1 Witt vectors

1.1 Construction of the witt vectors

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

Definition 1.1 (p-adic valuation). $v_p \colon \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ is defined by

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

Definition 1.2 (truncation set). Let $\mathbb{N}$ be the set of positive integers and let $S \subseteq \mathbb{N}$ be a subset with the property that $\forall n \in \mathbb{N}$: if d is a divisor of n, then $d \in S$. We then say that S is a *truncation set.*

As a set, we define the *big Witt ring* $\mathbb{W}_S(A)$ to be A^S, we will give it a unique ring structure, such that the *ghost map* is a ring homomorphism. Furthermore, if $f \colon A \to B$ is a ring homomorphism, we define $\mathbb{W}_S(f) \colon \mathbb{W}_S(A) \to \mathbb{W}_S(B)$ 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 1.3 (ghost map). We define $w \colon \mathbb{W}_S(A) \to A^S$ by $(a_n)_{n\in S} \mapsto (w_n)_{n\in S}$ where

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

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

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

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:

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

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 $\phi_p : A \to A$ 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 $w : \mathbb{W}_S(A) \to A^S$.*

(ii) *For every prime number p and every $n \in S$ with $v_p(n) \geqslant 1$,*

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

Proof: ($\Rightarrow$) 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:

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

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

$$
\begin{aligned}
\sum_{d \mid n/p} d \cdot \phi(a_d^{n/pd}) &\equiv \sum_{d \mid n/p} d \cdot a_d^{n/d} && \text{mod } p^{v_p(n)}A && (1.1) \\
&\equiv \sum_{d \mid n} d \cdot a_d^{n/d} && \text{mod } p^{v_p(n)}A && (1.2)
\end{aligned}
$$

so we get

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

Proof of (1.1). First, note that

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

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 $\phi_p(a_d^N) \equiv a_d^{p \cdot N} \bmod pA$, so we can calculate:

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

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

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

gives us

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

But

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

so it follows that for every d

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

which implies (1). □

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 $d \equiv 0 \bmod p^{v_p(n)}A$. □

proof-umgebung

($\Leftarrow$) Let $(x_n)_{n \in S}$ be a sequence such that $x_n \equiv \phi_p(x_{n/p}) \quad \mathit{mod}\ p^{v_p(n)}A$ $\forall p$ prime, $n \in S, v_p(n) \geqslant 1$. 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 $p \mid n$:

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

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

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

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*

$$w : \mathbb{W}_S(A) \longrightarrow A^s$$

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

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

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).

is is though?

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 $p \mid n$:

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

But plugging in the definitions, we see that

$$\begin{aligned}
w_n(a) + w_n(b) &= \sum_{d|n} d \cdot a_d^{n/d} + \sum_{d|n} d \cdot b_d^{n/d} \\
&= \sum_{d|n} d \cdot (a_d + b_d)^{n/d}, \\
\phi_p(w_{n/p}(a) + w_{n/p}(b)) &= \phi_p\left(\sum_{d|n/p} d \cdot a_d^{n/pd} + \sum_{d|n/p} d \cdot b_d^{n/pd}\right) = \phi_p\left(\sum_{d|n/p} d \cdot (a_d + b_d)^{n/pd}\right) \\
&= \sum_{d|n/p} d \cdot (a_d + b_d)^{n/d}
\end{aligned}$$

and those two sums are congruent modulo $p^{v_p(n)}A$, see the proof of (1.2). For the multiplication, we compute:

$$\begin{aligned}
w_n(a) \cdot w_n(b) &= \left(\sum_{d|n} d \cdot a_d^{n/d}\right) \cdot \left(\sum_{d|n} d \cdot b_d^{n/d}\right) \\
&= \sum_{d_1|n} \sum_{d_2|n} d_1 \cdot d_2 \cdot a_{d_1}^{n/d_1} \cdot b_{d_2}^{n/d_2}, \\
\phi_p(w_{n/p}(a) \cdot w_{n/p}(b)) &= \phi_p\left(\left(\sum_{d|n/p} d \cdot a_d^{n/pd}\right) \cdot \left(\sum_{d|n/p} d \cdot b_d^{n/pd}\right)\right) = \phi_p\left(\sum_{d_1|n/p} \sum_{d_2|n/p} d_1 \cdot d_2 \cdot a_{d_1}^{n/pd_1} \cdot b_{d_2}^{n/pd_2}\right) \\
&= \sum_{d_1|n/p} \sum_{d_2|n/p} d_1 \cdot d_2 \cdot a_{d_1}^{n/d_1} \cdot b_{d_2}^{n/d_2}
\end{aligned}$$

and by similar reasoning as before, the two sums are congruent. The proof for $-w(a)$ is analogous. // is this computation correct?

It follows there are sequences $s = (s_n)_{n\in S}$, $p = (p_n)_{n\in S}$ and $\iota = (\iota_n)_{n\in S}$ of polynomials such that

$$w(s) = w(a) + w(b), \;\; w(p) = w(a) \cdot w(b), \;\; w(\iota) = -w(a)$$

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

$$\begin{aligned}
f \colon A &\longrightarrow A'; \\
a_n &\longmapsto a'_n, \\
b_n &\longmapsto b'_n
\end{aligned}$$

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:

$$\begin{aligned}
a' + b' &:= \mathbb{W}_S(f)(s) \\
a' \cdot b' &:= \mathbb{W}_S(f)(p) \\
-a' &:= \mathbb{W}_S(f)(\iota)
\end{aligned}$$

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 //

Claim. *$w \colon \mathbb{W}_S(A) \to A^S$ is a natural ring homomorphism.*

finish

□

Corollary 1.8 *$w_n \colon \mathbb{W}_S(A) \longrightarrow A$ 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: Suppose first that A is torsion-free. 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^S. In the general case: □

general case

Proposition 1.10 *$\mathbb{W}_S(\_)$ is a functor* **CRing** $\longrightarrow$ **CRing**.

PROOF: $\mathbb{W}_S(\mathrm{id}) = \mathrm{id}$ and $\mathbb{W}_S(g \circ f) = \mathbb{W}_S(g) \circ W_S(f)$ 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 $f \colon A \longrightarrow B$, $\mathbb{W}_S(f) \colon W_S(A) \longrightarrow W_S(B)$ 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

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

□

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*

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

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

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

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

$$\widetilde{V_n} \colon A^{S/n} \to A^S;\; \widetilde{V_n}((x_d)_{d\in S/n})_m := \begin{cases} n \cdot x_d, & \text{if } m = n \cdot d \\ 0, & \text{else} \end{cases}$$

Lemma 1.13 *The Verschiebung map V_n is additive.*

Proof:

Claim.
$$\begin{tikzcd} \mathbb{W}_{S/n}(A) \arrow[r, "w"] \arrow[d, "V_n"] & A^{S/n} \arrow[d, "\widetilde{V_n}"] \\ \mathbb{W}_S(A) \arrow[r, "w"] & A^S \end{tikzcd}$$
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 $\widetilde{V_n}(w(a))_m = (\widetilde{V_n}(w_d)_{d\in S/n})_m = 0$ and

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

  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 $d \in S$:

  $$\widetilde{V_n}(w(a))_m = (\widetilde{V_n}(w_d)_{d\in S/n})_m = n \cdot w_d = n \cdot \sum_{k|d} k \cdot a_k^{d/k}.$$

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

  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. □ finish den bums

Define $\widetilde{F}_n \colon A^S \to A^{S/n}$ by $\widetilde{F}_n((x_m)_{m\in S})_d = x_{nd}$.

