

Astérisque

MICHIEL HAZEWINKEL

**On formal groups. The functional equation lemma
and some of its applications**

Astérisque, tome 63 (1979), p. 73-82

<http://www.numdam.org/item?id=AST_1979__63__73_0>

© Société mathématique de France, 1979, tous droits réservés.

L'accès aux archives de la collection « Astérisque » (<http://smf4.emath.fr/Publications/Asterisque/>) implique l'accord avec les conditions générales d'utilisation (<http://www.numdam.org/conditions>). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques

<http://www.numdam.org/>

ON FORMAL GROUPS. THE FUNCTIONAL EQUATION
LEMMA AND SOME OF ITS APPLICATIONS.

par

Michiel Hazewinkel

(Rotterdam)

--:--:--

1. INTRODUCTION. Let R be a ring and let $F(X,Y)$ be an n -dimensional commutative formal group law over R . Assume that R is torsion free and let $f(X)$ over $R \otimes \mathbb{Q}$ be the logarithm of $F(X,Y)$. Roughly, the functional equation lemma to be discussed below says what kind of regularity $f(X) \in R \otimes \mathbb{Q}[[X]]^n$ must exhibit in order that it be the logarithm of a formal group law with coefficients in R . The precise statement of the lemma is in section 2 below. The lemma turns out to have many more applications (then just the construction of universal formal group laws). It is the purpose of the present paper to outline a few of these and to try to convince the reader of the power of the lemma in proving a large variety of integrality statements. (Because commutative formal group laws over \mathbb{Q} -algebras are trivial, the theory of commutative formal group laws over torsion free rings is largely a matter of integrality statements). To cite a few instances: the integrality of the addition and multiplication polynomials of the Witt vectors, the Atkin-Swinnerton Dyer congruences, the construction of generalized Lubin-Tate formal group laws ("tapis de Cartier") can all be seen as applications of the functional equation lemma. Many more applications of the functional equation lemma can be found in [7] and [8]. This paper contains no new results or proofs which are not also in [7], with the exception of the proof of " $v(M,\eta)(X)$ reduces to $V(X)$ " in section 6 below, which in [7] is done in a needlessly cumbersome fashion.

2. THE FUNCTIONAL EQUATION LEMMA. The ingredients we need are the following

$$(2.1) \quad B \subset L, \mathfrak{a} \subset B, \sigma : L \rightarrow L, p, q, s_1, s_2, \dots$$

Here B is a subring of a ring L , \mathfrak{a} is an ideal in B , σ a ring endomorphism of L , p is a prime number, q is a power of p and the s_i , $i = 1, 2, \dots$ are $m \times m$ matrices with their coefficients in L . These ingredients are supposed to satisfy the following conditions

$$(2.2) \quad p \in \mathfrak{a}, \sigma(b) \equiv b^q \pmod{\mathfrak{a}} \text{ for all } b \in B, \sigma^r(s_i(j,k)) \mathfrak{a} \subset B \text{ for all } i, j, k, r$$

Here $s_i(j,k)$ is the (j,k) -entry of the matrix s_i . For example if $\mathfrak{a} = B$ then the last condition means that $s_i(j,k) \in B$; and if e.g. $B = \mathbb{Z}$, $L = \mathbb{Q}$, $\sigma = \text{id}$, $q = p$ then the conditions are satisfied iff $s_i(j,k) \in p^{-1}\mathbb{Z}$ for all i, j, k .

If $g(X)$ is an m -tuple of power series in X_1, \dots, X_n with coefficients in L then we denote with $\sigma_*g(X)$ the m -tuple of power series obtained by applying σ to the coefficients of $g(X)$.

