jk)$ $i = 1,2,\ldots;$ $j = 1,\ldots,n;$ $k = 1,\ldots,n$ be defined by

$$t_i(j,k) = 0 \text{ if } i \geq 2;\ j = 1,\ldots,n;\ k = 1,\ldots,n$$

(3.2.1) $$t_1(j,k) = 0 \text{ unless } j = k + 1$$

$$t_1(k+1,k) = 1 \quad k = 1,\ldots,n-1$$

I.e. the matrices t_i are equal to

$$(3.2.2) \qquad t_1 = \begin{pmatrix} 0 & & & \cdot & 0 \\ 1 & \ddots & & & \vdots \\ 0 & \ddots & \ddots & & \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \quad t_2 = 0, \ldots, t_n = 0, \ldots$$

3.3. Proposition.

Let G_t be the formal group obtained from the n-dimensional formal group G_T of (2.2) by substituting $t_i(jk)$ for $T_i(jk)$ where the $t_i(jk)$ are defined by (3.2.1). Then G_t is the group of Witt vectors of length n associated to the prime p.

Proof. Because both G_t and the formal group of Witt vectors of length n associated to p are defined over Z it suffices to prove this for A = Z.

According to (2.2.3) adn (2.2.4) the logarithm of G_t is equal to

$$(3.3.1) \qquad \log G_t(X_1,\ldots,X_n) = \sum_{i=o}^{\infty} a_i(X_1^{p^i},\ldots,X_n^{p^i}), \quad a_i = \frac{t_1 . t_1^{(p)} \ldots t_1^{(p^{i-1})}}{p^i} = \frac{(t_1)^i}{p^i}$$

I.e.

$$(3.3.2) \qquad \log G_t(X_1,\ldots,X_n) = \begin{pmatrix} X_1 \\ X_2 + \frac{1}{p} X_1^p \\ X_3 + \frac{1}{p} X_2^p + \frac{1}{p^2} X_1^{p^2} \\ \vdots \\ X_n + \frac{1}{p} X_{n-1}^p + \ldots + \frac{1}{p^{n-1}} X_1^{p^{n-1}} \end{pmatrix}$$

But according to (3.1.1) and (3.1.2) this is exactly the logarithm of the formal group of Witt vectors of length n associated to p.

q.e.d.

4. GENERALIZED WITT VECTORS

The formal group of generalized Witt vectors of length n (cf. [1], [7]) is a formal group over any commutative ring with unit element A. It must be therefore be equal to some formal group obtained from the formal group G of (2.3) by suitable substitutions for the $T_q(jk)$, q a prime power, and $S_d(i)$, $d \in \Upsilon \setminus \{e_1,\dots,e_n\}$.

It turns out to be convenient to choose the $n(q_1,\dots,q_t,d)$ in a rather special way (cf. 4.3) below).

4.1. Generalized Witt Vectors.

The generalized Witt polynomials are

(4.1.1)
$$\begin{aligned} \psi_1(X_1) &= X_1 \\ \psi_2(X_1,X_2) &= 2X_2 + X_1^2 \\ &\vdots \\ \psi_n(X_1,\dots,X_n) &= \sum_{d|n} d\, X_d^{n|d} \end{aligned}$$

The polynomials $S_i(X_1,\dots,X_i;\ Y_1,\dots,Y_i)$ defined by

(4.1.2)
$$\psi_i(S_1,\dots,S_i) = \psi_i(X_1,\dots,X_i) + \psi_i(Y_1,\dots,Y_i)$$

have their coefficients in Z and define a formal group of dimension n over any commutative ring with unit element A.

