

1 Witt vectors

The goal of this section is to give a very important example of a comonad: the Witt vector construction is a functor $\mathbf{CRing} \rightarrow \mathbf{CRing}$ which is used frequently in several mathematical fields, especially Number Theory and Algebraic Geometry. Historically, Witt vectors have been introduced by Ernst Witt in [Wit37], who discovered what is today called *p-typical Witt vectors* while studying cyclic algebras of degree p^n . The ring structure on the Witt vectors is highly unintuitive and the whole construction is rather complicated, which is why this section starts with a rigorous, detailed and self-contained introduction to the topic. We will define the p-typical Witt vectors as well as the *big Witt vectors*, which are due to [Car67]. This is essentially an elaboration of [Hes08] (some of the material is also covered in [Hes15]), making the proofs as seamless as possible, while only stating what is needed for proving the final theorem. For different expositions to Witt vectors, consider [Rab14], [Ser79]. The most complete account of Witt vectors that I know of is [Haz09].

1.1 Construction of the Witt vectors

Definition 1.1 (truncation set). Let \mathbb{N} be the set of positive integers and let $S \subseteq \mathbb{N}$ be a subset with the property that $\forall n \in \mathbb{N} : \text{if } d \text{ is a divisor of } n, \text{ then } d \in S$. We then say that S is a *truncation set*.

Now let S be a truncation set. As a set, we define the *big Witt ring* $\mathbb{W}_S(A)$ to be A^S , and we will give it a unique ring structure such that the *ghost map* is a ring homomorphism. Furthermore, if $f: A \rightarrow B$ is a ring homomorphism, we define $\mathbb{W}_S(f): \mathbb{W}_S(A) \rightarrow \mathbb{W}_S(B)$ to be the function which applies f componentwise, that is $(a_n)_{n \in S} \mapsto (f(a_n))_{n \in S}$. This construction will turn out to be functorial and we will see that the Witt vector functor admits a comonadic structure.

Definition 1.2 (ghost map). We define $w: \mathbb{W}_S(A) \rightarrow A^S$ by $(a_n)_{n \in S} \mapsto (w_n)_{n \in S}$ where

$$w_n = \sum_{d|n} da_d^{n/d}$$

Recall that for every prime number p , we have the *p-adic valuation map*:

Definition 1.3 (p-adic valuation). $v_p: \mathbb{Z} \rightarrow \mathbb{N} \cup \{\infty\}$ is defined by

$$v_p(n) = \begin{cases} \max\{k \in \mathbb{N} : p^k \mid n\} & \text{if } n \neq 0 \\ \infty & \text{if } n = 0 \end{cases}$$

Lemma 1.4 Let A be a ring, $a, b \in A$, $v \in \mathbb{N}$, and p a prime number. Then:

$$a \equiv b \pmod{pA} \implies a^{p^v} \equiv b^{p^v} \pmod{p^{v+1}A}.$$

PROOF: We can write $a = b + p\varepsilon$ for some $\varepsilon \in A$, then by the binomial theorem we get:

$$a^{p^v} = (b + p\varepsilon)^{p^v} = \sum_{i=0}^{p^v} \binom{p^v}{i} b^{p^v-i} (p\varepsilon)^i = b^{p^v} + \sum_{i=1}^{p^v} \binom{p^v}{i} b^{p^v-i} p^i \varepsilon^i.$$

CLAIM. for every $1 \leq i \leq p^v: v_p\left(\binom{p^v}{i}\right) = v - v_p(i)$.

Proof of claim. First, note that $v_p(p^v - i) = v - v_p(i)$. (Indeed: write $i = p^{v_p(i)} \cdot k$ for some $k \in \mathbb{Z}, p \nmid k$. Then $p^v - i = p^v - p^{v_p(i)} \cdot k = p^{v_p(i)} \cdot (p^{v-v_p(i)} - k)$, hence $p^{v_p(i)} \mid p^v - i$. But $p^{v_p(i)+1} \nmid p^v - i$, since $p \nmid k$.)

Now we can apply the p-adic valuation to the following equality:

$$\begin{aligned}
i! \cdot \binom{p^v}{i} &= p^v \cdot (p^v - 1) \cdot \dots \cdot (p^v - (i - 1)) \\
\implies v_p\left(i! \cdot \binom{p^v}{i}\right) &= v_p(p^v \cdot (p^v - 1) \cdot \dots \cdot (p^v - (i - 1))) \\
\iff v_p(i!) + v_p\left(\binom{p^v}{i}\right) &= v_p(p^v) + v_p(p^v - 1) + \dots + v_p(p^v - (i - 1)) \\
\iff v_p(i!) + v_p\left(\binom{p^v}{i}\right) &= v + v_p((i - 1)!) \\
\iff v_p\left(\binom{p^v}{i}\right) &= v + v_p((i - 1)!) - v_p(i!) \\
\iff v_p\left(\binom{p^v}{i}\right) &= v + v_p\left(\frac{(i - 1)!}{i!}\right) \\
\iff v_p\left(\binom{p^v}{i}\right) &= v - v_p(i)
\end{aligned}$$

where we use the multiplicativity of the p-adic valuation. //

It follows that

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

which means that those summands vanish mod $p^{v+1}A$. □

The core of the construction is contained in the following Lemma:

Lemma 1.5 (Dwork) *Suppose that for every prime number p there exists a ring homomorphism $\phi_p: A \rightarrow A$ with the property that $\phi_p(a) \equiv a^p$ modulo pA . Then for every sequence $x = (x_n)_{n \in S}$, the following are equivalent:*

- (i) *The sequence x is in the image of the ghost map $w: W_S(A) \rightarrow A^S$.*
- (ii) *For every prime number p and every $n \in S$ with $v_p(n) \geq 1$,*

$$x_n \equiv \phi_p(x_{n/p}) \quad \text{modulo } p^{v_p(n)}A.$$

PROOF: (\implies) Suppose x is in the image of the ghost map, that means there is a sequence $a = (a_n)_{n \in S}$ such that $x_n = w_n(a)$ for all $n \in S$. We calculate:

$$\phi(x_{n/p}) = \phi(w_{n/p}(a)) = \phi\left(\sum_{d \mid n/p} da_d^{n/pd}\right) = \sum_{d \mid n/p} d \cdot \phi(a_d^{n/pd})$$

since ϕ is a ring homomorphism and $d \in \mathbb{N}$. Now

$$\sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) \equiv \sum_{d|n/p} d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A} \quad (1.1)$$

$$\equiv \sum_{d|n} d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A} \quad (1.2)$$

so we get

$$\phi(x_{n/p}) \equiv \sum_{d|n} d \cdot a_d^{n/d} = w_n(a) = x_n \pmod{p^{v_p(n)} A}.$$

