ECONOMETRIC INSTITUTE

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

M. HAZEWINKEL

REPORT 7712/M

ERASMUS UNIVERSITY ROTTERDAM, P.O. BOX 1738, ROTTERDAM, THE NETHERLANDS

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

by Michiel Hazewinkel

ABSTRACT.

For any ring R let $\Lambda(R)$ denote the multiplicative group of power series of the form $1 + a_1t + \dots$ with coefficients in R. The Artin-Hasse exponential mappings are homomorphisms $W_{p,\infty}(k) \to \Lambda(W_{p,\infty}(k))$, which satisfy certain additional properties. Somewhat reformulated the Artin-Hasse exponentials turn out to be special cases of a functorial ring homomorphism E: $W_{p,\infty}(-) \to W_{p,\infty}(W_{p,\infty}(-))$, 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 $W^F_{q,\infty}(-)$, 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, which admits a Frobenius like endomorphism σ (we require $\sigma(a) \equiv a^q \bmod \mathfrak{m}$ for all $a \in A$, where $\mathfrak{m}$ is the maximal ideal of A). These ramified-Witt-vector functors $W^F_{q,\infty}(-)$ 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 $W^F_{q,\infty}(\ell)$ is the ring of integers of the unique unramified extension L/K covering ℓ/k.

CONTENTS.

Sept. 13, 1977

1. INTRODUCTION.

For each ring R (commutative with unit element 1) let $\Lambda(R)$ be the abelian group of power series of the form $1 + r_1t + r_2t^2 + \ldots$ 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

$$E: W_{p,\infty}(k) \to \Lambda(W_{p,\infty}(k))$$

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 $\underline{\underline{b}} = \sum_{i=1}^{\infty} \tau(c_i)p^i$, with $c_i \in k$, and $\tau: k \to W_{p,\infty}(k)$ the unique system of multiplicative representants. One now defines

$$E: W_{p,\infty}(k) \to \Lambda(W_{p,\infty}(k)),\ E(\underline{\underline{b}}) = \prod_{i=o}^{\infty} \Phi(\tau(c_i)t)^{p^i}$$

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

$$E: W_{p,\infty}(k) \to W_{p,\infty}(W_{p,\infty}(k))$$

<u>Theorem</u>. There exists a unique functorial homomorphism of ring-valued functors $E: W_{p,\infty}(-) \to W_{p,\infty}(W_{p,\infty}(-))$ such that for all n = 0,1,2,... $w_{p,n} \circ E = \underline{\underline{f}}^n$, where $\underline{\underline{f}}$ is the Frobenius endomorphism of $W_{p,\infty}(-)$ and where $w_{p,n}: W_{p,\infty}(-)) \to W_{p,\infty}(-)$ is the ring homomorphism which assigns to the sequence $(\underline{\underline{b}}_o,\underline{\underline{b}}_1,\ldots)$ of Witt-vectors the Witt-vector

$\underline{\underline{b}}_o^{p^n} + p\underline{\underline{b}}_1^{p^{n-1}} + \ldots + p^{n-1}\underline{\underline{b}}_{n-1}^p + p^n\underline{\underline{b}}_n$.

It should be noted 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 exists a power q of p and an automorphism σ of K, the quotient field of A, such that $\sigma(a) \equiv a^q \mod \mathfrak{m}$ 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

$$W^F_{q,\infty}(-): \underline{\underline{Alg}}_A \to \underline{\underline{Alg}}_A,$$

where $\underline{\underline{Alg}}_A$ is the category of A-algebras, and a ramified Artin-Hasse exponential mapping

$$E: W^F_{q,\infty}(-) \to W^F_{q,\infty}(W^F_{q,\infty}(-)).$$

There is such a ramified Witt-vector functor $W^F_{q,\infty}$ associated to every twisted Lubin-Tate formal group law $F(X,Y)$ over A. This last notion is defined as follows: let $f(X) = X + a_2X^2 + \ldots \in K[[X]]$ and suppose that $a_i \in A$ if q does not divide i and $a_{qi} - \omega^{-1}\tau(a_i) \in A$ 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 formal group laws. The Witt-vector-functors $W^F_{q,\infty}(-)$ 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 $g(\omega)(X) = X + \omega^{-1}X^q + \omega^{-1}\sigma(\omega)^{-1}X^{q^2} + \omega^{-1}\sigma(\omega)^{-1}\sigma^2(\omega)^{-1}X^{q^3} + \ldots$ 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 $W^F_{q,\infty}$ and the functor morphisms E are Witt-vector-like and Artin-Hasse-exponential-like in that

(i) $W^F_{q,\infty}(B) = \{(b_o, b_1, \ldots) | b_i \in B\}$ as a set valued functor and the A-algebra structure can be defined via suitable Witt-like polynomials $w^F_{q,n}(Z_o, \ldots, Z_n)$; cf below for more details.

