WITT VECTORS WITH p-ADIC COEFFICIENTS AND FONTAINE'S RINGS

CHRISTOPHER DAVIS AND KIRAN S. KEDLAYA

ABSTRACT. We describe an alternate construction of some of the basic rings introduced by Fontaine in p-adic Hodge theory. In our construction, the central role is played by the ring of p-typical Witt vectors over a p-adic valuation ring, rather than the Witt vectors over a ring of positive characteristic. This suggests the possibility of forming a meaningful global analogue of p-adic Hodge theory.

INTRODUCTION

For X a smooth projective variety over the complex numbers, there is a canonical isomorphism

$$H^i_{\mathrm{Betti}}(X, \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{C} \cong H^i_{\mathrm{dR}}(X, \mathbb{C})$$

of the Betti and (holomorphic) de Rham cohomologies. This isomorphism equips a single finite dimensional $\mathbb{C}$-vector space with two separate structures, an integral lattice (from the integral Betti cohomology) and a filtration (from the Hodge filtration on de Rham cohomology). The relationship between these, particularly in families, is the focus of *Hodge theory*.

Similarly, *p-adic Hodge theory* focuses on the relationship between different cohomology theories associated to varieties over p-adic fields, such as étale, de Rham, and crystalline cohomology. The most notable difference is that one role of the ring $\mathbb{C}$ in the comparison isomorphism of ordinary Hodge theory, as the common coefficient ring over which Betti and de Rham cohomology can be compared, is played by some rather larger *big rings* constructed by Fontaine.

Fontaine's rings are usually manufactured as follows. The first step is a *field of norms* construction: one forms the inverse limit of $\mathcal{O}_{\mathbb{C}_p}/p\mathcal{O}_{\mathbb{C}_p}$ under the Frobenius map, for $\mathcal{O}_{\mathbb{C}_p}$ the valuation subring of a completed algebraic closure $\mathbb{C}_p$ of $\mathbb{Q}_p$. This limit turns out to be the valuation subring of a complete algebraically closed field of characteristic p. One then returns to mixed characteristic using the functor of p-typical Witt vectors. The effect of the construction is to separate the cohomological and geometric functions of the prime number p: the cohomological functions remain with the number p, while the geometric functions are transferred to a certain Teichmüller element. By exploiting the relationship between these two elements (they are not equal, but are in some sense close together), one builds the various rings used in Fontaine's theory.

The goal of this paper is not to make any new assertions in p-adic Hodge theory itself, but to describe an alternate construction of some of Fontaine's rings. In this

---

Date: February 21, 2011.

Davis was supported by the Max-Planck-Institut für Mathematik (Bonn). Kedlaya was supported by NSF (CAREER grant DMS-0545904), DARPA (grant HR0011-09-1-0048), MIT (NEC Fund, Cecil and Ida Green professorship).

construction, rather than passing to characteristic p and back, we directly apply the p-typical Witt vector functor to the mixed-characteristic ring $\mathcal{O}_{\mathbb{C}_p}$. In the resulting construction, one has a natural interpretation of the evaluation map θ occurring in Fontaine's theory, in terms of the ghost map on Witt vectors. One also has a natural interpretation of the Gauss norms appearing in the work of Berger, Colmez, and others.

We do not have in mind any immediate application of this construction. Our interest in it is instead based on longer-term considerations (previously hinted at in [14, §4]). For one, we expect that one can use the p-typical part of the absolute de Rham-Witt complex of Hesselholt-Madsen [10] to give a simplified description of the comparison maps in p-adic Hodge theory. For another, we hope that one can go further, developing an analogue of p-adic Hodge theory encompassing the infinite place together with all finite places, which would again be related to the construction of Hesselholt-Madsen. Two necessary steps in the latter process are replacing p-typical Witt vectors with big Witt vectors, and allowing the use of an archimedean absolute value in place of the p-adic absolute value. Our presentation is structured with these ultimate goals in mind.

Notations and conventions. All rings considered will be commutative with unit unless otherwise specified. A *map* of rings will not be assumed to be a homomorphism (e.g., the Verschiebung map on Witt vectors). For K a field, we write $\overline{K}, \hat{K}, G_K$ for the algebraic closure, completion, and absolute Galois group of K.

We fix a completed algebraic closure $\mathbb{C}_p$ of $\mathbb{Q}_p$, and write $\mathcal{O}_{\mathbb{C}_p}$ for the ring of integers of $\mathbb{C}_p$. We write $|\cdot|$ for the p-adic norm on $\mathbb{C}_p$ with the normalization $|p| = p^{-1}$. (We use multiplicative rather than additive notation to emphasize a potential parallel with the archimedean norm on $\mathbb{C}$.)

The symbol $\mathbb{N}$ will denote the *positive* integers as a set or a multiplicative monoid. That is, $0 \notin \mathbb{N}$.

Acknowledgments. The authors thank Laurent Berger, James Borger, Lars Hesselholt, Abhinav Kumar, Ruochuan Liu, Joe Rabinoff, and Liang Xiao for helpful discussions and suggestions. In particular, Abhinav Kumar read an earlier draft of this paper and provided many useful comments, including improvements of several proofs.

1. Big Witt vectors

We begin by recalling the basic properties of the big Witt vector functor. (We will switch to p-typical Witt vectors in Section 2.) The standard published references are the book of Hazewinkel [8, §17] and the exercises of [3, Chapter IX]. An additional unpublished reference, which we found very helpful, is the preprint of Hesselholt [9].

Definition 1.1. *For A a commutative ring with unit, define $\mathbb{W}(A)$ to be the set $A^{\mathbb{N}}$, equipped with the* ghost map $w : \mathbb{W}(A) \to A^{\mathbb{N}}$ *defined by the formula*

$$(a_1, a_2, \dots) \mapsto (w_1, w_2, \dots), \qquad w_n = \sum_{d|n} d a_d^{n/d}.$$

Let $w_n : \mathbb{W}(A) \to A$ be the composition of w with the projection onto the n-th factor. For $\underline{a} = (a_1, a_2, \dots)$, we refer to a_n as the n-th Witt component *of $\underline{a}$ and to $w_n(\underline{a})$ as the n-th* ghost component *of $\underline{a}$.*

Define the set $\Lambda(A) = 1 + tA[\![t]\!]$ *and the bijective* exponential map $E : \mathbb{W}(A) \to \Lambda(A)$ *given by*

$$E((a_1, a_2, \dots)) = \prod_{i=1}^{\infty} (1 - a_i t^i)^{-1}.$$

This map satisfies $s \circ E = w$*, where* $s : \Lambda(A) \to A^{\mathbb{N}}$ *is given by the formula*

$$s(f) = (s_1, s_2, \dots), \qquad s_1 t + s_2 t^2 + \cdots = \frac{tf'}{f} = t\frac{d}{dt}\log(f).$$

Equip the target $A^{\mathbb{N}}$ *of the ghost map with the product ring structure. For* $n \in \mathbb{N}$*, define the polynomials* $d_n, p_n \in \mathbb{Q}[X_1, X_2, \dots, Y_1, Y_2, \dots]$ *by the formulas*

$$w(\underline{a}) - w(\underline{b}) = w((d_n(\underline{a}, \underline{b}))_{n \in \mathbb{N}}), \quad w(\underline{a})w(\underline{b}) = w((p_n(\underline{a}, \underline{b}))_{n \in \mathbb{N}}) \quad (\underline{a}, \underline{b} \in \mathbb{W}(A)).$$

By Proposition 1.2 below, these polynomials have coefficients in $\mathbb{Z}$*. We may thus use them to equip* $\mathbb{W}(A)$ *with a ring structure (functorially in* A*) for which*

$$(\underline{a} - \underline{b})_n = d_n(\underline{a}, \underline{b}), \quad (\underline{ab})_n = p_n(\underline{a}, \underline{b}) \qquad (\underline{a}, \underline{b} \in \mathbb{W}(A);\ n \in \mathbb{N})$$

(i.e., the ghost map is a ring homomorphism). We call $\mathbb{W}(A)$ *the* ring of big Witt vectors*, or the* big Witt ring*, with coefficients in* A*.*

Proposition 1.2. *The polynomials* $d_n(X_i, Y_i), p_n(X_i, Y_i)$ *have coefficients in* $\mathbb{Z}$*.*

Proof. This can be checked one prime at a time, directly as in [8, Lemma 17.1.3] or using the Dwork lemma (Lemma 1.6) as in [9, Proposition 1.2]. Another approach is as follows. Put $A = \mathbb{Z}[X_1, X_2, \dots, Y_1, Y_2, \dots]$ and

$$\underline{X} = (X_1, X_2, \dots), \quad \underline{Y} = (Y_1, Y_2, \dots) \in \mathbb{W}(A);$$

it suffices to check that $w(\underline{X}) - w(\underline{Y}), w(\underline{X})w(\underline{Y}) \in w(\mathbb{W}(A))$. We do this using a "splitting principle" modeled on [16], in the spirit of [7] (but without reference to Grothendieck groups). Let R be the integral closure of A in some algebraically closed field. For each $n \in \mathbb{N}$, we can then find $r_1, \dots, r_n, s_1, \dots, s_n \in R$ so that

$$E(\underline{X}), E(\underline{Y}) \equiv \prod_{i=1}^{n} (1 - r_i t)^{-1}, \prod_{j=1}^{n} (1 - s_j t)^{-1} \pmod{t^{n+1}}.$$

Since $s \circ E = w$ and s converts series multiplication into addition, we have

$$s^{-1}(w(\underline{X}) - w(\underline{Y})) \equiv \prod_{i=1}^{n} (1 - r_i t)^{-1}(1 - s_i t) \pmod{t^{n+1}}$$

$$s^{-1}(w(\underline{X})w(\underline{Y})) \equiv \prod_{i,j=1}^{n} (1 - r_i s_j t)^{-1} \pmod{t^{n+1}}.$$

The products on the right side belong to both $\Lambda(R)$ and $\Lambda(A \otimes_{\mathbb{Z}} \mathbb{Q})$, hence to $\Lambda(A)$ because A is factorial (and thus integrally closed in its fraction field). Since this holds for each $n \in \mathbb{N}$, we conclude that $w(\underline{X}) - w(\underline{Y}), w(\underline{X})w(\underline{Y}) \in w(\mathbb{W}(A))$, as desired. □

Remark 1.3. *The definition of the ring structure on* $\mathbb{W}(A)$ *also provides a ring structure on* $\Lambda(A)$*; this ring is called the* universal λ-ring *over* A*. Beware that there are at least four reasonable choices for the normalization of the definitions of* $\Lambda(A)$ *and* E*, depending on the signs on* $a_i t^i$ *and on the exponent of* $1 - a_i t^i$*.*

Remark 1.4. *From the definition of d_n and p_n, one observes that they only include the variables X_i, Y_i for $i \mid n$. Moreover, d_n is homogeneous of degree n under the weighting in which X_i, Y_i have degree i (because the same is true of w_n).*

We now introduce the mechanism for passing from big Witt vectors to p-typical Witt vectors.

Definition 1.5. *A* truncation set *is a nonempty subset S of $\mathbb{N}$ which is closed under taking divisors; that is, if $d \mid n$ and $n \in S$, then $d \in S$. For S a truncation set and A a ring, let $\mathbb{W}_S(A) \cong A^S$ denote the quotient of $\mathbb{W}(A)$ in which only the components indexed by S are retained. By Remark 1.4, the formulas defining addition and multiplication of Witt vectors induce ring operations on $\mathbb{W}_S(A)$ compatible with the projection $\mathbb{W}(A) \to \mathbb{W}_S(A)$.*

Because the ring $A^{\mathbb{N}}$ has simpler ring operations than $\mathbb{W}(A)$, it is helpful to identify the image of the ghost map inside $A^{\mathbb{N}}$, especially when the ghost map is injective (i.e., A is torsion-free). The following lemma (also known as the *Cartier-Dwork lemma* or the *Cartier-Dieudonné-Dwork lemma*) does this; as noted earlier, this is often used as part of the construction of Witt vectors (as part of a proof of Proposition 1.2).

Lemma 1.6 (Dwork's lemma)**.** *Let A be a commutative ring with unit. Let S be a truncation set. For every prime number $p \in S$, let $\phi_p : A \to A$ be a ring homomorphism with the property that $\phi_p(a) \equiv a^p \pmod{pA}$ for each $a \in A$. Then a sequence (w_n) is in the image of the ghost map on $\mathbb{W}_S(A)$ if and only if $w_n \equiv \phi_p(w_{n/p}) \pmod{p^{v_p(n)}A}$ for every prime number p and for every $n \in \mathbb{N}$ with $p|n$. (Here v_p denotes the p-adic valuation on $\mathbb{Z}$.)*

Proof. See [9, Lemma 1.1]. In the case $S = \mathbb{N}$, see also [8, Lemma 17.6.1] or [3, Exercise IX.1.32]. □

The construction of the ring of Witt vectors also provides some additional operations. Beware that of these, only Frobenius is a ring homomorphism in general.

Definition 1.7. *Fix a ring A and a natural number $n \in \mathbb{N}$.*

1. *The* Teichmüller map *$[\ ] : A \to \mathbb{W}(A)$ acts as $a \mapsto (a, 0, 0, \ldots)$. It is a multiplicative map.*
2. *Define the map $\tilde{F}_n : A^{\mathbb{N}} \to A^{\mathbb{N}}$ which sends a sequence $(w_1, w_2, \ldots)$ to $(w_n, w_{2n}, \ldots)$. There exists a unique functorial construction of a ring homomorphism $F_n : \mathbb{W}(A) \to \mathbb{W}(A)$ (the n-th* Frobenius map*) such that $w \circ F_n = \tilde{F}_n \circ w$. (As in the definition of the Witt vectors, this amounts to checking that certain universal polynomials have integer coefficients. One derivation uses the splitting principle; another is* [8, §17.3]*.) Note that $F_m \circ F_n = F_{mn}$ for all $m, n \in \mathbb{N}$.*
3. *The map $V_n : \mathbb{W}(A) \to \mathbb{W}(A)$ which sends $(a_1, a_2, \ldots)$ to the sequence $(b_1, b_2, \ldots)$, defined by $b_{nj} := a_j$ and $b_i := 0$ if $n \nmid i$, is an additive map (because it corresponds to the substitution $t \mapsto t^n$ in $\Lambda(A)$). It is called the n-th* Verschiebung map*. Note that $V_m \circ V_n = V_{mn}$ for all $m, n \in \mathbb{N}$.*

For S a truncation set, one composes with the projection $\mathbb{W}(A) \to \mathbb{W}_S(A)$ to obtain a Teichmüller map $[\ ] : A \to \mathbb{W}_S(A)$. For S, S' two truncation sets, one obtains a Frobenius map $F_n : \mathbb{W}_S(A) \to \mathbb{W}_{S'}(A)$ for each $n \in \mathbb{N}$ with $nS' \subseteq S$, and a Verschiebung map $V_n : \mathbb{W}_S(A) \to \mathbb{W}_{S'}(A)$ for each $n \in \mathbb{N}$ with $n^{-1}S' \cap \mathbb{N} \subseteq S$.

