DELIGNE-ILLUSIE CLASSES I: LIFTED TORSORS OF LIFTS OF THE FROBENIUS FOR CURVES.

TAYLOR DUPUY

ABSTRACT. For curves of genus bigger than one we prove that Buium's first arithmetic jet spaces admit the structure of a torsor under some line bundle. This result lifts a known constructions in characteristic p where the first p-jet space modulo p is a sheaf under the Frobenius tangent sheaf (parametrizing Frobenius linear derivations). In particular we show there is a natural family of lifts of the Frobenius tangent bundle so that the first p-jet space (and hence higher order lifts of the Frobenius) form torsor a under this bundle.

The cohomology classes associated to this torsor structure, which we call the Deligne-Illusie class, has strong analogies with the classical Kodaira-Spencer class from deformation theory.

CONTENTS

1. Introduction

In this paper p will always denote a prime. We will let CRing denote the category of commutative rings with a unit, CRing_B denote the category of commutative rings over a base ring B, Sch_S or Sch_B be the category of schemes over a scheme S or a ring B and Set denote the category of sets.

For a ring B over a ring of p-adic integers we will use the notation $B_n = B/p^{n+1}$. We will use $\widehat{B}$ or $B^{\hat{p}}$ to denote p-adic completion $\varprojlim B/p^{n+1}$. For a scheme Y over such a ring B we will use the notation Y_n for the reduction modulo p^{n+1} i.e. $Y := Y \otimes_B B_n$. We will let $\widehat{Y} = \varinjlim Y_n$ denote the p-formal completion of a scheme Y over a p-adic ring B.

By a curve in Sch_B we will mean a scheme of relative dimension 1.

1.1. **(Differential algebraic) Kodaira-Spencer classes.** Let K be a characteristic zero field with a derivation $D : K \to K$. Let X/K be a smooth scheme. Let $(U_i \to X)_{i \in I}$ be a Zariski affine open cover of X such that $D_i : \mathcal{O}(U_i) \to \mathcal{O}(U_i)$ are lifts of the derivation D on K. We can then form the cohomology class

$$\mathrm{KS}(X) := [D_i - D_j] \in H^1(X, T_{X/K})$$

where $T_{X/K}$ denotes the relative tangent sheaf, whose sections are K-linear derivations on $\mathcal{O}$. The class $\mathrm{KS}(X) \in H^1(X, T_{X/K})$ is called the **Kodaira-Spencer** class.

For a X/K a variety over a field with a derivation, one can define a twisted version of the tangent bundle $J^1(X/K, D) \to X$ whose local sections correspond to derivations lifting the derivation D on the base. The space $J^1(X/K, D)$ is called the **first jet space** of X/K.

Theorem 1.1 ([Bui94], Proposition 2.5, page 65)**.** *Let X/K be a smooth variety over a field with a derivation D. Suppose in addition that K is algebraically closed. The following are equivalent*

(1) $\mathrm{KS}(X) = 0$ *in* $H^1(X, T_{X/K})$
(2) $J^1(X/K, D) \cong T_{X/K}$ *as* $T_{X/K}$-*torsors.*
(3) *There exists some* $X' \in \mathsf{Sch}_{K^D}$ *such that*

$$X \cong X' \otimes_{K^D} K.$$

Here K^D denotes the field of constants

$$K^D = \{c \in K : D(c) = 0\}.$$

The aim of this paper is to show that an arithmetic analog of this theorem exists in the case of curves over the p-adic ring $R = \widehat{\mathbf{Z}_p^{ur}}$ the p-adic completion of the maximal unramified extension of the p-adic integers.

In the arithmetic variant of Theorem 1.1 the first jet space $J^1(X/K, D)$ is replaced by the first arithmetic jet space of Buium. Local sections of the first arithmetic jet space of a scheme correspond to local lifts of the Frobenius.

1.2. **Witt vectors.** We refer to Hazewinkel [Haz09] and for an introduction to Witt vectors.

We recall that the full (p-typical) witt vectors $W_{p,\infty}$ are a functor from rings to rings. A basic property is that $W_{p,\infty}(\mathbf{F}_p) = \mathbf{Z}_p$ the p-adic integers. For $k \subset \bar{\mathbf{F}}_p$ the ring $W_{p,\infty}(k)$ complete discrete valuation rings with residue field k; it is a p-adic completion of an unramified extension of the p-adic integers. The ring $W_{p,\infty}(\bar{\mathbf{F}}_p)$ is

isomorphic to $\widehat{\mathbf{Z}_p^{ur}} = \mathbf{Z}_p[\zeta; \zeta^n = 1, p \nmid n]$, the p-adic completion maximal unramified extension of the p-adic integers. All of there rings have a unique lift of the Frobenius ϕ which is constant on $\mathbf{Z}_p$ and acts on roots of unity by $\zeta \mapsto \zeta^p$.

We also recall that the truncated (p-typical) witt vectors of length two $W_{p,1}$ are a functor from rings to rings. For a ring A we have $W_{p,1}(A) = A \times A$ as sets with addition and multiplication rules given by

$$
\begin{aligned}
(x_0, x_1)(y_0, y_1) &= (x_0 y_0, x_0^p y_1 + y_0^p x_1 + p x_1 y_1), \\
(x_0, x_1) + (y_0, y_1) &= (x_0 + y_0, x_1 + y_1 + C_p(x_0, y_0)), \\
C_p(S, T) &= \frac{S^p + T^p - (S+T)^p}{p} \in \mathbf{Z}[S, T].
\end{aligned}
$$

This functor has the property that $W_{p,1}(\mathbf{F}_p) \cong \mathbf{Z}/p^2$. The ideal $V_p(W_{p,1}(A)) = \{(0, a) : a \in A\}$ has square zero for every ring A.

1.3. p-**derivations and lifts of the Frobenius.** Let A be a ring and B be an A-algebra. Let p be a prime number (p will always denote a prime in this paper). A p-**derivation** from A to B is a map of sets $\delta : A \to B$ such that for all $a, b \in A$ we have

$$
\begin{aligned}
\delta(a + b) &= \delta(a) + \delta(b) + C_p(a, b), \\
\delta(ab) &= \delta(a)b^p + a^p \delta(b) + p\delta(a)\delta(b), \\
\delta(1) &= 0. \\
C_p(S, T) &= \frac{S^p + T^p - (S+T)^p}{p} \in \mathbf{Z}[S, T].
\end{aligned}
$$

These operations were introduced independently by Joyal [Joy85] and Buium [Bui96]. The collection of p-derivations from a ring A to a ring B will be denoted by $p\text{-Der}(A \to B)$.

Example 1.2. (1) If $A = B = \mathbf{Z}_p$, the p-adic integers, then the map $\delta_p(x) = \frac{x - x^p}{p}$ defines a p-derivation.

(2) If $A = \mathbf{Z}/p^2$ and $B = \mathbf{Z}/p$ then the division-by-p map $[1/p] : p\mathbf{Z}/p^2 \to \mathbf{Z}/p$ makes sense and the map $\delta_p : \mathbf{Z}/p^2 \to \mathbf{Z}/p$ defined by $x \mapsto [1/p](x - x^p)$ gives a p-derivation.

For a ring A we will let $W_{p,1}(A)$ denote the ring of p-typical Witt vectors of length two.

A p-derivation $\delta : A \to B$ is equivalent to a map $A \to W_{p,1}(B)$ such that its composition with the canonical projection map $W_{p,1}(B) \to B$ is the underlying algebra map $A \to B$. This is similar to the fact that morphisms $A \to B[t]/(t^2)$ such that the composition with the projection $B[t]/(t^2) \to B$ give the algebra map $A \to B$, are equivalent to derivations from A to B.

A **lift of the Frobenius** from $A \to B$ is a morphism $\phi : A \to B$ such that

$$
\phi(x) \equiv x^p \mod p.
$$

If B is a p-torsion free ring then a lift of a Frobenius is equivalent to a p-derivation and they are related by the formula $\delta_p(x) = \frac{\phi(x) - x^p}{p}$.

An expression for involving polynomial combinations of ring elements together with p-derivations will be called a Wittferential equation or arithmetic differential equation. A basic reference for this material is [Bui05].

1.4. **Deligne-Illusie classes modulo** p. We will fix the following notation

- $R_0 = k$ is a perfect field of characteristic p.
- $R = W_{p,\infty}(k)$ the ring of p-typical Witt vectors (equivalently, the p-adic completion of the maximal unramified extension of the p-adic integers).
- X/R a smooth scheme of finite type.
- FT_{X_0} the $\mathcal{O}_{X_0}$-module of Frobenius derivations. For $D \in FT_{X_0}$ a local section and $x, y \in \mathcal{O}_{X_0}$ local sections we have

$$
\begin{aligned}
D(xy) &= D(x)y^p + x^p D(y), \\
D(x+y) &= D(x) + D(y).
\end{aligned}
$$

Such derivations are called **Frobenius derivations**.

Let $\delta : R_1 \to R_0$ be the unique p-derivation from R_1 to R_0. If X/R is smooth, we can cover X by affine open subsets $(U_i \to X_1)_{i \in I}$ and find local lifts of the p-derivations

$$
\delta_i : \mathcal{O}(U_i)_1 \to \mathcal{O}(U_i)_0.
$$

The difference $\delta_i - \delta_j$ give a well-defined map

$$
(\delta_i - \delta_j) : \mathcal{O}(U_{ij})_0 \to \mathcal{O}(U_{ij})_0,
$$

which is a derivation on the Frobenius, $(\delta_i - \delta_j) \in FT_{X_0}((U_{ij})_0)$. The differences define a Čech cocycle for FT_{X_0} and one can check that the associated cohomology class is independent of the choice of lifts δ_i. Hence we have a well defined map

$$
\mathrm{DI}_0 : p\text{-}\mathrm{Der}(R_1 \to R_0) \to H^1(X_0, FT_{X_0}).
$$

Since the p-derivation $R_1 \to R_0$ is unique it will not hurt to denote the class associated to the lift X_1 by $\mathrm{DI}_0(X_1)$.

