

ON THE WITT VECTOR FROBENIUS

CHRISTOPHER DAVIS AND KIRAN S. KEDLAYA

ABSTRACT. We study the kernel and cokernel of the Frobenius map on the p -typical Witt vectors of a commutative ring, not necessarily of characteristic p . We give some equivalent conditions to surjectivity of the Frobenius map on both finite and infinite length Witt vectors; the former condition turns out to be stable under certain integral extensions, a fact which relates closely to a generalization of Faltings's almost purity theorem.

INTRODUCTION

Fix a prime number p . To each ring R (always assumed commutative and with unit), we may associate in a functorial manner the ring of p -typical Witt vectors over R , denoted $W(R)$. This ring is set-theoretically an infinite product of copies of R , but with an exotic ring structure; for example, for R a perfect ring of characteristic p , $W(R)$ is the unique strict p -ring with $W(R)/pW(R) \cong R$. In particular, for $R = \mathbb{F}_p$, $W(R) = \mathbb{Z}_p$.

Although the Witt vector functor is defined for arbitrary rings, it is most often evaluated only on perfect rings of characteristic p . However, more general rings occur often in applications of Witt vectors in arithmetic (e.g., in the study of relative crystalline cohomology as in Langer-Zink [8, 9]) and topology (e.g., in K -theoretic contexts such as that of Hesselholt and Madsen [4]).

In this paper, we study the kernel and cokernel of the Frobenius endomorphism on $W(R)$. In case $p = 0$ in R , this map is induced by functoriality from the Frobenius endomorphism of R , and in particular is injective when R is reduced and bijective when R is perfect. If $p \neq 0$ in R , the Frobenius map is somewhat more mysterious; to begin with, it is never injective. In fact, it is easy and useful to construct many elements of the kernel. On the other hand, Frobenius is surjective in some cases, although these seem to be somewhat artificial; the simplest nontrivial example we have found is a spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ (the ring of integers in a completed algebraic closure of \mathbb{Q}_p).

While surjectivity of Frobenius on full Witt vectors is rather rare, various weaker conditions turn out to be far more commonly satisfied, and possibly more relevant in applications. For instance, one can view the full ring of Witt vectors as an inverse limit of finite-length truncations; surjectivity of Frobenius on finite levels turns out both to be equivalent to many other conditions and to be relatively easy to satisfy. For instance, this holds for R equal to the ring of integers in any infinite algebraic extension of \mathbb{Q} which is sufficiently ramified at p (e.g., the p -cyclotomic

Date: November 22, 2011.

Davis was supported by the Max-Planck-Institut für Mathematik (Bonn). Kedlaya was supported by NSF (CAREER grant DMS-0545904, grant DMS-1101343), DARPA (grant HR0011-09-1-0048), MIT (NEC Fund, Cecil and Ida Green professorship), UCSD (Stefan E. Warschawski professorship).

extension). This is related to such constructions as the *field of norms equivalence* of Fontaine-Wintenberger and the *almost purity theorem* of Faltings; at the end of the paper, we describe a very general form of almost purity (building on work of the second author and Liu [7] and of Scholze [11]) in which the condition of surjectivity of Frobenius on finite Witt vectors appears quite naturally.

Besides almost purity, one principal motivation for our study of the Frobenius on Witt vectors is to reframe p -adic Hodge theory in terms of Witt vectors of characteristic 0 rings, and ultimately to globalize the constructions with an eye towards study of global étale cohomology, K -theory, and L -functions. We will pursue these goals in subsequent papers.

1. BACKGROUND ON WITT VECTORS

We briefly recall the construction of rings of p -typical Witt vectors and the Frobenius homomorphism F . For more details, see Section 0.1 of [5].

Definition 1.1. *For each nonnegative integer n and each ring R , define the set $W_{p^n}(R) := R^{n+1}$, indexing tuples on the right side as $(r_1, r_p, \dots, r_{p^n})$. Define the Verschiebung map $V : W_{p^n}(R) \rightarrow W_{p^{n+1}}(R)$ by the formula $V(r_1, \dots, r_{p^n}) = (0, r_1, \dots, r_{p^n})$.*

There is a unique way to equip each $W_{p^n}(R)$ with a ring structure in a functorial manner (i.e., if $R \rightarrow S$ is a ring homomorphism, then the map $W_{p^n}(R) \rightarrow W_{p^n}(S)$ induced by the natural map $R^{n+1} \rightarrow S^{n+1}$ is a ring homomorphism) so that for $i = 0, \dots, n$, the p^i -th ghost component map $w_{p^i} : W_{p^n}(R) \rightarrow R$ defined by

$$w_{p^i}(r_1, \dots, r_{p^n}) = r_1^{p^i} + pr_p^{p^{i-1}} + \dots + p^i r_{p^i}$$

is a ring homomorphism.

There is also a unique way to define ring homomorphisms $F : W_{p^{n+1}}(R) \rightarrow W_{p^n}(R)$ in a functorial way (i.e., if $R \rightarrow S$ is a ring homomorphism, then the maps $W_{p^n}(R) \rightarrow W_{p^n}(S)$ are F -equivariant) so that for $i = 0, \dots, n$, we have $w_{p^i} \circ F = w_{p^{i+1}}$. Each such map is called the Frobenius homomorphism on its domain.

There is a natural restriction map $W_{p^{n+1}}(R) \rightarrow W_{p^n}(R)$ obtained by forgetting the last component; define $W(R)$ to be the inverse limit of the $W_{p^n}(R)$ via these restriction maps. The Frobenius homomorphisms at finite levels then collate to define another Frobenius homomorphism $F : W(R) \rightarrow W(R)$; there is also a collated Verschiebung map $V : W(R) \rightarrow W(R)$. The ghost component maps also collate to define a ghost map: $w : W(R) \rightarrow R^{\mathbb{N}}$. We equip the target with component-wise ring operations; the map w is then a ring homomorphism.

In either $W_{p^n}(R)$ or $W(R)$, an element of the form $(r, 0, 0, \dots)$ is called a Teichmüller element and denoted $[r]$.

Remark 1.2. *A standard method of proving identities about Witt vectors and their operations is reduction to the universal case: take R to be a polynomial ring in sufficiently many variables over \mathbb{Z} , form Witt vectors whose components are distinct variables, then verify the desired identities at the level of ghost components, which suffices because the ghost map is injective in this case. For example, the following identities can be checked in this manner.*

- (a) For $r \in R$, $F([r]) = [r^p]$.
- (b) For $\underline{x}, \underline{y} \in W_{p^n}(R)$, $V(\underline{x} + \underline{y}) = V(\underline{x}) + V(\underline{y})$.

- (c) For $\underline{x} \in W_{p^n}(R)$, $(F \circ V)(\underline{x}) = p\underline{x}$.
 (d) For $\underline{x} \in W_{p^n}(R)$ and $\underline{y} \in W_{p^{n+1}}(R)$, $V(\underline{x}F(\underline{y})) = V(\underline{x})\underline{y}$.

Remark 1.3. For properties of Witt vectors involving divisibilities by p , reduction to the universal case as described above is insufficient, because the inverse of the ghost map involves divisions by p . Instead, one must supplement with one of two other techniques.

- (1) The Cartier-Dieudonné-Dwork lemma: if $\varphi : R \rightarrow R$ is a ring homomorphism lifting the p -th power map on R/pR , then w_1, w_p, w_{p^2}, \dots forms a sequence of ghost components of an element of $W(R)$ if and only if $\varphi(w_{p^{n-1}}) \equiv w_{p^n} \pmod{p^n}$ for each positive integer n . (The corresponding statement on finite levels is also true.)
 (2) The splitting principle: for any ring R and any nonnegative integer n , there exists a faithfully flat ring homomorphism $R \rightarrow S$ such that each element of $W_{p^n}(R)$ splits as a sum of Teichmüller elements of $W_{p^n}(S)$.

2. FURTHER PROPERTIES OF WITT VECTORS

Throughout this section, let R denote an arbitrary ring.

Lemma 2.1. For any integers $0 \leq i \leq n$, and any $\underline{x}, \underline{y} \in W_{p^n}(R)$, for $\underline{z} = \underline{x} + p^n \underline{y}$, $z_{p^i} - x_{p^i}$ is divisible by p^{n-i} .

Proof. By reduction to the universal case, we may assume that R is p -torsion-free. In this case, we proceed by induction on i , the case $i = 0$ being apparent. Given the claim for all $j < i$, we apply w_{p^i} to the equation $\underline{z} = \underline{x} + p^n \underline{y}$ and find

$$z_{p^i} - x_{p^i} = p^{n-i} w_{p^i}(\underline{y}) - \sum_{j=0}^{i-1} p^{j-i} (z_{p^j}^{p^{i-j}} - x_{p^j}^{p^{i-j}}).$$

By the induction hypothesis, $z_{p^j} - x_{p^j}$ is divisible by p^{n-j} , so $z_{p^j}^{p^{i-j}} - x_{p^j}^{p^{i-j}}$ is divisible by $p^{n-j+i-j}$. This proves the claim. \square

The following result is well-known when R is p -torsion-free (e.g., see [3, Lemma 1.1.1]).

Lemma 2.2. Let n be a nonnegative integer. If any one of the rings $R, W_{p^n}(R), W(R)$ is p -adically separated (resp. separated and complete), then so are the others.

Proof. Suppose that $W(R)$ is p -adically separated. Given $r \in R$ divisible by p^i for each positive integer i , we can write $r = p^i r_i$ for some $r_i \in R$. In $W(R)$, we then have $[r] = [p^i][r_i]$. By the Dwork lemma, $[p^i]$ is divisible by p^{i-1} in $W(\mathbb{Z})$, so $[r]$ is divisible by p^{i-1} in $W(R)$. Since this is true for all i , $[r] = 0$ in $W(R)$, so $r = 0$ in R . Hence R is p -adically separated. Similarly, if $W_{p^n}(R)$ is p -adically separated, then so is R .

Suppose that $W(R)$ is p -adically separated and complete. Given a sequence $r_0, r_1, \dots \in R$, the sequence $[r_0], [r_0] + p[r_1], \dots$ has a p -adic limit x in $W(R)$. The first component of x is then a p -adic limit of the sequence $r_0, r_0 + pr_1, \dots$. Since R is p -adically separated by the previous paragraph, it follows that R is also p -adically complete. Similarly, if $W_{p^n}(R)$ is p -adically complete, then so is R .

