WITT VECTORS

OLIVIER BRINON

Abstract. These is a short introduction to Witt vectors. These notes have no originality. The main references used were [3, Chap. II, §6], [1, Chap. IX, §1] and [2, Chap. I].

In what follows, "ring" means commutative unitary ring. Let p be a prime integer. Let $\underline{X} = (X_0, X_1, \dots)$ be a indeterminate.

Definition 1. Let $n \in \mathbf{Z}_{\geqslant 0}$, the n-th *Witt polynomial* is

$$\Phi_n(\underline{X}) = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^{n-1}X_{n-1}^p + p^nX_n = \sum_{i=0}^{n} p^i X_i^{p^{n-i}}$$

If A is ring, the *ghost map* is:

$$\begin{aligned}\Phi_A \colon A^{\mathbf{Z}_{\geqslant 0}} &\to A^{\mathbf{Z}_{\geqslant 0}}\\ \underline{a} &\mapsto \big(\Phi_n(\underline{a})\big)_{n\in\mathbf{Z}_{\geqslant 0}}\end{aligned}$$

Lemma 2. Let A be a ring, and $x, y \in A$ such that $x \equiv y \mod pA$. Then $x^{p^i} \equiv y^{p^i} \mod p^{i+1}A$ for every $i \in \mathbf{Z}_{\geqslant 0}$.

Proof. We proceed by induction on $i \in \mathbf{Z}_{\geqslant 0}$, the case $i = 0$ being the hypothesis. Let $i \in \mathbf{Z}_{\geqslant 0}$ be such that $x^{p^i} \equiv y^{p^i} \mod p^{i+1}A$: write $x^{p^i} = y^{p^i} + p^{i+1}z$ with $z \in A$. By the binomial theorem, we have $x^{p^{i+1}} = \big(y^{p^i} + p^{i+1}z\big)^p = y^{p^{i+1}} + \sum\limits_{k=1}^{p-1} \binom{p}{k} p^{k(i+1)} y^{p^i(p-k)} z^k + p^{p(i+1)}z^p$. For $k \in \{1, \dots, p-1\}$, we have $v_p\big(\binom{p}{k}p^{k(i+1)}\big) = 1 + k(i+1) \geqslant i+2$, and $p(i+1) \geqslant i+2$ (because $p \geqslant 2$), so $x^{p^{i+1}} \equiv y^{p^{i+1}} \mod p^{i+2}A$. $\square$

Lemma 3. (Dwork). Let $\varphi \colon A \to A$ be a ring homomorphism such that $\varphi(a) \equiv a^p \mod pA$ for all $a \in A$. Then a sequence $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in A^{\mathbf{Z}_{\geqslant 0}}$ is in the image of Φ_A if and only if $\varphi(x_n) \equiv x_{n+1} \mod p^{n+1}A$ for all $n \in \mathbf{Z}_{\geqslant 0}$.

Proof. • As φ is a ring homomorphism, we have $\varphi(\Phi_n(\underline{a})) = \sum\limits_{i=0}^{n} p^i \varphi(a_i)^{p^{n-i}}$ for all $\underline{a} = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}}$. As $\varphi(a_i) \equiv a_i^p \mod pA$, we have $\varphi(a_i)^{p^{n-i}} \equiv a_i^{p^{n+1-i}} \mod p^{n+1-i}A$ for all $i \in \{0, \dots, n\}$ by lemma 2. This implies that $\varphi(\Phi_n(\underline{a})) \equiv \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} \mod p^{n+1}A$, *i.e.* $\varphi(\Phi_n(\underline{a})) \equiv \Phi_{n+1}(\underline{a}) \mod p^{n+1}A$.

