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 Frobenus 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 $W(R)$, 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; 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. 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 the ring of integers in 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 commonly satisfied and more relevant to applications. For instance, one can view the full ring of Witt vectors as an inverse limit of finite-length truncations, and the condition of 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*, based on recent work by the second author and Liu [5] and by Scholze [7].

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.

Date: September 29, 2014.

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).

1. Witt vectors

Throughout this section, let R denote an arbitrary ring. For more details on the construction of p-typical Witt vectors, see [3, Section 0.1].

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, the* Verschiebung *maps $V : W_{p^n}(R) \to W_{p^{n+1}}(R)$ defined by the formula $V(r_1, \dots, r_{p^n}) = (0, r_1, \dots, r_{p^n})$ are additive (but not multiplicative).*

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 $r_1, r_2 \in R$, $[r_1 r_2] = [r_1][r_2]$.*

Some additional properties of Witt vectors are the following.

(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 $p = 2$. To complete the argument, we show by induction on n that for each $n \geq 1$, we have $x_{p^i} \equiv 0$ mod 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 $x_p \equiv (-1)^{p-1} \mod p^{p-1}$ and so $x_p^p \equiv 1 \mod p^3$. We then have $x_p^{p^{n-1}} \equiv 1 \mod p^{3+n-2}$, 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} under the weighting in which the variable 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_{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. 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 [3, (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 y_{p^i} does not depend on $x_{p^{i+1}}$. We may 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 $x_p = x_{p^2} = \cdots = 0$, 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 $x_1 = x_{p^2} = x_{p^3} = \cdots = 0$, so that $\underline{x} = V([x_p])$. In this case, the claim is that $y_{p^i} \equiv 0 \mod p^2$ 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 $x_1 = x_{p^3} = x_{p^4} = \cdots = 0$, so that $\underline{x} = V([x_p]) + V^2([x_{p^2}])$. By homogeneity, it is sufficient to check the claim for $x_p = x_{p^2} = 1$. 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

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

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. By 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 $F : W_{p^n}(R) \to W_{p^{n-1}}(R)$, 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.*

2. The kernel of Frobenius

When R is a ring not of characteristic p, it is easy to see that $F : W(R) \to W(R)$ cannot be injective; for instance, the Cartier-Dieudonné-Dwork lemma 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 the 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 $I_\infty = \{r \in R \mid r^p \in pI_\infty\}$.*

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. *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 $\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^i}$, while I_∞ is the principal ideal generated by any element of valuation $\frac{1}{p-1}$.*

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.*

- *(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 1.4 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 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 1.4 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 1.4, 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_∞. □

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 $n \geq 2$.

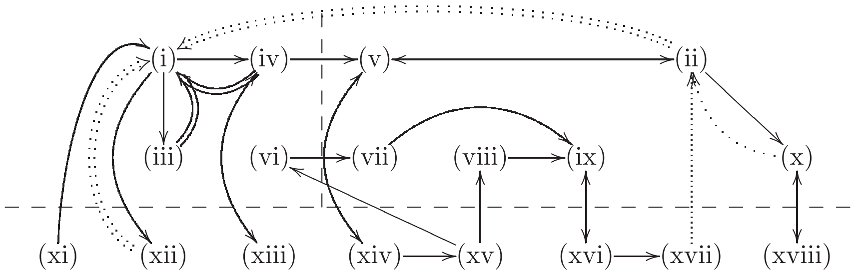


FIGURE 1. Logical implications among conditions on the ring R.

- *(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* $(r, 0, \ldots, 0)$ *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* $\cap_{i=0}^{\infty} B(r_i, I_i)$ *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. Note that conditions in the top left quadrant refer to infinite Witt vectors, conditions in the top right quadrant refer to finite Witt vectors, and conditions 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 tails of the arrows of that type together imply the condition at the target.*

The proof of Theorem 3.2 will occupy 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 5.