Proof of (1.1). First, note that

$$x \equiv y \pmod{p^m A} \implies dx \equiv dy \pmod{p^{m+v_p(d)} A} \quad (*)$$

for all $m \in \mathbb{N}, d \in \mathbb{Z}$. Now we can write $n/pd = p^\alpha \cdot N$ for some $N \in \mathbb{Z}, p \nmid N, \alpha = v_p(n/pd)$. Now by the assumptions of the lemma we get that $\phi_p(a_d^N) \equiv a_d^{p \cdot N} \pmod{pA}$, so we can calculate:

$$\phi_p(a_d^{n/pd}) \stackrel{\text{def.}}{=} \phi_p(a_d^{p^\alpha \cdot N}) = \phi_p(a_d^N)^{p^\alpha} \equiv a_d^{(p \cdot N)^{p^\alpha}} \pmod{p^{\alpha+1} A}$$

using Lemma 1.4 for the last congruence. Now $(*)$ and the fact that

$$a_d^{(p \cdot N)^{p^\alpha}} = a_d^{p \cdot N \cdot p^\alpha} \stackrel{\text{def.}}{=} a_d^{p \cdot n/pd} = a_d^{n/d}$$

gives us

$$d \cdot \phi_p(a_d^{n/pd}) \equiv d \cdot a_d^{n/d} \pmod{p^{\alpha+1+v_p(d)} A}$$

But

$$\alpha + 1 + v_p(d) \stackrel{\text{def.}}{=} v_p(n/pd) + 1 + v_p(d) = v_p(n/d) + v_p(d) = v_p(n)$$

so it follows that for every d

$$d \cdot \phi_p(a_d^{n/pd}) \equiv d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A}$$

which implies (1). \square

Proof of (1.2). It suffices to show that if $d \mid n, d \nmid n/p$, the term $d \cdot a_d^{n/d}$ vanishes mod $p^{v_p(n)} A$. But in this case, $v_p(d) = v_p(n)$, hence $d \equiv 0 \pmod{p^{v_p(n)} A}$. \square

(\Leftarrow) Let $(x_n)_{n \in S}$ be a sequence such that $x_n \equiv \phi_p(x_{n/p}) \pmod{p^{v_p(n)} A} \forall p \text{ prime}, n \in S, v_p(n) \geq 1$. Define $(a_n)_{n \in S}$ with $w_n((a_n)_{n \in S}) = x_n$ as follows:

$$a_1 := x_1$$

and if a_d has been chosen for all $d \mid n$ such that $w_d(a) = x_d$ we see that for every prime $p \mid n$:

$$\begin{aligned} x_n &\equiv \phi_p(x_{n/p}) \pmod{p^{v_p(n)} A} \\ &= \phi_p\left(\sum_{d|n/p} d \cdot a_d^{n/pd}\right) \\ &= \sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) \end{aligned}$$

because ϕ_p is a ring homomorphism. Using our previous calculations, we see that

$$\begin{aligned} \sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) &\stackrel{(1.1)}{\equiv} \sum_{d|n/p} d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A} \\ &\stackrel{(1.2)}{\equiv} \sum_{d|n} d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A} \\ &\equiv \sum_{d|n, d \neq n} d \cdot a_d^{n/d} \pmod{p^{v_p(n)} A} \end{aligned}$$

In conclusion:

$$p^{v_p(n)} \mid \left(x_n - \sum_{d|n, d \neq n} d \cdot a_d^{n/d} \right)$$

for all $p \mid n$. But this implies that

$$n \mid \left(x_n - \sum_{d|n, d \neq n} d \cdot a_d^{n/d} \right)$$

hence $\exists a_n \in A$ such that

$$x_n = \sum_{d|n, d \neq n} d \cdot a_d^{n/d} + n \cdot a_n = \sum_{d|n} d \cdot a_d^{n/d}.$$

□

We will often need the following

Lemma 1.6 *If A is a torsion-free ring, the ghost map is injective.*

PROOF: Let $a = (a_n)_{n \in S}$ such that $w(a) = 0$. This means $w_n = 0$ for all $n \in S$. We will prove by induction, that $a_n = 0$ for all $n \in S$. First, $a_1 = w_1 = 0$. And if $a_d = 0$ for all $d \in S, d < n$ we see that

$$0 = w_n = \sum_{d|n} d \cdot a_d^{n/d} = n \cdot a_n$$

and since A is torsion-free, this implies $a_n = 0$.

□

Now we can finish the construction of the Witt vectors:

Theorem 1.7 *There exists a unique ring structure such that the ghost map*

$$w : \mathbb{W}_S(A) \rightarrow A^S$$

is a natural transformation of functors from rings to rings.

PROOF: Step 1: Let $A = \mathbb{Z}[a_n, b_n \mid n \in S]$. Consider the unique ring homomorphism

$$\begin{aligned} \phi_p : A &\rightarrow A; \\ a_n &\mapsto a_n^p, \\ b_n &\mapsto b_n^p \end{aligned}$$

ϕ_p satisfies that $\phi_p(f) \equiv f^p$ modulo pA (Indeed: it suffices to show that $\overline{\phi_p(f)} = \overline{f^p}$ in $\mathbb{F}_p[a_n, b_n \mid n \in S]$, which is apparent).

CLAIM. $w(a) + w(b)$, $w(a) \cdot w(b)$ and $-w(a)$ are in the image of the ghost map.

