

WESTFÄLISCHE WILHELMS-UNIVERSITÄT
MÜNSTER

BACHELOR THESIS

Monads, Comonads and Witt Vectors

Author:

Jakob BERND
jbernd@uni-muenster.de
Matr.Nr. 514640

Supervisor:

Prof. Dr. Christopher
DENINGER

submitted on 25. August 2023



FACHBEREICH 10
MATHEMATIK UND
INFORMATIK

Preface

In this bachelor thesis, I will give an introduction to the concept of monads, which are a generalization of monoids, and their categorical duals, comonads. Every adjunction induces a monad, but every monad is induced by an adjunction as well. In the third and last section, will also introduce Witt vectors, which are used a lot in algebraic number theory and proof that they admit a comonad structure. At last, I will show that the teichmüller map induces a morphism of comonads between the free monoid ring comonad and the witt vector comonad.

Contents

1	Adjunctions	1
1.1	Definition of adjunctions	2
1.2	Examples	5
2	Monads and Comonads	6
2.1	Definition of monads and comonads	6
2.2	The Eilenberg-Moore-Category of a monad	14
2.3	The Kleisli category of a monad	18
3	Witt vectors	24
3.1	Construction of the Witt vectors	24
3.2	The Verschiebung, Frobenius and Teichmüller maps	31
3.3	The comonad structure of Witt vectors	36
3.4	The Teichmüller map induces a morphism of comonads	42
	Literature	44

1 Adjunctions

Let \mathbf{A}, \mathbf{B} be two categories. We say that \mathbf{A} and \mathbf{B} are *isomorphic*, denoted $\mathbf{A} \cong \mathbf{B}$, if there exist functors $G: \mathbf{A} \rightarrow \mathbf{B}, F: \mathbf{B} \rightarrow \mathbf{A}$ with $FG = \text{id}_A, GF = \text{id}_B$. This condition is too strict to provide us with many examples, which is why there is a different notion: We say that \mathbf{A} and \mathbf{B} are *equivalent*, denoted $\mathbf{A} \simeq \mathbf{B}$, if $FG \cong \text{id}_A, GF \cong \text{id}_B$ via natural isomorphisms $\alpha: FG \rightarrow \text{id}_A, \beta: GF \rightarrow \text{id}_B$. Equivalent categories are essentially the same, all categorical properties, like for example initial objects are preserved under equivalence. But there is an even less strict relation between categories, which was first introduced by Daniel Kan in [Kan58] and which is a powerful concept, because it arises so often: Consider the categories \mathbf{Set} and \mathbf{Vect}_K for a fixed field K . The two categories can't be equivalent, since \mathbf{Vect}_K has a zero object while \mathbf{Set} doesn't. But there still is a connection between them: A vector space is a set with additional structure and linear maps are maps of sets which respect these structures. A different way to say this is that there is a forgetful functor $U: \mathbf{Vect}_K \rightarrow \mathbf{Set}$. We can also go in the opposite direction, because there is a "natural" way to make a set X into a vector space:

- We form the set FX of all formal linear combinations of elements of X , i.e. all elements of the form $\sum_{i=1}^n a_i x_i$
- we define addition and scalar multiplication by:

$$\lambda \cdot \left(\sum_{i=1}^n a_i x_i \right) := \sum_{i=1}^n (\lambda \cdot a_i) \cdot x_i$$

$$\sum_{i=1}^n a_i x_i + \sum_{i=1}^n b_i x_i := \sum_{i=1}^n (a_i + b_i) x_i$$

(note that we can assume linear combinations in FX to have the same length, since we can just add 0.)

This gives a vector space which has X as a basis. Now the universal property of a vector space states that each map $X \rightarrow U(W)$ extends uniquely to a map $F(X) \rightarrow W$ and every map $F(X) \rightarrow W$ gives a map $X \rightarrow U(W)$ by restriction. This amounts to a bijection

$$\text{Hom}_{\mathbf{Vect}_K}(F(X), W) \cong \text{Hom}_{\mathbf{Set}}(X, U(W))$$

which is also natural in a sense we will discuss later. The functors F and U form what is called a *free-forgetful adjunction*, which is the first example of an adjunction.

1.1 Definition of adjunctions

We will start by giving two equivalent definitions of an adjunction, where the first one is especially useful when it comes to monads, while the second, more standard one, is easier to find examples.

Proposition 1.1 *Given two functors $\mathbf{B} \xrightleftharpoons[F]{F} \mathbf{A}$ the following are equivalent:*

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

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

(triangle identity)

(b) *There is a bijection*

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

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

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

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

PROOF: (a) \implies (b) :
define

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

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

for $g: F(b) \rightarrow a$, $f: b \rightarrow G(a)$.

CLAIM 1. $\phi \circ \psi = \text{id}$

Proof of claim 1. Let $f: b \rightarrow G(a)$.

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

//

CLAIM 2. $\psi \circ \phi = \text{id}$

Proof of claim 2.

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

//

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

Proof of claim 3. Let $p: a \rightarrow a'$. 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 $q: b \rightarrow b'$. Then by functoriality of G and naturality of η we have:

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

//

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

$$\eta: \text{id}_B \Rightarrow GF \quad \text{by} \quad \eta_b := \phi_{F(b),b}(\text{id}_{F(b)}): b \rightarrow GF(b)$$

$$\varepsilon: FG \Rightarrow \text{id}_A \quad \text{by} \quad \varepsilon_a := \psi_{a,G(a)}(\text{id}_{G(a)}): FG(a) \rightarrow a$$

CLAIM 5. η is a natural transformation.

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

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

finish

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

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

//

CLAIM 6. ε is a natural transformation.

finish

Proof of claim 6.

//

CLAIM 7. η and ε satisfy the triangle identities.

Proof of claim 7.

$$\text{id}_{F(b)} = \psi(\phi(\text{id}_{F(b)})) = \psi(\eta_b) = \psi(\eta_b \circ \text{id}_b) = \varepsilon_{F(b)} \circ F(\eta_b)$$

$$\text{id}_{G(a)} = \phi(\psi(\text{id}_{G(a)})) = \phi(\varepsilon_a) = \phi(\text{id}_a)$$

//

□

or yoneda
lemma, see
p.193 Bran-
denburg

Definition 1.2 (Adjunction). Let \mathbf{A} and \mathbf{B} be categories. We say that functors $F: \mathbf{B} \rightarrow \mathbf{A}$, $G: \mathbf{A} \rightarrow \mathbf{B}$ form an *adjunction between \mathbf{A} and \mathbf{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 $F \dashv_{\phi} G: \mathbf{B} \rightleftarrows \mathbf{A}$ or by $F \xrightarrow{\eta} G: \mathbf{B} \rightleftarrows \mathbf{A}$, sometimes even just $F \dashv G$, depending on the context.