Implicit in this construction is the fact that the sheaf $p\text{-}\mathrm{Der}(\mathcal{O}_{X_1} \to \mathcal{O}_{X_0})$ is a torsor under FT_{X_0}. We will say more about this in section **??**. This sheaf is representable, is called the first p-jet space of a curve modulo p, and will be denoted by $J^1_p(X)_0$. This torsor appears many places in the literature under different names. Sometimes it is refered to as "the torsor of lifts of the Frobenius" and is denoted by $\mathcal{L}$ in [OV07]. The first p-jet space modulo p, $J^1_p(X)_0$ is sometime known as the Greenberg transform $\mathrm{Gr}_1(X)$, this is the notation for example in [LS03].

Remark 1.3.   (1) The construction of the Deligne-Illusie class is implicit in the proof of Theorem 2.1 in [DI87]. The class $\mathrm{DI}_0(X)$ is denoted by $c = [h_{ij}]$ in [DI87]. See in particular Remark 2.2.iii. The construction also appears in [DI87] in the proof of Theorem 3.5 .

(2) Chapter II, section 1, Theorem 1.1 in [Moc96] also employs the Deligne-Illusie construction. Implicit in the proof that $\mathcal{D}$ (the lifts of $X_0^{(p)}$, a Frobenius twist of X, to $\mathbf{Z}/p^2$) is a torsor under the first sheaf cohomology of the Frobenius tangent sheaf. We should note that in his treatment, Mochizuki considers schemes with log structures while we do not. Mochizuki attributes the results in this section to [Kat89, proposition 4.12] who attributes to [DI87].

(3) The Deligne-Illusie class $\mathrm{DI}_0(X_1) \in H^1(X_0, FT_{X_0})$ should be compared to the classical deformation class $\mathrm{KS}(X_1) \in H^1(X_0, I_1 \otimes T_{X_0})$ where I_1 is the ideal sheaf of $X_0 \hookrightarrow X_1$. This construction of $\mathrm{KS}(X_1)$, in the equicharacteristic setting, can be found [Ols07].

1.5. **Buium's arithmetic jet spaces.** Let $R = W_{p,\infty}(k)$ where k is a perfect field of characteristic p. Let X/R be a scheme. We define the r**th** p-**jet space functor** by

$$J_p^r(X) : \mathsf{Sch}_R \to \mathsf{Set}$$
$$J_p^r(X)(A) = X(W_{p,r}(A)) \text{ for all } A \in \mathsf{CRing}_R.$$

The association $J_p^r : \mathsf{Sch}_R \to \mathrm{Fun}(\mathsf{Sch}_R, \mathsf{Set})$ is functorial. Here Fun denotes the category of functors where morphisms are natural transformations.

Proposition 1.4 (Borger [Bor11], (12.5)). *For every X/R a scheme of finite type, the functor $J_p^r(X)$ is representable in the category of schemes.*

Remark 1.5.   (1) The functors we denote as J_p^r have been denoted as W_{r*} by Borger in [Bor11].
     (2) In [Bui96] Buium proved that the functors $X \mapsto J_p^r(X)_n$ are representable for every $n \geq 0$. Buium simply denotes these functors as $J^r(-)$.

It is important to know that local sections of the map $J_p^1(X)_n \to X_n$ correspond to local lifts of the Frobenius.

1.6. **Statement of main result.** For $X \subset \mathbf{P}_R^n$ a curve we will denote by condition $(*)$ the following

(1.1) $$g(X) \geq 2 \text{ and } p > \deg(X \subset \mathbf{P}_R^n).$$

Theorem 1.6 ($\exists$ Lift of torsor of lifts of the Frobenius). *Let $X \subset \mathbf{P}_R^n$ a smooth projective curve. If X satisfies $(*)$ then there exists a system of "canonically lifted" $\mathcal{O}_{X_n}$-modules $(FT_{X_n})_{n \geq 0}$ such that the collection $(J_p^1(X)_n)_{n \geq 0}$ form a system of torsors under $(FT_{X_n})_{n \geq 0}$ compatible with the known structure in characteristic p. For each $n \geq 0$ the torsor structure for $J_p^1(X)_{n+1}$ under $FT_{X_{n+1}}$ lifts the previous.*

For each $n \geq 0$ we define the **Deligne-Illusie** class

$$\mathrm{DI}_n(X_n) \in H^1(X_n, FT_{X_n})$$

to be the cohomology class associated to the torsor structure.

Remark 1.7. Buium referes to these classes in [Bui95] and [Bui05] as Arithmetic Kodaira-Spencer classes and denotes them with KS instead of DI. See [Bui05], Definition 3.10 for Deligne-Illusie classes for varieties in characteristic p and [Bui05], Definition 8.50 for a variant for Abelian varieties (which can also be constructed in characteristic zero).

In [Bui95, Lemma 4.4], Buium relates $\mathrm{DI}_0(A)$ of an abelian variety (denoted ρ^{int} there) to $\mathrm{KS}(A_1/R_1)$ (denoted ρ^{ext} and viewed as a map). He proves

$$\mathrm{DI}_0(A/R) = F^*\mathrm{KS}([\delta(t(A)) \mod p]^{1/p}),$$

where F denotes the absolute Frobenius, $t : R[[t_{ij} : 1 \leq i, j \leq \dim_R(A)]] \to R$ is the Serre-Tate classifying map for A with image $t(A)$ and the bar denote reduction modulo p. We refer to [Bui95] for more details.

After pairing a Deligne-Illusie class with elements of its Serre dual one can obtain arithmetic differential equations in the coefficients of the variety which is zero precisely when the variety admits a lifts of the Frobenius. In the case that the variety under consideration is an elliptic curve, the resulting differential equation is a differential modular form (in the sense of Buium) which cuts out canonical lift on

modular curves. See [BP09, Section 3.9] for an appearence in an application and [Bui00] for more on differential modular forms.

Definition 1.8. The category of Λ_p-**Schemes** $\mathsf{Sch}_R^{\Lambda_p}$ (resp $\mathsf{Sch}_{R_n}^{\Lambda_p}$) is defined by

    Objects: Schemes X/R (resp X_n/R_n) with a lifts of the Frobenius on R (resp R_n)

    Morphisms: Morphisms of schemes over R_n equivariant with respect to the Frobeniuses.

For $X' \in \mathsf{Sch}_R^{\Lambda_p}$ (resp $\mathsf{Sch}_{R_n}^{\Lambda_p}$) we will let $- \otimes_{\Lambda_p} R : \mathsf{Sch}_R^{\Lambda_p} \to \mathsf{Sch}_R$ denote the forgetful functor (resp $- \otimes_{\Lambda_p} R_n$).

Corollary 1.9. *The following are equivalent*

  (1) $\mathrm{DI}_n(X_n) = 0$ *in* $H^1(X_n, FT_{X_n})$
  (2) $J_p^1(X)_n \cong FT_{X_n}$ *as a torsors under* FT_{X_n}.
  (3) X_n/R_n *descends to the category of* Λ_p-*schemes: There exists some* $X_n' \in \mathsf{Sch}_{R_n}^{\Lambda_p}$ *such that* $X_n' \otimes_{\Lambda_p} R_n = X_n$. [1]

Remark 1.10.   (1) Compare the statement to theorem 1.1.
  (2) When $R = W_{p,\infty}(\overline{\mathbf{F}}_p)$ we have

$$R^{\delta_p} = \{c \in R : \delta_p(c) = 0\} = \{\zeta : \zeta^n = 1, p \nmid n\} \cup \{0\}$$

    which is a monoid of roots of unity. It is unclear if there exists an interpretation of descent in algebro-geometric Categories from say [Lor12],[TV09] or [PL09].
  (3) The result of Raynaud [Ray83] show that curves X/R of genus $g \geq 2$ do not have lifts of the Frobenius. Hence curves X/R satisfying $(*)$ do not have lifts of the Frobenius and act as "non isotrivial" in our setting.

1.7. **Remarks on the proof.** Let R be an arbitrary commutative ring. A morphism of schemes $\pi : E \to X$ is called an $\mathbf{A}_R^1$-**bundle** if there exists an open cover $(U_i \to X)_{i \in I}$ and isomorphisms $\psi_i : \pi^{-1}(U_i) \to U_i \times_R \mathbf{A}_R^1$ which respect the projections down to U_i. A collections of trivializations together with the isomorphisms will be called a **atlas**.

We will let $\underline{\mathrm{Aut}}(\mathbf{A}^1)$ denote the functor which associates to a scheme U the opposite group of automorphisms of $\mathcal{O}(U)[t]$ which we view as groups of polynomials under composition with coeffients in $\mathcal{O}(U)$. When we restrict $\underline{\mathrm{Aut}}(\mathbf{A}^1)$ to open subsets of a scheme it becomes a sheaf of groups.

Let $G \leq \underline{\mathrm{Aut}}(\mathbf{A}^1)$ be a subgroup and $\pi : E \to X$ an $\mathbf{A}_R^1$ bundle. A G-**atlas** will be an atlas $(\psi, U_i \to X)_{i \in I}$ such that for all $i, j \in I$ we have $\psi_{ij} \in G(U_{ij})$. A G-**structure** will be a maximal G-atlas. When this happens we call G the **structure group** of the bundle. We record the following simple fact.

Let G and H be subgroups of $\underline{\mathrm{Aut}}(\mathbf{A}^1)$. Let $\widetilde{\psi}_{ij}, \psi_{ij} \in G(U_{ij})$ be cocycles with respect to some cover $(U_i \to X)_{i \in I}$. We say that ψ_{ij} and $\widetilde{\psi}_{ij}$ are H-**compatible** if there exists a collection of $\psi_i \in H(U_i)$ for $i \in I$ such that $\psi_i \psi_{ij} = \widetilde{\psi}_{ij} \psi_j$. When this is the case we write $\psi_{ij} \sim_H \widetilde{\psi}_{ij}$.

Let AL_1 denote the $a + bT$ subgroup of $\underline{\mathrm{Aut}}(\mathbf{A}^1)$.

---

[1] This is just a fancy notation for saying that X_n admits a lift of the Frobenius.

Lemma 1.11. *Let $\pi : E \to X$ be an $\mathbf{A}^1_R$-bundle. The bundle $E \to X$ is a torsor under some line bundle $L \to X$ if and only if π admits an AL_1-structure.*

Proof. It is clear that an AL_1-structure induces a line bundle under a torsor. The converse can be seen by considering the functor of points on E, imposing the obvious torsor structure on E and checking that the definition is well-defined. $\square$

Remark 1.12. The natural projection $\mathrm{AL}_1 = \mathcal{O}_{X_n} \rtimes \mathcal{O}^\times_{X_n} \to \mathcal{O}^\times_{X_n}$ induces a map $H^1(X_n, \mathrm{AL}_1) \to H^1(X_n, \mathcal{O}^\times) = \mathrm{Pic}(X_n)$.

