1 Adjoint situations

einleitender Satz

Moreover, adjunctions provide us with many (technically even all) examples of monads and comonads, as we will later see.

Proposition 1.1 *Given two functors* $\mathbf{B} \underset{G}{\overset{F}{\rightleftarrows}} \mathbf{A}$ *the following are equivalent:*

(a) *There are natural transformations* $\eta\colon \mathrm{id}_B \Rightarrow GF$ *and* $\varepsilon\colon FG \Rightarrow \mathrm{id}_A$ *such that for all objects* a *of* $\mathbf{A}$, b *of* $\mathbf{B}$ *the following two diagrams commute:*

$$\begin{array}{ccc} F(b) & \xrightarrow{F(\eta_b)} & FGF(b) \\ & \searrow^{\mathrm{id}_{F(b)}} & \downarrow{\scriptstyle \varepsilon_{F(b)}} \\ & & F(b) \end{array} \qquad \begin{array}{ccc} G(a) & \xrightarrow{\eta_{G(a)}} & GFG(a) \\ & \searrow^{id_{G(a)}} & \downarrow{\scriptstyle G(\varepsilon_a)} \\ & & G(a) \end{array} \qquad \text{(triangle identity)}$$

(b) *There is a bijection*

$$\phi_{a,b}\colon \mathrm{Hom}_{\mathbf{A}}(F(b), a) \cong \mathrm{Hom}_{\mathbf{B}}(b, G(a))$$

for all objects a *of* $\mathbf{A}$ *and* b *of* $\mathbf{B}$*, which is natural in* a *and* b*.*

Naturality here means that for $p\colon a \to a'$ and for $q\colon b \to b'$ the following two diagrams commute:

$$\begin{array}{ccc} \mathrm{Hom}_{\mathbf{A}}(F(b), a) & \xrightarrow{\phi_{a,b}} & \mathrm{Hom}_{\mathbf{B}}(b, G(a)) \\ \downarrow{\scriptstyle p\circ -} & & \downarrow{\scriptstyle G(p)\circ -} \\ \mathrm{Hom}_{\mathbf{A}}(F(b), a') & \xrightarrow{\phi_{a',b}} & \mathrm{Hom}_{\mathbf{B}}(b, G(a')) \end{array} \qquad \begin{array}{ccc} \mathrm{Hom}_{\mathbf{A}}(F(b'), a) & \xrightarrow{\phi_{a,b'}} & \mathrm{Hom}_{\mathbf{B}}(b', G(a)) \\ \downarrow{\scriptstyle -\circ F(q)} & & \downarrow{\scriptstyle -\circ q} \\ \mathrm{Hom}_{\mathbf{A}}(F(b), a) & \xrightarrow{\phi_{a,b}} & \mathrm{Hom}_{\mathbf{B}}(b, G(a)) \end{array}$$

Proof: $(a) \implies (b)$:
define

$$\phi_{a,b}\colon \mathrm{Hom}_{\mathbf{A}}(F(b), a) \to \mathrm{Hom}_{\mathbf{B}}(b, G(a)) \quad \text{by} \quad \phi_{a,b}(g) = G(g) \circ \eta_b\colon b \to G(a)$$

$$\psi_{a,b}\colon \mathrm{Hom}_{\mathbf{B}}(b, G(a)) \to \mathrm{Hom}_{\mathbf{A}}(F(b), a) \quad \text{by} \quad \psi_{a,b}(f) = \varepsilon_a \circ F(f)\colon F(b) \to a$$

for $g\colon F(b) \to a$, $f\colon b \to G(a)$.

Claim 1. $\phi \circ \psi = \mathrm{id}$

Proof of claim 1. Let $f\colon b \to G(a)$.

$$\begin{aligned} \phi(\psi(f)) &= \phi(\varepsilon_a \circ F(f)) && \text{(Definition of } \psi) \\ &= G(\varepsilon_a \circ F(f)) \circ \eta_b && \text{(Definition of } \phi) \\ &= G(\varepsilon_a) \circ G(F(f)) \circ \eta_b && \text{(Functoriality of } G) \\ &= G(\varepsilon_a) \circ \eta_{G(a)} \circ f && \text{(Naturality of } \eta) \\ &= \mathrm{id}_{G(a)} \circ f = f && \text{(right triangle identity)} \end{aligned}$$

//

Claim 2. $\psi \circ \phi = \mathrm{id}$

Proof of claim 2.

$$\begin{aligned}
\psi(\phi(g)) &= \psi(G(g) \circ \eta_b) && \text{(Definition of } \phi\text{)} \\
&= \varepsilon_a \circ F(G(g) \circ \eta_b) && \text{(Definition of } \psi\text{)} \\
&= \varepsilon_a \circ F(G(g)) \circ F(\eta_b) && \text{(Functoriality of } F\text{)} \\
&= g \circ \varepsilon_{F(b)} \circ F(\eta_b) && \text{(Naturality of } \varepsilon\text{)} \\
&= g \circ \mathrm{id}_{F(b)} = g && \text{(left triangle identity)}
\end{aligned}$$

//

Claim 3. *$\phi_{a,b}$ is natural in a.*

Proof of claim 3. Let $p\colon a \to a'$. Then by functoriality of G we have:

$$G(p) \circ G(g) \circ \eta_b = G(p \circ g) \circ \eta_b.$$

//

Claim 4. *$\phi_{a,b}$ is natural in b.*

Proof of claim 4. Let $q\colon b \to b'$. Then by functoriality of G and naturality of η we have:

$$G(g \circ F(q)) \circ \eta_b = G(g) \circ GF(q) \circ \eta_b = G(g) \circ \eta_{b'} \circ q$$

//

$(a) \Longleftarrow (b)$: Define

$$\begin{aligned}
&\eta\colon id_{\mathbf{B}} \Rightarrow GF \quad \text{by} \quad \eta_b \coloneqq \phi_{F(b),b}(\mathrm{id}_{F(b)})\colon b \to GF(b) \\
&\varepsilon\colon FG \Rightarrow id_{\mathbf{A}} \quad \text{by} \quad \varepsilon_a \coloneqq \psi_{a,G(a)}(\mathrm{id}_{G(a)})\colon FG(a) \to a
\end{aligned}$$

Claim 5. *η is a natural transformation.*

Proof of claim 5. For $p\colon b \to b'$ we need to show that

$$\begin{array}{ccc}
b & \xrightarrow{q} & b' \\
\downarrow{\scriptstyle \eta_b} & & \downarrow{\scriptstyle \eta_{b'}} \\
GF(b) & \xrightarrow{GF(q)} & GF(b')
\end{array}$$

