

TWISTED LUBIN-TATE FORMAL GROUP LAWS, RAMIFIED WITT VECTORS AND (RAMIFIED) ARTIN-HASSE EXPONENTIALS

BY

MICHIEL HAZEWINDEL

ABSTRACT. For any ring R let $\Lambda(R)$ denote the multiplicative group of power series of the form $1 + a_1t + \cdots$ with coefficients in R . The Artin-Hasse exponential mappings are homomorphisms $W_{p,\infty}(k) \rightarrow \Lambda(W_{p,\infty}(k))$, which satisfy certain additional properties. Somewhat reformulated, the Artin-Hasse exponentials turn out to be special cases of a functorial ring homomorphism $E: W_{p,\infty}(-) \rightarrow W_{p,\infty}(W_{p,\infty}(-))$, where $W_{p,\infty}$ is the functor of infinite-length Witt vectors associated to the prime p . In this paper we present ramified versions of both $W_{p,\infty}(-)$ and E , with $W_{p,\infty}(-)$ replaced by a functor $W_{q,\infty}^F(-)$, which is essentially the functor of q -typical curves in a (twisted) Lubin-Tate formal group law over A , where A is a discrete valuation ring that admits a Frobenius-like endomorphism σ (we require $\sigma(a) \equiv a^q \pmod{\mathfrak{m}}$ for all $a \in A$, where $\mathfrak{m}$ is the maximal ideal of A). These ramified-Witt-vector functors $W_{q,\infty}^F(-)$ do indeed have the property that, if $k = A/\mathfrak{m}$ is perfect, A is complete, and l/k is a finite extension of k , then $W_{q,\infty}^F(l)$ is the ring of integers of the unique unramified extension L/K covering l/k .

1. Introduction. For each ring R (commutative with unit element 1) let $\Lambda(R)$ be the abelian group of power series of the form $1 + r_1t + r_2t^2 + \cdots$. Let $W_{p,\infty}(R)$ be the ring of Witt vectors of infinite length associated to the prime p with coefficients in R . Then the "classical" Artin-Hasse exponential mapping is a map $E: W_{p,\infty}(k) \rightarrow \Lambda(W_{p,\infty}(k))$ defined for all perfect fields k as follows (cf. e.g. [1] and [13]). Let $\Phi(y)$ be the power series

$$\Phi(y) = \prod_{(p,n)=1} (1 - y^n)^{\mu(n)/n},$$

where $\mu(n)$ is the Möbius function. Then $\Phi(y)$ has its coefficients in $\mathbb{Z}_p$, cf. e.g. [13]. Because k is perfect every element of $W_{p,\infty}(k)$ can be written in the form $\mathbf{b} = \sum_{i=1}^{\infty} \tau(c_i)p^i$, with $c_i \in k$, and $\tau: k \rightarrow W_{p,\infty}(k)$ the unique system of multiplicative representatives. One now defines

$$E: W_{p,\infty}(k) \rightarrow \Lambda(W_{p,\infty}(k)), \quad E(\mathbf{b}) = \prod_{i=0}^{\infty} \Phi(\tau(c_i)t)^{p^i}.$$

Now let $W(-)$ be the ring functor of big Witt vectors. Then $W(-)$ and $\Lambda(-)$ are isomorphic, the isomorphism being given by $(a_1, a_2, \dots) \mapsto \prod_{i=1}^{\infty} (1 - a_i t^i)$, cf. [2]. Now there is a canonical quotient map $W(-) \rightarrow W_{p,\infty}(-)$ and composing E with $\Lambda(-) \simeq W(-)$ and $W(-) \rightarrow W_{p,\infty}(-)$ we find an Artin-Hasse exponential $E: W_{p,\infty}(k) \rightarrow W_{p,\infty}(W_{p,\infty}(k))$.

Received by the editors October 31, 1977.

AMS (MOS) subject classifications (1970). Primary 14L05; Secondary 12B25, 13K05.

© 1980 American Mathematical Society
0002-9947/80/0000-0202/\$05.25

1.1. THEOREM. *There exists a unique functorial homomorphism of ring-valued functors $E: W_{p,\infty}(-) \rightarrow W_{p,\infty}(W_{p,\infty}(-))$ such that for all $n = 0, 1, 2, \dots$, $w_{p,n} \circ E = \mathbf{f}^n$, where $\mathbf{f}$ is the Frobenius endomorphism of $W_{p,\infty}(-)$ and where $w_{p,n}: W_{p,\infty}(W_{p,\infty}(-)) \rightarrow W_{p,\infty}(-)$ is the ring homomorphism which assigns to the sequence $(b_0, b_1, \dots)$ of Witt vectors the Witt vector $b_0^p + pb_1^{p^{n-1}} + \dots + p^{n-1}b_{n-1}^p + p^n b_n$.*

It should be noted that the classical definition of E given above works only for perfect fields of characteristic $p > 0$. In this form Theorem 1.1 is probably due to Cartier, cf. [5].

Now let A be a complete discrete valuation ring with residue field of characteristic p , such that there exist a power q of p and an automorphism σ of K , the quotient field of A , such that $\sigma(a) \equiv a^q \pmod{\mathfrak{m}}$ for all $a \in A$, where $\mathfrak{m}$ is the maximal ideal of A . It is the purpose of the present paper to define ramified Witt vector functors $W_{q,\infty}^F(-): \mathbf{Alg}_A \rightarrow \mathbf{Alg}_A$, where $\mathbf{Alg}_A$ is the category of A -algebras, and a ramified Artin-Hasse exponential mapping $E: W_{q,\infty}^F(-) \rightarrow W_{q,\infty}^F(W_{q,\infty}^F(-))$.

There is such a ramified-Witt-vector functor $W_{q,\infty}^F$ associated to every twisted Lubin-Tate formal group law $F(X, Y)$ over A . This last notion is defined as follows. Let $f(X) = X + a_2 X^2 + \dots \in K[[X]]$ and suppose that $a_i \in A$ if q does not divide i and $a_{qi} - \omega^{-1}\sigma(a_i) \in A$ for all i for a certain fixed uniformizing element ω . Then $F(X, Y) = f^{-1}(f(X) + f(Y)) \in A[[X, Y]]$, and the formal group laws thus obtained are what we call twisted Lubin-Tate group laws. The Witt-vector functors $W_{q,\infty}^F(-)$ for varying F are isomorphic if the formal group laws are strictly isomorphic. Now every twisted Lubin-Tate formal group law is strictly isomorphic to one of the form $G_\omega(X, Y) = g_\omega^{-1}(g_\omega(X) + g_\omega(Y))$ with $g_\omega(X) = X + \omega^{-1}X^q + \omega^{-1}\sigma(\omega)^{-1}X^{q^2} + \omega^{-1}\sigma(\omega)^{-1}\sigma^2(\omega)^{-1}X^{q^3} + \dots$ which permits us to concentrate on the case $F(X, Y) = G_\omega(X, Y)$ for some ω . The formulas are more pleasing in this case, especially because the only constants which then appear are the $\sigma^i(\omega)$, which is esthetically attractive, because ω is an invariant of the strict isomorphism class of $F(X, Y)$.

The functors $W_{q,\infty}^F$ and the functor morphisms E are Witt-vector-like and Artin-Hasse-exponential-like in that

(i) $W_{q,\infty}^F(B) = \{(b_0, b_1, \dots) | b_i \in B\}$ as a set-valued functor and the A -algebra structure can be defined via suitable Witt-like polynomials $w_{q,n}^F(Z_0, \dots, Z_n)$; cf. below for more details.

(ii) There exist a σ -semilinear A -algebra homomorphism $\mathbf{f}$ (Frobenius) and a σ^{-1} -semilinear A -module homomorphism $\mathbf{V}$ (Verschiebung) with the expected properties, e.g. $\mathbf{fV} = \omega$ where ω is the uniformizing element of A associated to F , and $\mathbf{f}(\mathbf{b}) \equiv \mathbf{b}^q \pmod{\omega W_{q,\infty}^F(B)}$.

(iii) If k , the residue field of A , is perfect and l/k is a finite field extension, then $W_{q,\infty}^F(l) = B$, the ring of integers of the unique unramified extension L/K which covers l/k .

(iv) The Artin-Hasse exponential E is characterized by $w_{q,n}^F \circ E = \mathbf{f}^n$ for all $n = 0, 1, 2, \dots$.

I hope that these constructions will also be useful in a class-field theory setting.

Meanwhile they have been important in formal A -module theory. The results in question have been announced in two notes, [9] and [10], and I now propose to take half a page or so to try to explain these results to some extent.