Remark 1.8. *Another important feature of Witt vectors is the* diagonal homomorphism $\Delta : \mathbb{W}(A) \to \mathbb{W}(\mathbb{W}(A))$, *for which* $\Delta([r]) = [[r]]$. *See* [8, Theorem 17.6.17] *or* [3, Exercise IX.1.15(b)].

In terms of the Verschiebung, we have the following useful interpretation of the Witt components.

Proposition 1.9. *Equip* $\mathbb{W}(A)$ *with the product topology induced by the discrete topology on* A. *Then for* $\underline{a} \in \mathbb{W}(A)$, *there is a unique sequence* $(b_1, b_2, \dots)$ *in* A *for which*

$$\underline{a} = \sum_{i=1}^{\infty} V_i([b_i]),$$

namely the sequence $\underline{a}$ *itself.*

Proof. This is easily seen using the exponential map (see the proof of Proposition 1.2). See also [9, Lemma 1.5(i)]. □

Here are some useful relations among Frobenius and Verschiebung. (Each relation also applies to truncated Witt vectors, as long as all operations involved are valid.)

Proposition 1.10. *For any* $m, n \in \mathbb{N}$ *and any* $\underline{a}, \underline{b} \in \mathbb{W}(A)$,

$$\begin{aligned}
(F_n \circ V_n)(\underline{a}) &= n\underline{a} \\
\underline{a}V_n(\underline{b}) &= V_n(F_n(\underline{a})\underline{b}) \\
(F_m \circ V_n)(\underline{a}) &= (V_n \circ F_m)(\underline{a}) \quad \textit{if } \gcd(m,n) = 1 \\
V_m([a])V_n([b]) &= \gcd(m,n) V_{\mathrm{lcm}(m,n)}([a^{n/\gcd(m,n)} b^{m/\gcd(m,n)}]) \\
F_n([a]) &= [a^n] \\
[a] \sum_{i=1}^{\infty} V_i([b_i]) &= \sum_{i=1}^{\infty} V_i([a^i b_i]).
\end{aligned}$$

Proof. Each identity can be checked easily on ghost components. (Compare [9, Lemma 1.5].) □

Lemma 1.11. *Put* $\underline{a} = n \in \mathbb{W}(\mathbb{Z})$ *for some* $n \in \mathbb{Z}$. *Then for any* $d \in \mathbb{N}$, a_d *is divisible by* $n/\gcd(d,n)$.

Proof. It suffices to check that for each prime p, if we put $j = v_p(n)$, then for any $i \le j$ and any $d \in \mathbb{N}$ divisible by p^i, a_d is divisible by p^{j-i}. We prove this by induction on d. Since $w(\underline{a}) = (n, n, \dots)$, we have

$$\sum_{e|d} e a_e^{d/e} = n.$$

The right side is divisible by p^j. For each $e \neq d$ on the left side, we have $v_p(e) = k$ for some $k \le i$; then e is divisible by p^k while $a_e^{d/e}$ is divisible by $p^{(d/e)(j-k)}$ by the induction hypothesis. It follows that da_d is divisible by p^j, so a_d is divisible by p^{j-i} as desired. □

2. p-typical Witt vectors

Throughout this section, fix a prime number p. We now restrict attention to the p-typical Witt vectors; although these exhibit special features over a ring of characteristic p (i.e., in which $p \cdot 1 = 0$), it is crucial for our work not to restrict to this case. A useful summary of p-typical Witt vectors appears in Illusie's article on the de Rham-Witt complex [11].

Definition 2.1. *For A a commutative ring with unit, define the* ring of p-typical Witt vectors*, or* p-typical Witt ring*, with coefficients in A to be the ring $W(A) := \mathbb{W}_S(A)$ for the truncation set $S = \{1, p, p^2, \dots\}$. (Note the change from boldface $\mathbb{W}$ to roman W.) Similarly, for m a nonnegative integer, define the* ring of (p-typical) Witt vectors of length $m+1$ *with coefficients in A to be the ring $W_{p^m}(A) := \mathbb{W}_S(A)$ for the truncation set $\{1, p, \dots, p^m\}$. (This is often notated $W_{m+1}(A)$, e.g., in* [17]*. It might be more consistent to write $W_{p^\infty}(A)$ instead of $W(A)$, as is done in* [8]*, but we will refer to $W(A)$ so often that a more compact notation is desirable.) We have an isomorphism*

$$W(A) \cong \varprojlim W_{p^m}(A),$$

where the inverse limit is taken over all nonnegative integers m, and the transition maps are the natural projections $W_{p^{m+1}}(A) \to W_{p^m}(A)$.

The rings $W(A)$ and $W_{p^m}(A)$ again receive a multiplicative Teichmüller map $[\cdot]$ from A, by projection from $\mathbb{W}(A)$. However, we only have Frobenius and Verschiebung maps $F_n : W(A) \to W(A)$ if n is a power of p. When we speak of the *Frobenius map F or* the *Verschiebung map V on $W(A)$, we mean the one with $n = p$. Note that F induces a map $W_{p^m}(A) \to W_{p^{m-1}}(A)$ while V induces a map $W_{p^m}(A) \to W_{p^{m+1}}(A)$.*

Remark 2.2. *Often in contexts where big Witt vectors do not appear, the components of a p-typical Witt vector are indexed $a_0, a_1, a_2, \dots$ instead of $a_1, a_p, a_{p^2}, \dots$. We will not do this.*

Dwork's lemma (Lemma 1.6) specializes to the p-typical case as follows.

Lemma 2.3 (Dwork's lemma, p-typical case)**.** *Let A be a commutative ring with unit. Suppose that there exists a ring homomorphism $\phi : A \to A$ such that $\phi(a) \equiv a^p \pmod{pA}$ for each $a \in A$. Then a sequence (w_{p^i}) is in the image of the ghost map on $W(A)$ if and only if $w_{p^{i+1}} \equiv \phi(w_{p^i}) \pmod{p^{i+1}A}$ for all $i \geq 0$.*

Proof. This is immediate from Lemma 1.6; see also [3, IX.1, Lemma 2]. □

One rarely considers $W(A)$ in cases where p is a unit in A, as in this case the ghost map is an isomorphism of rings. Let us now consider the opposite extreme case, in which A is of characteristic p. Here, we have the following observation, which explains the name "Frobenius" for the maps F_n.

Proposition 2.4. *For A a ring of characteristic p, the Witt vector Frobenius map $F : W(A) \to W(A)$ is the same as the functorially induced map $W(\varphi)$, where $\varphi : a \mapsto a^p$ is the usual p-power Frobenius map. In other words, F takes $(a_1, a_p, \dots)$ to $(a_1^p, a_p^p, \dots)$.*

Proof. See [11, Part 0, (1.3.5)], or [9, Lemma 1.8]. □

In characteristic p, we can simplify the relations among F and V from Proposition 1.10, as follows.

Proposition 2.5. *If A is a characteristic p ring and $\underline{a} \in W(A)$, then $VF(\underline{a}) = p\underline{a}$; consequently, F and V commute.*

Proof. See [9, Lemma 1.12], [11, Part 0, (1.3.7) and (1.3.8)], or [8, Proposition 17.3.16]. □

Let us now assume further that A is a ring of characteristic p which is *perfect*, i.e., for which the p-th power (Frobenius) homomorphism on A is bijective. (Note that Frobenius is automatically injective whenever A is a field.) In this case, the additive description of Witt vectors from Proposition 1.9 specializes quite simply.

Corollary 2.6. *Let A be a perfect ring of characteristic p. Then every Witt vector $\underline{a} = (a_1, a_p, \ldots) \in W(A)$ has a unique representation as a sum*

$$\sum_{i=0}^{\infty} p^i [b_{p^i}] \qquad (b_{p^i} \in A)$$

convergent for the p-adic topology, namely with $b_{p^i} = a_{p^i}^{p^{-i}}$.

Proof. See [11, Part 0, Remark 1.3.24]. Alternatively, note that over any characteristic p ring, we have $p^i = V^i F^i$, by Proposition 2.5. Then use Proposition 2.4, Proposition 1.9, and the fact that our ring is perfect. □

Remark 2.7. *Using Corollary 2.6, it is not difficult to show that $W(A)$ is an integral domain whenever A is an integral domain of characteristic p (by reducing to the perfect case). Conversely, if $W(A)$ is a domain, then A must also be a domain because the Teichmüller map is multiplicative; moreover, A must be of characteristic p, or else the equation $V(p)(p - V(p)) = 0$ (a consequence of Proposition 1.10) would imply that $V(p)$ is a zero-divisor.*

Finally, in the case where A is a perfect field of characteristic p, one has the following well-known result of Witt, which sparked the development of the whole theory of Witt vectors. (There is an analogue for perfect rings of characteristic p; see [17, Chapter II, Section 5].)

Proposition 2.8. *Let A be a perfect field of characteristic p. Then every complete discrete valuation ring with maximal ideal (p) and residue field A is canonically isomorphic to $W(A)$.*

Proof. For the fact that $W(A)$ is indeed a complete DVR with maximal ideal (p) and residue field A, see [3, Proposition IX.1.8] or [11, Part 0, Corollary 1.3.23]. For the canonical isomorphism of any other such object with $W(A)$, see [17, *op. cit.*]. □

3. Submultiplicative seminorms

Recall that given a multiplicative norm $|\cdot|$ on a ring R, for any $\rho > 0$ one can define a multiplicative norm $|\cdot|_\rho$ on the polynomial ring $R[T]$ by the formula

$$\left| \sum_i a_i T^i \right|_\rho = \max_i \{ |a_i| \rho^i \}.$$

These are sometimes called *Gauss norms*, since the fact that they are multiplicative generalizes Gauss's observation that a product of primitive polynomials over the integers is primitive. Similarly, given a submultiplicative norm on a ring A, one can construct submultiplicative norms on certain truncated Witt vector rings with coefficients in A. However, in most cases these are not multiplicative even if the original norm is multiplicative.

Definition 3.1. *Let G be an abelian group. A* seminorm *on G is a function $|\cdot|: G \to [0, +\infty)$ satisfying the following conditions.*

(a) We have $|0| = 0$.

(b) For all $g, h \in G$, $|g - h| \leq |g| + |h|$.

If in (a) we have $|g| = 0$ if and only if $g = 0$, we say that the seminorm is a norm. *If in (b) we always have $|g - h| \leq \max\{|g|, |h|\}$, we also say that the seminorm is* nonarchimedean. *We will only consider nonarchimedean seminorms in this paper, but the reader is encouraged to imagine possible archimedean analogues of our constructions.*

Let A be a nonzero commutative ring with unit. A seminorm on the additive group on A is submultiplicative *if it satisfies the following conditions.*

(a) We have $|1| = 1$.

(b) For all $a, b \in A$, $|ab| \leq |a||b|$.

If in (b) we always have $|ab| = |a||b|$, we also say that the seminorm is multiplicative. *(For the zero ring, a reasonable convention seems to be that the zero norm is submultiplicative but not multiplicative.)*

Lemma 3.2. *Let A be a commutative ring with unit, equipped with a nonarchimedean submultiplicative seminorm $|\cdot|$. Let S be a truncation set. Choose $\underline{a}, \underline{b} \in \mathbb{W}_S(A)$ and put $\underline{c} = \underline{a} - \underline{b}$. Then for any $n \in S$,*

$$|c_n| \leq \max_{d|n}\{|a_{n/d}|^d, |b_{n/d}|^d\}.$$

Proof. This is immediate from the homogeneity assertion in Remark 1.4. □

Theorem 3.3. *Let A be a commutative ring with unit, equipped with a nonarchimedean submultiplicative seminorm $|\cdot|$. Let $|\cdot|_{\mathbb{Z}}$ be a multiplicative norm on $\mathbb{Z}$ such that $|n| \leq |n|_{\mathbb{Z}}$ for all $n \in \mathbb{Z}$. Let S be a truncation set. For any $r \in \mathbb{R}$ with*

$$0 \leq r \leq \inf_{n \in S}\{n^{-1}\},$$

the function $|\cdot|_r$ on $\mathbb{W}_S(A)$ defined by

$$|\underline{a}|_r = \sup_{n \in S}\{|a_n|^{1/n}|n|_{\mathbb{Z}}^r\} \tag{3.3.1}$$

defines a nonarchimedean submultiplicative seminorm on the subring of $\mathbb{W}_S(A)$ on which $|\cdot|_r$ is finite (provided that we interpret $|n|_{\mathbb{Z}}^r$ as 0 in case $|n|_{\mathbb{Z}} = r = 0$). In particular, if S is a finite truncation set, then $|\cdot|_r$ defines a nonarchimedean submultiplicative seminorm on all of $\mathbb{W}_S(A)$. Lastly, if $|\cdot|$ is a norm and $|n|_{\mathbb{Z}} \neq 0$ for all $n \in S$, then $|\cdot|_r$ is also a norm.