? commutes, which means $\phi_{F(b),b}(\mathrm{id}_{F(b)}) \circ p = GF(p) \circ \phi_{F(b'),b'}(\mathrm{id}_{F(b')})$. But

$$\phi(\mathrm{id}) \circ p = \phi(F(p)) = GF(p) \circ \phi$$

//

Claim 6. *ε is a natural transformation.*

? *Proof of claim 6.*

//

Claim 7. *η and ε satisfy the triangle identities.*

Proof of claim 7.

$$\mathrm{id}_{F(b)} = \psi(\phi(\mathrm{id}_{F(b)})) = \psi(\eta_b) = \psi(\eta_b \circ \mathrm{id}_b) = \varepsilon_{F(b)} \circ F(\eta_b)$$
$$\mathrm{id}_{G(a)} = \phi(\psi(\mathrm{id}_{G(a)})) = \phi(\varepsilon_a) = \phi(id_a)$$

//

□

Definition 1.2 (Adjunction). Let **A** and **B** be categories. We say that functors $F\colon \mathbf{B} \to \mathbf{A}$, $G\colon \mathbf{A} \to \mathbf{B}$ form an *adjunction between* **A** *and* **B**, if F and G satisfy the equivalent conditions of 1.1. We then say that F is *left-adjoint* to G and G is *right-adjoint* to F.

Remark 1.3. We will denote the adjunction either by $F \dashv_\phi G\colon \mathbf{B} \rightleftarrows \mathbf{A}$ or by $F \overset{\eta}{\underset{\varepsilon}{\dashv}} G\colon \mathbf{B} \rightleftarrows \mathbf{A}$, sometimes even just $F \dashv G$, depending on the context.

Remark 1.4. Let $F \dashv G$ be an adjunction. Then

1. G preserves limits
2. F preserves colimits.

Example 1 (Galois connection). blablabla examples include:

those are DUAL adjunctions!

1. (Fundamental theorem of Galois theory): this example.
2. (Algebraic geometry): that example.

Example 2 (Coproduct $\dashv \Delta \dashv$ Product). this.

Example 3 (free-forgetful adjunction). that.

Example 4 (Tensor-Hom-Adjunction). There is a natural bijection

$$\mathrm{Hom}_{\mathbf{A}}(M \otimes_A N, P) \cong \mathrm{Hom}_{\mathbf{A}}(M, \mathrm{Hom}_{\mathbf{A}}(N, P))$$

This implies that the tensor-product is right-exact, since it preserves cokernels.

2 Monads and Comonads

2.1 Definition of Monads and Comonads

definitionen nicht nummerieren?

A central notion in algebra is that of a *monoid*, that is, a set M equipped with a map $\mu\colon M \times M \to M$; $(a, b) \mapsto a \cdot b$ (often called *multiplication*) and an element $e \in M$ such that the following two axioms hold:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in M. \qquad \text{(associativity)}$$
$$e \cdot a = a \cdot e = a \quad \text{for all } a \in M \qquad \text{(identity element)}$$

We can give an equivalent definition in terms of maps and commuting diagrams as follows: A *monoid* is a set M together with two functions

$$\mu\colon M \times M \to M, \quad e\colon \{*\} \to M$$

such that the following diagrams commute:

$$\begin{array}{ccc} M \times M \times M & \xrightarrow{\mathrm{id} \times \mu} & M \times M \\ \downarrow{\scriptstyle \mu \times \mathrm{id}} & & \downarrow{\scriptstyle \mu} \\ M \times M & \xrightarrow{\mu} & M \end{array} \qquad \begin{array}{ccccc} \{*\} \times M & \xrightarrow{e \times \mathrm{id}} & M \times M & \xleftarrow{\mathrm{id} \times e} & M \times \{*\} \\ & {\scriptstyle l} \searrow & \downarrow{\scriptstyle \mu} & \swarrow {\scriptstyle r} & \\ & & M & & \end{array}$$

where id is the identity on m, and l and r are the canonical bijections

$$l\colon \{*\} \times M \to M;\ l(*, m) = m$$
$$r\colon M \times \{*\} \to M;\ r(m, *) = m.$$

Explicitly, the first diagram means that for all $a, b, c \in M$:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \text{for all } a, b, c \in M.$$

which is verbatim the associativity axiom, the second diagram means that for all $m \in M$:

$$e(*) \cdot m = l(*, m) = m = r(m, *) = m \cdot e(*)$$

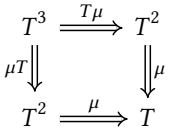
monoid/monad/ monoid object

which is clearly the identity element axiom for the element $e(*)$. This motivates the following definition:

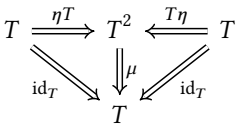
Definition 2.1 (Monad). A *Monad* (T, μ, η) in a category $\mathbf{X}$ consists of

- an endofunctor $T\colon \mathbf{X} \to \mathbf{X}$
- a natural transformation $\eta\colon \mathrm{id}_{\mathbf{X}} \Rightarrow T$
- a natural transformation $\mu\colon T^2 \Rightarrow T$

such that the following diagrams commute:

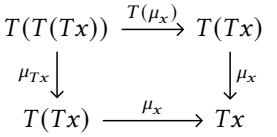


(associativity)

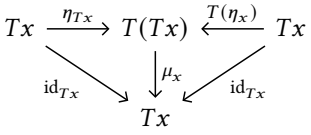


(unitality)

In terms of components, associativity and unitality mean that for every object x of $\mathbf{X}$ the following diagrams commute:



(associativity)



(unitality)

Example 5 (preorder). Recall: A *preorder* $(\mathbf{P}, \leq)$ is a category with $\mathbf{P}$ as objects and a morphism between X and Y iff $X \leq Y$. A functor $T\colon \mathbf{P} \to \mathbf{P}$ is thus a monotonic function $\mathbf{P} \to \mathbf{P}$ ($x \leq y \implies Tx \leq Ty$). The existence of the natural transformations η is equivalent to

$$x \leq Tx \; \forall x \in \mathbf{P}$$

and the existence of μ is equivalent to

$$T(Tx) \leq Tx \; \forall x \in \mathbf{P}$$

because there is at most one morphism $x \to y$, so the neccessary diagrams commute trivially.
Now suppose $\mathbf{P}$ is a *partial order*, i.e. $x \leq y \leq x \implies x = y \; \forall x, y \in \mathbf{P}$.
Then:

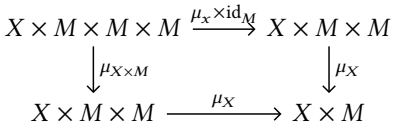
$$\begin{aligned} x \leq Tx &\implies Tx \leq T(Tx) \\ T(Tx) \leq Tx &\implies Tx = T(Tx) \end{aligned}$$

