Lecture notes on Witt vectors

Lars Hesselholt

The purpose of these notes is to give a self-contained introduction to Witt vectors. We cover both the classical p-typical Witt vectors of Teichmüller and Witt [**4**] and the generalized or big Witt vectors of Cartier [**1**]. In the approach taken here, all necessary congruences are isolated in the lemma of Dwork. A slightly different but very readable account may be found in Bergman [**3**, Appendix]. We conclude with a brief treatment of special λ-rings and Adams operations. We refer the reader to Langer-Zink [**2**, Appendix] for a careful analysis of the behavior of the ring of Witt vectors with respect to étale morphisms.

Let $\mathbb{N}$ be the set of positive integers, and let $S \subset \mathbb{N}$ be a subset with the property that, if $n \in S$, and if d is a divisor in n, then $d \in S$. We then say that S is a truncation set. The big Witt ring $\mathbb{W}_S(A)$ is defined to be the set A^S equipped with a ring structure such that the ghost map

$$w\colon \mathbb{W}_S(A) \to A^S$$

that takes the vector $(a_n \mid n \in S)$ to the sequence $(w_n \mid n \in S)$, where

$$w_n = \sum_{d \mid n} d a_d^{n/d},$$

is a natural transformation of functors from the category of rings to itself. Here, on the right-hand side, A^S is considered a ring with componentwise addition and multiplication. To prove that there exists a unique ring structure on $\mathbb{W}_S(A)$ that is characterized in this way, we first prove the following result.

Lemma 1 (Dwork). *Suppose that, for every prime number p, there exists a ring homomorphism $\phi_p\colon A \to A$ with the property that $\phi_p(a) \equiv a^p$ modulo pA. Then a sequence $(x_n \mid n \in S)$ is in the image of the ghost map*

$$w\colon \mathbb{W}_S(A) \to A^S$$

if and only if $x_n \equiv \phi_p(x_{n/p})$ modulo $p^{v_p(n)}A$, for every prime number p, and for every $n \in S$ with $v_p(n) \geqslant 1$. Here $v_p(n)$ denotes the p-adic valuation of n.

Proof. We first show that, if $a \equiv b$ modulo pA, then $a^{p^{v-1}} \equiv b^{p^{v-1}}$ modulo $p^v A$. If we write $a = b + p\epsilon$, then

$$a^{p^{v-1}} = b^{p^{v-1}} + \sum_{1 \leqslant i \leqslant p^{v-1}} \binom{p^{v-1}}{i} b^{p^{v-1}-i} p^i \epsilon^i.$$

The author was partially supported by the National Science Foundation.

In general, the p-adic valuation of the binomial coefficient $\binom{m+n}{n}$ is equal to the number of carriers in the addition of m and n in base p. So

$$v_p\left(\binom{p^{v-1}}{i}\right) = v - 1 - v_p(i),$$

and hence,

$$v_p\left(\binom{p^{v-1}}{i}p^i\right) = v - 1 + i - v_p(i) \geqslant v.$$

This proves the claim. Now, since ϕ_p is a ring-homomorphism,

$$\phi_p(w_{n/p}(a)) = \sum_{d\mid(n/p)} d\phi_p(a_d^{n/pd})$$

which is congruent to $\sum_{d\mid(n/p)} da_d^{n/d}$ modulo $p^{v_p(n)}A$. If d divides n but not n/p, then $v_p(d) = v_p(n)$, and hence this sum is congruent to $\sum_{d\mid n} da_d^{n/d} = w_n(a)$ modulo $p^{v_p(n)}A$ as stated. Conversely, if $(x_n \mid n \in S)$ is a sequence such that $x_n \equiv \phi_p(x_{n/p})$ modulo $p^{v_p(n)}A$, we find a vector $a = (a_n \mid n \in S)$ with $w_n(a) = x_n$ as follows. We let $a_1 = x_1$ and assume, inductively, that a_d has been chosen, for all d that divides n, such that $w_d(a) = x_d$. The calculation above shows that the difference

$$x_n - \sum_{d\mid n, d\neq n} da_d^{n/d}$$

is congruent to zero modulo $p^{v_p(n)}A$. Hence, we can find $a_n \in A$ such that na_n is equal to this difference. $\square$

Proposition 2. *There exists a unique ring structure such that the ghost map*

$$w\colon \mathbb{W}_S(A) \to A^S$$

is a natural transformation of functors from rings to rings.

