# 2 Witt vectors

Witt vectors have originally been developed by Ernst Witt [5] as a generalisation of the $p$-adic numbers. The $p$-typical version often occurs in mixed characteristic and lifting problems, providing a construction of the unramified extension of the $p$-adic integer. They are equipped with different universal properties, depending on which view point is to be taken. Furthermore, there is the generalisation to big Witt vectors, from which the $p$-typical ones for every prime $p$ can be deduced.

## 2.1 Strict $p$-rings with perfect residue rings

Much of this follows [4] and [3].

**Definition 2.1.** Let $W$ be a ring and $A$ perfect of characteristic $p > 0$. Then $W$ is a $p$-ring with residue ring $A$ if there is $\pi \in W$ such that $W$ is separated for the $\pi$-adic topology and complete, and $A = W/\pi$.

In particular $p \in \pi W$. A $p$-ring always has a unique set of multiplicative representatives $[-] : A \to W$, and for a sequence of elements $\{a_i \in A\}_{i\in\mathbb{N}}$ the series

$$\sum_{i\in\mathbb{N}_0} [a_i]p^i \tag{2.1}$$

converges to an element in $W$.

**Definition 2.2.** The ring $W$ is said to be strict if $p = \pi$.

In this case every element $a \in W$ can be written in a unique way in the form (2.1), and the $a_i$ are called coefficients of $a$.

**Example 2.3.** Let $S = \mathbb{Z}[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$ Its $p$-adic completion $\widehat{S} = \mathbb{Z}_p[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$ is a strict $p$-ring with residue ring $\mathbb{F}_p[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$, which is perfect of characteristic $p \neq 0$. The variables $X_i$ are multiplicative representatives in $\widehat{S}$ because they have $p^{n\text{th}}$ roots for each $n \geqslant 0$. (In fact, the multiplicative system of representatives is characterised by the fact, that the elements are $(p^n)^{\text{th}}$ roots for all $n$.) This ring will be useful in a later proof.

We look at the particular case, that $A$ is a perfect ring of characteristic $p$. In this case, we have the following theorem.

**Theorem 2.4.** *There is up to unique isomorphism a unique strict $p$-ring denoted by $W(A)$, called the ring of Witt vectors with coefficients in $A$, with residue ring $A$. Moreover on has:*

1. *There is a unique system of representatives $[-] : A \to W(A)$, called Teichmüller representatives, and this map is multiplicative*
$$[ab] = [a][b].$$
2. *Each element $a \in W(A)$ has a unique representation as a sum*
$$\underline{a} = \sum_{n=0}^{\infty} [a_n]p^n$$
*with $a_n \in A$.*
3. *The construction of $W(A)$ and $[-]$ is functorial in $A$, i.e. for a homomorphism $f : A \to A'$ of perfect rings of characteristic $p$, there is a unique homomorphism $W(f) : W(A) \to W(A')$ such that the diagrams*
$$\begin{array}{ccc} W(A) & \xrightarrow{\tilde{f}} & W(A') \\ \downarrow & & \downarrow \\ A & \xrightarrow{f} & A' \end{array}$$
*and*
$$\begin{array}{ccc} W(A) & \xrightarrow{\tilde{f}} & W(A') \\ {\scriptstyle [-]}\uparrow & & \uparrow{\scriptstyle [-]} \\ A & \xrightarrow{f} & A' \end{array}$$

*commute.*

**Example 2.5.** Any unramified extension $R/\mathbb{Z}_p$ with residue field $k = R/p \cong \mathbb{F}_q$, for some $q = p^r$ is a strict $p$-ring, and hence according to the theorem, the unique strict $p$-ring with residue field $\mathbb{F}_q$. The Teichmüller representatives have a very nice description. As $\mathbb{F}_q^* \cong \mathbb{Z}/(q-1)$, the non-zero elements of $\mathbb{F}_q$ are the roots of the polynomial $x^{q-1} - 1$. By Hensel's Lemma, each $x \in \mathbb{F}_q$ has a lift $[x] \in R$ such that also $[x]^{q-1} - 1 = 0$ in $R$. Lastly, we set $[0] = 0 \in R$. This set, the $(q-1)$st roots of unity togehter with 0 is of course multiplicative, and by the theorem this gives exactly the Teichmüller representatives of $R$.

There is a rather non-constructive proof of the existence and uniqueness of $W(A)$.

Consider the ring $\widehat{S} = \mathbb{Z}_p[X_i^{p^{-\infty}}, Y_j^{p^{-\infty}} \ : \ i,j \in \mathbb{N}_0]$, and take the elements

$$x = \sum [X_i]p^i \quad , \quad y = \sum [Y_i]p^i.$$

Then for any operation $* = +, -, \cdot$, the composition $x * y$ is again an element in $\widehat{S}$, and thus can be written again in the form

$$x * y = \sum [Q_i^*]p^i \quad , \quad \text{with } Q_i^* \in \mathbb{F}_p[X_i^{p^{-\infty}}, Y_j^{p^{-\infty}} \ : \ i,j \in \mathbb{N}_0].$$

As the $Q_i^*$ are polynomials with coefficients in the prime field $\mathbb{F}_p$ we can evaluate them in any perfect ring of characteristic $p$, and this allows us to determine the structure of a strict $p$-ring.