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

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

(iv) The Artin-Hasse exponential E is characterized by
$w^F_{q,n} \circ E = \underline{\underline{f}}^n$ for all $n = 0,1,2,\ldots$

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 $\mathrm{Cart}_p(R)$ be the Cartier-Dieudonné ring. This is a ring "generated" by two symbols f,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 $\mathrm{Cart}_p(R)$ 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 $\mathrm{Cart}_p(R)$ modules ([3]).

(c) There exists a theory of "lifting" formal groups, in which the Artin-Hasse exponential $E: W_{p,\infty}(-) \to W_{p,\infty}(W_{p,\infty}(-))$ plays an important rôle. These results relate to the socalled "Tapis de Cartier" and relate to certain conjectures of Grothendieck concerning cristalline cohomology, ([4] and [5]).

Now let A be a complete discrete valuation ring with residue field k of q-elements (for simplicity and/or nontriviality of the theory). A formal A-module over $B \in \underline{\underline{\mathrm{Alg}}}_A$ is a formal group law F(X,Y) over B together with a ring homomorphism $\rho_F\colon A \to \mathrm{End}_B(F(X,Y))$, such that $\rho_F(a) \equiv aX$ mod(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 $W^{\pi}_{q,\infty}(-)$ and $\hat{W}^{\pi}_{q,\infty}(-)$ associated to an untwisted, i.e. σ = 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 $W^{\pi}_{q,\infty}(-) \to W^{\pi}_{q,\infty}(W^{\pi}_{q,\infty}(-))$

As we remarked in (i) above, it is perfectly possible to define and analyse $W^F_{q,\infty}(-)$ by starting with the polynomials $w^F_{q,n}(Z)$ 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, independantly of this paper, and independantly 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 $X_o^{q^n} + \pi X_1^{q^{n-1}} + \dots + \pi^{n-1}X_{n-1}^q + \pi^n X_n$.

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. sections 6.1 and 6.5 below). Also this approach removes some of the mystery and exclusive status of the particular Witt polynomials $X_o^{p^n} + pX_1^{p^{n-1}} + \dots + p^nX_n$ (unramified case), $X_o^{q^n} + \pi X_1^{q^{n-1}} + \dots + \pi^n X_n$ (untwisted ramified case), $X_o^{q^n} + \sigma^{n-1}(\omega)X_1^{q^{n-1}} + \sigma^{n-1}(\omega)\sigma^{n-2}(\omega)X_2^{q^{n-2}} + \dots + \sigma^{n-1}(\omega) \dots \sigma(\omega)\omega X_n$ (twisted ramified case). From the theoretical (if not the esthetical and/or computational) point of view all polynomials $\tilde{w}_{q,n}(X_o,\ldots,X_n) = a_n^{-1}(a_nX_o^{q^n} + a_{n-1}X_1^{q^{n-1}} + \ldots + a_oX_n) \in A[X]$ are equally good, provided $a_o = 1$, $a_2, a_3,\ldots$ is a sequence of elements of K such that

$a_i - \omega^{-1}\sigma(a_{i-1}) \in A$ for all $i = 1,2,\ldots$. 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 exists a power q of p and an automorphism σ of K such that

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

The ring A does not need not be complete.

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

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

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

$$(2.4) \qquad f(X) = b_1X + b_2X^2 + \ldots,\ b_i \in B,\ b_1 \text{ a unit of } B$$

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

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

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

(2.6) $b_i \in B[[X]]$ if q does not divide i,

$b_{qi} - \omega^{-1}\tau(b_i) \in B[[X]]$ for all $i = 1, 2, \ldots$

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 $r,m \in \mathbb{N} = \{1,2,\ldots\}$, then $\alpha(X) \equiv \beta(X) \bmod(\omega^r B$, degree $m) \Longleftrightarrow$ $f(\alpha(X)) \equiv f(\beta(X)) \bmod(\omega^r B$, degree $m)$.

Proof. This lemma is a quite special case of the functional equation lemmas of [11], cf sections 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

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

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

$$g(Z_1,\ldots,Z_m)^{q^r n} \equiv \tau\, g(Z_1^q,\ldots,Z_m^q)^{q^{r-1}n} \bmod(\omega^r B) \tag{2.9}$$

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

$$h(Z) = f(g(Z)) = \sum_{i=1}^{\infty} b_i g(Z)^i \equiv \sum_{j=1}^{\infty} b_{qj} g(Z)^{qj} \equiv \omega^{-1} \sum_{j=1}^{\infty} \tau(b_j) g(Z)^{qj}$$

$$\equiv \omega^{-1} \sum_{j=1}^{\infty} \tau(b_j)\tau_* g(Z^q)^j = \omega^{-1}\tau_* f(\tau_* g(Z^q)) = \omega^{-1}\tau_* h(Z^q).$$