Remark 1.4 (proven for example in [Rie17, Chapter 4.5]). Let $F \dashv G$ be an adjunction. Then

1. G preserves limits
2. F preserves colimits.

1.2 Examples

finish Examples for adjunctions can be found all over mathematics. Here are a few:

Example 1 (Coproduct $\dashv \Delta \dashv$ Product). TODO

Example 2 (free-forgetful adjunction). TODO free group

Example 3 (Tensor-Hom-Adjunction). There is a natural bijection

$$\mathrm{Hom}_A(M \otimes_A N, P) \cong \mathrm{Hom}_A(M, \mathrm{Hom}_A(N, P))$$

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

Example 4 (Galois connection). monotone and antitone galois connections, examples are:

1. (Convex sets): TODO
2. (Fundamental theorem of Galois theory): TODO
3. (Algebraic geometry): TODO

2 Monads and Comonads

Monads were first introduced in 1958 under the name *standard construction* or *construction fondamentale* by Roger Godement in [God58, Appendix, 3.], where he used them for applications in sheaf cohomology. They were also used in algebraic topology and homotopy theory, for example in [Hub61]. In the early category theory literature monads were called *triples*, other names were *monoid*, *dual standard construction* and *triad*. The name *monad* first appeared in [Bén67], the exact reason for this name being unclear today, although it surely inspired by *monoids*, which monads are related to. Monads are closely connected to adjunctions, as we will explore in this chapter, besides giving lots of examples, with many interesting examples coming from [Per21]. In computer science, monads play an important role in functional programming. This chapter is based on [Mac98, Chapter VI], which is the standard resource for first learning about monads and comonads. Some of the proofs are taken from [HST14, Chapter II.3] instead. Another great exposition is [Per21, Chapter 5].

2.1 Definition of monads and comonads

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

$$\begin{aligned} (a \cdot b) \cdot c &= a \cdot (b \cdot c) && \text{for all } a, b, c \in M. && \text{(associativity)} \\ e \cdot a &= a \cdot e = a && \text{for all } a \in M && \text{(identity element)} \end{aligned}$$

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

$$\mu: M \times M \rightarrow M, \quad e: \{*\} \rightarrow M$$

such that the following diagrams commute:

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

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

$$\begin{aligned} l: \{*\} \times M &\rightarrow M; l(*, m) = m \\ r: M \times \{*\} &\rightarrow M; r(m, *) = m. \end{aligned}$$

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 $m \in M$:

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

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

monoid/monad/
monoid
object

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

- an endofunctor $T: \mathbf{X} \rightarrow \mathbf{X}$
- a natural transformation $\eta: \text{id}_{\mathbf{X}} \Rightarrow T$
- a natural transformation $\mu: T^2 \Rightarrow T$

such that the following diagrams commute:

$$\begin{array}{ccc} T^3 & \xrightarrow{T\mu} & T^2 \\ \mu T \downarrow & & \downarrow \mu \\ T^2 & \xrightarrow{\mu} & T \end{array}$$

(associativity)

$$\begin{array}{ccccc} T & \xrightarrow{\eta T} & T^2 & \xleftarrow{T\eta} & T \\ & \searrow \text{id}_T & \downarrow \mu & \swarrow \text{id}_T & \\ & & T & & \end{array}$$

(unitality)

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

$$\begin{array}{ccc} T(T(Tx)) & \xrightarrow{T(\mu_x)} & T(Tx) \\ \mu_{Tx} \downarrow & & \downarrow \mu_x \\ T(Tx) & \xrightarrow{\mu_x} & Tx \end{array}$$

(associativity)

$$\begin{array}{ccccc} Tx & \xrightarrow{\eta_{Tx}} & T(Tx) & \xleftarrow{T(\eta_x)} & Tx \\ & \searrow \text{id}_{Tx} & \downarrow \mu_x & \swarrow \text{id}_{Tx} & \\ & & Tx & & \end{array}$$

(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 $T: \mathbf{P} \rightarrow \mathbf{P}$ is thus a monotonic function

$\mathbf{P} \rightarrow \mathbf{P}$ ($x \leq y \implies Tx \leq Ty$). The existence of the natural transformations η is equivalent to

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

and the existence of μ is equivalent to

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

because there is at most one morphism $x \rightarrow y$, so the necessary diagrams commute trivially.

Now suppose \mathbf{P} is a *partial order*, i.e. $x \leq y \leq x \implies x = y \quad \forall x, y \in \mathbf{P}$.

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 $T: \mathbf{P} \rightarrow \mathbf{P}$ with $x \leq Tx$ and $T(Tx) = Tx \quad \forall x \in \mathbf{P}$.

Now every topological space X induces a partial order $\mathbf{P} = (\mathcal{P}(X), \subseteq)$. Here an example for a closure operation is taking the topological closure $A \mapsto \bar{A}$, since it holds for all $A \subseteq X$ that $A \subseteq \bar{A}$ and $\bar{\bar{A}} = \bar{A}$.

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 $f: X \rightarrow Y$ we have a map $f \times \text{id}_M: X \times M \rightarrow Y \times M; (x, m) \mapsto (f(x), m)$. 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 $\eta_X: X \rightarrow X \times M; x \mapsto (x, 1)$
- The multiplication μ is defined by $\mu_X: X \times M \times M \rightarrow X \times M; (x, m, n) \mapsto (x, m \cdot n)$

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

$$\begin{array}{ccc} X \times M \times M \times M & \xrightarrow{\mu_X \times \text{id}_M} & X \times M \times M \\ \downarrow \mu_{X \times M} & & \downarrow \mu_X \\ X \times M \times M & \xrightarrow{\mu_X} & X \times M \end{array} \quad \left| \quad \begin{array}{ccc} X \times M & \xrightarrow{\eta_X \times M} & X \times M \times M \xleftarrow{\eta_X \times \text{id}_M} X \times M \\ \searrow \text{id}_{X \times M} & & \downarrow \mu_X \swarrow \text{id}_{X \times M} \\ & X \times M & \end{array} \right|$$

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 its algebras, see Section 2.2.