**Proposition 2.6.** *Let $W$ be a $p$-ring with residue ring $A$. Let $a_i$ and $b_j \in A$. Then*

$$\sum [a_i]p^i * \sum [b_i]p^i = \sum [c_i]p^i$$

*with $c_i = Q_i^*(a_0, \ldots, b_o, \ldots)$.*

*Proof.* There is a homomorphism $\theta : \mathbb{Z}[X_i^{p^{-\infty}}, Y_j^{p^{-\infty}} \ : \ i,j \in \mathbb{N}_0] \to W$ sending $X_i \mapsto [a_i]$, which extends by continuity to $\mathbb{Z}_p[X_i^{p^{-\infty}}, Y_j^{p^{-\infty}} \ : \ i,j \in \mathbb{N}_0]$ and induces a morphism on residue fields

$$\overline{\theta} : \mathbb{F}_p[X_i^{p^{-\infty}}, Y_j^{p^{-\infty}} \ : \ i,j \in \mathbb{N}_0] \to A$$

sending the $X_i \mapsto a_i$ and $Y_i \mapsto b_i$. As $\theta$ is a morphism of $p$-rings, it commutes with multiplicative representatives, and we obtain

$$\begin{aligned} \sum [a_i]p^i * \sum [b_i]p^i &= \theta(x) * \theta(y) = \theta(x * y) \\ &= \sum \theta([Q_i^*])p^i \\ &= \sum [\overline{\theta}(Q_i^*)]p^i \end{aligned}$$

and $\overline{\theta}(Q_i^*) = c_i$. □

**Proposition 2.7.** *Let $W$ and $W'$ be $p$-rings, with residue rings $A$ and $A'$, and assume further that $W$ is strict. For any homomorphism $f : A \to A'$ there is a unique homomorphism $g : W \to W'$, such that the diagram*

$$\begin{array}{ccc} W & \xrightarrow{g} & W \\ \downarrow & & \downarrow \\ A & \xrightarrow{f} & A \end{array}$$

*is commutative.*

*Proof.* We have already mentioned that a morphism of $p$-rings always commutes with the system of multiplicative representatives. For an element $a \in W$ with coordinates $\{\alpha_i \in A\}_i$ one should have

$$g(a) = \sum_{i=0}^{\infty} g([\alpha_i]_W)p^i = \sum_{i=0}^{\infty} [f(\alpha_i)]_{W'}.$$

Because $W$ is strict, the $\alpha_i$ determine $a$ uniquely, so the above expression shows the uniquenes of $g$ if it exists. In fact, one can take this expression as definition to get existence, if we remark, that it defines in fact a homomorphism of rings, commuting with multiplication, addition and subtraction by Proposition 2.6. □

**Corollary 2.8.** *Two strict p-rings with the same residue ring are canonically isomorphic.*

**Lemma 2.9.** *Let $f : A \to A'$ a surjective homomorphism of perfect rings of characterisitic $p$. If there exists a strict $p$-ring $W$ with residue ring $A$, there exists as well a strict $p$-ring $W'$ with residue ring $A'$.*

*Proof.* We will define $W'$ as quotient of $W$. For this, we consider an equivalence relation: Let $a$ and $b \in W$ with coordinates $\{\alpha_i \in A\}_i$ and $\{\beta_i \in A\}_i$. Then $a \equiv b$ if $f(\alpha_i) = f(\beta_i)$ for all $i \in \mathbb{N}_0$. If $a \equiv a'$ and $b \equiv b'$, one shows using Proposition 2.6, that $a * b \equiv a' * b'$ for $* = +, -, \cdot$. Thus the quotient of $W$ by this equivalence relation

$$W' := W/\sim$$

is a ring.

Let $x \in W'$ be in the immage of an element $a \in W$ with coefficients $\{\alpha_i \in A\}_i$. Then the elements $\xi_i = f(\alpha_i)$ only depend on $x$ and not on the lift $a$. They are the coordinates of $x$. On the other hand, any sequence $\{\xi_i \in A'$ give rise to an element $x \in W'$ in a unique way.

The multiplication with $p$ in $W'$ is given by $(\xi_0, \xi_1, \ldots) \mapsto (0, \xi_0, \xi_1, \ldots)$, thus $p$ is not a zero divisor in $W'$. Moreover, $\bigcap p^n W' = 0$, and therefore the $p$-adic topology on $W'$ is separated. As a quotient of a complete ring, $W'$ is also complete. Finally, the morphism, $W' \to A'$ which assignes to $x$ its first coordinate $\xi_0$ descents to an automorphism $W'/p \to A'$. And this shows, that $W'$ has residue ring $A'$. □

**Theorem 2.10.** *For every perfect ring $A$ o characterisitic $p \neq 0$, there is a unique strict $p$-ring denoted by $W(A)$ with residue ring $A$.*

*Proof.* If exisctence is shown, uniqueness is Corollary 2.8.

