A JACOBIAN CRITERION FOR NONSINGULARITY IN MIXED CHARACTERISTIC

MELVIN HOCHSTER AND JACK JEFFRIES

ABSTRACT. We give a version of the usual Jacobian characterization of the defining ideal of the singular locus in the equal characteristic case: the new theorem is valid for essentially affine algebras over a complete local algebra over a mixed characteristic discrete valuation ring. The result makes use of the minors of a matrix that includes a row coming from the values of a p-derivation. To study the analogue of modules of differentials associated with the mixed Jacobian matrices that arise in our context, we introduce and investigate the notion of a *perivation*, which may be thought of, roughly, as a linearization of the notion of p-derivation. We also develop a mixed characteristic analogue of the positive characteristic Γ-construction, and apply this to give additional nonsingularity criteria.

1. INTRODUCTION

The Jacobian criterion is a familiar tool for finding the singular locus of a finitely generated algebra over a perfect field. In general, the Jacobian criterion computes the smooth locus of a morphism. Since a finitely generated algebra over a perfect field is smooth if and only if it is regular, the singular locus can be computed in this way. For $\mathbb{Z}$-algebras and rings of mixed characteristic, regularity cannot be characterized in terms of smoothness, and thus the singular locus is not computed by the usual Jacobian criterion.

In this paper, we give a Jacobian type criterion for nonsingularity in mixed characteristic. Our criterion describes the singular locus in terms of minors of matrices involving partial derivatives and p-derivations (in the sense of Buium [3] and Joyal [9]) of the generators. We recall the definition of p-derivation in Section 2 below; as an example, if V is the p-adic integers, and $T = V[x_1, \ldots, x_n]$ or $V[[x_1, \ldots, x_n]]$, the map δ given by

$$f(x_1, \ldots, x_n) \mapsto (f(x_1^p, \ldots, x_n^p) - f(x_1, \ldots, x_n)^p)/p$$

is a p-derivation.

Theorem A (Theorem 4.9). *Let V be a discrete valuation ring with uniformizer $p \in \mathbb{Z}$. Let T be a polynomial ring over a power series ring over V in n variables*

(polynomial and power series variables) $x_1, \ldots, x_n$ *total. Let* $R := T/I$ *for some ideal* $I = (f_1, \ldots, f_a)T$ *of pure height* h. *Then, for a prime* $\mathfrak{q}$ *of* R *containing* p, *the local ring* $R_\mathfrak{q}$ *is nonsingular if and only if* $\mathfrak{q}$ *does not contain the* $h \times h$ *minors of the matrix with columns*

- $[\delta(f_1), \ldots, \delta(f_a)]^T$, *for some* p-*derivation mod* p^2 *on* V *extended to* T,
- $\left[\left(\frac{\partial f_1}{\partial x_i} \right)^p, \ldots, \left(\frac{\partial f_a}{\partial x_i} \right)^p \right]^T$, *for* $i = 1, \ldots, n$,
- $\left[\left(\frac{\partial f_1}{\partial \lambda} \right)^p, \ldots, \left(\frac{\partial f_a}{\partial \lambda} \right)^p \right]^T$, *for* $\lambda \in \Lambda$ *for a* p-*base* Λ *of* K.

Note that for primes that do not contain p, $R_\mathfrak{q}$ is nonsingular if and only if $\mathfrak{q}$ does not contain the $h \times h$ minors of the usual Jacobian matrix.

We remark also that any choice of δ, any choice of Λ, and any choice of generators $f_1, \ldots, f_a$ for I, and any presentation $R \cong T/I$ with T as above is valid for the result above.

The use of p-derivations to study singularities is motivated by [4], where p-derivations were used to extend a classical theorem of Zariski and Nagata on symbolic powers. In fact, Theorem A in the special case of a principal ideal I follows from the main result of [4].

The cokernel of the classical Jacobian matrix is just the module of Kähler differentials. In the case of algebras over a perfect field, the Jacobian criterion characterizes the regular locus as the locus on which the module of Kähler differentials is free of the "correct" rank. Theorem A admits a similar interpretation along these lines. Given a ring A with a p-derivation δ and an A-algebra R, we define a module $\widetilde{\Omega}_{R|A}$; in the situation of Theorem A, this is just the cokernel of the matrix that appears in the statement. This module represents a functor of maps that satisfy simple functional identities analogous to derivations or p-derivations; we call these maps *perivations*, and the module $\widetilde{\Omega}_{R|A}$ the *universal perivation module*. In this language, we obtain the following version of Theorem A.

Theorem B (Theorem 4.12)**.** *Let* V *be a discrete valuation ring with uniformizer* $p \in \mathbb{Z}$ *and F-finite residue field (i.e., the Frobenius map on* V/pV *is of finite index). Let* $(R, \mathfrak{m}, k)$ *a local ring with* $p \in \mathfrak{m}$ *that is essentially of finite type over a complete* V-*algebra.*

The local ring R *is regular if and only if* $\widetilde{\Omega}_{R|\mathbb{Z}}$ *is free of rank* $\dim(R) + \log_p[k : k^p]$.

In equal characteristic $p > 0$, the notion of Γ-construction allows one to eliminate F-finiteness hypotheses from various statements; for an algebra R essentially of finite type over a complete local ring, there is an F-finite faithfully flat purely inseparable extension R^Γ that preserves many of the properties of R. In Section 5 below, we recall key properties of the Γ-construction, and develop a mixed characteristic analogue that we call the $\widetilde{\Gamma}$-construction with many of the same properties. Using the $\widetilde{\Gamma}$-construction, we state a version of Theorem B without any F-finiteness hypothesis.

Theorem C (Corollary 5.10)**.** *Let* V *be a discrete valuation ring with uniformizer* $p \in \mathbb{Z}$. *Let* $(R, \mathfrak{m}, k)$ *a local ring with* $p \in \mathfrak{m}$ *that is essentially of finite type over a complete* V-*algebra. Let* $\widetilde{\Lambda}$ *be a lift to* V *of a* p-*base for* V/pV.

The local ring R is regular if and only if, for sufficiently small cofinite $\widetilde{\Gamma} \subseteq \widetilde{\Lambda}$, $\widetilde{\Omega}_{R^{\widetilde{\Gamma}}|\mathbb{Z}}$ is free of rank $\dim(R) + \log_p[k(R^{\widetilde{\Gamma}}) : k(R^{\widetilde{\Gamma}})^p]$, where $k(R^{\widetilde{\Gamma}})$ denotes the residue field of $R^{\widetilde{\Gamma}}$.

A preliminary version of these results, namely Theorem A in the case of finitely generated unmixed algebras over complete unramified discrete valuation rings with perfect residue fields, was announced in the MSRI Fellowship of the Ring Seminar in May 2020. Our original method was based on the argument in Subsection 4.2. These results were extended to the complete case and the essentially-of-finite-type-over-complete case by a Néron-Popsecu desingularization [1, 16] argument in an earlier version of this manuscript, along with a version of Theorem B in the corresponding cases. In the meanwhile, we learned of the work of Saito [14], who established the analogue of Theorem B with the additional hypotheses that R/pR is essentially of finite type over an F-finite field and that R is flat over $\mathbb{Z}_{(p)}$. After learning of Saito's results, we used some of his ideas to give a different argument for Theorems A and B that does not require any hypotheses on V/pV, and that does not require the use of Néron-Popsecu desingularization to address the cases where R is complete or essentially of finite type over a complete ring. We have kept the original argument for the affine case here in Subsection 4.2 for heuristic reasons.

We note that the universal perivation modules defined here appear as modules of FW-differentials in [14], as total p^2-differentials in [5], and implicitly as an extension class in [17, §4.2]; they are also closely related to the construction in [6, 9.6.12].

2. p-DERIVATIONS AND PERIVATIONS

2.1. **p-derivations.** We recall first the notions of p-derivation and δ-ring, in the sense of Buium [3] and Joyal [9].

Notation 2.1. For a prime integer p, we set

$$C_p(X, Y) := \frac{X^p + Y^p - (X+Y)^p}{p} = -\sum_{i=1}^{p-1} \frac{\binom{p}{i}}{p} X^i Y^{p-i} \in \mathbb{Z}[X, Y].$$

More generally, we set

$$C_p(X_1, \ldots, X_t) := \frac{X_1^p + \cdots + X_t^p - (X_1 + \cdots + X_t)^p}{p}$$

$$= -\sum_{\substack{a_1 + \cdots + a_t = p \\ a_1, \ldots, a_t \neq p}} \frac{\binom{p}{a_1, \ldots, a_t}}{p} X_1^{a_1} \cdots X_t^{a_t} \in \mathbb{Z}[X_1, \ldots, X_t].$$

For all p, we have

(♣) $C_p(X, Y) \in (XY)\mathbb{Z}[X, Y]$ and $C_p(X_1, \ldots, X_t) \in (X_1, \ldots, X_t)^2 \mathbb{Z}[X_1, \ldots, X_t]$.

Definition 2.2. Let R be a ring, and p a prime integer. A map $\delta : R \to R$ is a *p-derivation* if, for all $x, y \in R$, we have

    (1) $\delta(0) = \delta(1) = 0$,
    (2) $\delta(x + y) = \delta(x) + \delta(y) + C_p(x, y)$, and
    (3) $\delta(xy) = x^p \delta(y) + y^p \delta(x) + p\delta(x)\delta(y)$.

A *δ-ring* is a pair (R, δ), where R is a ring, and δ is a p-derivation on R.

Note that if δ is a p-derivation, then

$$(\diamondsuit) \qquad \delta(x_1 + \cdots + x_t) = \delta(x_1) + \cdots + \delta(x_t) + C_p(x_1, \ldots, x_t).$$

If (R, δ) is a δ-ring, then the map

$$\Phi : R \to R \qquad \Phi(r) = r^p + p\delta(r)$$

is a ring homomorphism, and if $p \in R$ is not a unit, then the diagram

$$
\begin{array}{ccc}
R & \xrightarrow{\ \Phi\ } & R \\
\downarrow & & \downarrow \\
R/pR & \xrightarrow{\ F\ } & R/pR
\end{array}
$$

commutes, where F is the Frobenius map on R/pR; we call the map Φ the *lift of Frobenius* on (R, δ). Conversely, if p is a nonzerodivisor on R, and Φ is a ring endomorphism of R for which the previous diagram commutes, then the map

$$\delta : R \to R \qquad \delta(r) = \frac{\Phi(r) - r^p}{p}$$

is a p-derivation.

We note a few rings on which p-derivations exist:

Example 2.3.   (1) On $\mathbb{Z}$, for any p, the identity map is the unique lift of Frobenius, and $\delta(n) = \frac{n - n^p}{p}$ is the unique p-derivation.

(2) Similarly, on the ring of p-adic integers $V = \widehat{\mathbb{Z}_{(p)}}$, the identity map is the unique lift of Frobenius, and $\delta(n) = \frac{n - n^p}{p}$ is the unique p-derivation.

(3) Generalizing the last example, the ring of Witt vectors $W(k)$ over a field k of positive characteristic admits a p-derivation.

(4) Any lift of Frobenius Φ on a ring R extends to a lift of Frobenius $\tilde{\Phi}$ on $R[x_1, \ldots, x_n]$ by setting $\tilde{\Phi}(x_i) = x_i^p + pf_i$ for arbitrary elements $f_i \in R[x_1, \ldots, x_n]$.

(5) Any lift of Frobenius Φ on a p-adically complete ring R extends to a lift of Frobenius $\tilde{\Phi}$ on $R[[x_1, \ldots, x_n]]$ by setting $\tilde{\Phi}(x_i) := x_i^p + pf_i$ for arbitrary elements $f_i \in R[[x_1, \ldots, x_n]]$, since $R[[x_1, \ldots, x_n]]$ is complete with respect to $(p, x_1, \ldots, x_n)$.

Remark 2.4. Let δ be a p-derivation on R.

(1) If δ maps a set of generators of an ideal $\mathfrak{a}$ of R into $\mathfrak{a}' \supseteq \mathfrak{a}$, then δ maps $\mathfrak{a}$ into $\mathfrak{a}'$.

(2) If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals of R such that δ maps $\mathfrak{a}$ into $\mathfrak{a}' \supseteq \mathfrak{a}$ and δ maps $\mathfrak{b}$ into $\mathfrak{b}' \supseteq \mathfrak{b}$ then δ maps $\mathfrak{a}\mathfrak{b}$ into $\mathfrak{a}'\mathfrak{b}'$.

(3) If δ maps a set of generators of an ideal $\mathfrak{A}$ of R into $\mathfrak{a}' \supseteq \mathfrak{a}$, then δ maps $\mathfrak{a}^k$ into $\mathfrak{a}'^k$ for every positive integer k.

(4) If $\mathfrak{a}$ is an ideal containing p, then δ maps $\mathfrak{a}^{k+1}$ into $\mathfrak{a}^k$ for all $k \in \mathbb{N}$.

(5) If $\mathfrak{a} \subseteq \mathfrak{a}'$ are ideals with $\delta(\mathfrak{a}) \subseteq \mathfrak{a}'$ and $r \equiv s$ modulo $\mathfrak{a}$, then $\delta(r) \equiv \delta(s)$ modulo $\mathfrak{a}'$.