• Conversely, assume that $(x_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in A^{\mathbf{Z}_{\geqslant 0}}$ satisfies $\varphi(x_n) \equiv x_{n+1} \mod p^{n+1}A$ for all $n \in \mathbf{Z}_{\geqslant 0}$: we construct $\underline{a} = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in A^{\mathbf{Z}_{\geqslant 0}}$ inductively such that $x_n = \Phi_n(\underline{a})$ for all $n \in \mathbf{Z}_{\geqslant 0}$. Put $a_0 = x_0 \in A$. Let $n \in \mathbf{Z}_{\geqslant 0}$ be such that $a_0, \dots, a_n \in A$ have been constructed such that for all $k \in \{0, \dots, n\}$, we have $x_k = \Phi_k(a_0, \dots, a_k)$. By the computation above, we have $\varphi(x_n) = \varphi(\Phi_n(\underline{a})) \equiv \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} \mod p^{n+1}A$ *i.e.* $x_{n+1} - \sum\limits_{i=0}^{n} p^i a_i^{p^{n+1-i}} \in p^{n+1}A$ (since $x_{n+1} - \varphi(x_n) \equiv 0 \mod p^{n+1}A$): there exists $a_{n+1} \in A$ (that may not be unique when A has p-torsion) such that $x_{n+1} = \sum\limits_{i=0}^{n+1} p^i a_i^{p^{n+1-i}} = \Phi_{n+1}(a_0, \dots, a_{n+1})$. $\square$

Let $\underline{Y} = (Y_0, Y_1, \dots)$ be a indeterminate.

Proposition 4. (*cf* [3, Chap. II, §6, Theorem 5]). There exist unique sequences of polynomials

$$(S_n)_{n\in\mathbf{Z}_{\geqslant 0}}, (P_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}, \underline{Y}]^{\mathbf{Z}_{\geqslant 0}}$$

Version: June 20, 2023

and $(I_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$ such that:

$$\begin{aligned} S_n(\underline{X},\underline{Y}), P_n(\underline{X},\underline{Y}) &\in \mathbf{Z}[X_0,\ldots,X_n,Y_0,\ldots,Y_n] \\ I_n(\underline{X}) &\in \mathbf{Z}[X_0,\ldots,X_n] \\ \Phi_n\big(S_0(\underline{X},\underline{Y}),\ldots,S_n(\underline{X},\underline{Y})\big) &= \Phi_n(\underline{X}) + \Phi_n(\underline{Y}) \\ \Phi_n\big(P_0(\underline{X},\underline{Y}),\ldots,P_n(\underline{X},\underline{Y})\big) &= \Phi_n(\underline{X})\Phi_n(\underline{Y}) \\ \Phi_n\big(I_0(\underline{X}),\ldots,I_n(\underline{X})\big) &= -\Phi_n(\underline{X}) \end{aligned}$$