Suppose that R is p -adically separated. Given $\underline{x} \in W_{p^n}(R)$ divisible by p^i for each nonnegative integer i , by Lemma 2.1, x_{p^j} is divisible by p^{i-j} for each integer

$j \in \{0, \dots, n\}$ and each integer $i \geq j$. Consequently, $x_{p^j} = 0$ in R , so $\underline{x} = 0$ in $W_{p^n}(R)$. Hence $W_{p^n}(R)$ is p -adically separated, as is $W(R)$.

Suppose that R is p -adically separated and complete. Given a sequence $\underline{x}_0, \underline{x}_1, \dots \in W_{p^n}(R)$, by Lemma 2.1, the sequence $\underline{x}_0, \underline{x}_0 + p\underline{x}_1, \dots$ converges component-by-component to a unique limit \underline{y} . Note that for fixed i , we have that $\underline{y} - (\underline{x}_0 + p\underline{x}_1 + \dots + p^i \underline{x}_i)$ is the component-by-component limit of the sequence $p^{i+1} \underline{x}_{i+1}, p^{i+1}(\underline{x}_{i+1} + p\underline{x}_{i+2}), \dots$. The effect of multiplication by p^{i+1} on the components of a Witt vector is described in terms of polynomials with integer coefficients, so multiplication by p^{i+1} is continuous in the component-by-component p -adic topology. Thus we have $\underline{y} - (\underline{x}_0 + p\underline{x}_1 + \dots + p^i \underline{x}_i) = p^{i+1} \underline{z}$, for \underline{z} the component-by-component limit of the sequence $\underline{x}_{i+1}, \underline{x}_{i+1} + p\underline{x}_{i+2}, \dots$. This shows that \underline{y} is in fact the p -adic limit of $\underline{x}_0, \underline{x}_0 + p\underline{x}_1, \dots$. Hence $W_{p^n}(R)$ is p -adically complete. Similarly, $W(R)$ is p -adically complete. \square

When R is of characteristic p , we can completely determine when F is injective or surjective using the following explicit description.

Lemma 2.3. *Suppose R is a ring in which $p = 0$, and let $\varphi : R \rightarrow R$ denote the Frobenius homomorphism on R . Then the map $F : W_{p^{n+1}}(R) \rightarrow W_{p^n}(R)$ coincides with the composition of the functoriality map $W(\varphi) : W_{p^{n+1}}(R) \rightarrow W_{p^{n+1}}(R)$ with the restriction $W_{p^{n+1}}(R) \rightarrow W_{p^n}(R)$.*

Proof. The two maps agree on Teichmüller elements thanks to Remark 1.2(a). The general result then follows from the splitting principle. \square

Remark 2.4. *Suppose R is a ring in which $p = 0$, and let $\varphi : R \rightarrow R$ denote the Frobenius homomorphism on R . By Lemma 2.3, we have $F(r_1, r_p, r_{p^2}, \dots) = (r_1^p, r_p^p, r_{p^2}^p, \dots)$. As a result, F is injective/surjective/bijective if and only if φ is injective/surjective/bijective. In particular, F is injective if and only if R is reduced, and F is bijective if and only if R is perfect. Similarly, the finite level Frobenius map $F : W_{p^n}(R) \rightarrow W_{p^{n-1}}(R)$, which sends (r_1, \dots, r_{p^n}) to $(r_1^p, r_p^p, \dots, r_{p^{n-1}}^p)$, is injective only if $R = 0$, and is surjective if and only if φ is surjective.*

From Lemma 2.3, we may easily infer a divisibility property for the Frobenius homomorphism for general R .

Lemma 2.5. *Take $\underline{x}, \underline{y} \in W(R)$ with $F(\underline{x}) = \underline{y}$. Then for each nonnegative integer i , we have $y_{p^i} = x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, \dots, x_{p^i})$, where f_{p^i} is a certain universal polynomial with coefficients in \mathbb{Z} that involves only the coordinates x_1, \dots, x_{p^i} . Furthermore, the polynomial f_{p^i} is homogeneous of degree p^{i+1} under the weighting in which the variable x_{p^j} has weight p^j .*

Proof. By reduction to the universal case, we see that y_{p^i} equals a universal polynomial in $x_1, \dots, x_{p^{i+1}}$ with coefficients in \mathbb{Z} which is homogeneous of degree p^{i+1} for the given weighting. The fact that this polynomial is congruent to $x_{p^i}^p$ modulo p follows from Lemma 2.3. All that remains is to compute the coefficient of $x_{p^{i+1}}$; we may check this assuming that $x_1 = \dots = x_{p^i} = 0$, in which case we must verify that $F(0, \dots, 0, x_{p^{i+1}}) = (0, \dots, 0, px_{p^{i+1}})$. This follows from the identity $F(V^n([x_{p^{i+1}}])) = pV^{n-1}([x_{p^{i+1}}])$, for which we refer to Remark 1.2(c). \square

For a few calculations, we will need a more precise description of the polynomial f_{p^i} . We first prove the following lemma.

Lemma 2.6. *In $W(\mathbb{Z}/p^2\mathbb{Z})$, we have*

$$p = (p, (-1)^{p-1}, 0, 0, \dots).$$

Proof. Write $p = (x_1, x_p, \dots) \in W(\mathbb{Z})$. Then $x_1 = p$ and $x_p = (p-p^p)/p = 1-p^{p-1}$, which is congruent to 1 mod p^2 if $p > 2$ and to 3 mod 4 if $p = 2$. To complete the argument, we show by induction on n that for each $n \geq 1$, we have $x_{p^i} \equiv 0 \pmod{p^2}$ for $2 \leq i \leq n$. The base case $n = 1$ is vacuously true. For the induction step, considering the p^n -th ghost component of p , write

$$p^n x_{p^n} = -x_1^{p^n} + p(1 - x_p^{p^{n-1}}) - \sum_{i=2}^{n-1} p^i x_{p^i}^{p^{n-i}}.$$

To complete the induction, it suffices to check that each term on the right side has p -adic valuation at least $n+2$. This is clear for the first term because $p^n \geq n+2$. For the second term, treating $p = 2$ and $p > 2$ separately, we have $x_p \equiv (-1)^{p-1} \pmod{p^{p-1}}$ and so $x_p^p \equiv 1 \pmod{p^3}$. We then have $x_p^{p^{n-1}} \equiv 1 \pmod{p^{3+n-2}}$, so the second term is indeed divisible by p^{n+2} . For the terms in the sum, the claim is again clear because $i + 2p^{n-i} \geq i + 2(n-i+1) \geq n+2$. \square

Lemma 2.5'. *Set notation as in Lemma 2.5.*

- (a) *For $i \geq 1$, the coefficient of $x_1^{p^{i+1}}$ in f_{p^i} equals 0.*
- (b) *For $i \geq 2$, the coefficient of x_p^p in f_{p^i} is divisible by p .*
- (c) *The coefficient of x_p^p in f_p equals $-p^{p-2}$ modulo p .*
- (d) *For $p = 2$ and $i \geq 2$, f_{p^i} belongs to the ideal generated by $2, x_1, x_p^p - x_{p^2}, x_{p^3}, \dots, x_{p^i}$.*

Proof. To check (a), we assume that $x_p = x_{p^2} = \dots = 0$. In this case, the claim follows from the formula $F([x_1]) = [x_1^p]$, for which we refer to Remark 1.2(a).

To check (b), we may assume that $x_1 = 0$ and that $x_{p^2} = x_{p^3} = \dots = 0$. In this case, the claim is that if we write $F(V([x_p])) = y$, then $y_{p^i} \equiv 0 \pmod{p^2}$ for $i \geq 2$. The left side equals $p[x_p]$ by Remark 1.2(c), so by homogeneity it is sufficient to check the claim for $x_p = 1$. In this case, it follows from Lemma 2.6. We may similarly check (c).

To check (d), consider first $f_{p^i}(0, x_p, 1, 0, \dots)$ as a polynomial in x_p^p . If we show that this has a root at $x_p^p = 1$, then $f_{p^i}(0, x_p, 1, 0, \dots)$ is a multiple of $x_p^p - 1$, and hence, by homogeneity, $f_{p^i}(0, x_p, x_{p^2}, 0, \dots)$ is a multiple of $x_p^p - x_{p^2}$. Now define $\underline{y} = F(0, 1, 1, 0, 0, \dots)$ in $W(\mathbb{Z}/4\mathbb{Z})$; it will suffice to check that $\underline{y} = (2, 1, 1, 0, 0, \dots)$. To see this, first rewrite \underline{y} as $F(V(1)) + F(V^2(1)) = 2 + 2V(1) = 2 + V(2)$. Then Lemma 2.6 states that $\underline{2} = (2, -1, 0, 0, \dots) = [2] + V([-1])$ in $W(\mathbb{Z}/4\mathbb{Z})$. The desired equality may thus be rewritten as $[2] + V([-1]) + V(2) = [2] + V(1) + V^2(1)$, which is equivalent to $[-1] + 2 = 1 + V(1)$ or $[-1] + 1 = V(1)$. However, this last equality is true not only in $W(\mathbb{Z}/4\mathbb{Z})$ but also in $W(\mathbb{Z})$, as may be seen at the level of ghost components. \square

3. THE KERNEL OF FROBENIUS

When R is a ring not of characteristic p , it is easy to see that $F : W(R) \rightarrow W(R)$ cannot be injective.

Proposition 3.1. *For any ring R , there exists $\underline{x} \in W(R)$ with $x_1 = p$ and $F(\underline{x}) = 0$. Consequently, if $p \neq 0$ in R , then neither $F : W_{p^{n+1}}(R) \rightarrow W_{p^n}(R)$ for any nonnegative integer n nor $F : W(R) \rightarrow W(R)$ is injective.*

Proof. By the Dwork lemma, there exists $\underline{x} \in W(\mathbb{Z})$ with ghost components $p, 0, 0, \dots$. We may map this element to $W(R)$ by functoriality. \square

One can more generally determine exactly which elements of R can occur as the first component of an element of the kernel of F . This will be useful in our analysis of surjectivity of F . (Note that if R is p -torsion-free, then an element of the kernel of F is uniquely determined by its first component. This follows because the ghost map is injective in this case, and the image under the ghost map of any element in the kernel of F has the form $(*, 0, 0, \dots)$.)

