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

par

Michiel Hazewinkel
(Rotterdam)

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

\[ B \subseteq L, \mathfrak{a} \subseteq B, \psi : L \rightarrow L, \psi, q, s_1, s_2, \ldots \]

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

\[ p \in \mathfrak{a}, \quad \psi(b) \equiv b^p \mod \mathfrak{a} \text{ for all } b \in B, \quad \psi(s_i(j, k)) \mathfrak{a} \subseteq B \text{ for all } i, j, k, r \]

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

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

2.3. Functional Equation Lemma. Let \( f(X) \in B[[X]]^m \) be an \( m \)-tuple of power series in \( n \) indeterminates \( X_1, \ldots, X_n \) and \( f(X) \) an \( m \)-tuple of power series in \( n \) indeterminates \( \bar{X}_1, \ldots, \bar{X}_n \). Suppose that \( f(X) \equiv b_1X \mod(\text{degree } 2) \) where \( b_1 \) is a matrix with coefficients in \( B \) which is invertible (over \( B \)). Suppose moreover that

\[ f(X) = \sum_{i=1}^{\infty} s_i \mathcal{L}^i f(X^i) \in B[[X]]^m, \quad f(X) = \sum_{i=1}^{\infty} s_i \mathcal{P}^i \mathcal{X}^i \in B[[X]]^m \]

where \( X^i \) and \( \mathcal{X}^i \) are short for \( (X_1^i, \ldots, X_n^i) \) and \( (\bar{X}_1^i, \ldots, \bar{X}_n^i) \). Then we have

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

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

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

\[ f(X) \mathcal{L} f(X^i) \mathcal{X}^i = \sum_{i=1}^{\infty} s_i \mathcal{L}^i \mathcal{X}^i \mathcal{X}^i \in B[[X]] \]
Finally let $a(X) \in B[[X]]^m$, $\beta(X) \in L[[X]]^m$, $r \in \mathbb{N} = \{1, 2, \ldots \}$. Then

\[(2.8) \quad a(X) \equiv \beta(X) \mod a(X) \iff f(a(X)) \equiv f(\beta(X)) \mod a(X)^r\]

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

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

More generally let $d(X) = d_0X + d_1X^p + \ldots$, $d_i \in \mathbb{P}$. Using the same ingredients and combining (2.6) and (2.7) above one finds that $\exp(d(X)) \in \mathbb{Z}(p)[[X]]$ if and only if $d_i - p^{-1}d_{i-1} \in \mathbb{Z}(p)$ for all $i$ (where one takes $d_{-1} = 0$). This a lemma of Dieudonné [3].

An easy application with $\sigma$ non trivial is the following. Let $B$ be the ring of integers of the completed maximal unramified extension $T$ of $\mathbb{P}$; let $L = T$, $P = q$, $s_1 = p^{-1}$, $s_2 = s_3 = \ldots = 0$, and $\sigma$ the Frobenius automorphism of $T$.

Let $h(X) = 1 + a_1X + a_2X^2 + \ldots \in T[[X]]$. In this setting the combination of (2.6) and (2.7) yields that $h(X) \in B[[X]]$ if and only if $\sigma(h(X^p))/h(X)^p \in 1 + p\mathfrak{B}[X]$], which is lemma 1 of Dwork [6].

For an easy more dimensional application consider the slightly modified Witt vector polynomials $\tilde{w}_0(X) = X_0$, $\tilde{w}_1(X) = X_1 + p^{-1}X_0^p$, \ldots,

\[\tilde{w}_n(X) = X_n + p^{-1}X_{n-1}^p + \ldots + p^{-n}X_0^{p^n} \] Take $B = \mathbb{Z}$, $\mathfrak{a} = p\mathfrak{Z}$, $L = \mathfrak{P}$, $q = p$, $s_1$ be the $(n+1) \times (n+1)$ matrix with $p^{-1}$ on the first subdiagonal and zero's elsewhere; i.e. $s_1(j,k) = 0$ unless $j = k + 1$ and $s_1(k+1,k) = p^{-1}$, $k = 1, 2, \ldots, n$. Let $\tilde{w}(X)$ be the column vector $(\tilde{w}_0(X), \ldots, \tilde{w}_n(X))$. Then, obviously, $\tilde{w}(X) = X + s_1\tilde{w}(X^p)$. It now follows from (2.5) that $\Sigma(X) = \tilde{w}^{-1}(\tilde{w}(X) + \tilde{w}(Y))$ has integral coefficients; or, multiplying both sides of $\tilde{w}(L(X)) = \tilde{w}(X) + \tilde{w}(Y)$ with $p^n$, we see that we have shown that the addition polynomials of the Witt vectors have integral coefficients.