Let R be a $\mathbb{Z}_{(p)}$ -algebra and let $\text{Cart}_p(R)$ be the Cartier-Dieudonné ring. This is a ring “generated” by two symbols $\mathbf{f}, \mathbf{V}$ over $W_{p,\infty}(R)$ subject to “the relations suggested by the notation used”. For each formal group $F(X, Y)$ over R let $C_p(F; R)$ be its $\text{Cart}_p(R)$ module of p -typical curves. Finally let $\hat{W}_{p,\infty}(-)$ be the formal completion of the functor $W_{p,\infty}(-)$. Then one has

- (a) the functor $F \mapsto C_p(F; R)$ is representable by $\hat{W}_{p,\infty}$ [3].
- (b) The functor $F \mapsto C_p(F; R)$ is an equivalence of categories between the category of formal groups over R and a certain (explicitly describable) subcategory of $\text{Cart}_p(R)$ modules [3].
- (c) There exists a theory of “lifting” formal groups, in which the Artin-Hasse exponential $E: W_{p,\infty}(-) \rightarrow W_{p,\infty}(W_{p,\infty}(-))$ plays an important rôle. These results relate to the so-called “Tapis de Cartier” and relate to certain conjectures of Grothendieck concerning crystalline cohomology ([4] and [5]).

Now let A be a complete discrete valuation ring with residue field k with q elements (for simplicity and/or nontriviality of the theory). A formal A -module over $B \in \mathbf{Alg}_A$ is a formal group law $F(X, Y)$ over B together with a ring homomorphism $\rho_F: A \rightarrow \text{End}_B(F(X, Y))$, such that $\rho_F(a) \equiv aX \pmod{(\text{degree } 2)}$. Then there exist complete analogues of (a), (b), (c) above for the category of formal A -modules over B . Here the rôle of $C_p(F; R)$ is taken over by the q -typical curves $C_q(F; B)$, $W_{p,\infty}(-)$ and $\hat{W}_{p,\infty}$ are replaced by ramified-Witt-vector functors $W_{q,\infty}^\pi(-)$ and $\hat{W}_{q,\infty}^\pi(-)$ associated to an untwisted, i.e. $\sigma = \text{id}$, Lubin-Tate formal group law over A with associated uniformizing element π . Finally, the rôle of E in (c) is taken over by the ramified Hasse-Witt exponential $W_{q,\infty}^\pi(-) \rightarrow W_{q,\infty}^\pi(W_{q,\infty}^\pi(-))$.

As we remarked in (i) above, it is perfectly possible to define and analyse $W_{q,\infty}^F(-)$ by starting with the polynomials $w_{q,n}^F(Z)$ and then proceeding along the lines of Witt’s original paper. And, in fact, in the untwisted case, where k is a field of q -elements, this has been done, independently of this paper, and independently of each other by E. Ditters [7], V. Drinfel’d [8], J. Casey (unpublished) and, very possibly, several others. In this case the relevant polynomials are of course the polynomials $X_0^{q^n} + \pi X_1^{q^{n-1}} + \cdots + \pi^{n-1} X_{n-1}^{q^1} + \pi^n X_n$.

Of course the twisted version is necessary if one wants to describe also all ramified discrete valuation rings with not necessarily finite residue fields. A second main reason for considering “twisted formal A -modules” is that there exist no nontrivial formal A -modules if the residue field of A is infinite.

Let me add that, in my opinion, the formal group law approach to (ramified) Witt-vectors is technically and conceptually easier. Witness, e.g. the proof of Theorem 6.6 and the ease with which one defines Artin-Hasse exponentials in this setting (cf. §§6.1 and 6.5 below). Also this approach removes some of the mystery and exclusive status of the particular Witt polynomials $X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n$ (unramified case), $X_0^{q^n} + \pi X_1^{q^{n-1}} + \cdots + \pi^n X_n$ (untwisted ramified case),

$X_0^{q^n} + \sigma^{n-1}(\omega)X_1^{q^{n-1}} + \sigma^{n-1}(\omega)\sigma^{n-2}(\omega)X_2^{q^{n-2}} + \cdots + \sigma^{n-1}(\omega) \cdots \sigma(\omega)\omega X_n$
(twisted ramified case). From the theoretical (if not the esthetic and/or computational) point of view all polynomials $\tilde{w}_{q,n}(X_0, \dots, X_n) = a_n^{-1}(a_n X_0^{q^n} + a_{n-1} X_1^{q^{n-1}} + \cdots + a_0 X_n) \in A[X]$ are equally good, provided $a_0 = 1, a_2, a_3, \dots$ is a sequence of elements of K such that $a_i - \omega^{-1}\sigma(a_{i-1}) \in A$ for all $i = 1, 2, \dots$ (cf. in this connection also [6]).

2. The functional-equation-integrality lemma.

2.1. *The setting.* Let A be a discrete valuation ring with maximal ideal $\mathfrak{m}$, residue field k of characteristic $p > 0$ and field of quotients K . Both characteristic zero and characteristic $p > 0$ are allowed for K . We use v to denote the normalized exponential valuation on K and ω always denotes a uniformizing element, i.e. $v(\omega) = 1$ and $\mathfrak{m} = \omega A$. We assume that there exist a power q of p and an automorphism σ of K such that

$$\sigma(\mathfrak{m}) = \mathfrak{m}, \quad \sigma a \equiv a^q \pmod{\mathfrak{m}} \quad \text{for all } a \in A. \quad (2.2)$$

The ring A does not need to be complete.

Further let $B \in \mathbf{Alg}_A$, the category of A -algebras. We suppose that B is A -torsion free (i.e. that the natural map $B \rightarrow B \otimes_A K$ is injective) and we suppose that there exists an endomorphism $\tau: B \otimes_A K \rightarrow B \otimes_A K$ such that

$$\tau(b) \equiv b^q \pmod{\mathfrak{m}B} \quad \text{for all } b \in B. \quad (2.3)$$

Finally let $f(X)$ be any power series over $B \otimes_A K$ of the form

$$f(X) = b_1 X + b_2 X^2 + \cdots, \quad b_i \in B, b_1 \text{ a unit of } B, \quad (2.4)$$

for which there exists a uniformizing element $\omega \in A$ such that

$$f(X) - \omega^{-1}\tau_* f(X^q) \in B[[X]] \quad (2.5)$$

where τ_* means “apply τ to the coefficients”. In terms of the coefficients b_i of $f(X)$ condition (2.5) means that

$$\begin{aligned} b_i &\in B \quad \text{if } q \text{ does not divide } i, \\ b_{qi} - \omega^{-1}\tau(b_i) &\in B \quad \text{for all } i = 1, 2, \dots \end{aligned} \quad (2.6)$$

2.7. FUNCTIONAL EQUATION LEMMA. *Let $A, B, \sigma, \tau, K, p, q, f(X), \omega$ be as in 2.1 above such that (2.2)–(2.6) hold. Then we have*

(i) $F(X, Y) = f^{-1}(f(X) + f(Y))$ has its coefficients in B and hence is a commutative one-dimensional formal group law over B . (Here $f^{-1}(X)$ is the “inverse function” power series of $f(X)$; i.e. $f^{-1}(f(X)) = X$.)

(ii) If $g(X) \in B[[X]]$, $g(0) = 0$ and $h(X) = f(g(X))$ then we have $h(X) - \omega^{-1}\tau_* h(X^q) \in B[[X]]$.

(iii) If $h(X) \in B \otimes_A K[[X]]$, $h(0) = 0$ and $h(X) - \omega^{-1}\tau_* h(X^q) \in B[[X]]$, then $f^{-1}(h(X)) \in B[[X]]$.

(iv) If $\alpha(X) \in B[[X]]$, $\beta(X) \in B \otimes_A K[[X]]$, $\alpha(0) = \beta(0) = 0$ and $r, m \in \mathbb{N} = \{1, 2, \dots\}$, then $\alpha(X) \equiv \beta(X) \pmod{(\omega^r B, \text{degree } m)} \Leftrightarrow f(\alpha(X)) \equiv f(\beta(X)) \pmod{(\omega^r B, \text{degree } m)}$.