Proof. For $\underline{a}, \underline{b}, \underline{c} \in \mathbb{W}_S(A)$ with $\underline{c} = \underline{a} - \underline{b}$, we have by Lemma 3.2 that

$$\begin{aligned} |\underline{c}|_r &= \sup_{n \in S}\{|c_n|^{1/n}|n|_{\mathbb{Z}}^r\} \\ &\leq \sup_{n \in S, d|n}\{|a_{n/d}|^{d/n}|n|_{\mathbb{Z}}^r, |b_{n/d}|^{d/n}|n|_{\mathbb{Z}}^r\} \\ &\leq \max\{|\underline{a}|_r, |\underline{b}|_r\}. \end{aligned}$$

Hence $|\cdot|_r$ is a nonarchimedean seminorm. Given this plus Proposition 1.9, to check submultiplicativity it is enough to check that

$$|V_m([a])V_n([b])|_r \leq |V_m([a])|_r|V_n([b])|_r$$

for all $m, n \in S$ and all $a, b \in A$. The right side of this equation equals $|a|^{1/m}|b|^{1/n}|mn|_{\mathbb{Z}}^r$ because $|\cdot|_{\mathbb{Z}}$ is multiplicative. On the left side, we may invoke Proposition 1.10 to rewrite

$$V_m([a])V_n([b]) = V_{\mathrm{lcm}(m,n)}(\gcd(m,n)[a^{n/\gcd(m,n)}b^{m/\gcd(m,n)}]);$$

using Proposition 1.10 again to pull out $[a^{n/\gcd(m,n)}b^{m/\gcd(m,n)}]$, we obtain

$$|V_m([a])V_n([b])|_r \leq |a|^{1/m}|b|^{1/n}|V_{\mathrm{lcm}(m,n)}(\gcd(m,n))|_r.$$

Put $d = \mathrm{lcm}(m,n), e = \gcd(m,n)$, so that $e \mid d$ and $de = mn$. We are then reduced to checking that

$$|V_d(e)|_r \leq |de|_{\mathbb{Z}}^r.$$

Write e as $\underline{e} = (e_n)$. By Lemma 1.11, we have $|e_n| \leq |e/\gcd(e,n)|$ for any $n \in \mathbb{N}$. Since $r \leq 1/n$ for any $n \in S$, we have

$$\begin{aligned}
|V_d(e)|_r = \sup_{n\in S, d|n}\{|e_{n/d}|^{1/n}|n|_{\mathbb{Z}}^r\} &\leq \sup_{n\in S, d|n}\{|e_{n/d}|^r|n|_{\mathbb{Z}}^r\} \\
&\leq \sup_{n\in S, d|n}\left\{\left|\frac{e}{\gcd(e,n/d)}\right|_{\mathbb{Z}}^r|n|_{\mathbb{Z}}^r\right\} \\
&= \sup_{n\in S, d|n}\left\{|de|_{\mathbb{Z}}^r\left|\frac{n/d}{\gcd(e,n/d)}\right|_{\mathbb{Z}}^r\right\} \\
&\leq |de|_{\mathbb{Z}}^r.
\end{aligned}$$

This completes the proof that $|\cdot|_r$ is submultiplicative. The final statement, concerning when $|\cdot|_r$ is a norm, is obvious. □

The seminorms $|\cdot|_r$ also behave nicely with respect to Frobenius.

Proposition 3.4. *Keep notation as in Theorem 3.3. Choose $m \in S$, and put $S' = \mathbb{N} \cap m^{-1}S$, so that there is a Frobenius map $F_m : \mathbb{W}_S(A) \to \mathbb{W}_{S'}(A)$. Then for all $\underline{a} \in \mathbb{W}_S(A)$,*

$$|F_m(\underline{a})|_{mr} \leq |\underline{a}|_r^m.$$

Note that $|\cdot|_{mr}$ is a submultiplicative seminorm because $n \in S'$ implies $mn \in S$, so $\inf_{n\in S'}\{n^{-1}\} \geq m \inf_{n\in S}\{n^{-1}\} \geq mr$.

Proof. It suffices to check the case where m is equal to a prime number p. In this case, $pn \in S$ implies $r \leq 1/(pn)$, so $|p|^{1/n} \leq |p|_{\mathbb{Z}}^{pr}$. Consequently, for any nonnegative integers e_d with $\sum_{d|pn} de_d = pn$,

$$\begin{aligned} |p|^{1/n}|n|_{\mathbb{Z}}^{pr} \prod_{d|pn} |a_d|^{e_d/n} &\leq |pn|_{\mathbb{Z}}^{pr} \prod_{d|pn} |a_d|^{e_d/n} \\ &= \prod_{d|pn} |a_d|^{e_d/n} |pn|_{\mathbb{Z}}^{de_d r/n} \\ &\leq \prod_{d|pn} |a_d|^{e_d/n} |d|_{\mathbb{Z}}^{de_d r/n} \\ &\leq \prod_{d|pn} |\underline{a}|_r^{de_d/n} = |\underline{a}|_r^p. \end{aligned}$$

We may write $F_p(\underline{a})_n$ as a polynomial in the quantities a_d for $d \mid pn$ with integer coefficients, which is homogeneous of degree pn for the weighting in which a_d carries degree d. Moreover, by Proposition 2.4, the coefficients of $F_p(\underline{a})_n - a_n^p$ are all divisible by p. Hence

$$|F_p(\underline{a})_n - a_n^p|^{1/n}|n|_{\mathbb{Z}}^{pr} \leq \max\{|p|^{1/n}|n|_{\mathbb{Z}}^{pr} \prod_{d|pn} |a_d|^{e_d/n} : e_d \geq 0, \sum_{d|pn} de_d = pn\}.$$

Since the right side of this inequality is bounded above by $|\underline{a}|_r^p$, as is $|a_n^p|^{1/n}|n|_{\mathbb{Z}}^{pr}$, we conclude that $|F_p(\underline{a})|_{pr} \leq |\underline{a}|_r^p$ as desired. □

One cannot hope to define multiplicative norms on $\mathbb{W}_S(R)$ in general because Witt rings are usually not domains (see Remark 2.7). However, one does get multiplicative norms in the p-typical case when $|p| = 0$.

Proposition 3.5. *Let A be a commutative ring with unit, equipped with a nonarchimedean multiplicative seminorm $|\cdot|$ for which $|p| = 0$. Let $|\cdot|_{\mathbb{Z}}$ be a multiplicative norm on $\mathbb{Z}$ such that $|n| \leq |n|_{\mathbb{Z}}$ for all $n \in \mathbb{Z}$. Then for any $r \geq 0$, $|\cdot|_r$ is a nonarchimedean multiplicative seminorm on the subring of $W(A)$ on which it is finite.*

Proof. We may pass immediately to the case where $pA = 0$, then to the case where A is perfect. In the proof of Theorem 3.3, the bound on r is only needed to establish that $|e_{n/d}|^{1/n} \leq |e_{n/d}|^r$ for $e_{n/d} \in \mathbb{Z}$; in our setting, the conditions on the norm $|\cdot|$ imply that $|n| \in \{0, 1\}$ for all $n \in \mathbb{Z}$, and so no bound on r is needed. It follows that for any $r \geq 0$, $|\cdot|_r$ is a nonarchimedean submultiplicative seminorm on the subring of $W(A)$ on which it is finite.

By Corollary 2.6, we can write general elements $\underline{a}, \underline{b}$ of $W(A)$ in the form

$$\underline{a} = \sum_{m=0}^{\infty} p^m [a_{p^m}^{p^{-m}}], \quad \underline{b} = \sum_{n=0}^{\infty} p^n [b_{p^n}^{p^{-n}}];$$

it remains to check that $|\underline{ab}|_r \geq |\underline{a}|_r |\underline{b}|_r$. It is harmless to assume that $|\underline{a}|_r, |\underline{b}|_r > 0$, as otherwise there is nothing to check.

Since the a_{p^m} and b_{p^n} are the Witt components of $\underline{a}$ and $\underline{b}$, respectively, we have

$$|\underline{a}|_r = \sup_{m \geq 0}\{|a_{p^m}|^{p^{-m}} |p|_{\mathbb{Z}}^{mr}\}, \qquad |\underline{b}|_r = \sup_{n \geq 0}\{|b_{p^n}|^{p^{-n}} |p|_{\mathbb{Z}}^{nr}\}.$$

Assume for the moment that these suprema are achieved, and let m_0, n_0 be the smallest values of m, n doing so. Then define

$$\underline{a}' = \sum_{m=m_0}^{\infty} p^m [a_{p^m}^{p^{-m}}], \quad \underline{b}' = \sum_{n=n_0}^{\infty} p^n [b_{p^n}^{p^{-n}}].$$

The $p^{m_0+n_0}$-th Witt component of $\underline{a}'\underline{b}'$ equals $a_{p^{m_0}}^{p^{n_0}} b_{p^{n_0}}^{p^{m_0}}$, so $|\underline{a}'\underline{b}'|_r \geq |\underline{a}|_r |\underline{b}|_r$. Since $|\underline{a} - \underline{a}'|_r < |\underline{a}|_r$, $|\underline{b} - \underline{b}'|_r < |\underline{b}|_r$, we have $|\underline{a}\underline{b} - \underline{a}'\underline{b}'|_r < |\underline{a}|_r |\underline{b}|_r$. We thus deduce that $|\underline{a}\underline{b}|_r = |\underline{a}|_r |\underline{b}|_r$.

In case $|p|_{\mathbb{Z}} < 1$, for any given r for which $|\underline{a}|_r, |\underline{b}|_r$ are finite, the suprema are achieved when r is replaced by any larger value. Since $|\underline{a}|_r$ is continuous as a function of r for fixed $\underline{a}$, we may deduce multiplicativity by continuity.

In case $|p|_{\mathbb{Z}} = 1$, we may as well assume $r = 0$. We may then replace $|\cdot|_{\mathbb{Z}}$ by another norm under which p has norm strictly less than 1, and argue as above. (See also [13, Lemma 2.1.7].) □

4. The basic construction

From now on, we will fix a prime number p, and work exclusively with p-typical Witt vectors. However, we have attempted to set up our work to admit analogues when the p-typical Witt vectors are replaced by big Witt vectors, and when the field $\mathbb{C}_p$ is replaced by the usual complex field $\mathbb{C}$ with its archimedean absolute value. We plan to pursue such analogies in future work.

The construction of the big rings in Fontaine's theory begins with the ring $\tilde{\mathbf{A}}^+$ (in the notation of [1], which we follow here). This ring is usually made by first passing from $\mathcal{O}_{\mathbb{C}_p}$ to a ring of characteristic p using an inverse limit construction, then taking Witt vectors over the result. We will show that one can interchange these two steps, taking Witt vectors with coefficients in $\mathcal{O}_{\mathbb{C}_p}$ and then passing to an inverse limit (Proposition 4.5).

Definition 4.1. *For A a ring, let $\underleftarrow{W}(A)$ denote the inverse limit of the inverse system*

$$\cdots \xrightarrow{F} W(A) \xrightarrow{F} W(A),$$

where F denotes (as usual) the Witt vector Frobenius. Applying F term by term defines a bijective map $F : \underleftarrow{W}(A) \to \underleftarrow{W}(A)$. We express an element $\underline{x} \in \underleftarrow{W}(A)$ as a sequence $(x_1, x_p, \dots)$ of elements of $W(A)$ such that $F(x_{p^{m+1}}) = x_{p^m}$ for $m \geq 0$. For $m, n \geq 0$, let $x_{p^m p^n}$ denote the p^n-th Witt component of x_{p^m}. Finally, put

$$\tilde{\mathbf{A}}^+ := \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p}).$$

We next recall Fontaine's original construction of the ring $\tilde{\mathbf{A}}^+$. This uses the following lemma, which quantifies how the p-th power map brings elements of a ring p-adically closer together. Part (a) is also used in the proof of Dwork's lemma (Lemma 1.6); see [9, Lemma 1.1].

Lemma 4.2. *(a) Let A be any ring, choose $a, b \in A$, and let m, n be positive integers. If $a \equiv b \pmod{p^m A}$, then $a^{p^n} \equiv b^{p^n} \pmod{p^{n+m} A}$.*

(b) Let m, c be positive real numbers, and let n be a positive integer. If $a, b \in \mathbb{C}_p$ satisfy $|b| \leq c$, $|a - b| \leq m$, and $m \leq c p^{-1/(p-1)}$, then $|a^{p^n} - b^{p^n}| \leq p^{-n} m c^{p^n - 1}$.

Proof. (a). This follows by induction from the case $n = 1$, which is obtained by writing

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

On the right side, the term $(a - b)^p$ is divisible by p^{pm} and hence by p^{m+1}, while each summand is divisible by p (from the binomial coefficient) times p^m (from the factor $(a - b)^{p-i}$).

(b) As in part (a), this follows by induction from the case $n = 1$. Expanding $a^p - b^p$ as above, we note that $|(a-b)^p| \leq m^p \leq p^{-1} m c^{p-1}$, while the summand of index i has norm at most p^{-1} (from the binomial coefficient) times c^i (from the factor b^i) times $m^{p-i} \leq m c^{p-1-i}$ (from the factor $(a-b)^{p-i}$). □

Remark 4.3. *The inequality $m \leq cp^{-1/(p-1)}$ in Lemma 4.2(b) cannot be relaxed, as shown by the example $a = 1, b = \zeta_p$. From the above proof, we see that if $|b| \leq c$, $|a - b| \leq m$, and $m \geq cp^{-1/(p-1)}$, then $|a^p - b^p| \leq m^p$.*

We now recall how to use inverse limits to pass from characteristic 0 to characteristic p. This is an example of the "field of norms" construction introduced by Fontaine and Wintenberger [6].

Definition 4.4. *Let $\tilde{\mathbf{E}}^+, \tilde{\mathbf{E}}$ denote the projective limits $\varprojlim \mathcal{O}_{\mathbb{C}_p}, \varprojlim \mathbb{C}_p$ of sets with transition maps $x \mapsto x^p$. That is, the elements of $\tilde{\mathbf{E}}^+$ (resp. $\tilde{\mathbf{E}}$) are sequences $\underline{x} = (x^{(0)}, x^{(1)}, \dots)$ of elements of $\mathcal{O}_{\mathbb{C}_p}$ (resp. $\mathbb{C}_p$) for which $(x^{(i+1)})^p = x^{(i)}$ for $i \geq 0$. These sets are equipped with a ring structure by declaring that*

$$(x+y)^{(i)} := \lim_{j \to \infty} (x^{(i+j)} + y^{(i+j)})^{p^j}$$
$$(xy)^{(i)} := x^{(i)} y^{(i)}.$$

(The limit in the first line exists by Lemma 4.2.) We define the function $|\cdot|_{\tilde{\mathbf{E}}}$ on $\tilde{\mathbf{E}}^+, \tilde{\mathbf{E}}$ by setting $|\underline{x}|_{\tilde{\mathbf{E}}} := |x^{(0)}|$; it is not hard to check that this gives a nonarchimedean multiplicative norm.

In a few situations (e.g., Proposition 4.5), we will also consider $\varprojlim \mathcal{O}_{\mathbb{C}_p}/p$. This is again meant to be read as the set of coherent sequences in $\mathcal{O}_{\mathbb{C}_p}/p$ under the p-th power map, which in this case is a ring homomorphism.

We now reconcile our construction of $\tilde{\mathbf{A}}^+$ with Fontaine's construction; these are respectively the terms appearing on the far left and far right in the following proposition.

Proposition 4.5. *There are canonical isomorphisms*

$$\tilde{\mathbf{A}}^+ = \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p}) \xrightarrow{\pi} \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p}/p) \xrightarrow{\alpha} W(\varprojlim \mathcal{O}_{\mathbb{C}_p}/p) \xrightarrow{\beta} W(\varprojlim \mathcal{O}_{\mathbb{C}_p}) = W(\tilde{\mathbf{E}}^+).$$

Note that the canonicality here includes equivariance with respect to the action of the absolute Galois group of $\mathbb{Q}_p$ on every term.