Proof. • Let $A = \mathbf{Z}[\underline{X},\underline{Y}]$ be the polynomial ring. Denote by $\varphi\colon A \to A$ the unique ring endomorphism such that $\varphi(x_n) = X_n^p$ and $\varphi(Y_n) = Y_n^p$ for all $n \in \mathbf{Z}_{\geqslant 0}$. We have $\varphi(a) \equiv a^p \mod pA$ for all $a \in A$. As φ is a ring endomorphism and Φ_n has integral coefficients, we have $\varphi(\Phi_n(\underline{X}) + \Phi_n(\underline{Y})) = \Phi_n(\varphi(\underline{X})) + \Phi_n(\varphi(\underline{Y}))$ (resp. $\varphi(\Phi_n(\underline{X})\Phi_n(\underline{Y})) = \Phi_n(\varphi(\underline{X}))\Phi_n(\varphi(\underline{Y}))$, resp. $\varphi(-\Phi_n(\underline{X})) = -\Phi_n(\varphi(\underline{X}))$) for all $n \in \mathbf{Z}_{\geqslant 0}$. As $\Phi_n(\varphi(\underline{X})) = \Phi_{n+1}(\underline{X}) - p^{n+1}X_{n+1}$ and $\Phi_n(\varphi(\underline{Y})) = \Phi_{n+1}(\underline{Y}) - p^{n+1}Y_{n+1}$ by definition, this implies that $\varphi(\Phi_n(\underline{X}) + \Phi_n(\underline{Y})) \equiv \Phi_{n+1}(\underline{X}) + \Phi_{n+1}(\underline{Y}) \mod p^{n+1}A$ (resp. $\varphi(\Phi_n(\underline{X})\Phi_n(\underline{Y})) \equiv \Phi_{n+1}(\underline{X})\Phi_{n+1}(\underline{Y}) \mod p^{n+1}A$, resp. $\varphi(-\Phi_n(\underline{X})) \equiv -\Phi_{n+1}(\underline{X}) \mod p^{n+1}A$) for all $n \in \mathbf{Z}_{\geqslant 0}$. Lemma 3 thus implies that $\Phi_A(\underline{X})+\Phi_A(\underline{Y})$, $\Phi_A(\underline{X})\Phi_A(\underline{Y})$ and $-\Phi_A(\underline{X})$ belong to the image of Φ_A, which precisely means the existence of the sequences of polynomials $(S_n)_{n\in\mathbf{Z}_{\geqslant 0}}, (P_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X},\underline{Y}]^{\mathbf{Z}_{\geqslant 0}}$ and $(I_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$.
• The unicity is obvious in $\mathbf{Z}[p^{-1}][\underline{X},\underline{Y}]$ by induction. □

Example 5. One has

$$\begin{cases} S_0(X_0,Y_0) = X_0 + Y_0 \\ P_0(X_0,Y_0) = X_0Y_0 \end{cases}$$

and

$$\begin{cases} S_1(X_0,X_1,Y_0,Y_1) = X_1 + Y_1 - \sum\limits_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^iY_0^{p-i} \\ P_1(X_0,X_1,Y_0,Y_1) = X_1Y_0^p + X_0^pY_1 + pX_1Y_1 \end{cases}$$

Definition 6. Let A be a ring. Put

$$\mathsf{W}(A) = A^{\mathbf{Z}_{\geqslant 0}}$$

(as a set). If $\underline{a} = (a_0,a_1,\ldots), \underline{b} = (b_0,b_1,\ldots) \in \mathsf{W}(A)$, put

$$\begin{aligned} \underline{a} + \underline{b} &= \big(S_n(\underline{a},\underline{b})\big)_{n\in\mathbf{Z}_{\geqslant 0}} \\ \underline{a}.\underline{b} &= \big(P_n(\underline{a},\underline{b})\big)_{n\in\mathbf{Z}_{\geqslant 0}} \\ -\underline{a} &= \big(I_n(\underline{a})\big)_{n\in\mathbf{Z}_{\geqslant 0}} \end{aligned}$$

Remark 7. The map $\Phi_A\colon A^{\mathbf{Z}_{\geqslant 0}} \to A^{\mathbf{Z}_{\geqslant 0}}$ above is seen as a map $\Phi_A\colon \mathsf{W}(A) \to A^{\mathbf{Z}_{\geqslant 0}}$.

Proposition 8. (1) $A \mapsto (\mathsf{W}(A),+,.)$ is a functor on **Ring** to the category of sets endowed with two composition laws.
(2) If p is not a zero-divisor (resp. is a unit) in A, then Φ_A is injective (resp. bijective).
(3) $(\mathsf{W}(A),+,.)$ is a commutative ring with zero element $\underline{0} = (0,0,\ldots)$ and unit $(1,0,0,\ldots)$. The map Φ_A is a ring homomorphism.

