Astérisque

BERT DITTERS

On the classification of smooth commutative formal groops. Higher Hasse-Witt matrices of an Abelian variety in positive characteristic

Astérisque, tome 63 (1979), p. 67-71

<http://www.numdam.org/item?id=AST_1979__63__67_0>

Société Mathématique de France
Astérisque 63 (1979) p. 67-72

ON THE CLASSIFICATION OF SMOOTH COMMUTATIVE FORMAL GROUPS. HIGHER HASSE-WITT MATRICES OF AN ABELIAN VARIETY IN POSITIVE CHARACTERISTIC.

by

Bert DITTERS

(Amsterdam)

1. The aim of the present note is to report on the classification of smooth commutative formal groups -in short : formal groups- over a perfect basefield k of characteristic $p > o$ or over its Wittvectors $W(k)$. The main tool will be a set $c = \{c_i | i \geq o\}$ of matrices with entries in $W(k)$, called higher Hasse-Witt matrices, because for curves of positive genus these matrices are a natural lifting and generalization of the original definition of the Hasse-Witt matrix as given in [2], cf no. 4 below. There can be found various methods described in the litterature by which an explicit classification of formal groups may be given. We mention the one dimensional case over an algebraically closed k, described in the fifties by Dieudonné, using hyperalgebraical methods and at the same time by Lazard, using direct methods. The one dimensional case over $W(k)$ is given in Honda, [3], lemma 3.4, where he uses properties of the transformer. The higher dimensional case over k is treated in the well-known paper of Manin [5], where an explicit description of the two dimensional case is given, using extensiontheory for special submodules. In the sequel we present a method for explicit classification that works for both k and $W(k)$.

2. Let G be an n-parameter commutative formal grouplaw over $A = k$ or $A = W(k)$. In short : let G be a formal grouplaw over A. We denote $C = C_p(G)$ its group of p-typical curves and $O(G) = A[[X_1,..,X_n]]$ its contravariant bialgebra with co-multiplication μ given by $\mu(X_i) = G_i(X \hat{\otimes} 1, 1 \hat{\otimes} X)$ if $G = (G_1,\ldots,G_n)$. We assume the canonical curves $\phi_i: O(G) \to A[[t]]$, defined by $\phi_i(X_j) = \delta_{ij}\, t$, $1 \leq i, j \leq n$, to be p-typical. There is a natural action of $W(k)$ on C, $(a,\phi) \mapsto \underset{\sim}{a}\phi$ for $a \in W(k)$ and $\phi \in C$ satisfying the well known rules $F \underset{\sim}{a} = \underset{\sim}{a}^{\sigma} F$ and

$V\underset{\sim}{a}^{\sigma} = \underset{\sim}{a}V$. Here σ is the Frobenius on $W(k)$. We extend this action in the obvious way of $M_n(W(k))$ to the direct sum C^n. Denoting $\phi_G: = {}^t(\phi_1,\ldots,\phi_n) \in C^n$ the n-tuple of canonical curves, we recall the following facts:

F1. Every $\psi \in C^n$ may be written as $\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{\lambda}_i \phi_G$ with $\lambda_i \in M_n(W(k))$.

F2. In particular we have for the Frobenius F acting on C^n:

(2.1) $\quad F\phi_G = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}_i \phi_G \qquad c_i \in M_n(W(k))$.

G is determined by (2.1) and every choice of $c_i \in M_n(W(k))$ determines a formal grouplaw over A.

F3. If H is another formal grouplaw over A with $F\phi_H = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \phi_H$, then H is isomorphic to G over A if and only if C^n contains an element ψ as in F1 with λ_o invertible and such that $F\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \psi$.