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

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

finish

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

- an endofunctor $L: \mathbf{A} \rightarrow \mathbf{A}$
- a natural transformation $\varepsilon: L \Rightarrow \text{id}_{\mathbf{A}}$
- a natural transformation $\omega: L \Rightarrow L^2$

such that the following diagrams commute:

$$\begin{array}{ccc} L & \xrightarrow{\omega} & L^2 \\ \omega \downarrow & & \downarrow L\omega \\ L^2 & \xrightarrow{\omega L} & L^3 \end{array}$$

(coassociativity)

$$\begin{array}{ccccc} & & L & & \\ & \swarrow \text{id}_L & \downarrow \omega & \searrow \text{id}_L & \\ L & \xleftarrow{\varepsilon L} & L^2 & \xrightarrow{L\varepsilon} & L \end{array}$$

(counitality)

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

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

(coassociativity)

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

(counitality)

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

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

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

$$\begin{array}{ccc}
 X \times E & \xrightarrow{\omega_X} & X \times E \times E \\
 \downarrow \omega_X & & \downarrow \omega_X \times \text{id}_E \\
 X \times E \times E & \xrightarrow{\omega_{X \times E}} & X \times E \times E \times E
 \end{array}
 \qquad
 \begin{array}{ccccc}
 & & X \times E & & \\
 & \swarrow \text{id}_{X \times E} & \downarrow \omega_X & \searrow \text{id}_{X \times E} & \\
 X \times E & \xleftarrow{\varepsilon_{X \times E}} & X \times E \times E & \xrightarrow{\varepsilon_X \times \text{id}_E} & X \times E
 \end{array}$$

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.

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:

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

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 $\alpha: R \rightarrow R[G]; r \mapsto r \cdot 1$ and the monoid homomorphism $\beta: G \rightarrow R[G]; g \mapsto 1 \cdot g$ 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 $\gamma: R[G] \rightarrow S$ such that the following diagram commutes:

$$\begin{array}{ccccc}
 & & S & & \\
 & \nearrow \alpha' & \uparrow \gamma & \nwarrow \beta' & \\
 R & \xrightarrow{\alpha} & R[G] & \xleftarrow{\beta} & G
 \end{array}$$

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 $\mathbb{Z} \rightarrow S$, each monoid homomorphism $G \rightarrow S$ induces a unique ring homomorphism $\mathbb{Z}G \rightarrow S$ such that the following commutes:

$$\begin{array}{ccc}
 G & \xrightarrow{\quad} & S \\
 & \searrow & \uparrow \\
 & & \mathbb{Z}G
 \end{array}$$

Now if H is another monoid and $f: G \rightarrow H$ a monoid morphism, $G \xrightarrow{f} H \rightarrow \mathbb{Z}H$ is a monoid homomorphism, hence it extends uniquely to $f: \mathbb{Z}G \rightarrow \mathbb{Z}H$, $\sum_{g \in G} r_g \cdot g \mapsto \sum_{g \in G} r_g \cdot f(g)$.

In this way, the free monoid ring construction over \mathbb{Z} is functorial.

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

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

PROOF: Define the counit and comultiplication by

$$\begin{aligned} \varepsilon_R: \mathbb{Z}R &\rightarrow R \\ \sum_{r \in R} a_r \cdot [r] &\mapsto \sum_{r \in R} a_r \cdot r \end{aligned} \qquad \begin{aligned} \omega_R: \mathbb{Z}R &\rightarrow \mathbb{Z}\mathbb{Z}R \\ \sum_{r \in R} a_r \cdot [r] &\mapsto \left[\sum_{r \in R} a_r \cdot [r] \right] \end{aligned}$$

those are clearly natural and the following diagrams commute:

$$\begin{array}{ccc} \mathbb{Z}R & \xrightarrow{\omega_x} & \mathbb{Z}\mathbb{Z}R \\ \omega_x \downarrow & & \downarrow L(\omega_x) \\ \mathbb{Z}\mathbb{Z}R & \xrightarrow{\omega_{Lx}} & \mathbb{Z}\mathbb{Z}\mathbb{Z}R \end{array} \qquad \begin{array}{ccccc} & & \mathbb{Z}R & & \\ \text{id}_{Lx} \swarrow & & \downarrow \omega_x & & \searrow \text{id}_{Lx} \\ \mathbb{Z}R & \xleftarrow{\varepsilon_{Lx}} & \mathbb{Z}\mathbb{Z}R & \xrightarrow{L(\varepsilon_x)} & \mathbb{Z}R \end{array}$$

□

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:

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

this means

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

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

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 $\delta: T \Rightarrow T'$ is a *morphism of monads* if it preserves the unit and the multiplication, i.e. the following diagrams commute:

$$\begin{array}{ccc} \text{id}_T & \xrightarrow{\eta} & T \\ & \searrow \eta' & \downarrow \delta \\ & & T' \end{array} \quad \text{(unit-preserving)}$$

$$\begin{array}{ccc} T^2 & \xrightarrow{\mu} & T \\ \delta \otimes \delta \downarrow & & \downarrow \delta \\ T'^2 & \xrightarrow{\mu'} & T' \end{array} \quad \text{(multiplication-preserving)}$$

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 $\delta: L \Rightarrow L'$ is a *morphism of monads* if it preserves the counit and the comultiplication, i.e. the following diagrams commute:

$$\begin{array}{ccc} L & \xrightarrow{\delta} & L' \\ & \searrow \varepsilon & \downarrow \varepsilon' \\ & & \text{id}_A \end{array} \quad \text{(counit-preserving)}$$

$$\begin{array}{ccc} L & \xrightarrow{\omega} & L^2 \\ \downarrow \delta & & \downarrow \delta \otimes \delta \\ L' & \xrightarrow{\omega'} & L'^2 \end{array} \quad \text{(comultiplication-preserving)}$$

Example 11. Consider the *subsingletons monad* $\mathbb{P}^1: \mathbf{Set} \rightarrow \mathbf{Set}$, 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 $f: X \rightarrow Y$, 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

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

and the multiplication μ' by

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

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

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

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

The following theorem gives us a way to create many examples of monads and comonads. It was first proven in [Hub61].

Theorem 2.9 (Every adjunction induces a monad and a comonad) *Let $F \overset{\eta}{\underset{\varepsilon}{\dashv}} G: \mathbf{B} \rightleftarrows \mathbf{A}$ 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.

$$\begin{array}{ccc}
 GF\,GF\,GF & \xrightarrow{GF\,G\varepsilon\,F} & GF\,GF \\
 \Downarrow G\varepsilon\,FGF & & \Downarrow G\varepsilon\,F \\
 GF\,GF & \xrightarrow{G\varepsilon\,F} & GF
 \end{array}
 \qquad
 \begin{array}{ccc}
 FG\,FG & \xrightarrow{FG\,\varepsilon} & FG \\
 \Downarrow \varepsilon\,FG & & \Downarrow \varepsilon \\
 FG & \xrightarrow{\varepsilon} & \text{id}_B
 \end{array}$$

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

$$\begin{array}{ccccc}
 GF & \xrightarrow{\eta\,GF} & GF\,GF & \xleftarrow{GF\,\eta} & GF \\
 \searrow \text{id}_{GF} & & \Downarrow G\varepsilon\,F & & \swarrow \text{id}_{GF} \\
 & & GF & &
 \end{array}$$

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. \square

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* due to S. Eilenberg and J. Moore in [EM65]. 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 $h: Tx \rightarrow x$ is an arrow such that the following diagrams commute:

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

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

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

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 .