Proof. Let A be the polynomial ring $\mathbb{Z}[a_n, b_n \mid n \in S]$. Then the unique ring homomorphism

$$\phi_p\colon A \to A$$

that maps a_n to a_n^p and b_n to b_n^p satisfies that $\phi_p(f) = f^p$ modulo pA. Let a and b be the sequences $(a_n \mid n \in S)$ and $(b_n \mid n \in S)$. Since ϕ_p is a ring homomorphism, Lemma 1 shows immediately that the sequences $w(a) + w(b)$, $w(a) \cdot w(b)$, and $-w(a)$ are in the image of the ghost map. It follows that there are sequences of polynomials $s = (s_n \mid n \in S)$, $p = (p_n \mid n \in S)$, and $\iota = (\iota_n \mid n \in S)$ such that $w(s) = w(a) + w(b)$, $w(p) = w(a) \cdot w(b)$, and $w(\iota) = -w(a)$. Moreover, since A is torsion free, the ghost map is injective, and hence, these polynomials are unique.

Let now A' be any ring, and let $a' = (a'_n \mid n \in S)$ and $b' = (b'_n \mid n \in S)$ be two vectors in $\mathbb{W}_S(A')$. Then there is a unique ring homomorphism $f\colon A \to A'$ such that $\mathbb{W}_S(f)(a) = a'$ and $\mathbb{W}_S(f)(b) = b'$. We define $a' + b' = \mathbb{W}_S(f)(s)$, $a \cdot b = \mathbb{W}_S(f)(p)$, and $-a = \mathbb{W}_S(f)(\iota)$. It remains to prove that the ring axioms are verified. Suppose first that A' is torsion free. Then the ghost map is injective, and hence, the ring axioms are satisfied in this case. In general, we choose a surjective ring homomorphism $g\colon A'' \to A'$ from a torsion free ring A''. Then

$$\mathbb{W}_S(g)\colon \mathbb{W}_S(A'') \to \mathbb{W}_S(A')$$

is again surjective, and since the ring axioms are satisfied on the left-hand side, they are satisfied on the right-hand side. $\square$

If $T \subset S$ are two truncation sets, then the forgetful map

$$R^S_T \colon \mathbb{W}_S(A) \to \mathbb{W}_T(A)$$

is a natural ring homomorphism called the restriction from S to T. If $n \in \mathbb{N}$, and if $S \subset \mathbb{N}$ is a truncation set, then

$$S/n = \{d \in \mathbb{N} \mid nd \in S\}$$

is again a truncation set. We define the nth Verschiebung map

$$V_n \colon \mathbb{W}_{S/n}(A) \to \mathbb{W}_S(A)$$

by

$$V_n((a_d \mid d \in S/n))_m = \begin{cases} a_d, & \text{if } m = nd, \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 3. *The Verschiebung map V_n is additive.*

Proof. There is a commutative diagram

$$\begin{tikzcd} \mathbb{W}_{S/n}(A) \arrow[r, "w"] \arrow[d, "V_n"] & A^{S/n} \arrow[d, "V_n^w"] \\ \mathbb{W}_S(A) \arrow[r, "w"] & A^S \end{tikzcd}$$

where the map V_n^w is given by

$$V_n^w((x_d \mid d \in S/n))_m = \begin{cases} nx_d, & \text{if } m = nd, \\ 0, & \text{otherwise.} \end{cases}$$

Since the map V_n^w is additive, so is the map V_n. Indeed, if A is torsion free, the horizontal maps are both injective, and hence, V_n is additive in this case. In the general case, we choose a surjective ring homomorphism $g \colon A' \to A$ and argue as in the proof of Prop. 2 above. $\square$

Lemma 4. *There exists a unique natural ring homomorphism*

$$F_n \colon \mathbb{W}_S(A) \to \mathbb{W}_{S/n}(A)$$

such the diagram

$$\begin{tikzcd} \mathbb{W}_S(A) \arrow[r, "w"] \arrow[d, "F_n"] & A^S \arrow[d, "F_n^w"] \\ \mathbb{W}_{S/n}(A) \arrow[r, "w"] & A^{S/n}, \end{tikzcd}$$

where $F_n^w((x_m \mid m \in S))_d = x_{nd}$, commutes.