Assume H to be isomorphic over A to G, and first assume A = k. Then by F3 we have $F\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \psi$ and $\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{\lambda}_i \phi_G$ with λ_o invertible. It follows:

(2.2) $\quad \underset{\sim}{p}\,\psi = FV\,\psi = VF\,\psi = V\sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \left(\sum_{j=o}^{\infty} V^j \underset{\sim}{\lambda}_j \phi_G\right)$

(2.3) $\quad = \sum_{j=o}^{\infty} V^j \underset{\sim}{\lambda}_j \underset{\sim}{p}\phi_G = \sum_{j=o}^{\infty} V^j \underset{\sim}{\lambda}_j V\sum_{i=o}^{\infty} V^i \underset{\sim}{c}_i \phi_G.$

It does not follow that the coefficients of $V^{n+1}\phi_G$ in (2.2) and (2.3) are equal, i.e. it does not follow that

(2.4) $\quad \sum_{i+j=n} c_i'^{\sigma^j} \lambda_j = \sum_{i+j=n} \lambda_j^{\sigma^{i+1}} c_i \quad , n \geq o.$

If however (2.4) holds, both the sets $c = \{c_i | i \geq o\}$ and $c' = \{c_i' | i \geq o\}$ determine isomorphic formal grouplaws. Because a formal group over A is just an A-isomorphism class of formal grouplaws over A, we use (2.4) for an explicit classification as follows: given the c_i, determine $\lambda_j \in M_n(W(k))$ with λ_o invertible in order to find a set $c' = \{c_i' | i \geq o\}$ with the nicest possible properties. This c' then determines a representative of the isomorphism class of G.

If the base ring is W(k) we have: $F\phi_G = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}_i \phi_G$ and $\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{\lambda}_i \phi_G$ such that $F\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \psi$. It follows that :

$$F\psi = \sum_{i=o}^{\infty} V^i \underset{\sim}{c}'_i \sum_{j=o}^{\infty} V^j \underset{\sim}{\lambda}_j \phi_G$$

$$= F\sum_{i=o}^{\infty} V^i \underset{\sim}{\lambda}_i \phi_G = \underset{\sim}{\lambda}_o^{\sigma} F\phi_G + \underset{\sim}{p} \sum_{i=o}^{\infty} V^i \underset{\sim}{\lambda}_{i+1} \phi_G.$$

The set of equations, analogous to (2.4) then becomes:

$$(2.5) \qquad \sum_{i+j=n} c_i'^{\sigma^j} \lambda_j = \lambda_o^{\sigma^{n+1}} c_n + p\,\lambda_{n+1}, \; n \geq o.$$

3. Example: Suppose k algebraically closed and G to be an one parameter formal grouplaw. If all $c_i = o$, then $G = X + Y$. Suppose $h \geq 1$ minimal such that $c_{h-1} \neq o$, then $c_o' = .. = c_{h-2}' = o$ and $c_{h-1}' \lambda_o = \lambda_o^{\sigma^h} c_{h-1}$. Choose λ_o such that $c_{h-1}' = 1$. Assume $\lambda_o, \ldots, \lambda_s$ to be chosen such that $c_{h-1+i}' = o$ for $1 \leq i \leq s$, then (2.4) gives:

$$\lambda_{s+1} + c_{h+s}' \lambda_o = \lambda_o^{\sigma^{h+s+1}} c_{h+s} + \lambda_{s+1}^{\sigma^h} c_{h-1}.$$

This defines mod p a separable polynomial in λ_{s+1}, hence we may find λ_{s+1} such that $c_{h+s}' \lambda_o = o$, thus $c_{h+s}' = o$. A representative for G is given by the relation $F\phi = V^{h-1}\phi$, equivalently, $\underset{\sim}{p}\phi = V^h \phi$, thus we recover the well known result of Dieudonné-Lazard.

4. Definition. If the formal grouplaw G over A is given as in F2 by $F\phi_G = \sum_{i=o}^{\infty} V^i \underset{\sim i}{c} \phi_G$, we call the set of transposed matrices ${}^t c = \{{}^t c_i \mid i \geq o\}$ the (higher) Hasse-Witt matrices of G.

