1 Witt vectors

1.1 Construction of the witt vectors

1.1.1 Definition (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.

1.1.2 Definition (ghost map) We define $w\colon \mathbb{W}_S(A) \longrightarrow A^S$ by $(a_n)_{n\in S} \mapsto (w_n)_{n\in S}$ where

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

1.1.3 Lemma (Dwork) Suppose that for every prime number p there exists a ring homomorphism $\phi_p\colon A \longrightarrow A$ 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 $w\colon \mathbb{W}_S(A) \longrightarrow A^S$.

(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 $d \in \mathbb{N}$.

Claim 1. $\sum_{d|n/p} d \cdot \phi(a_d^{n/pd}) \equiv \sum_{d|n/p} d \cdot a_d^{n/d} \qquad mod\ p^{v_p(n)}A.$

Proof (Proof of claim 1):

Claim 2. $\sum_{d|n/p} d \cdot a_d^{n/d} \equiv \sum_{d|n} d \cdot a_d^{n/d} \qquad mod\ p^{v_p(n)}A$

Proof (Proof of claim 2):

so we get

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

$(\Leftarrow)$ 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 $w_n(a) = x_n$ 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

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

finish proof

□

We will often need the following

1.1.4 Lemma if A is a torsion-free ring, the ghost map is injective.

Now we can finish the construction of the Witt vectors:

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

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

is a natural transformation of functors from rings to rings.

Proof: □

1.1.6 Corollary $w_n : \mathbb{W}_S(A) \longrightarrow A$ is a natural transformation for all $n \in S$.

1.1.7 Proposition $\mathbb{W}_S$ is a functor **CRing** $\longrightarrow$ **CRing**.

1.2 The Verschiebung, Frobenius and Teichmüller maps

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

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

is again a truncation set.

1.2.1 Definition (Verschiebung) Define

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

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

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

1.2.2 Lemma The Verschiebung map V_n is additive.

1.3 The comonad structure of witt vectors

We will need the following lemma:

1.3.1 Lemma 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 (Proof of claim):

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

which we can extend to the following commutative diagram:

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

finish

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

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

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

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

1.3.5 Theorem 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.

Proof:

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

Proof (Proof of claim): evaluating the ghost coordinates leads to:

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

which simplifies to

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

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

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

evaluating the ghost coordinates again, keeping in mind that by Lemma 9, $w\colon \mathbb{W}(\mathbb{W}(A)) \to \mathbb{W}(A)^{\mathbb{N}}$ is injective as well, we get

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

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

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

which can again be simplified to

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

now this commutes by ???, hence we are finished. //

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

Proof (Proof of claim): evaluate the ghost coordinates:

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

we can then simplify to

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

now it suffices to show for all n that

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

commutes, which is true by ??? ($\varepsilon = w_1$).

//

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

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

This concludes the proof. □

1.4 The Teichmüller map induces a morphism of comonads

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

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

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

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

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

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

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

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

Let $G\colon \mathbf{CRing} \to \mathbf{CMon}$ be the forgetful functor and let $F\colon \mathbf{CMon} \to \mathbf{CRing}$ be the *free monoid ring functor*, $M \mapsto \mathbb{Z}M$.

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

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