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

$$\begin{array}{ccc} X \times M \times M & \xrightarrow{h \times id_M} & X \times M \\ \downarrow \mu_X & & \downarrow h \\ X \times M & \xrightarrow{h} & X \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{\eta_x} & X \times M \\ & \searrow id_x & \downarrow h \\ & & X \end{array}$$

commute. If we denote $h(x, m)$ by $(x.m)$, this means that $(x.m).n = x.(m \cdot n)$ and $x.1 = x$. 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.

Example 13 (preorder). If $T: \mathbf{P} \rightarrow \mathbf{P}$ is a monotonic function viewed as a monad, then a T -algebra is an object $x \in \mathbf{P}$ with $Tx \leq x$. Since $x \leq Tx$, it follows that $x = Tx$, which means that a T -algebra is just a *closed element* in \mathbf{P} . In particular, if we consider $A \mapsto \bar{A}$ in a topological space, the T -algebras are exactly the closed sets.

Example 14 (Maybe monad). The category of Y -algebras is isomorphic to the category of pointed spaces \mathbf{Set}_* . Indeed: by definition, a Y -algebra is a pair (X, h) where $h: X \cup \{*\} \rightarrow X$ and since

$$\begin{array}{ccc} X & \xrightarrow{\eta_x} & X \cup \{*\} \\ & \searrow id_x & \downarrow h \\ & & X \end{array}$$

commutes, $h|_X = \text{id}_X$. Now define $F: \mathbf{Set}^Y \rightarrow \mathbf{Set}_*$ by

$$\begin{aligned} (X, h) &\mapsto (X, h(*)) \\ f: (X, h) &\rightarrow (Y, i) \mapsto f: (X, h(*)) \rightarrow (Y, i(*)) \end{aligned}$$

and define $G: \mathbf{Set}_* \rightarrow \mathbf{Set}^Y$ by

$$\begin{aligned} (X, x) &\mapsto (X, \text{id}_X^x) \\ f: (X, x) &\rightarrow (Y, y) \mapsto f: (X, \text{id}_X^x) \rightarrow (Y, \text{id}_Y^y) \end{aligned}$$

where $\text{id}_X^x: X \cup \{*\} \rightarrow X$ is the identity on X and maps $*$ to x .

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 $F^T \dashv G^T: \mathbf{X} \rightleftarrows \mathbf{X}^T$ such that the monad induced by this adjunction is (T, η, μ) .*

PROOF: • Define $F^T: \mathbf{X} \rightarrow \mathbf{X}^T$ by

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

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

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

are just the commuting diagrams for the associativity respectively left unitality axioms from the definition of a monad.

$Tf: (Tx, \mu_x) \rightarrow (Tx', \mu_{x'})$ is indeed a morphism of T -algebras, since the commutativity of

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

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

- Define $G^T: \mathbf{X}^T \rightarrow \mathbf{X}$ 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 $f: x \rightarrow y$. Then $G^T(F^T(f)) = G^T(Tf) = Tf$. Finally, $F^T G^T(x, h) = F^T(x) = (Tx, \mu_x)$. \square

- So we can set

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

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

$$\varepsilon_{(x, h)}^T := h: (Tx, \mu_x) \rightarrow (x, h).$$

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 $f: (x, h) \rightarrow (x', h')$ 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.

- To show the triangle identity, we have to show that

$$\begin{array}{ccc} Tx & \xrightarrow{T\eta_x} & T^2x \\ & \searrow \text{id}_{Tx} & \downarrow \mu_x \\ & & Tx \end{array}$$

$$\begin{array}{ccc} x & \xrightarrow{\eta_x} & Tx \\ & \searrow \text{id}_x & \downarrow h \\ & & x \end{array}$$

commute, but the first diagram commutes by the right unitality law for the monad T , the second one commutes, since (x, h) is a T -algebra.

- The induced monad of the adjunction now has unit η^T and multiplication $\mu^T = G^T \varepsilon^T F^T$. But $G^T F^T = T$ and $\eta^T = \eta$ is already shown and $\mu_x^T = (G^T \varepsilon^T)_{F^T x} = (G^T \varepsilon^T)_{(Tx, \mu_x)} = G^T(\mu_x) = \mu_x$.

□

Theorem 2.12 (Comparison of adjunctions with algebras) *Let $F \overset{\eta}{\dashv} G: \mathbf{X} \rightleftarrows \mathbf{A}$ be an adjunction, $T = (GF, \eta, G\eta F)$ the monad it defines in \mathbf{X} . Then there is unique functor $K: \mathbf{A} \rightarrow \mathbf{X}^T$ such that the following diagrams commute:*

$$\begin{array}{ccc} \mathbf{A} & & \mathbf{A} \\ \downarrow G & \searrow K & \uparrow F \\ \mathbf{X} & \xleftarrow{G^T} \mathbf{X}^T & \xrightarrow{F^T} \mathbf{X}^T \end{array}$$

PROOF: Existence: For $f: a \rightarrow a'$ in \mathbf{A} we define K by:

$$\begin{aligned} Ka &= (Ga, G(\varepsilon_a)) \\ Kf &= Gf: (Ga, G(\varepsilon_a)) \rightarrow (Ga', G(\varepsilon_{a'})) \end{aligned}$$

We have to show that this is well-defined.

CLAIM 0. Ka is a T -algebra.

Proof of claim. Ka is the arrow $GF GF a \xrightarrow{G(\varepsilon_a)} Ga$ and we need to show that the following diagrams commute:

$$\begin{array}{ccc} GF GF a & \xrightarrow{GF(\varepsilon_a)} & GF Ga \\ \downarrow G(\varepsilon_{FGa}) & & \downarrow G(\varepsilon_a) \\ GF Ga & \xrightarrow{G(\varepsilon_a)} & Ga \end{array} \qquad \begin{array}{ccc} Ga & \xrightarrow{\eta_{Ga}} & GF Ga \\ \searrow \text{id}_{Ga} & & \downarrow G(\varepsilon_a) \\ & & Ga \end{array}$$

The second diagram is just one of the triangle identity for the adjunction. The first diagram is the image under G of:

$$\begin{array}{ccc} FG FG a & \xrightarrow{FG(\varepsilon_a)} & FG a \\ \downarrow \varepsilon_{FGa} & & \downarrow \varepsilon_a \\ FG a & \xrightarrow{\varepsilon_a} & a \end{array}$$

which commutes by 2.6.