2.3. Functional Equation Lemma. Let $f(X) \in L[[X]]^m$ be an m -tuple of power series in m indeterminates X_1, \dots, X_m and $\bar{f}(\bar{X})$ an m -tuple of power series in n indeterminates $\bar{X}_1, \dots, \bar{X}_n$. Suppose that $f(X) \equiv b_1 X \pmod{(\text{degree } 2)}$ where b_1 is a matrix with coefficients in B which is invertible (over $B)$. Suppose moreover that

$$(2.4) \quad f(X) - \sum_{i=1}^{\infty} s_i \sigma_*^i f(X^q) \in B[[X]]^m, \quad \bar{f}(\bar{X}) - \sum_{i=1}^{\infty} s_i \sigma_*^i \bar{f}(\bar{X}^q) \in B[[\bar{X}]]^m$$

where X^q and \bar{X}^q are short for (X_1^q, \dots, X_m^q) and $(\bar{X}_1^q, \dots, \bar{X}_n^q)$. Then we have

$$(2.5) \quad F(X, Y) = f^{-1}(f(X) + f(Y)) \in B[[X; Y]]^m$$

$$(2.6) \quad \bar{f}^{-1}(\bar{f}(X)) \in B[[\bar{X}]]^m.$$

Let $\hat{h}(\hat{X}) \in B[[\hat{X}]]^m$ be an m -tuple of power series with coefficients in B in yet another set of indeterminates and let $\hat{f}(X) = f(\hat{h}(\hat{X}))$. Then

$$(2.7) \quad \hat{f}(\hat{X}) - \sum_{i=1}^{\infty} s_i \sigma_*^i \hat{f}(\hat{X}^q) \in B[[\hat{X}]]$$

Finally let $\alpha(\hat{X}) \in B[[\hat{X}]]^m$, $\beta(\hat{X}) \in L[[\hat{X}]]^m$, $r \in \mathbb{N} = \{1, 2, \dots\}$. Then

$$(2.8) \quad \alpha(\hat{X}) \equiv \beta(\hat{X}) \pmod{\mathfrak{a}^r} \iff f(\alpha(\hat{X})) \equiv f(\beta(\hat{X})) \pmod{\mathfrak{a}^r}$$

For a proof cf. [7], sections 2 and 10.

3. SOME ALMOST TRIVIAL APPLICATIONS. Let $H(X) = X + p^{-1}X^p + p^{-2}X^{p^2} + \dots$ and $\ell(X) = \log(1+X) = \sum_{n=1}^{\infty} (-1)^{n+1} n^{-1} X^n$. One notes that $H(X) - p^{-1}H(X^p) = X$ and $\ell(X) - p^{-1}\ell(X^p) \in \mathbb{Z}_{(p)}[X]$. So taking $B = \mathbb{Z}_{(p)}$, $\mathfrak{a} = pB$, $L = \mathbb{Q}$, $q = p$, $s_1 = p^{-1}$, $s_2 = s_3 = \dots = 0$ and $\sigma = \text{id}$, we obtain from (2.6) Hasse's old result that $\exp(H(X))$ has its coefficients in $\mathbb{Z}_{(p)}$.

More generally let $d(X) = d_0 X + d_1 X^p + \dots$, $d_i \in \mathbb{Q}$. Using the same ingredients and combining (2.6) and (2.7) above one finds that $\exp(d(X)) \in \mathbb{Z}_{(p)}[[X]]$ if and only if $d_i \cdot p^{-1} d_{i-1} \in \mathbb{Z}_{(p)}$ for all i (where one takes $d_{-1} = 0$). This is a lemma of Dieudonné [3].

An easy application with σ non trivial is the following. Let B be the ring of integers of the completed maximal unramified extension T of \mathbb{Q}_p ; let $L = T$, $p = q$, $s_1 = p^{-1}$, $s_2 = s_3 = \dots = 0$, and σ the Frobenius automorphism of T . Let $h(X) = 1 + a_1 X + a_2 X^2 + \dots \in T[[X]]$. In this setting the combination of (2.6) and (2.7) yields that $h(X) \in B[[X]]$ if and only if $\sigma_* h(X^p)/h(X)^p \in 1 + pXB[[X]]$, which is lemma 1 of Dwork [6].