For the justification of this term, consider a function field K in one variable over the field of quotients B(k) of W(k). Let $g \geq 1$ be the genus of K. We adopt the notations of Hasse-Witt, [2], Satz 4: Assume that K has a non special divisior $\mathfrak{p} = \prod_{i=1}^{g} \mathfrak{p}_i$ and let π_i be a local parameter at $\mathfrak{p}_i$. By the theorem of Riemann-Roch it is clear that there exists for every $s \geq o$, a set $v^{(s)} = (v_1^{(s)}, \ldots, v_g^{(s)}) \in L(\mathfrak{p}^{p^{s+1}})$, essentially unique, and a matrix $H_s \in M_g(B(k))$ such that

$$(4.1) \qquad v^{(s)} \equiv \frac{E}{\pi^{p^{s+1}}} - \frac{H_o^{\sigma^s}}{\pi^{p^s}} - \ldots - \frac{p^i H_i^{\sigma^{s-i}}}{\pi^{p^{s-i}}} \ldots - \frac{p^s H_s}{\pi} \bmod \mathfrak{p}^o$$

For $s = o$, (4.1) just defines the usual Hasse-Witt matrix in the context however of characteristic zero.

Theorem 1. If K has good reduction at the prime (p) of B(k), the matrices H_i, $i \geq o$ all are p-integral. The choice of $\mathfrak{p}$ determines a formal grouplaw G over W(k) for the Jacobi functionfield of K and the covariant Dieudonné module of G is given by $F\phi_G = \sum_{i=o}^{\infty} V^i \, {}^t\underset{\sim i}{H} \phi_G$.

The proof uses the fact that by the residue theorem, cf.loc.cit. Satz 6, one has

$$(4.2) \qquad B_{p^{s+1}-1} = \sum_{i=o}^{s} p^i B_{p^{s-i}-1} H_i^{\sigma^{s-i}}, \qquad s \geq o.$$

By well known results of Honda, the differentials of the first kind $\frac{du}{d\pi} =$

$= \sum_{v=o}^{\infty} B_v \pi^v$ define G over W(k) if K has good reduction mod p, and the author's results on formal groups imply that G is defined over W(k) if and only if (4.2) holds with all $H_i \in M_g$ (W(k)). ($p^s \to {}^tB_{p^s-1}$ is a Hilbertfunction in the terminology of [1].) Moreover it can be shown, that $u = p - \sum_{i=o}^{\infty} H_i T^{i+1}$ is a special element for G in the sense of Honda [3], consequently, if $k = \mathbb{F}_p$ one has by loc. cit. section 5.5 that the Frobenius π on G mod p satisfies

$$(4.3) \qquad \det(p E - \sum_{i=o}^{\infty} H_i \pi^{i+1}) = o.$$

As is known, the Hasse-Witt matrix H_o mod p only gives information of the unit root part of the characteristic polynomial of the Frobenius on G, i.e. the horizontal slope of the Newton polygon of G. As (4.3) shows, the higher Hasse-Witt matrices determine the full Newton polygon. For instance, the example given by Koblitz [4], p 209 of curves having different rank Hasse-Witt matrices H_o mod p but the same Newtonpolygon and conversely, same rank Hasse-Witt matrices but different Newtonpolygons can fully be understood by looking at the first higher Hasse-Witt matrix H_1 of these curves.

5. A curve may have (and generically usually has) an infinite number of non zero Hasse-Witt matrices. At the oral exposition, the following result was conjectural, but has been established in the mean while:

Theorem 2. If k is algebraically closed then every formal group over k has a representative with only a finite number of non zero Hasse-Witt matrices.