Definition 3.2. *Let R denote a ring. We are going to recursively define ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \dots$. Let $I_0 = R$, and define $I_i := \{r \in R \mid r^p \in pI_{i-1}\}$. (The claim that $I_i \subseteq I_{i-1}$ can be easily proven using induction on i .) We show that I_i is indeed an ideal below. Also define $I_\infty = \bigcap_{i=1}^\infty I_i$, so that $I_\infty = \{r \in R \mid r^p \in pI_\infty\}$.*

Remark 3.3. *If R is the ring of integers in an algebraic closure of \mathbb{Q}_p (or the completion thereof), then I_i is the principal ideal generated by any element of valuation $\frac{1}{p} + \frac{1}{p^2} + \dots + \frac{1}{p^i}$, while I_∞ is the principal ideal generated by any element of valuation $\frac{1}{p-1}$.*

Lemma 3.4. *For each i , the set I_i defined above is an ideal.*

Proof. That I_i is closed under multiplication by arbitrary elements of R is clear. It remains to show that if $x, y \in I_i$, then $x + y \in I_i$. Using the definition, we must check that $x^p + px^{p-1}y + \dots + pxy^{p-1} + y^p \in pI_{i-1}$. That $x^p, y^p \in pI_{i-1}$ follows from $x, y \in I_i$. That the remaining terms are in pI_{i-1} follows from $x, y \in I_i \subseteq I_{i-1}$. \square

Definition 3.5. *For any ring R , any $r_0 \in R$, and any $i \geq 0$ (including $i = \infty$), define $B(r_0, I_i) := r_0 + I_i = \{r \in R \mid r - r_0 \in I_i\}$. The notation is meant to suggest that B is a ball centered at r_0 .*

The significance of the ideals I_i is the following.

Proposition 3.6. *Let R be a ring, let i be a positive integer, and let n be either ∞ or an integer greater than or equal to i .*

- (a) *If $\underline{x}, \underline{y} \in W_{p^i}(R)$ are such that $x_{p^j} - y_{p^j} \in I_{n-j}$ for $j = 0, \dots, i$, then for $\underline{x}' := F(\underline{x}), \underline{y}' := F(\underline{y})$, we have $x'_{p^j} - y'_{p^j} \in pI_{n-j-1}$ for $j = 0, \dots, i-1$.*
- (b) *Take $\underline{x}, \underline{y} \in W_{p^i}(R)$ and put $\underline{x}' := F(\underline{x}), \underline{y}' := F(\underline{y})$. If $x'_{p^j} - y'_{p^j} \in pI_{n-j}$ for $j = 0, \dots, i$ and $x_{p^i} - y_{p^i} \in I_{n-i}$, then $x_{p^j} - y_{p^j} \in I_{n-j}$ for $j = 0, \dots, i$. In particular, if $\underline{x}' = \underline{y}'$, then this always holds when $n = i$.*
- (c) *Choose $x_1, \dots, x_{p^{i-1}}, y_1, \dots, y_{p^i} \in R$ with $x_{p^j} - y_{p^j} \in I_{n-j}$ for $j = 0, \dots, i-1$. If $i > 1$, assume also that $F(x_1, x_p, \dots, x_{p^{i-1}}) = F(y_1, y_p, \dots, y_{p^{i-1}})$. Then there exists $x_{p^i} \in B(y_{p^i}, I_{n-i})$ such that $F(x_1, x_p, \dots, x_{p^i}) = F(y_1, y_p, \dots, y_{p^i})$.*
- (d) *For any $\underline{x} \in W(R)$ for which $x_{p^i} \in pI_\infty$ for all i , there exists $\underline{y} \in W(R)$ for which $y_1 = 0, y_{p^i} \in I_\infty$ for all i , and $F(\underline{y}) = \underline{x}$.*

Proof. To check (a), apply Lemma 2.5 to write $x'_{p^j} - y'_{p^j} = x_{p^j}^p - y_{p^j}^p + p(x_{p^{j+1}} - y_{p^{j+1}}) + p(f_{p^j}(x_1, \dots, x_{p^j}) - f_{p^j}(y_1, \dots, y_{p^j}))$. Writing $y_{p^j} = x_{p^j} - (x_{p^j} - y_{p^j})$, we note that $x_{p^j}^p - y_{p^j}^p$ belongs to the ideal generated by $(x_{p^j} - y_{p^j})^p$ and $p(x_{p^j} - y_{p^j})$.

Note also that $p(f_{p^j}(x_1, \dots, x_{p^j}) - f_{p^j}(y_1, \dots, y_{p^j}))$ belongs to the ideal generated by $p(x_1 - y_1), \dots, p(x_{p^j} - y_{p^j})$. It follows that $x'_{p^j} - y'_{p^j} \in pI_{n-j-1}$.

To check (b), we essentially run the previous argument. We first check that under the hypotheses of (b), if there exists $0 \leq k \leq n - i + 1$ such that $x_{p^j} - y_{p^j} \in I_k$ for $j = 0, \dots, i$, then $x_{p^j} - y_{p^j} \in I_{k+1}$ for $j = 0, \dots, i - 1$. For $j \in \{0, \dots, i - 1\}$, apply Lemma 2.5 to write

$$(x_{p^j} - y_{p^j})^p - (x'_{p^j} - y'_{p^j}) = ((x_{p^j} - y_{p^j})^p - x_{p^j}^p + y_{p^j}^p) - p(x_{p^{j+1}} - y_{p^{j+1}} + f_{p^j}(x_1, \dots, x_{p^j}) - f_{p^j}(y_1, \dots, y_{p^j})).$$

From this equality, we see that $(x_{p^j} - y_{p^j})^p - (x'_{p^j} - y'_{p^j})$ belongs to the ideal generated by $p(x_1 - y_1), \dots, p(x_{p^{j+1}} - y_{p^{j+1}})$. This ideal is contained in pI_k by hypothesis. By assumption we also have $x'_{p^j} - y'_{p^j} \in pI_{n-j}$, and because $n - j \geq n - i + 1 \geq k$, we have $x'_{p^j} - y'_{p^j} \in pI_k$ as well. Hence $(x_{p^j} - y_{p^j})^p \in pI_k$, and so we have $x_{p^j} - y_{p^j} \in I_{k+1}$ as claimed.

Note that the hypothesis of the previous paragraph is always satisfied for $k = 0$ because $I_0 = R$. The previous paragraph gives us control over the terms $x_1 - y_1, \dots, x_{p^{i-1}} - y_{p^{i-1}}$. Since $x_{p^i} - y_{p^i} \in I_{n-i}$ by assumption, we may induct on k to deduce that $x_{p^j} - y_{p^j} \in I_{n-i+1}$ for $j = 0, \dots, i - 1$. In particular, $x_{p^{i-1}} - y_{p^{i-1}} \in I_{n-i+1}$; we may now induct on i to deduce (b).

To check (c), note that by Lemma 2.5 again, it is sufficient to find $x_{p^i} \in B(y_{p^i}, I_{n-i})$ such that $x_{p^{i-1}}^p + px_{p^i} + pf_{p^{i-1}}(x_1, \dots, x_{p^{i-1}}) = y_{p^{i-1}}^p + py_{p^i} + pf_{p^{i-1}}(y_1, \dots, y_{p^{i-1}})$. This is possible because $x_{p^{i-1}} - y_{p^{i-1}} \in I_{n-i+1}$ and $x_1 - y_1, \dots, x_{p^{i-1}} - y_{p^{i-1}} \in I_{n-i}$, so as in the proof of (a) we have $x_{p^{i-1}}^p - y_{p^{i-1}}^p + p(f_{p^{i-1}}(x_1, \dots, x_{p^{i-1}}) - f_{p^{i-1}}(y_1, \dots, y_{p^{i-1}})) \in pI_{n-i}$.

To check (d), we construct the y_{p^i} recursively, choosing $y_1 = 0$. Given y_1, \dots, y_{p^i} , we must choose $y_{p^{i+1}}$ so that in the notation of Lemma 2.5, we have $y_{p^i}^p + py_{p^{i+1}} + pf_{p^i}(y_1, \dots, y_{p^i}) = x_{p^i}$. This is possible because $y_{p^i}^p, pf_{p^i}(y_1, \dots, y_{p^i})$, and x_{p^i} all belong to pI_∞ . \square

Corollary 3.7. *Let R be a ring and let n be either ∞ or a positive integer. Then an element $r \in R$ occurs as the first component of an element of the kernel of $F : W_{p^n}(R) \rightarrow W_{p^{n-1}}(R)$ if and only if $r \in I_n$.*

Proof. Suppose that $n < \infty$. If $r = z_1$ for $\underline{z} \in W_{p^n}(R)$ such that $F(\underline{z}) = 0$, then trivially $z_{p^n} \in I_0$. By Proposition 3.6(b), $z_1 \in I_n$; the same conclusion holds for $n = \infty$.

Conversely, suppose $r \in I_n$. Put $z_1 = r$. By Proposition 3.6(c) applied repeatedly, for each positive integer $i \leq n$, we can find $z_{p^i} \in I_{n-i}$ so that $F(z_1, z_p, \dots, z_{p^i}) = 0$. This proves the claim. \square

Remark 3.8. *If R is a p -torsion-free ring, then any element of the kernel of F is uniquely determined by its first component. In this case, we may combine Proposition 3.6(b) and (c) to deduce that if $\underline{z} \in W_{p^i}(R)$ is such that $F(\underline{z}) = 0$ and $z_1 \in I_n$ for some $n \geq i$, then $z_{p^j} \in I_{n-j}$ for $j = 0, \dots, i$.*

4. SURJECTIVITY CONDITIONS

Surjectivity of the Witt vector Frobenius turns out to be a subtler property than injectivity, because there are many partial forms of surjectivity which occur much

Theorem 4.2. *For any ring R , we have $(ii) \Leftrightarrow (ii)'$, $(vi) \Leftrightarrow (vi)'$, $(x) \Leftrightarrow (x)'$, and $(xiv) \Leftrightarrow (xiv)'$. In addition, each solid single arrow in Figure 1 represents a direct implication, and for each other arrow type, the conditions at the tails of the arrows of that type together imply the condition at the target.*

The proof of Theorem 4.2 will occupy the rest of this section. First, however, we mention some consequences of Theorem 4.2, and some negative results which follow from some examples considered in Section 6.