Proof. We construct the Frobenius map F_n in a manner similar to the construction of the ring operations on $\mathbb{W}_S(A)$ in Prop. 2. We let A be the polynomial ring $\mathbb{Z}[a_n \mid n \in S]$, and let a be the vector $(a_n \mid n \in S)$. Then Lemma 1 shows that the sequence $F_n^w(w(a)) \in A^{S/n}$ is the image of a (unique) element

$$F_n(a) = (f_{n,d} \mid d \in S/n) \in \mathbb{W}_{S/n}(A)$$

by the ghost map. If A' is any ring, and if $a' = (a'_n \mid n \in S)$ is a vector in $\mathbb{W}_S(A')$, then we define $F_n(a') = \mathbb{W}_{S/n}(g)(F_n(a))$, where $g\colon A \to A'$ is the unique ring homomorphism that maps a to a'. Finally, since F_n^w is a ring homomorphism, an argument similar to the proof of Lemma 3 shows that also F_n is a ring homomorphism. □

The Teichmüller representative is the map

$$[-]_S\colon A \to \mathbb{W}_S(A)$$

defined by

$$([a]_S)_n = \begin{cases} a, & \text{if } n = 1, \\ 0, & \text{otherwise.} \end{cases}$$

It is a multiplicative map. Indeed, there is a commutative diagram

$$\begin{tikzcd} A \arrow[r, equal] \arrow[d, "{[-]_S}"] & A \arrow[d, "{[-]_S^w}"] \\ \mathbb{W}_S(A) \arrow[r, "w"] & A^S, \end{tikzcd}$$

where $([a]_S^w)_n = a^n$, and $[-]_S^w$ is a multiplicative map.

Lemma 5. *The following relations holds.*
(i) $a = \sum_{n\in S} V_n([a_n]_{S/n})$.
(ii) $F_n V_n(a) = na$.
(iii) $aV_n(a') = V_n(F_n(a)a')$.
(iv) $F_m V_n = V_n F_m$, *if* $(m, n) = 1$.

Proof. One easily verifies that both sides of each equation have the same image by the ghost map. This shows that the relations hold, if A is torsion free, and hence, in general. □

Proposition 6. *The ring $\mathbb{W}_S(\mathbb{Z})$ of big Witt vectors in the ring of rational integers is equal to the product*

$$\mathbb{W}_S(\mathbb{Z}) = \prod_{n\in S} \mathbb{Z} \cdot V_n([1]_{S/n})$$

with the multiplication given by

$$V_m([1]_{S/m}) \cdot V_n([1]_{S/n}) = c \cdot V_d([1]_{S/d}),$$

where $c = (m, n)$ and $d = mn/(m, n)$ are the greatest common divisor and the least common multiple of m and n.

Proof. The formula for the multiplication follows from Lemma 5 (ii)-(iv). Suppose first that S is finite. If S is empty, the statement is trivial, so assume that S is non-empty. We let $m \in S$ be maximal, and let $T = S \smallsetminus \{m\}$. Then the sequence of abelian groups

$$0 \to \mathbb{W}_{\{1\}}(\mathbb{Z}) \xrightarrow{V_m} \mathbb{W}_S(\mathbb{Z}) \xrightarrow{R_T^S} \mathbb{W}_T(\mathbb{Z}) \to 0$$

is exact, and we wish to show that it is equal to the sequence

$$0 \to \mathbb{Z} \cdot [1]_{\{1\}} \xrightarrow{V_m} \prod_{n \in S} \mathbb{Z} \cdot V_n([1]_{S/n}) \xrightarrow{R_T^S} \prod_{n \in T} \mathbb{Z} \cdot V_n([1]_{T/n}) \to 0.$$

The latter sequence is a sub-sequence of the former sequence, and, inductively, the left-hand terms (resp. the right-hand terms) of the two sequences are equal. Hence, middle terms are equal, too. The statement for S finite follows. Finally, a general truncation set S is the union of the finite sub-truncation sets $S_\alpha \subset S$, and hence,

$$\mathbb{W}_S(\mathbb{Z}) = \lim_{\alpha} \mathbb{W}_{S_\alpha}(\mathbb{Z}).$$

This proves the stated formula in general. □

The action of the restriction, Frobenius, and Verschiebung operators on the generators $V_n([1]_{S/n})$ is easily derived from the relations Lemma 5 (ii)–(iv). To give a formula for the Teichmüller representative, we recall the Möbius inversion formula. Let $g \colon \mathbb{N} \to \mathbb{Z}$ be a function, and let $f \colon \mathbb{N} \to \mathbb{Z}$ be the function given by

$$f(n) = \sum_{d \mid n} g(d).$$

Then the function g is given by f by means of the formula

$$g(n) = \sum_{d \mid n} \mu(d) f(n/d),$$

where $\mu \colon \mathbb{N} \to \{-1, 0, 1\}$ is the Möbius function. Here $\mu(d) = (-1)^r$, if d is a product of $r \geqslant 0$ distinct prime numbers, and $\mu(d) = 0$, otherwise.