(6) If $p \in \mathfrak{a}$, $k \in \mathbb{N}$, and $r \equiv s$ modulo $\mathfrak{a}^{k+1}$, then $\delta(r) \equiv \delta(s)$ mod $\mathfrak{a}^k$.

(7) For any element $r \in R$, $\delta(pr) \equiv r^p$ modulo pR.

(8) For $r_1, \ldots, r_n \in R$, $\delta(r_1 \cdots r_n) \equiv \sum_{i=1}^{n}(\prod_{j \neq i} r_j^p)\delta(r_i)$ modulo pR. Hence, for any $r \in R$, $\delta(r^p) \equiv 0$ modulo pR.

Proof. Parts (1) and (2) are straightforward consequences of (♣), (♢), and part (3) of Definition 2.2. Part (3) follows from (1) and (2) by induction. For (4), we induce on k, with the base case $k = 1$ trivial. Take a generating set $a_1, \ldots, a_t$ for $\mathfrak{a}$ and a generating set $c_1, \ldots, c_s$ for $\mathfrak{a}^k$, so $\mathfrak{a}^{k+1}$ is generated by elements of the form $a_i c_j$. Then $\delta(a_i c_j) = a_i^p \delta(c_j) + c_j^p \delta(a_i) + p\delta(a_i)\delta(c_j) \in \mathfrak{a}^k$ by the induction hypothesis. Part (5) is immediate from part (1) of Definition 2.2 and (♣). Part (6) follows from (4) and (5). Part (7) follows from part (3) of Definition 2.2 and $\delta(p) = 1 - p^{p-1}$. Part (8) follows from part (3) of Definition 2.2 by a straightforward induction on n. $\qquad\square$

We refer the reader to [2, §2] for some basic properties of δ-rings, and [2, §3] for connections between the theory of δ-rings and perfectoid spaces.

2.2. Derivations of inseparability.

We briefly recall some basics of derivations in positive characteristic. We refer the reader to [13, Section 36] for the facts below. A *p-base* of a field K of positive characteristic is a set of elements $\Lambda \subset K$ such that $\{\lambda_1^{a_1} \cdots \lambda_t^{a_t} \mid \lambda_1, \ldots, \lambda_t \in \Lambda, 0 \leq a_1, \ldots, a_t < p\}$ forms a K^p-basis for K. Such a set exists, by an application of Zorn's Lemma, and the cardinality of any two p-bases for a field K are equal.

Given a p-base Λ for a field K, one obtains a derivation for each element $\lambda_0 \in \Lambda$: explicitly, $\frac{\partial}{\partial \gamma_{\lambda_0}}$ is the K^p-linear map that maps $\lambda_0^{a_0} \lambda_1^{a_1} \cdots \lambda_t^{a_t}$ to $a_0 \lambda_0^{a_0-1} \lambda_1^{a_1} \cdots \lambda_t^{a_t}$ for all $\lambda_1, \ldots, \lambda_t \in \Lambda \smallsetminus \{\lambda_0\}$, $0 \leq a_0, a_1, \ldots, a_t < p$.

The module of differentials of K has a K-vector space basis $\{d\lambda \mid \lambda \in \Lambda\}$ such that the dual element in $\mathrm{Hom}_K(\Omega_K, K)$ to $d\lambda_0$ is $\frac{\partial}{\partial \gamma_{\lambda_0}}$.

2.3. p-derivations modulo p^2.

Definition 2.5. We say that a map $\delta : R/p^2 R \to R/pR$ is a *p-derivation mod p^2* on R if δ satisfies the axioms (1)-(3) of Definition 2.2.

A *mod p^2 δ-ring* is a pair (A, δ), where δ is a p-derivation mod p^2 on A.

We note that the conclusions of Remark 2.4 also hold for a p-derivation mod p^2, since we may apply these statements to $R/p^2 R$.

If $R/p^2 R$ is flat over $\mathbb{Z}/p^2\mathbb{Z}$, e.g., if p is a regular element on R, then p-derivations mod p^2 are in bijection with lifts of Frobenius to $R/p^2 R$. By Remark 2.4, any p-derivation induces a p-derivation mod p^2. However, existence of a p-derivation mod p^2 is less stringent than existence of a p-derivation. This follows from the following lemma and subsequent example.

Lemma 2.6. *Let (A, δ) be a δ-ring, with p a regular element on A, and let S be a smooth A-algebra. Then there exists a p-derivation mod p^2 on S that extends δ.*

Proof. Let Ψ be the lift of Frobenius associated to A. There is a commutative diagram

$$
\begin{array}{ccccc}
S & \longrightarrow & S/pS & \xrightarrow{F} & S/pS \\
\uparrow & & & & \uparrow \\
A & \xrightarrow{\Phi} & A & \longrightarrow & S/p^2 S.
\end{array}
$$

By smoothness, there is a ring homomorphism $S \to S/p^2 S$ that makes the diagram commute; such a map is a lift of Frobenius mod p^2. $\qquad\square$

On the other hand, we note:

Example 2.7. Let

$$V = \widehat{\mathbb{Z}_{(p)}}, \ p \neq 2, 3, \ A = V[y], \text{ and } R = \frac{A[x]_{2x+y}}{(x^2 + yx + p)}.$$

Note that R is a standard étale extension of A. To extend the p-derivation δ on A that sends y to 0, we need $g \in R$ such that $x \mapsto x^p + pg, y \mapsto y^p$ yields a V-algebra homomorphism. For this, we need $(x^p + pg)^2 + y^p(x^p + pg) + p = 0$ in R. That is, g must be a solution of

$$p^2 g^2 + (2px^p + py^p)g + (x^{2p} + y^p x^p + p) = 0$$

in R. In the fraction field of R, we may apply the quadratic formula to obtain

$$g = \frac{-(2px^p + py^p) \pm p\sqrt{y^{2p} - 4p}}{2p^2} = \frac{-(2x^p + y^p) \pm \sqrt{y^{2p} - 4p}}{2p}.$$

Since g must be in R, $\sqrt{y^{2p} - 4p} \in R$. We will show that this is false. First note that $B = A[x]/(x^2 + yx + p) = A[\theta]$ where $\theta = (-y + \sigma)/2$ and σ is a square root of $y^2 - 4p$. Then $B = A[\sigma]$, since 2 is a unit in V. Since A is a UFD and $y^2 - 4p$ is squarefree in A, B is normal. Hence, if $y^{2p} - 4p$ has a square root in the fraction field of B (which contains R), it has a square root in B, and this will have the form $a_0 + a_1 \sigma$, with each $a_i \in A$. Since $B = A \oplus A\sigma$, it is clear that $(a_0 + a_1\sigma)^2$ is not in B unless $a_1 = 0$ or $a_2 = 0$. We cannot have $a_1 = 0$, since $y^{2p} - 4p$ is not a square in A. We cannot have $a_2 = 0$, or else $y^{2p} - 4p = a_1^2(y^2 - 4p)$. This is a contradiction, since substituting $y^2 = 4p$ in $y^{2p} - 4p$ does not yield 0: its value is $(4p)^p - 4p \neq 0$. We conclude that no such g exists, and hence no such extension of δ exists.

We now aim to show that any DVR with uniformizer p admits a p-derivation modulo p^2. Our construction is a variation on Saito [14, Lemma 1.3.1] in the case of a perfect residue field. We require a lemma first.

Lemma 2.8. *For any ring R, prime integer p, and elements $x, y \in R$,*

$$(x + y)^{p^2} + pC_p(x, y)^p \equiv x^{p^2} + y^{p^2} \mod p^2 R.$$

Proof. We have $(x + y)^{p^2} = \sum_{i+j=p^2} \binom{p^2}{i} x^i y^j$. By Kummer's Theorem [10] p^2 divides $\binom{p^2}{i}$ unless p divides i, so we have $(x+y)^{p^2} \equiv \sum_{i+j=p} \binom{p^2}{pi} x^{pi} y^{pj} \mod p^2 R$. We have that $\binom{pn}{pm} \equiv \binom{n}{m} \mod p^2 \mathbb{Z}$, (cf. [15, Exercise 1.6(c)]), so

$$(x + y)^{p^2} \equiv \sum_{i+j=p} \binom{p}{i} x^{pi} y^{pj}$$

$$\equiv x^{p^2} + y^{p^2} - pC_p(x^p, y^p)$$

$$\equiv \sum_{i+j=p} \binom{p}{i} x^{pi} y^{pj}$$

$$\equiv x^{p^2} + y^{p^2} - pC_p(x, y)^p$$

modulo $p^2 R$.   □

Proposition 2.9. *Let (V, pV, K) be a discrete valuation ring with uniformizer p. Let $\{\gamma_\lambda \mid \lambda \in \Lambda\}$ be a set of elements in V that maps bijectively to a p-base for K. Then the map*

$$\psi\left(\sum_{\substack{\alpha\in\mathbb{Z}^{\oplus\Lambda} \\ 0\le\alpha_\lambda<p}} a_\alpha^p \gamma^\alpha + pb\right) = \sum_{\substack{\alpha\in\mathbb{Z}^{\oplus\Lambda} \\ 0\le\alpha_\lambda<p}} a_\alpha^{p^2} \gamma^{p\alpha} + pb^p$$

is a lift of Frobenius modulo p^2 on V. Hence, the map $\delta : V \to K$ given by $\delta(f) = \frac{\psi(f)-f^p}{p}$ is a p-derivation modulo p^2 on V.

Proof. First, we show that the map ψ is well-defined. We have that $V/pV = \bigoplus_{\alpha\in\mathbb{Z}^\Lambda, 0\le\alpha_\lambda<p}(V/pV)^p\overline{\gamma^\alpha}$, so any element in V can be written as a finite sum $\sum a_\alpha^p \gamma^\alpha + pb$ for some elements $a_\alpha, b \in V$. If

$$\sum_{\substack{\alpha\in\mathbb{Z}^{\oplus\Lambda} \\ 0\le\alpha_\lambda<p}} a_\alpha^p \gamma^\alpha + pb = \sum_{\substack{\alpha\in\mathbb{Z}^{\oplus\Lambda} \\ 0\le\alpha_\lambda<p}} c_\alpha^p \gamma^\alpha + pd,$$

then $\sum_{\alpha\in\mathbb{Z}^\Lambda, 0\le\alpha_\lambda<p}(a_\alpha^p - c_\alpha^p)\gamma^\alpha \in pV$, so each $a_\alpha^p - c_\alpha^p \in pV$ by K^p-linear independence of the images of the elements γ_λ, and hence $a_\alpha - c_\alpha \in pV$ by injectivity of the Frobenius on K. Substituting back, we have that $p(b - d) \in \sum_{\alpha\in\mathbb{Z}^\Lambda, 0\le\alpha_\lambda<p}((a_\alpha + pe_\alpha^p) - a_\alpha^p)\gamma^\alpha$ for some elements $e_\alpha \in V$, and hence this is in p^2V. Since p is a regular element on V, $b - d \in pV$ as well. Well-definedness of the map is then evident.

We check now that ψ is additive. We have

$$\psi\left(\sum a_\alpha^p \gamma^\alpha + pb + \sum c_\alpha^p \gamma^\alpha + pd\right)$$
$$= \psi\left(\sum\left((a_\alpha + c_\alpha)^p + pC_p(a_\alpha, c_\alpha)\right)\gamma^\alpha + p(b+d)\right)$$
$$= \psi\left(\sum(a_\alpha + c_\alpha)^p\gamma^\alpha + p(b+d+\sum C_p(a_\alpha, c_\alpha)\gamma^\alpha)\right)$$
$$= \sum(a_\alpha + c_\alpha)^{p^2}\gamma^{p\alpha} + p(b+d+\sum C_p(a_\alpha, c_\alpha)\gamma^\alpha)^p$$
$$\equiv \sum(a_\alpha^{p^2} + c_\alpha^{p^2})\gamma^{p\alpha} + p(b^p + d^p)$$
$$= \psi\left(\sum a_\alpha^p \gamma^\alpha + pb\right) + \psi\left(\sum c_\alpha^p \gamma^\alpha + pd\right),$$

where the equivalence in the penultimate line is modulo p^2V, using the previous lemma and the fact that $p(X + Y + Z)^p \equiv p(X^p + Y^p + Z^p)$ modulo p^2.

The verification of multiplicativity modulo p^2V is straightforward, and omitted. $\square$

Combining this with Example 2.3, we obtain:

Corollary 2.10. *Let V be a discrete valuation ring with uniformizer $p \in \mathbb{Z}$. Any polynomial ring in arbitrarily many variables, power series ring in finitely many variables, or polynomial ring over a power series ring in finitely many variables over V admits a p-derivation mod p^2. Explicitly, one may take a p-derivation mod p^2 as constructed in Proposition 2.9 and extend by prescribing arbitrary values to the variables.*

Indeed, by parts (4) and (5) of Example 2.3 and the previous proposition, there is a p-derivation modulo p^2 on $\widehat{V}[[x]][y]$, for a finite set of variables x and an arbitrary set of variables y. Since we have canonical isomorphisms $\widehat{V}[[x]][y]/p^i\widehat{V}[[x]][y] \cong V[[x]][y]/p^iV[[x]][y]$ for $i = 1, 2$, such a map can be identified with a p-derivation modulo p^2 on $V[[x]][y]$.