For an easy more dimensional application consider the slightly modified Witt vector polynomials $\bar{w}_0(X) = X_0$, $\bar{w}_1(X) = X_1 + p^{-1}X_0^p$, \dots , $\bar{w}_n(X) = X_n + p^{-1}X_{n-1}^p + \dots + p^{-n}X_0^{p^n}$. Take $B = \mathbb{Z}$, $\mathfrak{a} = p\mathbb{Z}$, $L = \mathbb{Q}$, $\sigma = \text{id}$, $q = p$, $s_2, s_3, \dots = 0$ and let s_1 be the $(n+1) \times (n+1)$ matrix with p^{-1} on the first subdiagonal and zero's elsewhere; i.e. $s_1(j, k) = 0$ unless $j = k + 1$ and $s_1(k+1, k) = p^{-1}$, $k = 1, 2, \dots, n$. Let $\bar{w}(X)$ be the column vector $(\bar{w}_0(X), \dots, \bar{w}_n(X))$. Then, obviously, $\bar{w}(X) = X + s_1 \bar{w}(X^p)$. It now follows from (2.5) that $\Sigma(X) = \bar{w}^{-1}(\bar{w}(X) + \bar{w}(Y))$ has integral coefficients; or, multiplying both sides of $\bar{w}(\Sigma(X)) = \bar{w}(X) + \bar{w}(Y)$ with p^n , we see that we have shown that the addition polynomials of the Witt vectors have integral coefficients.

4. ATKIN-SWINNERTON DYER CONGRUENCES. Let E be an elliptic curve over \mathbb{Q} and let $L(s) = \prod_p (1 - a_p p^{-s} + b_p p^{1-2s})^{-1}$ be its global L-function, where the local factors $(1 - a_p p^{-s} + b_p p^{1-2s})^{-1}$ are defined as follows in terms of the

reductions mod p of a global minimal model D over \mathbb{Z} for E :

- (i) if p is good, i.e. if $D \otimes \mathbb{Z}/(p)$ is nonsingular then $(1 - a_p^{-s} + b_p^{-2s})$ is the numerator of the zetafunction of the elliptic curve $D \otimes \mathbb{Z}/(p)$ over $\mathbb{Z}/(p)$;
- (ii) if $D \otimes \mathbb{Z}/(p)$ has an ordinary doublepoint then $1 - a_p^{-s} + b_p^{-2s} = 1 - \varepsilon_p^{-s}$ where $\varepsilon_p = \pm 1$ depending on whether the tangents in the double point are rational over $\mathbb{Z}/(p)$ or not;
- (iii) if $D \otimes \mathbb{Z}/(p)$ has a cusp $1 - a_p^{-s} + b_p^{-2s} = 1$.

Now let $f_E(X) = \sum_{n=1}^{\infty} n^{-1} a_n X^n$ where $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$. Then an immediate and

obvious consequence of the Euler product structure of $L(s)$ is that for all p

$$(4.1) \quad f_E(X) - p^{-1} a_p f_E(X^p) + p^{-1} b_p f_E(X^{p^2}) \in \mathbb{Z}_{(p)}[X].$$

It now follows from (2.5) that $F_E(X,Y) = f_E^{-1}(f_E(X) + f_E(Y))$ is a formal group law over \mathbb{Z} . Let $G_E(X,Y)$ be the formal completion along the identity of the minimal model D over \mathbb{Z} . The formal group law $G_E(X,Y)$ can be explicitly described as follows. Let D be given by $y^2 + c_1 XY + c_3 Y = X^3 + c_2 X^2 + c_4 X + c_6$; let $\omega = (2Y + c_1 X + c_3)^{-1} dX$ be the invariant differential and $z = (2Y)^{-1} X$ a local parameter at zero. Let, locally, $\omega = \sum \beta(n) z^{n-1} dz$ and define $g_E(X) = \sum_{n=1}^{\infty} n^{-1} \beta(n) X^n$,

then $G_E(X,Y) = g_E^{-1}(g_E(X) + g_E(Y))$. This comes from the fact that if $f(X)$ is the logarithm of a formal group law $F(X,Y)$ over a torsion free ring R then $df(X)$ is an invariant differential for $F(X,Y)$.

4.2. Theorem (Honda, Hill; [11], [10] and [12]). The formal group laws $F_E(X,Y)$ and $G_E(X,Y)$ are strictly isomorphic over \mathbb{Z} (i.e. there exists a power series $\phi(X) = X + b_2 X^2 + \dots$, $b_i \in \mathbb{Z}$ such that $\phi(F_E(X,Y)) = G_E(\phi(X), \phi(Y))$).