Proof of claim. Since we can use Lemma 1.5, it suffices to show that for all prime p , for all $n \in S$ with $p \mid n$:

$$\begin{aligned} w_n(a) + w_n(b) &\equiv \phi_p(w_{n/p}(a) + w_{n/p}(b)) && \text{mod } p^{v_p(n)}A \\ w_n(a) \cdot w_n(b) &\equiv \phi_p(w_{n/p}(a) \cdot w_{n/p}(b)) && \text{mod } p^{v_p(n)}A \\ -w_n(a) &\equiv \phi_p(-w_{n/p}(a)) && \text{mod } p^{v_p(n)}A \end{aligned}$$

but since $w_n(a), w_n(b)$ are in the image of the ghost map, we know that $w_n(a) \equiv \phi_p(w_{n/p}(a)) \text{ mod } p^{v_p(n)}A$ and $w_n(b) \equiv \phi_p(w_{n/p}(b)) \text{ mod } p^{v_p(n)}A$. The claim now follows using the fact that ϕ_p is a ring homomorphism and that congruence is compatible with addition and multiplication. //

It follows there are sequences $S = (S_n)_{n \in S}$, $P = (P_n)_{n \in S}$ and $I = (I_n)_{n \in S}$ of polynomials such that

$$w(S) = w(a) + w(b), \quad w(P) = w(a) \cdot w(b), \quad w(I) = -w(a)$$

Since A is torsion-free, the ghost map is injective by 1.6 and hence, these polynomials are unique.

Step 2: Now let A' be any ring. Let $a' = (a'_n)_{n \in S}$, $b' = (b'_n)_{n \in S}$ be two vectors in $\mathbb{W}_S(A')$. Then there is a unique ring homomorphism

$$\begin{aligned} f: A &\rightarrow A'; \\ a_n &\mapsto a'_n, \\ b_n &\mapsto b'_n \end{aligned}$$

such that $\mathbb{W}_S(f)(a) = a'$ and $\mathbb{W}_S(f)(b) = b'$ (Remember that $A = \mathbb{Z}[a_n, b_n \mid n \in S]$). We define:

$$\begin{aligned} a' + b' &:= \mathbb{W}_S(f)(S) = (S_n(a'_1, \dots, a'_n, b'_1, \dots, b'_n))_{n \in S} \\ a' \cdot b' &:= \mathbb{W}_S(f)(P) = (P_n(a'_1, \dots, a'_n, b'_1, \dots, b'_n))_{n \in S} \\ -a' &:= \mathbb{W}_S(f)(I) = (I_n(a'_1, \dots, a'_n, b'_1, \dots, b'_n))_{n \in S} \end{aligned}$$

where f commutes with integer polynomials, since it is a ring homomorphism.

CLAIM. These operations make $\mathbb{W}_S(A)$ into a ring.

Proof of claim. Suppose first that A' is torsion-free, then the ghost map is injective and hence the ring axioms are satisfied. For the general case, choose a surjective ring homomorphism $g: A'' \rightarrow A'$ from a torsion-free ring A'' (For example, one could take A'' to be $\mathbb{Z}A'$). Then $\mathbb{W}_S(g): \mathbb{W}_S(A'') \rightarrow \mathbb{W}_S(A')$ is again surjective, and since the ring axioms are satisfied on the left-hand side, they are satisfied on the right-hand side. // ok so?

CLAIM. $w: \mathbb{W}_S(A) \rightarrow A^S$ is a natural ring homomorphism.

Naturality: let $f: A \rightarrow B$.

$$\begin{array}{ccc} \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(f)} & \mathbb{W}_S(B) \\ \downarrow w & & \downarrow w \\ A^S & \xrightarrow{f^S} & B^S \end{array}$$

commutes because f is a ring homomorphism, hence commutes with the integer polynomials w_n . Let $a', b' \in \mathbb{W}_S(A)$. Then:

$$w(a' + b') = w(\mathbb{W}_S(f)(S)) = f(w(s)) = f(w(a) + w(b)) = f(w(a)) + f(w(b)) = w(a') + w(b')$$

□ finish

Corollary 1.8 $w_n: \mathbb{W}_S(A) \rightarrow A$ is a natural ring homomorphism for all $n \in S$.

PROOF: This follows immediately from 1.7. □

Lemma 1.9 The zero element in $\mathbb{W}_S(A)$ is given by $(0, 0, 0, \dots)$ and the unit in $\mathbb{W}_S(A)$ is given by $(1, 0, 0, \dots)$.

PROOF: (For better readability, this proof assumes $S = \mathbb{N}$, but the general proof is exactly the same.) Suppose first that $A = \mathbb{Z}[a_n, b_n \mid n \in \mathbb{N}]$. Let $a = (a_n)_n$ be a Witt vector. Then:

$$w((0, 0, 0, \dots)) = (0, 0, 0, \dots)$$

since $w_n(0, 0, 0, \dots) = 0$ for all n .

$$w((1, 0, 0, \dots)) = (1, 1, 1, \dots)$$

since $w_n(1, 0, 0, \dots) = 1^n = 1$ for all n . By injectivity of the ghost map, the claim follows, because $(0, 0, 0, \dots)$ and $(1, 0, 0, \dots)$ are the zero element respectively the unit in $A^{\mathbb{N}}$. In the general case: For A' any ring, $(a'_n)_n \in \mathbb{W}_S(A')$, $(a'_n)_n + (0, 0, \dots)$ is defined as $(S_1(a'_1, 0), S_2(a'_1, a'_2, 0, 0), \dots)$ and since $(S_1(a_1, 0), S_2(a_1, a_2, 0, 0), \dots) = (a_1, a_2, \dots) \in \mathbb{Z}[a_n, b_n \mid n \in \mathbb{N}]$, these polynomial equations still hold if we plug in a different sequence. The same reasoning show that $(1, 0, \dots)$ is the unit. □

Proposition 1.10 $\mathbb{W}_S(-)$ is a functor $\mathbf{CRing} \rightarrow \mathbf{CRing}$.