PROOF. This lemma is a quite special case of the functional equation lemmas of [11, cf. §§2.2 and 10.2]. There are also infinite-dimensional versions. Here is a quick proof. First notice that (2.6) implies (with induction) that

$$b_j \in \omega^{-i}B \quad \text{if } j \text{ is not divisible by } q^{i+1}. \quad (2.8)$$

We now first prove a more general form of (ii). Let $g(Z) = g(Z_1, \dots, Z_m) \in B[[Z_1, \dots, Z_m]]$, $g(0) = 0$. Then by the hypotheses of 2.1 we have

$$g(Z_1, \dots, Z_m)^{q'^n} \equiv \tau_* g(Z_1^q, \dots, Z_m^q)^{q'^{n-1}} \pmod{\omega' B}. \quad (2.9)$$

Combining (2.8) and (2.9) and using (2.6) we see that $\text{mod}(B[[X]])$ we have

$$\begin{aligned} h(Z) &= f(g(Z)) = \sum_{i=1}^{\infty} b_i g(Z)^i \equiv \sum_{j=1}^{\infty} b_{q^j} g(Z)^{q^j} \equiv \omega^{-1} \sum_{j=1}^{\infty} \tau(b_j) g(Z)^{q^j} \\ &\equiv \omega^{-1} \sum_{j=1}^{\infty} \tau(b_j) \tau_* g(Z^q)^j = \omega^{-1} \tau_* f(\tau_* g(Z^q)) = \omega^{-1} \tau_* h(Z^q). \end{aligned}$$

This proves (ii). To prove (i) we write $F(X, Y) = F_1(X, Y) + F_2(X, Y) + \dots$, where $F_n(X, Y)$ is homogeneous of degree n . We now prove by induction that $F_n(X, Y) \in B[X, Y]$ for all $n = 1, 2, \dots$. The induction starts because $F_1(X, Y) = X + Y$. Now assume that $F_1(X, Y), \dots, F_m(X, Y) \in B[X, Y]$. We know that $f(F(X, Y)) \equiv b_1 F_{m+1}(X, Y) + f(g(X, Y)) \pmod{\text{degree } m+2}$, where $g(X, Y) = F_1(X, Y) + \dots + F_m(X, Y)$. Hence, using the more general form of (ii) proved just above, we find $\text{mod}(B[[X, Y]], \text{degree } m+2)$:

$$\begin{aligned} f(F(X, Y)) &\equiv b_1 F_{m+1}(X, Y) + f(g(X, Y)) \\ &\equiv b_1 F_{m+1}(X, Y) + \omega^{-1} \tau_* f(\tau_* g(X^q, Y^q)) \\ &\equiv b_1 F_{m+1}(X, Y) + \omega^{-1} \tau_* f(\tau_* F(X^q, Y^q)) \\ &= b_1 F_{m+1}(X, Y) + \omega^{-1} \tau_* f(X^q) + \omega^{-1} \tau_* f(Y^q) \\ &\equiv b_1 F_{m+1}(X, Y) + f(X) + f(Y) = b_1 F_{m+1}(X, Y) + f(F(X, Y)) \end{aligned}$$

where we have used the defining relation $f(F(X, Y)) = f(X) + f(Y)$, which implies $\tau_* f(\tau_* F(X^q, Y^q)) = \tau_* f(X^q) + \tau_* f(Y^q)$, and where we have also used the fact that $F(X, Y) \equiv g(X, Y) \pmod{\text{degree } m+1} \Rightarrow F(X^q, Y^q) \equiv g(X^q, Y^q) \pmod{\text{degree } m+2}$. It follows that $b_1 F_{m+1}(X, Y) \equiv 0 \pmod{B[[X, Y]], \text{degree } m+2}$ and hence $F_{m+1}(X, Y) \in B[X, Y]$ because b_1 is a unit.

The proof of (iii) is completely analogous to the proof of (i).

The implication $\Rightarrow$ of (iv) is easy to prove. If $\alpha(X) \equiv \beta(X) \pmod{\omega' B, \text{degree } m}$ and $\alpha(X) \in B[[X]]$ then $\alpha(X)^{q^j} \equiv \beta(X)^{q^j} \pmod{\omega'^{j+1} B, \text{degree } m}$ which, combined with (2.8), proves that $f(\alpha(X)) \equiv f(\beta(X)) \pmod{\omega' B, \text{degree } m}$. To prove the inverse implication $\Leftarrow$ of (iv) we first do the special case

$$f(\beta(X)) \equiv 0 \pmod{\omega' B, \text{degree } m} \Rightarrow \beta(X) \equiv 0 \pmod{\omega' B, \text{degree } m}.$$

Now $\beta(X) \equiv 0 \pmod{\text{degree } 1}$, hence $f(\beta(X)) = b_1 \beta(X) + b_2 \beta(X)^2 + \dots \equiv 0 \pmod{\omega' B, \text{degree } m}$, implies $\beta(X) \equiv 0 \pmod{\omega' B, \text{degree } 2}$, if $m > 2$ (if $m = 1$ there is nothing to prove), because b_1 is a unit. Now assume with induction that

$\beta(X) \equiv 0 \pmod{(\omega'B, \text{degree } n)}$ for some $n < m$. Then, because $\beta(X) \equiv 0 \pmod{(\text{degree } 1)}$ we have $\beta(X)^i \equiv 0 \pmod{(\omega'^i B, \text{degree}(n+i-1))}$ and hence $b_j \beta(X)^j \equiv 0 \pmod{(\omega'B, \text{degree } n+1)}$ if $j > 2$. Hence $f(\beta(X)) \equiv 0 \pmod{(\omega'B, \text{degree } m)}$ then gives $b_1 \beta(X) \equiv 0 \pmod{(\omega'B, \text{degree } n+1)}$, so that $\beta(X) \equiv 0 \pmod{(\omega'B, \text{degree } n+1)}$ because b_1 is a unit. This proves this special case of (iv). Now let $f(\alpha(X)) \equiv f(\beta(X)) \pmod{(\omega'B, \text{degree } m)}$. Write $\gamma(X) = f(\beta(X)) - f(\alpha(X))$ and $\delta(X) = f^{-1}(\gamma(X))$. Then $\delta(X) \equiv 0 \pmod{(\omega'B, \text{degree } m)}$ by the special case just proved, and $\beta(X) = f^{-1}(f(\alpha(X)) + f(\delta(X))) = F(\alpha(X), \delta(X)) \equiv \alpha(X) \pmod{(\omega'B, \text{degree } m)}$ because $F(X, Y)$ has integral coefficients, $F(X, 0) = 0$ and because $\alpha(X)$ is integral. This concludes the proof of the Functional Equation Lemma 2.7.

3. Twisted Lubin-Tate formal A -modules.

3.1. *Construction and definition.* Let A, K, k, p, m, σ, q be as in 2.1 above. We consider a power series $f(X) = X + c_2 X^2 + \dots \in K[[X]]$ such that there exists a uniformizing element $\omega \in m$ such that

$$f(X) - \omega^{-1} \sigma_* f(X^q) \in A[[X]]. \quad (3.2)$$

There are many such power series. The simplest are obtained as follows. Choose a uniformizing element ω of A . Define

$$g_\omega(X) = X + \omega^{-1} X^q + \omega^{-1} \sigma(\omega)^{-1} X^{q^2} + \omega^{-1} \sigma(\omega)^{-1} \sigma^2(\omega)^{-1} X^{q^3} + \dots \quad (3.3)$$

Given such a power series $f(X)$, part (i) of the Functional Equation Lemma says that

$$F(X, Y) = f^{-1}(f(X) + f(Y)) \quad (3.4)$$

has its coefficients in A , and hence is a one-dimensional formal group law over A . We shall call the formal group laws thus obtained *twisted Lubin-Tate formal A -modules over A* . The twisted Lubin-Tate formal A -module is called q -typical if the power series $f(X)$ that it is obtained from is of the form

$$f(X) = X + a_1 X^q + a_2 X^{q^2} + \dots \quad (3.5)$$

From now on all twisted Lubin-Tate formal A -modules will be assumed to be q -typical. This is hardly a restriction because of Lemma 3.6 below.

3.6. **LEMMA.** *Let $f(X) = X + c_2 X^2 + \dots \in K[[X]]$ be such that (3.2) holds. Let $\hat{f}(X) = \sum_{i=0}^{\infty} a_i X^{q^i}$ with $a_0 = 1$, $a_i = c_{q^i}$. Then $u(X) = \hat{f}^{-1}(f(X)) \in A[[X]]$ so that $F(X, Y)$ and $\hat{F}(X, Y)$ are strictly isomorphic formal group laws over A .*

PROOF. It follows from the definition of $\hat{f}(X)$, that $\hat{f}(X)$ also satisfies (3.2). The integrality of $u(X)$ now follows from part (iii) of the Functional Equation Lemma.

3.7. **REMARKS.** Let k , the residue field of K , be finite with q elements, and let $\sigma = \text{id}$. Then the twisted Lubin-Tate formal A -modules over A as defined above are precisely the Lubin-Tate formal group laws defined in [12], i.e. they are precisely the formal A -modules of A -height 1. If k is infinite there exist no nontrivial formal A -modules (cf. [11, Corollary 21.4.23]). This is a main reason for also considering *twisted* Lubin-Tate formal group laws.