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

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

such that the diagram

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

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 $d \in S/n$:

$$\begin{tikzcd} \mathbb{W}_S(A) \arrow[d, "F_n"] \arrow[dr, "w_{nd}"] & \\ \mathbb{W}_{S/n}(A) \arrow[r, "w_d"'] & A \end{tikzcd}$$

Proof of Lemma 1.14. We construct F_n similar to the construction of the ring operations on $\mathbb{W}_S A(A)$ 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 $\widetilde{F}_n(w(a)) \in A^{S/n}$ 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

$$\phi_p((\widetilde{F}_n(w(a)))_{m/p}) = \phi_p((w_{nm/p})) = \sum_{k|nm/p} k \cdot a_k^{nm/k}$$
$$\widetilde{F}_n(w(a))_m = w_{nm} = \sum_{k|nm} k \cdot a_k^{nm/k}$$

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

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

where $g \colon A \to A'$ is the unique ringhomomorphism that maps a to a'. Now since $\widetilde{F}_n$ 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 $f \colon A \to B$ be a ring homomorphism. Then we need to show that

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

why?

commutes, but it again suffices to show that it commutes after evaluating the ghost coordinates, i.e. we can look at the following diagram:

$$\begin{tikzcd}
\mathbb{W}_S(A) \arrow[r, "\mathbb{W}_S(F)"] \arrow[d, "F_n"] \arrow[dd, bend right, dotted, "w_{nd}"'] & \mathbb{W}_S(B) \arrow[d, "F_n"] \arrow[dd, bend left, dotted, "w_{nd}"] \\
\mathbb{W}_{S/n}(A) \arrow[r, "\mathbb{W}_S(f)"] \arrow[d, dotted, "w_d"] & \mathbb{W}_{S/n}(B) \arrow[d, "w_d"] \\
A \arrow[r, dotted, "f"] & B
\end{tikzcd}$$

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

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 $\widetilde{F}_n \circ \widetilde{F}_m = \widetilde{F}_{nm}$, since

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

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

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

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

$$\begin{tikzcd}
\mathbb{W}_S(A) \arrow[r, two heads, "\mathbb{W}(g)"] \arrow[d, "F_n"] & \mathbb{W}_S(A') \arrow[d, "F'_n"] \\
\mathbb{W}_{S/n}(A) \arrow[r, two heads, "\mathbb{W}(g)"] \arrow[d, "F_m"] & \mathbb{W}_{S/n} \arrow[d, "F'_m"] \\
\mathbb{W}_{S/nm}(A) \arrow[r, two heads, "\mathbb{W}(g)"] & \mathbb{W}_{S/nm}(A')
\end{tikzcd}$$

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 $F'_n \circ F'_m$ since $\mathbb{W}(g)$ is surjective, hence an epi. □

Lemma 1.16 $F_1 = \mathrm{id}\colon W_S(A) \to W_S(A)$.

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

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

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

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 $\widetilde{\tau}\colon A \to A^S$; $(\widetilde{\tau}(a))_n = a^n$ is multiplicative and there is a commutative diagram

$$\begin{tikzcd} & A \arrow[dl, "\tau"'] \arrow[dr, "\widetilde{\tau}"] & \\ \mathbb{W}_S(A) \arrow[rr, "w"] & & A^S. \end{tikzcd}$$

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 $\mathbb{W}_n(A) \cong \mathbb{W}_1(A) = A$ via V_n. 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

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

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

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\cdot m"] & \mathbb{W}_S(A) \arrow[r] \arrow[d, "\cdot m"] & \mathbb{W}_T(A) \arrow[r] \arrow[d, "\cdot m"] & 0 \\ 0 \arrow[r] & A \arrow[r] & \mathbb{W}_S(A) \arrow[r] & \mathbb{W}_T(A) \arrow[r] & 0 \end{tikzcd}$$

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. $\mathbb{W}(A) \coloneqq \mathbb{W}_{\mathbb{N}}(A)$

For the construction of a natural transformation $\mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(A))$ 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 $F_p\colon \mathbb{W}(A) \longrightarrow \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \bmod pA$.*