If $\sigma_n \in H^1(X_n, \mathrm{AL}_1)$ is the class associated to the torsor on $J^1_p(X)_n$ then the image of that class under the natural map is the class of the lifted Frobenius tangent sheaf $[FT_{X_n}] \in \mathrm{Pic}(X_n)$.

To prove that $J^1_p(X)_n$ has the structure of a torsor under FT_{X_n} it suffices to show that $J^1_p(X)_n$ admits an AL_1-structure. Here are the following reduction steps.

Step 1: Show that $J^1_p(X)_n$ admits the structure of an $\mathbf{A}^1_{R_n}$-bundle.

Step 2: Show that $J^1_p(X)_n$ admits A_n-structure. (We will introduce subgroups $A_n, A_{n,d} \leq \underline{\mathrm{Aut}}(\mathbf{A}^1_{R_n})$ of "automorphisms of bounded degree" which play a key roll in the proof.).[2]

Step 3: Show by induction on n that $J^1_p(X)_n$ admits an $A_{n,n}$-structure.

Step 4: Show by induction on d that $J^1_p(X)_n$ admits an $A_{n,d}$-structure it admits a $A_{n+1,d-1}$ structure for $d \geq 2$. $(A_{n,1} \leq \mathrm{AL}_1(\mathcal{O}_{X_n}))$ [3]

The first step is a theorem of Buium (section 4.1) The second step is where most of the work happens: we perform some local computations for transition maps for plane curves and extend these results to imply the existence of A_n structures for $n \geq 1$. This is done in section 4.3. The third and fourth steps are done simultaneously in section 4.4 and uses a "pairing" between group and Čech cohomology.

Sections 2 and 3 provide background on p-derivations and p-jet spaces.

Acknowledgements. The author is indebted to Alexandru Buium for his guidance and encouragement. We would also like to thank James Borger for reviewing an earlier version of this manuscript and giving many useful comments and suggestions. Final preparations of this manuscipt occured at MSRI during the Spring of 2014.

2. p-DERIVATIONS

The material for this section is standard and can be obtained from (say) [Bui05] and [Bui96] and contains no new information. We provide this introduction here for convenience of the reader.

2.1. p-derivations.
Let A and B be rings, with B an A-algebra. A p-**derivation** $\delta_p : A \to B$ is a map of sets satisfying the following axioms

$$\delta_p(a+b) = \delta_p(a) + \delta_p(b) + C_p(a,b)$$
$$\delta_p(ab) = \delta_p(a)b^p + a^p\delta_p(b) + p\delta_p(a)\delta_p(b)$$
$$\delta_p(1) = 0$$
$$C_p(x,y) = \frac{x^p + y^p - (x+y)^p}{p} \in \mathbf{Z}[x,y]$$

---

[2] This step uses the hypothesis $\deg(X) << p$.

[3] This step uses the hypotheses $g(X) \geq 2$.

The category of rings with p-derivations is called the category of Λ_p-**rings**.

2.2. **Examples.** Let A be a ring and $a \in A$. Recall that we have a well-defined morphism

$$\left[\frac{1}{a}\right] : aA \to A/\mathrm{ann}(a).$$

Here $\mathrm{ann}(a)$ denotes the annihilator ideal of a.

Example 2.1. $\delta : \mathbf{Z}/p^2 \to \mathbf{Z}/p$ given by $\delta(x) = (x - x^p)/p$ where we interpret $1/p$ as a map

$$\frac{1}{p} : p\mathbf{Z}/p^2 \to \mathbf{Z}/p.$$

Example 2.2. If $R = W_{p,\infty}(k)$ with k perfect of characterisic p then R has a unique lift of the Frobenius ϕ on it. It hence has a unique p-derivation $\delta(x) = (\phi(x) - x^p)/p$.

Theorem 2.3. *Let $R = W_{p,\infty}(k)$ where k is a perfect field of characteristic p.*

(1) $\delta_p(p^n) = \frac{p^n - p^{np}}{p} = p^{n-1} \cdot \mathrm{unit}$
(2) $\delta_p(p^n \cdot \mathrm{unit}) = p^{n-1} \cdot \mathrm{unit}$
(3) $(p^n, \delta_p(p^n), \delta_p^2(p^n), \ldots, \delta^r(p^n))_R = (p^{n-r})_R$

Proof. The first property is trivial. The second property follows from the computation

$$
\begin{aligned}
\delta_p(p^s \cdot u) \quad &- \quad \delta_p(p^s)u^p + p^{sp}\delta_p(u) + p\delta_p(p^s)\delta_p(u) \\
&= \quad p^{s-1} \cdot u^p + p^{sp}\delta_p(u) + p^s \cdot \mathrm{unit} \cdot \delta_p(u) \\
&= \quad p^{s-1}(\mathrm{unit} + p \cdot \mathrm{junk}).
\end{aligned}
$$

We prove the last property by induction on r. It is sufficient to show that $\delta_p^r(p^n) = p^{n-r} \cdot \mathrm{unit}$. We have

$$\delta_p(\delta_p^{r-1}(p^n)) = \delta_p(p^{n-r+1} \cdot \mathrm{unit}) = p^{n-r} \cdot \mathrm{unit},$$

where the first equality follows from inductive hypothesis and the second equality follows from the second proposition. $\square$

2.3. **First p-jet ring.** Define $(-)_{p,1} : \mathsf{CRing} \to \mathsf{CRing}$ by

$$A_{p,1} = A[\dot a : a \in A]/(\mathrm{relations})$$

where (relations) are generated by

$$(2.1) \qquad\qquad (a\dot{b+c}) \quad = \quad \dot{a}b^p + a^p\dot{b} + p\dot{a}\dot{b} + \dot{(c)} + C_p(ab,c),$$

$$(2.2) \qquad\qquad C_p(x,y) \quad = \quad \frac{x^p + y^p - (x+y)^p}{p} \in \mathbf{Z}[x,y],$$

For all $a, b, c \in A$.

Remark 2.4. Let $R = W_{p,\infty}(k)$ where $k \subset \bar{\mathbf{F}}_p$. If A is an R-algebra and R admits multiple p-derivations we may want to impose that the p-derivation on A extend the one on the base. Suppose $\delta_0 : R \to R$ is such a p-derivation on the base. The additional relation we impose is then $\dot r = \delta_0(r)$ where of course these are understood to be taken as an image in A.

Since we will work modulo pth powers or p-formal setting in this paper, this will not matter.

Example 2.5. A/R is finite type,

$$A = R[x_1, \ldots, x_n]/(f_1, \ldots, f_r) = R[x]/(f)$$

where $x = (x_1, \ldots, x_n)$, $f = (f_1, \ldots, f_r)$ then

$$A_{p,1} = R[x, \dot{x}]/(f, \dot{f})$$

where $\dot{x} = (\dot{x}_1, \ldots, \dot{x}_n)$ and $\dot{f} = (\dot{f}_1, \ldots, \dot{f}_r)$. Here $(\dot{f}_1), \ldots, (\dot{f}_r) \in R[x, \dot{x}]$ are computed using the rule for linear combinations above (2.1).

Theorem 2.6 (Universal Property). *There is a universal p-derivation $\delta_{p,1} : A \to A_{p,1}$ mapping a to $\dot{a}$. It satisfies the following universal property:*

For every p-derivation $\delta : A \to B$ of the ring homomorphism $A \to B$ there exists a unique ring homomorphism $u_\delta : A_{p,1} \to B$ such that

$$
\begin{array}{ccc}
A & \xrightarrow{\ \delta\ } & B \\
& \searrow{\scriptstyle \delta_{p,1}} & \uparrow{\scriptstyle u_\delta} \\
& & A_{p,1}
\end{array}
\quad .
$$

The ring homomorphism is the morphism of A-algebras defined by $u_\delta(\dot{a}) = \delta(a)$. [4]

Proof. It is clear the the morphism is well-defined from the definitions in section **??**. We leave it as an exercise to check the universality. $\qquad\square$

2.4. **Data of p-derivations.**

Lemma 2.7 (flatness over witt vectors= p-torsion free). *Let A be an $R = W_{p,\infty}(k)$ algebra with k-perfect of characteristic p. The following are equivalent*

1. *A is flat over R*
2. *The multiplication by p morphism is injective.*
3. *A is p-torsion free*

Proof. It is clear the (2) and (3) are the same. We will show p-torsion free implies flat. Flatness is equivalent to $I \otimes_R A \to IA$ given by $i \otimes_R a \mapsto ia$ is injective. We have $I = m^n$ for some m where $m = (p)$ is the maximal ideal of R. A general element of $m^n \otimes A$ looks like $\sum_i p^{n'+n_i} \otimes a_i$ with n' be the the gcd of all of the $p^{n'+n_i}$ where we can assume wlog that a_i's are not divisible by any powers of p. Suppose $\sum_i p^{n'+n_i} \otimes a_i \mapsto p^{n'}(\sum_i p^{n_i} a_i) = 0$. Since multplication by p is injective we have $\sum_i p^{n_i} a_i = 0$. This is a contradiction since $\sum_i p^{n_i} a_i$ was cooked up to be a unit.

We will show that flatness implies p-torsion free. We prove the converse by contrapositive: If it is not p-torsion free it will not be flat. Suppose that multiplication by p is not injective on A. This means that the map $pR \otimes_R A \to pA$ is not an injection. This contradicts flatness. $\qquad\square$

Theorem 2.8. *Let $B \in \mathsf{CRing}_A$, $A \in \mathsf{CRing}_R$ where $R = W_{p,\infty}(k)$ and k is a perfect field of characteristic p. Suppose that A and B are flat over R. The following data are equivalent.*

1. *A p-derivation $\delta : A \to B$ of the algebra map $A \to B$.*

---

[4] Warning: The diagram is not a diagram in the categorical sense but it is an exercise to show that the universal property can be formulated in terms of diagrams

(2) *An action $\rho : A \to W_{p,1}(B)$ (meaning a morphism of rings such that $(\pi_{p,1})_B \circ g) = f : A \to B$ the algebra map.*
(3) *A morphism of A-algebras $A_{p,1} \to B$.*

Proof. Follows from the definitions. □

Example 2.9. Let A and B be rings over $R = W_{p,\infty}(k)$ with k perfect of characteristic p. Suppose $p \neq 2$ and consider the diagram

$$A_{p,1} \xrightarrow{u} B$$
$$\uparrow$$
$$A$$

This induces $A \to B$.