If $A$ is of the form $\mathbb{F}_p[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$ then $W(A) = \mathbb{Z}_p[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$. The general case follows from Lemma 2.9, if we remark that any perfect ring of characteristic $p$ can be wriiten as a quotient of $\mathbb{F}_p[X_i^{p^{-\infty}}, i \in \mathbb{N}_0]$. Proposition 2.7 shows that this defines a functor $W(-)$ as

$$\mathrm{Hom}(A, A') \cong \mathrm{Hom}(W(A), W(A'))$$

is an isomorphism. □

**Corollary 2.11.** *For every perfect field $k$ of characteristic $p$, there is a unique complete dvr $W(k)$, which is totally unramified and as residue field $k$.*

*Proof.* This is just a special case of Theorem 2.14 if one realises that every complete totally unramified dvr with residue field $k$ is just a strict $p$-ring with residue field $k$. □

**Corollary 2.12.** *Let $V$ be a complete dvr of mixed characteristic and perfect residue field $k$. Let $e$ be the ramification index. There is a unique homomorphism $W(k) \to V$ such that the diagram*

*Proof.* Note that $V$ is a (possibly non-strict) $p$-ring. Thus we can apply Proposition 2.7 to the identity $\mathrm{id} : k \to k$, which gives existence and uniqueness of the morphism. It is injective trivially, as $V$ is of characteristic 0. Moreover, one can show, that if $\pi$ is a local uniormiser of $V$, any element $y \in V$ can be written in the form

$$y = \sum_{i=0}^{\infty} \sum_{j=0}^{e-1} [\alpha_{ij}] \pi^j p^i \quad , \quad \alpha_{ij} \in k$$

hence,$\{1, \pi, \ldots, \pi^{e-1}\}$ is a basis of $V$ as $W(k)$-module. □

*Remark* 2.13. Note that for the definition of addition, multiplication and subtraction on $W(A)$ via the functions $Q_i^*$, one has to use all $p^{n\text{th}}$ roots of the variables $X_i$ and $Y_i$. Thus we had to restict ourself to perfect residue rings. To be able to generalise this, one has to define the coordinates of an element $a \in W(A)$ by the formula

$$a = \sum_{i=0}^{\infty} [\alpha_i]^{p^{-i}} p^i.$$

This leads to the definition of Witt vectors.

## 2.2 The ring of $p$-typical Witt vectors

Let $\{X_i\}_{i\in\mathbb{N}_0}$ be a set f variables. COnsider the polynomials

$$w_n(\underline{X}) = \sum_{i=0}^{n} p^i X^{p^{n-i}}$$

called the Witt polynomials. It is clear, that one can express the $X_i$ as polynomials in the $w_n$ with coefficients in $\mathbb{Z}[p^{-1}]$. Let $\{Y_i\}_{i\in\mathbb{N}_0}$ be another set of variables.

**Theorem 2.14.** *For any polynomial $\Phi \in \mathbb{Z}[X, Z]$ there is a unique sequence of polynomials $\phi_0, \phi_1, \ldots \in \mathbb{Z}[X_i, Y_j]$ such that*

$$w_n(\underline{\phi}) = \Phi(w_n(\underline{X}), w_n(\underline{Y})).$$

*Proof.* Existence and uniqueness are rather evident over $\mathbb{Z}[p^{-1}]$.($\phi_n$ is defined recursively and uniquely by a system of $n$ equations.) So the main task is, to show that the coefficients of the $\phi_i$ lie in $\mathbb{Z}$. We do this again following ideas by Lazard as explained in [4, Sec. II. 6].

Take again $\widehat{S} = \mathbb{Z}_p[\underline{X}^{p^{-\infty}}, \underline{Y}^{p^{-\infty}}]$, and set

$$x' = \sum X_i^{p^{-i}} p^i \quad \text{and} \quad y' = \sum Y_i^{p^{-i}} p^i$$

As $\Phi(x', y') \in \widehat{S}$ we can write it in a unique way in the form

$$\Phi(x', y') = \sum [\overline{\psi}_i]^{p^{-i}} p^i \quad \text{with} \quad \overline{\psi}_i \in \mathbb{F}_p[\underline{X}^{p^{-\infty}}, \underline{Y}^{p^{-\infty}}]$$

Let $\psi_i$ be representatives of $\overline{\psi}_i$ in $\widehat{S}$. One has a congruence

$$\Phi(\sum_{i\leqslant n} X_i^{p^{-i}} p^i, \sum_{i\leqslant n} Y_i^{p^{-i}} p^i) \equiv \sum_{i\leqslant n} [\overline{\psi}_i]^{p^{-i}} p^i \mod p^{n+1}$$

Replacing $X_i$ by $X_i^{p^n}$ and $Y_i$ by $Y_i^{p^n}$, which is an automorphism of $\widehat{S}$, gives

$$\Phi(w_n(\underline{X}), w_n(\underline{Y})) \equiv \sum_{i\leqslant n} [\overline{\psi}_i(\underline{X}^{p^n}, \underline{Y}^{p^n})]^{p^{-i}} p^i \mod p^{n+1}$$

But $\overline{\psi}_i(\underline{X}^{p^n}, \underline{Y}^{p^n}) = \overline{\psi}(\underline{X}, \underline{Y})^{p^n}$ as the coefficients of $\overline{\psi}$ are in $\mathbb{F}_p$. Furthermore, we know that $[-]$ commutes with $p^{\text{th}}$ power, so

$$\Phi(w_n(\underline{X}), w_n(\underline{Y})) = w_n(\underline{\phi}) \equiv \sum_{i\leqslant n} [\overline{\psi}_i]^{p^{n-i}} p^i \mod p^{n+1}$$

But $[\overline{\psi}_i] \equiv \psi_i \mod p$ so $[\overline{\psi}_i]^{p^{n-i}} \equiv \psi^{p^{n-i}} \mod p^{n-i+1}$, thus

$$w_n(\underline{\phi}) \equiv w_n(\underline{\psi}) \mod p^{n+1}$$

By induction one can assume that $\phi_i$ for $i < n$ has integer coefficients and is congruent $\psi_i \mod p$. Then by the above congruence, one obtains

$$p^n \phi_n \equiv p^n \psi_n \mod p^{n+1}$$

so that $\phi_n$ has integer coefficients and is congruent $\psi_n \mod p$. □

**Definition 2.15.** Denote now by $\underline{S} \in \mathbb{Z}[\underline{X}, \underline{Y}]$ and $\underline{P} \in \mathbb{Z}[\underline{X}, \underline{Y}]$ the polynomials associated to addition ($\Phi(X, Y) = X + Y$) and multiplication ($\Phi(X, Y) = XY$).