2.4. **Perivations.** In this subsection, we discuss the notion of *perivation*, which is essentially the same as that of *total p-derivations* in the sense of Dupuy, Katz, Rabinoff, and Zureick-Brown [5], and the notion of FW-derivation of Saito [14].

Definition 2.11 (cf. [5, Definition 2.1.1])**.** Let R be a ring, and p a prime integer. Let M be an R/pR-module. A map $\alpha : R \to M$ is a *perivation* if for all $x, y \in R$, we have

(1) $\alpha(0) = \alpha(1) = 0$,
(2) $\alpha(x + y) = \alpha(x) + \alpha(y) + C_p(x, y)\alpha(p)$, and
(3) $\alpha(xy) = x^p\alpha(y) + y^p\alpha(x)$.

We call $\alpha(p)$ the *distinguished element* of α. If additionally, (A, δ) is a mod p^2 δ-ring, with A a subring of R, and

(4) $\alpha(a) = \delta(a)\alpha(p)$ for all $a \in A$,

then we say α is a *perivation over A*.

Example 2.12. If (R, δ) is a mod p^2 δ-ring, then the composition $R \xrightarrow{\delta} R \twoheadrightarrow R/pR$ is a perivation with distinguished element 1. More generally, if M is an R/pR-module, and $t \in M$, then the map $R \xrightarrow{\delta} R \xrightarrow{\cdot t} M$ is a perivation with distinguished element t; in this setting, we call a perivation of this form *trivial*. Thus, condition (4) above says that the restriction of α to A is trivial.

Example 2.13. Given a ring R, consider the ring homomorphism β given as the composition $R \twoheadrightarrow R/pR \xrightarrow{F} R/pR$, where F is the Frobenius map. If R/pR is considered as an R-algebra via β, then any derivation of R into an R/pR-module is a perivation with distinguished element zero. Conversely, a perivation to an (R/pR)-module with distinguished element zero is a derivation (with respect to β). We call such a map a *derivation of the Frobenius* for short. We write $\operatorname{Der}^F_{R|A}(M)$ for the collection of A-linear derivations of the Frobenius from R into an (R/pR)-module M.

If R has characteristic p, then for any perivation, we have $\alpha(p) = \alpha(0) = 0$, so a perivation is just a derivation of the Frobenius.

Remark 2.14. Any perivation on a ring R is a perivation over $\mathbb{Z}$. Indeed, the unique p-derivation on $\mathbb{Z}$ is given by the rule $\delta(n) = (n - n^p)/p$, and by a simple induction, we have $\alpha(n) = n\alpha(1) + C_p(1, \ldots, 1)\alpha(p) = (n - n^p)/p \cdot \alpha(p)$. Thus, we lose no generality by restriction to the relative setting of perivations over a δ-ring; we may take $\mathbb{Z}$ as the base ring.

We record a few basic observations on perivations.

Remark 2.15. (1) If M is an R/pR-module, then the collection of perivations from R to M admits a natural R/pR-module structure by postmultiplication, and likewise for perivations over a mod p^2 δ-ring A. We denote these modules by $\operatorname{Per}_R(M)$ and $\operatorname{Per}_{R|(A,\delta)}(M)$, respectively.

(2) If $\alpha : R \to M$ is a perivation, and $\phi : M \to N$ is an R-module homomorphism, then $\phi \circ \alpha$ is a perivation, as is readily verified from the definition.

Discussion 2.16 (p-linear maps and the Peskine-Szpiro functor). Recall that if R is a ring of prime characteristic $p > 0$, a map η between two R-modules M and N is *p-linear* if it is additive and $\eta(rm) = r^p \eta(m)$ for all $r \in R$ and $m \in M$. If $F : R \to R$ is the Frobenius map on R, let $^1(-) : R-\mathrm{mod} \to R-\mathrm{mod}$ be the functor of restriction of scalars through F, and $F_R(-) : R-\mathrm{mod} \to R-\mathrm{mod}$ be the functor of extension of scalars through F.

A map $\eta : M \to N$ is p-linear if and only $\eta : M \to {}^1N$ is R-linear. By Hom-tensor adjunction, there is a natural isomorphism

$$\mathrm{Hom}_R(M, {}^1N) \cong \mathrm{Hom}_R(F_R(M), N)$$
$$\eta \mapsto \big((r \otimes m) \mapsto r\eta(m)\big);$$

thus, we can identify p-linear maps from M to N with R-linear maps $F_R(M) \to N$. By abuse of notation, we will use the same name for maps we identify in this way.

Lemma 2.17. *Let (A, δ) be a mod p^2 δ-ring, R be an A-algebra, and I be an ideal of R. Let $\alpha : R \to M$ be a perivation over A.*

(1) *α descends to a well-defined perivation $\bar{\alpha} : R/(I^2 + pI) \to M/IM$.*
(2) *The restriction of $\bar{\alpha}$ to $I/(I^2 + pI) \to M/IM$ is a p-linear map over R/pR.*
(3) *If $\alpha(I) \subseteq IM$, then α descends to a perivation $\alpha' : R/I \to M/IM$.*
(4) *If $IM = 0$, then there is a natural bijection between perivations from R/I to M and perivations from R to M that map I to 0.*

Proof. For part (1), let $r \in R$, and $a_0, a_1, \ldots, a_t, a_1', \ldots, a_t' \in I$. Then

$$\alpha(r + pa_0 + \sum_i a_i a_i') = \alpha(r) + \alpha(pa_0) + \alpha(\sum_i a_i a_i') + C_p(r, pa_0, \sum_i a_i a_i')\alpha(p)$$

$$= \alpha(r) + \alpha(pa_0) + \sum_i \alpha(a_i a_i') + C_p(r, pa_0, \sum_i a_i a_i')\alpha(p) + C_p(a_1 a_1', \ldots, a_t a_t')\alpha(p).$$

Since $C_p(r, pa_0, \sum_i a_i a_i')$ and $C_p(a_1 a_1', \ldots, a_t a_t')$ lie in $I + (p)$, we have, modulo IM,

$$\alpha(r + pa_0 + \sum_i a_i a_i') \equiv \alpha(r) + \alpha(pa_0) + \sum_i \alpha(a_i a_i')$$

$$\equiv \alpha(r) + p^p \alpha(a_0) + a_0^p \alpha(p) + \sum_i a_i'^p \alpha(a_i) + \sum_i a_i^p \alpha(a'_i) \equiv \alpha(r).$$

For part (2), we note that

$$\alpha(ra_0) = r^p \alpha(a_0) + a_0^p \alpha(r) \equiv r^p \alpha(a_0) \quad \text{modulo } IM.$$

Part (3) is clear. For part (4), we note first that given a perivation from R/I to M, the map from R to M obtained by precomposing with the quotient map is a perivation from R to M that maps I to 0. Conversely, by part (3), a perivation from R to an R/I-module that sends I to 0 factors through the quotient map. $\square$

In particular, any perivation $R \to M$ factors through R/p^2R.

3. Universal perivation modules

In this subsection, we study universal objects for perivations.

Definition 3.1. Let (A, δ) be a mod p^2 δ-ring, and R be an A-algebra. We say that a perivation $\alpha : R \to M$ is a *universal perivation over A* and M is a *universal perivation module over A* if for any perivation $\beta : R \to N$ over A there is a unique R-module homomorphism $\phi : M \to N$ such that $\beta = \phi \circ \alpha$. We will write $\tilde{d}_{R|(A,\delta)} : R \to \widetilde{\Omega}_{R|(A,\delta)}$ for a universal perivation.

In particular, for a universal perivation module $\widetilde{\Omega}_{R|(A,\delta)}$, there are natural isomorphisms $\mathrm{Per}_{R|(A,\delta)}(M) \cong \mathrm{Hom}_R(\widetilde{\Omega}_{R|(A,\delta)}, M)$ for all R-modules M.

Universal perivations for $A = \mathbb{Z}$ were constructed in [5] (where universal perivation modules are called *total p-differentials*), and were used there to study existence of p-derivations on $\mathbb{Z}/p^2\mathbb{Z}$-algebras. In particular they always exist; a construction for these modules appears below. These modules appear in [14] as modules of FW-differentials; many of the properties established below also appear there. They also appear implicitly in the work of Zdanowicz [17, §4.2] on existence of lifts of Frobenius / p-derivations on $\mathbb{Z}/p^2\mathbb{Z}$-algebras, and are related to a construction of Gabber and Romero [6, 9.6.12].

In this section, we record some basic properties of universal perivations. Many of these results overlap with [5] and [14].

By uniqueness of representing objects (i.e., Yoneda's Lemma), universal perivation modules are unique up to natural isomorphism. Moreover, if $\phi : R \to S$ is an A-algebra homomorphism, and M is an S/pS-module, we obtain a map

$$\mathrm{Per}_{S|(A,\delta)}(M) \to \mathrm{Per}_{R|(A,\delta)}(M)$$
$$\alpha \mapsto \alpha \circ \phi$$

which induces the natural map

$$\widetilde{\Omega}_{R|(A,\delta)} \xrightarrow{\tilde{d}_\phi} \widetilde{\Omega}_{S|(A,\delta)}.$$

We record some analogues of the fundamental sequences for differentials.

Proposition 3.2 (First fundamental sequences). *(1) Let (A, δ) be a mod p^2 δ-ring. Let $R \xrightarrow{\phi} S$ be an A-algebra homomorphism. Then there is a natural exact sequence*

$$S \otimes_R \widetilde{\Omega}_{R|(A,\delta)} \to \widetilde{\Omega}_{S|(A,\delta)} \to F_{S/pS}(\Omega_{S/pS|R/pR}) \to 0.$$

(2) Let $(A, \delta) \to (B, \varepsilon)$ be a mod p^2 δ-ring homomorphism (i.e., a ring homomorphism ψ such that $\psi \circ \delta = \varepsilon \circ \psi$), and $B \to R$ be a ring homomorphism. Then there is a natural exact sequence

$$R \otimes_B F_{B/pB}(\Omega_{B/pB|A/pA}) \to \widetilde{\Omega}_{R|(A,\delta)} \to \widetilde{\Omega}_{R|(B,\varepsilon)} \to 0.$$

Proof.   (1) First, we claim that there are natural exact sequences

$$0 \to \mathrm{Der}^F_{S/pS|R/pR}(M) \to \mathrm{Per}_{S|(A,\delta)}(M) \to \mathrm{Per}_{R|(A,\delta)}(M)$$

for S/pS-modules M. We have the first inclusion, since $\mathrm{Der}^F_{S/pS|R/pR}(M)$ is naturally isomorphic to $\mathrm{Der}^F_{S|R}(M)$, and the latter naturally embeds as a subset in $\mathrm{Per}_{S|(A,\delta)}(M)$. For exactness in the middle, we need to see that a perivation that vanishes on R is an R-linear derivation of the Frobenius.

For such a perivation, the distinguished element is 0 (since $p \in R$), so it is a derivation of Frobenius, and the claim is then clear.

Now, since $\mathrm{Hom}_S(S \otimes_R \widetilde{\Omega}_{R|(A,\delta)}, M) \cong \mathrm{Hom}_R(\widetilde{\Omega}_{R|(A,\delta)}, \mathrm{Hom}_S(S, M)) \cong \mathrm{Per}_{R|(A,\delta)}(M)$ and $\mathrm{Hom}_{S|(A,\delta)}(F_{S/pS}(\Omega_{S/pS|R/pR})) \cong \mathrm{Der}^F_{S|R}(M)$ for all S/pS-modules M, by Yoneda's Lemma, there is a complex as in the statement, which must be exact.

(2) Along the same lines, it suffices to show that for every R/pR-module M we have an exact sequence

$$0 \to \mathrm{Per}_{R|(B,\varepsilon)}(M) \to \mathrm{Per}_{R|(A,\delta)}(M) \to \mathrm{Der}^F_{B|A}(M).$$

For the map $\mathrm{Per}_{R|(A,\delta)}(M) \to \mathrm{Der}^F_{B|A}(M)$, we send a perivation α to the map $\beta = \alpha - \alpha(p)\varepsilon$. One verifies immediately that this is an A-linear derivation of the Frobenius on B, and that β is zero if and only if α restricted to B is a trivial perivation. $\qquad \square$

Remark 3.3. As a particular case of the first fundamental sequence, when $R = A$, we have

$$S/pS \to \widetilde{\Omega}_{S|A} \to F_{S/pS}(\Omega_{S/pS|A/pA}) \to 0.$$

This exact sequence was considered in [5] and implicitly in [17] in connection with existence of lifts of Frobenius / p-derivations modulo p^2. In particular, this sequence is split exact if and only if δ extends to a p-derivation mod p^2 on R: such a map is a splitting from $\widetilde{\Omega}_{S|(A,\delta)} \to S/pS$.