Proof. We first describe the maps π, α, β. The map π is induced by functoriality of Witt vectors. The map α is defined as follows. For $\underline{x} \in \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p}/p)$, the sequence $\underline{y}_{p^i} = (x_{1p^i}, x_{pp^i}, \dots)$ defines an element of $\varprojlim \mathcal{O}_{\mathbb{C}_p}/p$ because the Witt vector Frobenius on $W(\mathcal{O}_{\mathbb{C}_p}/p)$ is induced by the map $x \mapsto x^p$ (Proposition 2.5). Using the polynomials defining the ring operations on Witt vectors (Definition 1.1), we see that setting $\alpha(\underline{x}) = (\underline{y}_1, \underline{y}_p, \dots)$ in $W(\varprojlim \mathcal{O}_{\mathbb{C}_p}/p)$ defines a ring homomorphism. The map β is induced by the map $\varprojlim \mathcal{O}_{\mathbb{C}_p}/p \to \varprojlim \mathcal{O}_{\mathbb{C}_p}$ defined as follows. Given $\underline{x} = (\overline{x}^{(0)}, \overline{x}^{(1)}, \dots) \in \varprojlim \mathcal{O}_{\mathbb{C}_p}/p$, let $x^{(i)}$ denote any lift of $\overline{x}^{(i)}$ to $\mathcal{O}_{\mathbb{C}_p}$. We then put $\beta(\underline{x}) = \underline{y}$, where $y^{(i)} := \lim_{j \to \infty} (x^{(i+j)})^{p^j}$. As in Definition 4.4, we see that the limit exists, does not depend on the choice of lifts, and induces a ring homomorphism.

We check that π is injective. For any $\underline{x} \in \varprojlim W(\mathcal{O}_{\mathbb{C}_p})$, by writing $F^n(x_{p^{i+n}}) = x_{p^i}$ and using the definition of the Witt vector Frobenius, we obtain the equation

$$x_{p^i 1} = \sum_{j=0}^{n} p^j x_{p^{i+n}p^j}^{p^{n-j}} \qquad (i, n \geq 0). \tag{4.5.1}$$

Suppose now that $\pi(\underline{x}) = 0$. By (4.5.1), for all $i, n \geq 0$, we have $|x_{p^i 1}| \leq p^{-n}$ because $j + p^{n-j} \geq n$ for $0 \leq j \leq n$. Hence $x_{p^i 1} = 0$ for all $i \geq 0$. If for some n we have $x_{p^i p^j} = 0$ for all i and all $j < n$, then from (4.5.1) we immediately obtain $x_{p^i p^n} = 0$ for all $i \geq 0$. We thus conclude that $x_{p^i p^j} = 0$ for all $i, j \geq 0$, so π is injective.

To see that π is surjective, we construct a preimage of $\underline{x} \in \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p}/p)$. For each $i, j \geq 0$, choose any lift $y_{p^i p^j} \in \mathcal{O}_{\mathbb{C}_p}$ of $\underline{x}_{p^i p^j} \in \mathcal{O}_{\mathbb{C}_p}/p$, and put $\underline{y}_{p^i} = (y_{p^i 1}, y_{p^i p}, \dots) \in W(\mathcal{O}_{\mathbb{C}_p})$. We then argue as in Lemma 4.4 (using the polynomials expressing Frobenius in terms of Witt components, as in [11, p. 507, (1.3.4)]) that for each $i, j \geq 0$, as $k \to \infty$, the p^j-th Witt component of $F^k(\underline{y}_{p^{i+k}})$ converges p-adically to some limit $z_{p^i p^j}$. These define an element $\underline{z} \in \underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p})$ with $\pi(\underline{z}) = \underline{x}$.

The map α is clearly injective and surjective. To check that β is an isomorphism, it suffices to check that the map $\varprojlim \mathcal{O}_{\mathbb{C}_p}/p \to \varprojlim \mathcal{O}_{\mathbb{C}_p}$ inducing β has an inverse given by the natural projection map $\varprojlim \mathcal{O}_{\mathbb{C}_p} \to \varprojlim \mathcal{O}_{\mathbb{C}_p}/p$. That the projection is a left inverse is clear; to see that it is a right inverse, note that if we start with an element $(x^{(0)}, x^{(1)}, \dots) \in \varprojlim \mathcal{O}_{\mathbb{C}_p}$, to evaluate β on the projection $(\overline{x}^{(0)}, \overline{x}^{(1)}, \dots)$, we may lift using the original sequence. □

To study $\tilde{\mathbf{A}}^+$ using its description as the inverse limit $\underleftarrow{W}(\mathcal{O}_{\mathbb{C}_p})$, we must better understand the transition maps in this inverse system. For a perfect ring k of characteristic p, the Witt vector Frobenius $F : W(k) \to W(k)$ is an isomorphism because it is induced by the Frobenius map on k (Proposition 2.5). On $W(\mathcal{O}_{\mathbb{C}_p})$, however, Frobenius is neither injective nor surjective; the latter is a symptom of the fact that $\mathbb{C}_p$ is not spherically complete.

Proposition 4.6. *(i) Given $n \geq 1$, suppose that for some $\underline{x} = (x_1, \dots, x_{p^{n-1}}) \in W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$, we have $F(x) = 0 \in W_{p^{n-2}}(\mathcal{O}_{\mathbb{C}_p})$. (This condition should be interpreted as an empty condition in case $n = 1$.) Then $\underline{x}$ extends to an element $\underline{x}' = (x_1, \dots, x_{p^n}) \in W_{p^n}(\mathcal{O}_{\mathbb{C}_p})$ for which $F(\underline{x}') = 0 \in W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$ if and only if*

$$|x_1| \leq p^{-1/p-\cdots-1/p^n}.$$

(ii) The Witt vector Frobenius $F : W(\mathcal{O}_{\mathbb{C}_p}) \to W(\mathcal{O}_{\mathbb{C}_p})$ is not injective. More precisely, for $w \in \mathcal{O}_{\mathbb{C}_p}$, there exists $\underline{x} \in W(\mathcal{O}_{\mathbb{C}_p})$ with $x_1 = w$ and $F(x) = 0$ if and only if $|w| \leq p^{-1/(p-1)}$.

(iii) The Witt vector Frobenius $F : W(\mathcal{O}_{\mathbb{C}_p}) \to W(\mathcal{O}_{\mathbb{C}_p})$ is not surjective.

Proof. (i) We begin with the "only if" direction. For $\underline{x}' = (x_1, \dots, x_{p^n}) \in W_{p^n}(\mathcal{O}_{\mathbb{C}_p})$, the condition $F(\underline{x}') = 0$ is equivalent to the conditions $w_{p^m}(\underline{x}') = 0$ for $m = 1, \dots, n$, or in other words,

$$x_1^{p^m} + \sum_{i=1}^{m} p^i x_{p^i}^{p^{m-i}} = 0 \qquad (m = 1, \dots, n). \tag{4.6.1}$$

We prove that (4.6.1) implies the inequality

$$|x_{p^j}| \leq p^{-1/p-\cdots-1/p^k} \tag{4.6.2}$$

for $k = 0, \dots, n$, $j = 1, \dots, n-k$, by induction primarily on k and secondarily on j. The base case $k = 0$ simply asserts that $|x_{p^j}| \leq 1$ for all j, which is evidently true. For a given pair (k, j) with $k > 0$, we are to prove that (4.6.2) holds for (k, j) given that it holds for all pairs (k', j') with $k' < k$ and for all pairs (k, j') with $j' < j$. In the equation (4.6.1) with $m = n = j+1$, the norm of the term $p^i x_{p^i}^{p^{n-i}}$ for $i < j$ (including $i = 0$) is at most

$$\begin{aligned} p^{-i} p^{p^{n-i}(-1/p-\cdots-1/p^k)} &\leq p^{-(j-1)} p^{p^2(-1/p-\cdots-1/p^k)} \\ &= p^{-(j-1)} p^{-p} p^{-1/p^0-\cdots-1/p^{k-2}} \\ &\leq p^{-(j+1)-1/p-\cdots-1/p^{k-1}}, \end{aligned}$$

while the norm of the term $p^i x_{p^i}^{p^{n-i}}$ for $i = j+1$ is at least

$$p^{-(j+1)-1/p-\cdots-1/p^{k-1}}.$$

Hence the term $p^j x_{p^j}^{p^{n-j}}$ has at most this norm, completing the induction.

We next turn to the "if" direction. Suppose now that $\underline{x} = (x_1, \dots, x_{p^{n-1}}) \in W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$ is such that $|x_1| \leq p^{-1/p-\cdots-1/p^n}$ and $F(\underline{x}) = 0 \in W_{p^{n-2}}(\mathcal{O}_{\mathbb{C}_p})$. Choose $x_{p^n} \in \mathbb{C}_p$ so that (4.6.1) holds. We claim that

$$|x_{p^i}| \leq p^{-1/p-\cdots-1/p^{n-i}} \qquad (i = 0, \dots, n),$$

where the right side is interpreted as 1 for $i = n$; this will imply that $x_{p^n} \in \mathcal{O}_{\mathbb{C}_p}$ and thus yield the desired result. To check this claim, we induct on i, the case $i = 0$ being given. If the claim holds for some $i < n$, then from (4.6.1) with $m = i+1$, we have

$$\begin{aligned} p^{-(i+1)} |x_{p^{i+1}}| &\leq \max_{0 \leq j \leq i} \{p^{-j} |x_{p^j}|^{p^{i+1-j}}\} \\ &\leq \max_{0 \leq j \leq i} \left\{ p^{-j+p^{i+1-j}(-1/p-\cdots-1/p^{n-j})} \right\} \\ &\leq p^{-i+p(-1/p-\cdots-1/p^{n-i})}, \end{aligned}$$

yielding the claim for $i+1$.

(ii) This follows from (i) by a straightforward induction argument.

(iii) Let $y_{p^i} \in \overline{\mathbb{F}_p}$ denote elements in the algebraic closure of $\mathbb{F}_p$. By Proposition 2.8, we have a natural inclusion $W(\overline{\mathbb{F}_p}) \subseteq \mathcal{O}_{\mathbb{C}_p}$, so in particular we can consider $[y_{p^i}] \in \mathcal{O}_{\mathbb{C}_p}$, which in turn admits a Teichmüller lift $[[y_{p^i}]] \in W(\mathcal{O}_{\mathbb{C}_p})$.

We claim that for fixed i, there exists an element

$$\underline{x}^{(i)} = (p^{\frac{1}{p}+\cdots+\frac{1}{p^i}}[y_{p^i}], x_p^{(i)}, x_{p^2}^{(i)}, \dots, x_{p^{i+1}}^{(i)}) \in W_{p^{i+1}}(\mathcal{O}_{\mathbb{C}_p}) \tag{4.6.3}$$

such that $F(\underline{x}^{(i)}) = V^i(\pm[[y_{p^i}^{p^{i+1}}]])$. (We leave the sign ambiguous to make the notation slightly less cumbersome.) More precisely, we will choose $\underline{x}^{(i)}$ to have the form

$$\underline{x}^{(i)} = (p^{\frac{1}{p}+\cdots+\frac{1}{p^i}}[y_{p^i}], p^{\frac{1}{p}+\cdots+\frac{1}{p^{i-1}}} a_p, \dots, p^{\frac{1}{p}} a_{p^{i-1}}, a_{p^i}, a_{p^{i+1}}) \in W_{p^{i+1}}(\mathcal{O}_{\mathbb{C}_p})$$

with $a_{p^j} \in \mathcal{O}_{\mathbb{C}_p}$. By (i), we can choose $a_p, \dots, a_{p^i}$ so that the ghost components of $\underline{x}^{(i)}$ have the form $(*, 0, \dots, 0, *)$; it remains to force the last ghost component to equal $\pm[y_{p^i}^{p^{i+1}}]$. By writing out the definition of the last ghost component, we see that it suffices to check that $a_{p^i}^p \equiv \pm[y_{p^i}^{p^{i+1}}] \pmod p$; this would follow if we knew that $a_{p^i} \equiv \pm[y_{p^i}^{p^i}] \pmod p$.

This last congruence will follow from the fact that $a_{p^j} \equiv \pm[y_{p^i}^{p^j}] \pmod p$ for each $1 \leq j \leq i$, which we check by induction on j. The base case follows from the vanishing of the second ghost component, which yields

$$p^{1+\frac{1}{p}+\cdots+\frac{1}{p^{i-1}}}[y_{p^i}^p] + p^{1+\frac{1}{p}+\cdots+\frac{1}{p^{i-1}}} a_p = 0.$$

For the induction step, we write the equation for the vanishing of the $(j+1)$-st ghost component as

$$\cdots + p^{j-1} p^{p(\frac{1}{p}+\cdots+\frac{1}{p^{i-j+1}})}[a_{p^{j-1}}^p] + p^j p^{\frac{1}{p}+\cdots+\frac{1}{p^{i-j}}}[a_{p^j}] = 0,$$

in which each unwritten term has norm at most $p^{-(j+1)-1/p-\cdots-1/p^{i-j}}$ (as in the proof of (i)).

Having constructed the $\underline{x}^{(i)}$, we now show that there exists a sequence $y_1, y_p, \dots$ for which $\underline{y} := \sum_{i=0}^{\infty} V^i([[y_{p^i}^{p^{i+1}}]])$ is not in the image of Frobenius. By (i) plus (4.6.3), if $\underline{y} = F(\underline{x})$ for some $\underline{x} \in W(\mathcal{O}_{\mathbb{C}_p})$, then for every $i \geq 0$,

$$x_1 \equiv [y_1] + p^{\frac{1}{p}}[y_p] + \cdots + p^{\frac{1}{p}+\cdots+\frac{1}{p^i}}[y_{p^i}] \pmod{p^{\frac{1}{p}+\cdots+\frac{1}{p^{i+1}}}}.$$

In particular, any two distinct sequences lead to values of x_1 which are distinct modulo $p^{\frac{1}{p-1}}$; this explains our use of Teichmüller lifts $[y_{p^i}] \in \mathcal{O}_{\mathbb{C}_p}$, and not arbitrary elements in $\mathcal{O}_{\mathbb{C}_p}$. Now note that there are uncountably many choices for the sequence $y_1, y_p, \dots$, but only countably many congruence classes in $\mathcal{O}_{\mathbb{C}_p}$ modulo $p^{\frac{1}{p-1}}$ (because each such class contains an element algebraic over $\mathbb{Q}$, by Krasner's lemma [15, p. 43]). Thus not every sequence $y_1, y_p, \dots$ leads to a value of $\underline{y}$ in the image of F, proving the desired result. □

Remark 4.7. *While the proof of (iii) given above is nonconstructive, it is also possible to exhibit explicit elements of $W(\mathcal{O}_{\mathbb{C}_p})$ which are not in the image of Frobenius. This uses the second author's description of $\mathcal{O}_{\mathbb{C}_p}$ in terms of generalized power series* [12].