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 $F_1(X,Y), \dots, F_m(X,Y) \in B[X,Y]$. Mod(degree m+2) we have that $f(F(X,Y)) \equiv b_1F_{m+1}(X,Y) + f(g(X,Y))$, 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 mod (B[[X,Y]], degree m+2).

$$f(F(X,Y)) \equiv b_1F_{m+1}(X,Y) + f(g(X,Y)) \equiv b_1F_{m+1}(X,Y) + \omega^{-1}\tau_*f(\tau_*g(X^q,Y^q)) \equiv$$

$$\equiv b_1F_{m+1}(X,Y) + \omega^{-1}\tau_*f(\tau_*F(X^q,Y^q))$$

$$= b_1F_{m+1}(X,Y) + \omega^{-1}\tau_*f(X^q) + \omega^{-1}\tau_*f(Y^q)$$

$$\equiv b_1F_{m+1}(X,Y) + f(X) + f(Y) = b_1F_{m+1}(X,Y) + f(F(X,Y))$$

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 that $F(X,Y) \equiv g(X,Y)$ mod(degree m+1) $\Rightarrow F(X^q,Y^q) \equiv g(X^q,Y^q)$ mod(degree m+2). It follows that $b_1F_{m+1}(X,Y) \equiv 0$ mod(B[[X,Y]], 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 $\alpha(X) \equiv \beta(X)$ mod mod(ω^rB, degree m) and $\alpha(X) \in B[[X]]$ then $\alpha(X)^{q^ij} \equiv \beta(X)^{q^ij}$ mod($\omega^{r+i}B$,degree m) which, combined with (2.8), proves that $f(\alpha(X)) \equiv f(\beta(X))$ mod(ω^rB,degree m). To prove the inverse implication $\Leftarrow$ of (iv) we first do the special case $f(\beta(X)) \equiv 0$ mod(ω^rB, degree m) $\Rightarrow \beta(X) \equiv 0$ mod (ω^rB, degree m). Now $\beta(X) \equiv 0$ mod(degree 1), hence $f(\beta(X)) = b_1\beta(X) + b_2\beta(X)^2 + \dots \equiv 0$ mod(ω^rB, degree m), implies $\beta(X) \equiv 0$ mod(ω^rB, degree 2), if $m \geq 2$ (if m = 1 there is nothing to prove), because b_1 is a unit. Now assume with induction that $\beta(X) \equiv 0$ mod(ω^rB, degree n) for some $n < m$. Then, because $\beta(X) \equiv 0$ mod(degree 1) we have $\beta(X)^i \equiv 0$ mod($\omega^{ri}B$, degree $(n+i-1)$) and hence $b_j\beta(X)^j \equiv 0$ mod(ω^rB, degree n+1) if $j \geq 2$. Hence $f(\beta(X)) \equiv 0$ mod(ω^rB, degree m) then gives $b_1\beta(X) \equiv 0$ mod(ω^rB, degree n+1), so that $\beta(X) \equiv 0$ mod(ω^rB, degree n+1) because b_1 is a unit. This proves this special case of (iv). Now let $f(\alpha(X)) \equiv f(\beta(X))$ mod(ω^rB, degree m).

Write $\gamma(X) = f(\beta(X)) - f(\alpha(X))$ and $\delta(X) = f^{-1}(\gamma(X))$. Then $\delta(X) \equiv 0$ mod($\omega^r B$, degree m) by the special case just proved, and $\beta(X) = f^{-1}(f(\alpha(X)) + f(\delta(X))) = F(\alpha(X), \delta(X)) \equiv \alpha(X)$ mod($\omega^r B$, 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 $A, K, k, p, \mathfrak{m}, \sigma, q$ be as in 2.1 above. We consider power series $f(X) = X + c_2X^2 + \ldots \in K[[X]]$ such that there exists a uniformizing element $\omega \in \mathfrak{m}$ such that

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

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

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

Given such a power series $f(X)$, part (i) of the functional equation lemma says that

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

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 $f(X)$, from which it is obtained, is of the form

(3.5) $$f(X) = X + a_1X^q + a_2X^{q^2} + \ldots$$

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 $f(X) = X + c_2X^2 + \ldots \in K[[X]]$ 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 τ = 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 considering also 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 $a_i - \omega^{-1}\tau(a_{i-1}) \in A \Rightarrow \omega \equiv a_i^{-1}\tau(a_{i-1}) \bmod \omega^{2i}A$ 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 τ = 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 sections 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 $\underline{Alg}_A$ be the category of A-algebras. Let $B \in \underline{Alg}_A$. 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 $\phi: B_1 \to B_2$ is in $\underline{Alg}_A$, then $\gamma(t) \mapsto \phi_*\gamma(t)$ (= "apply ϕ to the coefficients") defines a homomorphism of abelian groups $C(F;B_1) \to C(F;B_2)$. This defines us an abelian group valued functor $C(F;-): \underline{Alg}_A \to \underline{Ab}$. There is a natural filtration on $C(F;-)$ defined by the filtration subgroups $C^n(F;B) = \{\gamma(t) \in C(F;B) \mid \gamma(t) \equiv 0 \bmod(\text{degree } n)\}$. The groups $C(F;B)$ are complete with respect to the topology defined by the filtration