It follows that $g_E(X) = f_E(\phi^{-1}(X))$. So that by (2.7) we have that $g_E(X)$ also satisfies the integrality conditions (4.1). Writing this out in terms of coefficients one finds the Atkin Swinnerton-Dyer congruences.

$$(4.3) \quad \beta(np) - a_p \beta(n) + b_p \beta(n/p) \equiv 0 \pmod{p^s} \text{ if } n \equiv 0 \pmod{p^{s-1}}$$

where $\beta(n//p) = \beta(n/p)$ if $p|n$ and $\beta(n//p) = 0$ otherwise.

5. LUBIN-TATE FORMAL GROUP LAWS. The so-called Lubin-Tate formal group laws are constructed as follows in [13]. Let K be a local field with finite residue field (i.e. K is a finite extension of \mathbb{Q}_p or $\mathbb{F}_p(x)$); let A be the ring of integers of K , let π be a uniformizing element and let q be the number of

elements of k , the residue field of K . Let $e(X) \in A[[X]]$ be any power series in one variable such that

$$(5.1) \quad e(X) \equiv \pi X \pmod{\text{degree } 2}, \quad e(X) \equiv X^q \pmod{\pi}$$

Then there is a unique power series $F_e(X,Y)$ such that $F_e(e(X),e(Y)) = e(F_e(X,Y))$ and $F_e(X,Y) \equiv X + Y \pmod{\text{degree } 2}$. This is a formal group law over A . Moreover for all $a \in A$ there is a unique power series $[a]_e(X)$ such that $e([a]_e(X)) = [a]_e(e(X))$ and $[a]_e(X) \equiv aX \pmod{\text{degree } 2}$; the map $a \mapsto [a]_e(X)$ defines a ring homomorphism $A \rightarrow \text{End}_A(F(X,Y))$ and $[\pi]_e(X) = e(X)$. Finally if both $e(X)$ and $e'(X)$ satisfy (5.1) (with respect to the same π) then $F_e(X,Y)$ and $F_{e'}(X,Y)$ are strictly isomorphic over A .

In the ingredients (2.1) for the functional equation lemma now take $B = A$, $L = K$, $\mathfrak{a} = \pi A$, $p = \text{char}(k)$, $q = \frac{1}{p}k$, $\sigma = \text{id}$, $s_1 = \pi^{-1}$, $0 = s_2 = s_3 = \dots$. Then the conditions (2.2) are satisfied. Let $g(X) \in A[[X]]$ be any power series such that $g(X) \equiv X \pmod{\text{degree } 2}$, and consider $f(X) \in K[[X]]$ defined (recursively) by the functional equation

$$(5.2) \quad f(X) = g(X) + \pi^{-1}f(X^q)$$

Then parts (2.5) and (2.6) of the functional equation lemma say that the power series

$$(5.3) \quad F(X,Y) = f^{-1}(f(X) + f(Y)), \quad [a](X) = f^{-1}(af(X)), \quad a \in A$$

have their coefficients in A and hence define a formal A -module over A . (A formal A -module, where A is as above, over an A -algebra R is a formal group law $F(X,Y)$ over R together with a ring endomorphism $\rho_F: A \rightarrow \text{End}_R(F(X,Y))$ such that $\rho_F(a) \equiv aX \pmod{\text{degree } 2}$ for all $a \in A$). Now consider $[\pi](X)$. We have

$$(5.4) \quad f([\pi](X)) = \pi f(X) = \pi g(X) + f(X^q) \equiv f(X^q) \pmod{\pi}$$

It follows by part (2.8) of the functional equation lemma that $[\pi](X) \equiv X^q \pmod{\pi}$. Also of course (cf. (5.3)) $F([\pi](X),[\pi](Y)) = [\pi](F(X,Y))$ so that $F(X,Y)$ is a Lubin-Tate formal group law with $e(X) = [\pi](X)$. As all Lubin-Tate formal group laws constructed via the same uniformizing element π are strictly isomorphic, it follows from part (2.7) of the functional equation lemma that all Lubin-Tate formal group laws are obtained by the construction (5.2), (5.3) by varying

$g(X)$.

