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 many equivalent conditions to surjectivity of the Frobenus map on both finite and infinite length Witt vectors. In particular, surjectivity on finite Witt vectors turns out to be stable under certain integral extensions; this provides a clean formulation of a strong generalization of Faltings's almost purity theorem from p-adic Hodge theory, incorporating recent improvements by Kedlaya–Liu and by Scholze.

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 $W(R)$, and an endomorphism F of $W(R)$ called the *Frobenius endomorphism*. The ring $W(R)$ is set-theoretically an infinite product of copies of R, but with an exotic ring structure when p is not a unit in R; 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 $R = \mathbb{F}_p$, $W(R) = \mathbb{Z}_p$.

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; it is easy 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 the valuation subring of a spherical completion of $\overline{\mathbb{Q}_p}$.

While surjectivity of Frobenius on full Witt vectors is rather rare, some weaker conditions turn out to be more relevant to applications. For instance, one can view the full ring of Witt vectors as an inverse limit of finite-length truncations, and surjectivity of Frobenius on finite levels is satisfied quite often. 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 extension). In fact, this condition can be used to give a purely ring-theoretic formulation of a very strong generalization of Faltings's *almost purity theorem* [2]. The theorem of Faltings features prominently in the theory of comparison isomorphisms in p-adic Hodge

Date: October 1, 2012.

2010 *Mathematics Subject Classification.* Primary 13F35.

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, Green professorship), UCSD (Warschawski professorship).

theory; the generalization in question emerged recently from work of the second author and Liu [9] and of Scholze [11].

One principal motivation for studying 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. Witt vectors

Throughout this section, let R denote an arbitrary commutative ring. For more details on the construction of p-typical Witt vectors, see [7, Section 0.1] or [5, Section 17]; the latter treats big Witt vectors as well as p-typical Witt vectors.

Definition 1.1. For each nonnegative integer n, the ring $W_{p^n}(R)$ is defined to have underlying set $W_{p^n}(R) := R^{n+1}$ with an exotic ring structure characterized by functoriality in R and the property that for $i = 0, \dots, n$, the p^i-th *ghost component map* $w_{p^i} : W_{p^n}(R) \to R$ defined by

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

is a ring homomorphism. These rings carry *Frobenius homomorphisms*

$$F : W_{p^{n+1}}(R) \to W_{p^n}(R),$$

again functorial in R, such that for $i = 0, \dots, n$, we have $w_{p^i} \circ F = w_{p^{i+1}}$. Moreover, there are additive *Verschiebung* maps $V : W_{p^n}(R) \to W_{p^{n+1}}(R)$ defined by the formula $V(r_1, \dots, r_{p^n}) = (0, r_1, \dots, r_{p^n})$.

There is a natural restriction map $W_{p^{n+1}}(R) \to W_{p^n}(R)$ 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 $F : W(R) \to W(R)$; there is also a collated Verschiebung map $V : W(R) \to W(R)$. The ghost component maps also collate to define a ghost map: $w : W(R) \to R^{\mathbb{N}}$. 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 $[r]$. These elements are multiplicative: for all $r_1, r_2 \in R$, $[r_1 r_2] = [r_1][r_2]$.

We will need the following properties of Witt vectors for R arbitrary (not necessarily of characteristic p). See [6, Lemma 1.5]. Here and in what follows, we write $\underline{x}$ for a Witt vector with components $x_1, x_p, \dots$.

(a) For $r \in R$, $F([r]) = [r^p]$.
(b) For $\underline{x} \in W_{p^n}(R)$, $(F \circ V)(\underline{x}) = p\underline{x}$.
(c) For $\underline{x} \in W_{p^n}(R)$ and $\underline{y} \in W_{p^{n+1}}(R)$, $V(\underline{x}F(\underline{y})) = V(\underline{x})\underline{y}$.
(d) For $\underline{x} \in W_{p^n}(R)$, $\underline{x} = \sum_{i=0}^n V^i([x_{p^i}])$.

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 many variables over $\mathbb{Z}$, form Witt vectors whose components are distinct variables, then verify the desired identities at the level of ghost components. This suffices because R is now p-torsion-free, so the ghost map is injective.

We will need a couple of other p-divisibility properties. We first prove the following lemma.

Lemma 1.3. *In $W(\mathbb{Z}/p^2\mathbb{Z})$, we have*

$$p = (p, (-1)^{p-1}, 0, 0, \dots) = [p] + V([(-1)^{p-1}]).$$

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 $p = 2$. We now 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 we have $x_p \equiv (-1)^{p-1} \pmod{p^{p-1}}$ and so $x_p^p \equiv 1 \pmod{p^3}$ (we treat $p = 2$ and $p > 2$ separately). 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 $i + 2p^{n-i} \geq i + 2(n-i+1) \geq n+2$. □

Lemma 1.4. *Take $\underline{x}, \underline{y} \in W(R)$ with $F(\underline{x}) = \underline{y}$.*

- *(a) For each nonnegative integer i, we have $y_{p^i} = x_{p^i}^p + p x_{p^{i+1}} + p f_{p^i}(x_1, \dots, x_{p^i})$ where f_{p^i} is a certain universal polynomial with coefficients in $\mathbb{Z}$ which is homogeneous of degree p^{i+1} for the weighting in which x_{p^j} has weight p^j.*
- *(b) For $i \geq 1$, the coefficient of $x_1^{p^{i+1}}$ in f_{p^i} equals 0.*
- *(c) For $i \geq 2$, the coefficient of $x_p^{p^i}$ in f_{p^i} is divisible by p.*
- *(d) The coefficient of x_p^p in f_p equals $-p^{p-2}$ modulo p.*
- *(e) For $p = 2$ and $i \geq 2$, f_{2^i} belongs to the ideal generated by the elements $2, x_1, x_2^2 - x_4, x_8, \dots, x_{2^i}$.*

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. This polynomial is congruent to $x_{p^i}^p$ modulo p by [7, (1.3.5)]. Each of the remaining assertions concerns a particular coefficient of this polynomial, and so may be checked after setting all other variables to 0. To finish checking (a), we must check that f_{p^i} does not depend on $x_{p^{i+1}}$. We assume $x_1 = \cdots = x_{p^i} = 0$, so that $\underline{x} = V^{i+1}([x_{p^{i+1}}])$; then $F(\underline{x}) = pV^i([x_{p^{i+1}}]) = (0, \dots, 0, p x_{p^{i+1}})$.