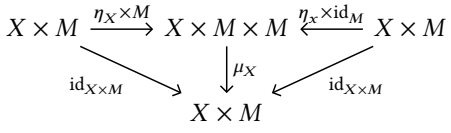
so a Monad T in a partial order $\mathbf{P}$ is a *closure operation* in $\mathbf{P}$, i.e. a monotonic function $T\colon \mathbf{P} \to \mathbf{P}$ with $x \leq Tx$ and $T(Tx) = Tx \; \forall x \in \mathbf{P}$.
Now every topological space X induces a partial order $\mathbf{P} = (\mathscr{P}(X), \subseteq)$. Here an example for a closure operation is taking the topological closure $A \mapsto \overline{A}$, since it holds for all $A \subseteq X$ that $A \subseteq \overline{A}$ and $\overline{\overline{A}} = \overline{A}$.

Example 6 (M-action Monad). Let $(M, \cdot, 1)$ be a monoid. Then for each set X we can form the set $X \times M$ and for a map $f\colon X \to Y$ we have a map $f \times \mathrm{id}_M\colon X \times M \to Y \times M; (x, m) \mapsto (f(x), m)$. This is functorial and the functor canonically has the structure of a Monad, induced by the monoid structure of M.

- The unit η is defined by $\eta_X\colon X \to X \times M; x \mapsto (x, 1)$
- The multiplication μ is defined by $\mu_X\colon X \times M \times M \to X \times M; (x, m, n) \mapsto (x, m \cdot n)$

These are clearly natural maps and the Monad axioms follow directly from the monoid axioms for M, if we look at the corresponding diagrams:





The associativity axiom means that $(m \cdot n) \cdot k = m \cdot (n \cdot k)$ which is just the associativity axiom for the monoid M, while unitality means that $1 \cdot m = m = m \cdot 1$ which holds by the identity element axiom for M. We will call this Monad on **Set** the *M-action Monad*, the reason for this name will be clear once we look at it's algebras, see Section 2.2.

Example 7 (Maybe monad). The *Maybe Monad* $Y\colon \mathbf{Set} \to \mathbf{Set}$ is defined by $X \mapsto X \cup \{*\}$ where $f\colon X \to Y$ gets mapped to the function $Y(f)\colon X \cup \{*\} \to Y \cup \{*\}$ which maps x to $f(x)$ and $*$ to $*$.

- $\eta_X\colon X \to X \cup \{*\}; x \mapsto x$
- $\mu_X\colon X \cup \{*_1\} \cup \{*_2\} \to X \cup \{*\}; x \mapsto x, *_1 \mapsto *, *_2 \mapsto *$

Definition 2.2 (Comonad). A *Comonad* (L, ε, ω) in a Category $\mathbf{A}$ consists of

- an endofunctor $L\colon \mathbf{A} \to \mathbf{A}$
- a natural transformation $\varepsilon\colon L \Rightarrow \mathrm{id}_{\mathbf{A}}$
- a natural transformation $\omega\colon L \Rightarrow L^2$

such that the following diagrams commute:

$$\begin{array}{ccc} L & \xRightarrow{\omega} & L^2 \\ {\scriptstyle\omega}\Downarrow & & \Downarrow{\scriptstyle L\omega} \\ L^2 & \xRightarrow{\omega L} & L^3 \end{array}$$

(coassociativity)

$$\begin{array}{ccccc} & & L & & \\ & {\scriptstyle \mathrm{id}_L}\swarrow & \Downarrow{\scriptstyle\omega} & \searrow{\scriptstyle \mathrm{id}_L} & \\ L & \xLeftarrow{\varepsilon L} & L^2 & \xRightarrow{L\varepsilon} & L \end{array}$$

(counitality)

In terms of components, this means that for every object x of $\mathbf{A}$ the following diagrams commute:

$$\begin{array}{ccc} Lx & \xrightarrow{\omega_x} & L(Lx) \\ {\scriptstyle\omega_x}\downarrow & & \downarrow{\scriptstyle L(\omega_x)} \\ L(Lx) & \xrightarrow{\omega_{Lx}} & L(L(Lx)) \end{array}$$

(coassociativity)

$$\begin{array}{ccccc} & & Lx & & \\ & {\scriptstyle \mathrm{id}_{Lx}}\swarrow & \downarrow{\scriptstyle\omega_x} & \searrow{\scriptstyle \mathrm{id}_{Lx}} & \\ Lx & \xleftarrow{\varepsilon_{Lx}} & L(Lx) & \xrightarrow{L(\varepsilon_x)} & Lx \end{array}$$

(counitality)

Example 8 (Reader Comonad). Let E be a set. Define a functor $C_E\colon \mathbf{Set} \to \mathbf{Set}$ by $C_E(X) = X \times E$ and, given $f\colon X \to Y$, $C_E(f) = f \times \mathrm{id}_E\colon X \times E \to Y \times E$. We can view E as "extra information" and give C_E a comonadic structure as follows:

- the counit $\varepsilon_X\colon X \times E \to X; (x, e) \mapsto x$ "forgets the extra information"
- the comultiplication $\omega_X\colon X \times E \to X \times E \times E; (x, e) \mapsto (x, e, e)$ "copies the extra information".

Now the comonad axioms say that the following diagrams have to commute:

$$\begin{array}{ccc} X \times E & \xrightarrow{\omega_X} & X \times E \times E \\ \downarrow{\scriptstyle\omega_X} & & \downarrow{\scriptstyle\omega_X \times \mathrm{id}_E} \\ X \times E \times E & \xrightarrow{\omega_{X\times E}} & X \times E \times E \times E \end{array}$$

$$\begin{array}{ccccc} & & X \times E & & \\ & {\scriptstyle \mathrm{id}_{X\times E}}\swarrow & \downarrow{\scriptstyle\omega_X} & \searrow{\scriptstyle \mathrm{id}_{X\times E}} & \\ X \times E & \xleftarrow{\varepsilon_{X\times E}} & X \times E \times E & \xrightarrow{\varepsilon_X \times \mathrm{id}_E} & X \times E \end{array}$$

The first diagram commutes, because for a tuple (x, e, e), copying the second or third element produces the same tuple. The second diagram commutes, because copying the extra information and the deleting either one of the copies gives the same result. The resulting comonad $(C_E, \varepsilon, \omega)$ on **Set** is called the *reader comonad*. Note that as a functor, it is almost the same as the *writer comonad*, but we gave it kind of a dual structure.