$C^n(F;B)$, $n = 1,2,\ldots$

The functor $C(F;-)$ is representable by the A-algebra $A[S] = A[S_1,S_2,\ldots]$. The isomorphism $\mathrm{Alg}_A(A[S],B) \overset{\sim}{\to} C(F;-)$ 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" $\gamma_S(t) = \sum_{i=1}^{\infty}{}^F S_i t^i \in C(F;A[S])$.

4.2. <u>q-typification.</u> 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 $\tau\colon K[S] \to K[S]$ be the ring endomorphism defined by $\tau(a) = \sigma(a)$ for $a \in K$ and $\tau(S_i) = S_i^q$ for $i = 1,2,\ldots$. 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

$$\hat{h}(t) = \sum_{i=o}^{\infty} x_{q^i}(S)t^{q^i}$$

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

$$\varepsilon_q\gamma_S(t) = f^{-1}\Big(\sum_{i=o}^{\infty} x_{q^i}(S)t^{q^i}\Big) \tag{4.3}$$

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

$$\varepsilon_q\gamma(t) = (\phi_\gamma)_*(\varepsilon_q\gamma_S(t)) \tag{4.4}$$

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

4.5. <u>Lemma</u>. Let B be A-torsion free so that $B \to B \otimes_A K$ is injective. Then we have for all $\gamma(t) \in C(F;B)$

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

and $\varepsilon_q C(F;B) = \{\gamma(t) \in C(F;B) | f(\gamma(t)) = \Sigma c_j t^{q^j}$ 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

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

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 $A[T] = A[T_o,T_1,\ldots]$.

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

$$f(\gamma_S(t)) = f(\sum_{i=1}^{\infty}{}^F S_i t^i) = \sum_{j=o}^{\infty} \sum_{i=1}^{\infty} a_j S_i^j t^{q^j i}$$

and it follows that

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

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

$\phi \mapsto \sum_{i=o}^{\infty}{}^F \phi(T_i) t^{q^i} = \phi_*(\gamma_T(t))$, where $\gamma_T(t)$ is the universal q-typical curve

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

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 section 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 $\underline{\underline{f}}_\omega$ and $\underline{\underline{V}}_q$. These constructions all follow the same pattern, the same pattern as was used to define and analyse ε_q in section 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 $\tau: K[T] \to K[T]$, viz. $\tau(a) = \sigma(a)$, $\tau(T_i) = T_i^q$, which extends σ and which is such that $\tau(x) \equiv x^q \bmod \omega A[T]$. 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 $\underline{\underline{f}}_\omega$, etc...

5.2. Constructions. Let $\gamma_T(t)$ be the universal q-typical curve (4.9). We write

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

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

We define

$$(5.4) \qquad \{a\}_F\gamma_T(t) = f^{-1}(\sum_{i=o}^{\infty} \sigma^i(a)x_i(T)t^{q^i})$$

$$(5.5) \qquad \underline{\underline{f}}_\omega\gamma_T(t) = f^{-1}(\sum_{i=o}^{\infty} \sigma^i(\omega)x_{i+1}(T)t^{q^i})$$

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 $\underline{\underline{f}}_\omega$. Let $\tau : K[T] \to K[T]$ be as in 5.1 above. Then by part (ii) of the functional equation lemma we know that

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

It follows by induction that

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

and we also know that

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

where v is the normalized exponential valuation on K. We thus have $\sigma^o(\omega)x_1 = \omega x_1 \in A[T]$ and $\sigma^i(\omega)x_{i+1} - \omega^{-1}\tau(\sigma^{i-1}(\omega)x_i) = \sigma^i(\omega)c_i + \sigma^i(\omega)\omega^{-1}\tau(x_i) - \omega^{-1}\tau(\sigma^{i-1}(\omega)x_i) = \sigma^i(\omega)c_i \in A[T]$. Hence part (iii) of the functional equation lemma says that $\underline{\underline{f}}_\omega\gamma_T(t) \in C(F;A[T])$.