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

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

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

- $(i) \not\Rightarrow (xi)$ *by Example 5.7.*
- $(ii) \not\Rightarrow (i)$ *by Example 5.4 (or from* $(ii) \not\Rightarrow (iv)$ *below).*
- $(ii) \not\Rightarrow (iii)$ *by Example 5.4.*
- $(ii) \not\Rightarrow (iv)$ *by Example 5.9.*
- $(ii) \not\Rightarrow (xii)$ *by Example 5.4.*
- $(iv) \not\Rightarrow (i)$ *by Example 5.4.*
- $(vi) \not\Rightarrow (xv)$ *by Example 5.8.*
- $(vi) \not\Rightarrow (xviii)$ *by Example 5.8.*
- $(xii) \not\Rightarrow (xvii)$ *by Example 5.2.*
- $(xv) \not\Rightarrow (xviii)$ *by Example 5.3.*
- $(xviii) \not\Rightarrow (xvii)$ *by Example 5.2.*

Remark 3.5. *It seems that there should be some relationship between (iii) and (xii), but we were unable to clarify this.*

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

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

  Proof. These are all obvious. □
- $(i) \Rightarrow (iii)$

  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 $F(\underline{x}) \equiv [x_1^p] \mod pW(R)$. 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 $\underline{y} \in W(R)$ 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 $\underline{y}^{(p^i)} \in W_{p^i}(R)$ 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(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 $x_1 \equiv \underline{x}_1^{(p^{i+1})}$ mod I_{i+1}. Because x_1 does not depend on i, and $x_1^{(p^{i+1})} = r_{i+1}$, we have that $x_1 \in \cap_{i=0}^{\infty} B(r_{i+1}, I_{i+1})$, 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 $\widetilde{x_{p^j}}$ 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 $\underline{\widetilde{y}} := F(\widetilde{x_1}, \widetilde{x_p}, \ldots)$. 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 $\underline{\widetilde{y}}$ have the same image in $W(R/pI_\infty)$, so the difference $\underline{z} = \underline{y} - \underline{\widetilde{y}}$ 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 $r \in R$ satisfy $F(\underline{x}) = [r]$. 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 to deduce that $x_{p^i}^p + px_{p^{i+1}} + pf_{p^i}(x_1, ..., x_{p^i}) = 0$. By Lemma 1.4′, 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 $-px_{p^{i+1}}$ and $-pf_{p^i}(x_1, \ldots, x_{p^i})$ 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 $r - x_1^p = px_p \in pI_{n-1}$. 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, $x_1^p + px_p = 0$ 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 $x_1^{p^2} \in p^pR$). The second equality now tells us $px_p^p \equiv p \mod p^2R$ and so $x_p^p \equiv 1 \mod pR$. 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 $x_1^p \equiv -p \mod psR$ where $s^p \in pR$, 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. By Lemma 1.4′, 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, this choice of $x_{p^{n+1}}$ has the desired effect. □

- $(xv) \Rightarrow (vi)$

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 $r^p \equiv -p \mod p^2$. 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, 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 first observe that $x_p^p \equiv 1 \mod p^2$. 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 1.4′, if $p > 2$ 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 $pf_p(x_1, x_p) \equiv -2 \pmod{p^2}$. 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 then claim that we can find $x_{p^{i+1}} \equiv 0 \mod p$ such that $F(x_1, x_p, \dots, x_{p^{i+1}}) = (0, (-1)^{p-1}, 0, \dots, 0)$. We wish to find $x_{p^{i+1}} \equiv 0 \mod p$ such that

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

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

- $(xv) \Rightarrow (viii)$

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 $\widetilde{x_{p^i}}$.

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 $0 \leq i \leq n-2$. Now we will find the actual values $x_1, \dots, x_{p^n}$. 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, 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

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

Because $\widetilde{x_{p^i}}^p + p\widetilde{x_{p^{i+1}}} \equiv 0 \mod p^2$ and $\widetilde{x_{p^i}} \equiv x_{p^i} \mod p$, we have that $x_{p^i}^p + p\widetilde{x_{p^{i+1}}} \equiv 0 \mod p^2$. We further have that $pf_{p^i}(x_1, \dots, x_{p^i}) \equiv 0 \mod p^2$;

this follows from the homogeneity result in Lemma 1.4 and the fact that $x_{p^j}^p \equiv 0 \mod p$ for all j. This shows that we can find the required $y_{p^{i+1}}$.