To check (b), we may assume that $x_p = x_{p^2} = \cdots = x_{p^i} = 0$, so that $\underline{x} = [x_1]$. In this case, $F(\underline{x}) = [x_1^p]$, so the claim follows. To check (c), we may assume that $x_1 = x_{p^2} = x_{p^3} = \cdots = x_{p^i} = 0$, so that $\underline{x} = V([x_p])$. In this case, the claim is that $y_{p^i} \equiv 0 \pmod{p^2}$ for $i \geq 2$. Since $F(\underline{x}) = p[x_p]$, by homogeneity it is sufficient to check the claim for $x_p = 1$. In this case, it follows from Lemma 1.3. We may similarly check (d).

To check (e), we may assume that $x_1 = x_8 = x_{16} = \cdots = 0$, and so we have $\underline{x} = V([x_2]) + V^2([x_4])$. By homogeneity, it is sufficient to check the claim in the case $x_2 = x_4 = 1$. In $W(\mathbb{Z})$, we have $V(1) = 1 + [-1]$ by computation of ghost components, so $1 + V(1) = 2 + [-1]$. In $W(\mathbb{Z}/4\mathbb{Z})$, by Lemma 1.3 we have

$$F(\underline{x}) = 2 + 2V(1) = [2] + V([-1]) + 2V(1) = [2] + V([-1] + 2) = [2] + V(1) + V^2(1).$$

This implies the desired result. □

Remark 1.5. Suppose R is a ring in which $p = 0$, and let $\varphi : R \to R$ denote the Frobenius homomorphism on R. Then applying Lemma 1.4, 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, 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.

2. The kernel of Frobenius

When R is a ring not of characteristic p, then $F : W(R) \to W(R)$ cannot be injective; for instance, the Cartier-Dieudonné-Dwork lemma [5, Lemma 17.6.1] implies that $p, 0, 0, \dots$ arises as the sequence of ghost components of some element of $W(\mathbb{Z})$. More generally, one can 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.

Definition 2.1. Given a ring R, define sets $I_0 := R$ and $I_i := \{r \in R \mid r^p \in pI_{i-1}\}$ for $i > 0$; it is apparent that $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots$. We will see below that each I_i is an ideal. Also define $I_\infty = \cap_{i=1}^\infty I_i$, so that $I_\infty = \{r \in R \mid r^p \in pI_i \text{ for all } i \geq 1\}$.

Lemma 2.2. *For each $i \geq 0$, the set I_i defined above is an ideal.*

Proof. We proceed by induction on i, the case $i = 0$ being obvious. Given that I_{i-1} is an ideal, it is clear that I_i is closed under multiplication by arbitrary elements of R. It remains to show that if $x, y \in I_i$, then $x+y \in I_i$. Using the definition, we must check that $x^p + px^{p-1}y + \cdots + pxy^{p-1} + y^p \in pI_{i-1}$. 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 $x, y \in I_i \subseteq I_{i-1}$. □

Remark 2.3. Suppose that R is a valuation ring with valuation v, p is nonzero in R, and $v(p)$ is p-divisible in the value group of v. Then for each nonnegative integer n, the ideal I_n consists of all $x \in R$ such that $v(x) \geq N_n$ for $N_n = \left(\frac{1}{p} + \cdots + \frac{1}{p^n}\right) v(p)$. In particular, I_n is principal, generated by any $x \in R$ for which $v(x) = N_n$. If moreover v is a real valuation 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. A typical example would be the ring of integers in an algebraic closure of $\mathbb{Q}_p$ or in the completion thereof.

Definition 2.4. 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 2.5. *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. For $\underline{x}, \underline{y} \in W_{p^i}(R)$, put $\underline{x}' := F(\underline{x})$, $\underline{y}' := F(\underline{y})$.*

(a) *If $x_{p^j} - y_{p^j} \in I_{n-j}$ for $j = 0, \dots, i$, then $x'_{p^j} - y'_{p^j} \in pI_{n-j-1}$ for $j = 0, \dots, i-1$.*
(b) *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 $F(\underline{x}) = F(\underline{y})$, then $x_{p^j} - y_{p^j} \in I_{i-j}$ for $j = 0, \dots, i-1$.*

(c) *Choose $x_1, \dots, x_{p^{i-1}}, y_1, \dots, y_{p^{i-1}} \in R$ with $x_{p^j} - y_{p^j} \in I_{n-j}$ for $j = 0, \dots, i-1$. Assume also that $F(x_1, x_p, \dots, x_{p^{i-1}}) = F(y_1, y_p, \dots, y_{p^{i-1}})$ if $i > 1$. Then for any $y_{p^i} \in R$, there exists $x_{p^i} \in B(y_{p^i}, I_{n-i})$ such that $F(\underline{x}) = F(\underline{y})$.*