Addendum 7. *Let m be an integer. Then*

$$[m]_S = \sum_{n \in S} \frac{1}{n} \Big(\sum_{d \mid n} \mu(d) m^{n/d} \Big) V_n([1]_{S/n}),$$

where $\mu \colon \mathbb{N} \to \{-1, 0, 1\}$ is the Möbius function.

Proof. It suffices to prove that the formula holds in $\mathbb{W}_S(\mathbb{Z})$. We know from Prop. 6 that there are unique integers r_d, $d \in S$, such that

$$[m]_S = \sum_{d \in S} r_d V_d([1]_{S/d}).$$

Evaluating the nth ghost component of this equation, we get

$$m^n = \sum_{d \mid n} d r_d,$$

and the stated formula now follows from the Möbius inversion formula. □

Lemma 8. *Suppose that A is an $\mathbb{F}_p$-algebra, and let $\varphi\colon A \to A$ be the Frobenius endomorphism. Then*

$$F_p = R^S_{S/p} \circ \mathbb{W}_S(\varphi)\colon \mathbb{W}_S(A) \to \mathbb{W}_{S/p}(A).$$

Proof. We recall from the proof of Prop. 4 that

$$F_p(a) = (f_{p,d}(a) \mid d \in S/p),$$

where $f_{p,d}$ are the integral polynomials defined by the equations

$$\sum_{d|n} d f_{p,d}^{n/d} = \sum_{d|pn} d a_d^{pn/d}$$

for all $n \in S$. Let $A = \mathbb{Z}[a_n \mid n \in S]$. We shall prove that for all $n \in S/p$,

$$f_{p,n} \equiv a_n^p$$

modulo pA. This is equivalent to the statement of the lemma. If $n = 1$, we have $f_{p,1} = a_1^p + p a_p$, and we are done in this case. So let $n > 1$ and assume, inductively, that the stated congruence has been proved for all proper divisors in n. Then, if d is a proper divisor in n, $f_{p,d} \equiv a_d^p$ modulo pA, so

$$d f_{p,d}^{n/d} \equiv d a_d^{pn/d}$$

modulo $p^{v_p(n)+1}A$; compare the proof of Lemma 1. Rewriting the defining equations

$$\sum_{d|n} d f_{p,d}^{n/d} = \sum_{d|n} d a_d^{pn/d} + \sum_{d|pn, d\nmid n} d a_d^{pn/d}$$

and noting that if $d \mid pn$ and $d \nmid n$, then $v_p(d) = v_p(n) + 1$, we find

$$n f_{p,n} \equiv n a_n^p$$

modulo $p^{v_p(n)+1}A$. Since A is torsion free, we conclude that $f_{p,n} \equiv a_n^p$ modulo pA as desired. □

We consider the truncation set $P = \{1, p, p^2, \dots\} \subset \mathbb{N}$ that consists of all powers of a fixed prime number p. The proper non-empty sub-truncation sets of P all are of the form $\{1, p, \dots, p^{n-1}\}$, for some positive integer n. The rings

$$W(A) = \mathbb{W}_P(A)$$
$$W_n(A) = \mathbb{W}_{\{1,p,\dots,p^{n-1}\}}(A)$$

are called the ring of p-typical Witt vectors in A and p-typical Witt vectors of length n in A, respectively. We shall now show that, if A is a $\mathbb{Z}_{(p)}$-algebra, the rings of big Witt vectors $\mathbb{W}_S(A)$ decompose canonically as a product of rings of p-typical Witt vectors. We begin with the following result.

Lemma 9. *Let m be an integer and suppose that m is invertible (resp. a non-zero-divisor) in A. Then m is invertible (resp. a non-zero-divisor) in $\mathbb{W}_S(A)$.*

Proof. It suffices to prove the lemma, for S finite. Indeed, in general, $\mathbb{W}_S(A)$ is the limit of $\mathbb{W}_T(A)$, where T ranges over the finite sub-truncation sets of S. So assume that S is finite and non-empty. Let $n \in S$ be maximal, and let $T = S \smallsetminus \{n\}$. Then $S/n = \{1\}$ and we have an exact sequence

$$0 \to A \xrightarrow{V_n} \mathbb{W}_S(A) \xrightarrow{R^S_T} \mathbb{W}_T(A) \to 0$$

from which the lemma follows by easy induction. $\square$

PROPOSITION 10. *Let p be a prime number, and let A be a $\mathbb{Z}_{(p)}$-algebra. Let S be a truncation set, and let $I(S) = \{k \in S \mid p \nmid k\}$. Then the ring $\mathbb{W}_S(A)$ has a natural idempotent decomposition*

$$\mathbb{W}_S(A) = \prod_{k \in I(S)} \mathbb{W}_S(A)e_k$$

where

$$e_k = \prod_{l \in I(S), l \neq 1} \left(\frac{1}{k} V_k([1]_{S/k}) - \frac{1}{kl} V_{kl}([1]_{S/kl}) \right).$$

Moreover, the composite map

$$\mathbb{W}_S(A)e_k \hookrightarrow \mathbb{W}_S(A) \xrightarrow{F_k} \mathbb{W}_{S/k}(A) \xrightarrow{R^{S/k}_{S/k\cap P}} \mathbb{W}_{S/k\cap P}(A)$$

is an isomorphism.