Let $A$ by any commutative ring (with unit). By the above formulae, we define composition laws on $A^{\mathbb{N}}$ for $\underline{a} = (a_0, a_1, \ldots)$ and $\underline{b} = (b_0, b_1, \ldots)$:

$$\begin{aligned} \underline{a} + \underline{b} &= (S_0(\underline{a}, \underline{b}), S_1(\underline{a}, \underline{b}), \ldots) \\ \underline{a} \cdot \underline{b} &= (P_0(\underline{a}, \underline{b}), P_1(\underline{a}, \underline{b}), \ldots) \end{aligned}$$

**Theorem 2.16.** *These composition laws make $A^{\mathbb{N}}$ into a commutative ring with unit, called the ring of Witt vectors with coefficients in $A$, and denoted by $W(A)$.*

*Proof.* By definition of the $\underline{S}$ and $\underline{P}$ the Witt polynomials define a homomorphism of rings

$$\begin{array}{rcl} w : W(A) & \to & A^{\mathbb{N}} \\ (a_0, a_1, \ldots) & \mapsto & (w_0(\underline{a}), w_1(\underline{a}), \ldots) \end{array}$$

where addition and multiplication on the right side is component wise, and on the left side by $\underline{S}$ and $\underline{P}$. It is an isomorphism, if $p$ is invertible in $A$, and in this case, it is easy to see, that the unit in $W(A)$ is given by $(1, 0, 0, \ldots)$.

But if the theorem is true for a ring $A$, it is also true for subrings and quotients. Since it holds for $\mathbb{Z}[p^{-1}][\underline{X}]$ it is also true for $\mathbb{Z}[\underline{X}]$ and thus for any commutative ring (with unit). □

**Exercise 2.17.** Compute a few polynomials $S_n$ and $P_n$.

We may also consider Witt vectors of inite length, by only considering the first $n$ variables $(a_0, \ldots, a_{n-1})$, denoted by $W_n(A)$ with underlying set $A^n$. As the $\phi_i$ from the theorem only contain variables of index $\leqslant i$, this is a quotient of $W(A)$. We have $W_1(A) = A$ (rememebr this for later) and $\varprojlim W_n(A) = W(A)$

We will now define some important operators.

Let $\underline{a} = (a_0, a_1, \ldots) \in W(A)$. Then one defines the Verschiebung map by

$$\begin{array}{rcl} V : W(A) & \to & W(A) \\ \underline{a} & \mapsto & (0, a_0, a_1, \ldots) \end{array}$$

It is additive: Similar to the above reasoning it is enough to show this when $p$ is invertible. In this case the ghost map

$$\begin{array}{rcl} W(A) & \to & A^{\mathbb{N}} \\ (a_0, a_1, \ldots, a_n, \ldots) & \mapsto & (a_0, a_0^p + pa_1, \ldots, \sum_{i=0}^{n} p^i a_i^{p^{n-i}}, \ldots) \end{array}$$

transforms $V$ int the map

$$(w_0, w_1, \ldots, w_n, \ldots) \mapsto (0, pw_0, \ldots, pw_{n-1}, \ldots).$$

By passing to the quotient, one obtains a map of finite Witt vectors $V : W_n(A) \to W_{n+1}(A)$ which can be iterated. On the other hand, there is a restriction map

$$R : W_{n+1}(A) \to W_n(A).$$

Together they give rise to short exact sequences of additive groups

$$0 \to W_k(A) \xrightarrow{V^r} W_{k+r}(A) \to W_r(A) \to 0$$
$$0 \to W(A) \xrightarrow{V^r} W(A) \xrightarrow{R^r} W_r(A) \to 0$$

For $x \in A$, there is a map

$$\begin{array}{rcl} A & \to & W(A) \\ x & \mapsto & [x] = (x, 0, \ldots) \end{array}$$

which gives a multiplicative set of representatives, called Teichmüller representatives, as it is a section of the canonical projection $W(A) \to W_1(A) = A$. Under the ghost map, the representative map is given by $x \mapsto (x, x^p, \ldots, x^{p^n})$. And one sees readily, that for $(a_0, a_1, \ldots) \in W(A)$

$$[x] \cdot \underline{a} = (xa_0, x^p a_1, \ldots x^{p^n} a_n, \ldots)$$

We can represent a Witt vector using Verschiebung and Teichmüller representatives

$$(a_0, a_1, \ldots) = \sum V^n[a_n].$$

We will prove that for a perfect ring of characteristic $p > 0$ this gives an explicit representation of the ring whose existence we showed earlier.