In this way we can construct the components $x_1, \ldots, x_{p^{n-1}}$. 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

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

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

- $(xvi) \Rightarrow (ix)$

Proof. By Lemma 1.4, 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 $x_p^p + pf(x_1, x_2) \equiv 1 \mod pR$, and so we can find x_{p^2} forcing $x_p^p + px_{p^2} + pf(x_1, x_2) = 1$, 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 $(xviii) \Rightarrow (x)$. □

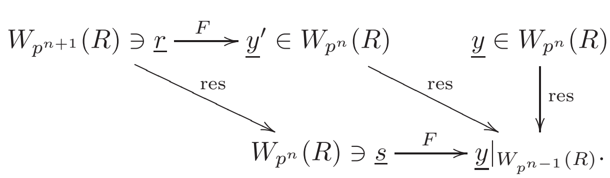
- $(x) + (xvii) \Rightarrow (xv)$

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 know that $(x) \Rightarrow (x)' \Rightarrow (xviii)$. Given any $r \in R$, by (xviii) we can find $s_3 \in R$ for which $s_3^p \equiv -r(1 + s_2 + \cdots + s_2^{N-1}) \mod p$. 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 also know that $(xv) \Rightarrow (viii)$. 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



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 find $\underline{x}'' \in W_{p^{n+1}}(R)$ with $\underline{y} - \underline{y}' = V^n(F^{n+1}(\underline{x}''))$ using (x). Then a calculation shows $F(\underline{r} + \underline{x}'\underline{x}'') = \underline{y}$, 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:

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

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

4. 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 a real valuation. This includes a number of the examples considered in Section 5.

Remark 4.1. *Suppose that $v(p)$ is p-divisible in the value group of v. Then for each nonnegative integer n, the ideal I_n is principal, generated by any $x \in R$ such that $v(x) = \left(\frac{1}{p} + \cdots + \frac{1}{p^n}\right) v(p)$. 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.*

Remark 4.2. *Condition (xii) holds whenever v is a real valuation, $v(p)$ is p-divisible (so the I_n are as computed in Remark 4.1), 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 5.4.*

Remark 4.3. *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 $y^p \equiv x \mod p$, $z^p \equiv p/x \mod pR$. 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. By (xviii) again, there exists $v \in R$ such that $v^p \equiv -u^{-1} \mod pR$. Thus we have $puv^p \equiv -p \mod p^2R$. Thus $(yzv)^p \equiv -p \mod p^2R$. 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 4.4. *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 $r_1^p = -p \mod p^2R$, 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 $\left(\frac{r_2}{r_1}\right)^p = \frac{-pxu+p^2y}{-pu} = x - pu^{-1}y \equiv x \mod p$. Hence (xviii) holds; since (xv) also implies (xvii), we may deduce (ii) as desired.*

Remark 4.5. *If R satisfies condition (ii), then it satisfies almost purity; see Section 6. Thus if S is the integral closure of R in a finite extension of* $\operatorname{Frac}(R)$, *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].

5. Examples

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

Example 5.1. *Take R to be any ring in which p is invertible. Then by Theorem 3.2, all of our conditions hold.*

Example 5.2. *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 5.3. *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 5.4. *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), (vi), (v), (vii), (viii), (ix), (x), (xiii), (xiv), (xv), (xvi), (xvii), (xviii). On the other hand, (xii) does not hold by Lemma 5.5, so R does not satisfy (i), (iii), (xi), (xii).*

Lemma 5.5. *The ring $R = \mathcal{O}_{\mathbb{C}_p}$ does not satisfy (xii).*

Proof. By Remark 4.1, 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 $x_0, x_1, \ldots$ to be Teichmüller elements in $W(\mathbb{F}_p) \subseteq \mathcal{O}_{\mathbb{C}_p}$, and put

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

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

Remark 5.6. *It is possible to give a more constructive proof of Lemma 5.5 using the explicit description of $\mathcal{O}_{\mathbb{C}_p}$ given in* [4].

Example 5.7. *Let R denote the spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ constructed by Poonen in* [6]. *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. 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. Poonen's spherical completion of $\mathcal{O}_{\mathbb{C}_p}$ is then 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) and (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 4.3 implies that R satisfies (ii). Putting this together, we deduce that R satisfies (i).

Example 5.8. *Take $R = \mathbb{Z}[\mu_{p^2}]$, where μ_{p^2} is a primitive (p^2)-nd root of unity. Condition (vi) holds because 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 $\frac{1}{p^2(p-1)}$. Similarly, (xv) does not hold.*

Example 5.9. *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 5.8. 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 $a_1, \ldots, a_n \in \mathbb{Z}$, 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 instead 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 $p = 2$ because $1-p = -1$ is the square of $i := \mu_4$; in this case, one can show by a similar argument (left to the reader) 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 4.1, 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 Lemma 5.10 below, $z^{p^{n-1}-p^{n-2}} \equiv -p \pmod{z^{p^n}}$; 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 $\mathbb{F}_p[T]$. But no such solution exists: we cannot have $w \equiv 0 \pmod{T^{p^{n-2}}}$, so there is a largest index $i < p^{n-2}$ such that the coefficient of T^i in w is nonzero, which forces $T^{i+p^{n-1}-p^{n-2}}$ to appear with a nonzero coefficient in $w^p - wT^{p^{n-1}-p^{n-2}}$.