3.8. REMARK. Let $f(X) \in K[[X]]$ be such that (3.2) holds for a certain uniformizing element ω . Then ω is uniquely determined by $f(X)$, because $a_i - \omega^{-1}\sigma(a_{i-1}) \in A \Rightarrow \omega \equiv a_i^{-1}\sigma(a_{i-1}) \pmod{\omega^{2i}A}$ as $v(a_i) = -i$. Using parts (ii) and (iii) of the Functional Equation Lemma we see that ω is in fact an invariant of the strict isomorphism class of $F(X, Y)$. Inversely, given ω we can construct $g_\omega(X)$ as in (3.3) and then $g_\omega^{-1}(f(X)) = u(X)$ is integral so that $F(X, Y)$ and $G_\omega(X, Y) = g_\omega^{-1}(g_\omega(X) + g_\omega(Y))$ are strictly isomorphic formal group laws. In case $\#k = q$ and $\sigma = \text{id}$, ω is in fact an invariant of the isomorphism class of $F(X, Y)$. For some more results on isomorphisms and endomorphisms of twisted Lubin-Tate formal A -modules cf. [11], especially §§8.3, 20.1, 21.8, 24.5.

4. Curves and q -typical curves. Let $F(X, Y)$ be a q -typical twisted Lubin-Tate formal A -module obtained via (3.4) from a power series $f(X) = X + a_1X^q + a_2X^{q^2} + \dots$.

4.1. Curves. Let $\mathbf{Alg}_A$ be the category of A -algebras. Let $B \in \mathbf{Alg}_A$. A *curve* in F over B is simply a power series $\gamma(t) \in B[[t]]$ such that $\gamma(0) = 0$. Two curves can be added by the formula $\gamma_1(t) +_F \gamma_2(t) = F(\gamma_1(t), \gamma_2(t))$, giving us an abelian group $C(F; B)$. Further, if $\phi: B_1 \rightarrow B_2$ is in $\mathbf{Alg}_A$, then $\gamma(t) \mapsto \phi_*\gamma(t)$ (=“apply ϕ to the coefficients”) defines a homomorphism of abelian groups $C(F; B_1) \rightarrow C(F; B_2)$. This defines an abelian-group-valued functor $C(F; -): \mathbf{Alg}_A \rightarrow \mathbf{Ab}$. There is a natural filtration on $C(F; -)$ defined by the filtration subgroups $C^n(F; B) = \{\gamma(t) \in C(F; B) \mid \gamma(t) \equiv 0 \pmod{(\text{degree } n)}\}$. The groups $C(F; B)$ are complete with respect to the topology defined by the filtration $C^n(F; B)$, $n = 1, 2, \dots$.

The functor $C(F; -)$ is representable by the A -algebra $A[S] = A[S_1, S_2, \dots]$. The isomorphism $\mathbf{Alg}_A(A[S], B) \xrightarrow{\sim} C(F; B)$ is given by

$$\phi \mapsto \sum_{i=1}^{\infty} {}^F \phi(S_i)t^i,$$

i.e. by $\phi \mapsto \phi_*\gamma_S(t)$, where $\gamma_S(t)$ is the “universal curve”

$$\gamma_S(t) = \sum_{i=1}^{\infty} {}^F S_i t^i \in C(F; A[S]).$$

Here the superscript F means that we sum in the group $C(F; B)$ just defined (to avoid possible confusion with ordinary sums).

4.2. q -typification. Let $\gamma_S(t) \in C(F; A[S])$ be the universal curve. Consider the power series

$$h(t) = f(\gamma_S(t)) = \sum_{i=1}^{\infty} x_i(S)t^i.$$

Let $\tau: K[S] \rightarrow K[S]$ be the ring endomorphism defined by $\tau(a) = \sigma(a)$ for $a \in K$ and $\tau(S_i) = S_i^q$ for $i = 1, 2, \dots$. Then the hypotheses of 2.1 are fulfilled and it follows from part (ii) of the Functional Equation Lemma that $h(t) - \omega^{-1}\tau_*h(t^q) \in A[S][[t]]$. Now let $\hat{h}(t) = \sum_{i=0}^{\infty} x_q(S)t^{q^i}$. Then, obviously, also $\hat{h}(t) - \omega^{-1}\tau_*\hat{h}(t^q) \in A[S][[t]]$ and by part (iii) of the Functional Equation Lemma it follows that

$$\varepsilon_q \gamma_S(t) = f^{-1} \left(\sum_{i=0}^{\infty} x_{q^i}(S) t^{q^i} \right) \quad (4.3)$$

is an element of $A[S][[t]]$. We now define a functorial group homomorphism $\varepsilon_q: C(F; -) \rightarrow C(F; -)$ by the formula

$$\varepsilon_q \gamma(t) = (\phi_\gamma)_* (\varepsilon_q \gamma_S(t)) \quad (4.4)$$

for $\gamma(t) \in C(F; B)$, where $\phi_\gamma: A[S] \rightarrow B$ is the unique A -algebra homomorphism such that $(\phi_\gamma)_* \gamma_S(t) = \gamma(t)$.

4.5. LEMMA. *Let B be A -torsion free so that $B \rightarrow B \otimes_A K$ is injective. Then we have for all $\gamma(t) \in C(F; B)$,*

$$f(\gamma(t)) = \sum_{i=1}^{\infty} b_i t^i \Rightarrow f(\varepsilon_q \gamma(t)) = \sum_{j=0}^{\infty} b_{q^j} t^{q^j} \quad (4.6)$$

and $\varepsilon_q C(F; B) = \{ \gamma(t) \in C(F; B) \mid f(\gamma(t)) = \sum c_j t^{q^j} \text{ for certain } c_j \in B \otimes_A K \}$.

PROOF. Immediate from (4.3) and (4.4).

4.7. LEMMA. ε_q is a functorial, idempotent, group endomorphism of $C(F; -)$.

PROOF. ε_q is functorial by definition. The facts that $\varepsilon_q \varepsilon_q = \varepsilon_q$ and that ε_q is a group homomorphism are obvious from Lemma 4.5 in case B is A -torsion free. Functoriality then implies that these properties hold for all A -algebras B .

4.8. The functor $C_q(F; -)$ of q -typical curves. We now define the abelian-group-valued functor $C_q(F; -)$ as

$$C_q(F; -) = \varepsilon_q C(F; -). \quad (4.9)$$

For each $n \in \mathbb{N} \cup \{0\}$ let $C_q^{(n)}(F; B)$ be the subgroup $C_q(F; B) \cap C^{q^n}(F; B)$. These groups define a filtration on $C_q(F; B)$, and $C_q(F; B)$ is complete with respect to the topology defined by this filtration.

The functor $C_q(F; -)$ is representable by the A -algebra $A[T] = A[T_0, T_1, \dots]$.

Indeed, writing $f(X) = \sum_{i=0}^{\infty} a_i X^{q^i}$ we have

$$f(\gamma_S(t)) = f \left(\sum_{i=1}^{\infty} S_i t^i \right) = \sum_{j=0}^{\infty} \sum_{i=1}^{\infty} a_j S_i^{q^j} t^{q^j i}$$

and it follows that

$$\varepsilon_q \gamma_S(t) = \sum_{j=0}^{\infty} S_{q^j} t^{q^j}.$$

From this one easily obtains that the functor $C_q(F; -)$ is representable by $A[T]$. The isomorphism $\text{Alg}_A(A[T], B) \xrightarrow{\sim} C_q(F; B)$ is given by

$$\phi \mapsto \sum_{i=0}^{\infty} \phi(T_i) t^{q^i} = \phi_*(\gamma_T(t)),$$

where $\gamma_T(t)$ is the universal q -typical curve

$$\gamma_T(t) = \sum_{i=0}^{\infty} T_i t^{q^i} \in C_q(F; A[T]). \quad (4.10)$$

4.11. REMARKS. The explicit formulas of 4.8 above depend on the fact that F was supposed to be q -typical. In general slightly more complicated formulae hold. For arbitrary formal groups q -typification (i.e. ε_q) is not defined (unless $q = p$). But a similar notion of q -typification exists for formal A -modules of any height and any dimension if $\#k = q$.

5. The A -algebra structure on $C_q(F; -)$, Frobenius and Verschiebung.

5.1. From now on we assume that $f(X) = g_\omega(X) = X + \omega^{-1}X^q + \omega^{-1}\sigma(\omega)^{-1}X^{q^2} + \dots$ for a certain uniformizing element ω . Otherwise we keep the notations and assumptions of §4. Thus we now have $a_i^{-1} = \omega\sigma(\omega) \dots \sigma^{i-1}(\omega)$, $a_0 = 1$. This restriction to “logarithms” $f(X)$ of the form $g_\omega(X)$ is not very serious, because every twisted Lubin-Tate formal A -module over A is strictly isomorphic to a $G_\omega(X, Y)$, (cf. Remark 3.8), and one can use the strict isomorphism $g_\omega^{-1}(f(X))$ to transport all the extra structure on $C_q(F; -)$ which we shall define in this section. The restriction $f(X) = g_\omega(X)$ does have the advantage of simplifying the defining formulas (5.4), (5.5), (5.8), ... somewhat, and it makes them look rather more natural especially in view of the fact that ω , the only “constant” which appears, is an invariant of strict isomorphism classes of twisted Lubin-Tate formal A -modules (cf. Remark 3.8 above).