(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 1.4(a) to write $x'_{p^j} - y'_{p^j} = x^p_{p^j} - y^p_{p^j} + p(x_{p^{j+1}} - y_{p^{j+1}}) + p(f_{p^j}(x_1, \dots, x_{p^j}) - f_{p^j}(y_1, \dots, y_{p^j}))$. Writing $y_{p^j} = x_{p^j} - (x_{p^j} - y_{p^j})$, we note that $x^p_{p^j} - y^p_{p^j}$ 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 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 1.4(a) to write

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

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. 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 $I_0 = R$. This 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), by Lemma 1.4(a) again, it suffices to find $x_{p^i} \in B(y_{p^i}, I_{n-i})$ such that $x^p_{p^{i-1}} + px_{p^i} + pf_{p^{i-1}}(x_1, \dots, x_{p^{i-1}}) = y^p_{p^{i-1}} + py_{p^i} + pf_{p^{i-1}}(y_1, \dots, y_{p^{i-1}})$. Note that $x_{p^{i-1}} - y_{p^{i-1}} \in I_{n-i+1}$ 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 $x^p_{p^{i-1}} - y^p_{p^{i-1}} + p(f_{p^{i-1}}(x_1, \dots, x_{p^{i-1}}) - f_{p^{i-1}}(y_1, \dots, y_{p^{i-1}})) \in pI_{n-i}$.

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 1.4(a), we have $y^p_{p^i} + py_{p^{i+1}} + pf_{p^i}(y_1, \dots, y_{p^i}) = x_{p^i}$. This is possible because $y^p_{p^i}$, $pf_{p^i}(y_1, \dots, y_{p^i})$, and x_{p^i} all belong to pI_∞. □

Corollary 2.6. *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 $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ 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 2.5(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 2.5(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. □

Remark 2.7. The image under the ghost map of any element in the kernel of F has the form $(*, 0, 0, \dots)$. If R is a p-torsion-free ring, the ghost map is injective, so any element of the kernel of F is uniquely determined by its first component. In this case, we may combine Proposition 2.5(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 $j = 0, \dots, i$.

3. 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 more frequently than full surjectivity. We first list a number of such conditions, then identify logical relationships among them.

Definition 3.1. For R an arbitrary ring, label the conditions on R as follows.

(i) $F : W(R) \to W(R)$ is surjective.
(ii) $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ is surjective for all $n \geq 2$.
(ii)′ $F : W_{p^2}(R) \to W_p(R)$ is surjective.
(iii) For every $\underline{x} \in W(R)$, there exists $r \in R$ such that $\underline{x} - [r] \in pW(R)$.
(iv) The image of $F : W(R) \to W(R)$ contains all Teichmüller elements $[r]$.
(v) $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ contains all elements of the form $(r, 0, \dots, 0)$ for all $n \geq 2$.
(v)′ $F : W_{p^2}(R) \to W_p(R)$ contains all elements of the form $(r, 0)$.
(vi) The image of $F : W(R) \to W(R)$ contains $V(1)$.
(vii) For all $n \geq 2$, the image of $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ contains $V(1)$.
(viii) For all $n \geq 2$, the image of $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ contains $V^{n-1}(1)$.
(ix) The image of $F : W_{p^2}(R) \to W_p(R)$ contains $V(1)$.
(x) $F^n : W_{p^n}(R) \to W_1(R)$ is surjective for all $n \geq 1$.
(x)′ $F : W_p(R) \to W_1(R)$ is surjective.
(xi) R contains p^{-1}.
(xii) For any $r_0, r_1, \dots \in R$ such that $B(r_0, I_0) \supseteq B(r_1, I_1) \supseteq \cdots$ (in the notation of Definition 2.4), the intersection $\cap_{i \in \mathbb{N}} B(r_i, I_i)$ is non-empty.
(xiii) The p-th power map on R/pI_∞ (which need not be a ring homomorphism) is surjective.
(xiv) For each $n \geq 1$, the p-th power map on R/pI_n is surjective.
(xiv)′ The p-th power map on R/pI_1 is surjective.
(xv) For every $r \in R$, there exists $s \in R$ such that $s^p \equiv pr \mod p^2R$.
(xvi) There exist r, s in R such that $r^p \equiv -p \mod psR$ and $s \in I_1$.
(xvii) There exist r, s in R such that $r^p \equiv -p \mod psR$ and $s^N \in pR$ for some integer $N > 0$.
(xviii) The Frobenius homomorphism $\varphi : \overline{r} \mapsto \overline{r}^p$ on R/pR is surjective.

These conditions are represented graphically in Figure 1. The conditions in the top left quadrant refer to infinite Witt vectors, those in the top right quadrant refer to finite Witt vectors, and those below the dashed line refer to R itself.

Theorem 3.2. *For any ring R, we have (ii) $\Leftrightarrow$ (ii)′, (v) $\Leftrightarrow$ (v)′, (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 sources of the arrows of that type together imply the condition at the target.*

The proof of Theorem 3.2 will occupy most of the rest of this section. First, however, we mention some consequences of Theorem 3.2 and some negative results which follow from some examples considered in Section 4.

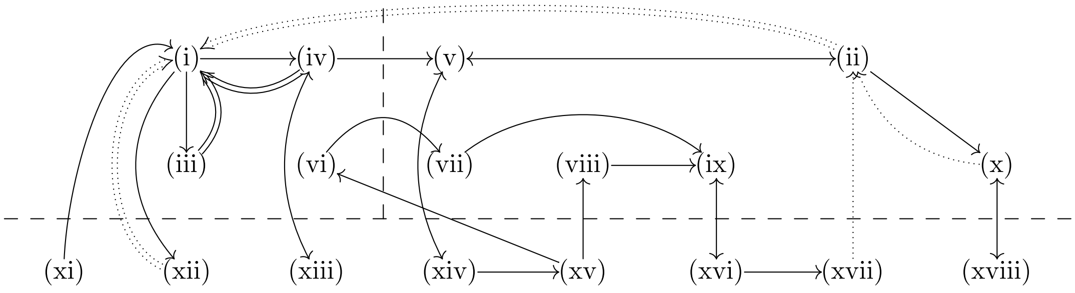

FIGURE 1. Logical implications among conditions on the ring R.