Proposition 3.4 (Second fundamental sequence)**.** *Let (A, δ) be a mod p^2 δ-ring. Let R be an A-algebra, and I an ideal of R. Then there is a natural exact sequence*

$$F_{R/(I+pR)}(I/I^2 + pI) \to R/I \otimes_R \widetilde{\Omega}_{R|(A,\delta)} \to \widetilde{\Omega}_{(R/I)|(A,\delta)} \to 0.$$

Proof. For the first map above, we consider the perivation given as the composition:

$$R \xrightarrow{\tilde{d}_R} \widetilde{\Omega}_{R|(A,\delta)} \twoheadrightarrow R/I \otimes_R \widetilde{\Omega}_{R|(A,\delta)};$$

by Lemma 2.17 (2), this induces a p-linear map from $I/(I^2+pI)$ to $R/I \otimes_R \widetilde{\Omega}_{R|(A,\delta)}$, which by Discussion 2.16, yields the map above.

Observe that if M is an $R/(I + pR)$-module, then

$$\mathrm{Per}_{R|(A,\delta)}(M) \cong \mathrm{Hom}_R(\widetilde{\Omega}_{R|(A,\delta)}, M) \cong \mathrm{Hom}_R(R/I \otimes_R \widetilde{\Omega}_{R|(A,\delta)}, M).$$

Thus, along the same lines as the proof of Proposition 3.2, it suffices to show that we have natural exact sequences

$$0 \to \mathrm{Per}_{R/I|(A,\delta)}(M) \to \mathrm{Per}_{R|(A,\delta)}(M) \to \mathrm{Hom}_{R/I}(F_{R/(I+pR)}(I/(I^2 + pI)), M)$$

for all $R/(I + pR)$-modules M. By Lemma 2.17 (4), any nonzero perivation of R/I into M pulls back to a nonzero perivation of R into M, so exactness holds at the first nonzero spot. A perivation of R into M maps to zero in $\mathrm{Hom}_{R/I}(F_{R/(I+pR)}(I/(I^2 + pI)), M)$ exactly if its restriction to I is zero; by Lemma 2.17 (4), this happens if and only if it is the image of a perivation from R/I to M. $\qquad \square$

We note that by [14, Proposition 2.4], if $(R, \mathfrak{m}, k)$ is local, with k of characteristic $p > 0$, and $A = \mathbb{Z}$, the second fundamental sequence

$$F_k(\mathfrak{m}/\mathfrak{m}^2) \to k \otimes_R \widetilde{\Omega}_{R|(\mathbb{Z},\delta)} \to \widetilde{\Omega}_{k|(\mathbb{Z},\delta)} \to 0$$

is split-exact.

Our next goal is to give a construction of universal perivation modules.

Construction 3.5. *Let (A, δ) be a mod p^2 δ-ring. Let T be an A-algebra with*

   (1) ε, a p-derivation mod p^2 on T extending δ, and

   (2) $\{t_\lambda\} \subset T$ such that $\{dt_\lambda \mid \lambda \in \Lambda\}$ form a free basis for $\Omega_{T/pT|A/pA}$.

Let $\{\partial_\lambda \mid \lambda \in \Lambda\}$ be the dual basis to $\{dt_\lambda\}$ in $\mathrm{Der}_{T/pT|A/pA}(T/pT)$.

   We set $\widetilde{\Omega}_{T|(A,\delta)}$ to be the free T/pT-module with basis $\{\tilde{d}p\} \cup \{\tilde{d}t_\lambda \mid \lambda \in \Lambda\}$. Let $\tilde{d}_{T|(A,\delta)} : T \to \widetilde{\Omega}_{T|(A,\delta)}$ be the perivation given by

$$\tilde{d}_{T|(A,\delta)}(t) = \varepsilon(t)\tilde{d}p + \sum_{\lambda \in \Lambda} (\partial_\lambda(t))^p \tilde{d}t_\lambda.$$

Note that since this is a sum of a p-derivation mod p^2 and derivations of the Frobenius, it is indeed a perivation.

Proposition 3.6. *In the setting of Construction 3.5, the map $\tilde{d}_{T|(A,\delta)}$ is a universal perivation, and $\widetilde{\Omega}_{T|(A,\delta)}$ is a universal perivation module.*

Proof. For any T/pT-module M, and any collection $\{m_p\} \cup \{m_\lambda \mid \lambda \in \Lambda\}$ of elements of M, there is a unique T/pT-module homomorphism $\varphi : \widetilde{\Omega}_{T|(A,\delta)} \to M$ such that the composition $\varphi \circ \tilde{d}_T$ is a perivation that sends p to m_p and t_λ to m_λ. Thus, it suffices to show that any perivation is uniquely determined by its values on p and $\{t_\lambda \mid \lambda \in \Lambda\}$.

To see this, let α be a perivation, and let $\beta = \alpha - \alpha(p)\varepsilon$. Then β is a derivation of the Frobenius, so we can write $\beta = \gamma \circ d_{T/pT|A/pA}$, where $d_{T/pT|A/pA}$ is the universal derivation $T/pT \to \Omega_{T/pT|A/pA}$, and γ is p-linear. As γ is determined by its values on $\{dt_\lambda \mid \lambda \in \Lambda\}$, β is determined by its values on $\{t_\lambda \mid \lambda \in \Lambda\}$, as required. $\square$

Remark 3.7. Construction 3.5 applies in the following settings:

   (1) Let $T = A[\{x_\lambda \mid \lambda \in \Lambda\}]$ be a polynomial ring in an arbitrary set of variables over A. Then, for $\widetilde{\Omega}_{T|(A,\delta)}$, we may take $\{t_\lambda\}$ to be the set of variables, and $\{\partial_\lambda\} = \{\frac{\partial}{\partial x_\lambda}\}$ for $\widetilde{\Omega}_{T|(A,\delta)}$.

   (2) Let $T = V[\{x_\lambda \mid \lambda \in \Lambda\}]$ be a polynomial ring in an arbitrary set of variables over a discrete valuation ring V with uniformizer p. Then, for $\widetilde{\Omega}_{T|(\mathbb{Z},\delta)}$, we may take $\{t_\lambda\}$ to be $S_1 \cup S_2$, where S_1 is the set of variables, and $S_2 = \{\gamma_\lambda\}$ is a set of elements of V that maps bijectively to a p-base for V/pV. Then $\{\partial_\lambda\} = D_1 \cup D_2$, where D_1 is the set of derivations of the form $\frac{\partial}{\partial x_\lambda}$, and D_2 is the set of derivations $\{\frac{\partial}{\partial \gamma_\lambda}\}$ obtained from the p-base.

   (3) Let $T = V[[x_1, \ldots, x_n]][y_1, \ldots, y_m]$ be a polynomial ring over power series ring over a discrete valuation ring with uniformizer p. Then, as in the previous case, for $\widetilde{\Omega}_{T|(\mathbb{Z},\delta)}$, we may take $\{t_\lambda\}$ to be the union of the variables (both power series and polynomial) and a lift of a p-base, and $\{\partial_\lambda\}$ to be the union of the derivations with respect to the variables and the derivations induced by the p-base.

Construction 3.8. *Let (A, δ) be a δ-ring, and R be an A-algebra. Let T be an A-algebra with $R = T/I$ for some ideal I, and*

   (1) ε, a p-derivation mod p^2 on T extending δ, and

   (2) $\{t_\lambda\} \subset T$ such that $\{dt_\lambda \mid \lambda \in \Lambda\}$ form a free basis for $\Omega_{T/pT|A/pA}$;

such a T always exists by Remark 3.7. Let $\{\partial_\lambda \mid \lambda \in \Lambda\}$ be the dual basis to $\{dt_\lambda\}$ in $\mathrm{Der}_{T/pT\lfloor A/pA}(T/pT)$.

We set $\widetilde{\Omega}_{R\mid(A,\delta)}$ to be the quotient of the free R/pR-module P_R with basis $\{\tilde{d}p\} \cup \{\tilde{d}t_\lambda \mid \lambda \in \Lambda\}$ by the submodule N of elements of the form

$$\{\varepsilon(a)\tilde{d}p + \sum_{\lambda \in \Lambda}(\partial_\lambda(a))^p\tilde{d}t_\lambda \mid a \in I\};$$

note that N is generated by the set of elements of this form as a varies though any generating set of I.

Let $\tilde{d}_{R\mid(A,\delta)} : R \to \widetilde{\Omega}_{R\mid(A,\delta)}$ be the perivation given by

$$\tilde{d}_{R\mid(A,\delta)}(r) = \varepsilon(r)\tilde{d}p + \sum_{\lambda \in \Lambda}(\partial_\lambda(r))^p\tilde{d}t_\lambda.$$

Proposition 3.9. *In the context of Construction 3.8, the map $\tilde{d}_{R\mid(A,\delta)}$ is a universal perivation, and $\widetilde{\Omega}_{R\mid(A,\delta)}$ is a universal perivation module.*

Proof. This follows from Propositions 3.6 and 3.4. □

We note also:

Lemma 3.10. *Let (A,δ) be a mod p^2 δ-ring.*

(1) If $R = \varinjlim_\lambda R_\lambda$ is a direct limit of A-algebras, then $\widetilde{\Omega}_{R\mid(A,\delta)} = \varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$.

(2) If $W \subseteq R$ is multiplicatively closed, then $\widetilde{\Omega}_{W^{-1}R\mid(A,\delta)} = W^{-1}\widetilde{\Omega}_{R\mid(A,\delta)}$.

Proof. (1) One can construct a universal perivation from R to $\varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$ using the universal properties. Namely, since the direct limits $\varinjlim_\lambda R_\lambda$ and $\varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$ can be computed at the level of sets, there is a canonical function $\varinjlim_\lambda R_\lambda \to \varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$; since any pair of elements $x, y \in R$ are in the image of some R_λ, and the canonical map from $R_\lambda \to \varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid A}$ satisfies the conditions of Definition 2.11, the canonical map $\varinjlim_\lambda R_\lambda \to \varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$ does as well. Now, given a perivation from R to M, we obtain a consistent system of perivations from R_λ to M which induces a unique consistent system of R_λ-linear homomorphisms from $\widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$ to M. This induces a unique factorization through $\varinjlim_\lambda \widetilde{\Omega}_{R_\lambda\mid(A,\delta)}$.

(2) Since we can write $W^{-1}R = \varinjlim_{f\in W} R_f$, it suffices to check for principal localizations. Moreover, using the second fundamental sequence, it suffices to check for the case of a polynomial ring. In this case, we can apply Construction 3.8 to the polynomial ring with one extra variable t modulo a relation of the form $ft - 1$ and verify directly. □

Remark 3.11. Since formation of $\widetilde{\Omega}$ commutes with localization, Construction 3.5 is valid for localizations of polynomial rings over power series rings over unramified discrete valuation rings.

4. JACOBIAN CRITERION

4.1. **Theorem A.** In this section, we prove Theorem A from the introduction.

Definition 4.1. Let (V, pV, K) be an unramified discrete valuation ring of mixed characteristic $(0, p)$. Let T be a polynomial ring over a power series ring over V with n total variables $x_1, \ldots, x_n$ of both types combined, and let δ be a p-derivation mod p^2 on T; cf. Corollary 2.10. We allow m or n to be zero. Fix a sequence of elements $\{\gamma_\lambda\}$ of V that map bijectively to a p-base of K.

For a sequence of elements $\boldsymbol{f} = (f_1, \ldots, f_a)$ in R, the *mixed Jacobian matrix* of $\boldsymbol{f}$ is the matrix $\widetilde{J}(\boldsymbol{f})$ over T/pT with

- rows indexed by $\{f_1, \ldots, f_a\}$,
- columns indexed by $\{p\} \cup \{x_1, \ldots, x_n\} \cup \{\gamma_\lambda\}$, and
- the entry in the row indexed by f_i and column indexed by g is $\delta(f_i)$ if $g = p$, and $(\frac{\partial f_i}{\partial g})^p$ if $g \neq p$.

The maps $\partial/\partial\gamma_\lambda$ are the derivations discussed in Remark 3.7.

Remark 4.2. If (V, pV, K) is a discrete valuation ring with K perfect, then

$$\widetilde{J}(\boldsymbol{f}) = \begin{bmatrix} \delta(f_1) & (\frac{\partial f_1}{\partial x_1})^p & \cdots & (\frac{\partial f_1}{\partial x_n})^p \\ \vdots & \vdots & \ddots & \vdots \\ \delta(f_a) & (\frac{\partial f_a}{\partial x_1})^p & \cdots & (\frac{\partial f_a}{\partial x_n})^p \end{bmatrix}.$$

Remark 4.3. The mixed Jacobian matrix depends on the choice of δ and the choice of a p-base for K, although these are suppressed from the notation. However, the cokernel of the matrix $\widetilde{J}(\boldsymbol{f})$ considered as a matrix over $T/(p, \boldsymbol{f})T$, is isomorphic to the module $\widetilde{\Omega}_{T|(\mathbb{Z},\delta)}$ by Construction 3.8 and Remark 3.7, and thus is independent of these choices.

Definition 4.4. In the same setting as Definition 4.1, we write $J(\boldsymbol{f})$ for the classical Jacobian matrix, with

- rows indexed by $\{f_1, \ldots, f_a\}$,
- columns indexed by $\{x_1, \ldots, x_n\}$, and
- the entry in the row indexed by f_i and column indexed by g is $\frac{\partial f_i}{\partial g}$.