In this section we shall define an A -algebra structure on the functor $C_q(F; -)$ and two endomorphisms $\mathbf{f}_\omega$ and $\mathbf{V}_q$. These constructions all follow the same pattern, the same pattern as was used to define and analyse ε_q in §4 above. First one defines the desired operations for universal curves like $\gamma_T(t)$ which are defined over rings like $A[T]$, which, and this is the crucial point, admit an endomorphism $\tau: K[T] \rightarrow K[T]$, viz. $\tau(a) = \sigma(a)$, $\tau(T_i) = T_i^q$, which extends σ and which is such that $\tau(x) \equiv x^q \pmod{\omega A[T]}$. In such a setting the Functional Equation Lemma assures us that our constructions do not take us out of $C(F; -)$ or $C_q(F; -)$. Second, the definitions are extended via representability and functoriality, and thirdly, one derives a characterization which holds over A -torsion free rings, and using this, one proves the various desired properties like associativity of products, σ -semilinearity of $\mathbf{f}_\omega$, etc.

5.2. *Constructions.* Let $\gamma_T(t)$ be the universal q -typical curve (4.10). We write

$$f(\gamma_T(t)) = \sum_{i=0}^{\infty} x_i(T) t^{q^i}. \quad (5.3)$$

Let $f(X) = g_\omega(X) = \sum_{i=0}^{\infty} a_i X^{q^i}$, i.e. $a_i = \omega^{-1}\sigma(\omega)^{-1} \dots \sigma^{i-1}(\omega)^{-1}$ and let $a \in A$.

We define

$$\{a\}_{F\gamma_T(t)} = f^{-1}\left(\sum_{i=0}^{\infty} \sigma^i(a) x_i(T) t^{q^i}\right), \quad (5.4)$$

$$\mathbf{f}_\omega \gamma_T(t) = f^{-1}\left(\sum_{i=0}^{\infty} \sigma^i(\omega) x_{i+1}(T) t^{q^i}\right). \quad (5.5)$$

The Functional Equation Lemma now assures us that (5.4) and (5.5) define elements of $C(F; A[T])$, which then are in $C_q(F; A[T])$ by Lemma 4.5. To illustrate

this we check the hypotheses necessary to apply (iii) of 2.7 in the case of $\mathbf{f}_\omega$. Let $\tau: K[T] \rightarrow K[T]$ be as in 5.1 above. Then by part (ii) of the Functional Equation Lemma we know that

$$x_0 \in A[T], \quad x_{i+1} - \omega^{-1}\tau(x_i) = c_i \in A[T].$$

It follows by induction that

$$x_i \in \omega^{-i}A[T] \quad (5.6)$$

and we also know that

$$v(a_i^{-1}) = v(\omega\sigma(\omega) \dots \sigma^{i-1}(\omega)) = i \quad (5.7)$$

where v is the normalized exponential valuation on K . We thus have $\sigma^0(\omega)x_1 = \omega x_1 \in A[T]$ and

$$\begin{aligned} \sigma^i(\omega)x_{i+1} - \omega^{-1}\tau(\sigma^{i-1}(\omega)x_i) &= \sigma^i(\omega)c_i + \sigma^i(\omega)\omega^{-1}\tau(x_i) - \omega^{-1}\tau(\sigma^{i-1}(\omega)x_i) \\ &= \sigma^i(\omega)c_i \in A[T]. \end{aligned}$$

Hence part (iii) of the Functional Equation Lemma says that $\mathbf{f}_\omega\gamma_T(t) \in C(F; A[T])$.

To define the multiplication on $C_q(F; -)$ we need two independent universal q -typical curves. Let $\gamma_T(t) = \sum^F T_i t^{q^i}$, $\delta_{\hat{T}}(t) = \sum^F \hat{T}_i t^{q^i} \in C_q(F; A[T; \hat{T}])$. We define

$$\gamma_T(t) * \delta_{\hat{T}}(t) = f^{-1} \left(\sum_{i=0}^{\infty} a_i^{-1} x_i y_i t^{q^i} \right) \quad (5.8)$$

where $f(\gamma_T(t)) = \sum x_i t^{q^i}$, $f(\delta_{\hat{T}}(t)) = \sum y_i t^{q^i}$. To prove that (5.8) defines something integral we proceed as usual. We have $x_0, y_0 \in A[T; \hat{T}]$, $x_{i+1} - \omega^{-1}\tau(x_i) = c_i \in A[T; \hat{T}]$, $y_{i+1} - \omega^{-1}\tau(y_i) = d_i \in A[T; \hat{T}]$, where $\tau: K[T; \hat{T}] \rightarrow K[T; \hat{T}]$ is defined by $\tau(a) = \sigma(a)$ for $a \in K$, and $\tau(T_i) = T_i^q$, $\tau(\hat{T}_i) = \hat{T}_i^q$, $i = 0, 1, 2, \dots$. Then $a_0 x_0 y_0 = x_0 y_0 \in A[T; \hat{T}]$ and

$$\begin{aligned} a_{i+1}^{-1} x_{i+1} y_{i+1} - \omega^{-1}\tau(a_i^{-1} x_i y_i) \\ &= \omega\sigma(a_i)^{-1} (c_i + \omega^{-1}\tau(x_i)) (d_i + \omega^{-1}\tau(y_i)) - \omega^{-1}\sigma(a_i^{-1})\tau(x_i)\tau(y_i) \\ &= \omega\sigma(a_i^{-1})c_i d_i + \sigma(a_i)^{-1} (c_i \tau(y_i) + d_i \tau(x_i)) \in A[T; \hat{T}] \end{aligned}$$

by (5.6) and (5.7).

5.9. DEFINITION. Let $\gamma(t), \delta(t)$ be two q -typical curves in F over $B \in \mathbf{Alg}_A$. Let $\phi: A[T] \rightarrow B$ be the unique A -algebra homomorphism such that $\phi_*\gamma_T(t) = \gamma(t)$, and let $\psi: A[T; \hat{T}] \rightarrow B$ be the unique A -algebra homomorphism such that $\psi_*\gamma_T(t) = \gamma(t)$, $\psi_*\delta_{\hat{T}}(t) = \delta(t)$. Let $a \in A$. We define

$$\{a\}_F \gamma(t) = \phi_* (\{a\}_F \gamma_T(t)), \quad (5.10)$$

$$\mathbf{f}_\omega \gamma(t) = \phi_* (\mathbf{f}_\omega \gamma_T(t)), \quad (5.11)$$

$$\gamma(t) * \delta(t) = \psi_* (\gamma_T(t) * \delta_{\hat{T}}(t)). \quad (5.12)$$

5.13. Characterizations. Let B be an A -torsion free A -algebra; i.e. $B \rightarrow B \otimes_A K$ is injective, then the definitions (5.10)–(5.12) are characterized by the implications

$$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \Rightarrow f(\{a\}_F \gamma(t)) = \sum_{i=0}^{\infty} \sigma^i(a) x_i t^{q^i}, \quad (5.14)$$

$$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \Rightarrow f(\mathbf{f}_{\omega} \gamma(t)) = \sum_{i=0}^{\infty} \sigma^i(\omega) x_{i+1} t^{q^i}, \quad (5.15)$$

$$\begin{aligned} f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i}, \quad f(\delta(t)) = \sum_{i=0}^{\infty} y_i t^{q^i} \Rightarrow \\ f(\gamma(t) * \delta(t)) = \sum_{i=0}^{\infty} a_i^{-1} x_i y_i t^{q^i}. \end{aligned} \quad (5.16)$$

This follows immediately from (5.4), (5.5) (5.8) compared with (5.10)–(5.12), because ϕ_* and ψ_* are defined by applying ϕ and ψ to coefficients, and because $\gamma(t) \mapsto f(\gamma(t))$ is injective, if B is A -torsion free.

5.17. THEOREM. *The operators $\{a\}_F$ defined by (5.10) define a functorial A -module structure on $C_q(F; -)$. The multiplication $*$ defined by (5.12) then makes $C_q(F; -)$ an A -algebra-valued functor, with as unit element the q -typical curve $\gamma_0(t) = t$. The operator $\mathbf{f}_{\omega}$ is a σ -semilinear A -algebra homomorphism, i.e. $\mathbf{f}_{\omega}$ is a unit and multiplication-preserving group endomorphism such that $\mathbf{f}_{\omega}\{a\}_F = \{\sigma(a)\}_F \mathbf{f}_{\omega}$.*

PROOF. In case B is A -torsion free the various identities in $C_q(F; B)$ like $(\{a\}_F \gamma(t)) * \delta(t) = \{a\}_F(\gamma(t) * \delta(t))$, $\gamma(t) * (\delta(t) +_F \varepsilon(t)) = (\gamma(t) * \delta(t)) +_F (\gamma(t) * \varepsilon(t))$, ... are obvious from the characterizations (5.14)–(5.16). The theorem then follows by functoriality.