Corollary 3.3. *For any ring R, we have the following equivalences.*

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

The equivalence $(ii) \Leftrightarrow (xviii) + (xvii)$ will be needed later in the proof of Theorem 5.2.

Remark 3.4. The following implications fail to hold by virtue of the indicated examples.

- $(i) \not\Rightarrow (xi)$ by Example 4.7.
- $(ii) \not\Rightarrow (i)$ by Example 4.4 (or from $(ii) \not\Rightarrow (iv)$ below).
- $(ii) \not\Rightarrow (iii)$ by Example 4.4.
- $(ii) \not\Rightarrow (iv)$ by Example 4.9.
- $(ii) \not\Rightarrow (xii)$ by Example 4.4.
- $(iv) \not\Rightarrow (i)$ by Example 4.4.
- $(vi) \not\Rightarrow (xv)$ by Example 4.8.
- $(vi) \not\Rightarrow (xviii)$ by Example 4.8.
- $(xii) \not\Rightarrow (xvii)$ by Example 4.2.
- $(xv) \not\Rightarrow (xviii)$ by Example 4.3.
- $(xviii) \not\Rightarrow (xvii)$ by Example 4.2.

Proof of Theorem 3.2. We now prove the implications represented in Figure 1.

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

  Proof. These are all obvious. □

- $(i) \Rightarrow (iii)$

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

- $(i) \Rightarrow (xii)$

  Proof. Fix elements r_i as in condition (xii). Our strategy is to define an element $\underline{y} \in W(R)$ 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 $\underline{y}^{(p^i)} \in W_{p^i}(R)$ 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 2.5(b,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 $F(\underline{z}^{(p^i)}) = 0$. Choose any $\underline{x}^{(p^{i+1})} \in W_{p^{i+1}}(R)$ 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 $\underline{y}^{(p^i)}$ yield 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 $x_1 \equiv x_1^{(p^{i+1})} \bmod I_{i+1}$ by Proposition 2.5(c). Because x_1 does not depend on i, and $x_1^{(p^{i+1})} = r_{i+1}$, we have that $x_1 \in \cap_{i=0}^{\infty} B(r_{i+1}, I_{i+1})$, as desired. □

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

  Proof. Choose any $\underline{y} \in W(R)$. We will construct $\underline{x} \in W(R)$ such that $F(\underline{x}) = \underline{y}$. We use (ii) to find elements $\underline{x}^{(1)}, \underline{x}^{(p)}, \ldots \in W(R)$ so that $F(\underline{x}^{(1)}) = (y_1, *, *, \cdots), F(\underline{x}^{(p)}) = (y_1, y_p, *, *, \cdots)$, and so on. By (xii) and Proposition 2.5(b), we may choose $\widetilde{x_{p^j}}$ which is in the intersection $B_0(x_{p^j}^{(p^j)}, I_0) \cap B_1(x_{p^j}^{(p^{j+1})}, I_1) \cap \cdots$. Put $\widetilde{\underline{y}} := F(\widetilde{x_1}, \widetilde{x_p}, \ldots)$. We first apply Proposition 2.5(a) to $(\widetilde{x_1}, \ldots, \widetilde{x_{p^{i+1}}})$ and $(x_1^{(p^k)}, \ldots, x_{p^{i+1}}^{(p^k)})$ 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 2.5(d), $\underline{z}$ is in the image of F, as then is $\underline{y}$. □

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

  Proof. This is obvious, given that any element $p\underline{x}' = F(V(\underline{x}'))$ is in the image of Frobenius. □

- $(iv) \Rightarrow (xiii)$; $(v) \Rightarrow (xiv)$; $(v)' \Rightarrow (xiv)'$

  Proof. Suppose that $n \geq 2$ and that $\underline{x} \in W_{p^n}(R)$ and $r \in R$ are such that $F(\underline{x}) = [r]$. For each of $k = 0, \ldots, n-1$, we check that $x_p, x_{p^2}, \ldots, x_{p^{n-k}}$ belong to I_k. This is clear for $k = 0$. Given the claim for some $k < n-1$, for $i = 1, \ldots, n-1-k$ we may apply Lemma 1.4(a) to deduce that $x_{p^i}^p + p x_{p^{i+1}} + p f_{p^i}(x_1, ..., x_{p^i}) = 0$. By Lemma 1.4(b), f_{p^i} contains no pure power of $x_1^{p^{i+1}}$, so $f_{p^i}(x_1, \ldots, x_{p^i})$ belongs to the ideal generated by $x_p, \ldots, x_{p^i}$. Therefore $-p x_{p^{i+1}}$ and $-p f_{p^i}(x_1, \ldots, x_{p^i})$ belong to pI_k, and so $x_{p^i} \in I_{k+1}$. This proves the claim. Consequently, $x_p \in I_{n-1}$, and so $r - x_1^p = p x_p \in pI_{n-1}$. The stated implications now follow. □

- $(ix) \Rightarrow (xvi)$

  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, $x_1^p + p x_p = 0$ and $x_1^{p^2} + p x_p^p + p^2 x_{p^2} = p$. The first equality tells us that $x_1^p \in pR$ (and hence $x_1^{p^2} \in p^pR$). The second equality now tells us $px_p^p \equiv p \mod p^2R$ and so $x_p^p \equiv 1 \mod pR$. By the binomial theorem, $x_p^p - 1 - (x_p - 1)^p$ is in pR, so if we put $s := x_p - 1$, we have $s^p \in pR$. Returning to the equation $x_1^p + px_p = 0$, we have $x_1^p \equiv -p \mod psR$ with $s^p \in pR$, as required. □

- $(x)' \Rightarrow (xviii)$; $(xi) \Rightarrow (i)$

  Proof. Working with ghost components as above, these are obvious. □

- $(xiii) \Rightarrow (iv)$

  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 $n \geq 1$.