PROOF. We calculate

$$w_n(\frac{1}{k} V_k([1]_{S/k})) = \begin{cases} 1, & \text{if } k \in S \cap k\mathbb{N}, \\ 0, & \text{otherwise,} \end{cases}$$

and hence,

$$w_n(e_k) = \begin{cases} 1, & \text{if } k \in S \cap kP, \\ 0, & \text{otherwise.} \end{cases}$$

It follows that the elements e_k, $k \in I(S)$, are orthogonal idempotents in $\mathbb{W}_S(A)$. This proves the former part of the statement. To prove the latter part, we note that multiplication by k defines a bijection

$$S/k \cap P = (S \cap kP)/k \xrightarrow{\sim} S \cap kP$$

and that the following diagram commutes:

$$\begin{tikzcd} \mathbb{W}_S(A)e_k \arrow[r, "w"] \arrow[d, "R^{S/k}_{S/k\cap P} F_k"] & A^{S\cap kP} \arrow[d, "k^*", "\sim"'] \\ \mathbb{W}_{S/k\cap k}(A) \arrow[r, "w"] & A^{S/k\cap P}. \end{tikzcd}$$

We first assume that A is torsion free and has an endomorphism $\phi_p \colon A \to A$ such that $\phi_p(a) \equiv a^p$ modulo pA. Then the horizontal maps w are both injective. Moreover, Lemma 1 identifies the image of the top horizontal map w with the set of sequences $(x_d \mid d \in S \cap kP)$ such that $x_d \equiv \phi_p(x_{d/p})$ modulo $p^{v_p(d)}A$. Similarly, the image of the lower horizontal map w is the set of sequences $(y_d \mid d \in S/k \cap P)$ such that $y_d \equiv \phi_p(y_{d/p})$ modulo $p^{v_p(d)}A$. Since the right-hand vertical map k^* induces an isomorphism of these subrings, the left-hand vertical map $R^{S/k}_{S/k\cap P}F_k$ is an isomorphism in this case. $\square$

EXAMPLE 11. Let $S = \{1, 2, \ldots, n\}$ such that $\mathbb{W}_S(A)$ is the ring $\mathbb{W}_n(A)$ of big Witt vectors of length n in A. Then $S/k \cap P = \{1, p, \ldots, p^{s-1}\}$ where $s = s(n, k)$ is the unique integer with $p^{s-1}k \leqslant n < p^s k$. Hence, if A is a $\mathbb{Z}_{(p)}$-algebra,

$$\mathbb{W}_n(A) \xrightarrow{\sim} \prod W_s(A)$$

where the product ranges over $1 \leqslant k \leqslant n$ with $p \nmid k$, and where $s = s(n,k)$ is given as above.

We now consider the ring $W_n(A)$ of p-typical Witt vectors of length n in A in more detail. The ghost map

$$w\colon W_n(A) \to A^n$$

takes the vector $(a_0, \dots, a_{n-1})$ to the sequence $(w_0, \dots, w_{n-1})$ where

$$w_i = a_0^{p^i} + pa_1^{p^{i-1}} + \dots + p^i a_i.$$

If $\phi\colon A \to A$ is a ring homomorphism with $\phi(a) \equiv a^p$ modulo pA, then Lemma 1 identifies the image of the ghost map with the subring of sequences $(x_0, \dots x_{n-1})$ such that $x_i \equiv \phi(x_{i-1})$ modulo $p^i A$, for all$1 \leqslant i \leqslant n-1$. We write

$$[-]_n\colon A \to W_n(A)$$

for the Teichmüller representative and

$$F\colon W_n(A) \to W_{n-1}(A)$$
$$V\colon W_{n-1}(A) \to W_n(A)$$

for the pth Frobenius and pth Verschiebung.