If $f : A \to B$ is already given and $A = A/p^{n+1}$ then $(A)_{p,1} = (A)_{p,1}/p^n$. This follows from the fact that

$$\delta(p^n) = \frac{p^n - p^{np}}{p} = p^{n-1}(1 - p^{n(p-1)})$$

when p is not a unit.

Hence we have a factorization

$$A_{p,1} \xrightarrow{u} B \quad ,$$
$$\uparrow \qquad \uparrow$$
$$A \xrightarrow{\pi^*_{p,1}} A/p^n$$

although $f : A \to B$ may not factor through a reduction modulo p^n in general.

Theorem 2.10. *Let B be a p-torsion free ring and ϕ a lift of the Frobenius on B inducing a lift of the Frobenius on $A_n = B/p^{n+1}$. This then induces a well-defined p-derivation*

$$\delta_p : A_n \to A_{n-1}.$$

Proof. In general, given any A and a lift of the Frobenius $\phi : A \to A$, one can try to define

$$\delta_p : A \to A/\text{ann}(p)$$

via

$$\delta_p(a) = (\left[\frac{1}{p}\right] \circ g)(a)$$

where $g(a) = \phi(a) - a^p$, and $g : A \to pA$ at least.

The difficulty in defining δ_p comes from the equality

$$\left[\frac{1}{p}\right](g(a)g(b)) = p \cdot \left[\frac{1}{p}\right](g(a)) \cdot \left[\frac{1}{p}\right](g(b)) \text{ in } A/\text{ann}(p).$$

We leave it to the reader to verify that this makes sense.

It is useful for the reader to note that if $A_n = B/p^{n+1}$ where B is p-torsion free then

$$\text{ann}_A(p^j) \cong p^{n-j}A$$
$$A/\text{ann}_A(p^j) \cong A/p^{n-j}$$

These give maps $[1/p] : pA_n \to A_{n-1}$. □

Theorem 2.11. *Let A, B be flat over $R = W_{p,\infty}(k)$ where $k \subset \bar{\mathbf{F}}_p$. Suppose that A is of finite type over R. Let $f : A \to B$ be a morphism of rings inducing the morphism of rings $f_n : A_n \to B_n$. The following are equivalent*

(1) *A lift of the Frobenius $\phi_n : A_n \to B_n$,*

$$\phi_n(a) \equiv f_0(a)^p \mod p$$

(2) *A p-derivation $\delta_p : A_n \to B_{n-1}$*
(3) *A morphism $(A_{p,1})_{n-1} \to B_{n-1}$ of A_{n-1}-algebras.*

Proof. To see that 2 implies 1 note that $\phi_n(a) := a^p + p\delta(a)$ defines a lift of the Frobenius. We will show that 3 and 2 are equivalent: Let $A = R[x]/(f)$ so that $(A_{p,1})_n = (R[x, \dot{x}]/(f, \dot{f}))/p^n = R_{n-1}[x, \dot{x}]/(f, \dot{f})$. The map clearly defines a p-derivation. (Note: $(\delta_{p,1})_n : A_n \to (A_{p,1})_{n-1}$ is universal).

We will not show 1 implies 2 but the reader can verify that this follows from the universal property of p-derivations. $\square$

Lemma 2.12. *Let A, B and C be flat $R = W_{p,\infty}(k)$-algebras where $k \subset \bar{\mathbf{F}}_p$. Suppose $A \to B$ is an ètale morphism of rings. Every p-derivations $B_n \to C_{n-1}$ lifts to a unique p-derivation $A_n \to C_{n-1}$.*

Proof. The proof is essentially the same as the standard proof for lifting infinitesimal deformations. We prove a stronger result from which our result follows a fortiori.

Recall that ètale ring homomorphisms have the infinitesimal lifting property: For every commutative diagram

(2.3)
$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} \\ C & \longrightarrow & C/I \end{array} \quad , \quad I^2 = 0,$$

there exists a unique map $\widetilde{\beta} : B \to C$ making the diagram commute.

We want to show that when we are given a p-derivation

$$\begin{array}{ccc} & A & \\ & \downarrow & \searrow \\ W_{p,1}(C') & \longrightarrow & C' \end{array}$$

There exists a diagram

$$\begin{array}{ccc} & B & \\ & \downarrow & \searrow \\ W_{p,1}(C') & \longrightarrow & C' \end{array}$$

lifting the previous.

To apply the infinitesimal lifting criterion (2.3) with the following choices:

$$
\begin{aligned}
C &= W_{p,1}(C'), \\
C/I &= C', \\
I &= V_p(W_{p,1}(C')), \\
\alpha &= \text{map assoc. to } p\text{-der } B \to C', \\
\beta &= \text{alg map } A \to C .
\end{aligned}
$$

$\square$

3. p-JETS

References for this section include [Bui05], [Bui96] and [Bor11]. Other than in presentation, this section contains no new information.

We summarize the results of this section:

(1) Suppose $X/R = W_{p,\infty}(\bar{\mathbf{F}}_p)$ is flat. Then local sections of the map $(\pi_{p,1})_n : J_p^1(X)_n \to X_n$ induce local p-derivations/lifts of the Frobenius on X_n on the ring A and conversely.
(2) If X/R is flat then $J_p^r(X_n) = J_p^r(X)_{n-r}$, in particular $J_p^1(X_n) = J_p^1(X)_{n-1}$.
(3) Suppose X/R is flat, we have the following compatibility between p-jet functors and open and closed immersions.

$$
\begin{aligned}
J_p^r(\text{ open immersion})_n &= \text{ open immersion.} \\
J_p^r(\text{ closed immersion})_n &= \text{ closed immersion}
\end{aligned}
$$

3.1. **p-jet spaces.** Let X/R be a scheme where $R = W_{p,\infty}(k)$, with k perfect of characteristic p. define the rth **p-jet functor** $J_p^r(X) : \mathsf{CRing}_R \to \mathsf{Set}$ to be the functor of $W_{p,r}$ valued points of X:

$$
J_p^r(X)(A) := X(W_{p,r}(A)) \quad A \in \mathsf{CRing}_R.
$$

The natural morphism of ring schemes $\pi_{r,s} : W_{p,r} \to W_{p,s}$ for $r > s$ induces functorial morphisms $J_p^r(X) \to J_p^s(X)$. The morphisms $\pi_r : W_{p,r} \to \mathcal{O}$ induce functorial morphisms $J_p^r(X) \to X$.

Example 3.1. When $X = \mathrm{Spec}(A)$ and A is an R algebra with $R = W_{p,\infty}(k)$ where k is perfect of characteristic p we have that $J_p^1(X)$ is representable and

$$
J_p^1(\mathrm{Spec}(A)) = \mathrm{Spec}(A_{p,1})
$$

as schemes over X.

Remark 3.2. Since the constuction $A \mapsto A_{p,1}$ does not localize well one needs to work hard to get that p-jet spaces are representable. This essentially follows from the quotient rule for p-derivations:

$$
\delta\left(\frac{1}{f}\right) = \frac{f^p\delta(f)}{f^p(f^p + p\delta(f))}.
$$

For $X/R = W_{p,\infty}(k)$ flat where $k \subset \bar{\mathbf{F}}_p$, we define the sheaf of $\mathcal{O}_{X_n}$-algebras $\mathcal{O}_{X_n}^{(1)}$ to be the sheaf associated to presheaf

$$
U \mapsto \mathcal{O}(U)_{p,1} \mod p^{n+1},
$$

for relevant open subsets of U. We will construct the global spectrum of this ring in order to produce the first p-jet spaces. For higher order p-jets one does something similar.

Theorem 3.3 ([Bui96]). *Let $R = W_{p,\infty}(k)$ where k is perfect of characteristic p.*
  (1) *Let X/R be a flat scheme. The functor $J_p^r(X) := X \circ W_{p,r}$ over X, is representable when reduced modulo p^{n+1} for every n.*
  (2) *Furthermore for every A in CRing_{R_n} we have*
$$J_p^r(X)_n(A) = J_p^r(X)(A) = X(W_{p,r}(A)) \to X(A) = X_n(A)$$
  where the map is $(\pi_{p,r})_A$.

A more difficult theorem of Borger proves the following:

Theorem 3.4 ([Bor11]). *Let X/R be any scheme and $R = W_{p,\infty}(k)$ with k perfect of characteristic p. The functor $J_p^r(X) := X \circ W_{p,r}$ is representable in the category of schemes over R.*

Theorem 3.5. *Let X/R be a scheme which is flat over R (so that multiplication by p is injective).*
  (1) *The natural morphism $\pi_{m,s} : J_p^m(X_n) \to J_p^s(X_n)$ factors through reduction modulo p^{n-m+1},*
$$J_p^m(X)_{n-m} \xrightarrow{(\pi_{p,r+s,s})_{n-r}} J_p^s(X)_{n-m} \ .$$
  This is a morphism of schemes over R_{n-m}.
  (2) *Local sections of the morphisms*
$$J_p^1(X)_m \xleftarrow[s]{\pi_{p,1}} X_n$$
  are in bijection with local lifts of the Frobenius/p-derivations
$$\delta : \mathcal{O}(X_{n+1}) \to \mathcal{O}(X_n) = \mathcal{O}(X_{n+1})/p^{n+1}.$$

Proof. The problem is local. Let $X = \mathrm{Spec}(R[x]/(f))$ (using multi-index notation). The map $\pi_{m,s}$ gives a map of rings

$$R[x, \dot{x}, \ldots, x^{(s)}]/(f, \dot{f}, \ldots, f^{(s)}) = \mathcal{O}(J_p^s(X)) \to \mathcal{O}(J_p^m(X)) = R[x, \dot{x}, \ldots, x^{(m)}]/(f, \dot{f}, \ldots, f^{(m)}).$$

The first part of the proposition follows from an explicit description of the ideals given previously (in Theorem 2.3). The second part follows from the characterization of lifts of the Frobenius on rings of the form $A_n = B/p^{n+1}$ (in 2.11). $\qquad\square$

Theorem 3.6. *Let X/R be flat where $R = W_{p,\infty}(k)$ where k is perfect and characteristic p.*
  (1) *If $i : U \hookrightarrow X$ is an open immersion of R-schemes of finite type then*
$$J_p^1(i)_n : J_p^1(U)_n \hookrightarrow J_p^1(X)_n$$
  is an open immersion.
  (2) *If $j : Z \hookrightarrow X$ is a closed immersion of R-schemes of finite type then*
$$J_p^1(j) : J_p^1(Z) \hookrightarrow J_p^1(X)$$
  is also a closed immersion.