maybe ins Kapitel Comonaden als Beispiel schieben

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

Definition 2.3 (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:

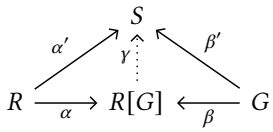
$$\Big(\sum_{g\in G} r_g \cdot g\Big) + \Big(\sum_{g\in G} s_g \cdot g\Big) \coloneqq \sum_{g\in G} (r_g + s_g) \cdot g$$
$$\Big(\sum_{g\in G} r_g \cdot g\Big) \cdot \Big(\sum_{g\in G} s_g \cdot g\Big) \coloneqq \sum_{g\in G} \Big(\sum_{k\cdot l=g} r_k \cdot s_l\Big) \cdot g$$

Example 9. $R = \mathbb{R}, G = \{x^n \mid n \in \mathbb{N}\} \implies RG = \mathbb{R}[X]$

Remark 2.4. $R[G]$ 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:

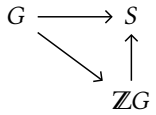
$$\alpha(r) \cdot \beta(g) = \beta(g) \cdot \alpha(r) \quad \forall r \in R, g \in G$$

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:



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 10. 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:



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.

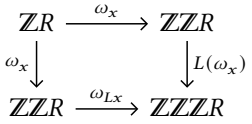
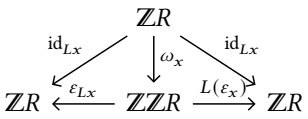
Let $G\colon$ **CRing** $\to$ **CMon**, $(R, +, \cdot) \mapsto (R, \cdot)$ be the forgetful functor and let $F\colon$ **CMon** $\to$ **CRing** be the functor $G \mapsto \mathbb{Z}G$. Then the composition $\mathbb{Z}[\_] \coloneqq F \circ G\colon$ **CRing** $\to$ **CRing** is the functor $R \mapsto \mathbb{Z}R$, which we call the *free monoid ring functor.*

Claim. $\mathbb{Z}[\_]$ *is a comonad on* **CRing**.

Proof: Define the counit and comultiplication by

$$\varepsilon_R\colon \mathbb{Z}R \to R \qquad \omega_R\colon \mathbb{Z}R \to \mathbb{Z}\mathbb{Z}R$$
$$\sum_{r\in R} a_r \cdot [r] \mapsto \sum_{r\in R} a_r \cdot r \qquad \sum_{r\in R} a_r \cdot [r] \mapsto \Big[\sum_{r\in R} a_r \cdot [r]\Big]$$

those are clearly natural and the following diagrams commute:

□

Remark 2.5. We can define a variation of this, by setting $\underline{\mathbb{Z}}R := {}^{\mathbb{Z}R}/_{(0)}$ where $(0) = \{r \cdot 0 \mid r \in \mathbb{Z}R\}$ is the ideal generated by $0 \in R$.

Lemma 2.6 *For every object x in $\mathbf{X}$, the following diagram commutes:*

$$\begin{array}{ccc} T(Tx) & \xrightarrow{T(\delta_x)} & T(T'x) \\ \downarrow{\scriptstyle \delta_{Tx}} & & \downarrow{\scriptstyle \delta_{T'x}} \\ T(T'x) & \xrightarrow{T'(\delta_x)} & T'(T'x) \end{array}$$

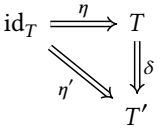
this means

$$\delta T' \circ T\delta = T'\delta \circ \delta T \colon T^2 \Rightarrow (T')^2.$$

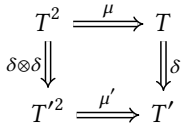
We denote this natural transformation by $\delta \otimes \delta$, since this is actually the monoidal product of morphisms in the monoidal category of endofunctors on $\mathbf{X}$.

Proof: $\delta_x \colon Tx \to T'x$ is a ring homomorphism. Since $\delta \colon T \Rightarrow T'$ is natural transformation, the square commutes. □

Definition 2.7 (Morphism of monads). Let $\mathbf{X}$ be a category, let (T, η, μ) and (T', η', μ') be monads in $\mathbf{X}$. We say that a natural transformation $\delta \colon T \Rightarrow T'$ is a *morphism of monads* if it preserves the unit and the multiplication, i.e. the following diagrams commute:

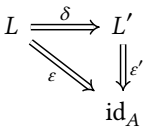


(unit-preserving)

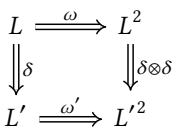


(multiplication-preserving)

Definition 2.8 (Morphism of comonads). Let $\mathbf{A}$ be a category, let (L, ε, ω) and $(L', \varepsilon', \omega')$ be comonads in $\mathbf{A}$. We say that a natural transformation $\delta \colon L \Rightarrow L'$ is a *morphism of monads* if it preserves the counit and the comultiplication, i.e. the following diagrams commute:



(counit-preserving)



(comultiplication-preserving)

Example 11. Consider the *subsingletons Monad* $\mathbb{P}^1 \colon \mathbf{Set} \to \mathbf{Set}$, which assigns to each set X the set of subsets of X containing *at most* one element, so an element of $\mathbb{P}^1(X)$ is either $\emptyset$ or a singleton $\{x\}$. For a function $f \colon X \to Y$, the induced function maps $\emptyset$ to $\emptyset$ and $\{x\}$ to $\{f(x)\}$, compare this to the power set functor. If we

define the unit η' by

$$\eta'_X : X \to \mathbb{P}^1(X); x \mapsto \{x\}$$

and the multiplication μ' by

$$\mu'_X : \mathbb{P}^1(\mathbb{P}^1(X)) \to \mathbb{P}^1(X); \{\{x\}\} \mapsto \{x\}, \{\emptyset\} \mapsto \emptyset, \emptyset \mapsto \emptyset$$

then the resulting monad looks really similar to the *Maybe Monad*. This is not a coincidence: the map

$$\delta_X : X \cup \{*\} \to \mathbb{P}^1(X); x \mapsto \{x\}, * \mapsto \emptyset$$

gives a natural isomorphism $Y \Rightarrow \mathbb{P}^1$ which is indeed an isomorphism of Monads. ausrechnen

Theorem 2.9 (Every adjunction induces a Monad and a Comonad) *Let $F \underset{\varepsilon}{\overset{\eta}{\dashv}} G : \mathbf{B} \rightleftarrows \mathbf{A}$ be an adjunction. Then $(GF, \eta, G\varepsilon F)$ is a Monad on B and $(FG, \varepsilon, F\eta G)$ is a Comonad on A, which we call the Monad respectively Comonad induced by the adjunction.*