Proof. (1) and (2) are obvious. For (3), let $B \to A$ be a surjective ring homomorphism, such that p is not a zero-divisor in B (one can take $B = \mathbf{Z}[X_a]_{a\in A}$, and $B \to A$; $X_a \mapsto a$). As Φ_B is injective, $(\mathsf{W}(B),+,.)$ identifies (*via* Φ_B) with a subring of $B^{\mathbf{Z}_{\geqslant 0}}$ (with the product structure). Since $B \to A$ is surjective, so is $\mathsf{W}(B) \to \mathsf{W}(A)$, and $(\mathsf{W}(A),+,.)$ fulfills the ring axioms. □

Definition 9. Let A be a ring. The *Teichmüller representative* of $a \in A$ is $[a] := (a,0,0,\ldots) \in \mathsf{W}(A)$.

Proposition 10. Let A be a ring. If $a,b \in A$, then $[ab] = [a].[b]$ in $\mathsf{W}(A)$.

Proof. Here again, it is enough to check the equality when A has no p-torsion, hence after applying Φ_A (since it is injective in the p-torsionfree case), but $\Phi_A([a]) = (a,a^p,a^{p^2},\ldots)$ is multiplicative. □

Proposition 11. There exists a sequence $(F_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathbf{Z}[\underline{X}]^{\mathbf{Z}_{\geqslant 0}}$ such that $F_n(\underline{X}) \in \mathbf{Z}[X_0,\ldots,X_{n+1}]$ and

$$(\forall n \in \mathbf{Z}_{\geqslant 0})\ \Phi_n\big(F_0(\underline{X}),\ldots,F_n(\underline{X})\big) = \Phi_{n+1}(\underline{X})$$

Proof. As in the proof of proposition 4, it is enough, using lemma 3, to check that if $A = \mathbf{Z}[\underline{X}]$, we have $\varphi(\Phi_n(\underline{X})) \equiv \Phi_{n+1}(\underline{X}) \mod p^{n+1}A$ for all $n \in \mathbf{Z}_{\geqslant 0}$, which is trivial. Here again, the unicity in $\mathbf{Z}[p^{-1}][\underline{X}]$ is obvious by induction. □

Example 12. We have

$$\begin{cases} F_0(X_0,X_1) = X_0^p + pX_1 \\ F_1(X_0,X_1,X_2) = X_1^p + pX_2 - \sum\limits_{i=1}^{p} \binom{p}{i} p^{i-1} X_1^i X_0^{p(p-i)} \end{cases}$$

Definition 13. Let A be a ring. The *Frobenius map* of $\mathsf{W}(A)$ is

$$F(\underline{a}) = \big(F_0(\underline{a}), F_1(\underline{a}), \ldots\big)$$

Proposition 14. Let A be a ring.
(1) $(\forall a \in A)\, F([a]) = [a^p]$.
(2) $(\forall n \in \mathbf{Z}_{\geqslant 0})\, F_n(\underline{X}) \equiv X_n^p \mod p\,\mathbf{Z}[\underline{X}]$. In particular, it $pA = 0$, then $F(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots)$.

Proof. (1) Considering a surjective ring homomorphism $B \to A$ where B has no p-torsion, which gives rise to a surjective ring homomorphism $\mathsf{W}(B) \to \mathsf{W}(A)$, we may reduce to the case where A has no p-torsion. Then $\Phi_A\colon \mathsf{W}(A) \to A^{\mathbf{Z}_{\geqslant 0}}$ is injective: it is enough to check that $\Phi_A(F([a])) = \Phi_A([a^p])$, *i.e.* that $\Phi_{n+1}([a]) = a^{p^{n+1}} = \Phi_n([a^p])$.
(2) By induction on $n \in \mathbf{Z}_{\geqslant 0}$, the case $n = 0$ following from the equality $F_0(\underline{X}) = X_0^p + pX_1$. Let $n \in \mathbf{Z}_{>0}$ be such that $F_i(\underline{X}) \equiv X_i^p \mod p\,\mathbf{Z}[\underline{X}]$ for $i \in \{0, \ldots, n-1\}$: we have $F_i(\underline{X})^{p^{n-i}} \equiv X_i^{p^{n+1-i}} \mod p^{n+1-i}\,\mathbf{Z}[\underline{X}]$ for $i \in \{0, \ldots, n-1\}$ by lemma 2, hence