5.18. Verschiebung. We now define the Verschiebung operator V_q on $C_q(F; -)$ by the formula $V_q \gamma(t) = \gamma(t^q)$. (It is obvious from Lemma 4.5 that this takes q -typical curves into q -typical curves.) In terms of the logarithm $f(X)$ one has for curves $\gamma(t)$ over A -torsion free A -algebras B ,

$$f(\gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^i} \Rightarrow f(V_q \gamma(t)) = \sum_{i=0}^{\infty} x_i t^{q^{i+1}}. \quad (5.19)$$

5.20. THEOREM. *For q -typical curves $\gamma(t)$ in F over an A -algebra B ,*

$$\mathbf{f}_{\omega} V_q \gamma(t) = \{\omega\}_F \gamma(t), \quad (5.21)$$

$$\mathbf{f}_{\omega} \gamma(t) \equiv \gamma(t)^{*q} \pmod{\{\omega\}_F C_q(F; B)}. \quad (5.22)$$

PROOF. (5.21) is immediate from (5.14), (5.15) and (5.19) in the case of A -torsion free B and then follows in general by functoriality. The proof of (5.22) is a bit longer. It suffices to prove (5.22) for curves $\gamma(t) \in C_q(F; A[T])$. In fact it suffices to prove (5.22) for $\gamma(t) = \gamma_T(t)$, the universal curve of (4.10). Let

$$\delta(t) = f^{-1} \left(\sum_{i=0}^{\infty} y_i t^{q^i} \right), \quad y_i = x_{i+1} - \sigma^i(\omega)^{-1} a_i a_i^{-q} x_i^q, \quad (5.23)$$

where the x_i , $i = 0, 1, 2, \dots$, are determined by $f(\gamma(t)) = \sum x_i t^{q^i}$. It then follows from (5.14)–(5.16) that indeed $\mathbf{f}_{\omega} \gamma(t) - \gamma(t)^{*q} = \{\omega\}_F \delta(t)$, provided that we can show that $\delta(t)$ is integral, i.e. that $\delta(t) \in C_q(F; A[T])$. To see this it suffices to show

that $y_0 \in A[T]$ and $y_{i+1} - \omega^{-1}\tau(y_i) \in A[T]$ because of part (iii) of the Functional Equation Lemma. Let $c_i = x_{i+1} - \omega^{-1}\tau(x_i) \in A[T]$. Then

$$y_0 = x_1 - \sigma^0(\omega)^{-1}x_0^q = c_0 + \omega^{-1}\tau(x_0) - \omega^{-1}x_0^q \in A[T]$$

because $\tau(x_0) \equiv x_0^q \pmod{\omega A[T]}$. Further from $x_{i+1} = c_i + \omega^{-1}\tau(x_i)$ we find

$$a_{i+1}^{-1}x_{i+1} = \omega\sigma(\omega) \dots \sigma^i(\omega)c_i + \sigma(\omega) \dots \sigma^i(\omega)\tau(x_i) = \omega^{i+1}d_i + \tau(a_i^{-1}x_i)$$

for a certain $d_i \in A[T]$, and hence

$$a_{i+1}^{-q}x_{i+1}^q = \tau(a_i^{-q}x_i^q) + \omega^{i+2}e_i \quad (5.24)$$

for a certain $e_i \in A[T]$. It follows that

$$\begin{aligned} y_{i+1} - \omega^{-1}\tau(y_i) &= x_{i+2} - \sigma^{i+1}(\omega)^{-1}a_{i+1}a_{i+1}^{-q}x_{i+1}^q - \omega^{-1}\tau(x_{i+1}) \\ &\quad + \omega^{-1}\tau(\sigma^i(\omega)^{-1}a_i a_i^{-q}x_i^q) \\ &= c_{i+1} - \sigma^{i+1}(\omega)^{-1}(a_{i+1}a_{i+1}^{-q}x_{i+1}^q - \omega^{-1}\sigma(a_i)\tau(a_i^{-q}x_i^q)) \\ &= c_{i+1} - \sigma^{i+1}(\omega)^{-1}a_{i+1}(a_{i+1}^{-q}x_{i+1}^q - \tau(a_i^{-q}x_i^q)) \in A[T] \end{aligned}$$

because $a_{i+1} = \omega^{-1}\sigma(a_i)$ and because of (5.24). (Recall that $v(a_{i+1}) = -i - 1$ by (5.7).) This concludes the proof of Theorem 5.20.

6. Ramified Witt vectors and ramified Artin-Hasse exponentials. We keep the assumptions and notations of §5.

6.1. A preliminary Artin-Hasse exponential. Let B be an A -algebra which is A -torsion free and which admits an endomorphism $\tau: B \otimes_A K \rightarrow B \otimes_A K$ which restricts to σ on $A \otimes_A K = K \subset B \otimes_A K$ and which is such that $\tau(b) \equiv b^q \pmod{\omega B}$. We define a map $\Delta_B: B \rightarrow C_q(F; B)$ as follows.

$$\Delta_B(b) = f^{-1} \left(\sum_{i=0}^{\infty} \tau^i(b) a_i t^q \right). \quad (6.2)$$

This is well defined by part (iii) of the Functional Equation Lemma. A quick check by means of (5.14)–(5.16) shows that Δ_B is a homomorphism of A -algebras such that, moreover,

$$\Delta_B \circ \tau = f_{\omega} \circ \Delta_B \quad (6.3)$$

(because $\sigma^i(\omega)a_{i+1} = a_i$), and that Δ_B is functorial in the sense that if (B', τ') is a second such A -algebra with endomorphism τ' of $B' \otimes_A K$ and $\phi: B \rightarrow B'$ is an A -algebra homomorphism such that $\tau'\phi = \phi\tau$, then $C_q(F; \phi) \circ \Delta_B = \Delta_{B'} \circ \phi$.

6.4. REMARK. Using (B, τ) instead of (A, σ) we can view $F(X, Y)$ as a twisted Lubin-Tate formal B -module over B , if we are willing to extend the definition a bit, because, of course, B need not be a discrete valuation ring, nor is $B \otimes_A K$ necessarily the quotient field of B . In fact B need not even be an integral domain. If we view $F(X, Y)$ in this way then $\Delta_B: B \rightarrow C_q(F; B)$ is just the B -algebra structure map of $C_q(F; B)$.

6.5. Now let B be any A -algebra. Then $C_q(F; B)$ is an A -algebra which admits an endomorphism τ , viz. $\tau = f_{\omega}$, which, as $\tau x \equiv x^q \pmod{\omega}$ by (5.22), satisfies the hypotheses of 6.1 above (because f_{ω} is σ -semilinear). It is also immediate from

(5.10) and (5.4), cf. also (5.14), that $C_q(F; B)$ is always A -torsion free. Substituting $C_q(F; B)$ for B in 6.1 we therefore find A -algebra homomorphisms $E_B: C_q(F; B) \rightarrow C_q(F; C_q(F; B))$ which are functorial in B because $\mathbf{f}_\omega$ is functorial, and because of the functoriality property of the Δ_B mentioned in 6.1 above. This functorial A -algebra homomorphism is in fact the ramified Artin-Hasse exponential we are seeking and, as is shown by the next theorem, $C_q(F; B)$ is the desired ramified-Witt-vector functor.

6.6. THEOREM. *Let A be complete with perfect residue field k . Let B be the ring of integers in a finite unramified extension L of K . Let l be the residue field of B . Consider the composed map*

$$\mu_B: B \xrightarrow{\Delta_B} C_q(F; B) \rightarrow C_q(F; l).$$

Then μ_B is an isomorphism of A -algebras. Moreover if $\tau: B \rightarrow B$ is the unique extension of $\sigma: A \rightarrow A$ such that $\tau(b) \equiv b^q \pmod{B}$, then $\mathbf{f}_\omega \mu_B = \mu_B \tau$, i.e. τ and $\mathbf{f}_\omega$ correspond under μ_B .