Proof: We have to show that the first of the following diagrams commutes, but by removing G from the left and F from the right, it suffices to show that the right diagram commutes.

$$\begin{array}{ccc} GFGFGF & \xRightarrow{GFG\varepsilon F} & GFGF \\ \Downarrow{\scriptstyle G\varepsilon FGF} & & \Downarrow{\scriptstyle G\varepsilon F} \\ GFGF & \xRightarrow{G\varepsilon F} & GF \end{array} \qquad \begin{array}{ccc} FGFG & \xRightarrow{FG\varepsilon} & FG \\ \Downarrow{\scriptstyle \varepsilon FG} & & \Downarrow{\scriptstyle \varepsilon} \\ FG & \xRightarrow{\varepsilon} & \mathrm{id}_B \end{array}$$

The second diagram now commutes by the interchange law for natural transformations. To show unitality we need to show that the following diagram commutes.

$$\begin{array}{ccccc} GF & \xRightarrow{\eta GF} & GFGF & \xLeftarrow{GF\eta} & GF \\ & \searrow^{\mathrm{id}_{GF}} & \Downarrow{\scriptstyle G\varepsilon F} & \swarrow_{\mathrm{id}_{GF}} & \\ & & GF & & \end{array}$$

but this is essentially the diagrams stating the left and right triangle identity for the adjunction after applying F respectively G. The proof that $(FG, \varepsilon, F\eta G)$ is a Comonad on A is dual. □

Now that we know that every adjunction induces a Monad, one may ask, if the converse is true, that is if every Monad is induced by an adjunction. We will see that this is the case and there are even multiple ways to induce a given Monad T. The first one is a construction called the *Eilenberg-Moore-Category* which is not only useful for forming the adjunction.

2.2 The Eilenberg-Moore-Category of a Monad

Definition 2.10 (Eilenberg-Moore-Category). Let $T = (T, \eta, \mu)$ be a monad in a category $\mathbf{X}$. A *T-algebra* is a pair (x, h) where x is an object of $\mathbf{X}$ and $h : Tx \to x$ is an arrow such that the following diagrams commute:

$$\begin{array}{ccc} T^2x & \xrightarrow{Th} & Tx \\ \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle h} \\ Tx & \xrightarrow{h} & x \end{array} \qquad \begin{array}{ccc} x & \xrightarrow{\eta_x} & Tx \\ & \searrow^{id_x} & \downarrow{\scriptstyle h} \\ & & x \end{array}$$

We call h the *stucture map* of (x, h). A *morphism of T-algebras* $f : (x, h) \to (x', h')$ is an arrow $f : x \to x'$

such that

$$\begin{array}{ccc} Tx & \xrightarrow{Tf} & Tx' \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle h'} \\ x & \xrightarrow{f} & x' \end{array}$$

commutes. The set of all T-algebras together with their morphisms form a category, which is called the *Eilenberg-Moore-Category* and denoted by $\mathbf{X}^T$.

Proof that this is indeed a category?

Example 12 (M-action Monad). A T_M-algebra is a set X together with a map $h\colon X \times M \to X$ such that

$$\begin{array}{ccc} X \times M \times M & \xrightarrow{h \times \mathrm{id}_M} & X \times M \\ \downarrow{\scriptstyle \mu_X} & & \downarrow{\scriptstyle h} \\ X \times M & \xrightarrow{h} & X \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\eta_x} & X \times M \\ & \searrow^{id_x} & \downarrow{\scriptstyle h} \\ & & X \end{array}$$

commute. If we denote $h(x, m)$ by $(x.m)$, this means that $(x.m).n = x.(m \cdot n)$ and $x.1 = 1$. So T_M-algebras are nothing but sets equipped with a right M-action. In particular, if M is a group, the T_M-algebras are just right M-sets.

all correct? right/left?

Theorem 2.11 (Every monad is defined by its T-algebras) *Let (T, η, μ) be a monad in a category $\mathbf{X}$. Then there is an adjunction $F^T \dashv G^T$, where F^T and G^T are functors $\mathbf{X}^\mathbf{T} \underset{F^T}{\overset{G^T}{\leftrightarrows}} \mathbf{X}$ such that the monad induced by this adjunction is (T, η, μ).*

Proof: Define $F^T\colon \mathbf{X} \to \mathbf{X}^T$ by

$$\begin{array}{ccc} x & \longmapsto & (Tx, \mu_x) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle Tf} \\ x' & \longmapsto & (Tx', \mu_{x'}) \end{array}$$

(Tx, μ_x) is indeed a T-algebra, since μ_x is an arrow $T^2x \to Tx$ and the diagrams

$$\begin{array}{ccc} T^3x & \xrightarrow{T(\mu_x)} & T^2x \\ \downarrow{\scriptstyle \mu_{Tx}} & & \downarrow{\scriptstyle \mu_x} \\ T^2x & \xrightarrow{\mu_x} & Tx \end{array} \qquad \begin{array}{ccc} Tx & \xrightarrow{\eta_{Tx}} & T^x \\ & \searrow^{id_{Tx}} & \downarrow{\scriptstyle \mu_x} \\ & & Tx \end{array}$$

are just the commuting diagrams for the associativity respectively left unitality axioms from the definition of a Monad.
$Tf\colon (Tx, \mu_x) \to (Tx', \mu_{x'})$ is indeed a morphism of T-algebras, since the commutativity of

$$\begin{array}{ccc} T^2x & \xrightarrow{T^2(f)} & T^2x' \\ \downarrow{\scriptstyle \mu_x} & & \downarrow{\scriptstyle \mu_{x'}} \\ Tx & \xrightarrow{T(f)} & Tx' \end{array}$$

is given by naturality of μ. The functoriality of F^T follows from the functoriality of T.

Define $G^T : \mathbf{X^T} \to \mathbf{X}$ by

$$\begin{array}{ccc} (x,h) & \longmapsto & x \\ \downarrow f & & \downarrow f \\ (x',h') & \longmapsto & x' \end{array}$$

so G is just the forgetful functor.