//

CLAIM 1. Kf is a morphism of T -algebras.

Proof of claim 1. We have to show that the first of the following two diagrams commutes:

$$\begin{array}{ccc}
 GFGa & \xrightarrow{G(\varepsilon_a)} & Ga \\
 \downarrow GFG(f) & & \downarrow G(f) \\
 GFGa' & \xrightarrow{G(\varepsilon_{a'})} & Ga'
 \end{array}
 \qquad
 \begin{array}{ccc}
 FGa & \xrightarrow{\varepsilon_a} & a \\
 \downarrow FG(f) & & \downarrow f \\
 FGa' & \xrightarrow{\varepsilon_{a'}} & a'
 \end{array}$$

but the first diagram is the image of the second diagram under G , which commutes by naturality of $\varepsilon: FG \Rightarrow \text{id}_A$. //

Functoriality of K follows from the Functoriality of G . For the commutativity of the two diagrams, let $f: a \rightarrow a'$ and $g: x \rightarrow x'$ be morphisms. Then the first diagram commutes, since we have:

$$\begin{aligned}
 G^T K a &= G^T (Ga, G(\varepsilon_a)) = Ga \\
 G^T K(f) &= G^T (Gf) = Gf
 \end{aligned}$$

and for the second diagram we compute:

$$\begin{aligned}
 KF x &= (Gf x, G(\varepsilon_{Fx})) = (Tx, \mu_x) = F^T x \\
 KF(g) &= GF(g) = T(g) = F^T(g)
 \end{aligned}$$

CLAIM 2. K is unique.

finish,v

Proof of claim 2.

//

□

2.3 The Kleisli category of a monad

There is another way to induce a monad by an adjunction, which was introduced by H.Kleisli in [Kle65]:

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 $x_T, y_T \in \mathbf{X}_T$, $f: x \rightarrow Ty$ is a morphism which we denote by $f^b: x_T \rightarrow y_T$.
- composition will be denoted by \bullet for distinction and is defined by

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

for $f^b: x_T \rightarrow y_T$, $g^b: y_T \rightarrow z_T$. This is indeed again a morphism:

$$x \xrightarrow{f} Ty \xrightarrow{Tg} T^2z \xrightarrow{\mu_z} Tz$$

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.

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

Now the associativity axiom for the monad T states that

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

commutes, hence

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

By naturality of μ , the diagram

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

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 $f^b: x_T \rightarrow y_T$ be a morphism.

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

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

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

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

Theorem 2.14 *Let (T, η, μ) be a monad in a category X . Then there is an adjunction $F_T \dashv G_T: X \rightleftarrows X_T$ such that the monad induced by this adjunction is (T, η, μ) .*

PROOF: • Define $F_T: X \rightarrow X_T$ by

$$\begin{aligned} x &\mapsto x_T \\ f: x \rightarrow y &\mapsto (Tf \circ \eta_x)^b: x_T \rightarrow y_T \end{aligned}$$

Then $F_T(\text{id}_x) = (\eta_x)^b$, which is the identity on x_T . Now

$$F_T(g \circ f) = (T(g \circ f) \circ \eta_x)^b = (Tg \circ Tf \circ \eta_x)^b$$

$$\begin{aligned} F_T(g) \bullet F_T(f) &= (Tg \circ \eta_y)^b \bullet (Tf \circ \eta_x)^b && \text{(Definition of } F_T) \\ &= (\mu_z \circ T(Tg \circ \eta_y) \circ Tf \circ \eta_x)^b && \text{(Definition of Kleisli composition)} \\ &= (\mu_z \circ T^2 g \circ T\eta_y \circ Tf \circ \eta_x)^b && \text{(Functoriality of } T) \\ &= (Tg \circ \mu_z \circ T\eta_y \circ Tf \circ \eta_x)^b && \text{(Naturality of } \mu) \\ &= (Tg \circ Tf \circ \eta_x)^b && \text{(right unitality law for } T) \end{aligned}$$

This proves that F_T is a functor.

- Define $G_T: X_T \rightarrow X$ by

$$\begin{aligned} x_T &\mapsto Tx \\ f^b: x_T \rightarrow y_T &\mapsto \mu_y \circ Tf: Tx \rightarrow Ty \end{aligned}$$

Then $G_T(\text{id}_{x_T}) = G_T(\eta_x^b) = \mu_x \circ T\eta_x = \text{id}_x$ by the right unitality law for T . Now we compute that

$$\begin{aligned} G_T(g^b \bullet f^b) &= G_T((\mu_z \circ Tg \circ f)^b) = \mu_z \circ T\mu_z \circ T^2g \circ Tf \\ G_T(g^b) \circ G_T(f^b) &= \mu_z \circ Tg \circ \mu_z \circ Tf \end{aligned}$$

so it suffices to show that the following diagram commutes:

$$\begin{array}{ccccccc} Tx & \xrightarrow{Tf} & T^2y & \xrightarrow{T^2g} & T^3z & \xrightarrow{T\mu_z} & T^2z \\ \downarrow Tf & & & & & & \downarrow \mu_z \\ T^2y & \xrightarrow{\mu_y} & Ty & \xrightarrow{Tg} & T^2z & \xrightarrow{\mu_z} & Tz \end{array}$$

But we can fill it in to get the following:

$$\begin{array}{ccccccc} Tx & \xrightarrow{Tf} & T^2y & \xrightarrow{T^2g} & T^3z & \xrightarrow{T\mu_z} & T^2z \\ \downarrow Tf & (1) & \downarrow \mu_y & (2) & \downarrow \mu_{Tz} & (3) & \downarrow \mu_z \\ T^2y & \xrightarrow{\mu_y} & Ty & \xrightarrow{Tg} & T^2z & \xrightarrow{\mu_z} & Tz \end{array}$$

where (1) commutes trivially, (2) by naturality of μ and (3) by the associativity of T .

CLAIM. $G_T F_T = T$.