(4.2) Let $p_1,\dots,p_s$ be a sequence of prime numbers, $p_1 < p_2 < \dots < p_s$. Let $J(p_1^{r_1},\dots,p_s^{r_s})$ be the set of all sequences $(p_1',\dots,p_n')$ such that $p_i' \in \{p_1,\dots,p_s\}$; for all i, $n = r_1 + \dots + r_s$, and such that p_i occurs exactly r_i times in $(p_1',\dots,p_n')$. If $(p_1',\dots,p_n') \in J(p_1^{r_1},\dots,p_s^{r_s})$ we also write $J(p_1',\dots,p_n') = J(p_1^{r_1},\dots,p_s^{r_s})$. For example

$J(2^2,3) = \{(2,2,3),\ (2,3,2),\ (3,2,2)\}$

$J(2,3,5) = \{(2,3,5),\ (2,5,3),\ (3,2,5),\ (3,5,2),\ (5,2,3),\ (5,3,2)\}$.

(4.3) Lemma.

There exist integers $\bar{n}(p_1',\dots,p_m')$, for all sequences of primes $(p_1',\dots,p_m')$ such that

a. If $p_1' \neq p_2' = \dots = p_r' \neq p_{r+1}'$, ($r \leq m$, take p_{r+1}' = any prime $\neq p_r'$ if $r = m$) then $\bar{n}(p_1',\dots,p_m') \equiv 1 \bmod p_1'$ and $\bar{n}(p_1',\dots,p_m') \equiv 0 \bmod (p_2')^{r-1}$

b. If $p_1' = p_2' = \dots = p_r' \neq p_{r+1}'$, ($r \leq m$, take p_{r+1}' = any prime $\neq p_r'$ if $r = m$) then $\bar{n}(p_1',\dots,p_m') \equiv 1 \bmod (p_1')^r$.

c. For all $J = J(p_1^{r_1},\dots,p_s^{r_s})$ one has

$$\sum_{(p_1',\dots,p_m') \in J} \bar{n}(p_1',\dots,p_m')\bar{n}(p_2',\dots,p_m')\dots\bar{n}(p_{m-1}',p_m')\bar{n}(p_m') = 1$$

<u>Proof</u>. We use induction on m. For $m = 1$ let $\bar{n}(p') = 1$ for all prime numbers p'. Suppose we have defined $\bar{n}$ for all sequences of primes of length $< m$. Let $J = J(p_1^{r_1},\dots,p_s^{r_s})$, $r_1 + \dots + r_s = m$, $p_1 < p_2 < \dots < p_s$ prime numbers. Then

$$\sum_{(p_1',\dots,p_m') \in J} \bar{n}(p_1',\dots,p_m')\bar{n}(p_2',\dots,p_m') \dots \bar{n}(p_{m-1}',p_m')\bar{n}(p_m') =$$

(4.3.1)
$$= \sum_{\substack{(p_1',\dots,p_m') \in J \\ p_1'=p_1}} \bar{n}(p_1',\dots,p_m')\bar{n}(p_2',\dots,p_m')\dots\bar{n}(p_{m-1}',p_m')\bar{n}(p_m') + \dots$$
$$+ \sum_{\substack{(p_1',\dots,p_m') \in J \\ p_1'=p_s}} \bar{n}(p_1',\dots,p_m')\bar{n}(p_2',\dots,p_m')\dots\bar{n}(p_{m-1}',p_m')\bar{n}(p_m')$$

Now for each $i = 1,2,\dots,s$ let $\sigma(i)$ be the sequence in J

(4.3.2) $$\sigma(i) = (p_i,\dots,p_i,\ p_{i+1},\dots,p_{i+1},\dots,p_s,\dots,p_s,p_1,\dots,p_1,\dots,\ p_{i-1},\dots,p_{i-1})$$

We define

(4.3.3) $$\bar{n}(p_1',\dots,p_m') = \bar{n}(\sigma(i)) \text{ if } p_1' = p_i$$

where the $\bar{n}(\sigma(i))$ are still to be determined. Then using (4.3.1) we see that

(4.3.4) $$\sum_{(p_1',\dots,p_m') \in J} \bar{n}(p_1',\dots,p_m') \dots \bar{n}(p_m') = \sum_{i=1}^{s} \bar{n}(\sigma(i))$$

Now let $r = \max_i r_i$. We define

$$\bar{n}(\sigma(i)) = \Big(\prod_{j\neq i} p_j\Big)^{(p_i-1)p_i^{r-1}} \qquad i = 1,\dots,s-1$$