Claim. *$G^T \circ F^T = T$ and $F^T G^T(x,h) = (Tx, \mu_x)$.*

Proof of claim. Let $x \in \mathbf{X}$. Then $G^T(F^T(x)) = G^T(Tx, \mu_x) = Tx$. Now let $f : x \to y$. Then $G^T(F^T(f)) = G^t(Tf) = Tf$. Finally, $F^T G^T(x,h) = F^T(x) = (Tx, \mu_x)$. □

So we can set

$$\eta^T := \eta : \mathrm{id}_{\mathbf{X}} \Rightarrow G^T F^T$$

as the unit and we can define $\varepsilon^T : F^T G^T \to \mathrm{id}_{\mathbf{X}^T}$ by

$$\varepsilon^T_{(x,h)} := h : (Tx, \mu_x) \to (x,h).$$

h is a morphism of T-algebras because (x,h) is a T-algebra, since both statements mean that the diagram

$$\begin{array}{ccc} T^2x & \xrightarrow{Th} & Tx \\ \downarrow \mu & & \downarrow h \\ T & \xrightarrow{h} & x \end{array}$$

commutes. ε^T is natural, because if $f : (x,h) \to (x',h')$ is a morphism of T-algebras, naturality means that the diagram

$$\begin{array}{ccc} Tx & \xrightarrow{Tf} & Tx' \\ \downarrow h & & \downarrow h' \\ x & \xrightarrow{f} & x' \end{array}$$

but this is exactly the definition of f being a morphism of T-algebras. □

triangle identities and induces T

Theorem 2.12 (Comparison of adjunctions with algebras)

2.3 The Kleisli category of a Monad

There is another way to induce a Monad by an adjunction:

Definition 2.13 (Kleisli category). Let $\mathbf{X}$ be a category, $T = (T, \eta, \mu)$ be a monad in $\mathbf{X}$. The *Kleisli category* $\mathbf{X}_T$ is defined by

- objects the same as in $\mathbf{X}$, but we relabel x to x_T for all $x \in \mathbf{X}$.
- for $x_T, y_T \in \mathbf{X}_T$, $f : x \to Ty$ is a morphism which we denote by $f^b : x_T \to y_T$.
- composition will be denoted by $\bullet$ for distinction and is defined by

$$g^b \bullet f^b := (\mu_z \circ Tg \circ f)^b : x_T \to z_T$$

for $f^b : x_T \to y_T$, $g^b : y_T \to z_T$. This is indeed again a morphism: $x \xrightarrow{f} Ty \xrightarrow{Tg} T^2 z \xrightarrow{\mu_z} Tz$

Claim. *This defines a category.*

Proof of claim. associativity: Let $x_T \xrightarrow{f^b} y_T \xrightarrow{g^b} z_T \xrightarrow{h^b} w_T$ be objects and morphisms in the Kleisli category.

$$\begin{aligned}(h^b \bullet g^b) \bullet f^b &= (\mu_w \circ Th \circ g)^b \bullet f^b \\ &= (\mu_w \circ T(\mu_w \circ Th \circ g) \circ f)^b \\ &= (\mu_w \circ T\mu_w \circ T^2 h \circ Tg \circ f)^b.\end{aligned}$$

Now the associativity axiom for the Monad T states that

$$\begin{array}{ccc} T(T(Tw)) & \xrightarrow{T(\mu_w)} & T(Tw) \\ {\scriptstyle \mu_{Tw}}\downarrow & & \downarrow{\scriptstyle \mu_w} \\ T(Tw) & \xrightarrow{\mu_w} & Tw \end{array}$$

commutes, hence

$$(\mu_w \circ T\mu_w \circ T^2 h \circ Tg \circ f)^b = (\mu_w \circ \mu_{Tw} \circ T^2 h \circ Tg \circ f)^b$$

By naturality of μ, the diagram

$$\begin{array}{ccc} T^2 z & \longrightarrow & T^3 w \\ \downarrow & & \downarrow \\ Tz & \longrightarrow & T^2 w \end{array}$$

commutes, so it follows that

$$\begin{aligned}(\mu_w \circ \mu_{Tw} \circ T^2 h \circ Tg \circ f)^b &= (\mu_w \circ Th \circ \mu_z \circ Tg \circ f)^b \\ &= h^b \bullet (g^b \bullet f^b)\end{aligned}$$

identity axiom: Let $f^b : x_T \to y_T$ be a morphism.

$$f^b \bullet (\eta_x)^b = (\mu_x \circ Tf \circ \eta_x)^b = (\mu_x \circ \eta_{Ty} \circ f)^b = (\mathrm{id}_{Ty} \circ f)^b = f^b$$

where the second equality follows from the naturality of η and the third equality is due to the left unitality law for T.

$$(\eta_y)^b \bullet f^b = (\mu_y \circ T\eta_y \circ f)^b = (id_{Ty} \circ f)^b = f^b$$

where the second equality is due to the right unitality law for T. This proves that for $x_T \in \mathbf{X}_T$ we have $\mathrm{id}_{x_T} = (\eta_x)^b \in \mathrm{Hom}_{\mathbf{X}_\mathbf{T}}(x_T, x_T)$ □

Theorem 2.14 *There is an adjoint situation $F_T \dashv G_T$: $\mathbf{X}_\mathbf{T} \rightleftarrows \mathbf{X}$ such that T is the induced monad by this adjunction.*

3 Witt vectors

3.1 Construction of the witt vectors

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

Definition 3.1 (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 3.2 (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 3.3 (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 3.4 *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 3.5 (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

$$\begin{aligned}
\sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) &\equiv \sum_{d|n/p} d \cdot a_d^{n/d} && \mod p^{v_p(n)}A && (3.1) \\
&\equiv \sum_{d|n} d \cdot a_d^{n/d} && \mod p^{v_p(n)}A && (3.2)
\end{aligned}$$

so we get

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

Proof of (3.1). First, note that

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

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

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

using Lemma 3.4 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

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

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

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

which implies (1). □

Proof of (3.2). 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 $d \equiv 0 \mod p^{v_p(n)}A$. □

proof-umgebung

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

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

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

$$\begin{aligned} \sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) &\overset{(3.1)}{\equiv} \sum_{d|n/p} d \cdot a_d^{n/d} \qquad \mod p^{v_p(n)}A \\ &\overset{(3.2)}{\equiv} \sum_{d|n} d \cdot a_d^{n/d} \qquad \mod p^{v_p(n)}A \\ &\equiv \sum_{d|n, d \neq n} d \cdot a_d^{n/d} \qquad \mod p^{v_p(n)}A \end{aligned}$$

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 3.6 *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 3.7 *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: Step 1: Let $A = \mathbb{Z}[a_n, b_n \mid n \in S]$. Consider the unique ring homomorphism

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

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).