Proof. We first show the open immersion property is local for the functors $J_p^1(-)_n$. Consider the case when $X = \mathrm{Spec}(A)$ with $A = R[x]/(f)$ (using multi-index notation). It is enough to show that the functor $J_p^1()_n$ respects principal open immersions (one globalizes this affine result in the usual way taking direct limits of principal open immersions).

$$
\begin{aligned}
(A_{p,1})_g &= (R[x,\dot{x}]/(f,\dot{f}))_g \\
(A_g)_{p,1} &- R[x,\dot{x},1/g(1/g)]/(f,\dot{f})] \\
&= R[x,\dot{x},1/g,\frac{-\dot{g}}{g^{2p}}\sum_{j\geq 0}\left(\frac{p\dot{g}}{g^p}\right)^j]/(f,\dot{f})
\end{aligned}
$$

so we clearly have

$$
(A_{p,1})_g \hookrightarrow (A_g)_{p,1}.
$$

Reducing modulo p^{n+1} gives

$$
\frac{-\dot{g}}{g^{2p}}\sum_{j\geq 0}\left(\frac{-p\dot{g}}{g^p}\right)^j \in ((A_{p,1})_g)_n.
$$

This shows

$$
((A_{p,1})_g)_n = ((A_g)_{p,1})_n.
$$

In the non-p-formal setting this result fails. We should also note that this is really the key observation construction of p-jet (Theorem 3.3).

In the non-p-formal, non-affine case one needs to do more work. For the full proof we refer the reader to [Bor11].

In the affine setting

$$
X = \mathrm{Spec}\ R[x]/(f), \qquad J_p^1(X) = \mathrm{Spec}\ R[x,\dot{x}]/(f,\dot{f}),
$$

$$
Z = \mathrm{Spec}\ R[x]/(f,g) \quad J_p^1(X) = \mathrm{Spec}\ R[x,\dot{x}]/(f,g,\dot{f},\dot{g}).
$$

and it is clear that $\dot{f}$ and $\dot{g}$ give extra elements of the ideal. $\square$

We remark that the above theorem is true for higher order finite jets as well and the contructions are analogous.

The above proposition implies that $J_p^1(Y)_n = (\pi_{p,1}^{-1})_n(Y_n)$ if $Y \hookrightarrow X$ is an open or closed immersion of R-schemes when X is flat over R.

3.2. *p-Formal schemes.* The construction of p-jet spaces associated to a scheme X/R where $R = W_{p,\infty}(\bar{\mathbf{F}}_p)$ gives a system of maps

The p-formal schemes $\widehat{J}_p^r(X) := \varinjlim \widehat{J}_p^r(X)_n$ used by Buium (in say [Bui05]) behave nicely. In some sense this means that the appropriate place for p-jet spaces would be some variant of the p-adic rigid analytic spaces. We make use of these limits in the subsequent sections.

3.3. **Examples.** We give some examples that we believe clarify the situation.

Example 3.7. Let $R = W_{p,\infty}(k)$ where k is a perfect field of characteritic p. Let $X = \mathrm{Spec}(R[x]/(f))$ (using multi-index notation). There are no sections of the morphism of R-schemes

$$J_p^1(X)_0 = J_p^1(X_1^{\pi_{p,1}^1}) \xleftarrow{\quad\quad} X_1 \ .$$

This would correspond to a map of rings

$$s^* : R[x, \dot{x}]/(f, p^2, \dot{f}, (\dot{p^2})) = R_0[x, \dot{x}]/(f, \dot{f}) \to R_1[x]/(f) = R[x]/(f, p^2).$$

Example 3.8. Let $R = W_{p,\infty}(\mathbf{F}_p)$. Write

$$\mathbf{P}_R^1 = \frac{\mathrm{Spec}(R[x]) \cup \mathrm{Spec}(R[y])}{\sim}$$

where $\sim$ denotes gluing along $\mathrm{Spec}\, R[x,y]/(xy - 1)$. Then

$$\widehat{J}_p^1(\mathbf{P}_R^1) = \frac{\mathrm{Spf}(R[x, \widehat{\dot{x}]}) \cup \mathrm{Spf}(R[y, \widehat{\dot{y}]})}{\sim}$$

where $\sim$ denotes gluing of the formal schemes along

$$\mathrm{Spf}(R[x, \dot{x}, y, \widehat{\dot{y}]}/(xy - 1, \dot{x}y^p + \dot{y}x^p + p\dot{x}\dot{y}).$$

4. PROOFS

4.1. **Step 1: Affine bundle structures.** Recall that any smooth scheme X/R of relative dimension d admits a Zariski affine open cover opens $(U_i \to X)_{i \in I}$ such that there exist étale maps $f_i : U_i \to \mathbf{A}_R^d$. Recall the following lemma:

Lemma 4.1 ([Bui05], Section (3.2)). *Let X and Y be finite dimensional smooth schemes over $R = W_{p,\infty}(\bar{\mathbf{F}}_p)$,*

   (1) *If $f : X \to Y$ is étale then $\widehat{J}_p^1(X) \cong \widehat{X} \widehat{\times}_Y \widehat{J}^1(Y)$.*
   (2) *If $f : X \to \mathbf{A}_R^d$ is étale then $\widehat{J}_p^1(X) \cong \widehat{X} \widehat{\times} \widehat{\mathbf{A}}_R^d$*

Remark 4.2. If $X = \mathrm{Spec}A$ and $f^* : R[T_1, \ldots, T_n] \to A$ is étale then $\mathcal{O}(J^1(X)) = \mathcal{O}(X)[\dot{T}_1, \ldots, \widehat{\dot{T}_n]}$. Here we have identified the étale parameters T_i with their image under f^*.

4.2. **Projections.** By a decomposition of $\mathbf{P}^n$ (over R) we will mean a collection of linear forms $\lambda = \{l_0, \ldots, l_n\}$ in general position together with its associated linear subspaces. For $0 \le d \le n$ we will let λ_r denote the collection of hyperplanes generated by λ of dimension d. For each such linear subspace Λ we will let Λ' denote is complementary subspace and $\pi_\Lambda^{\Lambda'}$ denote the linear projection onto Λ with center Λ'. For a linear subspace Λ of X and a point x of X we will let $\overline{x, \Lambda}$ denote the linear subspace spanned by Λ and all the lines passing through points of Λ and x. Complementary subspaces have the property that $\overline{x, \Lambda} \cap \overline{x, \Lambda'} = \overline{x, \pi_\Lambda^\Lambda(x)}$ is the unique line passing through x and the point of its projection. We will denote this line by $L(\Lambda, \Lambda', x)$. For a given $X \subset \mathbf{P}^n$ and a complementary pair of subspace

Λ, Λ' we will let X_Λ denote the open subset of X where $\pi_\Lambda^{\Lambda'}$ restricted to X is ètale onto its image.

4.3. **Step 2: Existence of an A_n-structure.** .

Let $R = W_{p,\infty}(\mathbf{F}_p)$. We define a subset of automorphisms of degree n mod p^n

$$A_n := \{a_0 + a_1 T + p a_2 T^2 + \cdots + p^{n-1} a_n T^n : a_1 \in \mathcal{O}_{X_n}^\times, a_i \in \mathcal{O}_{X_n}\} \subset \underline{\mathrm{Aut}}(\mathbf{A}_{R_{n-1}}^1).$$

Proposition 4.3. $A_n \subset \underline{\mathrm{Aut}}(\mathbf{A}_{R_{n-1}}^1)$ is a subgroup.

Proof. We will first show that A_n is closed under composition and then show that A_n is closed under taking inverses. Let

$$\begin{aligned} f(T) &= a_0 + a_1 T + p a_2 T^2 + \cdots + p^{n-1} a_n T^n, \\ g(T) &= b_0 + b_1 T + p b_2 T^2 + \cdots + p^{n-1} b_n T^n \end{aligned}$$

be elements of A_n. We claim that $g(f(T)) \in A_n$.

If is sufficient to show that every term in

$$p^{j-1} b_j (f(T))^j, 1 < j \le n - 1$$

of degree d is divisible by p^{d-1}.

A typical term in the expansion above takes the form

$$A = p^{j-1} \cdot (p^{i_1 - 1} a_{i_1} T^{i_1}) \cdots (p^{i_j - 1} a_{i_j} T^{i_j}),$$

has degree greater than d. This means that $i_1 + i_2 + \ldots + i_j = d$ and that $p^{d-j} = p^{i_1 + i_2 + \ldots + i_j - j}$ which means that A is of the form $A = p^{d-1} a_{i_1} \ldots a_{i_j} T^d$ and that every coefficient T^d in the expansion of $g(f(T))$ is divisible by p^{d-1}. In particular note that $g(f(T))$ has degree n mod p^n which shows that A_n is closed under composition.

We will now show that if $f \in A_n$ then $f^{-1} \in A_n$. Fix $f(T) = a_0 + a_1 T + p a_2 T^2 + \cdots + p^{n-1} a_n T^n$. We proceed by induction on n. The base case is $n = 2$ we have proved everything. Now suppose that

$$f(g(T)) = g(f(T)) = T \mod p^n$$

we need to show that $g \in A_n$. By induction we know that we can write (by rearranging terms if necessary)

$$g(T) = g_{n-1}(T) + p^{n-1} G(T)$$

where $G(T)$ has order greater than n and

$$g_{n-1}(T) = b_0 + b_1 T + p b_2 T^2 + \cdots + p^{n-2} b_{n-1} T^{n-1}.$$

We will assume that $G(T)$ has degree greater than strictly greater that n and derive a contradiction. Examining

$$g(f(T)) = g_{n-1}(f(T)) + p^n G(f(T)) \mod p^n$$

we know from the previous proposition that

$$\deg(g_{n-1}(f(T))) \le n.$$

We also know that

$$p^{n-1} G(f(T)) = p^{n-1} G(a_0 + a_1 T)$$

and that the degree of $G(f(T))$ is exactly the degree of $G(T)$ since a_1 is a unit. This means that $g(f(T)) = T \mod p^n$ has degree strictly greater than n which is a contradiction. This shows that $g(T)$ actually has degree n and hence $g(T) \in A_n$ which completes the proof. □

In what follows we let f_x and f_y denote the usual partial derivatives of f with respect to x and y respectively.