(4.3.5)

$$\bar{n}(\sigma(s)) = 1 - \sum_{i=1}^{s-1} \bar{n}(\sigma(i))$$

(N.B. if $s=1$, take $\bar{n}(\sigma(1)) = 1$). Then for $i = 1,\dots,s-1$

$\bar{n}(\sigma(i)) \equiv 1 \bmod p_i^{r_i}$ because $p_j^{p_i-1} \equiv 1 \bmod p_i$ for all $j \neq i$, and $r \geq r_i$

$\bar{n}(\sigma(i)) \equiv 0 \bmod p_j^{r_j}$ for $j \neq i$ because $p_i^{r-1} \geq r \geq r_j$

and for $i = s$ we have

$\bar{n}(\sigma(s)) \equiv 1 \bmod p_s^{r_s}$ because $\bar{n}(\sigma(i)) \equiv 0 \bmod p_s^{r_s}$ for all $i \neq s$.

$\bar{n}(\sigma(s)) \equiv 0 \bmod p_j^{r_j}$ for $j \neq s$ because $\bar{n}(\sigma(i)) \equiv 0 \bmod p_j^{r_j}$ for all $j \neq i,s$

and $\bar{n}(\sigma(j)) \equiv 1 \bmod p_j^{r_j}$.

It follows that the $\bar{n}$ defined by (4.3.3) and (4.3.5) satisfy the conditions a), b), c) of (4.3).

q.e.d.

(4.4) Specification.

We define $t_q(i,j)$ and $s_d(i)$ as follows

$t_q(i,j) = 0$ if q is a prime power but not a prime number

$t_p(i,j) = 0$ unless $i/j = p$

$t_p(i,j) = 1$ if $i/j = p$; $i, j \in \{1,\dots,n\}$

$s_d(i) = 0$ for all $d \in \mathcal{T} \setminus \{e_1,\dots,e_n\}$, $i = 1,\dots,n$

(4.5) Proposition.

Take $n(q_1,\dots,q_t,d) = \bar{n}(p_1,\dots,p_t)$ if q_i is a power p_i in the definition of the formal group G of (2.3) (where the $\bar{n}$ are as in lemma (4.3)). Let W_n be the formal group obtained from this G by substituting for the $T_q(jk)$ and $S_d(i)$ the values specified in (4.4). Then W_n is the formal group of generalized Witt vectors of length n.

Proof. According to (2.3) the logarithm of W_n is equal to

(4.5.1) $$\log W_n(X_1,\dots,X_n) = \sum_s a_s X_1^{s_1} \dots X_n^{s_n}$$

and using (2.2.3) and (4.4) we see that the column vector a_s is equal to zero unless the multiindex s is of the form $s = me_j$, for some $m \in N$, $j \in \{1,\dots,n\}$. And then

(4.5.2)
$$a_{me_j} = \sum_{(p_1',\dots,p_k')\in J} \frac{n(p_1',\dots,p_k',e_j)}{p_1'} \cdot \dots \cdot \frac{n(p_k',e_j)}{p_k'} t_{p_1'} \cdot t_{p_2'}^{(p_1')} \dots$$
$$\dots t_{p_k'}^{(p_1'\dots p_{k-1}')} e_j^{(p_1'\dots p_k')}$$

where $J = J(p_1^{r_1},\dots,p_\ell^{r_\ell})$ if $m = p_1^{r_1}\dots p_\ell^{r_\ell}$

Now we have $t_p^{(r)} = t_p$ for all prime numbers p and all $r \in N$ and

$$(t_{p_1} \cdot \dots \cdot t_{p_k'})_{a,b} = 0 \text{ if } a/b \neq p_1'\dots p_k' = m, \ (a,b \in \{1,\dots,n\})$$
(4.5.3)
$$(t'_{p_1} \cdot \dots \cdot t_{p_k'})_{a,b} = 1 \text{ if } a/b = p_1'\dots p_k' = m$$

Therefore, using $n(p_1',\dots,p_k',e_j) = \bar{n}(p_1',\dots,p_k')$ and (4,4) c) we see that the i-th entry $a_{me_j}(i)$ of a_{me_j} is equal to

(4.5.4) $a_{me_j}(i) = m^{-1}$ if $i/j = m$, $a_{me_j}(i) = 0$ if $i/j \neq m$.