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 3.5 , 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 since $w_n(a), w_n(b)$ are in the image of the ghost map, we know that $w_n(a) \equiv \phi_p(w_{n/p}(a)) \mod p^{v_p(n)}A$

and $w_n(b) \equiv \phi_p(w_{n/p}(b)) \bmod p^{v_p(n)}A$. 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

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

Since A is torsion-free, the ghost map is injective by 3.6 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

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

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 //

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

finish

□

Corollary 3.8 *$w_n\colon \mathbb{W}_S(A) \to A$ is a natural ring homomorphism for all $n \in S$.*

Proof: This follows immediately from 3.7. □

Lemma 3.9 *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 3.10 *$\mathbb{W}_S(\_)$ is a functor* **CRing** $\to$ **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 $f\colon A \to B$, $\mathbb{W}_S(f)\colon W_S(A) \to W_S(B)$ 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

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

□

3.2 The Verschiebung, Frobenius and Teichmüller maps

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

Definition 3.11 (Restriction map). If $T \subseteq S$ are two truncation sets, the *restriction from S to T*

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

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 3.12 (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 3.13 *The Verschiebung map V_n is additive.*

Proof:

Claim.
$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\ \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle \widetilde{V_n}} \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S \end{array} \quad \textit{commutes.}$$

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
$$w(V_n(a))_m = \sum_{k\mid m, k=nd} k \cdot a_d^{m/k} = 0$$
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 $d \in S$:
$$\begin{aligned} \widetilde{V_n}(w(a))_m &= (\widetilde{V_n}(w_d)_{d\in S/n})_m = n \cdot w_d = n \cdot \sum_{k\mid d} k \cdot a_k^{d/k}. \\ w(V_n(a))_m &= w_m(V_n(a)) = \sum_{k\mid nd} k \cdot (V_n(a))_k^{nd/k} \\ &= \sum_{k\mid nd, k=nd_k} k \cdot a_{d_k}^{nd/k} = n \cdot \sum_{k\mid nd, k=nd_k} d_k \cdot a_{d_k}^{nd/nd_k} \\ &= n \cdot \sum_{k\mid nd, k=nd_k} d_k \cdot a_{d_k}^{d/d_k} = n \cdot \sum_{k\mid d} k \cdot a_k^{d/k} \end{aligned}$$
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
$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{w} & A^{S/n} \\ \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle \widetilde{V_n}} \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S \end{array}$$
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 $g\colon A \to A'$, where A is torsion-free. Then the diagram
$$\begin{array}{ccc} \mathbb{W}_{S/n}(A) & \xrightarrow{\mathbb{W}_{S/n}(g)} & \mathbb{W}_{S/n}(A') \\ \downarrow{\scriptstyle V_n} & & \downarrow{\scriptstyle V_n} \\ \mathbb{W}_S(A) & \xrightarrow{\mathbb{W}_S(g)} & \mathbb{W}_S(A') \end{array}$$

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 a crucial rule in the proof of the comonadic structure of $\mathbb{W}(A)$ as well. For that, first define $\widetilde{F}_n \colon A^S \to A^{S/n}$ by $\widetilde{F}_n((x_m)_{m\in S})_d = x_{nd}$.

Lemma 3.14 (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

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

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 $d \in S/n$:

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

Proof of Lemma 3.14. We construct F_n similar to the construction of the ring operations on $\mathbb{W}_S A(A)$ using Lemma 3.5 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 3.5 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

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

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

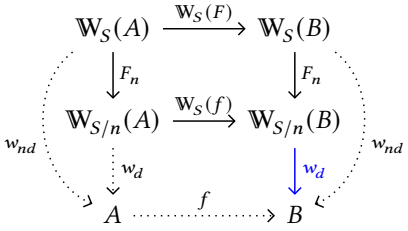
$$F_n(a') \coloneqq \mathbb{W}_{S/n}(g)(F_n(a))$$

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 3.13 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

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

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



but by naturality of w_{nd} (3.8), the claim follows. □

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

Lemma 3.15 *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:

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

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:

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

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

Lemma 3.16 $F_1 = \mathrm{id}\colon W_S(A) \to W_S(A)$.

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 3.17 (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 3.18 *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

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

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

□

3.3 The comonad structure of witt vectors

We will need the following lemma:

Lemma 3.19 *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

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

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:

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

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

Definition 3.21. $\mathbb{W}(A) \coloneqq \mathbb{W}_{\mathbb{N}}(A)$

For the construction of a natural transformation $\mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(A))$ we want to use Lemma 3.5 again. Hence we first show:

Lemma 3.22 *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 $F_p(a) \equiv a^p \mod pA$.*

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

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

it suffices to show there exists $b \in \mathbb{W}(A)$ such that $F_p(a) - a^p = p \cdot b$. By Lemma 3.19, this element is unique. Applying the ghost map gives us:

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

using Lemma 3.14. This is now congruent to 0 mod pA: indeed
It follows that there exists $x = (x_n)_{n \in \mathbb{N}}$ such that

$$p \cdot x_n = w_n(F_p(a) - a^p) \iff x_n = \frac{1}{p} \cdot w_n(F_p(a) - a^p) \tag{3.3}$$

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 3.5 again. Consider the unique ring homomorphism $\phi_l \colon A \to A$ which maps a_n to a_n^l. It satisfies $\phi_l(f) \equiv f^l \mod lA$. (indeed:). indeed
so by Lemma 3.5 it suffices to show:

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

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

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

and

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

(Using 3.3 we have for $l = p$:

$$\begin{aligned} x_n \equiv \phi_p(x_{n/p}) \bmod p^{v_p(n)}A \iff\ & p \cdot x_n \equiv p \cdot \phi_p(x_{n/p}) && \mod p^{v_p(n)+1}A \\ \overset{3.3}{\iff}\ & w_n(F_p(a) - a^p) \equiv \phi_p(w_{n/p}(F_p(a) - a^p)) && \mod p^{v_p(n)+1}A \end{aligned}$$

and for $l \neq p$:

$$\begin{aligned} x_n \equiv \phi_l(x_{n/l}) \bmod l^{v_l(n)}A &\iff p \cdot x_n \equiv p \cdot \phi_l(x_{n/l}) && \bmod l^{v_l(n)}A \\ &\overset{3.3}{\iff} w_n(F_p(a) - a^p) \equiv \phi_l(w_{n/l}(F_p(a) - a^p)) && \bmod l^{v_l(n)}A.) \end{aligned}$$

For $l \neq p$, the statement follows directly from Lemma 3.5. So now let $l = p$, let $n \in p\mathbb{N}$. Then:

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

using Lemma 3.14 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 3.2 and 3.4 again we have

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

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 $r \in A$. □

Proposition 3.23 *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:** As before, we can assume $A = \mathbb{Z}[a_n \mid n \in \mathbb{N}]$. By applying Corollary 3.20 twice, we get that the ghost map

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

is injective. Now by Lemma 3.22, $F_p \colon \mathbb{W}(A) \to \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \bmod p\mathbb{W}(A)$, hence we can use Lemma 3.5 again and just show that