  Given $x_1, \dots, x_{p^n}$, define f_{p^n} as in Lemma 1.4(a). By Lemma 1.4(b), 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 1.4(a), this choice of $x_{p^{n+1}}$ has the desired effect. □

- $(xv) \Rightarrow (vi)$

  Proof. We will 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 $r^p \equiv -p \mod p^2$. Set $x_1 := r$. Then clearly we can choose $x_p \equiv 1 \mod p$ such that $F(x_1, x_p) = (0)$. Next, in the notation of Lemma 1.4(a), 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 $x_{p^2} \equiv 0 \mod p$, while if $p = 2$, then $x_{p^2} = 1 \mod p$. To see that this is possible, we note $x_p^p \equiv 1 \mod p^2$. We then observe 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 1.4(c,d), when $p > 2$ this constant is divisible by p, so $pf_p(x_1, x_p) \equiv 0 \mod p^2$. If $p = 2$, this constant is $1 \mod 2$, so $pf_p(x_1, x_p) \equiv 2 \mod p^2$. In either case, we obtain x_{p^2} of the desired form.

  Now assume that for some $i \geq 2$, we have found $x_1, x_p, \dots, x_{p^i}$ such that $x_{p^j} \equiv 0 \mod p$ for $j \geq 3$ and such that $F(x_1, x_p, \dots, x_{p^i}) = (0, 1, 0, \dots, 0)$. We claim that we can find $x_{p^{i+1}} \equiv 0 \mod p$ with $F(x_1, x_p, \dots, x_{p^{i+1}}) = (0, 1, 0, \dots, 0)$. We claim we can find $x_{p^{i+1}} \equiv 0 \mod p$ such that

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

  and with $f_{p^i}(x_1, \dots, x_p) \equiv 0 \mod p$. This follows by Lemma 1.4(c,e). □

- $(xv) \Rightarrow (viii)$

  Proof. Our goal is to find an element $\underline{x} = (x_1, x_p, \dots, x_{p^n})$ such that $F(\underline{x}) = V^{n-1}(1)$. First, set $\widetilde{x_{p^{n-1}}} = 1$, and then find $\widetilde{x_{p^{n-2}}}, \dots, \widetilde{x_1}$ (in that order) such that $\widetilde{x_{p^i}}^p \equiv -p\widetilde{x_{p^{i+1}}} \mod p^2R$. This is possible by (xv). Note that $\widetilde{x_{p^i}}^p \in pR$ for $0 \leq i \leq n-2$.

  We next construct the elements $x_1, \dots, x_{p^{n-1}}$. Set $x_1 := \widetilde{x_1}$. Assume we have found $x_1, \dots, x_{p^i}$ with $x_{p^j} \equiv \widetilde{x_{p^j}} \mod pR$ for some $i \leq n-2$. Using the notation of Lemma 1.4(a), we first must choose $x_{p^{i+1}}$ which satisfies

$x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, \ldots, x_{p^i}) = 0$. Write $x_{p^{i+1}} = \widetilde{x_{p^{i+1}}} + py_{p^{i+1}}$. We must choose $y_{p^{i+1}}$ so that

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

Because $\widetilde{x_{p^i}}^p + p\widetilde{x_{p^{i+1}}} \equiv 0 \mod p^2$ and $\widetilde{x_{p^i}} \equiv x_{p^i} \mod p$, we deduce that $x_{p^i}^p + p\widetilde{x_{p^{i+1}}} \equiv 0 \mod p^2$. We further have that $pf_{p^i}(x_1, \ldots, x_{p^i}) \equiv 0 \mod p^2$; this follows from the homogeneity result in Lemma 1.4(a) and the fact that $x_{p^j}^p \equiv 0 \mod p$ for all j. This shows that we can find the required $y_{p^{i+1}}$.

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

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

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

- $(xvi) \Rightarrow (ix)$

Proof. By Lemma 1.4(a), we must find x_1, x_p, x_{p^2} such that $x_1^p + px_p = 0$ and $x_p^p + px_{p^2} + pf_p(x_1, x_p) = 1$. By (xvi), we can find an element x_1 such that $x_1^p + p + psr = 0$ where $s^p \in pR$; we then choose $x_p = 1 + sr$. It's then clear that $x_p^p + pf_p(x_1, x_p) \equiv 1 \mod pR$, and so we can find x_{p^2} forcing $x_p^p + px_{p^2} + pf_p(x_1, x_p) = 1$, as desired. □

- $(xviii) \Rightarrow (x)$

Proof. For any $r \in R$, we must find $r_1, \ldots, r_{p^n}$ 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. □

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

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

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

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 have already seen that $(x) \Rightarrow (x)' \Rightarrow (xviii)$. Given any $r \in R$, by (xviii) we can find $s_3 \in R$ with $s_3^p \equiv -r(1 + s_2 + \cdots + s_2^{N-1}) \mod p$. Since $s_2^N \equiv 0 \mod p$, for $s = s_1 s_3$ we have $s^p = pr(1 - s_2)(1 + s_2 + \cdots + s_2^{N-1}) = pr(1 - s_2^N) \equiv pr \mod p^2$. □