Discussion 4.5. We briefly discuss the notion of module of Kähler differentials for quotients of polynomial rings over power series rings that we will need for primes not containing p in Theorem 4.9. We refer the reader to the book of Kunz [12] for more details on the notions discussed here; see also [8] for a concise treatment of these notions.

Let (V, pV, K) be a complete discrete valuation ring, S a power series ring over V, and T a polynomial ring over S, and $\mathfrak{p}$ a prime ideal of T. Then, there is a *universally finite derivation* $\partial : S \to \Omega'_{S|V}$: a derivation such that for any finitely generated S-module M and derivation ζ, there is a unique S-module homomorphism ϕ such that $\zeta = \phi \circ \partial$. There is a *universal extension* $\hat{\partial} : T_\mathfrak{p} \to \Omega_{T_\mathfrak{p}|\partial}$ of ∂: for every T-module M and S-module homomorphism $\omega : \Omega'_{S|V} \to M$ and derivation $\sigma : T \to M$ such that the restriction of σ to R is $\omega \circ \partial$, σ factor through $\hat{\partial}$ compatibly with the other maps.

By [12, Proposition 4.22], we can identify $\Omega_{T_\mathfrak{p}|\partial}$ with $(\Omega_{T|\partial})_\mathfrak{p}$, and by [12, Formula 4.11(b) and Example 12.7], we can realize $\Omega_{T|\partial}$ as a free module with basis given by dx_i for each variable x_i, and $\hat{\partial} : T \to \Omega_{T|\partial}$ as $\hat{\partial}(f) = \sum_i \frac{\partial f}{\partial i}$.

Lemma 4.6. *Let (V, pV, K) be a complete discrete valuation ring with uniformizer $p \in \mathbb{Z}$, and T be a polynomial ring over a power series ring over V in n variables*

$x_1, \ldots, x_n$ total. Let I be an ideal of R, with generating set $\boldsymbol{f} = (f_1, \ldots, f_a)$, and let $\mathfrak{p}$ be a prime of R containing I, but not containing p. Then, the $\kappa(\mathfrak{p})$-vector space dimension of the image of I in $\mathfrak{p}/\mathfrak{p}^2$ is equal to the rank of the Jacobian matrix $J(\boldsymbol{f})$ considered as a matrix in $\kappa(\mathfrak{p})$.

Proof. In the notation of Discussion 4.5 by [12, Proposition 13.14], the map $\mathfrak{p}/\mathfrak{p}^2 \to \Omega_{T_\mathfrak{p}|\partial} \otimes_T \kappa(\mathfrak{p})$ induced by $\hat{\partial}$ is injective. By Discussion 4.5, we can identify this with the map $\Omega_{T_\mathfrak{p}|\partial} \otimes_T \kappa(\mathfrak{p})$ with $\Omega_{T|\partial} \otimes_T \kappa(\mathfrak{p})$. Thus,

$$\dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(I \to \mathfrak{p}/\mathfrak{p}^2) \right) = \dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(I \to \Omega_{T|\partial} \otimes_T \kappa(\mathfrak{p})) \right).$$

By Discussion 4.5, this image is the $\kappa(\mathfrak{p})$-subspace of $\Omega_{T|\partial} \otimes_T \kappa(\mathfrak{p})$ generated by the rows of the classical Jacobian matrix (with free basis for $\Omega_{T|\partial} \otimes_T \kappa(\mathfrak{p})$ as in Discussion 4.5). $\qquad\square$

Applying the universal perivation modules, we obtain a similar result for primes that contain p.

Lemma 4.7. *Let (V, pV, K) be a discrete valuation ring with uniformizer $p \in \mathbb{Z}$, and T be a polynomial ring over a power series ring over V in n variables $x_1, \ldots, x_n$ total. Let I be an ideal of R, with generating set $\boldsymbol{f} = (f_1, \ldots, f_a)$, and let $\mathfrak{p}$ be a prime of R containing I and p. Let δ be a p-derivation modulo p^2 on T; such a δ exists by Corollary 2.10. Then, the $\kappa(\mathfrak{p})$-vector space dimension of the image of I in $\mathfrak{p}/\mathfrak{p}^2$ is equal to the rank of the mixed Jacobian matrix $\widetilde{J}(\boldsymbol{f})$ considered as a matrix in $\kappa(\mathfrak{p})$.*

Proof. By [14, Proposition 2.4], the map $F_{\kappa(\mathfrak{p})}(\mathfrak{p}/\mathfrak{p}^2) \to \widetilde{\Omega}_{T_\mathfrak{p}|(\mathbb{Z},\delta)} \otimes_T \kappa(\mathfrak{p})$ induced by the universal perivation on $T_\mathfrak{p}$ is injective. Since the formation of the universal perivation module commutes with localization, we may identify this with the map $\rho : F_{\kappa(\mathfrak{p})}(\mathfrak{p}/\mathfrak{p}^2) \to \widetilde{\Omega}_{T|\mathbb{Z}} \otimes_T \kappa(\mathfrak{p})$ induced by the universal perivation on T. Thus,

$$\begin{aligned}
\dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(I \to \mathfrak{p}/\mathfrak{p}^2) \right) &= \dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(I/(\mathfrak{p}^2 \cap I) \to \mathfrak{p}/\mathfrak{p}^2) \right) \\
&= \dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(F_{\kappa(\mathfrak{p})}(I/(\mathfrak{p}^2 \cap I)) \to F_{\kappa(\mathfrak{p})}(\mathfrak{p}/\mathfrak{p}^2)) \right) \\
&= \dim_{\kappa(\mathfrak{p})} \left(\mathrm{im}(F_{\kappa(\mathfrak{p})}(I/(\mathfrak{p}^2 \cap I)) \to \widetilde{\Omega}_{T|\mathbb{Z}} \otimes_T \kappa(\mathfrak{p})) \right),
\end{aligned}$$

where the map on the second line is induced from the previous map by applying the Frobenius functor, and the last map is obtained from the previous map by postcomposing with the map ρ. It remains only to note that, by Construction 3.5, the image of this map is the $\kappa(\mathfrak{p})$-subspace of $\widetilde{\Omega}_{T|(\mathbb{Z},\delta)} \otimes_T \kappa(\mathfrak{p})$ generated by the rows of the mixed Jacobian matrix (given a compatible choice of free basis for $\Omega_{T/pT|\mathbb{Z}/p\mathbb{Z}}$ in Construction 3.5 and p-base in Definition 4.1). $\qquad\square$

We will also need the following fact.

Proposition 4.8. *Let $V \to W$ be a local map of discrete valuation rings of mixed characteristic p, and let B denote a local V-algebra such that B has maximal ideal $pB + \mathfrak{b}$ and is complete with respect to $\mathfrak{b}$. Let $C = W \widehat{\otimes}_V^{\mathfrak{b}} B$ be the completion of $W \otimes_V B$ with respect to the image of $\mathfrak{b}$. Then $C[1/p]$ is geometrically regular over $B[1/p]$. In particular, if $x_1, \ldots, x_d$ are indeterminates, the $V[[x_1, \ldots, x_d]][1/p] \to W[[x_1, \ldots, x_d]][1/p]$ is geometrically regular.*

Proof. It suffices to prove geometrically regular when B has the special form $A = V[[x_1, \ldots, x_d]]$: one may then get the general case by a base change from a suitable

choice of A to B. Flatness is obvious in the case of A, even if we do not localize at p. We are in equal characteristic 0, and so it suffices to show that the fiber of $B \to C$ over a prime $\mathfrak{q}$ not containing p is regular. Thus, we may replace B by $B/\mathfrak{q}$, and we only need to consider the generic fiber. We change notation and use B for the base domain. We may extend p to a system of parameters $u_1, \ldots, u_h$ for $\mathfrak{m}_B$ where the $u_j \in \mathfrak{b}$. Then we may map a new choice of A, namely, $V[[x_1, \ldots, x_h]]$, to B as an V-algebra so that $x_1, \ldots, x_h$ map to $u_1, \ldots, u_h$, using the completeness of B with respect to $\mathfrak{b}$. Then B is module-finite over this choice of A, and the problem of proving geometric regularity reduces to checking regularity the generic fiber for this choice of A, i.e., for $V[[x_1, \ldots, x_h]] \to W[[x_1, \ldots, x_h]]$. This is obvious since the target ring is now regular. $\qquad\square$

Theorem 4.9. *Let (V, pV, k) be a DVR with uniformizer p and T be a polynomial ring over a power series ring over V in n variables $x_1, \ldots, x_n$ total. Let $I = (f_1, \ldots, f_a)T$ be an ideal of pure height h in T, and $R = T/I$. Then, for a prime $\mathfrak{p}$ of R,*

(1) If $p \notin \mathfrak{p}$, then $R_{\mathfrak{p}}$ is regular if and only if the image of the ideal $I_h(J(\boldsymbol{f}))$ of $h \times h$ minors of the classical Jacobian matrix $J(\boldsymbol{f})$ is not contained in $\mathfrak{p}$;

(2) If $p \in \mathfrak{p}$, then $R_{\mathfrak{p}}$ is regular if and only if the image of the ideal $I_h(\widetilde{J}_T(\boldsymbol{f}))$ of $h \times h$ minors of the mixed Jacobian matrix $\widetilde{J}(\boldsymbol{f})$ is not contained in $\mathfrak{p}$.

Proof. In the first case, we note that by Proposition 4.8, we can reduce to the case where V is complete. Indeed, the map from R to $\widehat{V} \widehat{\otimes}_V^{\mathfrak{b}} R$, where $\mathfrak{b}$ is the ideal generated by the power series variables, is geometrically regular after inverting p, so the singular locus of the source expands to the singular locus of the target; the classical Jacobian matrix is also the same for both rings.

Then, we compute

$$\mu = \dim_{\kappa(\mathfrak{p})}(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2 R_{\mathfrak{p}}) - \dim(R_{\mathfrak{p}}).$$

We observe that $\dim(R_{\mathfrak{p}}) = \mathrm{ht}(\mathfrak{p}) - h$ and

$$\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2 R_{\mathfrak{p}}) = \dim_{\kappa(\mathfrak{p})}(\mathfrak{p}/\mathfrak{p}^2) - \dim_{\kappa(\mathfrak{p})}(\mathrm{im}(I \to \mathfrak{p}/\mathfrak{p}^2)).$$

Using Lemma 4.6 and regularity of $R_{\mathfrak{p}}$, we have that $\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2 R_{\mathfrak{p}})$ is equal to $\dim(R_{\mathfrak{p}})$ minus the rank of the classical Jacobian matrix $J(\boldsymbol{f})$ considered as a matrix over $\kappa(\mathfrak{p})$. Thus,

$$\mu = h - \mathrm{rank}(J(\boldsymbol{f})_{\kappa(\mathfrak{p})}).$$

Thus, $R_{\mathfrak{p}}$ is regular if and only if $\mu = 0$, which happens if and only if the rank of $J(\boldsymbol{f})$ considered as a matrix over $\kappa(\mathfrak{p})$ is equal to h, and this in turn happens if and only if $\mathfrak{p}$ does not contain the $h \times h$ minors of $J(\boldsymbol{f})$.

In the latter case, we proceed similarly. In this case, we use Lemma 4.7 to conclude that $\dim_{\kappa(\mathfrak{p})}(\mathfrak{p}R_{\mathfrak{p}}/\mathfrak{p}^2 R_{\mathfrak{p}})$ is equal to $\dim(R_{\mathfrak{p}})$ minus the rank of the mixed Jacobian matrix $\widetilde{J}(\boldsymbol{f})$ considered as a matrix over $\kappa(\mathfrak{p})$. Thus,

$$\mu = h - \mathrm{rank}(\widetilde{J}(\boldsymbol{f})_{\kappa(\mathfrak{p})}),$$

and $R_{\mathfrak{p}}$ is regular if and only if the rank of $\widetilde{J}(\boldsymbol{f})$ considered as a matrix over $\kappa(\mathfrak{p})$ is equal to h, which in turn happens if and only if $\mathfrak{p}$ does not contain the $h \times h$ minors of $J(\boldsymbol{f})$. $\qquad\square$

Example 4.10. Let $R = \dfrac{\mathbb{Z}[x]}{x^2 - n} \cong \mathbb{Z}[\sqrt{n}]$ for $n \in \mathbb{Z}$ a squarefree nonunit. Set $f = x^2 - n$. For p prime, we take $\widetilde{J}(f) = \begin{bmatrix} \delta_p(f) & (2x)^p \end{bmatrix}$, where δ_p is the unique p-derivation on $\mathbb{Z}$ extended to $\mathbb{Z}[x]$ via $\delta_p(x) = 0$. Observe that

$$\delta_p(x^2 - n) = \delta_p(-n) - C_p(x^2, n) \in \delta_p(-n) + (x).$$

For p odd,

$$\begin{aligned}
\mathcal{V}_R(p, I_1(\widetilde{J}(f))) &\cong \mathcal{V}_{\mathbb{Z}[x]}(p, \delta_p(f), (2x)^p, x^2 - n) = \mathcal{V}_{\mathbb{Z}[x]}(p, \delta_p(f), x, x^2 - n) \\
&= \mathcal{V}_{\mathbb{Z}[x]}(p, \delta_p(f), x, n) \cong \mathcal{V}_{\mathbb{Z}}(p, n, \delta_p(-n)).
\end{aligned}$$

If $p \nmid n$, this is empty since $(p, n) = \mathbb{Z}$. If $p \mid n$, since $p^2 \nmid n$, we have $p \nmid \delta_p(-n)$, so this locus is empty again.