To define the multiplication on $C_q(F;-)$ we need two independant 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

$$(5.8) \qquad \gamma_T(t) * \delta_{\hat{T}}(t) = f^{-1}\Big(\sum_{i=o}^{\infty} a_i^{-1} x_i y_i t^{q^i}\Big)$$

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 $x_o, y_o \in A[T;\hat{T}]$, $x_{i+1} - \omega^{-1}\tau(x_i) = c_i \in A[T;\hat{T}]$, $y_{i+1} - \omega^{-1}\tau(y_i) = d_i \in A[T;\hat{T}]$, where $\tau\colon K[T;\hat{T}] \to K[T;\hat{T}]$ is defined by $\tau(a) = a$ for $a \in K$, and $\tau(T_i) = T_i^q$, $\tau(\hat{T}_i) = T_i^q$, $i = 0,1,2,\ldots$.
Then $a_o x_o y_o = x_o y_o \in A[T;T]$ and $a_{i+1}^{-1} x_{i+1} y_{i+1} - \omega^{-1}\tau(a_i^{-1} x_i y_i) =$
$\omega\sigma(a_i)^{-1}(c_i + \omega^{-1}\tau(x_i))(d_i + \omega^{-1}\tau(y_i)) - \omega^{-1}\sigma(a_i^{-1})\tau(x_i)\tau(y_i) =$
$\omega\sigma(a_i^{-1})c_i d_i + \sigma(a_i)^{-1}(c_i\tau(y_i) + d_i\tau(x_i)) \in A[T;\hat{T}]$ by (5.6) and (5.7).

5.9. Definitions. Let $\gamma(t)$, $\delta(t)$ be two q-typical curves in F over $B \in \underline{\underline{\mathrm{Alg}}}_A$. Let $\phi\colon A[T] \to B$ be the unique A-algebra homomorphism such that $\phi_*\gamma_T(t) = \gamma(t)$, and let $\psi\colon A[T;\hat{T}] \to B$ 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

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

$$(5.11) \qquad \underline{\underline{f}}_\omega\gamma(t) = \phi_*(f_\omega\gamma_T(t))$$

$$(5.12) \qquad \gamma(t)*\delta(t) = \psi_*(\gamma_T(t)*\delta_T(t))$$

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

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

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

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

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 $\gamma_o(t) = t$. The operator $\underline{\underline{f}}_\omega$ is a σ-semilinear A-algebra homomorphism; i.e. $\underline{\underline{f}}_\omega$ is a unit and multiplication preserving group endomorphism such that $\underline{\underline{f}}_\omega \{a\}_F = \{\sigma(a)\}_F \underline{\underline{f}}_\omega$.

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

5.18. Verschiebung. We now define the Verschiebung operator $\underline{\underline{V}}_q$ on $C_q(F;-)$ by the formula $\underline{\underline{V}}_q\gamma(t) = \gamma(t^q)$. (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

(5.19) $$f(\gamma(t)) = \sum_{i=o}^{\infty} x_i t^{q^i} \Rightarrow f(\underline{\underline{V}}_q\gamma(t)) = \sum_{i=o}^{\infty} x_i t^{q^{i+1}}$$

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

(5.21) $$\underline{\underline{f}}_\omega \underline{\underline{V}}_q \gamma(t) = \{\omega\}_F \gamma(t)$$

(5.22) $$\underline{\underline{f}}_\omega \gamma(t) = \gamma(t)^{*q} \bmod \{\omega\}_F C_q(F;B)$$

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 (4.9). Let

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

where the x_i, $i = 0,1,2,\ldots$ are determined by $f(\gamma(t)) = \Sigma\, x_i t^{q^i}$.
It then follows from (5.14) - (5.16) that indeed

$\underline{\underline{f}}_\omega \gamma(t) - \gamma(t)^{*q} = \{\omega\}_F \delta(t)$, 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 $y_o \in A[T]$ 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

$$y_o = x_1 - \sigma^o(\omega)^{-1} x_o^q = c_o + \omega^{-1}\tau(x_o) - \omega^{-1} x_o^q \in A[T]$$

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

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

$$\omega^{i+1} d_i + \tau(a_i^{-1} x_i)$$

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

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

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

$$y_{i+1} - \omega^{-1}\tau(y_i) = x_{i+2} - \sigma^{i+1}(\omega)^{-1} a_{i+1} a_{i+1}^{-q} x_{i+1}^q - \omega^{-1}\tau(x_{i+1}) +$$

$$+ \omega^{-1}\tau(\sigma^i(\omega)^{-1} a_i a_i^{-q} x_i^q)$$

$$= c_{i+1} - \sigma^{i+1}(\omega)^{-1}(a_{i+1} a_{i+1}^{-q} x_{i+1}^q - \omega^{-1}\sigma(a_i)\tau(a_i^{-q} x_i^q))$$

$$= c_{i+1} - \sigma^{i+1}(\omega)^{-1} a_{i+1}(a_{i+1}^{-q} x_{i+1}^q - \tau(a_i^{-q} x_i^q)) \in A[T]$$

because $a_{i+1} = \omega^{-1}\sigma(a_i)$ and because of (5.23). (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 section 5 above.