If $k = \mathbb{F}_p$, the theorem is false even in dimension one. The theorem is not unexpected in view of Manin's finiteness theorem , [5], th. 3.4 but we were not able to derive theorem 2 from this. Specializing to the case of dimension 2 we have, using the relations (2.3):

Theorem 3. Let G be a two dimensional formal group over an algebraically closed field k of characteristic $p > o$, then G has a representative of the following possible types :

a. $p\phi = o$ and $G \cong 2\,\hat{G}_a$.

b. $p\phi = V^h \phi$, $1 \leq h < \infty$.

c1. $p\phi = V^h \begin{pmatrix} 1 & o \\ o & o \end{pmatrix}\phi + V^{h+k}\begin{pmatrix} o & o \\ o & 1 \end{pmatrix}\phi$, $1 \leq h < k < \infty$.

c2. $p\phi = V^h \begin{pmatrix} 1 & o \\ o & o \end{pmatrix}\phi$. $1 \leq h < \infty$.

d1. $p\phi = V^h \begin{pmatrix} o & 1 \\ o & o \end{pmatrix}\phi$. $1 \leq h < \infty$.

d2. $p\phi = V^h \begin{pmatrix} o & 1 \\ o & o \end{pmatrix}\phi - V^{h+m}\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}\phi$, $1 \leq h < m < \infty$.

d3. $p\phi = V^h \begin{pmatrix} o & 1 \\ o & o \end{pmatrix}\phi - V^{h+m}\begin{pmatrix} o & o \\ o & 1 \end{pmatrix}\phi$, $1 \leq h < m < \infty$.

d4. <u>there are</u> $1 \leq m, n < \infty$ such that if $\gamma = \min(n,n)$

$$p\phi = V^h \begin{pmatrix} o & 1 \\ o & o \end{pmatrix} - V^{h+m} \left(\sum_{i=o}^{\gamma-1} V^i \begin{pmatrix} o & o \\ o & a_i \end{pmatrix} \phi \right) - V^{h+m+n}\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}.$$

<u>All</u> a_i <u>are in the image of the Teichmüller map</u> $T : k \longrightarrow W(k)$ <u>and</u> $a_o \neq o$.

(For convenience we write $c\,\phi$ instead of $\underset{\sim}{c}\,\phi$ for matrices c and $\phi \in C^2$) The explicit form d4 of the theorem is due to Kneppers. The theorem gives explicit generators for the covariant Dieudonné module of G, e.g. in d4 it has two generators ϕ_1, ϕ_2 subject to the relations $p\,\phi_1 = V^h\,\phi_2$ and $p\,\phi_2 = -V^{h+m}\left(\sum_{i=o}^{\gamma-1} V^i \underset{\sim}{a}_i \phi_2\right) - V^{h+m+n}\phi_1$.
The subdivision a, b, c and d reflects a normal form for the first non zero Hasse-Witt matrix of G. Combining all possibilities for a curve of genus 2 with Hasse-Witt matrix $\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}$ one finds that the completion of its Jacobivariety over an algebraically closed field k of characteristic $p > o$ can be given in the form $p\phi = V\begin{pmatrix} o & 1 \\ o & o \end{pmatrix} - V^2\begin{pmatrix} o & o \\ o & a \end{pmatrix} - V^3\begin{pmatrix} o & o \\ 1 & o \end{pmatrix}$, $a \in \operatorname{Im} T$. Full proofs and results over the base ring W(k) will be published elsewhere.

References

1 E.J. DITTERS, Sur le congruences d'Atkin et de Swinnerton-Dyer. C.R. Acad. Sc. Paris, t. 282 (1976), série A 1131-1134.

2 H. HASSE-E. WITT, Zyklische unverzweigte Erweiterungs Körper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p. Monatshefte für Math. und Phys. 43 (1936), 477-492.

3 T. HONDA, On the theory of commutative formal groups. J. Math. Soc. Japan 22 (1970) 213-246.

4 N. KOBLITZ, p-adic variation of the zeta-function over families of varieties defined over finite fields. Comp. Math. 31 (1975), 119-218.

5 Yu. I. MANIN, The theory of commutative formal groups over fields of finite characteristic. Russ. Math. Surv. 18 (1963), 1-83.

Bert DITTERS
Wiskundig Seminarium
Vrije Universiteit
De Boelelaan 1081,
1007 MC Amsterdam,
the Netherlands.