4. ATKIN–SWINNERTON DYER CONGRUENCES. Let $E$ be an elliptic curve over $\mathbb{Q}$ and let $L(s) = \sum_{n=1}^{\infty} (1 - a_p p^{-s} + b_p p^{-2s})^{-1}$ be its global $L$-function, where the local factors $(1 - a_p p^{-s} + b_p p^{-2s})^{-1}$ are defined as follows in terms of the
reductions mod $p$ of a global minimal model $D$ over $\mathbb{Z}$ for $E$:

(i) if $p$ is good, i.e., if $D \otimes \mathbb{Z}/(p)$ is nonsingular then $(1-a_p p^{-s} + b_p p^{1-2s})$ is the numerator of the zetafunction of the elliptic curve $D \otimes \mathbb{Z}/(p)$ over $\mathbb{Z}(p)$;

(ii) if $D \otimes \mathbb{Z}/(p)$ has an ordinary doublepoint then $1-a_p p^{-s} + b_p p^{1-2s} = 1-c_p p^{-s}$ where $c_p = \pm 1$ depending on whether the tangents in the double point are rational over $\mathbb{Z}/(p)$ or not;

(iii) if $D \otimes \mathbb{Z}/(p)$ has a cuspidal parameter $1-a_p p^{-s} + b_p p^{1-2s} = 1$.

Now let $f_E(X) = \sum_{n=1}^{\infty} a_n X^n$ where $L(s) = \sum_{n=1}^{\infty} a_n^{-s}$. Then an immediate and obvious consequence of the Euler product structure of $L(s)$ is that for all $p$

$$f_E(X) = p^{-1} a_p f_E(X^p) + p^{-1} b_p f_E(X^{1/p}) \in \mathbb{Z}(p)[X].$$

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

4.2. Theorem (Honda, Hill, [11], [10] and [12]). The formal group laws $F_E(X,Y)$ and $G_E(X,Y)$ are strictly isomorphic over $\mathbb{Z}$ (i.e., there exists a power series $\psi(X) = X + b_1 X^2 + \ldots, b_1 \in \mathbb{Z}$ such that $\phi(F_E(X,Y)) = G_E(\psi(X),\psi(Y))$).

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

$$a_{np} = a_p b(n) + b_p \beta(n/p) \equiv 0 \mod p^{s-1}$$

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

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

Let e(X) ∈ A[[X]] be any power series in one variable such that

\[ e(X) \equiv \pi X \mod(\text{degree } 2), \quad e(X) \equiv X^q \mod \pi \]

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

In the ingredients (2.1) for the functional equation lemma now take \( B = A, \ L = K, \ A = \pi A, \ p = \text{char}(k), \ q = \infty, \ s_1 = 0, \ s_2 = s_3 = \ldots \).

Then the conditions (2.2) are satisfied. Let \( g(X) \in A[[X]] \) be any power series such that \( g(X) \equiv X \mod(\text{degree } 2) \), and consider \( f(X) \in K[[X]] \) defined (recursively) by the functional equation

\[ f(X) = g(X) + \pi^{-1}f(X^q) \]

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

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

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

\[ f([\pi](X)) = \pi f(X) = \pi g(X) + f(X^q) \equiv f(X^q) \mod \pi \]

It follows by part (2.8) of the functional equation lemma that \( [\pi](X) \equiv X^q \mod \pi \).