$$\Phi_{n+1}(\underline{X}) = \Phi_n\big(F_0(\underline{X}), \ldots, F_n(\underline{X})\big) = \sum_{i=0}^{n} p^i F_i(\underline{X})^{p^{n-i}} \equiv p^n F_n(\underline{X}) + \sum_{i=0}^{n-1} p^i X_i^{p^{n+1-i}} \mod p^{n+1}\,\mathbf{Z}[\underline{X}]$$

As $\sum\limits_{i=0}^{n-1} p^i X_i^{p^{n+1-i}} = \Phi_{n+1}(\underline{X}) - p^n X_n^p - p^{n+1} X_{n+1}$, this implies that $p^n F_n(\underline{X}) \equiv p^n X_n^p \mod p^{n+1}\,\mathbf{Z}[\underline{X}]$ *i.e.* $F_n(\underline{X}) \equiv X_n^p \mod p\,\mathbf{Z}[\underline{X}]$. □

Definition 15. Let A be a ring. The *Verschiebung* of $\underline{a} = (a_0, a_1, \ldots) \in \mathsf{W}(A)$ is

$$V(\underline{a}) = (0, a_0, a_1, \ldots)$$

Proposition 16. Let A be a ring and $\underline{a}, \underline{b} \in \mathsf{W}(A)$.
(1) We have

$$\begin{cases} \Phi_A(F(\underline{a})) = \big(\Phi_1(\underline{a}), \Phi_2(\underline{a}), \ldots\big) = f(\Phi_A(\underline{a})) \\ \Phi_A(V(\underline{a})) = \big(0, p\Phi_0(\underline{a}), p\Phi_1(\underline{a}), \ldots\big) = v(\Phi_A(\underline{a})) \end{cases}$$

where $f(\underline{X}) = (X_1, X_2, \ldots)$ and $v(\underline{X}) = (0, pX_0, pX_1, \ldots)$.
(2) F is a ring endomorphism.
(3) V is an group endomorphism of $(\mathsf{W}(A), +)$.
(4) $FV = p\,\mathsf{Id}_{\mathsf{W}(A)}$ and $VF(\underline{a}) = (0, 1, 0, \ldots).\underline{a}$.
(5) $V(\underline{a}.F(\underline{b})) = V(\underline{a}).\underline{b}$ and $V(\underline{a}).V(\underline{b}) = pV(\underline{a}.\underline{b})$.
(6) $F(\underline{a}) \equiv \underline{a}^p \mod p\,\mathsf{W}(A)$.
(7) $\underline{a} = [a_0] + V(\underline{a}')$ where $\underline{a}' = (a_1, a_2, \ldots)$. In particular $\underline{a} = \sum\limits_{n=0}^{\infty} V^n([a_n])$.

Proof. (1) is computation. Using the usual trick, the proof of properties (2)-(7) reduces to the case when A has no p-torsion, hence after applying Φ_A since the latter is injective. (2) (resp. (3)) follows from the fact that f (resp. v) is a ring (resp. a group) homomorphism. (4) follows from the equality $f \circ v = p$ and $\Phi_A(0, 1, 0, 0, \ldots) = (0, p, p, \ldots)$. (5) follows from the corresponding statements on f and v in $A^{\mathbf{Z}_{\geqslant 0}}$. To prove (6), we check that $\Phi_A(F(\underline{a})) \equiv \Phi_A(\underline{a}^p) \mod p\,\mathsf{Im}(\Phi_A)$, *i.e.* that $f(\Phi_A(\underline{a})) - \Phi_A(\underline{a}^p) \in p\,\mathsf{Im}(\Phi_A)$. By lemma 3, this follows from the congrucences