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

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

We prove that $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$ is surjective for $n \geq 1$ by induction on n. The base case $n = 1$ is exactly $(x)'$. Now assume the result for some fixed $n - 1$, pick any $\underline{y} \in W_{p^n}(R)$, and consider the diagram

$$\begin{tikzcd}
W_{p^{n+1}}(R) \ni \underline{r} \arrow[rr, "F"] \arrow[dr, "\text{res}"] & & \underline{y}' \in W_{p^n}(R) \arrow[dr, "\text{res}"] & \underline{y} \in W_{p^n}(R) \arrow[d, "\text{res}"] \\
& W_{p^n}(R) \ni \underline{s} \arrow[rr, "F"] & & \underline{y}|_{W_{p^{n-1}}(R)}.
\end{tikzcd}$$

The term $\underline{s}$ exists by our inductive hypothesis and the term $\underline{r}$ exists because restriction maps are surjective. 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, using (x), find $\underline{x}'' \in W_{p^{n+1}}(R)$ with $\underline{y} - \underline{y}' = V^n(F^{n+1}(\underline{x}''))$. A calculation now shows $F\left(\underline{r} + \underline{x}'\underline{x}''\right) = \underline{y}$, as desired. □

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

  Proof. These are compositions of implications we have already proved. □

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

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

$$\begin{tikzcd}
\text{(ii)} \arrow[r] \arrow[d] & \text{(v)} \arrow[r] \arrow[d] & \text{(xiv)} \arrow[d] \\
\text{(ii)}' \arrow[r] & \text{(v)}' \arrow[r] & \text{(xiv)}'.
\end{tikzcd}$$

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

We conclude the discussion by making some additional observations in the case of valuation rings.

Remark 3.5. Let R be a valuation ring with valuation v for which $0 < v(p) < +\infty$, and introduce the following new condition.

(xix) There exists $x \in R$ with $0 < v(x) < v(p)$.

We then have

$$(ii) \Leftrightarrow (xv) \Leftrightarrow (xviii) + (xix).$$

Namely, by Theorem 3.2, it suffices to check that (xv) implies (xviii) and that the two conditions (xviii) + (xix) together imply (xvi). These implications are verified as follows.

Given (xv), for any $x \in R$ we can find $y_1, y_2 \in R$ with $y_1^p \equiv px \mod p^2R$, $y_2^p \equiv p \mod p^2R$. Then $v(y_1) = \frac{1}{p}(v(p) + v(x))$, $v(y_2) = \frac{1}{p}v(p)$, so $z := y_1/y_2$ is an element of R satisfying $z^p \equiv x \mod pR$. This yields (xviii).

Given (xviii) + (xix), there exist $y, z \in R$ with $y^p \equiv x \mod p$, $z^p \equiv p/x \mod pR$. 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, so there exists $w \in R$ such that $w^p \equiv -u^{-1} \mod pR$. Thus we have $puw^p \equiv -p \mod p^2R$ and $(yzw)^p \equiv -p \mod p^2R$, yielding (xvi). (As a byproduct of the argument, we note that (ii) implies that $v(p)$ is p-divisible.)

4. Examples

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

Example 4.1. Take R to be any ring in which p is invertible. Then by Theorem 3.2, all of our conditions hold.

Example 4.2. Take $R = \mathbb{Z}$. In this case, $I_i = (p)$ for all $i \geq 1$. Thus (xvii) fails, and 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, which is clear.

Example 4.3. 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.

Example 4.4. Take $R = \mathcal{O}_{\mathbb{C}_p}$. Then (xiii) holds because R is integrally closed in the algebraically closed field $\mathbb{C}_p$; this implies that R satisfies (iv), (v), (vi), (vii), (viii), (ix), (x), (xiii), (xiv), (xv), (xvi), (xvii), (xviii). On the other hand, (xii) does not hold by Lemma 4.5, so R does not satisfy (i), (iii), (xi), (xii).

Lemma 4.5. *The ring $R = \mathcal{O}_{\mathbb{C}_p}$ does not satisfy (xii).*

Proof. By Remark 2.3, for n a nonnegative integer, I_n is the principal ideal generated by $p^{\frac{1}{p}+\cdots+\frac{1}{p^n}}$, 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 $B(r_0, I_0) \supseteq B(r_1, I_1) \supseteq \cdots$ 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 $\cap_{i=0}^{\infty} B(r_i, I_i)$ are disjoint. □

Remark 4.6. It is possible to give a more constructive proof of Lemma 4.5 using the explicit description of $\mathcal{O}_{\mathbb{C}_p}$ given in [8].

Example 4.7. Let R be a *spherically complete* valuation ring (i.e., any decreasing sequence of balls in R has nonempty intersection) such that the valuation of p is nonzero and p-divisible (so the I_n are as computed in Remark 2.3). Then R satisfies (xii).

In particular, let R denote the spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ constructed by Poonen in [10]. Namely, let $\mathbb{Z}_p[\![t^{\mathbb{Q}}]\!]$ denote the ring of *generalized power series* over $\mathbb{Z}_p$; its elements are formal sums $\sum_{i \in \mathbb{Q}, i \geq 0} c_i t^i$ with $c_i \in \mathbb{Z}_p$ 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. We then take $R = \mathbb{Z}_p[\![t^{\mathbb{Q}}]\!]/(t-p)$, so that $R/(p) \cong \mathbb{F}_p[\![t^{\mathbb{Q}}]\!]/(t)$. From this description, it is clear that R satisfies (xii) and (xviii); since R contains $\mathcal{O}_{\mathbb{C}_p}$, it also satisfies (xvi). Putting this together, we deduce that R satisfies (i).