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

77
Finally we use the functional equation lemma to show that Lubin-Tate formal group laws constructed via different uniformizing elements \( \tilde{\pi} \) and \( \tilde{\pi} \) become isomorphic over \( \hat{A}_{\text{nr}} \), the completion of the ring of integers of the completion \( K_{\text{nr}} \) of the maximal unramified extension \( K_{\text{nr}} \) of \( K \). Let therefore \( f(X), \tilde{f}(X) \in A[[X]] \) satisfy

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

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

\[
(5.6) \quad uf(X) - \pi^{-1} \circ (uf(X^q)) = uf(X) - \pi^{-1} uf(X^q) \in \hat{A}_{\text{nr}}[[X]]
\]

and also of course \( \tilde{f}(X) - \pi^{-1} \circ \tilde{f}(X^q) = \tilde{f}(X) - \pi^{-1} \tilde{f}(X^q) \in A[[X]] \subseteq \hat{A}_{\text{nr}}[[X]] \), so that by part (2,6) of the functional equation lemma we have that

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

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

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

\[
(6.1) \quad g(M,\eta)(X) = X + p^{-1} D(\eta)\mathfrak{s}_w g(M,\eta)(X^p)
\]

By part (2,5) of the functional equation lemma (with \( B = A, \mathfrak{L} = K, \mathfrak{a} = pA, \sigma \) as above, \( q = p, s_1 = p^{-1} D(\eta), s_2 = s_3 = \ldots = 0 \) it follows that

\[ G(M,\eta)(X,Y) = g(M,\eta)^{-1}(g(M,\eta)(X) + g(M,\eta)(Y)) \]

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

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

$$g(M,n)v(X^p) = D(\eta)g(N',\eta)(X^p) = D(\eta)\sigma_*(G(M,n))(X^p) \equiv pg(M,n)(X) \mod pA$$

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

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

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

Hence $f^{-1}(pf(X)) = [p](X) \equiv v(X^p) = f^{-1}(E_\sigma f(X^p))$. It follows by part (2.8) of the functional equation lemma that $pf(X) \equiv E_\sigma f(X^p) \mod pA$, i.e. that $f(X) - p^{-1}E_\sigma f(X^p) \in A[[X]]$, so that by part (2.6) of the functional equation
Let \( k \) be the residue field of the ring \( \mathbb{Q}_p \) or \( \mathbb{F}_p(X) \). Consider the power series

\[
\sum_{n=0}^{\infty} g_{q^n}(X, Y) = g_{q^0}(X) + g_{q^1}(Y) + \cdots
\]

Then \( g_q(X) = X + qX^2 + \cdots \), so that by section 5 above, \( G_q(X, Y) \) is a Lubin-Tate formal group law over \( A \). For every \( A \)-torsion free \( A \)-algebra \( B \) let \( \mathfrak{A}_{q^r}(B) \) be the following set of power series in one variable \( t \):

\[
\mathfrak{A}_{q^r}(B) = \{ \gamma(t) \in B[[t]] \mid \gamma(0) = 0, \gamma(t) = \sum_{i=0}^{\infty} a_i t^i \text{ for certain } a_i \in B \}
\]

For arbitrary \( A \)-algebras \( B \) one can define \( \mathfrak{A}_{q^r}(B) = \{ \gamma(t) \mid \gamma(t) \in \mathfrak{A}_{q^r}(B') \} \) where \( B' \) is any \( A \)-torsion free \( A \)-algebra with a surjective \( A \)-algebra homomorphism \( \phi : B' \to B \). The sets \( \mathfrak{A}_{q^r}(B) \) have a natural group structure defined by \( \gamma(t) + \delta(t) = G_q(\gamma(t), \delta(t)) \) and a topology defined by the subgroups

\[
\{ \gamma(t) \in \mathfrak{A}_{q^r}(B) \mid \gamma(t) \equiv 0 \mod t^N \}.
\]

There is an obvious morphism \( \mathfrak{A}_{q^r}(B) \to \mathfrak{A}_{q^s}(B) \) attached to an \( A \)-algebra homomorphism \( \phi : B_1 \to B_2 \), viz.

\[
(\gamma(t)) \mapsto (\gamma(t)) \phi(t).
\]

So that we have a complete topological group valued functor \( B \mapsto \mathfrak{A}_{q^r}(B) \).