$$\varphi\big(\Phi_{n+1}(\underline{X}) - \Phi_n(\underline{X})^p\big) \equiv \Phi_{n+2}(\underline{X}) - \Phi_{n+1}(\underline{X})^p \mod p^{n+2}\,\mathbf{Z}[\underline{X}],$$

which are obvious since $\varphi(\Phi_n(\underline{X})) = \Phi_{n+1}(\underline{X}) - p^{n+1} X_{n+1}$. Finally, (7) follows from the equalities $\Phi_0(\underline{a}) = a_0$ and $\Phi_n(\underline{a}) = a_0^{p^n} + p\Phi_{n-1}(\underline{a}')$ for all $n \in \mathbf{Z}_{>0}$, which precisely mean that $\Phi_A(\underline{a}) = \Phi_A([a_0] + V(\underline{a}'))$. □

Definition 17. Let A be a ring. For $n \in \mathbf{Z}_{\geqslant 0}$, let

$$\mathsf{Fil}^n\,\mathsf{W}(A) = V^n(\mathsf{W}(A)) = \big\{(0, \ldots, 0, a_n, a_{n+1}, \ldots)\,;\, (a_k)_{k \geqslant n} \in A^{\mathbf{Z}_{\geqslant n}}\big\} \subset \mathsf{W}(A).$$

This defines a decreasing filtration on $\mathsf{W}(A)$.

As $V^n(\underline{a} + \underline{b}) = V^n(\underline{a}) + V^n(\underline{b})$ and $V^n(\underline{a}).\underline{b} = V^n(\underline{a}.F^n(\underline{b}))$, $\mathsf{Fil}^n\,\mathsf{W}(A)$ is an ideal of $\mathsf{W}(A)$.

Definition 18. Let A be a ring. The *ring of Witt vectors of length* n is $\mathsf{W}_n(A) := \mathsf{W}(A)/\mathsf{Fil}^n\,\mathsf{W}(A)$.

Remark 19. In general, we have $V^n(\mathsf{W}(A))V^m(\mathsf{W}(A)) \not\subset V^{n+m}(\mathsf{W}(A))$, so the filtration is *not* compatible with the ring structure (however this is true if $pA = 0$).

Proposition 20. Let A be a ring such that $pA = 0$.
(1) $FV(\underline{a}) = VF(\underline{a}) = p\underline{a} = (0, a_0^p, a_1^p, \ldots)$ (so $(0, 1, 0, 0\ldots) = p$).
(2) $V^n(\underline{a})V^m(\underline{b}) = V^{n+m}\big(F^m(\underline{a}).F^n(\underline{b})\big)$.
(3) The p-adic and the $V(\mathsf{W}(A))$-adic filtration are the same, and finer than that defined by the filtration. In particular, $\mathsf{W}(A)$ is complete and separated for the p-adic topology.
(4) If A is perfect, all these topologies are the same, and $\mathsf{W}(A)/p\,\mathsf{W}(A) \xrightarrow{\sim} A$, and[1]

$$\underline{a} = (a_0, a_1, \ldots) = \sum_{n=0}^{\infty} V^n([a_n]) = \sum_{n=0}^{\infty} V^n F^n\big(\big[a_n^{p^{-n}}\big]\big) = \sum_{n=0}^{\infty} p^n\big[a_n^{p^{-n}}\big]$$