Therefore, as

(4.5.5) $$\log W_n(X_1,\dots,X_n) = \sum_s a_s X_1^{s_1} \dots X_n^{s_n} = \sum_{me_j} a_{me_j} X_j^m$$

we have

(4.5.5) $$\log W_n(X_1,\dots,X_n)(i) = \sum_{m|i} \frac{1}{m} X_{i/m}^m$$

and we see by (4.1.1) and (4.1.2) that $\log W_n$ is equal to the logarithm of the generalized Witt vectors of length n.

q.e.d.

5. CARTIER-DIEUDONNE MODULES (local, one dimensional case)

5.1. Definition of $C_p(G)$ (cf. 2)

Let G be an n-dimensional formal group over a ring A. A curve in G is an n-column-vector of power series in X over A without constant terms. Two curves $c_1(X)$ and $c_2(X)$ can be added as follows:

(5.1.1) $$(c_1+c_2)(X) = G(c_1(X),\ c_2(X))$$

This turns C(G), the set of all curves in G, into an abelian group. The subgroups $C^n(G)$ of curves $\equiv 0 \bmod(X^n)$ define a topology on C(G). The topological group C(G) admits operators [a], $a \in A$; V_n, $n \in \mathbb{N}$, F_n, $n \in \mathbb{N}$ which are defined as follows

(5.1.2) $$([a]c)(X) = c(aX) \qquad (V_nc)(X) = c(X^n)$$

The definition of F_n requires a bit more care. First suppose that A is an integral domain of characteristic zero and let ζ_n be a primitive n-th root of unity.

We set

(5.1.3) $$(F_nc)(X) = ([\zeta_n]c + \dots + [\zeta_n^n]c)(X^{1/n})$$

Galois theory shows that the right hand member of (5.1.3) is in fact a power series over A, and because the right hand side of (5.1.3) is invariant under the substitution $X^{1/n} \mapsto \zeta_n X^{1/n}$ it follows that the right hand side of (5.1.3) is in fact a power series in X. To define the operator F_n over arbitrary rings A one lifts both the formal group G and the curve c to a formal group G' and a curve c' over an integral domain of characteristic zero A', one calculates F_nc' over A' and then reduces F_nc' to a curve over A. This reduction is then the desired F_nc. One has the following relations between the various operators (cf. [2]).

(5.1.4) $$[a] + [b] = \sum_{n=1}^{\infty} V_n\, s_n(a,b)\, F_n$$

where the polynomials $s_n(X,Y)$ are defined by $X^n + Y^n = \sum_{d|n} d s_d(X,Y)^{n/d}$

(5.1.5) $$[a][b] = [ab]$$

(5.1.6) $V_m V_n = V_{mn}$, $F_m F_n = F_{mn}$

(5.1.7) $[a]V_n = V_n[a^n]$, $F_n[a] = [a^n]F_n$

(5.1.8) If $(n,m) = 1$, $F_m V_n = V_n F_m$

(5.1.9) $F_n V_n = n\, Id_{c(g)}$, $[1] = V_1 = F_1 = Id_{C(G)}$

where $Id_{C(g)}$ is the identity on C(G).

Choose a prime number p. A curve c in G is called p-typical if $F_q c = 0$ for all prime numbers $q \neq p$. The formal group G is called p-typical if the curves $\gamma_1, \ldots, \gamma_n$ defined by $\gamma_i(X) = (0,\ldots,0,X,0,\ldots,0)$, X in the i-th place, are p-typical.

Let A be an integral domain, and $g(X_1,\ldots,X_n)$ the logarithm of G. Then

(5.1.10) $$c \text{ is p-typical} \Leftrightarrow g(c(X)) = \sum_{j=1}^{\infty} \frac{m_j}{p^j} X^{p^j}$$

where the m_j are n-column-vectors of elements from A.