Example 4.8. Take $R = \mathbb{Z}[\mu_{p^2}]$, where μ_{p^2} is a primitive (p^2)-nd root of unity. Condition (vi) holds because if $\underline{x} = \sum_{i=0}^{p-1} [\mu_{p^2}^i] \in W(R)$, then $F(\underline{x}) = V(1)$. (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 $\frac{1}{p^2(p-1)}$. Similarly, (xv) does not hold.

Example 4.9. 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 (vi) because R contains the subring $\mathbb{Z}[\mu_{p^2}]$ which satisfies (vi) by Example 4.8. Thus to establish (ii), it is sufficient to check condition (xviii). For this, 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 $a_1\mu_{p^{i_1}} + \cdots + a_n\mu_{p^{i_n}} \equiv (a_1\mu_{p^{i_1+1}} + \cdots + a_n\mu_{p^{i_n+1}})^p \mod p$.

To establish that R does not satisfy (iv), we will check that R does not satisfy (xiii). We will do this assuming $p > 2$, by checking that the congruence $x^p \equiv 1 - p \mod pI_\infty$ has no solution. This breaks down for $p = 2$; in this case, one can show by a similar argument that the congruence $x^2 \equiv i + 2\mu_8 \mod 2I_\infty$ has no solution.

Assume by way of contradiction that $p > 2$ and there exists $x \in R$ for which $x^p - 1 + p \in pI_\infty$. Recall that by Remark 2.3, I_∞ is the principal ideal generated by $p^{1/(p-1)}$. Choose an integer $n \geq 2$ for which $x \in \mathbb{Z}[\mu_{p^n}]$, and put $z = 1 - \mu_{p^n}$. By an elementary calculation, $z^{p^{n-1}-p^{n-2}} \equiv -p \pmod{z^{p^n}}$; in particular, the p-adic valuation of $1 - \mu_{p^n}$ is $\frac{1}{p^{n-1}(p-1)}$. There must thus exist $y \in \mathbb{Z}[\mu_{p^n}]$ such that $(1 + yz^{p^{n-1}-p^{n-2}})^p \equiv 1 - p \pmod{z^{p^n}}$; subtracting 1 from both sides and dividing by p, we obtain the congruence $yz^{p^{n-1}-p^{n-2}} - y^p \equiv -1 \pmod{z^{p^{n-1}}}$. Using the isomorphism $\mathbb{Z}[\mu_{p^n}]/(z^{p^{n-1}}) \cong \mathbb{F}_p[T]/(T^{p^{n-1}})$ sending z to T, we obtain a solution w of the congruence $w^p - wT^{p^{n-1}-p^{n-2}} \equiv 1 \pmod{T^{p^{n-1}}}$ in $\mathbb{F}_p[T]$. However, no such solution exists: such a solution would satisfy $w \not\equiv 0 \pmod{T^{p^{n-2}}}$, so there would be a largest index $i < p^{n-2}$ such that the coefficient of T^i in w is nonzero. But then $T^{i+p^{n-1}-p^{n-2}}$ would appear with a nonzero coefficient in $w^p - wT^{p^{n-1}-p^{n-2}}$.

5. Almost purity

Let us say that a ring R is *Witt-perfect* if condition (ii) holds. We conclude with one motivation for studying Witt-perfect rings: they provide a natural context for the concept of *almost purity*, as introduced by Faltings [2] and studied more recently by the second author and Liu in [9] and by Scholze in [11]. More precisely, the Witt-perfect condition amounts to an absolute version (not relying on a valuation subring) of the condition for a ring to be *integral perfectoid* in the sense of Scholze. (For a valuation ring, another equivalent condition is to be *strictly perfect* in the sense of Fargues and Fontaine [3].)

We begin by defining the adverb *almost* in this context. See [4] for a more general setting.

Definition 5.1. A *p-ideal* of a ring R is an ideal I 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.

Theorem 5.2. *Let R be a p-torsion-free Witt-perfect ring which is integrally closed in $R_p := R[p^{-1}]$. Let S_p be a finite étale R_p-algebra and let S be the integral closure of R in S_p.*

(a) The ring S is also Witt-perfect.

(b) For any p-ideal I of R, there exist a finite free R-module F and R-module homomorphisms $S \to F \to S$ whose composition is multiplication by some $t \in R$ for which $I \subseteq (t)$.

(c) The image of S under the trace pairing map $S_p \to \operatorname{Hom}_{R_p}(S_p, R_p)$ is almost equal to the image of the natural map from $\operatorname{Hom}_R(S, R)$ to $\operatorname{Hom}_{R_p}(S_p, R_p)$.

In the language of almost ring theory, the conclusion here is that S is *almost finite étale* over R. Again, see [4] for detailed definitions.

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

$$R_t := \{x \in R_p : p^{-r}x^s \in R\}$$

depends only on t. The function $v : R_p \to (-\infty, +\infty]$ 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 $\psi : R_p \to A$ be the natural homomorphism; then $R \subseteq \psi^{-1}(\mathfrak{o}_A)$ and $\psi^{-1}(\mathfrak{m}_A) \subset R$, so $\psi^{-1}(\mathfrak{o}_A)/R$ is an almost zero R-module.

