1 Witt vectors

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). $v_p : \mathbb{Z} \to \mathbb{N} \cup \{\infty\}$ 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.

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:*

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

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

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

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

$$\begin{aligned} \sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) &\overset{(1)}{\equiv} \sum_{d|n/p} d \cdot a_d^{n/d} && \text{mod } p^{v_p(n)}A \\ &\overset{(2)}{\equiv} \sum_{d|n} d \cdot a_d^{n/d} && \text{mod } p^{v_p(n)}A \end{aligned}$$

so we get

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

Proof of (1). First, note that

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

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

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

using Lemma 1.4 for the last congruence. Now (a) 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

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

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

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

which implies (1). □

Proof of (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 $d \equiv 0$ mod $p^{v_p(n)}A$. □

($\Leftarrow$) Let $(x_n)_{n \in S}$ be a sequence such that $x_n \equiv \phi_p(x_{n/p}) \qquad \textit{mod } p^{v_p(n)}A$ $\forall p$ 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: proof-umgebung

$$a_1 := x_1$$

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 $p \mid n$:

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

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

$$\begin{aligned} \sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) &\overset{(2)}{\equiv} \sum_{d|n/p} d \cdot a_d^{n/d} \qquad \text{mod } p^{v_p(n)}A \\ &\overset{(3)}{\equiv} \sum_{d|n} d \cdot a_d^{n/d} \qquad \text{mod } p^{v_p(n)}A \\ &\equiv \sum_{d|n, d \neq n} d \cdot a_d^{n/d} \qquad \text{mod } p^{v_p(n)}A \end{aligned}$$

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*

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

is a natural transformation of functors from rings to rings.

Proof: □

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

Proposition 1.9 $\mathbb{W}_S$ *is a functor* **CRing** → **CRing**.

The Verschiebung, Frobenius and Teichmüller maps

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

Definition 1.10 (Restriction map). If $T \subseteq S$ are two truncation sets, the *restriction from S to T*

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

is a natural ring homomorphism.

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 1.11 (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 1.12 *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. //

□

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

Lemma 1.13 (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 1.13. easy □

Lemma 1.14 *Let $n, m \in \mathbb{N}$. Then*

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

Proof: □

Definition 1.15 (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 1.16 *The teichmüller map is multiplicative.*

Proof: The map $\widetilde{\tau}\colon A \to A^S$; $(\widetilde{\tau})_n = a^n$ 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.

□

The comonad structure of witt vectors

We will need the following lemma:

Lemma 1.17 *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:

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

which we can extend to the following commutative diagram:

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

finish

□

Corollary 1.18 *If A is torsion-free, then $\mathbb{W}_S(A)$ is torsion-free as well.*

Definition 1.19. $\mathbb{W}(A) := \mathbb{W}_{\mathbb{N}}(A)$

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 1.20 *Let p be a prime number, let A be any ring. Then the ring homomorphism $F_p\colon \mathbb{W}(A) \to \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \bmod pA$.*

Proposition 1.21 *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* $a \in A, n \in \mathbb{N}$.

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 1.22 *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:

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

which by 1.21 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 1.18 and 1.6, $w \colon \mathbb{W}(\mathbb{W}(A)) \to \mathbb{W}(A)^{\mathbb{N}}$ is injective as well, we get

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

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 ???, 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:

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

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 ??? ($\varepsilon = w_1$).

//

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 $F_1 = \mathrm{id}_{\mathbb{W}(A)}$. //

This concludes the proof. □

The Teichmüller map induces a morphism of comonads

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

maybe ins Kapitel Comonaden als Beispiel schieben

Definition 1.23 (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:

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

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

Remark 1.24. $R[G]$ 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 $G\colon \mathbf{CRing} \to \mathbf{CMon}$, $(R, +, \cdot) \mapsto (R, \cdot)$ be the forgetful functor and let $F\colon \mathbf{CMon} \to \mathbf{CRing}$ be the *free monoid ring functor*, $G \mapsto \mathbb{Z}G$.

Proposition 1.25 *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 1.26 $\tau\colon \mathbb{Z}A \to \mathbb{W}(A)$ *is a morphism of comonads.*