Corollary 4.3. *For any ring R , we have the following equivalences.*

- $(i) \Leftrightarrow (ii) + (xii) \Leftrightarrow (iii) + (iv) \Leftrightarrow (iii) + (xiii)$
- $(ii) \Leftrightarrow (vi) \Leftrightarrow (xiv) \Leftrightarrow \left\{ (x) \text{ or } (xviii) \right\} + \left\{ (v), (vii), (viii), (ix), (xv), (xvi), \text{ or } (xvii) \right\}$

Remark 4.4. *The following implications fail to hold by virtue of the indicated examples.*

- $(i) \not\Rightarrow (xi)$ by Example 6.7.
- $(ii) \not\Rightarrow (i)$ by Example 6.4 (or from $(ii) \not\Rightarrow (iv)$ below).
- $(ii) \not\Rightarrow (iii)$ by Example 6.4.
- $(ii) \not\Rightarrow (iv)$ by Example 6.9.
- $(ii) \not\Rightarrow (xii)$ by Example 6.4.
- $(iv) \not\Rightarrow (i)$ by Example 6.4.
- $(v) \not\Rightarrow (xv)$ by Example 6.8.
- $(v) \not\Rightarrow (xviii)$ by Example 6.8.
- $(xii) \not\Rightarrow (xvii)$ by Example 6.2.
- $(xv) \not\Rightarrow (xviii)$ by Example 6.3.
- $(xviii) \not\Rightarrow (xvii)$ by Example 6.2.

Remark 4.5. *It seems that there should be some relationship between (iii) and (xii) , but we were unable to clarify this.*

Proof of Theorem 4.2. We now prove the implications represented in Figure 1.

- $(i) \Rightarrow (iv)$; $(ii) \Rightarrow (ii)'$; $(ii) \Rightarrow (vi)$; $(ii)' \Rightarrow (vi)'$; $(vi) \Rightarrow (vi)'$; $(vii) \Rightarrow (ix)$; $(viii) \Rightarrow (ix)$; $(x) \Rightarrow (x)'$; $(xiv) \Rightarrow (xiv)'$; $(xvi) \Rightarrow (xvii)$

Proof. These are all obvious. \square

- $(iv) \Rightarrow (vi)$; $(v) \Rightarrow (vii)$

Proof. These are obvious, given that the Frobenius map commutes with restriction, and that the restriction maps are always surjective. \square

- $(i) \Rightarrow (iii)$

Proof. Let $\underline{x} \in W(R)$ denote an arbitrary element. We may write $\underline{x} = \sum V^i([x_{p^i}])$, and because $F \circ V = p$, we have $F(\underline{x}) \equiv [x_1^p] \pmod{pW(R)}$. Since we are assuming that F is surjective, we deduce (iii). \square

- $(i) \Rightarrow (xii)$

Proof. Fix elements r_i as in condition (xii). Our strategy is to define an element $\underline{y} \in W(R)$ in a special way so that if $\underline{x} \in W(R)$ is such that $F(\underline{x}) = \underline{y}$, then we must have $x_1 \in \cap_{i=0}^{\infty} B(r_i, I_i)$. To prescribe our element $\underline{y} \in W(R)$, it suffices to define compatible finite length Witt vectors $\underline{y}^{(p^i)} \in \overline{W}_{p^i}(R)$ for every i .

Define $\underline{x}^{(p)} \in W_p(R)$ by $\underline{x}^{(p)} = (r_1, 0)$ (the second component does not matter). Set $\underline{y}^{(1)} := F(\underline{x}^{(p)})$. Now inductively assume we have defined $\underline{x}^{(p^i)} \in W_{p^i}(R)$ for some $i \geq 1$ and with first component $x_1^{(p^i)} = r_i$. By Proposition 3.6(c), we can find an element $\underline{z}^{(p^i)} \in W_{p^i}(R)$ with $z_1^{(p^i)} = r_{i+1} - r_i \in I_i$ and with $F(\underline{z}^{(p^i)}) = 0$. Then let $\underline{x}^{(p^{i+1})} \in W_{p^{i+1}}(R)$ denote any element which restricts to $\underline{x}^{(p^i)} + \underline{z}^{(p^i)} \in W_{p^i}(R)$. Set $\underline{y}^{(p^i)} = F(\underline{x}^{(p^i)})$. Then by construction our elements $\underline{y}^{(p^i)}$ correspond to an element of $\varprojlim W_{p^i}(R) \cong W(R)$, which we call \underline{y} .

By (i), we can find an element \underline{x} such that $F(\underline{x}) = \underline{y}$. Because $F(\underline{x})$ and $F(\underline{x}^{(p^{i+1})})$ have the same initial $i+1$ components, we have that $x_1 \equiv \underline{x}_1^{(p^{i+1})} \pmod{I_{i+1}}$. Because x_1 does not depend on i , and $x_1^{(p^{i+1})} = r_{i+1}$, we have that $x_1 \in \bigcap_{i=0}^{\infty} B(r_{i+1}, I_{i+1})$, as desired. \square

- (ii) \Rightarrow (x)

Proof. We apply condition (ii) n times. \square

- (ii) + (xii) \Rightarrow (i)

Proof. Choose any $\underline{y} \in W(R)$. We will construct $\underline{x} \in W(R)$ such that $F(\underline{x}) = \underline{y}$. To do this, it is of course equivalent to choose coordinates of $\underline{x} = (x_1, x_p, x_{p^2}, \dots)$. We use (ii) to find elements $\underline{x}^{(1)}, \underline{x}^{(p)}, \dots \in W(R)$ so that $F(\underline{x}^{(1)}) = (y_1, *, *, \dots)$, $F(\underline{x}^{(p)}) = (y_1, y_p, *, *, \dots)$, and so on. By (xii) and Proposition 3.6(b), we may choose \widetilde{x}_{p^j} in the intersection $B_0(x_{p^j}^{(p^j)}, I_0) \cap B_1(x_{p^j}^{(p^{j+1})}, I_1) \cap \dots$.

Put $\widetilde{\underline{y}} := F(\widetilde{x}_1, \widetilde{x}_p, \dots)$. We first apply Proposition 3.6(a) to $(\widetilde{x}_1, \dots, \widetilde{x}_{p^{i+1}})$ and $(x_1^{(p^k)}, \dots, x_{p^{i+1}}^{(p^k)})$ for fixed i and increasing k , which implies that $\widetilde{y}_{p^i} - y_{p^i} \in pI_{\infty}$ for each nonnegative integer i . This means that \underline{y} and $\widetilde{\underline{y}}$ have the same image in $W(R/pI_{\infty})$, so the difference $\underline{z} = \underline{y} - \widetilde{\underline{y}}$ has all of its components in pI_{∞} . By Proposition 3.6(d), \underline{z} is in the image of F , as then is \underline{y} . \square

- (iii) + (iv) \Rightarrow (i)

Proof. Condition (iii) immediately implies that any Witt vector \underline{x} can be written as $[r] + p\underline{x}'$. Condition (iv) says that $[r_1]$ is in the image of Frobenius, but so is $p\underline{x}' = F(V(\underline{x}'))$. \square

- (iv) \Rightarrow (xiii); (vi) \Rightarrow (xiv); (vi)' \Rightarrow (xiv)'

Proof. Suppose that $n \geq 2$ and that $\underline{x} \in W_{p^n}(R)$ and $r \in R$ satisfy $F(\underline{x}) = [r]$. For each of $k = 0, \dots, n-1$, we check that $x_p, x_{p^2}, \dots, x_{p^{n-k}}$ belong to I_k . This is clear for $k = 0$. Given the claim for some $k < n-1$, for $i = 1, \dots, n-1-k$ we may apply Lemma 2.5 to deduce that $x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, \dots, x_{p^i}) = 0$. By Lemma 2.5', f_{p^i} contains no pure power of $x_1^{p^{i+1}}$, so $f_{p^i}(x_1, \dots, x_{p^i})$ belongs to the ideal generated by x_p, \dots, x_{p^i} . Therefore $-px_{p^{i+1}}$ and $-pf_{p^i}(x_1, \dots, x_{p^i})$ both belong to pI_k , and so x_{p^i} belongs to I_{k+1} . This completes the proof; as a corollary, we observe that $x_p \in I_{n-1}$, and so $r - x_1^p = px_p \in pI_{n-1}$.

If (iv) holds, then given any $r \in R$, we can find $\underline{x} \in W(R)$ with $F(\underline{x}) = [r]$. By the previous paragraph, $r - x_1^p \in pI_{\infty}$, so (xiii) holds. If (vi) holds

for some $n \geq 2$, then given any $r \in R$, we can $\underline{x} \in W_{p^n}(R)$ such that $F(\underline{x}) = [r]$, and then by the previous paragraph $r - x_1^p \in pI_{n-1}$. Thus (xiv) holds. Finally, if (vi)' holds, then taking $n = 2$ in the above discussion, we see that (xiv)' holds. \square

- (ix) \Rightarrow (xvi)

Proof. We are assuming that we can find \underline{x} such that $F(\underline{x}) = V([1])$. Then the ghost components of \underline{x} must be $(*, 0, p)$. In other words, $x_1^p + px_p = 0$ and $x_1^{p^2} + px_p^p + p^2x_{p^2} = p$. The first equality tells us that $x_1^p \in pR$ (and hence $x_1^{p^2} \in p^2R$). The second equality now tells us $px_p^p \equiv p \pmod{p^2R}$ and so $x_p^p \equiv 1 \pmod{pR}$. Write $x_p = 1 + s$. (We are not yet making any claims on s except that $s \in R$.) Raising both sides to the p -th power, we have $x_p^p = 1 + s^p + t$, where $t \in pR$ by the binomial theorem. On the other hand, we decided above that $x_p^p - 1 \in pR$ as well, so in turn we have $s^p \in pR$. Returning to the p -th ghost component equation $x_1^p + px_p = 0$, we now have $x_1^p \equiv -p \pmod{psR}$ where $s^p \in pR$, as required. \square

- (x)' \Rightarrow (xviii)

Proof. After unraveling definitions, the statement (x)' means that the map $R \times R \rightarrow R$ given by $(r_1, r_p) \mapsto r_1^p + pr_p$ is surjective. This proves the result. \square

- (xi) \Rightarrow (i)

Proof. In this case the ghost map is an isomorphism, and it's clear that the ghost map Frobenius $\bar{F} : (r_1, r_p, r_{p^2}, \dots) \mapsto (r_p, r_{p^2}, \dots)$ is surjective. \square

- (xiii) \Rightarrow (iv)

Proof. Given $r \in R$, by (xiii) we may choose $x_1 \in R$, $x_p \in I_\infty$ for which $r = x_1^p + px_p$. We now show that we can choose $x_{p^2}, x_{p^3}, \dots \in I_\infty$ so that $F(x_1, \dots, x_{p^n}) = (r, 0, \dots, 0)$ for each $n \geq 1$; then $\underline{x} = (x_1, x_p, \dots) \in W(R)$ will satisfy $F(\underline{x}) = [r]$ as needed.