Note the contrast between the surjectivity behavior of Frobenius at finite versus infinite levels.

Corollary 4.8. *For any $n \geq 0$, $F : W_{p^{n+1}}(\mathcal{O}_{\mathbb{C}_p}) \to W_{p^n}(\mathcal{O}_{\mathbb{C}_p})$ is surjective.*

Proof. We show this by induction on n. The case $n = 0$ follows because $\mathcal{O}_{\mathbb{C}_p}$ is closed under p-th roots, so for instance $[a_1] = F([a_1^{1/p}])$. For the inductive step, consider an element $\underline{y} := \sum_{i=0}^{n-1} V^i([a_{p^i}]) \in W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$. By the inductive hypothesis, we can find $\underline{x} \in W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$ such that $F(\underline{x}) = \sum_{i=0}^{n-2} V^i([a_{p^i}])$. Pick any $\underline{\tilde{x}} \in W_{p^n}(\mathcal{O}_{\mathbb{C}_p})$ such that $\underline{\tilde{x}}$ restricts to $\underline{x}$ in $W_{p^{n-1}}(\mathcal{O}_{\mathbb{C}_p})$. Then $\underline{y} - F(\underline{\tilde{x}}) = V^{n-1}([b])$ for some $b \in \mathcal{O}_{\mathbb{C}_p}$. The proof of Proposition 4.6(iii) produces an element $\underline{z} \in W_{p^n}(\mathcal{O}_{\mathbb{C}_p})$ with $F(\underline{z}) = V^{n-1}([1])$. Let c be a p^n-th root of b; then

$$[c^p]V^{n-1}([1]) = V^{n-1}([1]F^{n-1}([c^p])) = V^{n-1}([b])$$

by Proposition 1.10, so $\underline{y} = F(\underline{\tilde{x}} + \underline{z}[c])$. This completes the induction. □

Remark 4.9. *Because $F^n \circ V^n$ acts as multiplication by p^n (Proposition 1.10), any element of $W(\mathcal{O}_{\mathbb{C}_p})$ divisible by p^n belongs to the image of F^n. The element $[p^{n+1}]$ is divisible by p^n, as can be seen easily in $\Lambda(\mathcal{O}_{\mathbb{C}_p})$ (the series $(1-p^{n+1}t)^{-1}$ has a p^n-th root in $1 + t\mathcal{O}_{\mathbb{C}_p}[\![t]\!]$ by the binomial expansion). Consequently, if we let S be the multiplicative subset of $W(\mathcal{O}_{\mathbb{C}_p})$ consisting of all nonzero Teichmüller lifts, so in particular $[p^{n+1}] \in S$, then every power of F is surjective on $S^{-1}W(\mathcal{O}_{\mathbb{C}_p})$. (Note that $S^{-1}W(\mathcal{O}_{\mathbb{C}_p})$ may be naturally identified with a subring of $W(\mathbb{C}_p)$.)*

One can similarly let $\tilde{S}$ be the multiplicative subset of $\tilde{\mathbf{A}}^+$ consisting of sequences of nonzero Teichmüller lifts; these correspond to Teichmüller elements in $W(\tilde{\mathbf{E}}^+)$. The localization $\tilde{S}^{-1}\tilde{\mathbf{A}}^+$ maps to the inverse limit $\varprojlim S^{-1}W(\mathcal{O}_{\mathbb{C}_p})$, but this map is not surjective. Rather, one only gets sequences $(x_1, x_p, \dots) \in \varprojlim S^{-1}W(\mathcal{O}_{\mathbb{C}_p})$ for which $|x_{p^n}|_0^{p^n}$ remains bounded as $n \to \infty$.

5. Ghost components and the theta map

We now introduce a ghost map for $\tilde{\mathbf{A}}^+$, and use it to derive some basic properties of the ring $\tilde{\mathbf{A}}^+$. Although these properties are well-known, our point of view suggests a way to make similar analyses in the realm of big Witt vectors. We also use the ghost map to reinterpret the ring homomorphism $\theta : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbb{C}_p}$ appearing in p-adic Hodge theory (see again [1]).

Definition 5.1. *For $i \in \mathbb{Z}$, define $w_{p^i} : \tilde{\mathbf{A}}^+ \to \mathcal{O}_{\mathbb{C}_p}$ by the formula $w_{p^i}(\underline{x}) = w_{p^k}(x_{p^j})$ for any j, k with $k - j = i$. This does not depend on the choice of j, k because of how the Witt vector Frobenius interacts with ghost components. Since the usual ghost map is a ring homomorphism, so too is each w_{p^i}. Define the* ghost map

$$w : \tilde{\mathbf{A}}^+ \to \prod_{i \in p^{\mathbb{Z}}} \mathcal{O}_{\mathbb{C}_p}$$

as the product of the w_{p^i}. This map is injective, as we can recover $\underline{x}$ from its ghost components via the formula

$$x_{p^m p^n} = \frac{1}{p^n}\left(w_{p^{n-m}} - \sum_{j=0}^{n-1} p^j x_{p^m p^j}^{p^{n-j}} \right). \tag{5.1.1}$$

(Alternatively, it is injective because the usual ghost map is injective whenever the coefficient ring is p-torsion free.) For every $r \in p^{\mathbb{Z}}$, we have a Frobenius homomorphism $F_r : \tilde{\mathbf{A}}^+ \to \tilde{\mathbf{A}}^+$ defined as follows. Given $\underline{x} = (x_1, x_p, \dots) \in \tilde{\mathbf{A}}^+$, for $r = p^i$, put

$$F_r(\underline{x}) = \begin{cases} (F^i(x_1), F^i(x_p), \dots) & i \geq 0 \\ (x_{p^i}, x_{p^{i+1}}, \dots) & i < 0. \end{cases}$$

Note that for any $i, j \in \mathbb{Z}$,

$$w_{p^j}(F_{p^i}(\underline{x})) = w_{p^{i+j}}(\underline{x});$$

consequently, $F_{p^i} \circ F_{p^j} = F_{p^{i+j}}$. In particular, the F_r are all automorphisms.

We similarly obtain an injective ring homomorphism

$$w : \tilde{S}^{-1}\tilde{\mathbf{A}}^+ \to \prod_{i \in p^{\mathbb{Z}}} \mathbb{C}_p,$$

for $\tilde{S}$ the multiplicative set defined in Remark 4.9. This homomorphism is equivariant with respect to the obvious Frobenius maps F_r for $r \in p^{\mathbb{Z}}$ on both sides.

Lemma 5.2. *Suppose $\underline{a}, \underline{b} \in W(\mathcal{O}_{\mathbb{C}_p})$ satisfy $F(\underline{b}) = \underline{a}$ and $p \mid b_1$. Then $p \mid \underline{a}$.*

Proof. (Thanks to Abhinav Kumar for suggesting the following proof.) Since $p \mid b_1$, we can write $\underline{b} = p[b_1/p] + V(\underline{c})$ for some $\underline{c} \in W(\mathcal{O}_{\mathbb{C}_p})$. By Proposition 1.10,

$$\underline{a} = F(\underline{b}) = F(p[b_1/p] + V(\underline{c})) = p[(b_1/p)^p] + p\underline{c},$$

so $p \mid \underline{a}$ as desired. □

Proposition 5.3. *Suppose $\underline{x} \in \tilde{\mathbf{A}}^+$ satisfies $p \mid w_{p^{-i}}(\underline{x})$ for every $i \geq 0$. Then $p \mid \underline{x}$.*

Proof. Write $\underline{x}$ as a sequence $(x_1, x_p, \dots)$ in the inverse limit. By hypothesis, for each $i \geq 0$, we have $F(x_{p^{i+1}}) = x_{p^i}$ and $p \mid x_{p^{i+1}1}$, so $p \mid x_{p^i}$ by Lemma 5.2. Since $W(\mathcal{O}_{\mathbb{C}_p})$ is p-torsion free, this implies $p \mid \underline{x}$ as desired. □

Lemma 5.4. *The ring $\tilde{\mathbf{A}}^+$ is separated for the p-adic topology, and p-torsion free.*

Proof. From Definition 5.1 we know the ghost map is injective, so the result follows from the fact that $\mathcal{O}_{\mathbb{C}_p}$ is separated and p-torsion free. □

Lemma 5.5. *Fix $\underline{x} \in \tilde{\mathbf{A}}^+$. If some $w_{p^j}(\underline{x}) \neq 0$, then $w_{p^{j-i}}(\underline{x}) \neq 0$ for all $i \gg 0$.*

Proof. Because $\tilde{\mathbf{A}}^+$ is p-torsion free, we may use Proposition 5.3 to reduce to the case where $p \nmid w_{p^j}(\underline{x})$ for some j. Because the Frobenius maps are isomorphisms, we may assume $p^j = 1$. From the definition of the Witt vector Frobenius, $x_{p^i 1}^{p^i} \equiv x_{11} \pmod{p}$. Since $x_{p^i 1} = w_{p^{-i}}(\underline{x})$, we obtain $w_{p^{-i}}(\underline{x}) \not\equiv 0 \pmod{p}$ for all $-i \leq 0$, proving the desired result. □

Proposition 5.6. *The ring $\tilde{\mathbf{A}}^+$ is a domain.*

Proof. This follows from Lemma 5.5 and the fact that $\mathcal{O}_{\mathbb{C}_p}$ is a domain. □

We now recall the map θ used in p-adic Hodge theory, and relate it to the ghost map.

Definition 5.7. *Given $\underline{x} \in \tilde{\mathbf{A}}^+$, apply Proposition 4.5 to present $\underline{x}$ as an element $\underline{y} = (y_1, y_p, \dots)$ of $W(\varprojlim \mathcal{O}_{\mathbb{C}_p})$. Then set*

$$\theta(x) = \sum_{k=0}^{\infty} p^k((y_{p^k})^{(k)}).$$

Proposition 5.8. *The map θ coincides with the map w_1 from Definition 5.1 (i.e., the first ghost component map). In particular, θ is a ring homomorphism.*

Proof. (Thanks to Ruochuan Liu for suggesting the following proof.) We use the notation of Proposition 4.5. Let $\underline{z} := (\alpha \circ \pi)(\underline{x})$, so in particular $(z_{p^j})^{(i)} = \overline{x_{p^i p^j}}$. Our definition of β involves choosing lifts of the terms $(z_{p^j})^{(i)}$, for which we may choose $x_{p^i p^j}$. Then from the definition of β,

$$((\beta \circ \alpha \circ \pi(x))_{p^j})^{(j)} = \lim_{k \to \infty} x_{p^{j+k} p^j}^{p^k}.$$

Replacing k by $k-j$, which does not affect the limit, we have

$$((\beta \circ \alpha \circ \pi(x))_{p^j})^{(j)} = \lim_{k \to \infty} x_{p^k p^j}^{p^{k-j}}.$$

Plugging this into the definition of θ yields

$$(\theta \circ \beta \circ \alpha \circ \pi)(x) = \sum_{j=0}^{\infty} p^j \lim_{k \to \infty} x_{p^k p^j}^{p^{k-j}} = \sum_{j=0}^{\infty} \lim_{k \to \infty} p^j x_{p^k p^j}^{p^{k-j}} = \lim_{i \to \infty} \sum_{j=0}^{i} p^j x_{p^i p^j}^{p^{i-j}}.$$

Now note that $\sum_{j=0}^{i} p^j x_{p^i p^j}^{p^{i-j}}$ is precisely the p^i-th ghost component of x_{p^i}. But by the definition of the Frobenius map, this term is independent of i. Taking $i = 0$ completes the proof. □

6. Tails of ghost components

As noted earlier (Definition 5.1), an element of $\tilde{\mathbf{A}}^+$ is determined by its doubly infinite sequence of ghost components. In fact, one can explicitly recover an element of $\tilde{\mathbf{A}}^+$ just from the ghost components indexed by sufficiently negative powers of p, i.e., from the *tail* of the sequence of ghost components. In addition, the multiplicative norms $|\cdot|_r$ on $W(\tilde{\mathbf{E}})$ (Proposition 3.5) also admit a direct interpretation on the space of tails.

Definition 6.1. *For A a commutative ring with unit, let $\underleftarrow{W}_*(A)$ be the inverse limit of the inverse system*

$$\cdots \xrightarrow{F} W_{p^1}(A) \xrightarrow{F} W_{p^0}(A);$$

then we have a ghost map

$$w : \underleftarrow{W}_*(A) \to \prod_{i=p^{-\infty}}^{1} A.$$

If A is p-torsion-free, we can recover $\underline{x} \in \underleftarrow{W}_*(A)$ from its ghost image $(\ldots, w_{p^{-1}}, w_{p^0})$, using the formula (5.1.1).

We have the following statement, which refines the statement that the ghost map on $\tilde{\mathbf{A}}^+$ is injective (Definition 5.1).

Proposition 6.2. *Suppose the ring A is p-torsion free and p-adically separated and complete. Then the canonical restriction map $\underleftarrow{W}(A) \to \underleftarrow{W}_*(A)$ is bijective. In particular, we have an isomorphism $\tilde{\mathbf{A}}^+ \to \underleftarrow{W}_*(\mathcal{O}_{\mathbb{C}_p})$.*

Proof. Let $\underline{x} \in \underleftarrow{W}_*(A)$ be an element with ghost sequence $(\ldots, w_{p^{-1}}, w_1)$. For each m, the set of $w_p^{(m)} \in A$ for which $(w_{p^{-m}}, \ldots, w_1, w_p^{(m)})$ belongs to the image of the ghost map from $W_{p^{m+1}}(A)$ is a single congruence class modulo $p^{m+1}A$, namely the one containing the image of $(x_{p^m 1}, \ldots, x_{p^m p^m}, 0)$ under F^{m+1}. Since A is p-adically separated and complete, the intersection of these congruence classes over all m is a single element $w_p \in A$. Since A is p-torsion-free, we also obtain a unique element of $\underleftarrow{W}_*(A)$ with ghost sequence $(\ldots, w_{p^{-1}}, w_1, w_p)$. Repeating this process produces a unique set of Witt and ghost components of an element of $\underleftarrow{W}(A)$ lifting $\underline{x}$. □

This leads to some additional structural information concerning $\tilde{\mathbf{A}}^+$.