Proof of claim 2.

$$\begin{aligned} G_T(F_T(x)) &= G_T(x_T) = Tx \\ G_T(F_T(f)) &= G_T((Tf \circ \eta_x)^b) = \mu_y \circ T^2f \circ T\eta_x \\ &= \mu_y \circ T\eta_y \circ Tf && \text{(naturality of } \eta) \\ &= Tf && \text{(unitality of } T) \end{aligned}$$

//

- We now set the unit and counit to be

def. of eps?

$$\begin{aligned} \eta_x &: x \rightarrow Tx \\ \varepsilon_x &= \text{id}_{Tx}^b: (Tx)_T \rightarrow x_T \end{aligned}$$

We need to show that η and ε satisfy the triangle identities:

$$\begin{array}{ccc}
 F_T x & \xrightarrow{F_T(\eta_x)} & F_T G_T F_T x \\
 & \searrow \text{id}_{F_T x} & \downarrow \varepsilon_{F_T x} \\
 & & F_T x
 \end{array}
 \qquad
 \begin{array}{ccc}
 G_T x & \xrightarrow{\eta_{G_T x}} & G_T F_T G_T x \\
 & \searrow \text{id}_{G_T x} & \downarrow G_T(\varepsilon_x) \\
 & & G_T x
 \end{array}$$

the left diagram commutes, since we have

$$\begin{aligned}
 \varepsilon_{F_T x} \bullet F_T(\eta_x) &= (\text{id}_{T_x})^b \bullet (T\eta_x \circ \eta_x)^b = (\mu_x \circ T(\text{id}_{T_x}) \circ T\eta_x \circ \eta_x)^b \\
 &= (\mu_x \circ T\eta_x \circ \eta_x)^b = (\eta_x)^b = \text{id}_{F_T x}
 \end{aligned}$$

using the right unitality of T . The right diagram commutes, since we have

$$G_T(\varepsilon_x) \circ \eta_{G_T x} = \mu_x \circ T(\text{id}_{T_x}) \circ \eta_{T_x} = \mu_x \circ \eta_{T_x} = \text{id}_{T_x}$$

using the left unitality of T . The only thing left to show is that $\mu = G_T \varepsilon F_T$:

$$G_T(\varepsilon_{F_T x}) = G_T(\varepsilon_{x_T}) = G_T(\text{id}_{T_x}^b) = \mu_x \circ T(\text{id}_{T_x}) = \mu_x$$

□

Theorem 2.15 (Comparison of adjunctions with the Kleisli-construction) *Let $F \xrightarrow[\varepsilon]{\eta} G$ be an adjunction, $T = (GF, \eta, G\eta F)$ the monad it defines in \mathbf{X} . Then there is a unique functor $L: \mathbf{X}_T \rightarrow \mathbf{A}$ such that the following diagrams commute:*

PROOF: • Define L by

$$\begin{aligned}
 x_T &\mapsto Fx \\
 f^b: x_t \rightarrow y_t &\mapsto \varepsilon_{Fy} \circ F(f): Fx \rightarrow FGFy \rightarrow Fy
 \end{aligned}$$

- $L(\text{id}_{x_t}) = L(\eta_x^b) = \varepsilon_{Fx} \circ F(\eta_x) = \text{id}_{Fx}$ by the triangle identity of the adjunction.
- Let $x_T \xrightarrow{f} y_T \xrightarrow{g} z_T$.

$$\begin{aligned}
 L(g \bullet f) &= \varepsilon_{Fz} \circ F(\mu_z \circ GF(g) \circ f) = \varepsilon_{Fz} \circ F(\mu_z) \circ FGF(g) \circ F(f) \\
 L(g) \circ L(f) &= \varepsilon_{Fz} \circ Fg \circ \varepsilon_{Fy} \circ F(f)
 \end{aligned}$$

so we have to show that the following diagram commutes:

$$\begin{array}{ccccccc}
 Fx & \xrightarrow{F(f)} & FGFy & \xrightarrow{FGF(g)} & FGFGFz & \xrightarrow{F(\mu_z)} & FGFz \\
 \downarrow F(f) & & & & & & \downarrow \varepsilon_{Fz} \\
 FGFy & \xrightarrow{\varepsilon_{Fy}} & Fy & \xrightarrow{F(g)} & FGFz & \xrightarrow{\varepsilon_{Fz}} & Fz
 \end{array}$$

but we can fill in the counit morphisms:

$$\begin{array}{ccccccc}
 Fx & \xrightarrow{F(f)} & FGFy & \xrightarrow{FGF(g)} & FGFGFz & \xrightarrow{F(\mu_z)} & FGFz \\
 \downarrow F(f) & (1) & \downarrow \varepsilon_{Fy} & (2) & \downarrow \varepsilon_{FGFz} & (3) & \downarrow \varepsilon_{Fz} \\
 FGFy & \xrightarrow{\varepsilon_{Fy}} & Fy & \xrightarrow{F(g)} & FGFz & \xrightarrow{\varepsilon_{Fz}} & Fz
 \end{array}$$

and now (1) commutes trivially, while (2) and (3) commute by naturality of ε since $\mu_z = G(\varepsilon_{Fz})$.

- Commutativity of the diagrams: Let $f: x \rightarrow y$.

$$\begin{aligned}
 GLx_T &= GFx = Tx = G_Tx_T \\
 GL(f^b) &= G(\varepsilon_{Fy} \circ F(f)) = G(\varepsilon_{Fy}) \circ GF(f) = \mu_y \circ T(f) = G_T(F^b) \\
 LF_Tx &= Lx_T = Fx \\
 LF_T(f) &= L((T(f) \circ \eta_x)^b) = \varepsilon_{Fy} \circ F(T(f) \circ \eta_x) = \varepsilon_{Fy} \circ FGF(f) \circ F(\eta_x) \\
 &= F(f) \circ \varepsilon_{Fx} \circ F(\eta_x) && \text{(naturality of } \varepsilon \text{)} \\
 &= F(f) \circ \text{id}_{Fx} = F(f) && \text{(triangle identity)}
 \end{aligned}$$

- Uniqueness: Let L' be another functor making the diagrams commute. Then since F_T is surjective on objects we have

$$L'F_T = F \Rightarrow L'x_T = Fx = Lx_T \text{ for all objects } x_T$$

and for $f^b: x_T \rightarrow y_T$ we can precompose with the identity to see that

$$\begin{aligned}
 L'(f^b) &= L'(f^b) \circ \text{id}_{L'x} = L'(f^b) \circ \varepsilon_{Fx} \circ F(\eta_x) && \text{(triangle identity)} \\
 &= \varepsilon_{Fy} \circ FGL'(f^b) \circ F(\eta_x) = \varepsilon_{Fy} \circ FG_T(f^b) \circ F(\eta_x) \\
 &= \varepsilon_{Fy} \circ F(\mu_y \circ T(f)) \circ F(\eta_x) = \varepsilon_{Fy} \circ F(\mu_y) \circ FGF(f) \circ F(\eta_x) \\
 &= \varepsilon_{Fy} \circ F(\mu_y) \circ F(\eta_{GFy}) \circ F(f) && \text{(naturality of } \eta \text{)} \\
 &= \varepsilon_{Fy} \circ F(\mu_y \circ \eta_{GFy}) \circ F(f) \\
 &= \varepsilon_{Fy} \circ F(f) = L(f^b) && \text{(triangle identity)}
 \end{aligned}$$

□

3 Witt vectors

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

3.1 Construction of the Witt vectors

Definition 3.1 (truncation set). Let \mathbb{N} be the set of positive integers and let $S \subseteq \mathbb{N}$ be a subset with the property that $\forall n \in \mathbb{N} : \text{if } d \text{ is a divisor of } n, \text{ then } d \in S$. We then say that S is a *truncation set*.