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

\[
\text{if } g_q(t) = \sum x_i t^i, \quad g_{q^r}(t) = \sum y_i t^i, \quad \text{then } \gamma(t) \delta(t) = g_{q^r}(\sum x_i y_i q^{r-1} t^i)
\]

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

Assume that \( B \) is \( A \)-torsion free and admits an \( A \)-algebra endomorphism \( \delta \) such that \( \delta(b) \equiv b^q \mod B \) for all \( b \in B \). By part (2,7) of lemma 2.3 we then
FUNCTIONNAL EQUATION LEMMA

have $x_i - n^{-1} x_{i-1} = a_i \in B$, $y_i - n^{-1} x_{i-1} = b_i \in B$ for all $i$ (with $x_{-1} = y_{-1} = 0$).

Hence $n^{-1} x_i n^{-1} y_i \in B$ for all $i$. It follows that $n^{-1} x_i y_i - n^{-1}(n^{-1} x_{i-1} y_{i-1}) = n^{-1} a_i b_i + n^{-1} a_i y_i - n^{-1} b_i x_i \in B$, so that by part (2.6) of lemma 2.3 we

have indeed that $g_i (\sum_{i} n^{i} x_i y_i t^i)$ has its coefficients in $B$. To extend this definition to the case of arbitrary $A$-algebras $B$ use an argument similar as just below (7.2) using that every $A$-algebra $B$ is a quotient of an $A$-algebra $B'$ which satisfies our assumptions, e.g. $B' = A[Z_b/b \in B]$. There is also a natural $A$-module structure on $W_{q,w}(B)$ defined by $\gamma(t) \mapsto [a](\gamma(t))$ where $[a](X) = g_{q,w}(ag_w(X))$, $a \in A$, cf. also section 5. All in all this defines a functor $W^A_{q,w} : Alg_A \rightarrow Alg_A$, which, we claim, possibly deserves the name "ramified Witt vector functor". To bolster this claim we remark the following:

- There is an additive Verschiebung morphism $\mathcal{V}_q$ defined by $\mathcal{V}_q(\gamma(t)) = \gamma(q t^q)$ and a Frobenius $A$-algebra functor endomorphism $\tau_q$. The latter is defined for $A$-torsion free $A$-algebras $B$ by the formula $\tau_q(\gamma(t)) = g_{q,w}^{-1}(\sum_{i=0}^{\infty} n^{-i} \tau_q \gamma(t^q)^i)$ where the $x_i$ are as in (7.3). Of course the integrality of $\mathcal{V}_q \gamma(t)$ is proved by means of the functional equation lemma. We have $\mathcal{V}_q = [\tau_q]$, $\mathcal{V}_q \gamma(t) \equiv \gamma(t^q) \mod [\tau_q]W^A_{q,w}(B)$.

- Let $A'$ be the ring of integers of an unramified extension $K'$ of $K$ and let $\sigma \in Gal(K'/K)$ be the Frobenius automorphism. For each $a' \in A'$, let $\Delta(a') = g_{q,w}^{-1}(\sum_{i=0}^{\infty} n^{-i} \sigma (a') t^q)^i) \in W^A_{q,w}(B)$. (Integrality of $\Delta(a')$ is of course proved by means of the functional equation lemma). Then $a' \mapsto \Delta(a')$ is a homomorphism of $A$-algebras and the composite $A' \overset{\Delta}{\rightarrow} W^A_{q,w}(A') \rightarrow W^A_{q,w}(k')$ is an isomorphism. In particular $W^A_{q,w}(k') = A'$ with $\sigma$

corresponding to $\mathcal{V}_q$, generalizing a well-known property of the Witt vectors.

- There is an $A$-algebra homorphism $\Delta : W^A_{q,w}(k') \rightarrow W^A_{q,w}(k')$, the ramified Artin-Hasse exponential, characterized by $\mathcal{V}_q \circ \Delta = \tau_q^1$, where $\mathcal{V}_q \circ \Delta : W^A_{q,w}(B) \rightarrow B$ is the functorial $A$-algebra homomorphism $W^A_{q,w}(\gamma(t)) = n^i$ times the coefficient of $t^q^i$ in $g_{q,w}(\gamma(t))$.

For more details concerning this construction cf. [7], section 25; for a twisted version of these constructions which also works for local fields with not necessarily finite residue field cf. also [9]. Another construction of the functors $W^A_{q,w}$ has independently been given by Bitters [4] and Drinfeld [5].
M. HAZEWINKEL

BIBLIOGRAPHY.


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