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

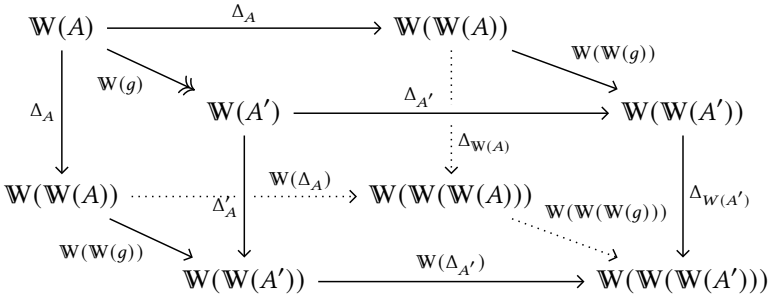
for all p prime, $n \in p\mathbb{N}$. But this immediately follows from Lemma 3.15, so there is a unique $\Delta(a) \in \mathbb{W}(\mathbb{W}(A))$ such that $w_n(\Delta(a)) = F_n(a)$. □

Recall that by 3.8, $w_1 \colon \mathbb{W}(A) \to A$; $(a_n)_{n\in\mathbb{N}} \mapsto a_1$ is a natural transformation $\mathbb{W} \Rightarrow \mathrm{id}_{\mathbf{CRing}}$.

Theorem 3.24 *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: By naturality of Δ, we can assume that A is torsion-free, because if A' is an arbitrary ring, to show

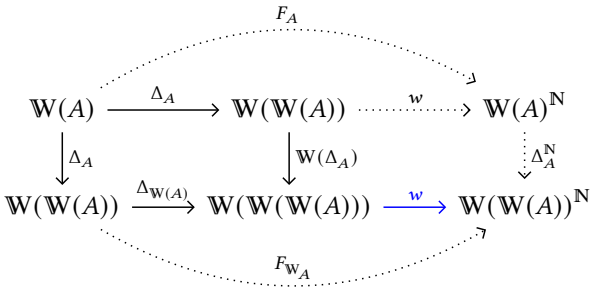
the associativity axiom, we can choose $g\colon A \to A'$ surjective as always and then consider the following cube:



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.

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

Proof of claim. evaluating the ghost coordinates leads to:



which by Proposition 3.23 simplifies to

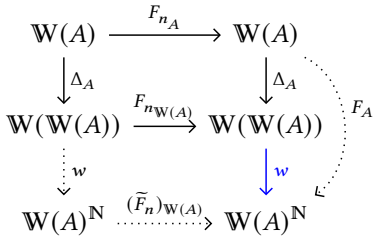
$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{F_A} & \mathbb{W}(A)^{\mathbb{N}} \\ \downarrow{\scriptstyle \Delta_A} & & \downarrow{\scriptstyle \Delta_A^{\mathbb{N}}} \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{F_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(A))^{\mathbb{N}} \end{array}$$

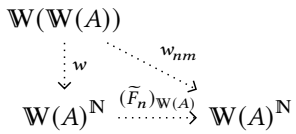
now it suffices to show for an arbitrary n that the following diagram commutes:

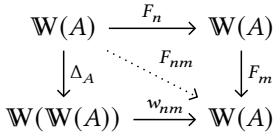
$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{F_{n_A}} & \mathbb{W}(A) \\ \downarrow{\scriptstyle \Delta_A} & & \downarrow{\scriptstyle \Delta_A} \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{F_{n_{\mathbb{W}(A)}}} & \mathbb{W}(\mathbb{W}(A)) \end{array}$$

evaluating the ghost coordinates again, keeping in mind that by 3.20 and 3.6, $w\colon \mathbb{W}(\mathbb{W}(A)) \to \mathbb{W}(A)^{\mathbb{N}}$ is

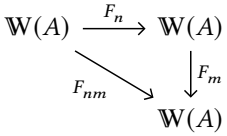
injective as well, we get



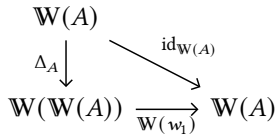
using the fact that  commutes, we can simplify the situation to



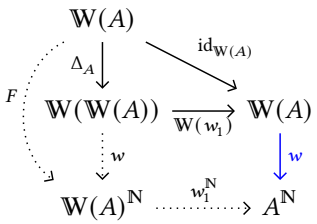
which can again be simplified to



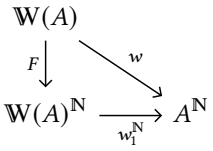
now this commutes by Lemma 3.15, hence we are finished. //

Claim.  *commutes.*

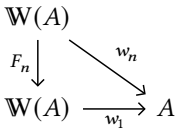
Proof of claim. evaluate the ghost coordinates:



we can then simplify to

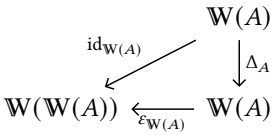


now it suffices to show for all n that



commutes, which is true by Lemma 3.14.

//

Claim.  *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 3.16. //

This concludes the proof. □

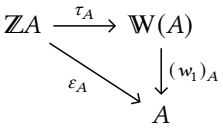
3.4 The Teichmüller map induces a morphism of comonads

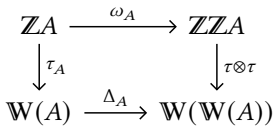
Now consider the *teichmüller map* $\tau\colon A \to \mathbb{W}(A); a \mapsto (a, 0, 0, 0, \dots)$. τ is multiplicative and preserves the unit, hence it extends uniquely to a ring homomorphism

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

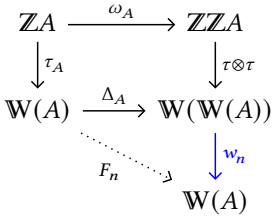
Theorem 3.25 *$\tau\colon \mathbb{Z}A \to \mathbb{W}(A)$ is a morphism of comonads.*

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



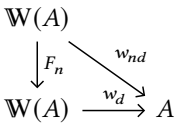


By the universal property of $\mathbb{Z}A$, it suffices to consider elements of the form $[a]$ for $a \in A$. For the first diagram: $w_1(\tau([a])) = a = \varepsilon([a])$. For the second diagram, arguing as above, it suffices to show commutativity after evaluating the ghost coordinates:



But $w_n(\tau \otimes \tau(\omega([a]))) = w_n(\tau \otimes \tau([[a]])) = w_n(((a, 0, \dots), 0, \dots)) = (a, 0, \dots)^n = (a^n, 0, \dots)$ and

$F_n(\tau([a])) = F_n((a, 0, \dots)) = (a^n, 0, \dots)$ because F_n is the unique map that makes the diagram



what? commute. □