Lemma 5.10. *For p an odd prime, $n \geq 2$ an integer, and μ_{p^n} a primitive p^n-th root of unity, in $\mathbb{Z}[\mu_{p^n}]$ we have $(1-\mu_{p^n})^{p^n - p^{n-1}} \equiv -p \mod (1-\mu_{p^n})^{p^n}$.*

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 $1-T$. As

$$\Phi(1-T) \equiv \sum_{i=0}^{p-1} (1-T^{p^{n-2}})^{pi} \mod p^2,$$

we have $T^{p^n - p^{n-1}} - \Phi(1-T) \equiv 0 \mod p$. Since the constant term of $\Phi(1-T)$ is p, it suffices to check that $\Phi(1-T) \equiv p \mod (p^2, T^{p^{n-1}})$; this reduces to the case $n = 2$. In this case, for $k = 1, \ldots, p-1$, the coefficient of T^k in $\Phi(1-T)$ is $\sum_{i=0}^{p-1}(-1)^k\binom{ip}{k}$. We may write $\binom{pi}{k} = \frac{ik}{p}\binom{ip-1}{kp-1}$ and then invoke Lucas's criterion to deduce that $\binom{ip-1}{kp-1} \cong \binom{p-1}{k-1} \mod p$. Therefore, $\sum_{i=0}^{p-1}(-1)^k\binom{ip}{k} \equiv (-1)^k\binom{p}{k}\sum_{i=0}^{p-1} i \equiv 0 \mod p^2$, as desired. □

6. Almost purity

We conclude with 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 [5] and by Scholze in [7]. More precisely, (ii) 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.

We begin by defining the adjective *almost*. See [2] for more general setting.

Definition 6.1. *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.*

Theorem 6.2. *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.*

(a) The ring S also satisfies condition (ii).
(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 $\operatorname{Hom}_{R_p}(S_p, R_p)$.

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

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

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 $\psi^{-1}(\mathfrak{o}_A)$ 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

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

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 $y \in R[p^{-1}]$ 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 $\mathfrak{o}_A/(\psi(x_1)^{p-1})$. 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 $z^p \equiv y \mod p\mathfrak{o}_A$. 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 $\psi : S_p \to B$. By [5, 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 [5, Remark 2.3.14], for $\mathfrak{m}_B = \{x \in B : |x| < 1\}$, we have $\psi^{-1}(\mathfrak{m}_B) \subset S$.

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 $S/(x_1, p)$; by arguing as before (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 [5, Theorem 5.5.9] or [7]. □

Corollary 6.3. *For R and S as in Theorem 6.2, $\Omega_{S/R} = 0$.*

Proof. Since $S[p^{-1}]$ is finite étale over $R[p^{-1}]$, $\Omega_{S/R}$ is killed by p^n for some nonnegative integer n. If $n > 0$, then for each $x \in S$ we may apply Theorem 6.2 to write $x = y^p + pz$. Then $dx = py^{p-1}\,dy + p\,dz$ is also killed by p^{n-1}. By induction, it follows that we may take $n = 0$, proving the claim. □

Remark 6.4. *Note that the proof of Theorem 6.2 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 6.2 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).*

Acknowledgements

The authors thank Laurent Berger, 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(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] Luc Illusie. Complexe de de Rham-Witt et cohomologie cristalline. *Annales scientifiques de l'Ecole Normale Superieure*, 12(4):501–661, 1979.

[4] Kiran S. Kedlaya. Power series and p-adic algebraic closures. *Journal of Number Theory*, 89(2):324–339, 2001.

[5] Kiran S. Kedlaya and Ruochuan Liu. Relative p-adic Hodge theory, I: Foundations. 2011. `http://math.mit.edu/~kedlaya/papers/`.

[6] Bjorn Poonen. Maximally complete fields. *Enseign. Math. (2)*, 39(1-2):87–106, 1993.

[7] 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`

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