The p-typical curves in G constitute a subgroup of C(G) which is denoted $C_p(G)$. This subgroup is stable under the operations [a], V_n, F_n.

5.2. The Ring $Cart_{\{p\}}(A)$ (cf. [2] and [6])

Choose a prime number p. The (in general non-commutative) topological ring $Cart_{\{p\}}(A)$ consists of all expressions

(5.2.1) $$x = \sum_{i,j \in \mathbb{N}}^{\infty} V_p^i [a_{ij}] F_p^j$$

such that for all i there are only finitely many j such that $a_{ij} \neq 0$ (I.e. every element x can be written in a unique way as such a (convergent) sum. Addition and multiplication in $Cart_{\{p\}}(A)$ are defined by the relations

$$[a] + [b] = \sum_{n=o}^{\infty} V_p^n s_{p^n}(a,b) F_p^n$$, where $s_{p^n}(X,Y)$ is defined in (5.1.4)

(5.2.2) $[a][b] = [ab]$, $V_p^o = F_p^o = Id$, $F_p V_p = p.Id$

$[a]V_p = V_p[a^p]$, $F_p[a] = [a^p]F_p$

where Id is the identity element of $\text{Cart}_{\{p\}}(A)$. The ring is topologized by the subgroups $\text{Cart}^n_{\{p\}}(A)$ consisting of those elements x such that $a_{ij} = 0$ if $i \leq n$.

The operators [a] and F_p, V_p defined in (5.1) turn $C_p(G)$, the group of p-typical curves of G into a left (continuous, complete) module over $\text{Cart}_{\{p\}}(A)$.

Now let A be a commutative ring with unit element such that every prime number $q \neq p$ is invertible in A. Then Cartier's classification theory says that the functor $G \mapsto C_p(G)$ is an equivalence of categories between the commutative formal groups over A and a certain full subcategory of (complete, continuous) left modules over $\text{Cart}_{\{p\}}(A)$. (There is also a global version of this theory (cf.[2,6])).

It is the aim of the next few subsections and §6 to calculate these modules (as modules) in the case that G is a p-typical group over A (A as before; note that every commutative formal group over A is strictly isomorphic to a p-typical one).

From now on A is a commutative ring with unit element such that all prime numbers $q \neq p$ are invertible in A.

5.3. Let now G be a one dimensional group over A, and γ be the curve $\gamma(X) = X$. Suppose that G is p-typical. It is clear from (5.1) that every p-typical curve in G can be written in a unique way as a (convergent) sum

$$(5.3.1) \qquad \sum_{i=0}^{\infty} V_p^i [a_i]\gamma$$

(Use (5.1.10) to prove this for characteristic zero integral domains A, and then use a lifting argument to prove this for all A).

In particular the curve $F_p\gamma$ can be written as a sum (5.3.1). It follows that the modules $C_p(G)$ arising from one-dimensional (p-typical) formal groups over A are of the form.

$$(5.3.2) \qquad \text{Cart}_{\{p\}}(A)/\text{Cart}_{\{p\}}(A)(F_p - \sum_{i=0}^{\infty} V_p^i[a_i])$$

for certain $a_0, a_1, \ldots \in A$

5.4. <u>Lemma</u>.

Let $g_T(X)$ be the formal power series of (2.1.1) then

$$g_T(X) = X + \frac{1}{p}\, g_T(T_1X^p) + \ldots + \frac{1}{p}\, g_T(T_iX^{p^i}) + \ldots$$

Proof. this is an immediate consequence of (2.1.3).

5.5. Theorem.

Let G_t be the formal group over A obtained from the formal group G_T of (2.1) by substituting t_i for T_i. Then

$$C_p(G_t) = \mathrm{Cart}_{\{p\}}(A)/\mathrm{Cart}_{\{p\}}(A)(F_p - \sum_{i=o}^{\infty} V_p^i[t_{i+1}])$$

as a left $\mathrm{Cart}_{\{p\}}(A)$ module.