Corollary 6.3. *The ring $\tilde{\mathbf{A}}^+$ is complete for the p-adic topology.*

Proof. By Proposition 5.3, the p-adic topology on $\tilde{\mathbf{A}}^+$ is induced by the supremum norm on $\prod_{i=p^{-\infty}}^{1} \mathcal{O}_{\mathbb{C}_p}$. Among all sequences $(\dots, w_{p^{-1}}, w_1)$, $w_{p^{-i}} \in \mathcal{O}_{\mathbb{C}_p}$, we can distinguish which ones arise from $\tilde{\mathbf{A}}^+$ by using the equations (5.1.1) with $m \geq n$. In this manner, we see that the image of $\tilde{\mathbf{A}}^+$ is complete for the supremum norm; this yields the desired result. □

Corollary 6.4. *The ring $\tilde{\mathbf{A}}^+$ is local, with units consisting of those $\underline{x}$ such that $v_p(x_{11}) = 0$.*

Proof. Consider the composition

$$\tilde{\mathbf{A}}^+ \xrightarrow{\theta} \mathcal{O}_{\mathbb{C}_p} \twoheadrightarrow \overline{\mathbb{F}_p}.$$

The kernel of this map is a maximal ideal consisting of the complement of the elements described above, so it suffices to show that each $\underline{x}$ with $v_p(x_{11}) = 0$ is a unit.

Since $w_{p^{-n}}(\underline{x})^p \equiv w_{p^{-(n-1)}}(\underline{x}) \pmod p$, for each $m \in \mathbb{Z}$, the limit

$$y_{p^m} := \lim_{n \to \infty} w_{p^{-n+m}}(\underline{x})^{p^n}$$

exists by Lemma 4.2. This corresponds to a sequence of terms that is in the image of the ghost map: it is the image of $y := ([y_1], [y_{p^{-1}}], [y_{p^{-2}}], \dots) \in \tilde{\mathbf{A}}^+$.

For each m, we have $y_{p^m} \equiv w_{p^m}(\underline{x}) \pmod p$. By Proposition 5.3, we can write $\underline{x} = \underline{y} + p\underline{z}$ for some $\underline{z} \in \tilde{\mathbf{A}}^+$. Since $v_p(x_{11}) = 0$, $\underline{y}$ is a unit in $\tilde{\mathbf{A}}^+$; since $\tilde{\mathbf{A}}^+$ is p-adically complete by Corollary 6.3, $1 + p\underline{y}^{-1}\underline{z}$ is also a unit in $\tilde{\mathbf{A}}^+$. Hence $\underline{x}$ is a unit, as desired. □

We now describe how Gauss norms may be read off from tails.

Definition 6.5. *Let A be a commutative ring with unit, equipped with a nonarchimedean submultiplicative seminorm $|\cdot|$. For $r \in [0,1)$ and $m \geq 0$, the function $|\cdot|_{rp^{-m}}$ introduced in Theorem 3.3 is a nonarchimedean submultiplicative seminorm on $W_{p^m}(A)$. (This much also holds for $r = 1$, but it will be convenient later to have this case excluded from the outset.) For $\underline{x} = (x_1, x_p, \dots) \in \underleftarrow{W}_*(A)$, the sequence $|x_{p^m}|_{rp^{-m}}^{p^m}$ is nondecreasing by Proposition 3.4; it thus has a (possibly infinite) limit, denoted $|\underline{x}|_r$. We may also write*

$$|\underline{x}|_r = \sup_{0 \leq n \leq m} \{|x_{p^m p^n}|^{p^{m-n}} p^{-rn}\} \tag{6.5.1}$$

for $x_{p^m p^n}$ as in (5.1.1)*. If A is separated and complete under $|\cdot|$, then the subring of $\underleftarrow{W}_*(A)$ on which $|\cdot|_r$ is finite is separated and complete under $|\cdot|_r$. Note that by definition, we have $|F(\underline{x})|_{pr} = |\underline{x}|_r^p$ for all $r \in [0, 1/p)$.*

Example 6.6. *The subring of $\underleftarrow{W}_*(\mathbb{C}_p)$ on which $|\cdot|_0$ is finite is the ring $\tilde{S}^{-1}\tilde{\mathbf{A}}^+$ of Remark 4.9.*

Lemma 6.7. *Let $0 \leq n \leq j \leq m$ be integers, and choose $r \in [0,1)$ and $c \in \mathbb{R}$. Suppose $a, b \in \mathbb{C}_p$ are such that*

$$|a|^{p^{m-n}} p^{-rn} \leq c, \qquad |a - b| \leq p^{-1+r(n+1)p^{n-m}} c^{p^{n-m}}.$$

Then

$$|a^{p^{j-n}} - b^{p^{j-n}}| \leq p^{-(j-n+1)+r(j+1)p^{j-m}} c^{p^{j-m}}.$$

Proof. We may assume $j > n$, as the case $j = n$ is given. Suppose first that $p \geq 3$; then $1 - rp^{n-m} \geq 1 - p^{-1} \geq 1/(p-1)$, so $p^{-1+rp^{n-m}} \leq p^{-1/(p-1)}$. By Lemma 4.2, we have

$$|a^{p^{j-n}} - b^{p^{j-n}}| \leq p^{-(j-n+1)+r(n+1)p^{n-m}+(p^{j-n}-1)rnp^{n-m}} c^{p^{j-m}}.$$

Since

$$\begin{aligned} j - n + 1 &- r(n+1)p^{n-m} - (p^{j-n}-1)rnp^{n-m} \\ &\geq j - n + 1 - r(j+1)p^{j-m} - (p^{j-n}-1)r(j+1)p^{n-m} \\ &= j - n + 1 - r(j+1)p^{j-m}, \end{aligned}$$

we obtain the desired bound in this case.

Suppose next that $p = 2$; in this case, $p^{-1/(p-1)} \leq p^{-1+rp^{n-m}} \leq p^{-1/p(p-1)}$. By Remark 4.3, we have

$$|a^p - b^p| \leq p^{-p(1-r(n+1)p^{n-m})} c^{p^{n-m+1}};$$

we may then apply Lemma 4.2 to obtain

$$|a^{p^{j-n}} - b^{p^{j-n}}| \leq p^{-(j-n-1)-p(1-r(n+1)p^{n-m})+(p^{j-n}-p)rnp^{n-m}} c^{p^{j-m}}.$$

In this case,

$$\begin{aligned} (j - n - 1) &+ p(1 - r(n+1)p^{n-m}) - (p^{j-n} - p)rnp^{n-m} \\ &= j - n + (p-1) - rp^{n+1-m} - rnp^{j-m} \\ &\geq j - n + 1 - rp^{j-m} - rjp^{j-m} \\ &= j - n + 1 - r(j+1)p^{j-m}, \end{aligned}$$

so we again obtain the desired bound. □

Theorem 6.8. *Let $(\dots, w_{p^{-2}}, w_{p^{-1}}, w_1)$ be a singly infinite sequence of elements in $\mathbb{C}_p$, and define $x_{p^m p^n} \in \mathbb{C}_p$ for $0 \leq n \leq m$ as in (5.1.1). Then for any $r \in [0,1)$ and any $c \in \mathbb{R}$, there exists an element $\underline{y} \in W(\tilde{\mathbf{E}})$ with $|\underline{y}|_r \leq c$ for which*

$$w_{p^{-j}} = \sum_{i=0}^{\infty} p^i (y_{p^i})^{(i+j)} \tag{6.8.1}$$

for all $j \geq 0$ if and only if

$$|x_{p^m p^n}|^{p^{m-n}} p^{-rn} \leq c \tag{6.8.2}$$

for all $0 \leq n \leq m$ (i.e., the $x_{p^m p^n}$ are the components of some $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ with $|\underline{x}|_r \leq c$).

Proof. Suppose first that $|\underline{y}|_r \leq c$, so that for all $i, j \geq 0$,

$$|(y_{p^i})^{(j)}|^{p^{j-i}} p^{-ri} \leq c. \tag{6.8.3}$$

We will prove that

$$\left| x_{p^m p^n}^{p^{j-n}} - (y_{p^n})^{(m-j+n)} \right| \leq p^{-(j-n+1)+r(j+1)p^{j-m}} c^{p^{j-m}} \tag{6.8.4}$$

for all $0 \leq n \leq j \leq m$, by induction on n. Assume that (6.8.4) holds with n replaced by any smaller value. Then write

$$\begin{aligned} x_{p^m p^n} - (y_{p^n})^{(m)} &= \frac{w_{p^{n-m}} - p^n (y_{p^n})^{(m)}}{p^n} - \sum_{i=0}^{n-1} p^{i-n} x_{p^m p^i}^{p^{n-i}} \\ &= \sum_{i=0}^{n-1} p^{i-n} ((y_{p^i})^{(i+m-n)} - x_{p^m p^i}^{p^{n-i}}) + \sum_{i=n+1}^{\infty} p^{i-n} (y_{p^i})^{(i+m-n)}. \end{aligned}$$

By the induction hypothesis, each summand in the first sum has norm at most $p^{-1+r(n+1)p^{n-m}} c^{p^{n-m}}$. The same is true of each summand in the second sum, thanks to (6.8.3) and the fact that for $i \geq n+1$,

$$(i-n) - rip^{n-m} \geq (i-n) - r(n+1)p^{n-m} - (i-n-1) = 1 - r(n+1)p^{n-m}.$$

This proves (6.8.4) in case $j = n$; the general case follows from (6.8.3) and Lemma 6.7. This completes the induction establishing (6.8.4); by taking $j = n$ therein, we deduce (6.8.2).

Conversely, assume (6.8.2). We establish the following variant of (6.8.4): for all $0 \leq n \leq j \leq m$,

$$\left| x_{p^m p^n}^{p^{j-n}} - x_{p^{m+1} p^n}^{p^{j-n+1}} \right| \leq p^{-(j-n+1)+r(j+1)p^{j-m}} c^{p^{j-m}}. \tag{6.8.5}$$

We again proceed by induction on n. Assume that (6.8.5) holds with n replaced by any smaller value. From the equalities

$$w_{p^{n-m}} = \sum_{i=0}^{n} p^i x_{p^m p^i}^{p^{n-i}} = \sum_{i=0}^{n+1} p^i x_{p^{m+1} p^i}^{p^{n+1-i}}$$

we deduce that

$$p^{n+1} x_{p^{m+1} p^{n+1}} = \sum_{i=0}^{n} p^i (x_{p^m p^i}^{p^{n-i}} - x_{p^{m+1} p^i}^{p^{n+1-i}}),$$

or equivalently

$$x_{p^m p^n} - x_{p^{m+1} p^n}^p = p x_{p^{m+1} p^{n+1}} - \sum_{i=0}^{n-1} p^{i-n} (x_{p^m p^i}^{p^{n-i}} - x_{p^{m+1} p^i}^{p^{n+1-i}}).$$

By (6.8.2) plus the induction hypothesis, each term on the right side has norm at most $p^{-1+r(n+1)p^{n-m}} c^{p^{n-m}}$. This establishes (6.8.5) in case $j = n$; the general case follows by (6.8.2) plus Lemma 6.7.

We may rewrite (6.8.5) as

$$\left| x_{p^{m+j} p^i}^{p^m} - x_{p^{m+j+1} p^i}^{p^{m+1}} \right| \leq p^{-(m+1)+r(m+i+1)p^{i-j}} c^{p^{i-j}}, \tag{6.8.6}$$

where now $m \geq 0$ and $j \geq i \geq 0$. For any fixed i, j, the right side of (6.8.6) is decreasing in m, so the limit

$$(y_{p^i})^{(j)} = \lim_{m \to \infty} x_{p^{m+j} p^i}^{p^m}$$

exists and satisfies (6.8.4); moreover, (6.8.2) implies that the limit satisfies (6.8.3). For each i, the sequence $(y_{p^i})^{(j)}$ defines an element $y_{p^i} \in \tilde{\mathbf{E}}$. Put $\underline{y} = (y_{p^i}) \in W(\tilde{\mathbf{E}})$; then (6.8.3) implies $|\underline{y}|_r \leq c$.

It remains to check (6.8.1). Given $j \geq 0$, for any $m \geq 0$ we can write

$$\begin{aligned} w_{p^{-j}} - \sum_{i=0}^{\infty} p^i (y_{p^i})^{(i+j)} &= \sum_{i=0}^{m} p^i x_{p^{m+j}p^i}^{p^{m-i}} - \sum_{i=0}^{\infty} p^i (y_{p^i})^{(i+j)} \\ &= \sum_{i=0}^{m} p^i (x_{p^{m+j}p^i}^{p^{m-i}} - (y_{p^i})^{(i+j)}) - \sum_{i=m+1}^{\infty} p^i (y_{p^i})^{(i+j)}. \end{aligned}$$

On the right side, each summand has norm at most $p^{-(m+1)+r(m+1)p^{-j}} c^{p^{-j}}$: in the first sum this follows from (6.8.4), while in the second sum it follows from (6.8.3) because $i - rip^{-j} \geq m + 1 - r(m+1)p^{-j}$ for $i \geq m+1$. We conclude that

$$\left| w_{p^{-j}} - \sum_{i=0}^{\infty} p^i (y_{p^i})^{(i+j)} \right| \leq p^{-(m+1)+r(m+1)p^{-j}} c^{p^{-j}}.$$

Since m was arbitrary, this implies (6.8.1). This completes the proof. □

Corollary 6.9. *For $r \in [0,1)$, let $W(\tilde{\mathbf{E}})_r$ denote the subring of $W(\tilde{\mathbf{E}})$ on which $|\cdot|_r$ is finite, and let $\underleftarrow{W}_*(\mathbb{C}_p)_r$ denote the subring of $\underleftarrow{W}_*(\mathbb{C}_p)$ on which $|\cdot|_r$ is finite. We then obtain an isomorphism*

$$\psi : W(\tilde{\mathbf{E}})_r \to \underleftarrow{W}_*(\mathbb{C}_p)_r$$

by passing from $\underline{y} \in W(\tilde{\mathbf{E}})_r$ to a sequence $(\dots, w_{p^{-1}}, w_1)$ using (6.8.1)*, then obtaining an element of $\underleftarrow{W}_*(\mathbb{C}_p)_r$ using* (5.1.1)*. Moreover, for any $\underline{y} \in W(\tilde{\mathbf{E}})_r$, we have $|\psi(\underline{y})|_r = |\underline{y}|_r$.*

Remark 6.10. *Proposition 3.5 and Corollary 6.9 together imply that for $r \in [0,1)$, the submultiplicative norm $|\cdot|_r$ on $\underleftarrow{W}_*(\mathbb{C}_p)_r$ is in fact multiplicative. It seems difficult to give a direct proof of this.*