**Theorem 2.18.** *If $A$ is a perfect ring of characteristic $p > 0$. Then $W(A)$ is a strict $p$-ring with residue ring $A$.*

*Proof.* Let $H$ be the unique strict $p$-ring with residue ring $A$, and $f : A \to H$ the multiplicative system of representatives. To construct a morphism $W(A) \to H$, associate to $\underline{a} \in W(A)$ the element

$$\theta(\underline{a}) = \sum_{i=0}^{\infty} f(a_i)^{p^{-i}} p^i.$$

Note that $f(a_i)^{p^{-i}} = f(a_i)$ because $A$ is perfect. It is easy (exercise!) to see that the so defined map is additive and multiplicative, if $H = \widehat{S}$. Clearly $\theta$ is bijective, so that one gets an isomorphism of rings. □

**Example 2.19.** $W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n$.

The second important map of Witt vectors is the Frobenius morphism. If $A$ is a ring of characteristic $p \neq 0$ (not necessarily perfect), the morphism

$$\begin{array}{ccc} A & \to & A \\ x & \mapsto & x^p \end{array}$$

induces by functoriality a unique endomorphism

$$\mathrm{F} : W(A) \to W(A)$$

given by the formula

$$F(a_0, a_1, \ldots, a_n, \ldots) = (a_0^p, a_1^p, \ldots, a_n^p, \ldots)$$

called the Frobenius. Under the ghost map,

$$\begin{array}{ccc} W(A) & \xrightarrow{\mathrm{F}} & W(A) \\ \downarrow & & \downarrow \\ A^{\mathbb{N}} & \longrightarrow & A^{\mathbb{N}} \end{array}$$

it is given on $A^{\mathbb{N}}$ by

$$(x_0, x_1, \ldots) \mapsto (x_1, x_2, \ldots)$$

We can use this formula to define the Frobenius morphism also for general commutative residue fields by polynomials. On $W(A)$

$$\mathrm{F}(\underline{a}) = (f_0(\underline{a}), f_1(\underline{a}), \ldots)$$

with $f_n \in \mathbb{Z}[X_0, \ldots X_{n+1}]$ determined recursively by a system

$$\begin{array}{rcl} f_0 & = & X_0^p + pX_1 \\ f_0^p + pf_1 & = & X_0^{p^2} + pX_1^p + p^2X_2 \\ & \vdots & \\ f_0^{p^n} + \cdots p^n f_n & = & X_0^{p^{n+1}} + \cdots + p^{n+1}X_{n+1} \end{array}$$

We have the following easy (exercise!) to verify identities

$$\begin{array}{rcll} xVy & = & V(Fx.y) & \text{for } x, y \in W(A) \\ FV & = & p & \text{always} \\ VF & = & p & \text{iff } p = 0 \text{ in } A \end{array}$$

One can also restrict this in an obvious way to finite length Witt vectors

$$\mathrm{F} : W_{n+1}(A) \to W_n(A)$$

and together with the restriction map, we have for characteristic-$p$-rings $A$

$$RFV = FVR = p$$

The filtration by $V$ is compatible with the ring structure as

$$V^m x.V^n y = V^{m+n}(F^n x.F^m y) \subset V^{m+n}W(A).$$

We denote by $\mathrm{gr}_V W(A)$ the associated graded ring.

Let $A$ now be a ring without $p$-torsion, and $f : A \to A$ a lift of Frobenius. Due to a lemma by Dieudonné-Cartier, there is a unique section if the canonical projection

$$s_f : A \to W(A)$$

, such that $s_f \circ f = F \circ s_f$. It is again defined by an inductive system of polynomials $w_n(s_f(x)) = f^n(x)$. In particular for $x$ with $f(x) = x^p$, we have $s_f(x) = [x]$. Since it is functorial in the pair $(A, f)$, we obtain with the canonical projection

$$t_f : A \to W(A) \to W(A/p).$$

If $A/p$ is perfect, this induces an isomorphism $A/p^n \cong W_n(A/p)$. It follows that if $A/p$ is perfect, and $A$ $p$-adically separated and complete, then $t_f : A \to W(A/p)$ is an isomorphism.

Another important feature of Witt vectors that has already been mentioned, is that they have naturally divided powers. Let $A$ ba an $\mathbb{F}_p$-algebra. Then $W(A)$ is naturally a $\mathbb{Z}_p$-aglebra(, which has divided powers). Then $(Vx)^n = p^{n-1}Vx^n$ and we can define a divided power structure on the ideal $VW(A)$ by

$$\begin{aligned} \gamma_n : VW(A) &\to W(A) \\ \gamma_n(Vx) &= \begin{cases} 1 & \text{if } n = 0 \\ (\frac{p^{n-1}}{n!})Vx^n & \text{otherwise} \end{cases} \end{aligned}$$

and Frobenius and restriction are a PD-morphisms. The PD-structure is functorial in the sense, that for any morphism $A \to B$ the induced map $W(A) \to W(B)$ is a PD-morphism.

The notopn of Witt vectors globalises in the sense that for a ringed topos $(X, \mathscr{O}_X)$ the pre sheaf defined by

$$U \mapsto W(\mathscr{O}_X(U))$$

is actually a sheaf denoted by $W(\mathscr{O}_X)$, and the ringed tops $(X, W(\mathscr{O}_X))$ is also denoted by $W(X)$, and the relevant morphisms, $w_n, R, F, V, s_f, t_f, \gamma_n$, sheafify as well.

Let $X$ be of characteristic $p$. Then since $(VW_{n-1}(\mathscr{O}_X))^n = 0$, it follows that $W_n(X)$ is an infinitesimal neighbourhood of $X = W_1(X)$. Thus for a locally ringed $X$, all $W_n(X)$ are also locally ringed and in particular

$$W_n(\mathscr{O}_{X,x}) \xleftarrow{\sim} W_n(\mathscr{O}_X)_x$$

It follows moreover, that for an $\mathbb{F}_p$-scheme $X$, $W_n(X)$ is a $\mathbb{Z}/p^n$-scheme with the same underlying space. More precisely, it is a PD-thickening of $X$. If $X$ is locally noetherian, and the Frobenius on $X$ is finite, then $W_n(X)$ is also locally noetherian.