Lemma 4.4 (Local Computations)**.** *Let $C = V(f)$ be a plane curve over $R = W_{p,\infty}(\mathbf{F}_p)$ with $f \in R[x,y]$. Let $U = D(f_x)$ and $V = D(f_y)$ and ε_U and ε_V be the étale projections to the y and x axes of $\mathbf{A}^2$ and let $\psi_U : J_p^1(U) \to \widehat{U} \widehat{\times} \widehat{\mathbf{A}}^1$ and $\psi_V : J^1(V) \to \widehat{V} \widehat{\times} \widehat{\mathbf{A}}^1$ be the associated affine bundle trivializations[5].*

(1) *If f_x or f_y is not identically zero modulo p then the transition map $\psi_{VU} := \psi_V \circ \psi_U^{-1}$ has the property that*

$$\psi_{UV} \otimes_R R_n \in A_n$$

for each $n \geq 2$.
(2) *If $\deg(f) < p$ then f_x or f_y is not identically zero modulo p.*

Proof. Assume without loss of generality that $f_y \neq 0 \mod p$. The maps $\varepsilon_U : U \to \mathbb{A}^1$ given by $(x,y) \mapsto y$ and $\varepsilon_V : V \to \mathbb{A}^1$ given by $(x,y) \mapsto x$ are étale. On these open sets we have $\mathcal{O}^1(U) = O(U)[\dot{y}]^{\widehat{}}$ and $\mathcal{O}^1(V) = \mathcal{O}(V)[\dot{x}]^{\widehat{p}}$. This means we have

$$\mathcal{O}(J^1(U \cap V)) = \mathcal{O}(U \cap V)^1 = \mathcal{O}(U \cap V)[\dot{x}]^{\widehat{p}} = \mathcal{O}(U \cap V)[\dot{y}]^{\widehat{p}}.$$

Let $\psi_U : J^1(U) \to \widehat{U} \widehat{\times} \widehat{\mathbf{A}}^1$ be given by $t \mapsto \dot{y}$ and $\psi_V : J^1(V) \to \widehat{V} \widehat{\times} \widehat{\mathbf{A}}^1$ be given by $t \mapsto \dot{x}$. We can compute the transition map $\psi_V \circ \psi_U^{-1} \in \underline{\mathrm{Aut}}(\widehat{\mathbf{A}}^1)(U \cap V)$ by first computing what $\dot{y}$ is in terms of $\dot{x}$. We first have

$$\begin{aligned} \delta f &\equiv \frac{1}{p}[f^\phi(x^p, y^p) - f(x,y)^p] + \nabla f^\phi(x^p, y^p) \cdot (\dot{x}, \dot{y}) \\ &\quad + \frac{p}{2}[f^\phi_{xx}(x^p, y^p)\dot{x}^2 + 2f^\phi_{xy}(x^p, y^p)\dot{x}\dot{y} + f^\phi_{yy}(x^p, y^p)\dot{y}^2] \\ &\equiv 0 \mod p^2 \text{ in } \mathcal{O}(U \cap V)[\dot{y}]^{\widehat{}} \end{aligned}$$

where for a polynoimal $g(x) = a_0 + a_1 x + \cdots + a_n x^n$ the polynomial $g^\phi(x) := \phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$ as usual and $\nabla f = (f_x, f_y)$ is the usual gradient from calculus.

Let

$$\begin{aligned} A &= R + f^\phi_x(x^p, y^p)\dot{x} + pf^\phi_{xx}(x^p, y^p)\dot{x}^2/2, \\ B &= f^\phi_y(x^p, y^p) + pf^\phi_{xy}(x^p, y^p)\dot{x}, \\ C &= f^\phi_{yy}(x^p, y^p)/2, \\ R &= (f^\phi(x^p, y^p) - f(x,y)^p)/p \end{aligned}$$

then, solving the equation $A + B\dot{y} + C\dot{y}^2 = 0$ gives

$$\dot{y} = -\frac{A}{B} + p\frac{A^2 C}{B^3}.$$

---

[5] see Lemma 4.1

Since

$$pB^{-3}A^2C \;=\; p\frac{(R + f^\phi{}_x(x^p, y^p)\dot{x})^2 f^\phi{}_{yy}(x^p, y^p)}{2f^\phi{}_y(x^p, y^p)^3}$$

$$AB^{-1} \;=\; \frac{1}{f^\phi{}_y(x^p, y^p)}[R + f^\phi{}_x(x^p, y^p)\dot{x} + pf^\phi{}_{xx}(x^p.y^p)\dot{x}^2/2$$

$$-p\frac{f^\phi{}_{xy}(x^p, y^p)\dot{x}}{f^\phi{}_y(x^p, y^p)}(R + f^\phi{}_x(x^p, y^p)\dot{x})]$$

we get

(4.1) $$\dot{y} = \alpha + \beta\dot{x} + p\gamma\dot{x}^2$$

where

$$\alpha \;=\; -\frac{R}{f^\phi{}_y(x^p, y^p)} + p\frac{R^2 f^\phi{}_yy(x^p, y^p)}{2f^\phi{}_y(x^p, y^p)^3}$$

$$\beta \;=\; \frac{-f^\phi{}_x(x^p, y^p)}{f^\phi{}_y(x^p, y^p)} + p\frac{f^\phi{}_{xy}(x^p, y^p)R}{f^\phi{}_y(x^p, y^p)^2} + \frac{pRf^\phi{}_x(x^p, y^p)f^\phi{}_yy(x^p, y^p)}{f^\phi{}_y(x^p, y^p)^3},$$

$$\gamma \;=\; -\frac{f^\phi{}_{xx}(x^p, y^p)}{2f^\phi{}_y(x^p, y^p)} + \frac{f^\phi{}_{xy}(x^p, y^p)f^\phi{}_x(x^p, y^p)}{f^\phi{}_y(x^p, y^p)^2} + \frac{f^\phi{}_x(x^p, y^p)^2 f^\phi{}_{yy}(x^p, y^p)}{2f^\phi{}_y(x^p, y^p)^3}.$$

We will now show that $\dot{y} \equiv a_0 + a_1\dot{x} + pa_2\dot{x}^2 + \cdots + p^n a_{n+1}\dot{x}^{n+1} \mod p^{n+1}$ by induction. We have proven the base case and proceed to solve for $\dot{y}$ in terms of $\dot{x}$ as we did before inductively. As before we have

$$\delta(f(x, y)) = \frac{1}{p}\left(f^\phi(x^p + p\dot{x}, y^p + p\dot{y}) - f(x, y)^p\right) = 0.$$

We use the expansion

$$f^\phi(x^p + p\dot{x}, y^p + p\dot{y}) = \sum_{d \geq 0} p^{d-1}h_d(\dot{x}, \dot{y})$$

where h_d are homogeneous polynomials of degree d in $\dot{x}$ and $\dot{y}$ with coefficients in $R[x, y]/(f)$; this gives

(4.2) $$\frac{f^\phi(x^p, y^p) - f(x, y)^p}{p} + \sum_{d=1}^{n} p^{d-1}h_d(\dot{x}, \dot{y}) \equiv 0 \mod p^{n+1}.$$

By inductive hypothesis we may assume $\dot{y} = A + p^n B$ where $A = a_0 + \sum_{j=1}^{n} p^{j-1}a_j\dot{x}^j$. Expanding the homogeneous polynomials gives

$$h_d(\dot{x}, \dot{y}) = h_d(\dot{x}, A + p^n B) = h_d(\dot{x}, A) + \frac{\partial h_d}{\partial \dot{y}}(\dot{x}, A)p^n B \mod p^{n+1}$$

and substituting into equation 4.2 we get
(4.3)
$$r + \sum_{d=1}^{n} p^{d-1}\left(h_d(\dot{x}, A) + \frac{\partial h_d}{\partial \dot{y}}(x, A)p^n B\right) = r + \sum_{d=1}^{n} p^{d-1}h_d(\dot{x}, A) + \sum_{d=1}^{n} p^{d-1}\frac{\partial h_d}{\partial \dot{y}}(\dot{x}, A)p^n B$$

where $r = \frac{f^\phi(x^p, y^p) - f(x, y)^p}{p}$. Note that the left terms on the right side of equation 4.3 can be written as

$$r + \sum_{d=1}^{n} p^{d-1}h_d(\dot{x}, A) = p^n C$$

and the term on the right can be written as

$$\sum_{d=1}^{n} p^{d-1}\frac{\partial h_d}{\partial \dot{y}}(\dot{x},A)p^n B \equiv \frac{\partial h_1}{\partial \dot{y}}(\dot{x},A)p^n B \mod p^{n+1}.$$

Using the fact that $h_1 = f^\phi{}_x(x^p,y^p)\dot{x}+f^\phi{}_y(x^p,y^p)\dot{y}$ we have $\frac{\partial h_1}{\partial \dot{y}}(x,A) = f^\phi{}_y(x^p,y^p)$ which tells us that $p^n C + f^\phi{}_y(x^p,y^p)p^n B \equiv 0 \mod p^{n+1}$ and hence that $C + f^\phi{}_y(x^p,y^p)B \equiv 0 \mod p$ and finally that

$$B = -C/f^\phi{}_y \mod p.$$

It remains to show that B has degree less than or equal to n in $\dot{x}$.