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

$$x_1^p \equiv -p \mod p^2R, \qquad x_2^p \equiv x_1 \mod pR.$$

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

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

Given $\overline{y} \in \mathfrak{o}_A/(p)$, choose $y \in R_p$ so that $\psi(y)$ lifts $\overline{y}$. 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 $x_2^p y \equiv z^p \mod pR$. The element $\psi(z/x_2) \in \mathfrak{o}_A$ has the property that $\psi(z/x_2)^p \equiv \psi(y) \mod (p/\psi(x_2)^p)\mathfrak{o}_A$; it follows that Frobenius is surjective on $\mathfrak{o}_A/(\psi(x_1)^{p-1})$. Since $\psi(x_2)^{p(p-1)} \equiv \psi(x_1)^{p-1} \mod p\mathfrak{o}_A$, it also follows that Frobenius is surjective on $\mathfrak{o}_A/(p)$. That is, $\mathfrak{o}_A$ also satisfies (xviii); since (xvi) is evident (using x_1), $\mathfrak{o}_A$ satisfies (ii).

Put $B = A \otimes_{R_p} S_p$ and extend ψ by linearity to a homomorphism $\psi : S_p \to B$. By [9, 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 [9, Remark 2.3.14], for $\mathfrak{m}_B = \{x \in B : |x| < 1\}$, we have $\psi^{-1}(\mathfrak{m}_B) \subset S$, so $\psi^{-1}(\mathfrak{o}_B)/S$ is an almost zero R-module. Given $\overline{y} \in S/(p)$, choose a lift $y \in S$ of $\overline{y}$. 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 $x_1^p = -p + p^2 w$ for some $w \in R$ and then write

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

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 $S/(x_1, p)$; using the fact that $x_2^p \equiv x_1 \mod pR$, 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). This proves (a). The proofs of (b) and (c) similarly reduce to the corresponding statements about $\mathfrak{o}_A$ and $\mathfrak{o}_B$, for which see [9, Theorem 5.5.9] or [11, Theorem 5.25]. □

Corollary 5.3. *For R and S as in Theorem 5.2, $\Omega_{S/R} = 0$.*

Proof. Since S_p is finite étale over R_p, $\Omega_{S/R}$ is killed by p^n for some nonnegative integer n. If $n > 0$, then for each $x \in S$ we may apply Theorem 5.2 to write $x = y^p + pz$, and so $dx = py^{p-1}\,dy + p\,dz$ is also killed by p^{n-1}. By induction, it follows that we may take $n = 0$, proving the claim. □

Remark 5.4. Parts (b) and (c) of Theorem 5.2 remain true if we replace S with a R-subalgebra S' of S_p which is almost equal to S.

Remark 5.5. Let R be a Witt-perfect valuation ring in which $p \neq 0$. Then Theorem 5.2 implies that for S the integral closure of R in a finite extension of $\mathrm{Frac}(R)$, 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]. The case $R = \mathcal{O}_{\mathbb{C}_p}$ of this result was previously established by Tate.

Remark 5.6. The result of Tate described in Remark 5.5 was previously generalized by Faltings's original almost purity theorem, which may also be deduced from Theorem 5.2. A typical case of the latter result covered by Faltings is

$$R = \mathbb{Z}_p[\mu_{p^\infty}][T_1^{\pm}, \dots, T_n^{\pm}][T_1^{1/p^\infty}, \dots, T_n^{1/p^\infty}],$$

for which it is clear that R is Witt-perfect but not at all apparent that S is.

Theorem 5.2 also includes, and indeed is a reformulation of, the generalizations of almost purity given in [9, Theorem 5.5.9] and [11, Theorem 5.25]. Those results are stated in terms of p-adically complete rings and use nonarchimedean analytic geometry in their proofs. The reformulation in terms of the Witt-perfect condition suggests the intriguing possibility of looking at Witt-perfectness for multiple primes at once, with a view towards extending the constructions of p-adic Hodge theory to a more global setting.

Acknowledgements

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

References

[1] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), no. 1-3, 129–174. MR 1369413 (97b:11079)

[2] Gerd Faltings, *p-adic Hodge theory*, J. Amer. Math. Soc. **1** (1988), no. 1, 255–299. MR 924705 (89g:14008)

[3] Laurent Fargues and Jean-Marc Fontaine, *Courbes et fibrés vectoriels en théorie de Hodge p-adique*, (2011), in preparation; draft available at http://www.math.u-psud.fr/~fargues/Prepublications.html.

[4] Ofer Gabber and Lorenzo Ramero, *Almost ring theory*, Lecture Notes in Mathematics, vol. 1800, Springer-Verlag, Berlin, 2003. MR 2004652 (2004k:13027)

[5] Michiel Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, no. v. 78, Academic Press, 1978.

[6] Lars Hesselholt, *The big de Rham-Witt complex*, (2010), http://www.math.nagoya-u.ac.jp/~larsh/papers/028/.

[7] Luc Illusie, *Complexe de de Rham-Witt et cohomologie cristalline*, Annales scientifiques de l'Ecole Normale Superieure **12** (1979), no. 4, 501–661.

[8] Kiran S. Kedlaya, *Power series and p-adic algebraic closures*, Journal of Number Theory **89** (2001), no. 2, 324–339.

[9] Kiran S. Kedlaya and Ruochuan Liu, *Relative p-adic Hodge theory, I: Foundations*, (2011), http://math.ucsd.edu/~kedlaya/papers/.

[10] Bjorn Poonen, *Maximally complete fields*, Enseign. Math. (2) **39** (1993), no. 1-2, 87–106. MR 1225257 (94h:12005)

[11] Peter Scholze, *Perfectoid spaces*, (2011), http://www.math.uni-bonn.de/people/scholze/.

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

University of California, San Diego, Dept of Mathematics, La Jolla, CA 92093
E-mail address: kedlaya@ucsd.edu