Proof. We have to calculate $F_p\gamma$. Suppose first that A is an integral domain of characteristic zero. Then, if $g_t(X)$ is the logarithm of G_t,

$$(5.5.1)\quad g_t(F_p\gamma) = \sum_{i=1}^{p} g_t(\zeta_p^i X^{1/p}) = g_t(t_1X) + g_t(t_2X^p) + \ldots + g_t(t_iX^{p^{i-1}}) + \ldots$$

according to lemma (5.4). It follows that in $C_p(G_t)$

$$(5.5.2)\qquad F_p\gamma = [t_1]\gamma + V_p[t_2]\gamma + \ldots + V_p^i[t_{i+1}]\gamma + \ldots$$

which proves the theorem in the case that A is an integral domain of characteristic zero. The general case follows by a lifting argument.

5.6. Lemma.

Let $g_{T,S}(X)$ be the formal power series of (2.1.5) then

$$g_{T,S}(X) = g_T(X) + g_T(S_1X^p) + \ldots + g_T(S_iX^{p^i})$$

where $g_T(X)$ is the power series of (2.1.1).

Proof. This is an immediate consequence of (2.1.6).

5.7. Isomorphisms.

Suppose that A is an integral domain of characteristic zero. Then the formal groups G_t and $G_{t'}$ are strictly isomorphic if and only if there are $s_1, s_2, \ldots \in A$ such that $g_{t,s}(X) = g_{t'}(X)$. Cf. [3].

5.8. Proposition.

Let G_t and $G_{t'}$ be strictly isomorphic over the characteristic zero integral domain A, and let $s_1, s_2, \ldots \in A$ be such that $g_{t,s}(X) = g_{t'}(X)$. Then the corresponding isomorphism.

$$\mathrm{Cart}_{\{p\}}(A)/\mathrm{Cart}_{\{p\}}(A)(F_p - \Sigma V_p^i[t_{i+1}]) \to \mathrm{Cart}_{\{p\}}(A)/\mathrm{Cart}_{\{p\}}(A)(F_p - \Sigma V_p^i[t'_{i+1}])$$

is given by

$$1 \mapsto \sum_{i=0}^{\infty} V_p^i[s_i]$$

where $s_0 = 1$.

Proof. This follows from lemma (5.6).

6. CARTIER-DIEUDONNE MODULES (local, more dimensional case)

Again, choose a prime number p, and let A be a commutative ring with unit element in which all prime numbers $q \neq p$ are invertible.

(6.1) Let G be an n-dimensional p-typical formal group over A. Let γ_i be the curve $\gamma_i(X) = (0,\ldots,0,X,0,\ldots,0)^t$, X in the i-th place. It is clear from (5.1) that every p-typical curve in G can be written uniquely as a (convergent) sum

$$\sum_{j=1}^{n} \sum_{i=1}^{\infty} V_p^i[a_{ij}]\gamma_j \tag{6.1.1}$$

(Use the same arguments as in (5.3)).
In particular the curves $F_p\gamma_j$ can written in the form (6.1.1) and the module structure of $C_p(G)$ is completely specified by these "relations".

(6.2) Lemma.

Let g_T be the power series of (2. 2.1). Then

$$g_T(\gamma_i(X)) = \gamma_i(X) + \sum_{\ell=1}^{n} \sum_{m=1}^{\infty} \frac{1}{p} g_T(V_p^m[T_m(\ell,i)]\gamma_\ell(X))$$

Proof. According to (2.2.2) and (2.2.3) we have

$$g_T(\gamma_i(X)) = \gamma_i(X) + \sum_{r=1}^{\infty} \sum_{j_1+\dots+j_k=r} \frac{T_{j_1} T_{j_2}^{(p^{j_1})} \cdots T_{j_k}^{(p^{j_1+\dots+j_{k-1}})}}{p^k} \begin{pmatrix} 0 \\ 0 \\ X^{p^r} \\ 0 \\ 0 \end{pmatrix}$$