We note that $p^n C = r + \sum_{d=1}^{n+1} p^{j-1}h_d(\dot{x},A) \mod p^{n+1}$ where we can write $h_d(S,T) = \sum_{j+k=d} a^d_{j,k}S^j T^k$, where $a^d_{j.k} \in R[S,T]/(f)$. We can expand the expression

$$(4.4) \qquad p^{d-1}h_d(\dot{x},A) = p^{d-1}h_d(\dot{x},a_0 + a_1\dot{x} + \cdots + p^{n-2}a_{n-1}\dot{x}^{n-1})$$

so that its general term takes the form

$$p^{d-1}a^d_{i,j}\dot{x}^i(a_0 + a_1\dot{x} + pa_2\dot{x}^2 + \cdots + p^{n-2}a_{n-1}\dot{x}^{n-1})^j.$$

We expand this general term further to get

$$(a_0 + a_1\dot{x} + pa_2\dot{x}^2 + \cdots + p^{n-2}a_{n-1}\dot{x}^{n-1})^j$$
$$= \sum_{j_0+j_1+\cdots+j_{n-1}=j} a_0^{j_0}(a_1\dot{x})^{j_1}(pa_2\dot{x}^2)^{j_2}\cdots(p^{n-2}a_{n-1}\dot{x}^{n-1})^{j_{n-1}}$$
$$= \sum_{j_0+j_1+\cdots+j_{n-1}=j} a_0^{j_0}a_1^{j_1}a_2^{j_2}\cdots a_{n-1}^{j_{n-1}}p^{j_2+2j_3+3j_4+\cdots+(n-2)j_{n-1}}\dot{x}^{j_1+2j_2+3j_3+\cdots+(n-1)j_{n-1}}$$

So that a general term of equation 4.4 takes the form

$$\alpha p^a \dot{x}^b$$

where $\alpha \in \mathcal{O}(U)$ and

$$\begin{aligned}
i+j &= d \\
a &= d-1+j_2+2j_3+\cdots+(n-2)j_{n-1} \\
b &= i+j_1+2j_2+\cdots+(n-1)j_{n-1} \\
j &= j_0+j_1+\cdots+j_{n-1}
\end{aligned}$$

Using these relations we show

$$\begin{aligned}
a &= d-1+j_2+2j_3+\cdots+(n-2)j_{n-1} \\
&= i+j-1+j_2+2j_3+\cdots+(n-2)j_{n-1} \\
&= i-1+j_0+j_1+2j_2+3j_3+\cdots+(n-1)j_{n-1} \\
&= i-1+j_0+(b-i) \\
&= b-1+j_0
\end{aligned}$$

Which tells us the $a = b-1+j_0 \geq b-1$. Notice that the degree of the general term is b and we want to show that $b \leq n+1$. Suppose this is not the case and that $b > n+1$. This implies that $a > n$ which implies $\alpha p^a \dot{x}^b \equiv 0 \mod p^{n+1}$; so such a term doesn't contribute to $\dot{y} \mod p^{n+1}$. This concludes the proof.

We will now prove the second part of the theorem. Let $f \in R[S,T]$, and write $f(S,T) = \sum_{k=0}^{d} f_k(S,T)$ where f_k homogeneous of degree d i.e. $f_0 = a_{00}$, $f_1 = a_{10}S + a_{01}T$, $f_2 = a_{20}S^2 + a_{11}ST + a_{02}T^2$ and so on. We have $f_d \neq 0$ since f is of degree d

Using this decomposition we can compute the partial derivatives term-wise to get

$$\frac{\partial f}{\partial S} = \sum_{k=1}^{d} \frac{\partial f_k}{\partial S}, \qquad \frac{\partial f}{\partial T} = \sum_{k=1}^{d} \frac{\partial f_k}{\partial T}.$$

If $\frac{\partial f}{\partial S} \equiv \frac{\partial f}{\partial T} \equiv 0 \mod p$ identically then

$$S\frac{\partial f}{\partial S} + T\frac{\partial f}{\partial T} = \sum_{k=1}^{d} \left(S\frac{\partial f_k}{\partial S} + T\frac{\partial f_k}{\partial T} \right) = \sum_{k=1}^{d} k f_k \equiv 0 \mod p$$

and since $R_0[S,T] \equiv \bigoplus_{k \geq 0} (R_0[S,T])_k$ we must have that $k f_k(S,T) \equiv 0 \mod p$ for $k = 1, \ldots, d$. If $p \nmid k$ this means that $f_k(S,T) = 0$ which tells us that

$$f(S,T) = h(S^p, T^p) + p g(S,T).$$

Note in particular that

$$\frac{\partial f}{\partial S} \equiv \frac{\partial f}{\partial T} \equiv 0 \mod p \implies \deg(f) \geq p.$$

$\square$

Lemma 4.5. *Let $X \subset \mathbf{P}^n$ be a smooth projective curve. Suppose Λ and Λ' are complementary linear subspaces of $\mathbf{P}^n$. $\pi = \pi_\Lambda^{\Lambda'} : X \setminus (X \cap \Lambda') \to \Lambda$ is étale at $x \in X$ if and only if $\overline{x, \pi(x)} \neq T_{X,x}$.*

If $X = V(f(x,y))$ is an affine plane curve, the projection to the x-axis is ètale if and only if $\partial f / \partial y \neq 0$. Similarly for projections to the y-axis.

Proof. By change of coordinates and by localness of the problem one only needs to consider projections $\pi : \mathbf{A}_R^n \to \mathbf{A}_R^r$ defined by $\pi(x_1, \ldots, x_r, \ldots, x_n) = (x_1, \ldots, x_r)$ and curves of the form $X = \operatorname{Spec} R[x_1, \ldots, x_n]/(f_1, \ldots, f_e)$.

Let a be a point of X not in Λ. The lines of projection $\overline{a, \pi(a)}$ are the unique lines connecting the a and $\pi(a)$ which one can compute explicitly.

Let $J(a)$ be the jacobian of $f = (f_1, \ldots, f_e)$ with respect to the variables $(x_{r+1}, \ldots, x_n)$ evaluated at a.

We use the following two facts:

(1) The condition on π being ètale is equivalent to the $J(a)$ having maximal rank.

(2) The condition that $\overline{a, \pi(a)} \subset T_{X,a}$ is equivalent to $J(a) \cdot \begin{bmatrix} a_{r+1} \\ \vdots \\ a_n \end{bmatrix} = 0$.

Suppose that π is ètale at $a \in X$. By the property 1, $J(a)$ has full rank. This implies there exists a left inverse K such that $K \cdot J(a)$ is the $n - r \times n - r$ identity matrix. The existence of such a K contradicts $\overline{a, \pi(a)} \subset T_{X,a}$ in view of property 2.

Conversely suppose that $\overline{a, \pi(a)}$ is not contained in $T_{X,a}$. This is equivalent to

$$J(a) \cdot \begin{bmatrix} a_{r+1} \\ \vdots \\ a_n \end{bmatrix} \neq 0,$$

by property 2. This implies that $J(a)$ has rank at least one. Since $J(a)$ has rank at most one it has full rank which is equivalent to ètaleness by property 1.

The second property is a special case of the first. $\qquad\square$

Figure 1 shows the projection from a line to another line.
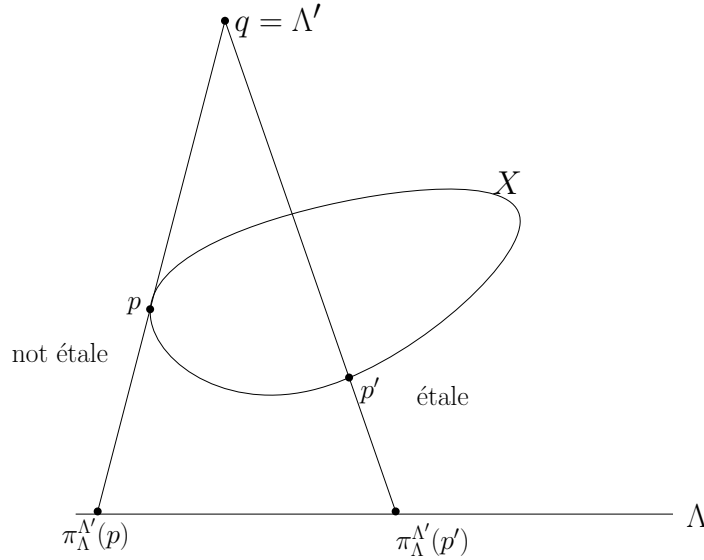

FIGURE 1. A projection in to Λ with center Λ'.

Lemma 4.6. *Let $X \subset \mathbf{P}_R^n$ be a smooth irreducible curve of degree $d < p$. Let π_1 and π_2 be projections onto lines in $\mathbf{P}_R^2 \subset \mathbf{P}_R^n$ where the centers of projections do not intersect X.*

Let $\varepsilon_1, \varepsilon_2 : U \to \mathbf{A}_R^1$ be restrictions of π_1 and π_2 so that they are both étale onto their image.

(1) *The map $\sigma := (\varepsilon_1 \times \varepsilon_2)^* : R[S,T] \to \mathcal{O}(U)$ has the property that the induced map $\sigma_0 : R_0[S,T]/(\bar{f}) \to \mathcal{O}(U)/p$ is injective.*

(2) *Let $\psi_1, \psi_2 : J^1(U) \cong \widehat{\mathbf{A}}^1 \widehat{\times} \widehat{U}$ denote the affine bundle trivializations associated to ε_1 and ε_2 respectively. For every $n \geq 1$ we have*

$$\psi_{21} \otimes_R R_n \in A_n.$$

Proof. In what follows an overline will denote a Zariski closure.