PROOF: $\mathbb{W}_S(\text{id}) = \text{id}$ and $\mathbb{W}_S(g \circ f) = \mathbb{W}_S(g) \circ \mathbb{W}_S(f)$ are clear, since $\mathbb{W}_S(-)$ on morphisms is identical with the countable product functor $(-)^{\mathbb{N}}$. All that is left to show is that for a ring homomorphism $f: A \rightarrow B$, $\mathbb{W}_S(f): \mathbb{W}_S(A) \rightarrow \mathbb{W}_S(B)$ is again a ring homomorphism.

$$\mathbb{W}_S(f)(1, 0, \dots) = (f(1), f(0), \dots) = (1, 0, \dots)$$

Now let $x = (x_n)_n, y = (y_n)_n$ be two Witt vectors.

$$\begin{aligned} \mathbb{W}_S(f)(x + y) &= \mathbb{W}_S(f)(S_n(x_1, \dots, x_n, y_1, \dots, y_n))_n \\ &= (f(S_n(x_1, \dots, x_n, y_1, \dots, y_n)))_n \\ &= (S_n(f(x_1), \dots, f(x_n), f(y_1), \dots, f(y_n)))_n \\ &= \mathbb{W}_S(f)(x) + \mathbb{W}_S(f)(y) \end{aligned}$$

where f commutes with integer polynomials since it is a ring homomorphism. An identical computation shows that

$$\mathbb{W}_S(f)(x \cdot y) = \mathbb{W}_S(f)(x) \cdot \mathbb{W}_S(f)(y)$$

□

1.2 The Verschiebung, Frobenius and Teichmüller maps

We have various operations on Witt vectors that are of interest.

Definition 1.11 (Restriction map). If $T \subseteq S$ are two truncation sets, the *restriction from S to T*

$$R_T^S: \mathbb{W}_S(A) \rightarrow \mathbb{W}_T(A)$$

is a natural ring homomorphism. This follows from the fact that for the polynomials used to define addition and multiplication in the Witt vector ring we have $S_n, P_n \in \mathbb{Z}[a_1, \dots, a_n, b_1, \dots, b_n]$ (see the proof of Dwork's lemma, (\Leftarrow)).

is that obvious?

If $S \subseteq \mathbb{N}$ is a truncation set, $n \in \mathbb{N}$, then

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

is again a truncation set.

Definition 1.12 (Verschiebung). Define

$$V_n: \mathbb{W}_{S/n} \rightarrow \mathbb{W}_S(A); V_n((a_d)_{d \in S/n})_m := \begin{cases} a_d, & \text{if } m = n \cdot d \\ 0, & \text{else} \end{cases}$$

which is called the *n -th Verschiebung map*. Furthermore define

$$\tilde{V}_n: A^{S/n} \rightarrow A^S; \tilde{V}_n((x_d)_{d \in S/n})_m := \begin{cases} n \cdot x_d, & \text{if } m = n \cdot d \\ 0, & \text{else} \end{cases}$$

Lemma 1.13 The Verschiebung map V_n is additive.

PROOF:

CLAIM.
$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\ \downarrow V_n & & \downarrow \tilde{V}_n \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S \end{array} \text{ commutes.}$$

Proof of claim. Let $a = (a_d)_{d \in S/n} \in \mathbb{W}_{S/n}(A)$. Let $m \in S$.

- case 1: $m \neq n \cdot d \forall d \in S$: Then $\tilde{V}_n(w(a))_m = (\tilde{V}_n(w_d)_{d \in S/n})_m = 0$ and

$$w(V_n(a))_m = \sum_{k \mid m, k=nd} k \cdot a_d^{m/k} = 0$$

because if there would be $k \mid m, k = nd$, this would mean that $m = k \cdot d' = n \cdot d \cdot d'$ for $d, d' \in S$ and then $d \cdot d' \mid m$ which is a contradiction to case 1.

- case 2: $m = n \cdot d$ for some $d \in S$:

$$\begin{aligned}
\widetilde{V}_n(w(a))_m &= (\widetilde{V}_n(w_d)_{d \in S/n})_m = n \cdot w_d = n \cdot \sum_{k|d} k \cdot a_k^{d/k} \\
w(V_n(a))_m &= w_m(V_n(a)) = \sum_{k|nd} k \cdot (V_n(a))_k^{nd/k} \\
&= \sum_{k|nd, k=nd_k} k \cdot a_{d_k}^{nd/k} = n \cdot \sum_{k|nd, k=nd_k} d_k \cdot a_{d_k}^{nd/nd_k} \\
&= n \cdot \sum_{k|nd, k=nd_k} d_k \cdot a_{d_k}^{d/d_k} = n \cdot \sum_{k|d} k \cdot a_k^{d/k}
\end{aligned}$$

because $nd_k \mid nd \iff d_k \mid d$ for $d_k, d, n \in \mathbb{N}$.

//

\widetilde{V}_n is obviously additive, so assume now that A is torsion-free. Then the ghost map is injective, so it is enough to check that $w(V_n(a+b)) = w(V_n(a) + V_n(b))$ for $a, b \in \mathbb{W}_{S/n}$. Since

$$\begin{array}{ccc}
\mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\
\downarrow V_n & & \downarrow \widetilde{V}_n \\
\mathbb{W}_S(A) & \xrightarrow{w} & A^S
\end{array}$$

commutes, we calculate:

$$\begin{aligned}
w(V_n(a+b)) &= \widetilde{V}_n(w(a+b)) = \widetilde{V}_n(w(a) + w(b)) \\
&= \widetilde{V}_n(w(a)) + \widetilde{V}_n(w(b)) = w(V_n(a)) + w(V_n(b)) = w(V_n(a) + V_n(b))
\end{aligned}$$

For the general case, choose a surjective ring homomorphism $g: A \rightarrow A'$, where A is torsion-free. Then the diagram

$$\begin{array}{ccc}
\mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}_{S/n}(g)} & \mathbb{W}_{S/n}(A') \\
\downarrow V_n & & \downarrow V_n \\
\mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(g)} & \mathbb{W}_S(A')
\end{array}$$

clearly commutes and since $\mathbb{W}_{S/n}(g)$ is surjective, there are $x, y \in \mathbb{W}_{S/n}(A)$ such that $\mathbb{W}_{S/n}(g)(x) = a$, $\mathbb{W}_{S/n}(g)(y) = b$. Then

$$\begin{aligned}
V_n(a+b) &= V_n(\mathbb{W}g(x)) = V_n(\mathbb{W}_{S/n}(g)(x+y)) = \mathbb{W}_S(g)(V_n(x+y)) \\
&= \mathbb{W}_S(g)(V_n(x)) + \mathbb{W}_S(g)(V_n(y)) = V_n(a) + V_n(b)
\end{aligned}$$

$\mathbb{W}g$ statt
 $\mathbb{W}_S(g)$

□

Next, we will introduce the *frobenius homomorphism*, which will play an important role in the proof of the comonadic structure of \mathbb{W} as well. For that, first define $\widetilde{F}_n: A^S \rightarrow A^{S/n}$ by $\widetilde{F}_n((x_m)_{m \in S}) = (x_{nm})_{m \in S/n}$.