For $p = 2$,

$$\begin{aligned}
\mathcal{V}_R(p, I_1(\widetilde{J}(f))) &\cong \mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(f), (2x)^p, x^2 - n) \\
&= \mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(f), x^2 - n) = \mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(-n) + nx^2, x^2 - n).
\end{aligned}$$

If $n \equiv 1 \bmod 4$, then $\delta_2(-n) = -\frac{n^2 + n}{2}$ is odd, so

$$\mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(-n) + nx^2, x^2 - n) = \mathcal{V}_{\mathbb{Z}[x]}(2, x^2 - 1)$$

is nonempty, corresponding to the singular maximal ideal $(2, \sqrt{n} - 1) \subset R$.

If $n \equiv 2 \bmod 4$, then $\delta_2(-2) = -3$ is odd, so

$$\mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(-n) + nx^2, x^2 - n) = \mathcal{V}_{\mathbb{Z}[x]}(2, 1, x^2)$$

is empty. If $n \equiv 3 \bmod 4$, then $\delta_2(-n)$ is even, so

$$\mathcal{V}_{\mathbb{Z}[x]}(2, \delta_2(-n) + nx^2, x^2 - n) = \mathcal{V}_{\mathbb{Z}[x]}(2, x^2, x^2 - 1)$$

is empty. Of course, this agrees with the basic number theory fact that for a squarefree nonunit n, $\mathbb{Z}[\sqrt{n}]$ is integrally closed in its fraction field (and equivalently regular, as R is a one-dimensional domain) if and only if $n \not\equiv 1 \bmod 4$.

4.2. **Elementary proof.** We now provide a concrete self-contained proof of Theorem A in the affine case. For simplicity, we assume that the residue field of the base discrete valuation ring is algebraically closed, though the perfect case follows easily.

Theorem 4.11. *Let (V, pV, K) be an unramified discrete valuation ring of mixed characteristic. Assume that K is algebraically closed. Let $T = V[x_1, \ldots, x_n]$, and δ be a p-derivation mod p^2 on T extending the p-derivation mod p^2 on V. Let $I = (f_1, \ldots, f_a)$ be an ideal of pure height h in T, and $R = T/I$. Let $\mathfrak{p}$ be a prime ideal of R with $p \in \mathfrak{p}$.*

Then, the mixed Jacobian matrix $\widetilde{J}(\boldsymbol{f})$ considered in $\kappa(\mathfrak{p})$ has rank at most h, and equality holds if and only if $R_{\mathfrak{p}}$ is regular.

Proof. First, we consider the case where $\mathfrak{p}$ is a maximal ideal $\mathfrak{m}$. Let $\mathfrak{n}$ be the preimage of $\mathfrak{m}$ in T. It follows from the Nullstellensatz that the image of $\mathfrak{n}$ in T/pT is of the form $(x_1 - a_1, \ldots, x_n - a_n)$ for some $a_1, \ldots, a_n \in K$, so $\mathfrak{n}$ is of the form $\mathfrak{n} = (p, x_1 - v_1, \ldots, x_n - v_n)$ for some $v_1, \ldots, v_n \in V$ with $v_i = a_i + pV$, and $f_j(v_1, \ldots, v_n) \in pV$ for $j = 1, \ldots, a$.

We aim to compute the dimension of $\mathfrak{m}/\mathfrak{m}^2$ as a K-vector space. To this end, there is a short exact sequence

$$0 \to \frac{I}{\mathfrak{n}^2 \cap I} \to \frac{\mathfrak{n}}{\mathfrak{n}^2} \to \frac{\mathfrak{m}}{\mathfrak{m}^2} \to 0,$$

so $R_\mathfrak{m}$ is regular if and only if the K-vector space dimension of $I/(\mathfrak{n}^2 \cap I)$ is equal to $\dim(T_\mathfrak{n}) - \dim(R_\mathfrak{m})$. Since $T_\mathfrak{n}$ is catenary, and I each minimal prime of I has the same height, we have that $\dim(T_\mathfrak{n}) - \dim(R_\mathfrak{m}) = \mathrm{ht}(IT_\mathfrak{n}) = h$ for $\mathfrak{n} \supseteq I$.

Write $\tilde{x}_i = x_i - v_i$ for $i = 1, \ldots, n$, so that $\mathfrak{n} = (p, \tilde{x}_1, \ldots, \tilde{x}_n)$. Using Taylor's formula, for each f_j, we get

$$f_j = \sum_{(\alpha_1,\ldots,\alpha_n)} \frac{\partial^{\alpha_1+\cdots+\alpha_n} f_j}{\partial x_1^{\alpha_1} \cdots \partial x_n^{\alpha_n}}(v_1,\ldots,v_n)\tilde{x}_1^{\alpha_1} \cdots \tilde{x}_n^{\alpha_n}$$

$$\equiv f_j(v_1,\ldots,v_n) + \sum_{i=1}^n \frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i \mod \mathfrak{n}^2.$$

By Remark 2.4(6) we then have

$$\delta(f_j) \equiv \delta\left(f_j(v_1,\ldots,v_n) + \sum_{i=1}^n \frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i\right) \mod \mathfrak{n}.$$

Since $f_j(v_1,\ldots,v_n) \in pV \subseteq \mathfrak{n}$, we have

$$C_p\left(\delta(f_j(v_1,\ldots,v_n)), \delta\left(\sum_{i=1}^n \frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i\right)\right) \in \mathfrak{n},$$

so

$$\delta(f_j) \equiv \delta\left(f_j(v_1,\ldots,v_n) + \sum_{i=1}^n \frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i\right) \mod \mathfrak{n}.$$

Likewise, since $\tilde{x}_i \in \mathfrak{n}$, $C_p(\{\frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i\}) \in \mathfrak{n}$, and hence

$$\delta(f_j) \equiv \delta(f_j(v_1,\ldots,v_n)) + \sum_{i=1}^n \delta\left(\frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\tilde{x}_i\right) \mod \mathfrak{n}.$$

By the product rule for p-derivations, we then have

$$\delta(f_j) \equiv \delta(f_j(v_1,\ldots,v_n)) + \sum_{i=1}^n \left(\frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\right)^p \delta(\tilde{x}_i) \mod \mathfrak{n}.$$

Note that, for $\alpha \in V$, by Remark 2.4(7), if we write $f_j(v_1,\ldots,v_n) \equiv p\alpha \mod p^2V$, we obtain that $\delta(f_j(v_1,\ldots,v_n)) \equiv \alpha^p$ in $K = V/pV$. Thus,

$$\alpha \equiv \overline{\delta(f_j)}^{1/p} - \sum_i \frac{\partial f_j}{\partial x_i}(v_1,\ldots,v_n)\overline{\delta(\tilde{x}_i)}^{1/p} \mod \mathfrak{n}.$$

Therefore, the K-linear expression for $[f_j] \in \mathfrak{n}/\mathfrak{n}^2$ in terms of the basis

$$[p], [\tilde{x}_1 - p\overline{\delta(\tilde{x}_1)}^{1/p}], \ldots, [\tilde{x}_n - p\overline{\delta(\tilde{x}_n)}^{1/p}]$$

is

$$[f_j] = \overline{\delta(f_j)(v)}^{1/p}[p] + \overline{\frac{\partial f_j}{\partial x_1}}(v)[\tilde{x}_1 - p\overline{\delta(\tilde{x}_1)}^{1/p}] + \cdots + \overline{\frac{\partial f_j}{\partial x_n}}(v)[\tilde{x}_n - p\overline{\delta(\tilde{x}_n)}^{1/p}].$$

Thus, the dimension of $I/(\mathfrak{n}^2 \cap I)$ as a K-vector space is the rank of the matrix

$$
\begin{bmatrix}
\overline{\delta(f_1)(\underline{v})}^{1/p} & \overline{\frac{\partial f_1}{\partial x_1}(\underline{v})} & \cdots & \overline{\frac{\partial f_1}{\partial x_n}(\underline{v})} \\
\overline{\delta(f_2)(\underline{v})}^{1/p} & \overline{\frac{\partial f_2}{\partial x_1}(\underline{v})} & \cdots & \overline{\frac{\partial f_2}{\partial x_n}(\underline{v})} \\
\vdots & \vdots & \ddots & \vdots \\
\overline{\delta(f_a)(\underline{v})}^{1/p} & \overline{\frac{\partial f_a}{\partial x_1}(\underline{v})} & \cdots & \overline{\frac{\partial f_a}{\partial x_n}(\underline{v})}
\end{bmatrix}.
$$

Raising elements to pth powers in K does not affect which minors are zero, so the rank of the matrix above is the same as that of

$$
\begin{bmatrix}
\overline{\delta(f_1)(\underline{v})} & \overline{\frac{\partial f_1}{\partial x_1}(\underline{v})}^{p} & \cdots & \overline{\frac{\partial f_1}{\partial x_n}(\underline{v})}^{p} \\
\overline{\delta(f_2)(\underline{v})} & \overline{\frac{\partial f_2}{\partial x_1}(\underline{v})}^{p} & \cdots & \overline{\frac{\partial f_2}{\partial x_n}(\underline{v})}^{p} \\
\vdots & \vdots & \ddots & \vdots \\
\overline{\delta(f_a)(\underline{v})} & \overline{\frac{\partial f_a}{\partial x_1}(\underline{v})}^{p} & \cdots & \overline{\frac{\partial f_a}{\partial x_n}(\underline{v})}^{p}
\end{bmatrix}.
$$

This is just the image of $\widetilde{J}(\boldsymbol{f})$ in $T/\mathfrak{n} = R/\mathfrak{m}$, and thus the K-dimension of $I/(\mathfrak{n}^2 \cap I)$ is equal to the rank of $\widetilde{J}(\boldsymbol{f})$ considered in $\kappa(\mathfrak{m})$.

Since the K-vector space dimension of $I/(\mathfrak{n}^2 \cap I)$ is less than or equal to the height with equality if and only if $R_\mathfrak{m}$ is regular, the theorem is established in the case of a maximal ideal.

Now, the inequality on the rank of $\widetilde{J}(\boldsymbol{f})$ for general prime ideals follows by a basic semicontinuity argument, since maximal ideals are dense in $V_R(p)$. Likewise, the characterization of equality in terms of nonsingularity follows, since R is excellent, and so the singular locus is closed. $\qquad\square$

4.3. **Theorem B.** We now give the proof of Theorem B.

Theorem 4.12. *Let V be a discrete valuation ring with uniformizer p, and F-finite residue field. Let $(R, \mathfrak{m}, k)$ a local ring with $p \in \mathfrak{m}$ that is essentially of finite type over a complete V-algebra.*

The local ring R is regular if and only if $\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}$ is free of rank $\dim(R) + \log_p[k : k^p]$.

Proof. Let $K = V/pV$, and set $a = \log_p[K : K^p]$ and $b = \log_p[k : k^p]$. Write $R \cong (T/I)_\mathfrak{p}$, where T is a polynomial ring over a power series ring over V, and $\mathfrak{p}$ is a prime ideal of T that contains I. We observe that $\widetilde{J}(\boldsymbol{f})$ is a presentation matrix for $\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}$, with $\dim(T) + a$ generators.

First, we claim that $\dim(T) + a = \text{height}(I_\mathfrak{p}) + \dim(R) + b$. We use the formula $\log_p[\kappa(\mathfrak{q}) : \kappa(\mathfrak{q})^p] - \log_p[\kappa(\mathfrak{q}') : \kappa(\mathfrak{q}')^p] = \text{height}(\mathfrak{q}'/\mathfrak{q})$ for $\mathfrak{q} \subseteq \mathfrak{q}'$ in an F-finite ring of positive characteristic; cf., [11], [13, Lemma 42.7]. Applying this in T with the maximal ideal generated by the variables and the zero ideal, and then with $\mathfrak{p}$ and the zero ideal, we have that

$$
\dim(T) + a = \log_p[\text{frac}(T) : \text{frac}(T)^p] = \text{height}(\mathfrak{p}) + b.
$$

Since $\dim(R) = \text{height}(\mathfrak{p}) - \text{height}(I_\mathfrak{p})$, the claim holds.