On the other hand, for the construction of Fontaine's rings, one needs not the full strength of multiplicativity, but only the special case $|p\underline{x}|_r = p^{-r}|\underline{x}|_r$. This may be established directly as follows. For $\underline{y} = p\underline{x}$ and $c = |\underline{x}|_r$, we establish the bound

$$\text{(6.10.1)} \qquad |y_{p^{m+1}p^{n+1}}^{p^{j-n}} - x_{p^m p^n}^{p^{j-n}}| \leq p^{-(j-n+1)+r(j+1)p^{j-m}} c^{p^{j-m}}$$

whenever $0 \leq n \leq j \leq m$, by induction on n. Assume that (6.10.1) *holds with n replaced by any smaller value. From the equalities*

$$pw_{p^{n-m}} = \sum_{i=0}^{n+1} p^i y_{p^{m+1}p^i}^{p^{n+1-i}} = \sum_{i=0}^{n+1} p^{i+1} x_{p^{m+1}p^i}^{p^{n+1-i}},$$

we obtain

$$y_{p^{m+1}p^{n+1}} - x_{p^{m+1}p^n}^p = px_{p^{m+1}p^{n+1}} - p^{-n-1} y_{p^{m+1}1}^{p^{n+1}} - \sum_{i=0}^{n-1} p^{i-n} (y_{p^{m+1}p^{i+1}}^{p^{n-i}} - x_{p^{m+1}p^i}^{p^{n-i+1}}).$$

We claim each term on the right side is bounded above by $p^{-1+r(n+1)p^{n-m}} c^{p^{n-m}}$. The bound holds for the first term by (6.8.2)*, and likewise for the second term after rewriting it as $p^{-n-1}(pw_{p^{-m-1}})^{p^{n+1}} = p^{-n-1+p^{n+1}} x_{p^{m+1}1}^{p^{n+1}}$ and noting that $p^{n+1} - n - 1 \geq 1 \geq 1 - r(n+1)p^{n-m}$. The bound for the other summands comes from the induction hypothesis. This establishes* (6.10.1) *in case $j = n$; the general case follows from Lemma 6.7.*

From (6.10.1) *and* (6.8.2)*, we immediately have* $|y_{p^{m+1}p^{n+1}}| \leq p^{rnp^{n-m}} c^{p^{n-m}}$ *(and* $y_{11} = px_{11}$ *has norm at most* $p^{-1}c \leq p^{-r}c$*), so* $|\underline{y}|_r \leq p^{-r}c$*. On the other hand, for each* $\epsilon \in (0, 1-p^{-1+r})$*, there exist* m, n *for which* $|x_{p^m p^n}| \geq (1-\epsilon)p^{rnp^{n-m}} c^{p^{n-m}}$*, and from* (6.10.1) *we then have* $|y_{p^{m+1}p^{n+1}}| \geq (1-\epsilon)p^{rnp^{n-m}} c^{p^{n-m}}$*. Hence* $|\underline{y}|_r \geq p^{-r}c$*, proving the desired equality.*

Lemma 6.11. *For* $r \in [0, 1)$*, the ring* $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *is* p*-adically separated.*

Proof. This follows from Corollary 6.9, but can be seen more directly as follows. Choose any $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ and put $c = |\underline{x}|_r$. Then $|x_{p^m 1}| \leq c^{p^{-m}}$ for all $m \geq 0$, and so $\limsup_{m\to\infty} |x_{p^m 1}| \leq \lim_{m\to\infty} c^{p^{-m}} \leq 1$.

If $\underline{x} = p^n \underline{y}$ for some positive integer n and some $\underline{y} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$, then $x_{p^m 1} = p^n y_{p^m 1}$ for all $m \geq 0$. By the previous paragraph, $\limsup_{m\to\infty} |y_{p^m 1}| \leq 1$, and so $\limsup_{m\to\infty} |x_{p^m 1}| \leq p^{-n}$.

If $\underline{x}$ is divisible by arbitrary powers of p, we now see that $\lim_{m\to\infty} |x_{p^m 1}| = 0$. By induction on n plus the equation

$$x_{p^m 1} = p^n x_{p^{m+n}p^n} + \sum_{i=0}^{n-1} p^i x_{p^{m+n}p^i}^{p^{n-i}}, \tag{6.11.1}$$

we see that $\lim_{m\to\infty} |x_{p^m p^n}| = 0$ for each nonnegative integer n. By (6.8.6), $|x_{p^{m+n}p^i}^{p^{n-i}}| \leq p^{-(n-i+1)+r(n+1)p^{-m}} c^{p^{-m}}$ whenever $m \geq 0$ and $n \geq i \geq 0$. By (6.11.1), $|x_{p^m 1}| \leq p^{-(n+1)+r(n+1)p^{-m}} c^{p^{-m}}$ for any nonnegative integer n. Hence $\underline{x} = 0$, proving the claim. □

We have the following refinement of Proposition 6.2. Here by the *tail map*, we mean the composition of the ghost map with the projection onto the space of tails (the direct limit of the spaces of sequences $(\dots, w_{p^{-n+1}}, w_{p^{-n}})$ as $n \to \infty$).

Proposition 6.12. *For any* $r \in [0, 1)$*, the tail map on* $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *is injective.*

Proof. It suffices to check that a sequence $(\dots, w_{p^{-1}}, w_1)$ with $w_{p^{-n}} = 0$ for all $n > 0$ can only belong to the image of the ghost map on $\underleftarrow{W}_*(\mathbb{C}_p)_r$ if $w_1 = 0$. Suppose $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ maps to such a sequence; then $x_{p^m p^n} = 0$ whenever $n < m$, and $x_{p^m p^m} = p^{-m} w_1$. But then (6.8.2) would imply

$$p^m |w_1| = |x_{p^m p^m}| \leq p^{rm} |\underline{x}|_r,$$

which gives a contradiction for m large unless $|w_1| = 0$. Hence $w_1 = 0$ as desired. □

Definition 6.13. *By Proposition 6.12, for* $r \in [0, 1)$*, we may identify* $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *with its image under the tail map. We may then formally define* $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *for* $r \geq 1$ *by declaring that for each positive integer* m*,* $\underleftarrow{W}_*(\mathbb{C}_p)_{p^m r}$ *is the image of the tail set of* $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *under* F^m*, equipped with the norm* $|\cdot|_{p^m r}$ *for which*

$$|F^m(\underline{x})|_{p^m r} = |\underline{x}|_r^{p^m}.$$

With this definition, $\underleftarrow{W}_*(\mathbb{C}_p)_r$ *is complete under* $|\cdot|_r$ *for all* $r \geq 0$*.*

7. More rings from p-adic Hodge theory

To conclude, we indicate how to describe some other rings occurring in p-adic Hodge theory in the style of our description of $\tilde{\mathbf{A}}^+$. Our notation for these rings differs somewhat from Fontaine's original notation; we follow more recent conventions of Berger, Colmez, et al. (as in [1]).

Definition 7.1. *Define $\tilde{\mathbf{A}}^\dagger$ as the union of the rings $\underleftarrow{W}_*(\mathbb{C}_p)_r$ over all $r \geq 0$, using Definition 6.13 to define $\underleftarrow{W}_*(\mathbb{C}_p)_r$ for $r \geq 1$. By construction, this ring admits an injective tail map. By Theorem 6.8 (and the fact that $\underleftarrow{W}_*(\mathbb{C}_p)_r$ is complete under $|\cdot|_r$), we may identify $\tilde{\mathbf{A}}^\dagger$ with the union over all $r \geq 0$ of the completion of $\tilde{S}^{-1}\tilde{\mathbf{A}}^+ \cong \tilde{S}^{-1}W(\tilde{\mathbf{E}}^+)$ under v_r. That is, our construction $\tilde{\mathbf{A}}^\dagger$ agrees with the usual definition.*

Define $\tilde{\mathbf{B}}^\dagger := \tilde{\mathbf{A}}^\dagger[\frac{1}{p}]$. We may again identify $\tilde{\mathbf{B}}^\dagger$ with a ring of tails satisfying certain bounds, using the identity $|p\underline{x}|_r = |p|_r|\underline{x}|_r$ (Remark 6.10).

The following lemma enables us to use the tail of ghost components to determine when an element $\underline{x}$ is divisible by p. In rough terms, it says that if the ghost components have norms approaching at most $\frac{1}{p}$, then $\underline{x}$ is divisible by p.

Lemma 7.2. *Let $0 \leq r < 1$ and $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$. Let $(\dots, w_{p^{-1}}, w_1)$ denote the tail of ghost components corresponding to $\underline{x}$. If there exists κ such that $|w_{p^{-m}}| \leq p^{-1+\kappa p^{-m}}$ for all $m \geq 0$, then there exists $\underline{\tilde{x}} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ with $p\underline{\tilde{x}} = \underline{x}$.*

Proof. Since the ghost map is injective, we need only check that the sequence $(\dots, \tilde{w}_{p^{-1}}, \tilde{w}_1)$ with $\tilde{w}_{p^{-m}} = \frac{1}{p} w_{p^{-m}}$ comprises the ghost components of some $\underline{\tilde{x}} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$. Define $\tilde{x}_{p^m p^n} \in \mathbb{C}_p$ for $0 \leq n \leq m$ using $\tilde{w}_{p^{-m}}$ as in (5.1.1); we must show that for some $\tilde{c} \geq 0$, we have $|\tilde{x}_{p^m p^n}|^{p^{m-n}} p^{-rn} \leq \tilde{c}$ for all $0 \leq n \leq m$. We will prove this for $\tilde{c} = \max\{p^\kappa, pc\}$, where $c = |\underline{x}|_r = \sup_{0 \leq n \leq m}\{|x_{p^m p^n}|^{p^{m-n}} p^{-rn}\}$.

We first prove that

$$|\tilde{x}_{p^m p^n} - x^{p^n}_{p^{m+n+1}p^{n+1}}| \leq p^{-1+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}} \tag{7.2.1}$$

for all $0 \leq n \leq m$. To prove (7.2.1), we write the ghost component $\tilde{w}_{p^{n-m}} = \frac{w_{p^{n-m}}}{p}$ in two different ways:

$$\begin{aligned} &\tilde{x}^{p^n}_{p^m 1} + p\tilde{x}^{p^{n-1}}_{p^m p} + \cdots + p^n \tilde{x}_{p^m p^n} = \\ &\qquad \frac{1}{p}\Big(x^{p^{2n+1}}_{p^{m+n+1}1} + p x^{p^{2n}}_{p^{m+n+1}p} + \cdots \\ &\qquad\qquad + p^{n+1} x^{p^n}_{p^{m+n+1}p^{n+1}} + \cdots + p^{2n+1} x_{p^{m+n+1}p^{2n+1}}\Big). \end{aligned} \tag{7.2.2}$$

Consider first the case $n = 0$. Then the above equation becomes

$$\tilde{x}_{p^m 1} = \frac{1}{p}(x^p_{p^{m+1}1} + p x_{p^{m+1}p}).$$

Equation (7.2.1) holds for $n = 0$ because

$$\tilde{x}_{p^m 1} - x_{p^{m+1}p} = \frac{1}{p} x^p_{p^{m+1}1} = \frac{1}{p} w^p_{p^{-m-1}},$$

and so

$$\begin{aligned}|\tilde{x}_{p^m 1} - x_{p^{m+1}p}| &\le p(p^{-1+\kappa p^{-m-1}})^p = p^{-(p-1)+\kappa p^{-m}} \\ &\le p^{-1+\kappa p^{-m}} \le p^{-1+rp^{-m}} \tilde{c}^{p^{-m}}.\end{aligned}$$

The last inequality holds because $r \ge 0$ and $\tilde{c} \ge p^\kappa$.

Now assume that (7.2.1) holds with n replaced by any smaller value. We will show that it holds for n. By (7.2.2), it suffices to show the following:

$$|p^{-n-1} x^{p^{2n+1}}_{p^{m+n+1}1}| \le p^{-1+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}}, \tag{7.2.3}$$

$$|p^{i-n} \tilde{x}^{p^{n-i}}_{p^m p^i} - p^{i-n} x^{p^{2n-i}}_{p^{m+n+1}p^{i+1}}| \le p^{-1+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}} \text{ for } 0 \le i < n, \tag{7.2.4}$$

$$|p^j x^{p^{n-j}}_{p^{m+n+1}p^{n+1+j}}| \le p^{-1+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}} \text{ for } 1 \le j \le n. \tag{7.2.5}$$

To prove (7.2.3), we note that

$$\begin{aligned}|p^{-n-1} x^{p^{2n+1}}_{p^{m+n+1}1}| &\le p^{n+1} \left(p^{-1+\kappa p^{-m-n-1}}\right)^{p^{2n+1}} \\ &= p^{n+1-p^{2n+1}} p^{\kappa p^{n-m}} \\ &\le p^{-1} (p^\kappa)^{p^{n-m}},\end{aligned}$$

and so we are again done because $r \ge 0$ and $\tilde{c} \ge p^\kappa$.

To prove (7.2.4), we will use the induction hypothesis. This tells us that

$$|\tilde{x}_{p^m p^i} - x^{p^i}_{p^{m+i+1}p^{i+1}}| \le p^{-1+r(i+1)p^{i-m}} \tilde{c}^{p^{i-m}}.$$

From the definition of c,

$$|x^{p^i}_{p^{m+i+1}p^{i+1}}|^{p^{m-i}} p^{-ri} = |x^{p^m}_{p^{m+i+1}p^{i+1}}| p^{-ri} \le p^r c \le \tilde{c},$$

so we may apply Lemma 6.7 to obtain

$$|\tilde{x}^{p^{n-i}}_{p^m p^i} - x^{p^n}_{p^{m+i+1}p^{i+1}}| \le p^{-(n-i+1)+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}}.$$

This immediately implies

$$|p^{i-n} \tilde{x}^{p^{n-i}}_{p^m p^i} - p^{i-n} x^{p^n}_{p^{m+i+1}p^{i+1}}| \le p^{-1+r(n+1)p^{n-m}} \tilde{c}^{p^{n-m}}.$$

By applying (6.8.5) $n-i$ times, we get

$$|p^{i-n} x^{p^n}_{p^{m+i+1}p^{i+1}} - p^{i-n} x^{p^{2n-i}}_{p^{m+n+1}p^{i+1}}| \le p^{-(i+1)+r(n+i+2)p^{n-m}} \tilde{c}^{p^{n-m}}.$$

Combining the last two inequalities yields (7.2.4).