Proof. (1) Follows from proposition 14 (2): if $\underline{a} = (a_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathsf{W}(A)$, we have $F(\underline{a}) = (a_0^p, a_1^p, \ldots)$, so $VF(\underline{a}) = (0, a_0^p, a_1^p, \ldots) = FV(\underline{a})$, so that $VF = FV = p\,\mathsf{Id}_{\mathsf{W}(A)}$.
By proposition 16 (5), we have $V(\underline{a}).\underline{b} = V(\underline{a}.F(\underline{b}))$, hence $V^n(\underline{a}).\underline{b} = V^n(\underline{a}.F^n(\underline{b}))$ by an immediate induction on $n \in \mathbf{Z}_{\geqslant 0}$. Applied to $V^m(\underline{b})$ instead of $\underline{b}$, we get $V^n(\underline{a}).V^m(\underline{b}) = V^n\big(\underline{a}.F^nV^m(\underline{b})\big)$. As $F^nV^m(\underline{b}) = V^mF^n(\underline{b})$ (by (1)), we have $\underline{a}.F^nV^m(\underline{b}) = V^m(F^m(\underline{a}).F^n(\underline{b}))$, hence the result.
For (3), one proves by induction that $(V(\mathsf{W}(A)))^k = p^{k-1}V(\mathsf{W}(A))$ (using the second formula of proposition 16 (5)). As $p\,\mathsf{W}(A) = VF(\mathsf{W}(A)) \subset V(\mathsf{W}(A))$, one has $p^k\,\mathsf{W}(A) \subset (V(\mathsf{W}(A)))^k \subset p^{k-1}\,\mathsf{W}(A)$. Moreover, we have

$$(*) \qquad p^k\,\mathsf{W}(A) = V^nF^n(\mathsf{W}(A)) = \big\{(0, \ldots, 0, a_k, a_{k+1}, \ldots) \in \mathsf{W}(A)\,;\,(\forall n \in \mathbf{Z}_{\geqslant 0})\, a_n \in A^{p^k}\big\} \subset \mathsf{Fil}^k\,\mathsf{W}(A)$$

so that the p-adic topology is finer that that defined by the filtration $\mathsf{Fil}^\bullet\,\mathsf{W}(A)$.
(4) follows from the fact that $(*)$ is an equality when A is perfect. $\square$

Exercises[2]

Exercise 21. Let p be a prime number and A a ring of characteristic p.
(1) Show that $\mathsf{W}(A)$ is an integral domain if and only if A is an integral domain.
(2) Show that $\mathsf{W}(A)$ is reduced if and only if A is reduced.
(3) Show that A is perfect if and only if $\mathsf{W}(A)/p\,\mathsf{W}(A)$ is reduced.

Exercise 22. Let A be a ring of characteristic p. Show that the V-adic and the p-adic topologies coincide if and only if the map $A \to A$; $a \mapsto a^p$ is surjective.

Exercise 23. Let k be a field of characteristic p. Show that $\mathsf{W}(k)$ is noetherian if and only if k is perfect [hint: compute $\dim_k(V(\mathsf{W}(k))/V(\mathsf{W}(k))^2)$].

Exercise 24. Let A be a ring and p a prime number which is not a zero divisor in A. Let $\sigma\colon A \to A$ be an endomorphism such that $\sigma(a) \equiv a^p \mod pA$ for all $a \in A$.
(1) Show that there exists a unique ring homomorphism $s_\sigma\colon A \to \mathsf{W}(A)$ such that $s_\sigma \circ \sigma = F_A \circ s_\sigma$ and $\Phi_0 \circ s_\sigma = \mathsf{Id}_A$.
(2) Let B be a ring such that p is not a zero divisor in B, and $\sigma'\colon B \to B$ an endomorphism such that $\sigma'(b) \equiv b^p \mod pB$ for all $b \in B$, and $u\colon A \to B$ a ring homomorphism such that $u \circ \sigma = \sigma' \circ u$. Show that $\mathsf{W}(u) \circ s_\sigma = s_{\sigma'} \circ u$.
(3) Let $t_\sigma\colon A \to \mathsf{W}(A/pA)$ be the composite of s_σ and the natural ring homomorphism $\mathsf{W}(A) \to \mathsf{W}(A/pA)$. Show that t_σ induces a ring homomorphism $t_{\sigma,n}\colon A/p^nA \to \mathsf{W}_n(A/pA)$ for all $n \in \mathbf{Z}_{>0}$.
(4) Show that $t_{\sigma,n}$ is an isomorphism when A/pA is perfect.
(5) Show that if A/pA is perfect and A is separated and complete for the p-adic topology, then t_σ is an isomorphism.