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

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

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:

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

using Lemma 1.14. This is now congruent to 0 mod pA: indeed
It follows that there exists $x = (x_n)_{n \in \mathbb{N}}$ such that

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

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 $\phi_l\colon A \longrightarrow A$ which maps a_n to a_n^l. It satisfies $\phi_l(f) \equiv f^l \bmod lA$. (indeed:). indeed
so by Lemma 1.5 it suffices to show:

$$x_n \equiv \phi_l(x_{n/l}) \qquad \bmod l^{v_l(n)}$$

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

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

and

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

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

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

and for $l \neq p$:

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

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

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

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

$$\sum_{d \mid n} d \cdot a_d^{n/d} \equiv \sum_{d \mid n/p} d \cdot a_d^{n/d} \bmod p^{v_p(n)} A \implies (\sum_{d \mid n} d \cdot a_d^{n/d})^p \equiv (\sum_{d \mid n/p} d \cdot a_d^{n/d})^p \bmod p^{v_p(n)+1} A$$

which proves the claim. □

Proposition 1.23 *There exists a unique natural transformation*

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

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

?

Proof: First, by naturality, we may and will assume that A is torsion-free. indeed: □

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

Theorem 1.24 *The functor $\mathbb{W}(\_) \colon \mathbf{CRing} \to \mathbf{CRing}$ together with the natural transformations $\Delta \colon \mathbb{W} \Rightarrow \mathbb{W}^2$, $w_1 \colon \mathbb{W} \Rightarrow \mathrm{id}_{\mathbf{CRing}}$ form a comonad $(\mathbb{W}, w_1, \Delta)$.*

Proof:

Claim.
$$\begin{tikzcd} \mathbb{W}(A) \arrow[r, "\Delta_A"] \arrow[d, "\Delta_A"] \arrow[dr, phantom, "\#"] & \mathbb{W}(\mathbb{W}(A)) \arrow[d, "\mathbb{W}(\Delta_A)"] \\ \mathbb{W}(\mathbb{W}(A)) \arrow[r, "\Delta_{\mathbb{W}(A)}"] & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) \end{tikzcd}$$
commutes.

Proof of claim. evaluating the ghost coordinates leads to:

$$\begin{tikzcd} \mathbb{W}(A) \arrow[r, "\Delta_A"] \arrow[d, "\Delta_A"] \arrow[rr, bend left, dotted, "F_A"] & \mathbb{W}(\mathbb{W}(A)) \arrow[r, dotted, "w"] \arrow[d, "\mathbb{W}(\Delta_A)"] & \mathbb{W}(A)^{\mathbb{N}} \arrow[d, dotted, "\Delta_A^{\mathbb{N}}"] \\ \mathbb{W}(\mathbb{W}(A)) \arrow[r, "\Delta_{\mathbb{W}(A)}"] \arrow[rr, bend right, dotted, "F_{\mathbb{W}_A}"'] & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) \arrow[r, blue, "w"] & \mathbb{W}(\mathbb{W}(A))^{\mathbb{N}} \end{tikzcd}$$

which by Proposition 1.23 simplifies to

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "F_A"] \arrow[d, "\Delta_A"] & \mathbb{W}(A)^{\mathbb{N}} \arrow[d, "\Delta_A^{\mathbb{N}}"] \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "F_{\mathbb{W}(A)}"] & \mathbb{W}(\mathbb{W}(A))^{\mathbb{N}}
\end{tikzcd}$$

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

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "F_{n_A}"] \arrow[d, "\Delta_A"] & \mathbb{W}(A) \arrow[d, "\Delta_A"] \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "F_{n_{\mathbb{W}(A)}}"] & \mathbb{W}(\mathbb{W}(A))
\end{tikzcd}$$