Now, by the characterization of locally free modules via Fitting ideals (cf. [12, Proposition D.8]), $\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}$ is locally free of rank $\dim(R) + b$ if and only if

$$F_{\dim(R)+b}(\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}) = R \qquad \text{and} \qquad F_{<\dim(R)+b}(\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}) = 0.$$

Using the equality above and the presentation by the mixed Jacobian matrix, $\widetilde{\Omega}_{R|(\mathbb{Z},\delta)}$ is locally free of rank $\dim(R) + b$ if and only if

$$I_{\text{height}(I_\mathfrak{p})}(\widetilde{J}(\boldsymbol{f})) = R \qquad \text{and} \qquad I_{>\text{height}(I_\mathfrak{p})}(\widetilde{J}(\boldsymbol{f})) = 0.$$

Now, if $I_{\text{height}(I_\mathfrak{p})}(\widetilde{J}(\boldsymbol{f})) = R$, then by Lemma 4.6, $\dim_k(\text{im}(I_\mathfrak{p} \to \mathfrak{p}/\mathfrak{p}^2)) = \text{height}(I_\mathfrak{p})$, so $I_\mathfrak{p}$ can be generated by $\text{height}(I_\mathfrak{p})$ elements; in this case we can replace $\boldsymbol{f}$ by such a generating set and the latter condition above is automatic. Thus, $\widetilde{\Omega}_{R|\mathbb{Z}}$ is locally free of rank $\dim(R) + b$ if and only if $I_{\text{height}(I_\mathfrak{p})}(\widetilde{J}(\boldsymbol{f})) = R$, which happens if and only if $I_{\text{height}(I_\mathfrak{p})}(\widetilde{J}(\boldsymbol{f})_k) = k$, which by Lemma 4.6 again is equivalent to $\dim_k(\text{image}(I_\mathfrak{p} \to \mathfrak{p}/\mathfrak{p}^2)) = \text{height}(I_\mathfrak{p})$. But this just means that the image of I in $T_\mathfrak{p}$ is minimally generated by a regular system of parameters, so this is equivalent to nonsingularity of R. □

5. Lifting the Γ-construction to mixed characteristic

The hypothesis of Theorem B in §1 (Theorem 4.12) requires that the discrete valuation ring have an F-finite residue field. Let R be essentially of finite type over a complete local K-algebra whose residue class field is K of characteristic $p > 0$. In [7] a construction is given in terms of a p-base Λ for such a field K of characteristic p and a sufficiently small but cofinite subset Γ of Λ to give a faithfully flat purely inseparable extension of R, denoted R^Γ, such that certain properties of R are preserved by the extension, e.g., being reduced, a domain, regular, or Gorenstein F-regular. See (6.3) – (6.13) of [7]. Since $R \hookrightarrow R^\Gamma$ is purely inseparable, the prime spectra of the two rings may be identified, and if Γ is sufficiently small the singular locus is preserved. Note that certain results of [7] stated for K-algebras of finite type over a complete local K-algebra extend at once to the case of K-algebras essentially of finite type. Also note that the term "Γ-construction" is not used in [7], but has become standard in a number of papers where it has been utilized.

In this section we discuss lifting this construction to mixed characteristic, which broadens the applicability of Theorem B. Instead of working over a field K of positive prime characteristic, we work over a mixed characteristic unramified discrete valuation ring (V, pV, K). We fix a p-base Λ for K and a lifting $\widetilde{\Lambda}$ of that p-base to V. We consider a local ring B containing V complete with respect to an ideal $\mathfrak{b}$ such that $pB + \mathfrak{b}$ is the maximal ideal of B (for example, B might be $V[[x_1, \ldots, x_n]]$ whether or not V is complete) and an algebra R essentially of finite type over B. We construct a faithfully flat extension $R^{\widetilde{\Gamma}}$ of R such that the defining ideal of the singular locus in R extends to the defining ideal of the singular locus in $R^{\widetilde{\Gamma}}$ when $\widetilde{\Gamma}$ is a sufficiently small cofinite subset of $\widetilde{\Lambda}$. Moreover, $R^{\widetilde{\Gamma}}/pR^{\widetilde{\Gamma}} \cong (R/pR)^\Gamma$.

We first review the Γ-construction in characteristic p, and then discuss the mixed characteristic version.

5.1. The Γ-construction in positive prime characteristic.

Discussion 5.1. Fix a field K of positive prime characteristic p, and fix a p-base Λ for K. Let e denote an integer varying in $\mathbb{N}$. If $\lambda_1, \ldots, \lambda_n$ are elements of the p-base Λ,

then $K^{p^e}[\lambda_1, \ldots, \lambda_n]$ has degree p^{ne} over K^{p^e}, or, equivalently, $K[\lambda_1^{1/p^e}, \ldots, \lambda_n^{1/p^e}]$ has degree p^{en} over K, where the elements λ_i^{1/p^e} are taken in a suitably large algebraic field extension of K. It follows that if the z_λ are indeterminates indexed by Λ, then for any subset $\Lambda_0 \subseteq \Lambda$, $K[\lambda^{1/p^e} : \lambda \in \Lambda_0] \cong K[z_\lambda : \lambda \in \Lambda_0]/(z_\lambda^{p^e} - \lambda : \lambda \in \Lambda_0)$.

Let K and Λ be as in Discussion 5.1. In the sequel, Γ will always denote a subset of Λ, usually *cofinite* in Λ, i.e., a subset such that $\Lambda \smallsetminus \Gamma$ is finite. Let K_e^Γ denote the field extension $K[\gamma^{1/p^e} : \gamma \in \Gamma]$. If $(B, \mathfrak{m}_B)$ is a complete local K-algebra with residue class field K, let $B_e^\Gamma := K_e^\Gamma \widehat{\otimes}_K B$, where for a field extension $K \to L$, $L \widehat{\otimes}_K B$ denotes the completion of $L \otimes_K B$ with respect to $\mathfrak{m}_B(L \otimes_K B)$. If we write B as a module-finite extension of $A = K[[x_1, \ldots, x_d]]$, then $A_e^\Gamma \cong K_e^\Gamma[[x_1, \ldots, x_d]]$, $B_e^\Gamma \cong B \otimes_A A_e^\Gamma$. If R is any ring essentially of finite type over B, we define $R_e^\Gamma = R \otimes_B B_e^\Gamma$. R may also be viewed as essentially of finite type over A, and it is also correct that $R_e^\Gamma = R \otimes_A A_e^\Gamma$. Finally, we define

$$R^\Gamma := \bigcup_e R_e^\Gamma.$$

We also have

$$R^\Gamma \cong R \otimes_B B^\Gamma \cong R \otimes_A A^\Gamma.$$

In characteristic $p > 0$, we say that $R \hookrightarrow S$ is *purely inseparable* if every element in S has a p^e th power in R for some e, which may depend on the element. This implies $\mathrm{Spec}(S) \cong \mathrm{Spec}(R)$: the unique prime of S lying over P in R is the radical of PS. Note that

$$A^\Gamma = \bigcup_e K_e^\Gamma[[x_1, \ldots, x_d]]$$

is regular, with maximal ideal generated by $x_1, \ldots, x_d$, and that it is purely inseparable over A. It is shown in [7] that A^Γ is F-finite, and it follows that B^Γ and R^Γ are F-finite as well. Since A^Γ is evidently faithfully flat over A, it follows that R^Γ is faithfully flat over R in general. We summarize these facts as well as some other results proved in [7] in the next theorem.

Notation 5.2. We let $(B, \mathfrak{m}_B, K)$ be a complete local ring K-algebra, and K be a field of positive prime characteristic p, so that $K \subseteq B$ is a coefficient field. Let Λ be a fixed p-base for K, let R be an algebra essentially of finite type over B, and let Γ be a varying cofinite subset of Λ, so that $R^\Gamma := B^\Gamma \otimes_B R$ is defined.

Theorem 5.3. *Let notation be as in 5.2. Then:*
  (1) *$R^\Gamma = B^\Gamma \otimes_B R$ is an F-finite ring that is a faithfully flat purely inseparable extension of R.*
  (2) *If $(A, \mathfrak{m}_A, K)$ is a complete local K-algebra such that $A \to B$ is a local module-finite homomorphism, then $A^\Gamma \otimes_A R \cong B^\Gamma \otimes_B R = R^\Gamma$.*
  (3) *If $\Gamma \subseteq \Gamma_0$ are cofinite in Λ, then $R^\Gamma \to R^{\Gamma_0}$ is faithfully flat and purely inseparable.*
  (4) *If I is an ideal of R, then $(R/I)^\Gamma \cong R^\Gamma/IR^\Gamma$.*
  (5) *Given finitely many prime or radical ideals in R, there exists Γ_0 cofinite in Λ such that for all $\Gamma \subseteq \Gamma_0$ cofinite in Γ, the expansions of these ideals to R^Γ remain prime or reduced, respectively. In particular, if R is a domain or reduced, one can choose Γ_0 so that R^Γ is a domain or reduced, respectively, for all $\Gamma \subseteq \Gamma_0$ cofinite in Γ_0.*

For (c), note that for complete local rings of the form $A = K[[x_1, \ldots, x_n]]$, the faithful flatness of $A^\Gamma \to A^{\Gamma_0}$ is clear, and the general case follows by base change to R.

We note that part (e) reduces to the case of one prime ideal, which may be taken to be (0), since a radical ideal is a finite intersection of prime ideals, and the various choices of Γ for individual primes may be intersected. For the proof part (e), see (6.13) of [7] (the extension from finite to essentially finite algebras is immediate).

Consider a property $\mathcal{P}$ of rings (e.g., Cohen-Macaulay, Gorenstein, or regular). We are interested in the existence of Γ_0 cofinite in Λ such that for all $\Gamma \subseteq \Gamma_0$ cofinite in Γ, the locus of primes $\mathfrak{p}$ where R has property $\mathcal{P}$ is the same in R as in R^Γ. If the locus is closed and defined by $I \subseteq R$, this is equivalent to the assertion that the corresponding locus is defined by IR^Γ in R^Γ.

Discussion 5.4. Recall that if one has a flat local map $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ then S is Cohen-Macaulay if and only if both R and the closed fiber $S/\mathfrak{m}S$ are Cohen-Macaulay, in which case the type of S is the product of the types of R and $S/\mathfrak{m}S$. Moreover, if S is regular, then R is regular; cf. [13].

Theorem 5.5. *Let notation be as in 5.2. Let $\mathcal{P}$ be a property of Noetherian rings such that*

> (1) R *has $\mathcal{P}$ if and only if all of its localizations have $\mathcal{P}$.*
> (2) *If R is essentially of finite type over an excellent local ring, the locus where R has $\mathcal{P}$ is open.*
> (3) *if R to S is a flat local homomorphism and S has $\mathcal{P}$ then R has $\mathcal{P}$.*
> (4) *If R to S is a flat, purely inseparable, local homomorphism such that R has $\mathcal{P}$ and the closed fiber is a field, then S has $\mathcal{P}$.*

Then there exists a cofinite subset Γ_0 of Λ such that for all cofinite subsets $\Gamma \subseteq \Gamma_0$, the locus where R has property $\mathcal{P}$ (and, consequently, the locus where R does not have property $\mathcal{P}$) is the same as the corresponding locus for R^Γ under the identification $Spec(R) \cong Spec(R^\Gamma)$.

Hence, if the locus where R does not have $\mathcal{P}$ is Zariski closed with defining ideal I, for all $\Gamma \in \Gamma_0$ cofinite in Λ, the locus where R^Γ does not have $\mathcal{P}$ is closed and defind by IR^Γ.

In particular, this is the case if $\mathcal{P}$ is the property of being any of the following:

> (i) *regular*
> (ii) *Cohen-Macaulay*
> (iii) *Cohen-Macaulay of type at most h*
> (iv) *Gorenstein*
> (v) *Gorenstein and F-regular.*

Proof. As Γ cofinite in Λ decreases, the locus where R^Γ has $\mathcal{P}$ is ascending by Theorem 5.3(c). Since open sets in $Spec(R)$ have ACC, we can choose Γ_0 for which this locus is maximal. We claim that this choice of Γ_0 has the required property. If not, there is some prime $\mathfrak{p}$ in R corresponding to $\mathfrak{q}$ in R^{Γ_0} such that $R_\mathfrak{p}$ has property $\mathcal{P}$ by $R_Q^{\Gamma_0}$ does not. But we may choose Γ_1 cofinite in Γ_0 such that $\mathfrak{q}_1 = \mathfrak{p}R^{\Gamma_1}$ is prime. This implies that the closed fiber of the flat local map $R_\mathfrak{p} \to (R^{\Gamma_1})_{\mathfrak{q}_1}$ is a field, since $\mathfrak{q}_1 = \mathfrak{p}R^{\Gamma_1}$. Thus, the set of points of $Spec(R^{\Gamma_1})$ where $\mathcal{P}$ holds has increased strictly to contain the point Q_1 corresponding to P, contradicting the maximality of the $\mathcal{P}$ locus corresponding to Γ_0.