Given x_1, \dots, x_{p^n} , define f_{p^n} as in Lemma 2.5. By Lemma 2.5', f_{p^n} contains no pure power of $x_1^{p^{n+1}}$, so $f_{p^n}(x_1, \dots, x_{p^n})$ belongs to the ideal generated by x_p, \dots, x_{p^n} , which by construction is contained in I_∞ . It follows that $-x_{p^n}^p - f_{p^n}(x_1, \dots, x_{p^n}) \in pI_\infty$, so we can find $x_{p^{n+1}} \in pI_\infty$ for which $x_{p^n}^p + px_{p^{n+1}} + f_{p^n}(x_1, \dots, x_{p^n}) = 0$. By Lemma 2.5, this choice of $x_{p^{n+1}}$ has the desired effect. \square

- (xv) \Rightarrow (v)

Proof. We wish to produce elements x_1, x_p, \dots of R such that $F(x_1, x_p, \dots) = (0, 1, 0, 0, \dots) = V(1)$. Using (xv), choose r so that $r^p \equiv -p \pmod{p^2}$. Set $x_1 := r$. Then clearly we can choose $x_p \equiv 1 \pmod{p}$ such that $F(x_1, x_p) = (0)$.

Next, in the notation of Lemma 2.5, we wish to choose x_{p^2} so that

$$x_p^p + px_{p^2} + pf_p(x_1, x_p) = 1.$$

We also wish to ensure that if $p > 2$, then $x_{p^2} \equiv 0 \pmod{p}$, while if $p = 2$, then $x_{p^2} = 1 \pmod{p}$. To see that this is possible, we first observe that $x_p^p \equiv 1 \pmod{p^2}$. We then note that $f_p(x_1, x_p)$ consists of an element of the ideal generated by x_1^p (which is a multiple of p) plus some constant times x_p^p . By Lemma 2.5', if $p > 2$ this constant is divisible by p , so $pf_p(x_1, x_p) \equiv$

$0 \pmod{p^2}$. If $p = 2$, this constant is $-1 \pmod{2}$, so $pf_p(x_1, x_p) \equiv -2 \pmod{p^2}$. In either case, we obtain x_{p^2} of the desired form.

Now inductively assume that for some $i \geq 2$, we have found x_1, x_p, \dots, x_{p^i} such that $x_{p^j} \equiv 0 \pmod{p}$ for $j \geq 3$ and such that $F(x_1, x_p, \dots, x_{p^i}) = (0, 1, 0, \dots, 0)$. We then claim that we can find $x_{p^{i+1}} \equiv 0 \pmod{p}$ such that $F(x_1, x_p, \dots, x_{p^{i+1}}) = (0, (-1)^{p-1}, 0, \dots, 0)$. Using the notation of Lemma 2.5, we wish to find $x_{p^{i+1}} \equiv 0 \pmod{p}$ such that

$$x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, \dots, x_p) = 0.$$

We are done if we show that $f_{p^i}(x_1, \dots, x_p)$ is divisible by p . If $p > 2$, this follows from Lemma 2.5', which guarantees that each term in f_{p^i} is divisible by one of x_1^p, x_{p^j} for some $j \geq 2$, or $px_{p^i}^p$, and all of these are in turn divisible by p . If $p = 2$, Lemma 2.5' also implies that each term in f_{p^i} is divisible by one of $p, x_1^p, x_p^p - x_{p^2}$, or x_{p^j} for some $j \geq 3$. \square

- (xv) \Rightarrow (viii)

Proof. Our goal is to find an element $\underline{x} = (x_1, x_p, \dots, x_{p^n})$ such that $F(\underline{x}) = V^{n-1}(1)$. Ignoring x_{p^n} temporarily, we will first find preliminary values for $x_{p^{n-1}}, \dots, x_1$ (in that order), then we will find the actual values for x_1, \dots, x_{p^n} (in that order). We will write the preliminary values as \widetilde{x}_{p^i} .

Ignore x_{p^n} for the moment. Set $\widetilde{x}_{p^{n-1}} = 1$, and then find $\widetilde{x}_{p^{n-2}}, \dots, \widetilde{x}_1$ (in that order) such that $\widetilde{x}_{p^i}^p \equiv -p\widetilde{x}_{p^{i+1}} \pmod{p^2R}$. This is possible by (xv). Note that $\widetilde{x}_{p^i}^p \in pR$ for $0 \leq i \leq n-2$.

Now we will find the actual values x_1, \dots, x_{p^n} . Set $x_1 := \widetilde{x}_1$. Now assume x_1, \dots, x_{p^i} have been found satisfying $x_{p^j} \equiv \widetilde{x}_{p^j} \pmod{pR}$, with $i \leq n-2$. We now must choose $x_{p^{i+1}}$ such that the p^i -th Witt component of $F(\underline{x})$ is equal to 0. Using the notation of Lemma 2.5, we must choose $x_{p^{i+1}}$ such that $x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, \dots, x_{p^i}) = 0$. Write $x_{p^{i+1}} = \widetilde{x}_{p^{i+1}} + py_{p^{i+1}}$. We must choose $y_{p^{i+1}}$ so that

$$x_{p^i}^p + p\widetilde{x}_{p^{i+1}} + p^2y_{p^{i+1}} + pf_{p^i}(x_1, \dots, x_{p^i}) = 0.$$

Because $\widetilde{x}_{p^i}^p + p\widetilde{x}_{p^{i+1}} \equiv 0 \pmod{p^2}$ and $\widetilde{x}_{p^i} \equiv x_{p^i} \pmod{p}$, we have that

$$x_{p^i}^p + p\widetilde{x}_{p^{i+1}} \equiv 0 \pmod{p^2}.$$

We further have that

$$pf_{p^i}(x_1, \dots, x_{p^i}) \equiv 0 \pmod{p^2};$$

this follows from the homogeneity result in Lemma 2.5 and the fact that $x_{p^j}^p \equiv 0 \pmod{p}$ for all j . Together this shows that we can find the required $y_{p^{i+1}}$.

In this way we can construct the components $x_1, \dots, x_{p^{n-1}}$. Finding the last component x_{p^n} is a little different, because the last component of $V^{n-1}(1)$ is 1 instead of 0. This means that we need

$$x_{p^{n-1}}^p + px_{p^n} + pf_{p^{n-1}}(x_1, \dots, x_{p^{n-1}}) = 1.$$

But this is easy, because we know $x_{p^{n-1}} \equiv 1 \pmod{p}$. \square

- (xvi) \Rightarrow (ix)

Proof. By Lemma 2.5, we must find x_1, x_p, x_{p^2} such that $x_1^p + px_p = 0$ and $x_p^p + px_{p^2} + pf(x_1, x_2) = 1$. By (xvi), we can find an element x_1 such that $x_1^p + p + psr = 0$ where $s^p \in pR$. Thus we choose that element for x_1 , and we choose $x_p = 1 + sr$. It's then clear that $x_p^p + pf(x_1, x_2) \equiv 1 \pmod{pR}$, and so we can find x_{p^2} forcing $x_p^p + px_{p^2} + pf(x_1, x_2) = 1$, as desired. \square

- (xviii) \Rightarrow (x)

Proof. Considering the definition of Frobenius in terms of ghost components, we must show that the (p^n) -th ghost map $w_{p^n} : R^{n+1} \rightarrow R$ is surjective. We show the surjectivity of w_{p^n} using induction on n . Proving the base case $n = 1$ amounts to showing that for any $r \in R$, we can find $r_1, r_p \in R$ with $r_1^p + pr_p = r$, which is exactly (xviii). We now let n be arbitrary. For any $r \in R$, we must find r_1, \dots, r_{p^n} such that $\sum_{i=0}^n p^i r_{p^i}^{p^{n-i}} = r$. We first find r_1, s such that $r - r_1^{p^n} = ps$ by repeatedly applying (xviii). To find the remaining r_{p^i} , we apply the induction hypothesis to s . \square

- (x) \Rightarrow (xviii); (x)' \Rightarrow (x)

Proof. We have already seen (x)' \Rightarrow (xviii). The two results follow because we have also shown (x) \Rightarrow (x)' and (xviii) \Rightarrow (x). \square

- (x) + (xvii) \Rightarrow (xv)

Proof. By (xvii), we can find $s_1, s_2 \in R$ for which $s_1^p = -p(1 - s_2)$ and $s_2^N \in (p)$ for some $N > 0$. We know that (x) \Rightarrow (x)' \Rightarrow (xviii). Given any $r \in R$, by (xviii) we can find $s_3 \in R$ for which $s_3^p \equiv -r(1 + s_2 + \dots + s_2^{N-1}) \pmod{p}$. Since $s_2^N \equiv 0 \pmod{p}$, for $s = s_1 s_3$ we have $s^p = pr(1 - s_2)(1 + s_2 + \dots + s_2^{N-1}) = pr(1 - s_2^N) \equiv pr \pmod{p^2}$. \square

- (x) + (xvii) \Rightarrow (ii)

Proof. We just saw that (x) + (xvii) \Rightarrow (xv), and we also know that (xv) \Rightarrow (viii). We will thus use (viii) freely below.