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

(6.2) $$\Delta_B(b) = f^{-1}\Big(\sum_{i=o}^{\infty} \tau^i(b)a_i t^{q^i}\Big)$$

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

(6.3) $$\Delta_B \circ \tau = \underline{\underline{f}}_\omega \circ \Delta_B$$

(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 $\phi: B \to B'$ 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 $\Delta_B: B \to C_q(F;B)$ 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. $\tau = \underline{\underline{f}}_\omega$, which, as $\tau x \equiv x^q \bmod \omega$ by (5.22), satisfies the hypotheses of 6.1 above (because $\underline{\underline{f}}_\omega$ 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

$$E_B: C_q(F;B) \to C_q(F;C_q(F;B))$$

which are functorial in B because $\underline{\underline{f}}_\omega$ 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 of a finite separable extension L of K. Let ℓ be the residue field of B. Consider the composed map

$$\mu_B\colon B \xrightarrow{\Delta_B} C_q(F;B) \to C_q(F;\ell)$$

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

Proof. Let $b \in B$. Consider $\Delta_B(\omega^r b)$. Then from (6.2) we see that

$$f(\Delta_B(\omega^r b)) \equiv a_\tau \tau^r(\omega^r)\tau^r(b)t^{q^r} \bmod(\omega B, \text{ degree } q^{r+1})$$

By part (iv) of the functional equation lemma 2.7 it follows that

$$\Delta_B(\omega^r b) \equiv y_r \tau^r(b)t^{q^r} \qquad \bmod(\omega B, \text{ degree } q^{r+1})$$

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

$$\ell \overset{\sim}{\to} \omega^r B/\omega^{r+1} B \xrightarrow{\mu_B} C_q^{(r)}(F;\ell)/C_q^{(r+1)}(F,\ell) \overset{\sim}{\to} \ell$$

are given by $x \mapsto y_r x^{q^r}$, for $x \in \ell$. (Here $\ell \overset{\sim}{\to} \omega^r B/\omega^{r+1}B$ is induced by $\omega^r b \to \bar{b}$ with $\bar{b}$ the image of b in ℓ under the canonical projection $B \to \ell$, and $C_q^{(r)}(F;\ell)/C_q^{r+1}(F;\ell) \overset{\sim}{\to} \ell$ is induced by $C_q^{(r)}(F;\ell) \to \ell$, $\gamma(t) \mapsto$ (coefficient of t^{q^r} 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 $C_q(F;\ell)$ 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 $\mu_B^{-1}\underline{\underline{f}}_\omega\mu_B$ extend σ and $\tau(b) \equiv b^q \equiv \mu_B^{-1}\underline{\underline{f}}_\omega\mu_B(b) \bmod \omega B$.

6.7. The maps $s_{q,n}$ and $w^F_{q,n}$. 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 ressemble 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, $W^F_{q,\infty}$: $\underline{\underline{\mathrm{Alg}}}_A \to \underline{\underline{\mathrm{Set}}}$ be defined by

(6.8) $$W^F_{q,\infty}(B) = \{(b_o,b_1,b_2,\ldots)\,|\,b_i \in B\},\ W^F_{q,\infty}(\phi)(b_o,b_1,\ldots) = = (\phi(b_o),\ \phi(b_1),\ldots)$$

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

(6.9) $$e_B(b_o,b_1,\ldots) = \sum_{i=o}^{\infty}{}^F b_i t^{q^i},$$

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

(6.10) $$\underline{\underline{V}}(b_o,b_1,\ldots) = (0,b_o,b_1,\ldots)$$

and in fact

(6.11) $$\underline{\underline{f}}(b_o,b_1,\ldots) = (\hat{b}_o,\hat{b}_1,\ldots) \Rightarrow \hat{b}_i \equiv b_i^q \bmod \omega B$$

(We have not proved the analogon of this for $\underline{\underline{f}}_\omega$; this is not difficult to do by using part (iv) of the functional equation lemma and the additivity of $\underline{\underline{f}}_\omega$).

Next we discuss the analogue of the Witt-polynomials

$X_o^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n$. We define for the universal curve $\gamma_T(t) \in C_q(F;A[T])$

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

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

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

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

$$s_{q,n}(\gamma(t) +_F \delta(t)) = s_{q,n}(\gamma(t)) + s_{q,n}(\delta(t)),\ s_{q,n}(\gamma(t)*\delta(t)) = s_{q,n}(\gamma(t))s_{q,n}(\delta(t)),\ s_{q,n}(\{a\}_F\gamma(t)) = \sigma^n(a)s_{q,n}(\gamma(t)),$$

$$(6.14) \qquad s_{q,n}(f_\omega\gamma(t)) = s_{q,n+1}(\gamma(t)),\ s_{q,n}(\underline{\underline{V}}_q\gamma(t)) = \sigma^{n-1}(\omega)s_{q,n-1}(\gamma(t)) \text{ if } \geq 1,\ s_{q,o}(\underline{\underline{V}}_q\gamma(t)) = 0$$