PROOF. Let $b \in B$. Consider $\Delta_B(\omega' b)$. Then from (6.2) we see that

$$f(\Delta_B(\omega' b)) \equiv a_r \tau'(\omega') \tau'(b) t^{q'} \pmod{(\omega B, \text{degree } q^{r+1})}.$$

By part (iv) of the Functional Equation Lemma 2.7 it follows that

$$\Delta_B(\omega' b) \equiv y_r \tau'(b) t^{q'} \pmod{(\omega B, \text{degree } q^{r+1})}$$

where $y_r = a_r \tau'(\omega')$ is a unit of B . It follows that μ_B maps the filtration subgroups $\omega' B$ of B into the filtration subgroups $C_q^{(r)}(F; l)$ and that the induced maps

$$l \xrightarrow{\sim} \omega' B / \omega^{r+1} B \xrightarrow{\mu_B} C_q^{(r)}(F; l) / C_q^{(r+1)}(F; l) \xrightarrow{\sim} l$$

are given by $x \mapsto y_r x^{q'}$ for $x \in l$. (Here $l \xrightarrow{\sim} \omega' B / \omega^{r+1} B$ is induced by $\omega' b \mapsto \bar{b}$ with $\bar{b}$ the image of b in l under the canonical projection $B \rightarrow l$, and $C_q^{(r)}(F; l) / C_q^{(r+1)}(F; l) \xrightarrow{\sim} l$ is induced by $C_q^{(r)}(F; l) \rightarrow l$, $\gamma(t) \mapsto (\text{coefficient of } t^{q'} \text{ in } \gamma(t))$.) Because l is perfect and $\bar{y}_r \neq 0$, it follows that the induced maps $\bar{\mu}_B$ are all isomorphisms. Hence μ_B is an isomorphism because B and $C_q(F; l)$ are both complete in their filtration topologies. The map μ_B is an A -algebra homomorphism because Δ_B is an A -algebra homomorphism and $C_q(F; -)$ is an A -algebra-valued functor. Finally the last statement of Theorem 6.6 follows because both τ and $\mu_B^{-1} \mathbf{f}_\omega \mu_B$ extend σ and $\tau(b) \equiv b^q \equiv \mu_B^{-1} \mathbf{f}_\omega \mu_B(b) \pmod{\omega B}$.

6.7. The maps $s_{q,n}$ and $w_{q,n}^F$. The last thing to do is to reformulate the definitions of $C_q(F; B)$ and E_B in such a way that they more closely resemble the corresponding objects in the unramified case, i.e. in the case of the ordinary Witt vectors. This is easily done, essentially because $C_q(F; -)$ is representable.

Indeed, let, as a set-valued functor, $W_{q,\infty}^F: \mathbf{Alg}_A \rightarrow \mathbf{Set}$ be defined by

$$\begin{aligned} W_{q,\infty}^F(B) &= \{(b_0, b_1, b_2, \dots) | b_i \in B\}, \\ W_{q,\infty}^F(\phi)(b_0, b_1, \dots) &= (\phi(b_0), \phi(b_1), \dots). \end{aligned} \tag{6.8}$$

We now identify the set-valued functors $W_{q,\infty}^F(-)$ and $C_q(F; -)$ by the functorial isomorphism

$$e_B(b_0, b_1, \dots) = \sum_{i=0}^{\infty} {}^F b_i t^{q^i}, \quad (6.9)$$

and define $W_{q,\infty}^F(-)$ as an A -algebra-valued functor by transporting the A -algebra structure on $C_q(F; B)$ via e_B for all $B \in \mathbf{Alg}_B$. We use $\mathbf{f}$ and $\mathbf{V}$ to denote the endomorphisms of $W_{q,\infty}^F(-)$ obtained by transporting $\mathbf{f}_\omega$ and $\mathbf{V}_q$ via e_B . Then one has immediately that

$$\mathbf{V}(b_0, b_1, \dots) = (0, b_0, b_1, \dots) \quad (6.10)$$

and in fact

$$\mathbf{f}(b_0, b_1, \dots) = (\hat{b}_0, \hat{b}_1, \dots) \Rightarrow \hat{b}_i \equiv b_i^q \pmod{\omega B}. \quad (6.11)$$

(We have not proved the analog of this for $\mathbf{f}_\omega$; this is not difficult to do by using part (iv) of the Functional Equation Lemma and the additivity of $\mathbf{f}_\omega$.)

Next we discuss the analog of the Witt polynomials $X_0^p + pX_1^{p^{n-1}} + \dots + p^n X_n$. We define for the universal curve $\gamma_T(t) \in C_q(F; A[T])$,

$$s_{q,n}(\gamma_T(t)) = a_n^{-1}(\text{coefficient of } t^{q^n} \text{ in } f(\gamma_T(t))) \quad (6.12)$$

and, as usual, this is extended functorially for arbitrary curves $\gamma(t)$ over arbitrary A -algebras by

$$s_{q,n}\gamma(t) = \phi(s_{q,n}(\gamma_T(t))) \quad (6.13)$$

where $\phi: A[T] \rightarrow B$ is the unique A -algebra homomorphism such that $\phi_* \gamma_T(t) = \gamma(t)$. If B is A -torsion free one has, of course, the result that $s_{q,n}\gamma(t) = a_n^{-1}$ (coefficient of t^{q^n} in $f(\gamma(t))$). Using this one checks that

$$\begin{aligned} s_{q,n}(\gamma(t) + {}_F \delta(t)) &= s_{q,n}(\gamma(t)) + s_{q,n}(\delta(t)), \\ s_{q,n}(\gamma(t) * \delta(t)) &= s_{q,n}(\gamma(t))s_{q,n}(\delta(t)), \\ s_{q,n}(\{a\}_F \gamma(t)) &= \sigma^n(a)s_{q,n}(\gamma(t)), \\ s_{q,n}(\mathbf{f}_\omega \gamma(t)) &= s_{q,n+1}(\gamma(t)), \\ s_{q,n}(\mathbf{V}_q \gamma(t)) &= \sigma^{n-1}(\omega)s_{q,n-1}(\gamma(t)) \quad \text{if } n > 1, \\ s_{q,0}(\mathbf{V}_q \gamma(t)) &= 0, \\ s_{q,n}(t) &= 1 \quad \text{for all } n. \end{aligned} \quad (6.14)$$

Now suppose that we are in the situation of 6.1 above. Then, by the definition of Δ_B , we have

$$s_{q,n}(\Delta_B(b)) = \tau^n(b). \quad (6.15)$$

Now define $w_{q,n}^F(B): W_{q,\infty}^F(B) \rightarrow B$ by $w_{q,n}^F = s_{q,n} \circ e_B$. It is not difficult to calculate $w_{q,n}^F$. Indeed

$$f(\gamma_T(t)) = f\left(\sum_{i=0}^{\infty} {}^F T_i t^{q^i}\right) = \sum_{j=0}^{\infty} \sum_{i=0}^{\infty} a_j T_i^j t^{q^{i+j}} = \sum_{r=0}^{\infty} \left(\sum_{i=0}^r a_i T_{r-i}^{q^i}\right) t^{q^r}$$

and it follows that $w_{q,n}^F$ is the functorial map $W_{q,\infty}^F(B) \rightarrow B$ defined by the polynomials

$$\begin{aligned} w_{q,n}^F(Z_0, \dots, Z_n) &= a_n^{-1} \left(\sum_{i=0}^n a_i Z_{n-i}^{q^i} \right) \\ &= Z_0^{q^n} + \sigma^{n-1}(\omega) Z_1^{q^{n-1}} + \sigma^{n-1}(\omega) \sigma^{n-2}(\omega) Z_2^{q^{n-2}} + \dots \\ &\quad + \sigma^{n-1}(\omega) \dots \sigma(\omega) \omega Z_n. \end{aligned} \quad (6.16)$$

6.17. THEOREM. Let (A, σ) be a pair consisting of a discrete valuation ring A of residue characteristic $p > 0$ and a Frobenius-like automorphism $\sigma: K \rightarrow K$ such that (2.2) holds for some power q of p . Let ω be any uniformizing element of A , and let $w_{q,n}^F(Z)$, $n = 0, 1, \dots$, be the polynomials defined by (6.16). Then there exists a unique A -algebra-valued functor $W_{q,\infty}^F: \mathbf{Alg}_A \rightarrow \mathbf{Alg}_A$ such that

- (i) as a set-valued functor $W_{q,\infty}^F(B) = \{(b_0, b_1, b_2, \dots) | b_i \in B\}$ and $W_{q,\infty}^F(\phi)(b_0, b_1, \dots) = (\phi(b_0), \phi(b_1), \dots)$ for all $\phi: B \rightarrow B'$ in $\mathbf{Alg}_A$,
- (ii) the polynomials $w_{q,n}^F(Z)$ induce functorial σ^n -semilinear A -algebra homomorphisms $w_{q,\infty}^F: W_{q,\infty}^F(B) \rightarrow B$, $(b_0, b_1, \dots) \mapsto w_{q,n}^F(b_0, \dots, b_n)$.

