# 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 $w \colon \mathbb{W}_S(A) \to A^S$ by $(a_n)_{n \in S} \mapsto (w_n)_{n \in S}$ where

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

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

(i) The sequence $x$ is in the image of the ghost map $w \colon \mathbb{W}_S(A) \to A^S$.

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

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

**PROOF**: ($\Rightarrow$) Suppose $x$ is in the image of the ghost map, that means there is a sequence $a = (a_n)_{n \in S}$ such that $x_n = w_n(a)$ for all $n \in S$. We calculate:

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

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

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

**PROOF** (Proof of claim 1): _____ //

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

**PROOF** (Proof of claim 2): _____ //

so we get

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

($\Leftarrow$) 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

$$x_n \equiv \phi_p(x_{n/p}) \qquad mod \; p^{v_p(n)} A$$
$$= \phi_p(\sum_{d \mid n/p} d \cdot a_d^{n/pd})$$
$$= \sum_{d \mid n/p} d \cdot \phi(a_d^{n/pd})$$

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

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

is a natural transformation of functors from rings to rings.

PROOF:

□

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

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

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

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

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

**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):

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

which we can extend to the following commutative diagram:

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

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 $F_p(a) \equiv a^p \bmod pA$.

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

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

$$
\begin{array}{ccccc}
& & F_A & & \\
\mathbb{W}(A) & \xrightarrow{\Delta_A} & \mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\ \ w\ \ } & \mathbb{W}(A)^{\mathbb{N}} \\
\Big\downarrow{\scriptstyle \Delta_A} & & \Big\downarrow{\scriptstyle \mathbb{W}(\Delta_A)} & & \Big\downarrow{\scriptstyle \Delta_A^{\mathbb{N}}} \\
\mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\Delta_{\mathbb{W}(A)}} & \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) & \xrightarrow{\ \ w\ \ } & \mathbb{W}(\mathbb{W}(A))^{\mathbb{N}} \\
& & F_{\mathbb{W}_A} & &
\end{array}
$$

which simplifies to

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

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

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

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

$$
\begin{array}{ccc}
\mathbb{W}(A) & \xrightarrow{\ F_{n_A}\ } & \mathbb{W}(A) \\
\Big\downarrow{\scriptstyle \Delta_A} & & \Big\downarrow{\scriptstyle \Delta_A} \\
\mathbb{W}(\mathbb{W}(A)) & \xrightarrow{\ F_{n_{\mathbb{W}(A)}}\ } & \mathbb{W}(\mathbb{W}(A)) \\
\Big\downarrow{\scriptstyle w} & & \Big\downarrow{\scriptstyle w} \\
\mathbb{W}(A)^{\mathbb{N}} & \dashrightarrow{\ \widetilde{F_n}_{\mathbb{W}(A)}\ } & \mathbb{W}(A)^{\mathbb{N}}
\end{array}
$$

using the fact that

$$
\begin{array}{ccc}
\mathbb{W}(\mathbb{W}(A)) & & \\
\Big\downarrow{\scriptstyle w} & \searrow{\scriptstyle w_{nm}} & \\
\mathbb{W}(A)^{\mathbb{N}} & \xrightarrow{\ \widetilde{F_n}_{\mathbb{W}(A)}\ } & \mathbb{W}(A)^{\mathbb{N}}
\end{array}
$$

commutes, we can simplify the situation to

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

which can again be simplified to

$$\mathbb{W}(A) \xrightarrow{F_n} \mathbb{W}(A)$$
$$F_{nm} \searrow \quad \downarrow F_m$$
$$\mathbb{W}(A)$$

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

**CLAIM.**
$$\mathbb{W}(A)$$
$$\Delta_A \downarrow \quad \searrow^{\text{id}_{\mathbb{W}(A)}}$$
$$\mathbb{W}(\mathbb{W}(A)) \xrightarrow[\mathbb{W}(\varepsilon_A)]{} \mathbb{W}(A)$$
*commutes.*

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

$$\mathbb{W}(A)$$
$$\Delta_A \downarrow \quad \searrow^{\text{id}_{\mathbb{W}(A)}}$$
$$F \quad \mathbb{W}(\mathbb{W}(A)) \xrightarrow[\mathbb{W}(\varepsilon_A)]{} \mathbb{W}(A)$$
$$w \downarrow \qquad \qquad \downarrow w$$
$$\mathbb{W}(A)^{\mathbb{N}} \dashrightarrow_{\varepsilon_A^{\mathbb{N}}} A^{\mathbb{N}}$$

we can then simplify to

$$\mathbb{W}(A)$$
$$F \downarrow \quad \searrow^{w}$$
$$\mathbb{W}(A)^{\mathbb{N}} \xrightarrow[\varepsilon_A^{\mathbb{N}}]{} A^{\mathbb{N}}$$

now it suffices to show for all $n$ that

$$\mathbb{W}(A)$$
$$F_n \downarrow \quad \searrow^{w_n}$$
$$\mathbb{W}(A) \xrightarrow[\varepsilon_A]{} A$$

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

⫽

**CLAIM.**
$$\mathbb{W}(A)$$
$$\text{id}_{\mathbb{W}(A)} \swarrow \quad \downarrow \Delta_A$$
$$\mathbb{W}(\mathbb{W}(A)) \xleftarrow[\varepsilon_{\mathbb{W}(A)}]{} \mathbb{W}(A)$$
*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 $F_1 = \text{id}_{\mathbb{W}(A)}$. ⫽

This concludes the proof. □