$$s_{q,n}(t) = 1 \text{ for all } n.$$

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

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

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

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

and it follows that $w^F_{q,n}$ is the functorial map $W^F_{q,\infty}(B) \to B$ defined by the polynomials

$$w^F_{q,n}(Z_o,\dots,Z_n) = a_n^{-1}\Big(\sum_{i=o}^{n} a_i Z_{n-i}^{q^i}\Big)$$

$$(6.16) \qquad = Z_o^{q^n} + \sigma^{n-1}(\omega)Z_1^{q^{n-1}} + \sigma^{n-1}(\omega)\sigma^{n-2}(\omega)Z_2^{q^{n-2}} + \dots +$$

$$+ \sigma^{n-1}(\omega)\ \dots\ \sigma(\omega)\omega Z_n$$

6.17. <u>Theorem</u>. Let (A,σ) be a pair consisting of a discrete valuation ring A of residue characteristic $p > 0$ and a Frobenius-like automorphism $\sigma : K \to K$ such that (2.2) holds for some power q of p. Let ω be any uniformizing element of A, and let $w^F_{q,n}(Z)$, $n = 0, 1, \dots$ be the polynomials defined by (6.15). Then there exists a unique A-algebra valued functor $W^F_{q,\infty}: \underline{\underline{\mathrm{Alg}}}_A \to \underline{\underline{\mathrm{Alg}}}_A$ such that

(i) as a set-valued functor $W^F_{q,\infty}(B) = \{(b_o,b_1,b_2,\dots) \mid b_i \in B\}$ and $W^F_{q,\infty}(\phi)(b_o,b_1,\dots) = (\phi(b_o), \phi(b_1),\dots)$ for all $\phi: B \to B'$ in $\underline{\underline{\mathrm{Alg}}}_A$

(ii) the polynomials $w^F_{q,n}(Z)$ induce functorial σ^n-semilinear A-algebra homomorphisms $w^F_{q,\infty}: W^F_{q,\infty}(B) \to B$, $(b_o,b_1,\dots) \mapsto w^F_{q,\infty}(b_o,\dots,b_n)$.

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

(iii) $w^F_{q,n} \circ \underline{\underline{V}} = \sigma^{n-1}(\omega)w^F_{q,n-1}$ if $n = 1,2,\dots$; $w^F_{q,o} \circ \underline{\underline{V}} = 0$

(iv) $w^F_{q,n} \circ \underline{\underline{f}} = w^F_{q,n+1}$

These endomorphisms $\underline{\underline{f}}$ and $\underline{\underline{V}}$ have (among others) the properties

(v) $\underline{\underline{f}}\underline{\underline{V}} = \omega$

(vi) $\underline{\underline{f}}b \equiv b^q \bmod \omega W^F_{q,\infty}(B)$ for all $\underline{\underline{b}} \in W^F_{q,\infty}(B)$, $B \in \underline{\underline{\mathrm{Alg}}}_A$

(vii) $\underline{\underline{V}}(\underline{\underline{b}}(\underline{\underline{f}}\underline{\underline{c}})) = (\underline{\underline{V}}\underline{\underline{b}})\underline{\underline{c}}$ for all $\underline{\underline{b}}$, $\underline{\underline{c}} \in W^F_{q,\infty}(B)$, $B \in \underline{\underline{\mathrm{Alg}}}_A$

Further there exists a unique functorial A-algebra homomorphism

$$E: W^F_{q,\infty}(-) \to W^F_{q,\infty}(W^F_{q,\infty}(-))$$

which satisfies and is characterized by

(viii) $\qquad w^F_{q,n} \circ E = \underline{\underline{f}}^n$ for all $n = 0,1,2,\dots$

(Here $w^F_{q,n} : W^F_{q,\infty}(W^F_{q,\infty}(B)) \to W^F_{q,\infty}(B)$ is short for $w^F_{q,n,W^F_{q,\infty}(B)}$, i.e. it is the map which assigns to a sequence $(\underline{\underline{b}}_o,\underline{\underline{b}}_1,\ldots)$ of elements of $W^F_{q,\infty}(B)$ the element $w^F_{q,n}(\underline{\underline{b}}_o,\underline{\underline{b}}_1,\ldots) \in W^F_{q,\infty}(B)$). The functor homomorphism E further satisfies

(ix) $$W^F_{q,\infty}(w^F_{q,n}) \circ E = \underline{\underline{f}}^n,$$

where $W^F_{q,\infty}(w^F_{q,n}) : W^F_{q,\infty}(W^F_{q,\infty}(B)) \to W^F_{q,\infty}(B)$ assigns to a sequence $(\underline{\underline{b}}_o,\underline{\underline{b}}_1,\ldots)$ of elements of $W^F_{q,\infty}(B)$ the sequence $(w^F_{q,n}(\underline{\underline{b}}_o),w^F_{q,n}(\underline{\underline{b}}_1),\ldots)$
$\in W^F_{q,\infty}(B)$

Finally if A is complete with perfect residue field k and ℓ/k is a finite separable extension, then $W^F_{q,\infty}(\ell)$ 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 $\underline{\underline{f}}$ corresponds to the unique extension of σ to τ: $B \to B$ which satisfies $\tau(b) \equiv b^q \bmod \omega B$. In particular $W^F_{q,\infty}(k) \simeq A$ with $\underline{\underline{f}}$ corresponding to σ.