Finally we use the functional equation lemma to show that Lubin-Tate formal group laws constructed via different uniformizing elements π and $\bar{\pi}$ become isomorphic over \hat{A}_{nr} , the completion of the ring of integers of the completion \hat{K}_{nr} of the maximal unramified extension K_{nr} of K . Let therefore $f(X), \bar{f}(X) \in A[[X]]$ satisfy

$$(5.5) \quad f(X) - \pi^{-1}f(X^q) \in A[[X]], \quad \bar{f}(X) - \bar{\pi}^{-1}\bar{f}(X^q) \in A[[X]]$$

Now take as functional equation ingredients $B = \hat{A}_{nr}$, $\mathfrak{a} = \pi B$, $L = \hat{K}_{nr}$, σ the Frobenius substitution in $\text{Gal}(K_{nr}/K)$ extended by continuity to \hat{K}_{nr} , p, q, s_1, s_2, \dots as before. Let $u \in \hat{A}_{nr}^*$, the units of \hat{A}_{nr} , be such that $u^{-1}\sigma(u) = \pi^{-1}\bar{\pi}$. (Such a u exists). Then we have

$$(5.6) \quad \begin{aligned} uf(X) - \bar{\pi}^{-1}\sigma_*(uf(X^q)) &= uf(X) - \bar{\pi}^{-1}\sigma(u)f(X^q) = \\ &= u(f(X) - \pi^{-1}f(X^q)) \in \hat{A}_{nr}[[X]] \end{aligned}$$

and also of course $\bar{f}(X) - \bar{\pi}^{-1}\sigma_*\bar{f}(X^q) = \bar{f}(X) - \pi^{-1}\bar{f}(X^q) \in A[[X]] \subset \hat{A}_{nr}[[X]]$, so that by part (2.6) of the functional equation lemma we have that

$$(5.7) \quad \phi(X) = \bar{f}^{-1}(uf(X)) \in \hat{A}_{nr}[[X]]$$

which defines as an isomorphism $\phi(X)$ between the formal A -modules defined by $f(X)$ and $\bar{f}(X)$ as in (5.3).

6. TAPIS DE CARTIER. Let A be the ring of integers of an unramified extension K of \mathbb{Q}_p . Let $\sigma \in \text{Gal}(K/\mathbb{Q}_p)$ be the Frobenius automorphism. Now suppose we have given a free A -module M of finite rank $h < \infty$ together with a semilinear endomorphism $\eta : M \rightarrow M$ (i.e. $\eta(m+m') = \eta(m) + \eta(m')$, $\eta(am) = \sigma(a)\eta(m)$). To these data we associate a formal group law over A as follows. Let $D(\eta)$ be the matrix of η with respect to some basis for M . Define $g(M, \eta)(X) \in K[[X_1, \dots, X_h]]^h$ by the equation

$$(6.1) \quad g(M, \eta)(X) = X + p^{-1}D(\eta)\sigma_*g(M, \eta)(X^p)$$

By part (2.5) of the functional equation lemma (with $B = A$, $L = K$, $\mathfrak{a} = pA$, σ as above, $q = p$, $s_1 = p^{-1}D(\eta)$, $s_2 = s_3 = \dots = 0$) it follows that $G(M, \eta)(X, Y) = g(M, \eta)^{-1}(g(M, \eta)(X) + g(M, \eta)(Y))$ is a formal group law over A . This

construction is functorial in the following sense. Let $\alpha : (M, \eta) \rightarrow (M', \eta')$ be a morphism. This means that $\alpha : M \rightarrow M'$ is A -linear and that $\eta'\alpha = \alpha\eta$. Let $E(\alpha)$ be the matrix of α with respect to the chosen bases of M and M' . Then we have $E(\alpha)g(M, \eta)(X) - p^{-1}D(\eta')\sigma_*(E(\alpha)g(M, \eta)(X^p)) = E(\alpha)X \in A[[X]]^h$, because $\eta'\alpha = \alpha\eta$, together with the semilinearity of η and η' , precisely means that $D(\eta')\sigma_*(E(\alpha)) = E(\alpha)D(\eta)$. It follows in particular that $G(M, \eta)(X, Y)$ does not depend (up to isomorphism) on the choice of a basis for M .