We have the following functoriality: Let $f : (X, \mathscr{O}_X) \to (Y, \mathscr{O}_Y)$ be y morphism of ringed topoi, then the canonical homomorphism $\mathscr{O}_Y \to f_* \mathscr{O}_X$ induces on sheaves $W(\mathscr{O}_Y) \to W(f_* \mathscr{O}_X) = f_* W(\mathscr{O}_X)$ and therefore a mrophism of ringed topoi

$$W(f) : W(X) \to W(Y)$$

**Proposition 2.20.** *Let $f : X \to Y$ be a morphism of $\mathbb{F}_p$-schemes.*

1. *If $f$ is a closed immersion with ideal $I$, then $W_n(f)$ is a closed immersion with ideal $W_n(I)$*
2. *If $f$ is of finite type and the Frobenius on $X$ is finite, then $W_n(f)$ is of finite type.*
3. *If $f$ is étale, then $W_n(f)$ is étale and we have cartesian squares*

$$\begin{array}{ccccc} X & \hookrightarrow & W_n(X) & \xrightarrow{F} & W_n(X) \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle W_n(f)} & & \downarrow{\scriptstyle W_n(f)} \\ Y & \hookrightarrow & W_n(Y) & \xrightarrow{F} & W_n(Y) \end{array}$$

Note that of $f$ is finite type, the Frobenius of $X$ is finite if the Frobenius of $Y$ is finite. In particular, from the above it follows, that if $Y$ is perfect. $W_n(f)$ is of finite type if $f$ is of finite type.

### 2.3 Big Witt vectors

We will now discuss the multi-prime generalisation of Witt vectors [2]. The difference is, that we generalise the index set.

**Definition 2.21.** Let $S \subset \mathbb{N}$. We say that $S$ is a truncation set, or divisor stable, if for $n \in S$, and $d \in \mathbb{N}$ a divisor of $n$, then $d \in S$.

**Examples 2.22.** $\mathbb{N}$ itself and the finite subsets $\{1, \ldots, n\}$ are truncation sets. For a prime number $p$, the set $\{1, p, p^2, \ldots\}$ and the finite sets $\{1, p, \ldots, p^n\}$ are truncation sets.

For a commutative ring $A$ we define.

**Definition 2.23.** The big Witt ring $\mathbb{W}_S(A)$ is the set $A^S$ equipped with the ring structure such that the ghost map defined by the Witt polynomials

$$\begin{aligned} w : \mathbb{W}_S(A) &\to A^S \\ w_n(\underline{a}) &= \sum_{d|n} d a_d^{\frac{n}{d}} \end{aligned}$$

is a natural transformation of ring functors.

As usual, on the right hand side, we take component wise addition and multiplication.

**Examples 2.24.** If $S = \mathbb{N}$, we write $\mathbb{W}(A) := \mathbb{W}_S(A)$. For $S = \{1 = p^0, p = p^1, p^2, \ldots\}$ for a prime number $p$, we obtain the ring of $p$-typical Witt vectors (usually indexed by the exponents of $p$), which we denote as usual by $W(A)$ and for a finite set $S = \{1, \ldots, n\}$ we obtain truncated Witt vectors. In particular, for $S = \{1, p, \ldots, p^n\}$, we obtain the usual ($p$-typical) truncated Witt vectors.

To prove that there exists such a ring structure, we follow a similar strategy as in the case of $p$-typical Witt vectors, that is, we need a criterion similar to (but more general than) Theorem 2.14 that tells us, when an element is in the image of the ghost map: roughly we have to be able to take $(p^n)^{\text{th}}$ roots of representatives for all primes $p$.

**Lemma 2.25** (Dwork). *Suppose that for every prime number p, there is a ring homomorphism $\phi_p : A \to A$ such that $\phi_p(a) \equiv a^p \mod p$. Then a sequence $\{x_n \mid n \in S\}$ is in the image of the ghost map, if and only if $x_n \equiv \phi_p(x_{\frac{n}{p}}) \mod p^{\nu_p(n)}$ for all p, and for all $n \in S$ with $\nu_p(n) \geqslant 1$.*

*Proof.* It is easy (exercise!) to see that if $a \equiv b \mod p$, then $a^{p^{n-1}} \equiv b^{p^{n-1}}$ (we have already used this above). Since $\phi_p$ is a ring homomorphism,

$$\phi_p(w_{\frac{n}{p}}(\underline{a})) = \sum_{d|(\frac{n}{p})} d\phi_p(a_d^{\frac{n}{pd}}) \equiv \sum_{d|(\frac{n}{p})} d a_d^{\frac{n}{d}} \mod p^{\nu_p(n)}.$$

The last congruence comes from the fact just stated, and because we summ over all divisors of $\frac{n}{p}$. For an integer $d$ dividing $n$ but not $\frac{n}{p}$, we have $\nu_p(n) = \nu_p(d)$, thus $0 \equiv d \mod p^{\nu_p(d)} \equiv d \mod p^{\nu_p(n)}$ and we can rewrite the sum $\mod p^{\nu_p(n)}$ as $\sum_{d|n} d a_d^{\frac{n}{d}} = w_n(\underline{a})$. Together

$$w_n(\underline{a}) \equiv \phi_p(w_{\frac{n}{p}}(\underline{a})) \mod p^{\nu_p(n)}.$$