We prove that $F : W_{p^n}(R) \rightarrow W_{p^{n-1}}(R)$ is surjective for all $n \geq 1$ using induction on n , beginning with the case $n = 1$. This base case is exactly (x)', which (x) implies. Hence we may assume the result has been proven for some fixed $n - 1$, and we wish to deduce it for n . To this end, pick an arbitrary element $\underline{y} \in W_{p^n}(R)$. Consider the following diagram

$$\begin{array}{ccc} & \underline{y} \in W_{p^n}(R) & \\ & \downarrow \text{res} & \\ W_{p^n}(R) \ni \underline{s} & \xrightarrow{F} & \underline{y}|_{W_{p^{n-1}}(R)}. \end{array}$$

The term \underline{s} exists by our inductive hypothesis. Because the restriction maps are surjective and commute with F , we may expand this to a commutative diagram

$$\begin{array}{ccccc} W_{p^{n+1}}(R) \ni \underline{r} & \xrightarrow{F} & \underline{y}' \in W_{p^n}(R) & & \underline{y} \in W_{p^n}(R) \\ & \searrow \text{res} & \searrow \text{res} & & \downarrow \text{res} \\ & & W_{p^n}(R) \ni \underline{s} & \xrightarrow{F} & \underline{y}|_{W_{p^{n-1}}(R)}. \end{array}$$

If we had $\underline{y} = \underline{y}'$, we would be done.

Find $\underline{x}' \in W_{p^{n+1}}(R)$ with $F(\underline{x}') = V^n([1])$ using (viii). Then find $\underline{x}'' \in W_{p^{n+1}}(R)$ with $\underline{y} - \underline{y}' = V^n(F^{n+1}(\underline{x}''))$ using (x). Then we compute

$$\begin{aligned} F(\underline{x} + \underline{x}'\underline{x}'') &= \underline{y}' + V^n([1])F(\underline{x}'') \\ &= \underline{y}' + V^n(F^{n+1}(\underline{x}'')) \\ &= \underline{y}' + \underline{y} - \underline{y}' \\ &= \underline{y}, \end{aligned}$$

as desired. \square

- $(xiv)' \Rightarrow (x) + (xvii)$

Proof. We trivially have that $(xiv)' \Rightarrow (xvii) + (xviii)$. Now we are done because $(xviii) \Rightarrow (x)$. \square

- $(xiv) \Rightarrow (xv)$

Proof. We have already shown all of the implications $(xiv) \Rightarrow (xiv)' \Rightarrow (x) + (xvii) \Rightarrow (xv)$. \square

- $(ii)' \Rightarrow (ii); (vi) \Rightarrow (ii); (vi)' \Rightarrow (vi); (xiv) \Rightarrow (vi); (xiv)' \Rightarrow (xiv)$

Proof. We will prove that all six conditions appearing in the statement are equivalent. We have already proven the following implications:

$$\begin{array}{ccccc} (ii) & \longrightarrow & (vi) & \longrightarrow & (xiv) \\ \downarrow & & \downarrow & & \downarrow \\ (ii)' & \longrightarrow & (vi)' & \longrightarrow & (xiv)' \end{array}$$

Thus, it suffices to prove that $(xiv)'$ implies (ii). This follows because we have seen above that $(xiv)' \Rightarrow (x) + (xvii) \Rightarrow (ii)$. \square

5. VALUATION RINGS

Throughout this section, we assume that R is a valuation ring with valuation v , in which p is nonzero. In several cases, we also assume that v is archimedean (i.e., the value group is isomorphic to a subgroup of \mathbb{R}). This includes a number of the examples considered in Section 6.

Remark 5.1. *Suppose that $v(p)$ is p -divisible (in the value group of v). Then for each nonnegative integer n , the ideal I_n is the principal ideal generated by any $x \in R$ such that $v(x) = \left(\frac{1}{p} + \dots + \frac{1}{p^n}\right)v(p)$. If in addition v is archimedean and there exists $y \in R$ such that $v(y) = \frac{1}{p-1}v(p)$, then I_∞ is the principal ideal generated by y .*

Remark 5.2. *Condition (xii) holds whenever v is archimedean, $v(p)$ is p -divisible (so the I_n are as computed in Remark 5.1), and R is spherically complete (i.e., any decreasing sequence of balls in R has nonempty intersection). The spherically complete condition is in practice quite rare; for instance, an infinite algebraic extension of \mathbb{Q}_p which is not discretely valued is never spherically complete. As a result, (xii) is also rather rare, as then is (i); see Example 6.4.*

Remark 5.3. *Condition (ii) implies (xviii) (the Frobenius homomorphism on R/pR is surjective) and that there exists an element $x \in R$ with $0 < v(x) < v(p)$ (e.g., by (xvi)). The converse is also true, as follows. By (xviii), there exist $y, z \in R$*

with $y^p \equiv x \pmod{p}$, $z^p \equiv p/x \pmod{pR}$. Since $0 < v(x), v(p/x) < v(p)$, we have $v(y) = \frac{1}{p}v(x)$, $v(z) = \frac{1}{p}(v(p) - v(x))$, so $v(yz) = \frac{1}{p}$. Therefore, $u := (yz)^p/p$ is a unit in R . By (xviii) again, there exists $v \in R$ such that $v^p \equiv -u^{-1} \pmod{pR}$. Thus we have $pv^p \equiv -p \pmod{p^2R}$. Thus $(yzv)^p \equiv -p \pmod{p^2R}$. This implies (xvi), which together with (xviii) implies (ii). As a byproduct of the argument, we note that (ii) implies that $v(p)$ is p -divisible.

Remark 5.4. For valuation rings, (xv) implies (ii), and so the two conditions become equivalent. To see this, note that if R satisfies (xv), we can find r_1 such that $r_1^p \equiv -p \pmod{p^2R}$, and in particular, $r_1^p = -pu$ for some unit $u \in R$. By (xv) again, for any $x \in R$ we may find $r_2 \in R$ with $r_2^p = -pxu + p^2y$, with $y \in R$ and u as above. Since $pv(r_1) = v(-p) \leq v(-px) = pv(r_2)$, we have that r_2/r_1 is an element of R . We then compute $\left(\frac{r_2}{r_1}\right)^p = \frac{-pxu+p^2y}{-pu} = x - pu^{-1}y \equiv x \pmod{p}$. Hence (xviii) holds; since (xv) also implies (xvii), we may deduce (ii) as desired.

Remark 5.5. If R satisfies condition (ii), then it satisfies almost purity; see Section 7. This implies that if S is the integral closure of R in a finite extension of $\text{Frac}(R)$, then the maximal ideal of S surjects onto the maximal ideal of R under the trace map. In other words, R is deeply ramified in the sense of Coates and Greenberg [1].

6. EXAMPLES

We now describe some simple examples realizing distinct subsets of the conditions considered above.

Example 6.1. Take R to be any ring in which p is invertible. Then by Theorem 4.2, all of our conditions hold.

Example 6.2. Take $R = \mathbb{Z}$. We begin by checking that $I_i = (p)$ for all $i \geq 1$, by induction on i . It is clear that $I_1 = \{r \in \mathbb{Z} \mid r^p \in (p)\} = (p)$ because $(p) \subseteq \mathbb{Z}$ is a prime ideal. Next, assume that $I_{i-1} = (p)$. Then $I_i = \{r \in \mathbb{Z} \mid r^p \in (p^2)\} = (p)$ also.

From the previous paragraph, we see that (xvii) fails: it would require that we find $r \in \mathbb{Z}$ such that $r^p \equiv -p \pmod{p^2}$, and this is impossible. Consequently, neither (i) nor (ii) holds for $R = \mathbb{Z}$.

On the other hand, (xii) does hold for $R = \mathbb{Z}$. To see this, we must show that any descending chain of balls $\cdots \supseteq B(r_{i-1}, (p)) \supseteq B(r_i, (p)) \supseteq \cdots$ has nonempty intersection. But here containment is enough to imply $B(r_{i-1}, (p)) = B(r_i, (p))$, and so the intersection is certainly nonempty.

Example 6.3. Take $R = \mathbb{F}_p[T]$. In this case, (xv) is satisfied trivially, because $pr = 0$ for all $r \in R$. On the other hand, (xviii) is not satisfied, because there is no p -th root of T in R .

Example 6.4. Take $R = \mathcal{O}_{\mathbb{C}_p}$. It is clear that (xiii) holds (because $\mathcal{O}_{\mathbb{C}_p}$ is integrally closed in the algebraically closed field \mathbb{C}_p), which implies that $\mathcal{O}_{\mathbb{C}_p}$ satisfies (iv), (v), (vi), (vii), (viii), (ix), (x), (xiii), (xiv), (xv), (xvi), (xvii), (xviii). On the other hand, (xii) does not hold by Lemma 6.5, which implies that $\mathcal{O}_{\mathbb{C}_p}$ does not satisfy (i), (iii), (xi), (xii).

Lemma 6.5. The ring $R = \mathcal{O}_{\mathbb{C}_p}$ does not satisfy (xii).