Lemma 12. *If A is an $\mathbb{F}_p$-algebra, then $VF = p$.*

Proof. For any ring A, the composite VF is given by multiplication by the element $V([1]_{n-1})$. Suppose that A is an $\mathbb{F}_p$-algebra. The exact sequences

$$0 \to A \xrightarrow{V^{n-1}} W_n(A) \xrightarrow{R} W_{n-1}(A) \to 0$$

show, inductively, that $W_n(A)$ is annihilated by p^n. Hence, $V([1]_{n-1})$ is annihilated by p^{n-1}. We show by induction on n that $V([1]_{n-1}) = p[1]_n$, the case $n = 1$ being trivial. The formula from Addendum 7 gives that

$$[p]_n = p[1]_n + \sum_{0<s<n} \frac{p^{p^s} - p^{p^{s-1}}}{p^s} V^s([1]_{n-s}).$$

Since $[p]_n = 0$, and since, inductively, $V^s([1]_{n-s}) = p^{s-1}V([1]_{n-1})$, for $0 < s < n$, we can rewrite this formula as

$$0 = p[1]_n + (p^{p^{n-1}-1} - 1)V([1]_{n-1}).$$

But $p^{n-1} - 1 \geqslant n-1$, so we get $p[1]_n = V([1]_{n-1})$ as stated. □

We now suppose that A is a p-torsion free ring and that there exists a ring homomorphism $\phi\colon A \to A$ such that $\phi(a) \equiv a^p$ modulo pA. It follows from Lemma 1 that there is a unique ring homomorphism

$$s_\phi\colon A \to W(A)$$

such that the composite

$$A \xrightarrow{s_\phi} W(A) \xrightarrow{w} A^{\mathbb{N}_0}$$

maps a to $(a, \phi(a), \phi^2(a), \dots)$. We then define

$$t_\phi\colon A \to W(A/pA)$$

to be the composite of s_ϕ and the map induced by the canonical projection of A onto A/pA. We recall that the $\mathbb{F}_p$-algebra A/pA is said to be perfect, if the Frobenius endomorphism $\varphi\colon A/pA \to A/pA$ is an automorphism.

Proposition 13. *Let A be a p-torsion free ring, and let $\phi\colon A \to A$ be a ring homomorphism such that $\phi(a) \equiv a^p$ modulo pA. Suppose that A/pA is a perfect $\mathbb{F}_p$-algebra. Then the map t_ϕ induces an isomorphism*

$$t_\phi\colon A/p^nA \xrightarrow{\sim} W_n(A),$$

for all $n \geqslant 1$.

Proof. The map t_ϕ factors as in the statement since

$$V^nW(A/pA) = V^nW(\phi^n(A/pA)) = V^nF^nW(A/pA) = p^nW(A/pA).$$

The proof is now completed by an induction argument based on the following commutative diagram:

$$\begin{tikzcd}
0 \arrow[r] & A/pA \arrow[r, "p^{n-1}"] \arrow[d, "\varphi^{n-1}"] & A/p^nA \arrow[r, "\mathrm{pr}"] \arrow[d, "t_\phi"] & A/p^{n-1}A \arrow[r] \arrow[d, "t_\phi"] & 0 \\
0 \arrow[r] & A/pA \arrow[r, "V^{n-1}"] & W_n(A/pA) \arrow[r, "R"] & W_{n-1}(A/pA) \arrow[r] & 0.
\end{tikzcd}$$

The top horizontal sequence is exact, since A is p-torsion free, and the left-hand vertical map is an isomorphism, since A/pA is perfect. The statement follows by induction on $n \geqslant 1$. $\square$

We return to the ring of big Witt vectors. We write $(1 + tA[\![t]\!])^*$ for the multiplicative group of power series over A with constant term 1.

Proposition 14. *There is a natural commutative diagram*

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "\gamma"] \arrow[d, "w"] & (1 + tA[\![t]\!])^* \arrow[d, "t\frac{d}{dt}\log"] \\
A^{\mathbb{N}} \arrow[r, "\gamma^w"] & tA[\![t]\!]
\end{tikzcd}$$

where

$$\gamma(a_1, a_2, \dots) = \prod_{n \geqslant 1}(1 - a_nt^n)^{-1},$$
$$\gamma^w(x_1, x_2, \dots) = \sum_{n \geqslant 1} x_nt^n,$$

and the horizontal maps are isomorphisms of abelian groups.