|

Lemma 1.14 (Frobenius homomorphism) *There exists a unique natural ring homomorphism*

$$F_n: \mathbb{W}_S(A) \rightarrow \mathbb{W}_{S/n}(A)$$

such that the diagram

$$\begin{array}{ccc} \mathbb{W}_S(A) & \xrightarrow{w} & A^S \\ \downarrow F_n & & \downarrow \tilde{F}_n \\ \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \end{array}$$

commutes.

remark und definition haben andere font

We call F_n the *nth Frobenius homomorphism*. The commutativity of the diagram above is equivalent to commutativity of the following diagram for every $d \in S/n$:

$$\begin{array}{ccc} \mathbb{W}_S(A) & & \\ \downarrow F_n & \searrow w_{nd} & \\ \mathbb{W}_{S/n}(A) & \xrightarrow{w_d} & A \end{array}$$

Proof of Lemma 1.14. We construct F_n similar to the construction of the ring operations on $\mathbb{W}_S(A)$ using Lemma 1.5 again. So let A be the polynomial ring $\mathbb{Z}[a_n \mid n \in S]$, let $a = (a_n)_{n \in S}$ and let ϕ_p be the unique ring homomorphism $a_n \mapsto a_n^p$. Then Lemma 1.5 shows that the sequence $\tilde{F}_n(w(a)) \in A^{S/n}$ is in the image of a unique element

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

by the ghost map. (Indeed: we have

$$\begin{aligned} \phi_p((\tilde{F}_n(w(a)))_{m/p}) &= \phi_p((w_{nm/p})) = \sum_{k \mid nm/p} k \cdot a_k^{nm/k} \\ \tilde{F}_n(w(a))_m &= w_{nm} = \sum_{k \mid nm} k \cdot a_k^{nm/k} \end{aligned}$$

and both sums are congruent mod $p^{v_p(m)}$.) If A' is any ring and if $a' = (a'_n)_{n \in S}$ is a vector in $\mathbb{W}_S(A)$, then we define

$$F_n(a') := \mathbb{W}_{S/n}(g)(F_n(a))$$

where $g: A \rightarrow A'$ is the unique ringhomomorphism that maps a to a' . Now since \tilde{F}_n is clearly a ring homomorphism, we can argue similar as in the proof of Lemma 1.13 to show that F_n is a ring homomorphism. Finally, we show that F_n is natural. For that, let $f: A \rightarrow B$ be a ring homomorphism. Then we need to show that

$$\begin{array}{ccc} \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(f)} & \mathbb{W}_S(B) \\ \downarrow F_n & & \downarrow F_n \\ \mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}_{S/n}(f)} & \mathbb{W}_{S/n}(B) \end{array}$$

commutes, but it again suffices to show that it commutes after evaluating the ghost coordinates, i.e. we can

naturality

look at the following diagram:

$$\begin{array}{ccc}
 \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(f)} & \mathbb{W}_S(B) \\
 \downarrow F_n & & \downarrow F_n \\
 \mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}_S(f)} & \mathbb{W}_{S/n}(B) \\
 \downarrow w_d & & \downarrow w_d \\
 A & \xrightarrow{f} & B
 \end{array}$$

(Dotted lines and arrows labeled w_{nd} connect the top and bottom rows on the left and right sides.)

but by naturality of w_{nd} (1.8), the claim follows. \square

Note that for $n, m \in \mathbb{N}$ we have $(S/n)/m = S/nm$ by definition.

Lemma 1.15 *Let $n, m \in \mathbb{N}$. Then*

$$F_n \circ F_m = F_{nm}.$$

PROOF: We have $\tilde{F}_n \circ \tilde{F}_m = \tilde{F}_{nm}$, since

$$\tilde{F}_n(\tilde{F}_m(x_d)_{d \in S}) = \tilde{F}_n((x_{md})_{d \in S/m}) = (x_{nmd})_{d \in S/nm} = \tilde{F}_{nm}((x_d)_{d \in S}).$$

Now suppose that A is torsion-free, which means that the ghost map is injective. We have the following commutative diagram:

$$\begin{array}{ccc}
 \mathbb{W}_S(A) & \xrightarrow{w} & A^S \\
 \downarrow F_n & & \downarrow \tilde{F}_n \\
 \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\
 \downarrow F_m & & \downarrow \tilde{F}_m \\
 \mathbb{W}_{S/nm}(A) & \xrightarrow{w} & A^{S/nm}
 \end{array}$$

and then $w \circ (F_n \circ F_m) = \tilde{F}_n \circ \tilde{F}_m \circ w = \tilde{F}_{nm} \circ w = w \circ (F_{nm})$ which implies $F_n \circ F_m = F_{nm}$, since w is injective, hence a mono. Now, for the general case choose $g: A \rightarrow A'$ surjective, then we have the following commuting diagram:

$$\begin{array}{ccc}
 \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}(g)} & \mathbb{W}_S(A') \\
 \downarrow F_n & & \downarrow F'_n \\
 \mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}(g)} & \mathbb{W}_{S/n}(A') \\
 \downarrow F_m & & \downarrow F'_m \\
 \mathbb{W}_{S/nm}(A) & \xrightarrow{\mathbb{W}(g)} & \mathbb{W}_{S/nm}(A')
 \end{array}$$

and then $F'_n \circ F'_m \circ \mathbb{W}(g) = \mathbb{W}(g) \circ F_n \circ F_m = \mathbb{W}(g) \circ F_{nm} = F'_{nm} \circ \mathbb{W}(g)$ which implies $F'_n \circ F'_m = F'_{nm}$ since $\mathbb{W}(g)$ is surjective, hence an epi. \square

Lemma 1.16 $F_1 = \text{id}: \mathbb{W}_S(A) \rightarrow \mathbb{W}_S(A)$.