[1] Using proposition 16 (7).
[2] Mostly from Bourbaki.

Exercise 25. Let A be a ring and p a prime number which is not a zero divisor in A.
(1) Show there exists a unique ring homomorphism $s_A\colon \mathsf{W}(A) \to \mathsf{W}(\mathsf{W}(A))$ such that $s_A \circ F_A = F_{\mathsf{W}(A)} \circ s_A$ and $\Phi_0 \circ s_A = \mathsf{Id}_{W(A)}$. Show that it is the unique ring homomorphism such that $\Phi_n \circ s_\sigma = F_A^n$ for all $n \in \mathbf{Z}_{\geqslant 0}$.
(2) Let $\mathcal{A} = \mathbf{Z}[X_n]_{n\in\mathbf{Z}_{\geqslant 0}}$ and $\mathbf{X} = (X_n)_{n\in\mathbf{Z}_{\geqslant 0}} \in \mathsf{W}(\mathcal{A})$. Write $s_{\mathcal{A}}(\mathbf{X}) = (s_n(\mathbf{X}))_{n\in\mathbf{Z}_{\geqslant 0}}$, where $s_n(\mathbf{X}) \in \mathsf{W}(\mathcal{A})$. Show that $s_A(\underline{a}) = (s_n(\underline{a}))_{n\in\mathbf{Z}_{\geqslant 0}}$ for all $\underline{a} = (a_0, a_1, \ldots) \in \mathsf{W}(A)$.
(3) For all ring homomorphism $u\colon A \to B$, show that $s_B \circ \mathsf{W}(u) = \mathsf{W}(\mathsf{W}(u)) \circ s_A$.
(4) Show that the maps $\mathsf{W}(s_A) \circ s_A$ and $s_{\mathsf{W}(A)} \circ s_A$ from $W(A)$ to $\mathsf{W}(\mathsf{W}(\mathsf{W}(A)))$ are equal.

Exercise 26. Let K be a local field of characteristic $p > 0$. Show that it has only one coefficient field.

Exercise 27. Let $(K, |.|)$ be a local field, $\overline{K}$ an algebraic closure of K, and k/κ_K a finite field extension. Denote by L the unique subextension of $\overline{K}/K$ that is unramified and such that $\kappa_L = k$. Show that

$$L \simeq \begin{cases} k \otimes_{\kappa_K} K & \text{if } \mathsf{char}(K) = \mathsf{char}(\kappa_K) \\ \mathsf{W}(k) \otimes_{\mathsf{W}(\kappa_K)} K & \text{if } \mathsf{char}(K) \neq \mathsf{char}(\kappa_K) \end{cases}$$

Exercise 28. Let $\mathbf{Q}_p^{\mathrm{ur}}$ be the maximal unramified extension of $\mathbf{Q}_p$ in $\overline{\mathbf{Q}}_p$. Show that the completion of $\mathbf{Q}_p^{\mathrm{ur}}$ for $|.|_p$ is $\mathsf{W}(\overline{\mathbf{F}}_p)[p^{-1}]$.

References

[1] N. Bourbaki – *Éléments de mathématique. Algèbre commutative, chapitres 8 et 9*, Masson, 1983.
[2] A. Grothendieck – *Groupes de Barsotti-Tate et cristaux de Dieudonné*, Séminaire de Mathématiques Supérieures, vol. 45, Les Presses de l'Université de Montréal, 1974.
[3] J.-P. Serre – *Corps locaux*, Publications de l'Institut de Mathématique de l'Université de Nancago, vol. VIII, Hermann, 1962.

Institut de Mathématiques de Bordeaux, Université Bordeaux, 351, cours de la Libération, 33405 Talence, France
Email address: olivier.brinon@math.u-bordeaux.fr