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

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "F_{n_A}"] \arrow[d, "\Delta_A"] & \mathbb{W}(A) \arrow[d, "\Delta_A"] \arrow[dd, dotted, bend left, "F_A"] \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "F_{n_{\mathbb{W}(A)}}"] \arrow[d, dotted, "w"] & \mathbb{W}(\mathbb{W}(A)) \arrow[d, "w"] \\
\mathbb{W}(A)^{\mathbb{N}} \arrow[r, dotted, "(\widetilde{F}_n)_{\mathbb{W}(A)}"] & \mathbb{W}(A)^{\mathbb{N}}
\end{tikzcd}$$

using the fact that
$$\begin{tikzcd}
\mathbb{W}(\mathbb{W}(A)) \arrow[d, dotted, "w"] \arrow[dr, dotted, "w_{nm}"] & \\
\mathbb{W}(A)^{\mathbb{N}} \arrow[r, dotted, "(\widetilde{F}_n)_{\mathbb{W}(A)}"] & \mathbb{W}(A)^{\mathbb{N}}
\end{tikzcd}$$
commutes, we can simplify the situation to

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "F_n"] \arrow[d, "\Delta_A"] \arrow[dr, dotted, "F_{nm}"] & \mathbb{W}(A) \arrow[d, "F_m"] \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "w_{nm}"] & \mathbb{W}(A)
\end{tikzcd}$$

which can again be simplified to

$$\begin{tikzcd}
\mathbb{W}(A) \arrow[r, "F_n"] \arrow[dr, "F_{nm}"'] & \mathbb{W}(A) \arrow[d, "F_m"] \\
 & \mathbb{W}(A)
\end{tikzcd}$$

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

Claim.
$$\begin{tikzcd}
\mathbb{W}(A) \arrow[d, "\Delta_A"'] \arrow[dr, "\mathrm{id}_{\mathbb{W}(A)}"] & \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "\mathbb{W}(w_1)"'] & \mathbb{W}(A)
\end{tikzcd}$$
commutes.

Proof of claim. evaluate the ghost coordinates:

$$
\begin{tikzcd}
\mathbb{W}(A) \arrow[d, "\Delta_A"'] \arrow[dr, "\mathrm{id}_{\mathbb{W}(A)}"] \arrow[dd, dotted, bend right, "F"'] & \\
\mathbb{W}(\mathbb{W}(A)) \arrow[r, "\mathbb{W}(w_1)"'] \arrow[d, dotted, "w"] & \mathbb{W}(A) \arrow[d, "w"] \\
\mathbb{W}(A)^{\mathbb{N}} \arrow[r, dotted, "w_1^{\mathbb{N}}"] & A^{\mathbb{N}}
\end{tikzcd}
$$

we can then simplify to

$$
\begin{tikzcd}
\mathbb{W}(A) \arrow[d, "F"'] \arrow[dr, "w"] & \\
\mathbb{W}(A)^{\mathbb{N}} \arrow[r, "w_1^{\mathbb{N}}"'] & A^{\mathbb{N}}
\end{tikzcd}
$$

now it suffices to show for all n that

$$
\begin{tikzcd}
\mathbb{W}(A) \arrow[d, "F_n"'] \arrow[dr, "w_n"] & \\
\mathbb{W}(A) \arrow[r, "w_1"'] & A
\end{tikzcd}
$$

commutes, which is true by Lemma 1.14.

⫽

Claim.
$$
\begin{tikzcd}
 & \mathbb{W}(A) \arrow[dl, "\mathrm{id}_{\mathbb{W}(A)}"'] \arrow[d, "\Delta_A"] \\
\mathbb{W}(\mathbb{W}(A)) & \mathbb{W}(A) \arrow[l, "\varepsilon_{\mathbb{W}(A)}"]
\end{tikzcd}
$$
commutes.