For each (M, η) as above let (M^σ, η) be the pair obtained by leaving the additive group M and the map η unchanged but by changing the A -action to $a \cdot m = \sigma^{-1}(a)m$. One easily checks that $G(M^\sigma, \eta) = \sigma_*G(M, \eta)$. There is an obvious morphism $(M^\sigma, \eta) \rightarrow (M, \eta)$, viz. η itself. Let $v(M, \eta) : \sigma_*G(M, \eta) \rightarrow G(M, \eta)$ be the corresponding morphism of formal groups. We claim that $v(M, \eta)$ reduces mod p to the Verschiebung morphism $V(X) : \sigma_*\bar{G}(X, Y) \rightarrow \bar{G}(X, Y)$ over k where the bar denotes reduction mod p and where we omitted to write (M, η) . (If $F(X, Y)$ is a formal group law over k , then $V(X) : \sigma_*F(X, Y) \rightarrow F(X, Y)$ is the power series over k defined by $V(X^p) = [p](X)$ (because $\text{char}(k) = p$, $[p](X)$ is necessarily a power series in X^p). This is seen as follows. We have

$$g(M, \eta)v(X^q) = D(\eta)g(M^\sigma, \eta)(X^q) = D(\eta)\sigma_*g(M, \eta)(X^q) \equiv pg(M, \eta)(X) \pmod{pA}$$

It follows by part (2.8) of the functional equation lemma that $v(X^q) \equiv g(M, \eta)^{-1}(pg(M, \eta)(X)) = [p](X) \pmod{pB}$, proving our claim.

Thus we have a functor $(M, \eta) \mapsto (G(M, \eta), v(M, \eta))$. There is an obvious functor in the inverse direction, viz. taking Lie-algebras. And we clearly have $\text{Lie}(G(M, \eta)) = M$, $\text{Lie}(v(M, \eta)) = \eta$. The Tapis de Cartier ([1], [2], [7]) now says that these functors are inverse equivalence of categories. To prove this we have to show that every formal group law $F(X, Y)$ together with a morphism $v : \sigma_*F(X, Y) \rightarrow F(X, Y)$ over A which reduces to $V(X) \pmod{pA}$ comes from a pair (M, η) .

To prove this we first remark that, because A is unramified, every $F(X, Y)$ over A is of functional equation type (Honda [12], cf. [7], section 20.3) i.e. if $f(X)$ is the logarithm of $F(X, Y)$ then there are s_1, s_2, \dots such that $f(X) - \sum s_i \sigma_i^* f(X^{p^i}) \in A[[X]]^h$, where $h = \dim(F(X, Y))$. Now a homomorphism $v(X) : \sigma_*F(X, Y) \rightarrow F(X, Y)$ is necessarily of the form $v(X) = f^{-1}(E\sigma_*f(X))$ for some matrix E .

Hence $f^{-1}(pf(X)) = [p](X) \equiv v(X^p) = f^{-1}(E\sigma_*f(X^p))$. It follows by part (2.8) of the functional equation lemma that $pf(X) \equiv E\sigma_*f(X^p) \pmod{pA}$, i.e. that $f(X) - p^{-1}E\sigma_*f(X^p) \in A[[X]]$, so that by part (2.6) of the functional equation

lemma $F(X,Y)$ is strictly isomorphic to the formal group law with logarithm defined by $g(X) = X + p^{-1}\text{Eg}(X^p)$ which is of the form $g(M,\eta)(X)$.

For some details about the rôle which the tapis de Cartier plays in the theory of lifting formal group laws cf. [7], section 30, as well as for an analogous theory for formal A -modules, where A is a finite extension of \mathbb{Q}_p or $\mathbb{F}_p(x)$.