Proof. Existence of $W^F_{q,\infty}(-)$, $\underline{\underline{V}}$, $\underline{\underline{f}}$, 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 $B^{\mathbb{N}\cup\{0\}}$, $\underline{\underline{V}}$, $\underline{\underline{f}}$, 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 $B' \to B$. 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 $w^F_{q,n}$. 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

$$w^F_{q,o}(\underline{\underline{V}}(\underline{\underline{b}}(\underline{\underline{fc}}))) = 0$$

$$w^F_{q,n}(\underline{\underline{V}}(\underline{\underline{b}}(\underline{\underline{fc}}))) = \sigma^{n-1}(\omega)w^F_{q,n-1}(\underline{\underline{b}}(\underline{\underline{fc}})) = \sigma^{n-1}(\omega)w^F_{q,n-1}(b)w^F_{q,n-1}(\underline{\underline{fc}})$$

$$= \sigma^{n-1}(\omega)w^F_{q,n-1}(\underline{\underline{b}})w^F_{q,n}(\underline{\underline{c}})$$

and, on the other hand

$$w^F_{q,o}((\underline{\underline{Vb}})\underline{\underline{c}}) = w^F_{q,o}(\underline{\underline{Vb}})w^F_{q,o}(\underline{\underline{c}}) = o\ w^F_{q,o}(\underline{\underline{c}}) = 0$$

$$w^F_{q,n}((\underline{\underline{Vb}})\underline{\underline{c}}) = w^F_{q,n}(\underline{\underline{Vb}})w^F_{q,n}(\underline{\underline{c}}) = \sigma^{n-1}(\omega)w^F_{q,n-1}(\underline{\underline{b}})w^F_{q,n}(\underline{\underline{c}})$$

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

$$w^F_{q,m} \circ W^F_{q,\infty}(w^F_{q,n}) \circ E = w^F_{q,n} \circ w^F_{q,m} \circ E = w^F_{q,n} \circ \underline{\underline{f}}^m$$

$$= w^F_{q,n+m} = w^F_{q,m} \circ \underline{\underline{f}}^n$$

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

6.18. Remark. $\underline{\underline{Vf}} = \underline{\underline{fV}}$ does of course not hold in general (also not in the case of the usual Witt vectors). It is however, true in $W^F_{q,\infty}(B)$ if $\omega B = 0$, as easily follows from (6.11), which implies that $f(b_o,b_1,\dots) = (b_o^q,b_1^q,\dots)$ if $\omega B = 0$.

REFERENCES.

1. E. Artin, H. Hasse, Die beide Ergänzungssätze zum Reciprozitätsgesetz der ℓ^n-ten Potenzreste im Körper der ℓ^n-ten Einheitswürzeln, Abh. Math. Sem. Hamburg 6 (1928), 146-162.
2. P. Cartier, Groupes formels associés aux anneaux de Witt génélisés, C.R. Acad. Sci.(Paris) 265(1967). A50-52.
3. P. Cartier, Modules associes à un groupe formel commutatif. Courbes typiques, C.R. Acad. Sci (Paris) 265(1967). A 129-132.

4. P. Cartier, Relèvement des groupes formels commutatifs, Sem. Bourbaki 1968/1969, exposé 359, Lect. Notes Math. 179, Springer, 1971.

5. P. Cartier, Seminaire sur les groupes formels, IHES 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 (Russian), Funkt. Analiz i ego pril. 10, 2(1976), 29-40.

9. M. Hazewinkel, Une théorie de Cartier-Dieudonné pour les A-modules formels, C.R. Acad. Sci. (Paris) 284 (1977), 655-657.

10. M. Hazewinkel, "Tapis de Cartier" pour les A-modules formels, C.R. Acad. Sci. (Paris) 284 (1977), 739-740.

11. M. Hazewinkel, Formal groups and applications, Acad. Press, to appear.

12. J. Lubin, J. Tate, Formal complex multiplication in local fields, Ann. of Math 81 (1965), 380-387.

13. G. Whaples, Generalized local class field theory III. Second form of the existence theorem. Structure of analytic groups, Duke Math. J. 21(1954), 575-581.

14. E. Witt, Zyklische Körper und Algebren der Characteristik p vom Grad p^m, J. reine und angew. Math. 176(1937), 126-140.