Proof of claim. Let $a \in \mathbb{W}(A)$.
$\varepsilon(\Delta_A(a)) = w_1(\Delta_A(a)) = F_1(a) = a$, since $F_1 = \mathrm{id}_{\mathbb{W}(A)}$ by Lemma 1.16. ⫽

This concludes the proof. □

1.4 The Teichmüller map induces a morphism of comonads

maybe ins Kapitel Comonaden als Beispiel schieben

We now consider another example of a comonad; the *free monoid comonad.*

Definition 1.25 (monoid ring). Let R be a ring and let G be a monoid. The *monoid ring* of G over R, denoted $R[G]$ or RG is the set of formal finite sums $\sum_{g \in G} r_g \cdot g$ with addition and multiplication defined by:

$$
\begin{aligned}
\sum_{g\in G} r_g \cdot g + \sum_{g \in G} s_g \cdot g &:= \sum_{g \in G} (r_g + s_g) \cdot g \\
\sum_{g\in G} r_g \cdot g \cdot \sum_{g \in G} s_g \cdot g &:= \sum_{g \in G} \Big(\sum_{k \cdot l = g} r_k \cdot s_l \Big) \cdot g
\end{aligned}
$$

Example 1. $R = \mathbb{R}, G = \{x^n \mid n \in \mathbb{N}\} \implies RG = \mathbb{R}[X]$

Remark 1.26. $R[G]$ together with the ring homomorphism $\alpha\colon R \to R[G]; r \mapsto r \cdot 1$ and the monoid homomorphism $\beta\colon G \to R[G]; g \mapsto 1 \cdot g$ enjoys the following universal property:

$$\alpha(r) \cdot \beta(g) = \beta(g) \cdot \alpha(r) \quad \forall r \in R, g \in G$$

and if (S, α', β') is another such triple with $\alpha'(r) \cdot \beta'(g) = \beta'(g) \cdot \alpha'(r) \quad \forall r \in R, g \in G$, there is a unique monoid homomorphism $\gamma \colon R[G] \to S$ such that the following diagram commutes:

$$\begin{tikzcd} & S & \\ R \arrow[ur, "\alpha'"] \arrow[r, "\alpha"'] & R[G] \arrow[u, dotted, "\gamma"] & G \arrow[ul, "\beta'"'] \arrow[l, "\beta"] \end{tikzcd}$$

Here, γ is defined by $\sum_{g\in G} r_g \cdot g \mapsto \sum_{g\in G} \alpha'(r_g) \cdot \beta'(g)$.

Example 2. Let S be a ring, G be a monoid. Since there is a unique ring homomorphism $\mathbb{Z} \to S$, each monoid homomorphism $G \to S$ induces a unique ring homomorphism $\mathbb{Z}G \to S$ such that the following commutes:

$$\begin{tikzcd} G \arrow[r] \arrow[dr] & S \\ & \mathbb{Z}G \arrow[u] \end{tikzcd}$$

Now if H is another monoid and $f \colon G \to H$ a monoid morphism, $G \xrightarrow{f} H \to \mathbb{Z}H$ is a monoid homomorphism, hence it extends uniquely to $f \colon \mathbb{Z}G \to \mathbb{Z}H$, $\sum_{g\in G} r_g \cdot g \mapsto \sum_{g\in G} r_g \cdot f(g)$.
In this way, the free monoid ring construction over $\mathbb{Z}$ is functorial.

Let $G \colon$ **CRing** $\to$ **CMon**, $(R, +, \cdot) \mapsto (R, \cdot)$ be the forgetful functor and let $F \colon$ **CMon** $\to$ **CRing** be the *free monoid ring functor*, $G \mapsto \mathbb{Z}G$.

Proposition 1.27 *There is an adjoint situation* $\begin{tikzcd} \mathbf{CMon} \arrow[r, bend left, "F"] \arrow[r, phantom, "\perp"] & \mathbf{CRing} \arrow[l, bend left, "G"] \end{tikzcd}$

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

$$\tau \colon \mathbb{Z}A \to \mathbb{W}(A)$$

Theorem 1.28 $\tau \colon \mathbb{Z}A \to \mathbb{W}(A)$ *is a morphism of comonads.*