On the other hand, if a sequence $(x_n \mid n \in S)$ satisfies $x_n \equiv \phi_p(x_{\frac{n}{p}}) \mod p^{\nu_p(n)}$, we have to find $\underline{a}$ such that $w_n(\underline{a}) = x_n$. We do this by induction: let $a_1 = x_1$ and assume for an $n$ all $a_d$ with $n \neq d|n$ chosen such that $w_d(\underline{a}) = x_d$. Then

$$x_n \equiv \sum_{n \neq d|n} d a_d^{\frac{n}{d}} \mod p^{\nu_p n}$$

and we can find $a_n = x_n - \sum_{n \neq d|n} d a_d^{\frac{n}{d}}$. □

**Proposition 2.26.** *There is a unique ring structure on the set $\mathbb{W}_S(A)$ that makes the ghost map a natural transformation of ring functors.*

*Proof.* As done previously, we start with a polynomial ring, where the variables are indexed by $S$, $A = \mathbb{Z}_{[} X_n, Y_n \mid n \in S]$. Then the ring homomorphism given by

$$\begin{array}{rcl} \phi_p : A & \to & A \\ X_n & \mapsto & X_n^p \text{ and} \\ Y_n & \mapsto & Y_n^p \end{array}$$

satisfies the conditions of Dwork's Lemma. It follows then that for $\underline{a} \in \mathbb{W}_S(A)$ and $\underline{b} \in \mathbb{W}_S(A)$ the elements $w(\underline{a}) + w(\underline{b})$, $w(\underline{a}) \cdot w(\underline{b})$ and $-w(\underline{a})$ in $A^{\mathbb{N}}$ are in the image of the ghost map (this is clear for $\underline{a} = \underline{X}$ and $\underline{b} = \underline{Y}$ and follows then immediately as $A$ is torsion free), so there are sequences of polynomials $(s_n^* \mid n \in S)$, $* = +, -, \cdot$, such that $w(\underline{s}^+) = w(\underline{a}) + w(\underline{b})$, etc.

For a general commutative ring $A'$, there is a homomorphism $f : A \to A'$ such that for $\underline{a}', \underline{b}' \in \mathbb{W}_S(A')$ the induced homomorphism

$$\mathbb{W}_S(f) : \mathbb{W}_S(A) \to \mathbb{W}_S(A')$$

sends $\underline{X} \mapsto \underline{a}$ and $\underline{Y} \mapsto \underline{b}$. Then

$$\underline{a}' * \underline{b}' = \mathbb{W}_S(f)(s^*(\underline{a}, \underline{b}))$$

and this defines the ring structure. □

Most of the additional structure from $p$-typical Witt vectors generalises to big Witt vectors.

**The restriction map.** If $T \subset S$ are both truncation sets, the forgetful functor

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

corresponds to the restriction map. If $S = \{p^i \mid i \in \mathbb{N}_0\}$ and $T = \{p^0, \dots p^{n-1}\}$ we obtain the usual restriction map.

**Verschiebung.** If $n \in \mathbb{N}$ and $S$ is a truncation set, then

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

is also a truncation set, and we define

$$\begin{array}{rcl} V_n : \mathbb{W}_{\frac{S}{n}}(A) & \to & \mathbb{W}_S(A) \\ (V_n(A_d \mid d \in \frac{S}{n}))_m & = & \begin{cases} a_d & \text{if } m = nd \\ 0 & \text{otherwise.} \end{cases} \end{array}$$

which shifts an entry $a_d$ from the $d^{\text{th}}$ to the $n \cdot d^{\text{th}}$ slot. For $S = \{p^0, \dots, p^n\}$, $\frac{S}{p} = \{p^0, \dots, p^{n-1}$ and

$$V_p : W_n(A) \to W_{n+1}(A)$$

is the usual Verschiebung. It is an easy (exercise!) lemma to show the $V_n$ is additive (hint: apply the ghost map).

**Frobenius.** Recall that in the $p$-typical case, the Frobenius map could be constructed recursively, by solving polynomial equations, to make a certain diagram commute. Frobenius should make the diagram

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

with $(\mathrm{F}_n^w(x_m \mid m \in S))_d = x_{nd}$ commute. First for $A = \mathbb{Z}[X_m \mid m \in S]$. Then by Dwork's Lemma with the map $\phi_p(X_i) = X_i^p$, $\mathrm{F}_n^w(w(\underline{X}))$ is again in the image of the ghost map, given by a set of polynomials $(f_i | i \in S)$, which can be determined recursively. Now we pass to a general commutative ring $A'$ as in the proof of the ring operations.

Exercise: show that if $A$ is an $\mathbb{F}_p$-algebra, and $\varphi : A \to A$ the Frobenius endomorphism, then the Frobenius for $p$ on $\mathbb{W}_S(A)$ is given by the formula

$$\mathrm{F}_p = R_{\frac{S}{p}}^S \circ \mathbb{W}_S(\varphi).$$

**Teichmüller representatives.** The map

$$\begin{array}{rcl} [-]_S : A & \to & \mathbb{W}_S(A) \\ ([a]_S)_n & = & \begin{cases} a & \text{if } n = 1 \\ 0 & \text{otherwise,} \end{cases} \end{array}$$

is multiplicative, making the diagram

$$\begin{array}{ccc} A & = & A \\ {\scriptstyle [-]_S}\downarrow & & \downarrow{\scriptstyle [-]_S^w} \\ \mathbb{W}_S(A) & \xrightarrow{w} & A^S \end{array}$$

with $([a]_S^w)_n = a^n$ commutative.