Proof. By Remark 5.1, for n a nonnegative integer, I_n is the principal ideal generated by $p^{\frac{1}{p} + \dots + \frac{1}{p^n}}$, while I_∞ is the principal ideal generated by $p^{\frac{1}{p-1}}$. Each ball $B(r, I_\infty)$ contains an element which is algebraic over \mathbb{Q} , since such elements are dense in \mathbb{C}_p by Krasner's lemma. Furthermore, if two balls $B(r, I_\infty)$ and $B(r', I_\infty)$ intersect, they are in fact equal. Therefore, there are only countably many such balls. On the other hand, one can construct uncountably many decreasing sequences $B(r_0, I_0) \supseteq B(r_1, I_1) \supseteq \dots$ no two of which have the same intersection. For instance, take x_0, x_1, \dots to be Teichmüller elements in $W(\mathbb{F}_p) \subseteq \mathcal{O}_{\mathbb{C}_p}$, and put

$$r_0 = x_0, r_1 = r_0 + x_1 p^{\frac{1}{p}}, r_2 = r_1 + x_2 p^{\frac{1}{p} + \frac{1}{p^2}}, \dots$$

Then any two of the resulting intersections $\bigcap_{i=0}^\infty B(r_i, I_i)$ are disjoint. \square

Remark 6.6. *It is possible to give a more constructive proof of Lemma 6.5 using the explicit description of $\mathcal{O}_{\mathbb{C}_p}$ given in [6].*

Example 6.7. *Let R denote the spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ constructed by Poonen in [10]. We will show that R satisfies (i), and thus satisfies all of the labeled conditions except for (xi).*

We first recall the explicit construction of R . For an arbitrary ring S , let $S[[t^{\mathbb{Q}}]]$ denote the ring of generalized power series over S ; the elements of this ring are the formal sums $\sum_{i \in \mathbb{Q}, i \geq 0} c_i t^i$ with $c_i \in S$ such that the set $\{i \in \mathbb{Q} : c_i \neq 0\}$ is well-ordered. This ring is spherically complete for the t -adic valuation: given any sequence $i_0 \leq i_1 \leq \dots$ of nonnegative rationals and any $x_0, x_1, \dots \in S[[t^{\mathbb{Q}}]]$ such that $x_j - x_{j+1}$ is divisible by t^{i_j} , we can find $x \in S[[t^{\mathbb{Q}}]]$ congruent to x_j modulo t^{i_j} for each $j \geq 0$. Explicitly, we take the coefficient of t^k in x to be equal to the coefficient of t^k in x_j if there exists $j \geq 0$ for which $k \leq i_j$ for some j , and 0 otherwise.

In this notation, Poonen's spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ is the ring $\mathbb{Z}_p[[t^{\mathbb{Q}}]]/(t-p)$. In particular, $R/(p) \cong \mathbb{F}_p[[t^{\mathbb{Q}}]]/(t)$. From this description, it is clear that R satisfies (xii) because $\mathbb{F}_p[[t^{\mathbb{Q}}]]$ is spherically complete. Similarly, it is clear that R satisfies (xviii). Finally, since R is a valuation ring and there exists $x \in R$ for which $0 < v(x) < v(p)$ (e.g., the image of $t^{1/p}$), Remark 5.3 implies that R satisfies (ii). Putting this together, we deduce that R satisfies (i).

Example 6.8. *Take $R = \mathbb{Z}[\mu_{p^2}]$, where μ_{p^2} is a primitive (p^2) -nd root of unity. Condition (v) holds because the element $\underline{x} = \sum_{i=0}^{p-1} [\mu_{p^2}^i] \in W(R)$ satisfies $F(\underline{x}) = V(1)$. (Since R is p -torsion-free, this last equality can be checked at the ghost component level, where it is apparent.) On the other hand, (xviii) does not hold: the element $(1 - \omega_{p^2})$ has p -adic valuation $\frac{1}{p(p-1)}$, but there is no element of R which has p -adic valuation $\frac{1}{p^2(p-1)}$. A similar argument shows that (xv) does not hold: if it did, then since $\mathbb{Z}[\mu_{p^2}]$ has an element of valuation $\frac{1}{p}$, it would also be forced to have an element of valuation $\frac{1}{p} + \frac{1}{p^2}$, a contradiction.*

Example 6.9. *Take $R = \mathbb{Z}[\mu_{p^\infty}]$, i.e., the ring of integers in the maximal abelian extension of \mathbb{Q} . We will see that (ii) holds but (iv) does not. (The same analysis applies to $\mathbb{Z}_p[\mu_{p^\infty}]$ or its p -adic completion.)*

Note that R satisfies (v) because R contains the subring $\mathbb{Z}[\mu_{p^2}]$ which satisfies (v) (see Example 6.8). Thus to establish (ii), it is sufficient to check condition (xviii). (One can also make this reduction by replacing R by its completion, which

is a valuation ring, then using Remark 5.3.) To verify (xviii), note that for any expression $a_1\mu_{p^{i_1}} + \cdots + a_n\mu_{p^{i_n}}$ with $a_1, \dots, a_n \in \mathbb{Z}$, we have $a_1\mu_{p^{i_1}} + \cdots + a_n\mu_{p^{i_n}} \equiv (a_1\mu_{p^{i_1+1}} + \cdots + a_n\mu_{p^{i_n+1}})^p \pmod{p}$.

To establish that R does not satisfy (iv), we will instead check that R does not satisfy the equivalent condition (xiii). We first do this for $p > 2$ by checking that the congruence $x^p \equiv 1 - p \pmod{pI_\infty}$ has no solution. Recall that by Remark 5.1, I_n is the principal ideal generated by p^k for $k = \sum_{i=0}^n \frac{1}{p^k}$.

Assume by way of contradiction that there exists $x \in R$ for which $x^p - 1 + p \in pI_\infty$. Choose an integer $n \geq 2$ for which $x \in \mathbb{Z}[\mu_{p^n}]$. The unique prime ideal of $\mathbb{Z}[\mu_{p^n}]$ lying above (p) is generated by $1 - \mu_{p^n}$ and has residue field \mathbb{F}_p ; we must therefore have $x \equiv 1 \pmod{(1 - \mu_{p^n})}$. Modulo p , we have $1 - p \equiv x^p \equiv 1 + (1 - x)^p$, so $1 - x$ must have p -adic valuation at least $\frac{1}{p}$. Since the p -adic valuation of $1 - \mu_{p^n}$ is $\frac{1}{p^{n-1}(p-1)}$ (e.g., by Lemma 6.10 below), we must have $x \equiv 1 \pmod{(1 - \mu_{p^n})^{p^{n-1}-p^{n-2}}}$. We can thus find $y_i \in \mathbb{Z}$ for which

$$x \equiv 1 + \sum_{i=p^{n-1}-p^{n-2}}^{p^{n-1}-1} y_i(1 - \mu_{p^n})^i \pmod{(1 - \mu_{p^n})^{p^{n-1}}}.$$

Raising both sides to the p -th power, our original congruence now implies

$$1 - p \equiv 1 + \sum_{i=p^{n-1}-p^{n-2}}^{p^{n-1}-1} y_i^p(1 - \mu_{p^n})^{pi} + p \sum_{i=p^{n-1}-p^{n-2}}^{p^{n-1}-1} y_i(1 - \mu_{p^n})^i \pmod{(1 - \mu_{p^n})^{p^n}}.$$

By Lemma 6.10 below, we can rewrite this congruence as

$$-1 \equiv - \sum_{i=p^{n-1}-p^{n-2}}^{p^{n-1}-1} y_i^p(1 - \mu_{p^n})^{pi-p^n+p^{n-1}} + \sum_{i=p^{n-1}-p^{n-2}}^{p^{n-1}-1} y_i(1 - \mu_{p^n})^i \pmod{(1 - \mu_{p^n})^{p^{n-1}}}.$$

On one hand, this clearly implies $y_{p^{n-1}-p^{n-2}}^p \equiv 1 \pmod{(1 - \mu_{p^n})}$, and hence $y_{p^{n-1}-p^{n-2}} \equiv 1 \pmod{p}$, since $y_{p^{n-1}-p^{n-2}} \in \mathbb{Z}$. On the other hand, as an equality in the ring $\mathbb{Z}[\mu_{p^n}]/((1 - \mu_{p^n})^{p^{n-1}}) \cong \mathbb{F}_p[\mu_{p^n}]/((1 - \mu_{p^n})^{p^{n-1}})$, it implies that

$$\begin{aligned} y_i &\equiv y_{i/p+p^{n-1}-p^{n-2}}^p & (p^{n-1} - p^{n-2} \leq i \leq p^{n-1} - 1, i \equiv 0 \pmod{p}) \\ y_i &\equiv 0 & (p^{n-1} - p^{n-2} \leq i \leq p^{n-1} - 1, i \not\equiv 0 \pmod{p}). \end{aligned}$$

By the second congruence, $y_{p^{n-1}-1} \equiv 0 \pmod{p}$. By the first congruence applied repeatedly, $y_{p^{n-1}-p}, y_{p^{n-1}-p^2}, \dots, y_{p^{n-1}-p^{n-2}}$ are also forced to be zero modulo p . This yields a contradiction.

For $p = 2$, the above argument cannot apply because $1 - p = -1$ is the square of $i := \mu_4$. However, a similar but somewhat more complicated argument shows that the congruence $x^p \equiv i + 2\mu_8 \pmod{pI_\infty}$ has no solution. We leave the details to the reader.

Lemma 6.10. For p an odd prime, n a positive integer, and μ_{p^n} a primitive p^n -th root of unity, in $\mathbb{Z}[\mu_{p^n}]$ we have $(1 - \mu_{p^n})^{p^n - p^{n-1}} \equiv -p \pmod{(1 - \mu_{p^n})^{p^n}}$.

Proof. Let $\Phi(T) = \sum_{i=0}^{p-1} T^{ip^{n-1}}$ denote the p^n -th cyclotomic polynomial, so that we may identify $\mathbb{Z}[\mu_{p^n}]$ with $\mathbb{Z}[T]/(\Phi(1 - T))$ by identifying μ_{p^n} with $1 - T$. Note

that

$$\Phi(1-T) \equiv \sum_{i=0}^{p-1} (1-T^{p^{n-1}})^i \equiv \frac{1-(1-T^{p^{n-1}})^p}{T^{p^{n-1}}} \equiv \frac{1-(1-T^{p^n})}{T^{p^{n-1}}} \pmod{p};$$

that is, the coefficients of the polynomial $T^{p^n - p^{n-1}} - \Phi(1-T)$ are all divisible by p . Since the constant term of this polynomial is $-\Phi(1) = -p$, we need only check that the coefficient of T^j in $\Phi(1-T)$ is divisible by p^2 for $j = 1, \dots, p^{n-1} - 1$. Write this coefficient as $\sum_{i=0}^{p-1} (-1)^j \binom{ip^{n-1}}{j}$. For j not divisible by p^{n-2} , Kummer's criterion implies that each $\binom{ip^{n-1}}{j}$ is divisible by p^2 . For $j = kp^{n-2}$ with $k \in \{1, \dots, p-1\}$, we may write $\binom{ip^{n-1}}{kp^{n-2}} = \frac{ik}{p} \binom{ip^{n-1}-1}{kp^{n-2}-1}$ and then invoke Lucas's criterion to deduce that $\binom{ip^{n-1}-1}{kp^{n-2}-1} \cong \binom{p-1}{k-1} \pmod{p}$. Therefore, $\sum_{i=0}^{p-1} (-1)^j \binom{ip^{n-1}}{j} \equiv (-1)^j \binom{p}{k} \sum_{i=0}^{p-1} i \equiv 0 \pmod{p^2}$, as desired. \square

7. ALMOST PURITY

We conclude by giving one motivation for studying condition (ii): it provides a natural context for the concept of *almost purity*, as introduced by Faltings and studied more recently by the second author and Liu in [7] and by Scholze in [11]. We begin by giving meaning to the adjective *almost*; see [2] for the definitions in a more general setting.