$$= \gamma_i(X) + \sum_{r=1}^{\infty} \sum_{j_1+\dots+j_k=r} \frac{T_{j_1} \cdots T_{j_{k-1}}^{(p^{j_1+\dots+j_{k-2}})}}{p^k} \begin{pmatrix} T_{j_k}(1,i)^{p^{j_1+\dots+j_{k-1}}} X^{p^r} \\ \vdots \\ T_{j_k}(n,i)^{p^{j_1+\dots+j_{k-1}}} X^{p^r} \end{pmatrix}$$

$$= \gamma_i(X) + \sum_{r=1}^{\infty} \sum_{j_1+\dots+j_k=r} \sum_{\ell=1}^{n} \frac{T_{j_1} \cdots T_{j_{k-1}}^{(p^{j_1+\dots+j_{k-2}})}}{p^k} \begin{pmatrix} 0 \\ 0 \\ T_{j_k}(\ell,i)^{p^{j_1+\dots+j_{k-1}}} X^{p^r} \\ 0 \\ 0 \end{pmatrix}$$

$$= \gamma_i(X) + \frac{1}{p} \sum_{\ell=1}^{n} \sum_{m=1}^{\infty} g_T(V_p^m[T_m(\ell,i)]\gamma_\ell(X))$$

(take "$m = j_k$" in the previous formula to obtain this last equality).

q.e.d.

(6.3) <u>Theorem.</u>

Let G_t be the formal group over A obtained from the G_T of (2.2) by substituting $t_i(j,k)$ for $T_i(j,k)$. Then $C_p(G_t)$ is generated by $\gamma_1,\dots,\gamma_n$, every element of $C_p(G_t)$ can be uniquely written as a (convergent) sum $\sum_{\ell=1}^{n} \sum_{i=1}^{\infty} V_p^i[a_{i\ell}]\gamma_\ell$, and the module structure of $C_p(G_t)$ is then given by the relations

$$F_p\gamma_i = \sum_{\ell=1}^{n} \sum_{m=o}^{\infty} V_p^m[t_{m+1}(\ell,i)]\gamma_\ell, \quad i = 1,\dots,n$$

Proof. This follows from (6.2) for characteristic zero integral domains A and then by a lifting argument also for all A.

q.e.d.

(6.4) Remarks.

One would of course like to give the same sort of description for C (G) in the global case, i.e. when there is more than one prime number not invertible in A. Then one has of course that C(G) is generated by $\gamma_1, \ldots, \gamma_n$ (if G is n-dimensional) and that every element of C(G) can be uniquely written as a sum

$\sum_{\ell=1}^{n} \sum_{i=1}^{\infty} V_i[a_{i\ell}]\gamma_\ell$; and the Cart(A)-module structure of C(G), where

Cart(A) is the global counterpart of $\mathrm{Cart}_{\{p\}}(A)$, is then given by a set of relations

$$F_q\gamma_i = \sum_{\ell=1}^{n} \sum_{j=1}^{\infty} V_j[b_{q,i,j,\ell}]\gamma_\ell$$

where q runs through all primes. In this case the $b_{q,i,j,\ell}$ are not independant as they are in the local case (by theorem (6.3)). I hope to be able to do something on this in the near future. At the moment the calculations look exceedingly messy and intractable.

REFERENCES

[1]. P. Cartier (1967), Groupes Formels Associés aux Anneaux de Witt Généralisés. C.R. Acad. Sci. Paris 265, 49-52.

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

[3]. M. Hazewinkel (1971), Constructing Formal Groups I: Over $Z_{(p)}$-algebras Report 7119 + appendix, Econometric Inst., Erasmus Univ. Rotterdam.

[4]. M. Hazewinkel (1972), Constructing Formal Groups II: Over Z-algebras Report 7201, Econometric Institute , Erasmus Univ. Rotterdam.

[5]. M. Hazewinkel (1972), Constructing Formal Groups III: Over $Z_{(p)}$, Z_p and Z. Report 7207, Econometric Inst., Erasmus Univ Rotterdam.

[6]. M. Lazard, Sur les Théorèmes Fondamentaux des Groupes Formels Commutatifs (to appear).

[7]. D. Mumford (1966), Lectures on Curves on an Algebraic Surface. Princeton Univ. Press.