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

Definition 3.2 (ghost map). We define $w: \mathbb{W}_S(A) \rightarrow A^S$ by $(a_n)_{n \in S} \mapsto (w_n)_{n \in S}$ where

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

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

Definition 3.3 (p-adic valuation). $v_p: \mathbb{Z} \rightarrow \mathbb{N} \cup \{\infty\}$ is defined by

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

Lemma 3.4 *Let A be a ring, $a, b \in A$, $v \in \mathbb{N}$, and p a prime number. Then:*

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

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

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

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

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

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

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

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

It follows that

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

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

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

Lemma 3.5 (Dwork) *Suppose that for every prime number p there exists a ring homomorphism $\phi_p: A \rightarrow A$ with the property that $\phi_p(a) \equiv a^p$ modulo pA . Then for every sequence $x = (x_n)_{n \in S}$, the following are equivalent:*

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

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

PROOF: (\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:

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

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

$$\sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) \equiv \sum_{d|n/p} d \cdot a_d^{n/d} \quad \text{mod } p^{v_p(n)}A \quad (3.1)$$

$$\equiv \sum_{d|n} d \cdot a_d^{n/d} \quad \text{mod } p^{v_p(n)}A \quad (3.2)$$

so we get

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

Proof of (3.1). First, note that

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

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

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

using Lemma 3.4 for the last congruence. Now (*) and the fact that

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

gives us

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

But

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

so it follows that for every d

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

which implies (1). \square

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 $d \equiv 0 \pmod{p^{v_p(n)}A}$. \square

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

$$a_1 := x_1$$

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

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

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

$$\begin{aligned} \sum_{d \mid n/p} d \cdot \phi(a_d^{n/pd}) &\stackrel{(3.1)}{\equiv} \sum_{d \mid n/p} d \cdot a_d^{n/d} \pmod{p^{v_p(n)}A} \\ &\stackrel{(3.2)}{\equiv} \sum_{d \mid n} d \cdot a_d^{n/d} \pmod{p^{v_p(n)}A} \\ &\equiv \sum_{d \mid n, d \neq n} d \cdot a_d^{n/d} \pmod{p^{v_p(n)}A} \end{aligned}$$

In conclusion:

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

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

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

hence $\exists a_n \in A$ such that

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

□

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

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

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*

$$w : W_S(A) \rightarrow A^S$$

is a natural transformation of functors from rings to rings.

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

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

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

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

Proof of claim. Since we can use Lemma 3.5, it suffices to show that for all prime p , for all $n \in S$ with $p \mid n$:

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

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

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

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

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

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

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

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

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

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

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

ok so?

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

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

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

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

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

finish

□

Corollary 3.8 $w_n: \mathbb{W}_S(A) \rightarrow A$ 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 $\mathbf{CRing} \rightarrow \mathbf{CRing}$.

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

ring homomorphism $f: A \rightarrow B$, $\mathbb{W}_S(f): \mathbb{W}_S(A) \rightarrow \mathbb{W}_S(B)$ is again a ring homomorphism.

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

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

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

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

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

□

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*

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

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

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

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

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

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

is that obvious?

Lemma 3.13 *The Verschiebung map V_n is additive.*

PROOF:

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

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

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

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

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 $d \in S$:

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

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

//

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

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

commutes, we calculate:

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

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

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

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

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

□

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

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

Lemma 3.14 (Frobenius homomorphism) *There exists a unique natural ring homomorphism*

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

such that the diagram

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

commutes.

We call F_n the *nth Frobenius homomorphism*. The commutativity of the diagram above is

remark und
definition
haben ande-
re font

equivalent to commutativity of the following diagram for every $d \in S/n$:

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

Proof of Lemma 3.14. We construct F_n similar to the construction of the ring operations on $\mathbb{W}_S(A)$ 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 $\tilde{F}_n(w(a)) \in A^{S/n}$ is in the image of a unique element

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

by the ghost map. (Indeed: we have

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

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

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

where $g: A \rightarrow A'$ is the unique ringhomomorphism that maps a to a' . Now since \tilde{F}_n is clearly a ring homomorphism, we can argue similar as in the proof of Lemma 3.13 to show that F_n is a ring homomorphism. Finally, we show that F_n is natural. For that, let $f: A \rightarrow B$ be a ring homomorphism. Then we need to show that

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

naturality

commutes, but it again suffices to show that it commutes after evaluating the ghost

coordinates, i.e. we can look at the following diagram:

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

w_{nd} (left) w_{nd} (right)

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

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

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

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

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

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

then we have the following commuting diagram:

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

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

Lemma 3.16 $F_1 = \text{id}: W_S(A) \rightarrow W_S(A)$.

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

Definition 3.17 (teichmüller representative). The *teichmüller representative* is the map

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

defined by

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

Lemma 3.18 The teichmüller map is multiplicative.

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

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

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

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 $\mathbb{W}_n(A) \cong A$ via w . Now for the induction step, let $n \in S$ be maximal and let $T = S - \{n\}$. Then $S/n = \{1\}$ and therefore we have a short exact sequence

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

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

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

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

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

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

p-typical Witt vectors, big Witt vectors

For the construction of a natural transformation $\mathbb{W}(A) \rightarrow \mathbb{W}(\mathbb{W}(A))$ we want to use Lemma 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 $F_p: \mathbb{W}(A) \rightarrow \mathbb{W}(A)$ satisfies $F_p(a) \equiv a^p \pmod{pA}$.*

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

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

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

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

indeed

using Lemma 3.14. This is now congruent to 0 mod pA :

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

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

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 $\phi_l: A \rightarrow A$ which maps a_n to a_n^l . It satisfies $\phi_l(f) \equiv f^l \pmod{lA}$. (indeed:).

indeed

so by Lemma 3.5 it suffices to show:

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

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

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

and

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

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

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

and for $l \neq p$:

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

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

Then:

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

using Lemma 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

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

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

Proposition 3.23 *There exists a unique natural transformation*

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

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

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

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

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

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

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

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

Theorem 3.24 *The functor $\mathbb{W}(-): \text{CRing} \rightarrow \text{CRing}$ together with the natural transformations $\Delta: \mathbb{W} \Rightarrow \mathbb{W}^2, w_1: \mathbb{W} \Rightarrow \text{id}_{\text{CRing}}$ form a comonad $(\mathbb{W}, w_1, \Delta)$.*

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

always and then consider the following cube:

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

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

CLAIM.