The fact that we may apply this result in cases (i)–(iv) follows from Discussion 5.4. In the case of (v) we need check (4). Note that in the excellent Gorenstein case, weakly F-regular and F-regular are equivalent, and in the local case it suffices to check that the ideal I generated by one system of parameters $f_1, \ldots, f_d$ is tightly closed. Let the image of u be a socle generator in $R/(f_1, \ldots, f_d)$. Since the closed fiber is a field, the image of u is a socle generator in S/IS as well. Let c be a test element in S. After replacing c by c^{p^e} we may assume that $c \in R$. If u is in the tight closure of IS then $cu^q \in (IS)^{[q]} = I^{[q]}S$ for all $q \gg 0$, and so $cu^q \in I^{[q]}S \cap R = I^{[q]}$ for all $q \gg 0$, contradicting that R is weakly F-regular. $\qquad\square$

5.2. The $\widetilde{\Gamma}$-construction in mixed characteristic.

Notation 5.6. Let (V, pV, K) be a discrete valuation ring of mixed characteristic p. Let Λ be a p-base for K, and $\widetilde{\Lambda}$ be a fixed lifting to V. We denote the by $\widetilde{\lambda}$ the element lifting $\lambda \in \Lambda$. For each subset Γ of Λ we have a corresponding set $\widetilde{\Gamma}$ in $\widetilde{\Lambda}$. We shall eventually restrict Γ to be cofinite in Λ, but this is not needed in the definitions. We assume that we have, for every $e \geq 1$, a family of indeterminates $Z_{\widetilde{\lambda}, e}$ indexed bijectively by the elements of $\widetilde{\Lambda}$. Of course, they are also in bijective correspondence with the elements of Λ. We define $V_e^{\widetilde{\Gamma}}$ to be the ring $V[Z_{\widetilde{\gamma}, e} : \widetilde{\gamma} \in \widetilde{\Gamma}]/(Z_{\widetilde{\gamma}, e}^{p^e} - \widetilde{\gamma} : \widetilde{\gamma} \in \widetilde{\Gamma})$. Note that there is a V-algebra injection of $V_e^{\widetilde{\Gamma}} \hookrightarrow V_{e+1}^{\widetilde{\Gamma}}$ that sends the image of $Z_{\widetilde{\gamma}, e}$ to the image of $Z_{\widetilde{\gamma}, e+1}^p$. We define $V^{\widetilde{\Gamma}} := \bigcup_e V_e^{\widetilde{\Gamma}}$ using these injections.

We first note:

Proposition 5.7. *All of the rings $V_e^{\widetilde{\Gamma}}$ as well as $V^{\widetilde{\Gamma}}$ are DVRs with maximal ideal generated by p. Moreover, $V_e^{\widetilde{\Gamma}}/pV_e^{\widetilde{\Gamma}} \cong K_e^{\Gamma}$, and $V^{\widetilde{\Gamma}}/pV^{\widetilde{\Gamma}} \cong K^{\Gamma}$. For $e' > e$, and $\Gamma' \supset \Gamma$, The inclusion maps among the rings*

$$(\dagger) \quad V \hookrightarrow V_e^{\widetilde{\Gamma}} \hookrightarrow V_{e'}^{\widetilde{\Gamma'}} \hookrightarrow V^{\widetilde{\Gamma'}} \hookrightarrow V^{\widetilde{\Lambda}}$$

are all free local maps.

Proof. Since the extension $V \to V_e^{\widetilde{\Gamma}}$ is integral, all maximal ideals of $V_e^{\widetilde{\Gamma}}$ must lie over pV.

Modulo $pV_e^{\widetilde{\Gamma}}$, we obtain $K[Z_{\widetilde{\gamma}}]/(Z_{\widetilde{\gamma}}^{p^e} - \gamma : \gamma \in \Gamma)$. Since the extensions of K obtained by adjoining p^e th roots of a p-base are linearly disjoint, the quotient mod $pV_e^{\widetilde{\Gamma}}$ is the field K_e^{Γ}. To show this is a DVR with maximal ideal generated by p, it suffices to show this for finite subsets of $\widetilde{\Gamma}$, and take a direct limit. But in the case where where we adjoin p^e th roots for a finite subset of Γ, we obtain a module-finite extension, free over V, which is local with maximal ideal (p), and p is not nilpotent. These hypotheses suffice to guarantee that the extension ring is a discrete valuation ring. Likewise, by a direct limit argument, $V^{\widetilde{\Gamma}}$ is a DVR with maximal ideal $pV^{\widetilde{\Gamma}}$ and residue class field K^{Γ}.

The freeness assertions for $V^{\widetilde{\Lambda}}$ over V follows because one has a free basis consisting of all monomials $\widetilde{\lambda}_{i_1}^{\alpha_1} \cdots \widetilde{\lambda}_{i_s}^{\alpha_s}$ where $\lambda_{i_1}, \ldots, \lambda_{i_s}$ are distinct, s varies, and the α_i are positive rational numbers less than 1 whose denominators are powers of p. One gets a basis for each $V^{\widetilde{\Gamma}}$ (respectively, $V_e^{\widetilde{\Gamma}}$) by using the part of the basis

involving only monomials with $\lambda_{i_j} \in \Gamma$ (respectively, and the exponents in the denominators are most p. Descriptions of the free bases in the remaining cases are left to the reader. □

Construction 5.8. *Let* $A := V[[x_1, \ldots, x_d]]$. *We let*

$$A_e^{\widetilde{\Gamma}} := V_e^{\widetilde{\Gamma}} \widehat{\otimes}_V^x A \cong V_e^{\widetilde{\Gamma}}[[x_1, \ldots, x_d]],$$

where $\widehat{\otimes}^x$ *is completion with respect to the expansion of the ideal* $(x_1, \ldots, x_d)$. *We then let* $A^{\widetilde{\Gamma}} := \bigcup_e A_e^{\widetilde{\Gamma}}$.

Now suppose that R *is essentially of finite type over* A. *We define* $R_e^{\widetilde{\Gamma}} := A_e^{\widetilde{\Gamma}} \otimes_A R$, *and* $R^{\widetilde{\Gamma}} := A^{\widetilde{\Gamma}} \otimes_A R \cong \bigcup_e R_e^{\widetilde{\Gamma}}$, *since* $\otimes_A$ *commutes with direct limit.*

We also describe a more invariant formulation that does not directly utilize formal power series.

Let B *denote a local* V-*algebra with residue class field* K *such that* B *is complete with respect to an ideal* $\mathfrak{b}$ *such that* $p + \mathfrak{b}$ *is the maximal ideal of* B.

Then there is a V-*algebra surjection* $A = V[[x_1, \ldots, x_d]] \twoheadrightarrow B$ *such that the* x_j *map to generators of* $\mathfrak{B}$. *Then we can construct* $B_e^{\widetilde{\Gamma}}$ *using the fact that* B *is an image of* A, *or directly, as the completion of* $V_e^{\widetilde{\Gamma}} \otimes_V B$ *with respect to the expansion of* $\mathfrak{B}$, *which we denote* $V_e^{\widetilde{\Gamma}} \widehat{\otimes}_V^{\mathfrak{b}} B$.

Likewise, we may construct $B^{\widetilde{\Gamma}}$ *by thinking of* B *as an* A-*algebra, or directly as* $\bigcup_e B_e^{\widetilde{\Gamma}}$. *Now, if* R *is essentially of finite type over* B, *it does not matter whether we take* $R_e^{\widetilde{\Gamma}}$ *(respectively* $R^{\widetilde{\Gamma}}$*) as* $B_e^{\widetilde{\Gamma}} \otimes_B R$ *(respectively,* $B^{\widetilde{\Gamma}} \otimes_V R$ *) or as* $A_e^{\widetilde{\Gamma}} \otimes_A R$ *(respectively,* $A^{\widetilde{\Gamma}} \otimes_V R$*). It also follows that if we have two choices of* B, *say* $B \to C$ *with the map local and* C *module-finite over the image of* B, *and* R *is essentially of finite type over* C *and, hence,* B, *we may calculate* $R_e^{\widetilde{\Gamma}}$ *or* $R^{\widetilde{\Gamma}}$ *using either* B *or* C.

Theorem 5.9. *Let notation be as in Construction 5.8. For all sufficiently small cofinite* $\widetilde{\Gamma} \subseteq \widetilde{\Lambda}$, *the defining ideal of the singular locus in* R *expands to the defining ideal of the singular locus in* $R^{\widetilde{\Gamma}}$.

Proof. Choose Γ so that the set of primes $\mathfrak{q}$ containing p where $R_{\mathfrak{q}}$ and $R_{\widetilde{\mathfrak{q}}}^{\widetilde{\Gamma}}$ are both regular is maximal. Note that we may identify $V_R(p) \cong \mathrm{Spec}(R/pR)$ with $V_{R^{\widetilde{\Gamma}}}(p) \cong \mathrm{Spec}(R^{\widetilde{\Gamma}}/(p)) \cong (R/pR)^{\Gamma}$: here $\widetilde{\mathfrak{q}}$ denotes the unique prime of $R^{\widetilde{\Gamma}}$ lying over $\mathfrak{q}$. One can do this since the open sets in $\mathrm{Spec}(R/pR)$ have ACC.

For primes of R containing p the maximality of Γ implies that the regular locus in R is identified with the regular locus of primes in $R^{\widetilde{\Gamma}}$ containing p: if this fails for $\mathfrak{q}$, one may decrease Γ so that $\mathfrak{q}R^{\widetilde{\Gamma}} = \widetilde{\mathfrak{q}}$ (the issues may be considered modulo p, where the statement follows from the corresponding result for the Γ-construction). Hence, the regular loci for primes containing p agree for this Γ or any other smaller cofinite choice of Γ. At primes not containing p, one may localize both rings at the element p. The map is then geometrically regular, and one has regularity at a prime of the target if and only if one has regularity at its contraction. □

We conclude by applying the mixed characteristic Γ-construction to give a regularity criterion without any F-finiteness hypotheses on the residue field. The following is Theorem C from the introduction.

Corollary 5.10. *Let V be an unramified discrete valuation ring of mixed characteristic, and let $(R, \mathfrak{m}, k)$ be essentially of finite type over a complete local V-algebra with $p \in \mathfrak{m}$. We retain the notation of Construction 5.8.*

The ring R is regular if and only if for any sufficiently small cofinite subset $\widetilde{\Gamma} \subseteq \widetilde{\Lambda}$, $\widetilde{\Omega}_{R^{\widetilde{\Gamma}}|(\mathbb{Z},\delta)}$ is free of rank $\dim(R) + \log_p[k(R^{\widetilde{\Gamma}}) : k(R^{\widetilde{\Gamma}})^p]$, where $k(R^{\widetilde{\Gamma}})$ denotes the residue field of $R^{\widetilde{\Gamma}}$.

Acknowledgments

References

[1] Michael Artin and Christel Rotthaus, *A structure theorem for power series rings*, in Algebraic geometry and commutative algebra, Vol. I, 35–44, Kinokuniya, Tokyo, 1988.

[2] Bhargav Bhatt and Peter Scholze, *Prisms and prismatic cohomology*, preprint, arXiv:1905.08229.

[3] Alexandru Buium, *Geometry of p-jets*, Duke Math. J. 82 (1996), no. 2, 349–367.

[4] Alessandro De Stefani, Eloísa Grifo, and Jack Jeffries, *A Zariski-Nagata theorem for smooth $\mathbb{Z}$-algebras*, to appear in J. Reine Angew. Math., preprint: arXiv:1709.01049.

[5] Taylor Dupuy, Eric Katz, Joseph Rabinoff, and David Zureick-Brown, *Total p-differentials on schemes over $\mathbb{Z}/p^2$*, J. Algebra, 524 (2019), 110–123.

[6] O. Gabber and L. Ramero, Foundations for almost ring theory – Release 7.5, `https://arxiv.org/abs/math/0409584`.

[7] Melvin Hochster and Craig Huneke, *F-regularity, test elements, and smooth base change*, Trans. Amer. Math. Soc. **346** (1994), 1-62.

[8] Zhan Jiang, *Test Elements, Analogues of Tight Closure, and Size for Ideals*, Ph.D. thesis, University of Michigan, 2021.

[9] André Joyal, *δ-anneaux et vecteurs de Witt*, C. R. Math. Rep. Acad. Sci. Canada 7 (1985), no. 3, 177–182.

[10] Ernst Kummer, *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, J. Reine Angew. Math. 44 (1852), 93–146.

[11] Ernst Kunz, *On Noetherian rings of characteristic p*, Amer. J. Math. 98 (1976), no. 4, 999–1013.

[12] Ernst Kunz, *Kähler differentials*, Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1986. viii+402 pp.

[13] H. Matsumura, Commutative algebra, second ed., Mathematics Lecture Note Series, vol. 56, Benjamin/Cummings Publishing Co., Inc., Reading, Mass., 1980.

[14] Takeshi Saito, *Frobenius-Witt diifferentials and regularity*, preprint, arXiv:2008.04728v2 [math.AG] 14 Aug 2020.
vol. 41 (1955), 647–650.

[15] Richard P. Stanley, *Enumerative combinatorics.* Volume 1. Second edition. Cambridge Studies in Advanced Mathematics, 49. Cambridge University Press, Cambridge, 2012. xiv+626 pp.

[16] Richard G. Swan, *Néron-Popescu desingularization*, in Algebra and geometry (Taipei, 1995), 135–192, Lect. Algebra Geom., 2, Int. Press, Cambridge, MA, 1998.

[17] Maciej Zdanowicz, *Liftability of singularities and their Frobenius morphism modulo p^2*, Int. Math. Res. Not. IMRN 2018, no. 14, 4513–4577.

DEPARTMENT OF MATHEMATICS, EAST HALL, 530 CHURCH ST., ANN ARBOR, MI 48109–1043, USA

Email address: hochster@umich.edu

DEPARTMENT OF MATHEMATICS, AVERY HALL, 1144 T ST, LINCOLN, NE 68588–0130, USA

Email address: jack.jeffries@unl.edu