Finally, we prove (7.2.5). From the definition of c,

$$|p^j x^{p^{n-j}}_{p^{m+n+1}p^{n+1+j}}| = p^{-j} |x^{p^{m-j}}_{p^{m+n+1}p^{n+1+j}}|^{p^{n-m}} \le p^{-j+r(n+1+j)p^{n-m}} c^{p^{n-m}}.$$

Recalling that $\tilde{c} \ge pc$, we are done if we show that $-j + rjp^{n-m} \le -1 + p^{n-m}$. This holds for all $j \ge 1$, because $r < 1$ and $p^{n-m} \le 1$.

This completes the proof of (7.2.1). Combining (7.2.1) and Lemma 6.7 (the conditions of which we checked above), we have that

$$\begin{aligned}|\tilde{x}^{p^{m-n}}_{p^m p^n} - x^{p^m}_{p^{m+n+1}p^{n+1}}| &\le p^{-(m-n+1)+r(m+1)} \tilde{c} \\ &= p^{(r-1)(m+1)+n} \tilde{c} \\ &\le p^{(r-1)n+n} \tilde{c}\end{aligned}$$

(because $r-1<0$ and $n \leq m$)

$$= p^{rn}\tilde{c}.$$

Since also $|x_{p^{m+n+1}p^{n+1}}^{p^m}| \leq p^{r(n+1)}c \leq p^{rn}\tilde{c}$ by the definition of c, we have that $|\tilde{x}_{p^m p^n}^{p^{m-n}}| \leq p^{rn}\tilde{c}$. As noted earlier, this proves the desired result. $\square$

Corollary 7.3. *Let $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$, for $0 \leq r < 1$. Let $(\dots, w_{p^{-1}}, w_1)$ denote the tail of ghost components corresponding to $\underline{x}$. If $\lim_{m\to\infty} w_{p^{-m}}^{p^m} = 0$, then $\underline{x}$ is divisible by p in $\underleftarrow{W}_*(\mathbb{C}_p)_r$.*

Proof. Note first that the limit in question always exists; this was shown in the proof of Theorem 6.8, where the limit was denoted $(y_1)^{(0)}$. The proof showed moreover that $|w_{p^{-m}} - (y_1)^{(m)}| \leq p^{-1+rp^{-m}}c^{p^{-m}}$. In our case, $(y_1)^{(m)} = 0$ for every m, so $|w_{p^{-m}}| \leq p^{-1+rp^{-m}}c^{p^{-m}}$. Thus we see that the condition of Lemma 7.2 is satisfied (with $\kappa = r + \log_p(c)$). $\square$

Proposition 7.4. *The ring $\tilde{\mathbf{A}}^\dagger$ is local, with maximal ideal (p). In particular, the ring $\tilde{\mathbf{B}}^\dagger$ is a field.*

Proof. We first check that p belongs to the Jacobson radical of $\tilde{\mathbf{A}}^\dagger$, i.e., that for any $\underline{x} \in \tilde{\mathbf{A}}^\dagger$, $1 + p\underline{x}$ is a unit in $\tilde{\mathbf{A}}^\dagger$. Since F is bijective on $\tilde{\mathbf{A}}^\dagger$, $1+p\underline{x}$ is a unit if and only if $1 + pF(\underline{x})$ is; we may thus assume without loss of generality that $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ for some $r \in [0,1)$. Put $c = |\underline{x}|_r = \sup_{m,n\geq 0}\{|x_{p^m p^n}|^{p^{m-n}} p^{-nr}\}$. For each nonnegative integer k, we have

$$|\underline{x}|_{p^k r} = |F^{-k}(\underline{x})|_r = \sup_{n,m\geq 0}\{|x_{p^{m+k}p^n}|^{p^{m-n}} p^{-nr}\} \leq \sup_{n\geq 0}\{(cp^{nr})^{p^{-k}} p^{-nr}\}.$$

As $k \to \infty$, the term in the final supremum tends to $p^{-nr} \leq 1$ unless $c = 0$, so $\limsup_{k\to\infty} |\underline{x}|_{p^k r} \leq 1$. By Remark 6.10, $|p\underline{x}|_{p^k r} = p^{-p^k r}|\underline{x}|_{p^k r}$, so we can choose k so that $|p\underline{x}|_{p^k r} < 1$. Since the set of $\underline{y} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ with $|\underline{y}|_r \leq |pF^{-k}(\underline{x})|_r$ is p-adically complete, the geometric series $(1 + pF^{-k}(\underline{x}))^{-1}$ converges in $\underleftarrow{W}_*(\mathbb{C}_p)_r$. We conclude that $1 + pF^{-k}(\underline{x})$ is a unit in $\tilde{\mathbf{A}}^\dagger$, as then is $1 + p\underline{x}$.

We next verify that if $\underline{x} \in \tilde{\mathbf{A}}^\dagger$ is not a multiple of p, then there is a unit $\underline{y} \in \tilde{\mathbf{A}}^\dagger$ congruent to $\underline{x}$ modulo p. Once again, we may assume without loss of generality that $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ for some $r \in [0,1)$. We choose $\underline{y}$ with $y_{p^m 1} = \lim_{j\to\infty} x_{p^{m+j}1}^{p^j}$ and $y_{p^m p^n} = 0$ for $n \geq 1$ (we saw in the proof of Theorem 6.8 that the limit in question exists). In other words, we are choosing $\underline{y}$ to be a sequence of Teichmüller elements. Because we are assuming $\underline{x}$ is not divisible by p even in $\tilde{\mathbf{A}}^\dagger$, we know by Corollary 7.3 that the element $\underline{y}$ is nonzero. Clearly any nonzero element of $\underleftarrow{W}_*(\mathbb{C}_p)_r$ consisting of Teichmüller elements is invertible. So we are done if we show that $\underline{x} - \underline{y}$ is divisible by p in $\underleftarrow{W}_*(\mathbb{C}_p)_r$. We are done if we can find κ with

$$|x_{p^m 1} - y_{p^m 1}| \leq p^{-1+\kappa p^{-m}},$$

and this is implied by the proof of Theorem 6.8 (see (6.8.4)).

We have just shown that each element in the complement of (p) is a unit. Conversely, $\tilde{\mathbf{A}}^\dagger$ is p-adically separated by Lemma 6.11 and the fact that if an element of $\underleftarrow{W}_*(\mathbb{C}_p)_r$ is divisible by p in $\tilde{\mathbf{A}}^\dagger$, then it is divisible by p in $\underleftarrow{W}_*(\mathbb{C}_p)_r$ (see the proof of Lemma 7.2). In particular, p is not a unit, so it generates the unique maximal ideal of $\tilde{\mathbf{A}}^\dagger$. This ring is thus local; again because it is p-adically separated, $\tilde{\mathbf{B}}^\dagger$ is a field. □

For any finite extension K of $\mathbb{Q}_p$, the absolute Galois group G_K acts on $\mathcal{O}_{\mathbb{C}_p}$ and $\mathbb{C}_p$, and hence on all rings constructed functorially from these. (See for instance [4, Section 2.1] for some properties of this action.)

Proposition 7.5. *Let $K \supseteq \mathbb{Q}_p$ denote a finite extension, and let $K \supseteq K_0 \supseteq \mathbb{Q}_p$ denote the maximal unramified subextension. Then $(\tilde{\mathbf{B}}^\dagger)^{G_K} = K_0$.*

Note that for k_0 the residue field of K_0, there is a natural identification of $K_0 \cong W(k_0)[\frac{1}{p}]$ with a subring of $\tilde{\mathbf{A}}^+[\frac{1}{p}]$. This can be seen either using Dwork's lemma (Lemma 1.6) or using the diagonal homomorphism $W(k_0) \to W(W(k_0))$ (Remark 1.8) followed by Witt vector functoriality.

Proof. Suppose $\underline{x} \in \tilde{\mathbf{B}}^\dagger$ is invariant; after multiplying by a power of p and applying a suitable power of Frobenius, we may reduce to the case $\underline{x} \in \underleftarrow{W}_*(\mathbb{C}_p)_r$ for some $r \in [0,1)$. The tail of $\underline{x}$ must be G_K-invariant, so by Proposition 6.12, the entire ghost sequence $(\dots, w_{p^{-1}}, w_1)$ must consist of elements of K.

Since the $w_{p^{-j}}$ are all in K, so are the $x_{p^m p^n}$. From the proof of Theorem 6.8, the $y_{p^i}^{(j)}$ are p-adic limits of certain powers of the $x_{p^m p^n}$, so they also belong to K. But the only way to obtain a sequence of elements of K which is coherent for the p-power map is to take a sequence consisting of powers of a fixed Teichmüller element (since those are the only elements admitting all p-power roots in K). Since Teichmüller elements of K generate unramified extensions of $\mathbb{Q}_p$, this shows that the terms $y_{p^i}^{(j)}$ are in fact in K_0. The proof of Theorem 6.8 expresses each $w_{p^{-j}}$ as a p-adic limit of the terms $y_{p^i}^{(j)}$, and hence each $w_{p^{-j}}$ is also in K_0. Finally, the particular expressions for the elements $w_{p^{-j}}$ show that $\varphi(w_{p^{-j-1}}) = w_{p^{-j}}$, where φ is the Frobenius map on K_0, hence we can associate such a sequence with the single element $w_1 \in K_0$. This completes the proof. □

Definition 7.6. *Put $\tilde{\mathbf{B}}^+ := \tilde{\mathbf{A}}^+[\frac{1}{p}]$. Let $\tilde{\mathbf{B}}^+_{\mathrm{rig}}$ denote the Fréchet completion of $\tilde{\mathbf{B}}^+$ with respect to the norms $|\cdot|_r$ for all $r \geq 0$. Let $\tilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ denote the union over all $r \geq 0$ of the Fréchet completion of $\underleftarrow{W}_*(\mathbb{C}_p)_r[\frac{1}{p}]$ with respect to the norms $|\cdot|_s$ for all $s \geq r$.*

The ring $\tilde{\mathbf{B}}^\dagger_{\mathrm{rig}}$ admits a tail map, while $\tilde{\mathbf{B}}^+_{\mathrm{rig}}$ admits a full ghost map to $\prod_{p^{\mathbb{Z}}} \mathbb{C}_p$. However, neither of these maps is injective. For example, choose $[\epsilon] = ([\epsilon_1], [\epsilon_p], \dots) \in \tilde{\mathbf{A}}^+$ with $\epsilon_{p^n} \in \mathcal{O}_{\mathbb{C}_p}$ a primitive p^n-th root of unity. Then the series

$$t := \log([\epsilon]) = -\sum_{i=1}^{\infty} \frac{1}{i}(1-[\epsilon])^i$$

defines an element of $\tilde{\mathbf{B}}^+_{\mathrm{rig}}$ for which $F(t) = pt$. However, since $\epsilon_1 = 1$, we have $w_1(t) = 0$, and hence $w_{p^n}(t) = 0$ for all n.

Definition 7.7. *Let $\mathbf{B}^+_{\mathrm{dR}}$ be the completion of $\tilde{\mathbf{B}}^+$ with respect to the kernel of w_1; this gives the usual definition because w_1 coincides with the map θ by Proposition 5.8. It is equivalent to take the completion of $\tilde{S}^{-1}\tilde{\mathbf{A}}^+$ with respect to the kernel of w_1.*

Let $\mathbf{B}_e$ denote the graded ring whose component at a nonnegative rational number r/s consists of those $\underline{x} \in \tilde{\mathbf{B}}^+_{\mathrm{rig}}$ for which $F^s(\underline{x}) = p^r \underline{x}$. The rings $\mathbf{B}_e$ and $\mathbf{B}^+_{\mathrm{dR}}$ can be used together to give a very compact description of all of the operations in p-adic Hodge theory; this was originally done by Berger [2]. *More recently, Fargues and Fontaine* [5] *have reformulated Berger's description in a manner that improves the analogy with certain related constructions in positive characteristic, by using the language of vector bundles on curves.*

References

[1] Laurent Berger. An introduction to the theory of p-adic representations. *Geometric Aspects of Dwork Theory*, 2004.
[2] Laurent Berger. Construction de (ϕ, Γ)-modules: représentations p-adiques et B-paires. *Algebra Number Theory*, 2(1):91–120, 2008.
[3] N. Bourbaki. *Algèbre Commutative: Chapitres 8 et 9.* Masson, 1983.
[4] Olivier Brinon and Brian Conrad. CMI summer school notes on p-adic Hodge theory. 2009. http://math.stanford.edu/~conrad/papers/notes.pdf.
[5] Laurent Fargues and Jean-Marc Fontaine. Courbes et fibrés vectoriels en théorie de Hodge p-adique. 2010. in preparation; draft available at http://www.math.u-psud.fr/\~{}fargues/Prepublications.html.
[6] Jean-Marc Fontaine and Jean-Pierre Wintenberger. Le "corps des normes" de certaines extensions algébriques de corps locaux. *C. R. Acad. Sci. Paris Sér. A-B*, 288(6):A367–A370, 1979.
[7] Daniel R. Grayson. Grothendieck rings and Witt vectors. *Comm. Algebra*, 6(3):249–255, 1978.
[8] Michiel Hazewinkel. *Formal Groups and Applications.* Academic Press, 1978.
[9] Lars Hesselholt. The big de Rham-Witt complex. 2010. http://www.math.nagoya-u.ac.jp/~larsh/papers/028/.
[10] Lars Hesselholt and Ib Madsen. The de Rham-Witt complex in mixed characteristic. *Annales scientifiques de l'Ecole Normale Superieure*, 37(4):1–43, 2004.
[11] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Annales scientifiques de l'Ecole Normale Superieure*, 12(4):501–661, 1979.
[12] Kiran S. Kedlaya. Power series and p-adic algebraic closures. *Journal of Number Theory*, 89(2):324–339, 2001.
[13] Kiran S. Kedlaya. Slope filtrations revisited. *Doc. Math.*, 10:447–525, 2005. errata, *ibid.* **12** (2007), 361–362.
[14] Kiran S. Kedlaya. Some new directions in p-adic Hodge theory. *J. Théor. Nombres Bordeaux*, 21(2):285–300, 2009.
[15] Serge Lang. *Algebraic Number Theory.* Springer, 1994.
[16] H.W. Lenstra, Jr. Construction of the ring of Witt vectors. 2002. http://www.math.leidenuniv.nl/~hwl.
[17] Jean-Pierre Serre. *Local Fields.* Springer, 1979.

University of California, Irvine, Dept of Mathematics, Irvine, CA 92697
E-mail address: davis@math.uci.edu

Massachusetts Institute of Technology, Dept of Mathematics, Cambridge, MA 02139
E-mail address: kedlaya@mit.edu