Definition 7.1. *Let R be a p -torsion-free ring which is integrally closed in $R_p := R[p^{-1}]$ and which satisfies condition (ii). A p -ideal of R is an ideal I of R such that $I^n \subseteq (p)$ for some positive integer n .*

An R -module M is almost zero if $IM = 0$ for every p -ideal I of R . A morphism of R -modules is almost injective/surjective if its kernel/cokernel is almost zero, and almost bijective (or an almost isomorphism) if it is both almost injective and almost surjective.

Theorem 7.2. *Let R be a p -torsion-free ring which is integrally closed in $R_p := R[p^{-1}]$ and which satisfies condition (ii). Let S_p be a finite étale R_p -algebra, let S_0 be the integral closure of R in S_p , and let S be any R -subalgebra of S_0 such that S/S_0 is an almost zero R -module. Then S also satisfies condition (ii).*

Proof. For each $t \in \mathbb{Q}$, choose integers $r, s \in \mathbb{Z}$, $s > 0$, and $r/s = t$. Since R is integrally closed in R_p , the set

$$R_t := \{x \in R[p^{-1}] : p^{-r}x^s \in R\}$$

depends only on t . The function $v : R_p \rightarrow (-\infty, +\infty]$ given by

$$v(x) := \sup\{t \in \mathbb{Q} : x \in R_t\}$$

satisfies $v(x-y) \geq \min\{v(x), v(y)\}$, $v(xy) \geq v(x) + v(y)$, and $v(x^2) = 2v(x)$.

Let A be the separated completion of R_p under the norm $|\cdot| = e^{-v(\cdot)}$, and define the subring $\mathfrak{o}_A = \{x \in A : |x| \leq 1\}$ and the ideal $\mathfrak{m}_A = \{x \in A : |x| < 1\}$. Let $\psi : R_p \rightarrow A$ be the natural homomorphism; then $\psi^{-1}(\mathfrak{o}_A)$ contains R but may be larger. However, we do have $\psi^{-1}(\mathfrak{m}_A) \subset R$.

Since (ii) implies (xviii) and (xv), we can choose $x_1, x_2 \in R$ with

$$x_1^p \equiv -p \pmod{p^2 R}, \quad x_2^p \equiv x_1 \pmod{pR}.$$

Then $\psi(x_1), \psi(x_2)$ are units in A , and for all $y \in A$,

$$|\psi(x_1)y| = p^{-1/p}|y|, \quad |\psi(x_2)y| = p^{-1/p^2}|y|.$$

Given $\bar{y} \in \mathfrak{o}_A/(p)$, choose $y \in R[p^{-1}]$ so that $\psi(y)$ lifts \bar{y} . Then $x_2^p y \in \psi^{-1}(\mathfrak{m}_A) \subset R$, so since R satisfies (ii), we can find $z \in R$ with $x_2^p y \equiv z^p \pmod{pR}$. The element $\psi(z/x_2) \in \mathfrak{o}_A$ has the property that $\psi(z/x_2)^p \equiv \psi(y) \pmod{(p/\psi(x_2)^p)\mathfrak{o}_A}$; it follows that Frobenius is surjective on $\mathfrak{o}_A/(\psi(x_1)^{p-1})$. This implies that Frobenius is also surjective on \mathfrak{o}_A : given $y \in \mathfrak{o}_A$, we can first find $z_0, y_1 \in \mathfrak{o}_A$ with $y = z_0^p + \psi(x_1)^{p-1}y_1$, then find $z_1, y_2 \in \mathfrak{o}_A$ with $y_1 = z_1^p + \psi(x_1)^{p-1}y_2$, and then $z := z_0 + \psi(x_2)^{p-1}z_1$ will have the property that $z^p \equiv y \pmod{p\mathfrak{o}_A}$. That is, \mathfrak{o}_A also satisfies (xviii); since (xvi) is evident (using x_1), \mathfrak{o}_A satisfies (ii).

Put $B = A \otimes_R S$, and extend ψ by linearity to a homomorphism $\psi : S_p \rightarrow B$. By [7, Theorem 3.6.12], there is a unique power-multiplicative norm on B under which it is a finite Banach A -module, and for this norm the subring $\mathfrak{o}_B = \{x \in B : |x| \leq 1\}$ also satisfies (ii). As in [7, Remark 2.3.14], for $\mathfrak{m}_B = \{x \in B : |x| < 1\}$, we have $\psi^{-1}(\mathfrak{m}_B) \subset S$.

Given $\bar{y} \in S/(p)$, choose a lift $y \in S$ of \bar{y} . Since B satisfies (ii) and $\psi(B[p^{-1}])$ is dense in S , we can find $z \in \psi^{-1}(\mathfrak{o}_B)$ for which $u := z^p - y$ satisfies $|\psi(u)| \leq p^{-1}$. In particular, $u \in \psi^{-1}(\mathfrak{m}_B) \subset S$; moreover, we may write $x_1^p = -p + p^2w$ for some $w \in R$ and then write

$$u = p(u/p) = (-x_1^p + p^2w)(u/p) = -x_1(x_1^{p-1}u/p) + puw.$$

The quantity $x_1^{p-1}u/p$ again belongs to $\psi^{-1}(\mathfrak{m}_B) \subset S$, so $u \in (x_1, p)S$. Therefore Frobenius is surjective on $S/(x_1, p)$; by arguing as before (using the fact that $x_2^p \equiv x_1 \pmod{pR}$), we deduce that Frobenius is surjective on $S/(x_1^i, p)$ for $i = 2, \dots, p$. Therefore, S satisfies (xviii); since (xvi) is again evident, S satisfies (ii) as desired. \square

Corollary 7.3. *For R and S as in Theorem 7.2, $\Omega_{S/R} = 0$.*

Proof. Since $S[p^{-1}]$ is finite étale over $R[p^{-1}]$, $\Omega_{S/R}$ is killed by p^n for some non-negative integer n . If $n > 0$, then for each $x \in S$ we may apply Theorem 7.2 to write $x = y^p + pz$. Then $dx = py^{p-1}dy + pdz$ is also killed by p^{n-1} . By induction, it follows that we may take $n = 0$, proving the claim. \square

Remark 7.4. *Note that the proof of Theorem 7.2 involves the facts that $\psi(R)$ and \mathfrak{o}_A are almost isomorphic (using \mathfrak{o}_A to define almost), as are $\psi(S)$ and \mathfrak{o}_B . Also, Theorem 7.2 can be applied with $S_p = R_p$, to show that any R -subalgebra R' of R for which R/R' is almost zero also satisfies (ii).*

To refine Theorem 7.2 to an *almost purity theorem*, one must establish that S is an *almost finite projective R -module* and an *almost finite étale R -algebra*. These are the properties asserted in the following theorem; see [2] for a more thorough discussion of these concepts.

Theorem 7.5. *Take R and S as in Theorem 7.2.*

- (a) *For any p -ideal I of R , there exist a finite free R -module F and R -module homomorphisms $S \rightarrow F \rightarrow S$ whose composition is multiplication by some $t \in R$ for which $I \subseteq (t)$.*
- (b) *The image of S under the trace pairing map $S_p \rightarrow \text{Hom}_{R_p}(S_p, R_p)$ is almost equal to the image of the natural map from $\text{Hom}_R(S, R)$ to $\text{Hom}_{R_p}(S_p, R_p)$.*

Proof. These again reduce to the corresponding statements about \mathfrak{o}_A and \mathfrak{o}_B , for which see [7, Theorem 5.5.9] or the corresponding statement in [11]. \square

ACKNOWLEDGEMENTS

The authors thank Laurent Berger, James Borger, Lars Hesselholt, Abhinav Kumar, Ruochuan Liu, Joe Rabinoff, and Liang Xiao for helpful discussions and suggestions.

REFERENCES

- [1] J. Coates and R. Greenberg. Kummer theory for abelian varieties over local fields. *Invent. Math.*, 124(1-3):129–174, 1996.
- [2] Ofer Gabber and Lorenzo Ramero. *Almost ring theory*, volume 1800 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 2003.
- [3] Lars Hesselholt. On the topological cyclic homology of the algebraic closure of a local field. In *An alpine anthology of homotopy theory*, volume 399 of *Contemp. Math.*, pages 133–162. Amer. Math. Soc., Providence, RI, 2006.
- [4] Lars Hesselholt and Ib Madsen. The de Rham-Witt complex in mixed characteristic. *Annales scientifiques de l’Ecole Normale Supérieure*, 37(4):1–43, 2004.
- [5] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Annales scientifiques de l’Ecole Normale Supérieure*, 12(4):501–661, 1979.
- [6] Kiran S. Kedlaya. Power series and p -adic algebraic closures. *Journal of Number Theory*, 89(2):324–339, 2001.
- [7] Kiran S. Kedlaya and Ruochuan Liu. Relative p -adic Hodge theory, I: Foundations. 2011. <http://math.mit.edu/~kedlaya/papers/>.
- [8] Andreas Langer and Thomas Zink. De Rham-Witt cohomology for a proper and smooth morphism. *J. Inst. Math. Jussieu*, 3(2):231–314, 2004.
- [9] Andreas Langer and Thomas Zink. Gauss-Manin connection via Witt-differentials. *Nagoya Math. J.*, 179:1–16, 2005.
- [10] Bjorn Poonen. Maximally complete fields. *Enseign. Math. (2)*, 39(1-2):87–106, 1993.
- [11] Peter Scholze. Perfectoid spaces, II: p -adic Hodge theory. 2011. In preparation.

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`

UNIVERSITY OF CALIFORNIA, SAN DIEGO, DEPT OF MATHEMATICS, LA JOLLA, CA 92093
E-mail address: `kedlaya@ucsd.edu`