7. RAMIFIED WITT VECTORS. Let A be the ring of integers of a finite (not necessarily unramified) extension K of \mathbb{Q}_p or $\mathbb{F}_p(x)$. Let k be the residue field of K , $q = \#k = p^r$, π a uniformizing element. Consider the power series

$$(7.1) \quad g_\pi(X) = X + \pi^{-1}X^q + \pi^{-2}X^{q^2} + \dots, \quad G_\pi(X,Y) = g_\pi^{-1}(g_\pi(X) + g_\pi(Y))$$

Then $g_\pi(X) = X + \pi^{-1}g_\pi(X^q)$ so that by section 5 above, $G_\pi(X,Y)$ is a Lubin-Tate formal group law over A . For every A -torsion free A -algebra B let $W_{q,\infty}^A(B)$ be the following set of power series in one variable t

$$(7.2) \quad W_{q,\infty}^A(B) = \{\gamma(t) \in B[[t]] \mid \gamma(0) = 0, g_\pi \gamma(t) = \sum_{i=0}^{\infty} x_i t^{q^i} \text{ for certain } x_i \in B \otimes_A K\}$$

For arbitrary A -algebras B one can define $W_{q,\infty}^A(B) = \{\phi_* \gamma(t) \mid \gamma(t) \in W_{q,\infty}^A(B')\}$ where B' is any A -torsion free A -algebra with a surjective A -algebra homomorphism $\phi : B' \rightarrow B$. The sets $W_{q,\infty}^A(B)$ have a natural group structure defined by $\gamma(t) + \delta(t) = G_\pi(\gamma(t), \delta(t))$ and a topology defined by the subgroups $\{\gamma(t) \in W_{q,\infty}^A(B) \mid \gamma(t) \equiv 0 \pmod{t^{q^n}}\}$. There is an obvious morphism $W_{q,\infty}^A(B_1) \rightarrow W_{q,\infty}^A(B_2)$ attached to an A -algebra homomorphism $\phi : B_1 \rightarrow B_2$, viz. $\gamma(t) \mapsto \phi_* \gamma(t)$. So that we have a complete topological group valued functor $B \mapsto W_{q,\infty}^A(B)$.

We are now going to define a functorial ring structure on $W_{q,\infty}^A(B)$. The definition for A -torsion free A -algebras B is:

$$(7.3) \quad \text{if } g_\pi \gamma(t) = \sum x_i t^{q^i}, g_\pi \delta(t) = \sum y_i t^{q^i}, \text{ then } \gamma(t)\delta(t) = g_\pi^{-1}(\sum \pi^i x_i y_i t^{q^i})$$

To show that this is welldefined we must show that the coefficients of $\gamma(t)\delta(t)$ are in B (and not just in $B \otimes_A K$). This is seen as follows.

Assume that B is A -torsion free and admits an A -algebra endomorphism σ such that $\sigma(b) \equiv b^q \pmod{\pi B}$ for all $b \in B$. By part (2.7) of lemma 2.3 we then

have $x_i - \pi^{-1}x_{i-1} = a_i \in B$, $y_i - \pi^{-1}x_{i-1} = b_i \in B$ for all i (with $x_{-1} = y_{-1} = 0$). Hence $\pi^i x_i, \pi^i y_i \in B$ for all i . It follows that $\pi^i x_i y_i - \pi^{-1}(\pi^{i-1} x_{i-1} y_{i-1}) = \pi^i a_i b_i + \pi^{i-1} a_i y_{i-1} + \pi^{i-1} b_i x_{i-1} \in B$, so that by part (2.6) of lemma 2.3 we have indeed that $g_\pi^{-1}(\sum \pi^i x_i y_i t^{q^i})$ has its coefficients in B . To extend this definition to the case of arbitrary A -algebras B use an argument similar as just below (7.2) using that every A -algebra B is a quotient of an A -algebra B' which satisfies our assumptions, e.g. $B' = A[Z_b | b \in B]$. There is also a natural A -module structure on $W_{q,\infty}^A(B)$ defined by $\gamma(t) \mapsto [a](\gamma(t))$ where $[a](X) = g_\pi^{-1}(ag_\pi(X))$, $a \in A$, cf. also section 5. All in all this defines a functor $W_{q,\infty}^A: \underline{\text{Alg}}_A \rightarrow \underline{\text{Alg}}_A$, which, we claim, possibly deserves the name "ramified Witt vector functor". To bolster this claim we remark the following

- There is an additive Verschiebung morphism \underline{V}_q defined by $\underline{V}_q \gamma(t) = \gamma(t^q)$ and a Frobenius A -algebra functor endomorphism \underline{f}_π . The latter is defined for A -torsion free A -algebras B by the formula $\underline{f}_\pi \gamma(t) = g_\pi^{-1}(\sum_{i=0}^{\infty} \pi x_{i+1} t^{q^i})$ where the

x_i are as in (7.3). Of course the integrality of $\underline{f}_\pi \gamma(t)$ is proved by means of the functional equation lemma. We have $\underline{f}_\pi \underline{V}_q = [\pi]$, $\underline{f}_\pi \gamma(t) \equiv \gamma(t)^q \pmod{[\pi]W_{q,\infty}^A(B)}$.