PROOF: clearly, $\tilde{F}_1 = \text{id}_{A^S}$, now if A is torsion-free, the claim follows, and in the general case we can argue as before. \square

Definition 1.17 (teichmüller representative). The *teichmüller representative* is the map

$$\tau: A \rightarrow \mathbb{W}_S(A)$$

defined by

$$(\tau(a))_m = \begin{cases} a, & \text{if } m = 1 \\ 0, & \text{else} \end{cases}$$

Lemma 1.18 *The teichmüller map is multiplicative.*

PROOF: The map $\tilde{\tau}: A \rightarrow A^S$; $(\tilde{\tau}(a))_n = a^n$ is multiplicative and there is a commutative diagram

$$\begin{array}{ccc} & A & \\ \tau \swarrow & & \searrow \tilde{\tau} \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S. \end{array}$$

Indeed, $w_n(\tau(a)) = w_n((a, 0, 0, \dots)) = a^n$ by definition of w_n . □

1.3 The comonad structure of Witt vectors

We will need the following lemma:

Lemma 1.19 *Let $m \in \mathbb{Z}$. If m is a non-zero divisor in A , then it is a non-zero divisor in $\mathbb{W}_S(A)$ as well.*

PROOF: We can assume that S is finite, since $\mathbb{W}_S(A)$ is the projective limit of all $\mathbb{W}_T(A)$ where T is a finite subset of S . We will prove the Lemma by induction over $|S|$. If $S = \emptyset$, the statement is trivial, so let $|S| = 1$, this means that $S = \{n\}$ for some $n \in \mathbb{N}$, but then $\mathbb{W}_n(A) \cong A$ via w . Now for the induction step, let $n \in S$ be maximal and let $T = S - \{n\}$. Then $S/n = \{1\}$ and therefore we have a short exact sequence

$$0 \longrightarrow A \xrightarrow{V_n} \mathbb{W}_S(A) \xrightarrow{R_T^S} \mathbb{W}_T(A) \longrightarrow 0$$

since V_n maps a to $(0, \dots, a)$ and R_T^S forgets the last coordinate. We can extend the sequence to the following commutative diagram:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A & \longrightarrow & \mathbb{W}_S(A) & \longrightarrow & \mathbb{W}_T(A) \longrightarrow 0 \\ & & \downarrow \cdot m & & \downarrow \cdot m & & \downarrow \cdot m \\ 0 & \longrightarrow & A & \longrightarrow & \mathbb{W}_S(A) & \longrightarrow & \mathbb{W}_T(A) \longrightarrow 0 \end{array}$$

Now m being a non-zero divisor is equivalent to $\cdot m$ being injective, but if the two outer vertical maps are injective, applying the snake lemma yields that the middle map has to be injective, too. □

Corollary 1.20 *If A is torsion-free, then $\mathbb{W}_S(A)$ is torsion-free as well.*

Definition 1.21. $\mathbb{W}(A) := \mathbb{W}_{\mathbb{N}}(A)$

p-typical Witt vectors, big Witt vectors

For the construction of a natural transformation $\mathbb{W}(A) \rightarrow \mathbb{W}(\mathbb{W}(A))$ we want to use Lemma 1.5 again. Hence we first show:

Lemma 1.22 *Let p be a prime number, let A be any ring. Then the ring homomorphism $F_p: \mathbb{W}(A) \rightarrow \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \pmod{pA}$.*

PROOF: Suppose first, that $A = \mathbb{Z}[a_1, a_2, \dots]$ and let $a = (a_1, a_2, \dots)$. Since

$$\begin{aligned} F_p(a) &\equiv a^p && \pmod{p\mathbb{W}(A)} \\ \iff F_p(a) - a^p &\equiv 0 && \pmod{p\mathbb{W}(A)} \\ \iff F_p(a) - a^p &\in p\mathbb{W}(A) \end{aligned}$$

it suffices to show there exists $b \in \mathbb{W}(A)$ such that $F_p(a) - a^p = p \cdot b$. By Lemma 1.19, this element is unique. Applying the ghost map gives us:

$$w_n(F_p(a) - a^p) = w_n(F_p(a)) - w_n(a)^p = w_{pn}(a) - w_n(a)^p = \sum_{d|pn} d \cdot a_d^{pn/d} - \left(\sum_{d|n} d \cdot a_d^{n/d} \right)^p$$

indeed

using Lemma 1.14. This is now congruent to 0 mod pA :

It follows that there exists $x = (x_n)_{n \in \mathbb{N}}$ such that

$$p \cdot x_n = w_n(F_p(a) - a^p) \iff x_n = \frac{1}{p} \cdot w_n(F_p(a) - a^p) \quad (1.3)$$

We want to show that $x = w(b)$ for some $b \in \mathbb{W}(A)$. Then

$$w(p \cdot b) = p \cdot w(b) = p \cdot x = w(F_p(a) - a^p)$$

which implies by injectivity of w that $p \cdot b = F_p(a) - a^p$. So we want to use Lemma 1.5 again. Consider the unique ring homomorphism $\phi_l: A \rightarrow A$ which maps a_n to a_n^l . It satisfies $\phi_l(f) \equiv f^l \pmod{lA}$. (indeed:). so by Lemma 1.5 it suffices to show:

indeed

$$x_n \equiv \phi_l(x_{n/l}) \pmod{l^{v_l(n)}A}$$

for all primes l , for all $n \in \mathbb{N}$ with $l \mid n$. But this is equivalent to:

$$w_n(F_p(a) - a^p) \equiv \phi_l(w_{n/l}(F_p(a) - a^p)) \pmod{l^{v_l(n)}A} \quad \forall l \neq p, \forall n \in \mathbb{N}$$

and

$$w_n(F_p(a) - a^p) \equiv \phi_p(w_{n/p}(F_p(a) - a^p)) \pmod{p^{v_p(n)+1}A} \quad \forall n \in p\mathbb{N}$$

(Using 1.3 we have for $l = p$:

$$\begin{aligned} x_n \equiv \phi_p(x_{n/p}) \pmod{p^{v_p(n)}A} &\iff p \cdot x_n \equiv p \cdot \phi_p(x_{n/p}) \pmod{p^{v_p(n)+1}A} \\ &\stackrel{1.3}{\iff} w_n(F_p(a) - a^p) \equiv \phi_p(w_{n/p}(F_p(a) - a^p)) \pmod{p^{v_p(n)+1}A} \end{aligned}$$

and for $l \neq p$:

$$\begin{aligned} x_n \equiv \phi_l(x_{n/l}) \pmod{l^{v_l(n)}A} &\iff p \cdot x_n \equiv p \cdot \phi_l(x_{n/l}) \pmod{l^{v_l(n)}A} \\ &\stackrel{1.3}{\iff} w_n(F_p(a) - a^p) \equiv \phi_l(w_{n/l}(F_p(a) - a^p)) \pmod{l^{v_l(n)}A.} \end{aligned}$$