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

Proof of claim. evaluating the ghost coordinates leads to:

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

which by Proposition 3.23 simplifies to

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

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

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

evaluating the ghost coordinates again, keeping in mind that by 3.20 and 3.6, $w: \mathbb{W}(\mathbb{W}(A)) \rightarrow \mathbb{W}(A)^{\mathbb{N}}$ is injective as well, we get

$$\begin{array}{ccc} \mathbb{W}(A) & \xrightarrow{(F_n)_A} & \mathbb{W}(A) \\ \downarrow \Delta_A & & \downarrow \Delta_A \\ \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{(F_n)_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(A)) \\ \vdots \downarrow w & & \downarrow w \\ \mathbb{W}(A)^{\mathbb{N}} & \xrightarrow{(\tilde{F}_n)_{\mathbb{W}(A)}} & \mathbb{W}(A)^{\mathbb{N}} \end{array} \quad \begin{array}{c} \text{dotted arrow } F_A \text{ from } \mathbb{W}(A) \text{ to } \mathbb{W}(A)^{\mathbb{N}} \\ \text{dotted arrow } \epsilon \text{ from } \mathbb{W}(\mathbb{W}(A)) \text{ to } \mathbb{W}(A)^{\mathbb{N}} \end{array}$$

using the fact that $\begin{array}{ccc} \mathbb{W}(\mathbb{W}(A)) & & \\ \downarrow w & \searrow w_{nm} & \\ \mathbb{W}(A)^{\mathbb{N}} & \xrightarrow{(\tilde{F}_n)_{\mathbb{W}(A)}} & \mathbb{W}(A)^{\mathbb{N}} \end{array}$ commutes, we can simplify the situation to

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

which can again be simplified to

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

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

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

Proof of claim. evaluate the ghost coordinates:

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

we can then simplify to

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

now it suffices to show for all n that

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

commutes, which is true by Lemma 3.14. //

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

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

$w_1(\Delta_A(a)) = F_1(a) = a$, since $F_1 = \text{id}_{\mathbb{W}(A)}$ by Lemma 3.16. //

This concludes the proof. □

3.4 The Teichmüller map induces a morphism of comonads

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

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

Theorem 3.25 $\tau: \mathbb{Z}A \rightarrow \mathbb{W}(A)$ is a morphism of comonads.

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

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

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

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

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

?

□

Literature

- [Bén67] Jean Bénabou. „Introduction to bicategories“. In: (1967) (siehe S. 6).
- [Car67] Pierre Cartier. „Groupes formels associés aux anneaux de Witt généralisés“. In: *Compt. Rend. Acad. Sc. Paris* 265 (1967). Sér. A, juillet, A129-132 (siehe S. 24).
- [EM65] Samuel Eilenberg und John C Moore. „Adjoint functors and triples“. In: *Illinois Journal of Mathematics* 9.3 (1965) (siehe S. 13).
- [God58] Roger Godement. *Topologie algébrique et théorie des faisceaux*. Publications de l’institut de mathématique de l’Université de Strasbourg 13. Paris: Hermann, 1958 (siehe S. 6).
- [Haz09] Michiel Hazewinkel. „Witt vectors. I“. In: *Handbook of algebra. Vol. 6*. Bd. 6. Handb. Algebr. Elsevier/North-Holland, Amsterdam, 2009, S. 319–472. DOI: 10.1016/S1570-7954(08)00207-6. URL: [https://doi.org/10.1016/S1570-7954\(08\)00207-6](https://doi.org/10.1016/S1570-7954(08)00207-6) (siehe S. 24).
- [Hes08] Lars Hesselholt. *Lecture Notes on Witt vectors*. 2008 (siehe S. 24).
- [Hes15] Lars Hesselholt. *The big de Rham-Witt complex*. Bd. 214. 1. 2015, S. 135–207 (siehe S. 24).
- [HST14] D. Hofmann, G.J. Seal und W. Tholen. *Monoidal Topology: A Categorical Approach to Order, Metric and Topology*. Encyclopedia of Mathematics and its Applications. Cambridge University Press, 2014. ISBN: 9781107063945. URL: <https://books.google.de/books?id=yIj2AwAAQBAJ> (siehe S. 6).
- [Hub61] Peter J. Huber. „Homotopy theory in general categories“. In: *Mathematische Annalen* 144 (1961) (siehe S. 6, 12).
- [Kan58] Daniel M. Kan. „Adjoint functors“. In: *Trans. Amer. Math. Soc.* 87 (1958), S. 294–329. URL: <https://doi.org/10.2307/1993102> (siehe S. 1).
- [Kle65] Heinrich Kleisli. „Every Standard Construction is Induced by a Pair of Adjoint Functors“. In: *Proceedings of the American Mathematical Society* 16.3 (1965) (siehe S. 18).
- [Mac98] Saunders Mac Lane. *Categories for the working mathematician*. 2. Aufl. Bd. 5. Graduate Texts in Mathematics. Springer-Verlag, New York, 1998 (siehe S. 6).
- [Per21] Paolo Perrone. *Notes on Category Theory with examples from basic mathematics*. 2021. arXiv: 1912.10642v6 [math.CT] (siehe S. 6).
- [Rab14] Joseph Rabinoff. *The Theory of Witt Vectors*. 2014. arXiv: 1409.7445 [math.NT] (siehe S. 24).

- [Rie17] Emily Riehl. *Category theory in context*. Aurora: Dover modern math originals. Dover Publications, 2017. ISBN: 978-0-486-82080-4 (siehe S. 4).
- [Ser79] Jean-Pierre Serre. *Local Fields*. Bd. 67. Graduate Texts in Mathematics. Springer-Verlag, New York-Berlin, 1979 (siehe S. 24).
- [Wit37] Ernst Witt. „Zyklische Körper und Algebren der Charakteristik p vom Grad p^n . Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p .“ In: *Journal für die reine und angewandte Mathematik* 1937.176 (1937), S. 126–140. DOI: doi:10.1515/crll.1937.176.126. URL: <https://doi.org/10.1515/crll.1937.176.126> (siehe S. 24).