Moreover, the functor $W_{q,\infty}^F(-)$ has a σ^{-1} -semilinear A -module functor endomorphism V and a functorial σ -semilinear A -algebra endomorphism f which satisfy and are characterized by

- (iii) $w_{q,n}^F \circ V = \sigma^{n-1}(\omega) w_{q,n-1}^F$ if $n = 1, 2, \dots$; $w_{q,0}^F \circ V = 0$,
- (iv) $w_{q,n}^F \circ f = w_{q,n+1}^F$.

These endomorphisms f and V have (among others) the properties

- (v) $fV = \omega$,
- (vi) $f\mathbf{b} \equiv b^q \pmod{\omega W_{q,\infty}^F(B)}$ for all $\mathbf{b} \in W_{q,\infty}^F(B)$, $B \in \mathbf{Alg}_A$,
- (vii) $V(\mathbf{b}(f\mathbf{c})) = (V\mathbf{b})\mathbf{c}$ for all $\mathbf{b}, \mathbf{c} \in W_{q,\infty}^F(B)$, $B \in \mathbf{Alg}_A$.

Further there exists a unique functorial A -algebra homomorphism

$$E: W_{q,\infty}^F(-) \rightarrow W_{q,\infty}^F(W_{q,\infty}^F(-))$$

which satisfies and is characterized by

- (viii) $w_{q,n}^F \circ E = f^n$ for all $n = 0, 1, 2, \dots$. (Here $w_{q,n}^F: W_{q,\infty}^F(W_{q,\infty}^F(B)) \rightarrow W_{q,\infty}^F(B)$ is short for $w_{q,n,w_{q,\infty}^F(B)}^F$, i.e. it is the map which assigns to a sequence $(\mathbf{b}_0, \mathbf{b}_1, \dots)$ of elements of $W_{q,\infty}^F(B)$ the element $w_{q,n}^F(\mathbf{b}_0, \mathbf{b}_1, \dots) \in W_{q,\infty}^F(B)$.) The functor homomorphism E further satisfies

- (ix) $W_{q,\infty}^F(w_{q,n}^F) \circ E = f^n$, where $W_{q,\infty}^F(w_{q,n}^F): W_{q,\infty}^F(W_{q,\infty}^F(B)) \rightarrow W_{q,\infty}^F(B)$ assigns to a sequence $(\mathbf{b}_0, \mathbf{b}_1, \dots)$ of elements of $W_{q,\infty}^F(B)$ the sequence $(w_{q,n}^F(\mathbf{b}_0), w_{q,n}^F(\mathbf{b}_1), \dots) \in W_{q,\infty}^F(B)$.

Finally if A is complete with perfect residue field k and l/k is a finite separable extension, then $W_{q,\infty}^F(l)$ is the ring of integers B of the unique unramified extension L/K covering the residue field extension l/k and under this A -algebra isomorphism f corresponds to the unique extension of σ to $\tau: B \rightarrow B$ which satisfies $\tau(b) \equiv b^q \pmod{\omega B}$. In particular $W_{q,\infty}^F(k) \simeq A$ with f corresponding to σ .

PROOF. Existence of $W_{q,\infty}^F(-)$, V , f , E such that (i), (ii), (iii), (iv), (viii) hold follows from the constructions above. Uniqueness follows because (i), (ii), (iii), (iv),

(viii) determine the A -algebra structure on $B^{N \cup \{0\}}$, $\mathbf{V}$, $\mathbf{f}$, E uniquely for A -torsion free A -algebras B , and then these structure elements are uniquely determined by (i)–(iv), (viii) for all A -algebras, by the functoriality requirement (because for every A -algebra B there exists an A -torsion free A -algebra B' together with a surjective A -algebra homomorphism $B' \rightarrow B$). Of the remaining identities some have already been proved in the $C_q(F; -)$ -setting ((v) and (vi)). They can all be proved by checking that they give the right answers whenever composed with the $w_{q,n}^F$. This proves that they hold over A -torsion free algebras B , and then they hold in general by functoriality. So to prove (vii) we calculate

$$\begin{aligned} w_{q,0}^F(\mathbf{V}(\mathbf{b}(\mathbf{f}\mathbf{c}))) &= 0, \\ w_{q,n}^F(\mathbf{V}(\mathbf{b}(\mathbf{f}\mathbf{c}))) &= \sigma^{n-1}(\omega)w_{q,n-1}^F(\mathbf{b}(\mathbf{f}\mathbf{c})) = \sigma^{n-1}(\omega)w_{q,n-1}^F(\mathbf{b})w_{q,n-1}^F(\mathbf{f}\mathbf{c}) \\ &= \sigma^{n-1}(\omega)w_{q,n-1}^F(\mathbf{b})w_{q,n}^F(\mathbf{c}) \end{aligned}$$

and, on the other hand,

$$\begin{aligned} w_{q,0}^F((\mathbf{V}\mathbf{b})\mathbf{c}) &= w_{q,0}^F(\mathbf{V}\mathbf{b})w_{q,0}^F(\mathbf{c}) = 0, \quad w_{q,0}^F(\mathbf{c}) = 0, \\ w_{q,n}^F((\mathbf{V}\mathbf{b})\mathbf{c}) &= w_{q,n}^F(\mathbf{V}\mathbf{b})w_{q,n}^F(\mathbf{c}) = \sigma^{n-1}(\omega)w_{q,n-1}^F(\mathbf{b})w_{q,n}^F(\mathbf{c}). \end{aligned}$$

This proves (vii). To prove (ix) we proceed similarly.

$$w_{q,m}^F \circ W_{q,\infty}^F(w_{q,n}^F) \circ E = w_{q,n}^F \circ w_{q,m}^F \circ E = w_{q,n}^F \circ \mathbf{f}^m = w_{q,n+m}^F = w_{q,m}^F \circ \mathbf{f}^n.$$

(Here the first equality follows from the functoriality of the morphisms $w_{q,m}^F$ which says that for all $\phi: B' \rightarrow B \in \mathbf{Alg}_A$ we have $w_{q,m}^F \circ W_{q,\infty}^F(\phi) = \phi \circ w_{q,m}^F$; now substitute $w_{q,n}^F$ for ϕ .)

6.18. REMARK. $\mathbf{V}\mathbf{f} = \mathbf{f}\mathbf{V}$ does not, of course, hold in general (also not in the case of the usual Witt vectors). It is, however, true in $W_{q,\infty}^F(B)$ if $\omega B = 0$, as easily follows from (6.11), which implies that $\mathbf{f}(b_0, b_1, \dots) = (b_0^q, b_1^q, \dots)$ if $\omega B = 0$.

REFERENCES

1. E. Artin and H. Hasse, *Die beide Ergänzungssätze zum Reziprozitätsgesetz der l^n -ten Potenzreste im Körper der l^n -ten Einheitswurzeln*, Abh. Math. Sem. Hamburg **6** (1928), 146–162.
2. P. Cartier, *Groupes formels associés aux anneaux de Witt généralisés*, C. R. Acad. Sci. Paris Sér. A–B **265** (1967), A49–A52.
3. ———, *Modules associés à un groupe formel commutatif. Courbes typiques*, C. R. Acad. Sci. Paris Sér. A–B **265** (1967), A129–A132.
4. ———, *Relèvement des groupes formels commutatifs*, Sem. Bourbaki (1968/1969), exposé 359, Lecture Notes in Math., no. 179, Springer-Verlag, Berlin and New York, 1971.
5. ———, *Séminaire sur les groupes formels*, Inst. Hautes Etudes Sci., 1972 (unpublished notes).
6. J. Dieudonné, *On the Artin-Hasse exponential series*, Proc. Amer. Math. Soc. **8** (1957), 210–214.
7. E. J. Ditters, *Formale Gruppen, die Vermutungen von Atkin-Swinnerton Dyer und verzweigte Witt-vektoren*, Lecture Notes, Göttingen, 1975.
8. V. G. Drinfel'd, *Coverings of p -adic symmetric domains*, Funkcional. Anal. i Prilozhen. **10** (1976), 29–40. (Russian)
9. M. Hazewinkel, *Une théorie de Cartier-Dieudonné pour les A -modules formels*, C. R. Acad. Sci. Paris Sér. A–B **284** (1977), 655–657.
10. ———, *“Tapis de Cartier” pour les A -modules formels*, C. R. Acad. Sci. Paris Sér. A–B **284** (1977), 739–740.

11. _____, *Formal groups and applications*, Academic Press, New York, 1978.
12. J. Lubin and J. Tate, *Formal complex multiplication in local fields*, *Ann. of Math. (2)* **81** (1965), 380–387.
13. G. Whaples, *Generalized local class field theory. III, Second form of existence theorem, Structure of analytic groups*, *Duke Math. J.* **21** (1954), 575–581.
14. E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^m* , *J. Reine Angew. Math.* **176** (1937), 126–140.

DEPARTMENT OF MATHEMATICS, ERASMUS UNIVERSITY, 50, BURG. OUDLAAN, ROTTERDAM, THE NETHERLANDS