Proof. It is clear that γ^w is an isomorphism of additive abelian groups. We show that γ is a bijection. We have

$$\prod_{n \geqslant 1}(1 - a_nt^n)^{-1} = (1 + b_1t + b_2t^2 + \dots)^{-1}$$

where the coefficient b_n is given by the sum

$$b_n = \sum (-1)^r a_{i_1} \dots a_{i_r}$$

that runs over all $1 \leqslant i_1 < \cdots < i_r \leqslant n$ such that $i_1 + 2i_2 + \cdots + ri_r = n$. This formula shows that the coefficients a_n, $n \geqslant 1$, are determined uniquely by the coefficients b_n, $n \geqslant 1$. Indeed, we have the recursive formula

$$a_n = b_n - \sum (-1)^r a_{i_1} \dots a_{i_r},$$

where the sum on the right-hand side ranges over $1 \leqslant i_1 < \cdots < i_r < n$ such that $i_1 + 2i_2 + \cdots + ri_r = n$. To prove that the map γ is a homomorphism from the additive group $\mathbb{W}(A)$ to the multiplicative group $(1 + tA[\![t]\!])^*$, it suffices as usual to consider the case where A is torsion free. In this case the vertical maps in the diagram of the statement are both injective, and hence, it suffices to show that the diagram of the statement commutes. We calculate:

$$\begin{aligned} t\frac{d}{dt}\log\Big(\prod_{d\geqslant 1}(1 - a_d t^d)^{-1}\Big) &= -\sum_{d\geqslant 1} t\frac{d}{dt}\log(1 - a_d t^d) = \sum_{d\geqslant 1}\frac{t a_d t^d}{1 - a_d t^d} \\ = \sum_{d\geqslant 1}\sum_{s\geqslant 0} d a_d t^d \cdot a_d^s t^{sd} &= \sum_{d\geqslant 1}\sum_{q\geqslant 1} d a_d^q t^{qd} = \sum_{n\geqslant 1}\Big(\sum_{d\mid n} d a_d^{n/d}\Big)t^n. \end{aligned}$$

This completes the proof. $\square$

ADDENDUM 15. *The map γ induces an isomorphism of abelian groups*

$$\gamma_S \colon \mathbb{W}_S(A) \xrightarrow{\sim} \Gamma_S(A)$$

where $\Gamma_S(A)$ is the quotient of the multiplicative group $\Gamma(A) = (1 + tA[\![t]\!])^*$ by the subgroup $I_S(A)$ of all power series of the form $\prod_{n\in\mathbb{N}\smallsetminus S}(1 - a_n t^n)^{-1}$.

PROOF. The kernel of the restriction map

$$R_S^{\mathbb{N}} \colon \mathbb{W}(A) \to \mathbb{W}_S(A)$$

is equal to the subset of all vectors $a = (a_n \mid n \in \mathbb{N})$ such that $a_n = 0$, if $n \in S$. The image of this subset by the map γ is the subset $I_S(A) \subset \Gamma$. $\square$

EXAMPLE 16. If $S = \{1, 2, \dots, m\}$, then $I_S(A) = (1 + t^{m+1}A[\![t]\!])^*$. Hence, in this case, Addendum 15 gives an isomorphism of abelian groups

$$\gamma_S \colon \mathbb{W}_m(A) \xrightarrow{\sim} \Gamma_S(A) = (1 + tA[\![t]\!])^*/(1 + t^{m+1}A[\![t]\!])^*.$$

The structure of this group, for A a $\mathbb{Z}_{(p)}$-algebra, was examined in Example 11.

LEMMA 17. *Let p be a prime number, and let A be any ring. Then the ring homomorphism $F_p \colon \mathbb{W}(A) \to \mathbb{W}(A)$ satisfies that $F_p(a) \equiv a^p$ modulo $p\mathbb{W}(A)$.*

PROOF. We first let $A = \mathbb{Z}[a_1, a_2, \dots]$ and $a = (a_1, a_2, \dots)$. If suffices to show that there exists $b \in \mathbb{W}(A)$ such that $F_p(a) - a^p = pb$. By Lemma 9, the element is necessarily unique; we use Lemma 1 to prove that it exists. We have

$$w_n(F_p(a) - a^p) = \sum_{d\mid pn} d a_d^{pn/d} - \Big(\sum_{d\mid n} d a_d^{n/d}\Big)^p$$

which is clearly congruent to zero modulo pA. So let $x = (x_n \mid n \in \mathbb{N})$ with

$$x_n = \frac{1}{p}(F_p(a) - a^p).$$

We wish to show that $x = w(b)$, for some $b \in \mathbb{W}(A)$. The unique ring homomorphism $\phi_\ell \colon A \to A$ that maps a_n to a_n^ℓ satisfies that $\phi_\ell(f) = f^\ell$ modulo ℓA, and hence, Lemma 1 shows that x is in the image of the ghost map if and only if

$$x_n \equiv \phi_\ell(x_{n/\ell})$$

modulo $\ell^{v_\ell(n)}A$, for all primes ℓ and all $n \in \ell\mathbb{N}$. This is equivalent to showing that