**Relations.** The following relations are easy to verify (exercise!). Let $\underline{a}, \underline{a}' \in \mathbb{W}_S(A)$.

$$\begin{array}{rcl} \underline{a} & = & \sum_{n \in S} V_n([a_n]_{\frac{S}{n}}) \\ \mathrm{F}_n V_n(\underline{a}) & = & n\underline{a} \\ \underline{a} V_n(\underline{a}') & = & V_n(\mathrm{F}_n(\underline{a})\underline{a}') \\ \mathrm{F}_m V_n & = & V_n \mathrm{F}_m \qquad \text{if } (m,n) = 1 \end{array}$$

Exercise: show that

$$\mathbb{W}_S(\mathbb{Z}) = \prod_{n \in S} \mathbb{Z} \cdot V_n([1]_{\frac{S}{n}}).$$

**Projective limit.** Let $S$ be a truncation set. Then by definition

$$\mathbb{W}_S(A) = \lim_{T \subset S \text{ finite}} \mathbb{W}_T(A).$$

**Decomposition.** Let $p$ be a prime and denote by $P = \{1, p, p^2, \ldots\}$. Let $I(S) = \{k \in S \mid p \nmid k\}$. Assume further, that every $k \in I(S)$ is invertible in $A$. Then there is a natural idempotent decomposition

$$\mathbb{W}_S(A) = \prod_{k \in I(S)} \mathbb{W}_{\frac{S}{k} \cap P}(A).$$

**Functoriality.** Let again $A = \mathbb{Z}[X_n \mid n \in S]$ then for any ring $B$ there is a natural identification

$$\mathrm{Hom}(A, B) \cong \mathbb{W}_S(B)$$

meaning that $\mathbb{W}_S(-)$ is representable. The ring structure on $\mathbb{W}_S(B)$ makes $R$ into a ring object in the category of $\mathbb{Z}$-algebras.

*Remark* 2.27. Witt–Burnside rings are a generalisation of Witt vectors using pro finite groups $G$. In this set-up the usual $p$-typical Witt vectors correspond to $G = \mathbb{Z}_p$. Examples for $G = \mathbb{Z}_p^n$ can be thought of as tree version of $W(-)$. Examples are extremely hard to compute, and not many applications are known.

*Remark* 2.28. Consider the natural projection

$$\begin{array}{rcl} \epsilon : \mathbb{W}(A) & \to & A \\ \underline{a} & \mapsto & a_1 \end{array}$$

There is a unique natural ring homomorphism

$$\Lambda : \mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(A))$$

such that $w_n(\Lambda(a)) = \mathrm{F}_n(a)$ for all $n \in \mathbb{N}$.

The element $(\mathrm{F}_n(a))_{n\in\mathbb{N}} \in \mathbb{W}(A)^{\mathbb{N}}$ is in the image of the ghost map according to Dworks Lemma (use that $\mathrm{F}_p : \mathbb{W}(A \to \mathbb{W}(A)$ satisfies $\mathrm{F}_p(a) \equiv a^p \mod p\,\mathbb{W}(A))$. This determines the map $\Lambda$ such that

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

Moreover, the triple $(\mathbb{W}(-), \Lambda, \epsilon)$ form a comonad on the category of rings. This means that

$$\begin{aligned} \mathbb{W}(\Lambda_A) \circ \Lambda_A &= \Lambda_{\mathbb{W}(A)} \circ \Lambda_A : \mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(\mathbb{W}(A))) \\ \mathbb{W}(\epsilon_A) \circ \Lambda_A &= \epsilon_{\mathbb{W}(A)} \circ \Lambda_A : \mathbb{W}(A) \to \mathbb{W}(A) \end{aligned}$$

(A monad is in some sense a monoid object in a bicategory, a command is a monad in the dual category.) A special $\lambda$-ring is a ring $A$ together with a map $\lambda : A \to \mathbb{W}(A)$ that makes $A$ into a coalgebra over the comonad $(\mathbb{W}(-), \Lambda, \epsilon)$. For such a ring we can then define the $n^{\text{th}}$ Adams operation by $\psi_n = w_n \circ \lambda : A \to \mathbb{W}(A) \to A$.

# References

[1] Christopher James Davis. On the de Rham–Witt complex.

[2] Lars Hesselholt. Lecture notes on the big de Rham–Witt complex. 2009.

[3] Joseph Rabinoff. The theory of Witt vectors. 2007.

[4] Jean-Pierre Serre. *Corps locaux*. Publications de l'Institut de mathématique de l'université de Nancago. Hermann, 2004, Paris, 1968. Autre tirage : 1980.

[5] Ernst Witt. Zyklische körper und algebren der charakteristik p vom grad pn. struktur diskret bewerteter perfekter körper mit vollkommenem restklassenkörper der charakteristik p. *Journal für die reine und angewandte Mathematik*, 176:126–140, 1937.

---

Universität Regensburg
Fakultät für Mathematik
Universitätsstraße 31
93053 Regensburg
Germany
(+ 49) 941-943-2664
`veronika.ertl@mathematik.uni-regensburg.de`
`http://www.mathematik.uni-regensburg.de/ertl/`