- Let A' be the ring of integers of an unramified extension K' of K . Let k' be the residue field of K' and let $\sigma \in \text{Gal}(K'/K)$ be the Frobenius automorphism. For each $a' \in A'$ let $\Delta(a') = g_\pi^{-1}(\sum_{i=0}^{\infty} \pi^{-i} \sigma^i(a') t^{q^i}) \in W_{q,\infty}^A(B)$. (Integrality of

$\Delta(a')$ is of course proved by means of the functional equation lemma). Then

$a' \mapsto \Delta(a')$ is a homomorphism of A -algebras and the composite $A' \xrightarrow{\Delta} W_{q,\infty}^A(A') \rightarrow W_{q,\infty}^A(k')$ is an isomorphism. In particular $W_{q,\infty}^A(k') = A'$ with σ corresponding to \underline{f}_π , generalizing a wellknown property of the Witt vectors.

- There is an A -algebra homomorphism $\Delta: W_{q,\infty}^A(-) \rightarrow W_{q,\infty}^A(W_{q,\infty}^A(-))$, the ramified Artin-Hasse exponential, characterized by $w_{q,i}^A \circ \Delta = \underline{f}_\pi^i$, where $w_{q,i}^A: W_{q,\infty}^A(B) \rightarrow B$ is the functorial A -algebra homomorphism $w_{q,i}^A(\gamma(t)) = \pi^i$ times the coefficient of t^{q^i} in $g_\pi(\gamma(t))$.

For more details concerning this construction cf. [7], section 25 ; for a twisted version of these constructions which also works for local fields with not necessarily finite residue field cf. also [9]. Another construction of the functors $W_{q,\infty}^A$ has independently been given by Ditters [4] and Drinfel'd [5].

BIBLIOGRAPHY.

1. P. Cartier, Groupes de Lubin-Tate Généralisés, *Inv. Math.* 35(1976), 273-284.
2. P. Cartier, Séminaire sur les groupes formels IHES 1972, Unpublished Notes.
3. J. Dieudonné, On the Artin-Hasse exponential series, *Proc. Amer. Math. Soc.* 8 (1957), 210-214.
4. E. Ditters, Formale Gruppen, die Vermutungen von Atkin-Swinnerton Dyer und verzweigte Witt Vektoren, *Lecture Notes*, Göttingen, 1975.
5. V.G. Drinfel'd, Coverings of p-adic symmetric domains (Russian), *Funk. Analiz i ego pril.* 10(1976), 29-40.
6. B. Dwork, Norm residue symbol in local number fields, *Abh. Math. Sem. Hamburg* 22(1958), 180-190.
7. M. Hazewinkel, Formal groups and applications, *Acad. Pr.*, 1978.
8. M. Hazewinkel, Infinite dimensional universal formal group laws and formal A-modules, In: *Proc. Copenhagen Summer Meeting Algebraic Geometry 1978*, to appear *Lect. Notes in Math.*, Springer 1979.
9. M. Hazewinkel, Twisted Lubin-Tate formal groups laws, ramified Witt vectors and ramified Artin-Hasse exponential mappings, preprint Erasmus univ. R'dam, 1977.
10. W. Hill, Formal groups and zeta-functions of elliptic curves, *Inv. Math.* 12 (1971), 321-336.
11. T. Honda, Formal groups and zeta functions, *Osaka J. Math.* 5(1968), 199-213.
12. T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan* 22(1970), 213-246.
13. J. Lubin, J. Tate, Formal complex multiplication in local fields, *Ann. of Math.* 81 (1965), 380-387.

Michiel HAZEWINDEL
Department of Mathematics
Erasmus Universiteit Rotterdam
P.O. Box 1738
Rotterdam, The Netherlands