$$w_n(F_p(a) - a^p) \equiv \phi_\ell(w_{n/p}(F_p(a) - a^p))$$

modulo $\ell^{v_\ell(n)}A$, if $\ell \neq p$ and $n \in \ell\mathbb{N}$, and modulo $\ell^{v_\ell(n)+1}A$, if $\ell = p$ and $n \in \ell\mathbb{N}$. If $\ell \neq p$, the statement follows from Lemma 1, and if $\ell = p$ and $n \in \ell\mathbb{N}$, we calculate

$$\begin{aligned} & w_n(F_p(a) - a^p) - \phi_p(w_{n/p}(F_p(a) - a^p)) \\ &= \sum_{d \mid pn, d \nmid n} d a_d^{pn/d} - \big(\sum_{d \mid n} d a_d^{n/d}\big)^p + \big(\sum_{d \mid (n/p)} d a_d^{n/d}\big)^p. \end{aligned}$$

If $d \mid pn$ and $d \nmid n$, then $v_p(d) = v_p(n) + 1$, so the first summand is congruent to zero modulo $p^{v_p(n)+1}A$. Similarly, if $d \mid n$ and $d \nmid (n/p)$, then $v_p(d) = v_p(n)$, and hence,

$$\sum_{d \mid n} d a_d^{n/d} \equiv \sum_{d \mid (n/p)} d a_d^{n/d}$$

modulo $p^{v_p(n)}A$. But then

$$\big(\sum_{d \mid n} d a_d^{n/d}\big)^p \equiv \big(\sum_{d \mid (n/p)} d a_d^{n/d}\big)^p$$

modulo $p^{v_p(n)+1}A$; compare the proof of Lemma 1. This completes the proof. □

Let $\epsilon \colon \mathbb{W}(A) \to A$ be the ring homomorphism that takes $a = (a_n \mid n \in \mathbb{N})$ to a_1.

Proposition 18. *There exists a unique natural ring homomorphism*

$$\Delta \colon \mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(A))$$

such that $w_n(\Delta(a)) = F_n(a)$, for all $n \in \mathbb{N}$. Moreover, the functor $\mathbb{W}(-)$ and the ring homomorphisms Δ and ϵ form a comonad on the category of rings.

Proof. By naturality, we may assume that A is torsion free. Then Lemma 9 shows that also $\mathbb{W}(A)$ is torsion free, and hence, the ghost map

$$w \colon \mathbb{W}(\mathbb{W}(A)) \to \mathbb{W}(A)^{\mathbb{N}}$$

is injective. Lemma 17 and Lemma 1 show that the sequence $(F_n(a) \mid a \in \mathbb{N})$ is in the image of the ghost map. Hence, the natural ring homomorphism Δ exists. The second part of the statement means that

$$\mathbb{W}(\Delta_A) \circ \Delta_A = \Delta_{\mathbb{W}(A)} \circ \Delta_A \colon \mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(\mathbb{W}(A)))$$

and

$$\mathbb{W}(\epsilon_A) \circ \Delta_A = \epsilon_{\mathbb{W}(A)} \circ \Delta_A \colon \mathbb{W}(A) \to \mathbb{W}(A).$$

Both equalities are readily verified by evaluating the ghost coordinates. □

Definition 19. A *special λ-ring* is a ring A and a ring homomorphism

$$\lambda \colon A \to \mathbb{W}(A)$$

that makes A a coalgebra over the comonad $(\mathbb{W}(-), \Delta, \epsilon)$.

Let $(A, \lambda \colon A \to \mathbb{W}(A))$ be a special λ-ring. Then the associated nth Adams operation is the ring homomorphism defined to be the composition

$$\psi^n \colon A \xrightarrow{\lambda} \mathbb{W}(A) \xrightarrow{w_n} A$$

of the structure map and the nth ghost map.

References

[1] P. Cartier, *Groupes formels associés aux anneaux de Witt généralisés*, C. R. Acac. Sci. Paris, Sér. A–B **265** (1967), A129–A132.

[2] A. Langer and T. Zink, *De Rham-Witt cohomology for a proper and smooth morphism*, J. Inst. Math. Jussieu **3** (2004), 231–314.

[3] D. Mumford, *Lectures on curves on an algebraic surface*, Annals of Mathematics Studies, vol. 59, Princeton University Press, Princeton, N.J., 1966.

[4] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, J. reine angw. Math. **176** (1937), 126–140.

Massachusetts Institute of Technology, Cambridge, Massachusetts

E-mail address: `larsh@math.mit.edu`

Nagoya University, Nagoya, Japan

E-mail address: `larsh@math.nagoya-u.ac.jp`