For $l \neq p$, the statement follows directly from Lemma 1.5. So now let $l = p$, let $n \in p\mathbb{N}$. Then:

$$\begin{aligned} & w_n(F_p(a) - a^p) - \phi_p(w_{n/p}(F_p(a) - a^p)) \\ &= w_{pn}(a) - w_n(a)^p - \phi_p(w_n(a)) + \phi_p(w_{n/p}(a))^p \\ &= \sum_{d|pn} d \cdot a_d^{pn/d} - \left(\sum_{d|n} d \cdot a_d^{n/d} \right)^p - \sum_{d|n} d \cdot a_d^{np/d} + \left(\sum_{d|n/p} d \cdot a_d^{n/d} \right)^p \end{aligned}$$

using Lemma 1.14 for the first equality. Now if $d \mid pn, d \nmid n$, then $v_p(d) = v_p(n) + 1$, hence the first and third summand cancel each other out, and for the second and forth summand, using 1.2 and 1.4 again we have

$$\sum_{d|n} d \cdot a_d^{n/d} \equiv \sum_{d|n/p} d \cdot a_d^{n/d} \pmod{p^{v_p(n)}A} \implies \left(\sum_{d|n} d \cdot a_d^{n/d} \right)^p \equiv \left(\sum_{d|n/p} d \cdot a_d^{n/d} \right)^p \pmod{p^{v_p(n)+1}A}$$

which proves the claim. Now in the general case, let $a' \in \mathbb{W}(A')$. Then $F_p(a') = \mathbb{W}g(F_p(a)) = \mathbb{W}g(a^p + p \cdot r) = a'^p + p \cdot \mathbb{W}g(r)$ for some $r \in A$. \square

Proposition 1.23 *There exists a unique natural transformation*

$$\Delta: \mathbb{W}(A) \rightarrow \mathbb{W}(\mathbb{W}(A))$$

such that $w_n(\Delta(a)) = F_n(A)$ for all $a \in A, n \in \mathbb{N}$.

PROOF: As before, we can assume $A = \mathbb{Z}[a_n \mid n \in \mathbb{N}]$. By applying Corollary 1.20 twice, we get that the ghost map

$$w: \mathbb{W}(\mathbb{W}(A)) \rightarrow \mathbb{W}(A)^{\mathbb{N}}$$

is injective. Now by Lemma 1.22, $F_p: \mathbb{W}(A) \rightarrow \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \pmod{p\mathbb{W}(A)}$, hence we can use Lemma 1.5 again and just show that

$$F_n(a) \equiv F_p(F_{n/p}(a)) \pmod{p^{v_p(n)}A}$$

for all p prime, $n \in p\mathbb{N}$. But this immediately follows from Lemma 1.15, so there is a unique $\Delta(a) \in \mathbb{W}(\mathbb{W}(A))$ such that $w_n(\Delta(a)) = F_n(a)$. \square

Recall that by 1.8, $w_1: \mathbb{W}(A) \rightarrow A; (a_n)_{n \in \mathbb{N}} \mapsto a_1$ is a natural transformation $\mathbb{W} \Rightarrow \text{id}_{\text{CRing}}$.

Theorem 1.24 *The functor $\mathbb{W}(\cdot): \text{CRing} \rightarrow \text{CRing}$ together with the natural transformations $\Delta: \mathbb{W} \Rightarrow \mathbb{W}^2, w_1: \mathbb{W} \Rightarrow \text{id}_{\text{CRing}}$ form a comonad $(\mathbb{W}, w_1, \Delta)$.*

PROOF: By naturality of Δ , we can assume that A is torsion-free, because if A' is an arbitrary ring, to show the associativity axiom, we can choose $g: A \rightarrow A'$ surjective as always and then consider the following cube:

$$\begin{array}{ccccc} \mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A)) & & \\ \downarrow \Delta_A & \searrow \mathbb{W}(g) & \downarrow \Delta_{\mathbb{W}(A)} & \searrow \mathbb{W}(\mathbb{W}(g)) & \\ & \mathbb{W}(A') & \xrightarrow{\Delta_{A'}} & \mathbb{W}(\mathbb{W}(A')) & \\ & \downarrow \mathbb{W}(\Delta_A) & \downarrow \Delta_{\mathbb{W}(A')} & \downarrow \mathbb{W}(\mathbb{W}(g)) & \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\Delta_{A'}} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) & \xrightarrow{\mathbb{W}(\mathbb{W}(g))} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A'))) \\ & \downarrow \mathbb{W}(\mathbb{W}(g)) & \downarrow \mathbb{W}(\Delta_{A'}) & \downarrow \mathbb{W}(\mathbb{W}(g)) & \\ & \mathbb{W}(\mathbb{W}(A')) & \xrightarrow{\mathbb{W}(\Delta_{A'})} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A'))) & \end{array}$$

Since all the other faces of the cube commute and $\mathbb{W}(g)$ is surjective, the front face has to commute as well. By the same reasoning we get the unitality axiom in the general case.

$$\text{CLAIM.} \quad \begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A)) \\ \downarrow \Delta_A & \# & \downarrow \mathbb{W}(\Delta_A) \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\Delta_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) \end{array} \text{ commutes.}$$

Proof of claim. evaluating the ghost coordinates leads to:

$$\begin{array}{ccccc} & & F_A & & \\ & \swarrow & \cdots & \searrow & \\ \mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{w} & \mathbb{W}(A)^N \\ \downarrow \Delta_A & & \downarrow \mathbb{W}(\Delta_A) & & \downarrow \Delta_A^N \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\Delta_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) & \xrightarrow{w} & \mathbb{W}(\mathbb{W}(A))^N \\ & \swarrow & F_{\mathbb{W}A} & \searrow & \end{array}$$

which by Proposition 1.23 simplifies to

$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{F_A} & \mathbb{W}(A)^N \\ \downarrow \Delta_A & & \downarrow \Delta_A^N \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{F_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(A))^N \end{array}$$

now it suffices to show for an arbitrary n that the following diagram commutes:

$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{(F_n)_A} & \mathbb{W}(A) \\ \downarrow \Delta_A & & \downarrow \Delta_A \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{(F_n)_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(A)) \end{array}$$

evaluating the ghost coordinates again, keeping in mind that by 1.20 and 1.6, $w: \mathbb{W}(\mathbb{W}(A)) \rightarrow \mathbb{W}(A)^N$ is injective as well, we get

$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{(F_n)_A} & \mathbb{W}(A) \\ \downarrow \Delta_A & & \downarrow \Delta_A \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{(F_n)_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(A)) \\ \downarrow w & & \downarrow w \\ \mathbb{W}(A)^N & \xrightarrow{(\tilde{F}_n)_{\mathbb{W}(A)}} & \mathbb{W}(A)^N \end{array} \quad \begin{array}{c} \nearrow F_A \\ \nwarrow F_A \end{array}$$

using the fact that

$$\begin{array}{ccc}
 \mathbb{W}(\mathbb{W}(A)) & & \\
 \downarrow w & \searrow w_{nm} & \\
 \mathbb{W}(A)^N & \xrightarrow{(\tilde{F}_n)^{\mathbb{W}(A)}} & \mathbb{W}(A)^N
 \end{array}$$

commutes, we can simplify the situation to

$$\begin{array}{ccc}
 \mathbb{W}(A) & \xrightarrow{F_n} & \mathbb{W}(A) \\
 \downarrow \Delta_A & \searrow F_{nm} & \downarrow F_m \\
 \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{w_{nm}} & \mathbb{W}(A)
 \end{array}$$

which can again be simplified to

$$\begin{array}{ccc}
 \mathbb{W}(A) & \xrightarrow{F_n} & \mathbb{W}(A) \\
 & \searrow F_{nm} & \downarrow F_m \\
 & & \mathbb{W}(A)
 \end{array}$$

now this commutes by Lemma 1.15, hence we are finished. //

CLAIM.

$$\begin{array}{ccc}
 \mathbb{W}(A) & & \\
 \Delta_A \downarrow & \searrow \text{id}_{\mathbb{W}(A)} & \\
 \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\mathbb{W}(w_1)} & \mathbb{W}(A)
 \end{array}$$

commutes.

Proof of claim. evaluate the ghost coordinates:

$$\begin{array}{ccc}
 \mathbb{W}(A) & & \\
 \Delta_A \downarrow & \searrow \text{id}_{\mathbb{W}(A)} & \\
 \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\mathbb{W}(w_1)} & \mathbb{W}(A) \\
 \downarrow w & & \downarrow w \\
 \mathbb{W}(A)^N & \xrightarrow{w_1^N} & A^N
 \end{array}$$

(A dotted arrow labeled F connects $\mathbb{W}(A)$ to $\mathbb{W}(A)^N$ on the left, and a blue arrow labeled w connects $\mathbb{W}(A)$ to A^N on the right.)

we can then simplify to

$$\begin{array}{ccc}
 \mathbb{W}(A) & & \\
 F \downarrow & \searrow w & \\
 \mathbb{W}(A)^N & \xrightarrow{w_1^N} & A^N
 \end{array}$$

now it suffices to show for all n that

$$\begin{array}{ccc}
 \mathbb{W}(A) & & \\
 F_n \downarrow & \searrow w_n & \\
 \mathbb{W}(A) & \xrightarrow{w_1} & A
 \end{array}$$

commutes, which is true by Lemma 1.14. //

CLAIM.

$$\begin{array}{ccc}
 & \mathbb{W}(A) & \\
 \text{id}_{\mathbb{W}(A)} \swarrow & \downarrow \Delta_A & \\
 \mathbb{W}(\mathbb{W}(A)) & \xleftarrow{\varepsilon_{\mathbb{W}(A)}} & \mathbb{W}(A)
 \end{array} \text{ commutes.}$$

Proof of claim. Let $a \in \mathbb{W}(A)$.

$w_1(\Delta_A(a)) = F_1(a) = a$, since $F_1 = \text{id}_{\mathbb{W}(A)}$ by Lemma 1.16. //

This concludes the proof. \square

1.4 The Teichmüller map induces a morphism of comonads

Now consider the *teichmüller map* $\tau: A \rightarrow \mathbb{W}(A); a \mapsto (a, 0, 0, 0, \dots)$. It is multiplicative and preserves the unit, hence it extends uniquely to a ring homomorphism

$$\tau: \mathbb{Z}A \rightarrow \mathbb{W}(A)$$

Theorem 1.25 $\tau: \mathbb{Z}A \rightarrow \mathbb{W}(A)$ is a morphism of comonads.

PROOF: We need to show that the following diagrams commute:

$$\begin{array}{ccc}
 \mathbb{Z}A & \xrightarrow{\tau_A} & \mathbb{W}(A) \\
 & \searrow \varepsilon_A & \downarrow (w_1)_A \\
 & & A
 \end{array}
 \qquad
 \begin{array}{ccc}
 \mathbb{Z}A & \xrightarrow{\omega_A} & \mathbb{Z}\mathbb{Z}A \\
 \downarrow \tau_A & & \downarrow \tau \otimes \tau \\
 \mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A))
 \end{array}$$

By the universal property of $\mathbb{Z}A$, it suffices to consider elements of the form $[a]$ for $a \in A$. For the first diagram: $w_1(\tau([a])) = a = \varepsilon([a])$. For the second diagram, arguing as above, it suffices to show commutativity after evaluating the ghost coordinates:

$$\begin{array}{ccc}
 \mathbb{Z}A & \xrightarrow{\omega_A} & \mathbb{Z}\mathbb{Z}A \\
 \downarrow \tau_A & & \downarrow \tau \otimes \tau \\
 \mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A)) \\
 & \searrow F_n & \downarrow w_n \\
 & & \mathbb{W}(A)
 \end{array}$$

Note that $F_n(\tau(a)) = \tau(a^n)$ since evaluating the ghost coordinates shows that the equation holds if A is torsion-free, and hence, in general. Using this, we see that $w_n(\tau \otimes \tau(\omega([a]))) = w_n(\tau \otimes \tau([a])) = w_n(((a, 0, \dots), 0, \dots)) = (a, 0, \dots)^n = (a^n, 0, \dots)$ and $F_n(\tau([a])) = F_n((a, 0, \dots)) = (a^n, 0, \dots)$

\square