Let $\varepsilon_1^*(T) = x$ and $\varepsilon_2^*(T) = y$ where T is the étale parameter on $\mathbf{A}^1$. Define $\sigma : R[S,T] \to \mathcal{O}(U) := B$ by $S \mapsto x$ and $T \mapsto y$. Since the image of σ is an integral domain we know that $\ker(\sigma)$ is a prime ideal. Since $R[S,T]$ is a UFD and the $\ker(\sigma)$ has height 1 we know that there exists some irreducible $f \in R[S,T]$ such
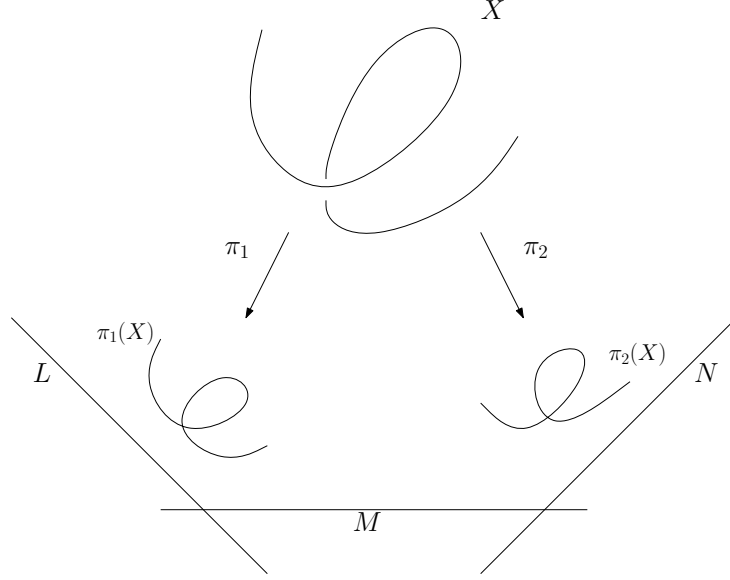
FIGURE 2. A curve $X \subset \mathbf{P}^N$ with two projections onto $\Lambda_1 = \overline{L, M}$ and $\Lambda_2 = \overline{M, N}$ both isomorphic to $\mathbf{P}^2$. The étale projections $\varepsilon_L, \varepsilon_M$ and ε_N to the lines L, M and N which induce the trivializations on the $J^1(X)$ factor through the projections π_1 and π_2

that $\ker(\sigma) = (f)$. This f is the minimal relation among x and y and we have the equation $f(x, y) = 0$. Geometrically we have

$$\overline{\varepsilon_1 \times \varepsilon_2(U)} = V(f) \subset \mathbf{A}^2,$$

where f is a dehomogenization of F where F defines $\pi(X) = V(F) \subset \mathbf{P}^2$. We know that f is irreducible by topological considerations. Note that the image is not necessarily non-singular or even flat.

We will now show that $\overline{\pi_0(U_0)} = \overline{\pi(U)}_0$ by demonstrating a closed immersion $\overline{\pi_0(U_0)} \subset (\overline{\pi(U)})_0$ and $\deg(\overline{\pi_0(U_0)}) = \deg(\overline{\pi(U)}_0).$[6]

Let $J \subset R[S, T]$ be the ideal defining $\overline{\pi_0(U_0)} \subset \mathbf{A}^2_R$. By commutativity of

$$
\begin{array}{ccc}
R[S, T] & \xrightarrow{\ \sigma\ } & B \\
\downarrow{\scriptstyle\alpha} & & \downarrow \\
R[S, T]/p & \xrightarrow{\ \sigma_0\ } & B/p.
\end{array}
$$

we have $(f, p) \subset \ker(\alpha \circ \sigma_0) = J$. This implies $\overline{\pi_0(U_0)} = V(J) \subset V(f, p) = (\overline{\pi(U)})_0 \subset \mathbf{A}^2_R$.

---

[6] Let $X = X_1 \cup \ldots \cup X_r$ is a decomposition into irreducible components and write $X_i = V(f_i)$ where f_i is an irreducible polynomial. This implies $X = V(f)$ where $f = \prod_{i=1}^{r} f_i$. This implies $\deg(X) \geq \deg(X_i)$. We have $\deg(X) \geq \deg(X_i)$.

Note that if $\deg(X) = \deg(X_i)$ then $X = X_i$. This is because $f_i | f$ and $\deg(f_i) = \deg(f)$ implies $\deg(f/f_i) = 0$ which implies $(f) = (f_i)$.

Observe $\deg(\overline{\pi_0(U_0)}) = \deg(\pi_0(X_0)) = \deg(X_0) = d$. On the other hand $\deg(\overline{\pi(U)}_0) = \deg(\pi(X_0)) = \deg(F \mod p) \leq d = \deg(\overline{\pi_0(U_0)})$.We can now conclude that $(f, p) = J$.

This implies that $\ker(\sigma_0) = J/(p) = (\bar{f})$. Since $A_0/(\bar{f}) = A_0/\ker(\sigma_0) \hookrightarrow \mathcal{O}(U_0)$ We can work directly with the equation $f(x, y) = 0$. In particular we use nonvanishing of $\partial f/\partial x$ and $\partial f/\partial y$ which follows from the description of ètale projections (Lemma 4.5)

$$\frac{\partial f}{\partial p} + f^\phi{}_x(x^p, y^p)\dot{x} + f^\phi{}_y(x^p, y^p)\dot{y}$$

$$+\frac{p}{2}(f^\phi{}_{xx}(x^p, y^p)\dot{x}^2 + 2f^\phi{}_{xy}(x^p, y^p)\dot{x}\dot{y} + f^\phi{}_{yy}(x^p, y^p)\dot{y}^2 \equiv 0 \mod p^2$$

where $\frac{\partial f}{\partial p} = \frac{f^\phi(x^p, y^p) - f(x, y)^p}{p} \in \mathcal{O}(U)$.

Hence ψ_{21} can be computed by solving for either $\dot{x}$ in terms of $\dot{y}$ or $\dot{y}$ in terms of $\dot{x}$. This is possible mod p^n for every $n \geq 2$ if either $f_x(x^p, y^p)$ or $f_y(x^p, y^p)$ is invertible in $\mathcal{O}(U)_0$. This is equivalent to having f_x or f_y being not identically zero mod p and the projections are ètale on U exactly when the partial derivatives are nonvanishing. This is true since the morphisms $\sigma_0 : R_0[S, T]/(f) \to \mathcal{O}(U)/p$ is injective (which we just proved). We now apply the local computations (Lemmm 4.4 to establish

$$\psi_{21} \mod p^n \in A_n$$

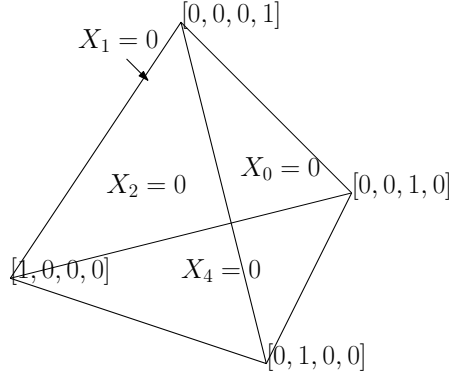for each $n \geq 2$. $\qquad\square$

FIGURE 3. A picture of $\mathbf{P}^3$ with its standard decomposition.

Lemma 4.7. *Let $R = W_{p,\infty}(k)$ where $k \subset \bar{\mathbf{F}}_p$. Let $X \subset \mathbf{P}^n_R$ be a smooth irreducible curve. There exists a system of linear forms $\lambda = \{l_0, \ldots, l_n\}$ such that $(X_\Lambda \to X)_{\Lambda \in \lambda_2}$ form a cover and which $\pi_\Lambda : X_\Lambda \to \mathbf{A}^1_R \subset \mathbf{P}^1_R$ ètale onto its image. (cf section 4.2).*

Proof. It suffice to show that there exists a decomposition λ over $\bar{\mathbf{F}}_p$ since we can lift any such decomposition to R.

Suppose in addition that $X \subset \mathbf{P}^N$ is a curve and that for all $\Lambda' \in \lambda_{N+1-2} \cup \lambda_{N+1-3}$ we have $X \cap \Lambda' = \emptyset$ so that all of the projections

$$\pi_\Lambda^{\Lambda'} : X \to \Lambda \cong \mathbf{P}^1 \text{ or } \mathbf{P}^2$$
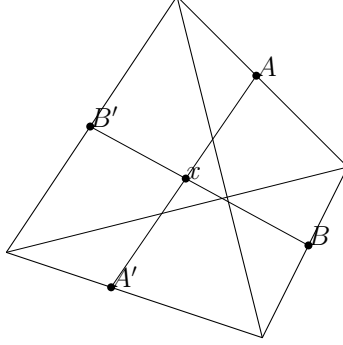
FIGURE 4. If there exists some point x such that $T_x X$ is equal $L(\Lambda', \Lambda, P)$ for all $\Lambda \in \lambda_2$ then we would have $\overline{AA'} = \overline{B'B}$. The situation looks very bad in this simple case.

are well-defined. Without loss of generality we can assume that the decomposition λ comes from the coordinates $X_0, \ldots, X_N$ on $\mathbf{P}^N$.

Suppose that there exists some $x \in X$ such that for all $\Lambda \in \lambda_2$ that $\pi_\Lambda^{\Lambda'}(x)$ is not étale at x. Using the notation introduced in equation **??** we would have

$$L(\Lambda', \Lambda, x) = T_x X$$

for all $x \in X$. Here $T_x X$ is interpreted as the physical tangent line for the embedded curve X. This leads a silly situation which we will show cannot be possible by means of synthetic argument. See figures 4.3 and 4.3 for a picture of this situation.

Suppose that $M, N \in \lambda_2$ are not equal and let $L = L(M, M', x)$ and $K = L(N, N', x)$. We claim that not both L and K can be in the tangent space of x.

Let A be the unique point where L intersects M and A' be the unique point where L intersects M'. Define B and B' similarly for N and N'. If both L and K are lines tangent to X at $x \notin \lambda_1$ we have $L = K$. This implies L intersects M at A. This also implies L also intersects N at B. But M and N intersect in a unique point C. This means that M, N and L are contained in the unique plane π spanned by A, B and C. Since π is also the unique plane spanned by M and N, this means that $\pi \in \lambda_3$. But by hypothesis we supposed that x was not in any $\pi \in \lambda_3$ which is a contradiction.

It remains to show that for every curve $X \subset \mathbf{P}_{\overline{\mathbf{F}}_p}^N$ there exists some decomposition λ such that X does not intersect any $\Lambda' \in \lambda_{N+1-3}$. This can be done by the moving lemma and dimension counting.

Recall that if X and W are subvarieties of $\mathbf{P}^N$ we say they intersect properly if

$$\dim(X \cap W) = \max\{\dim(W) + \dim(X) - N, 0\}.$$

Let W be the unions of the centers of projections to coordinate planes. $W = \bigcup_{\Lambda \in \lambda_3} \Lambda'$. Since W has dimension $N - 1 - 2$ and X has dimension 1 if W and X intersected properly we would have

$$\dim(X \cap W) = (N - 1 - 2) + 1 - N = -2$$

which imply that the intersection is empty. By the moving lemma ($\overline{\mathbf{F}}_p$ is an infinite field) we can arrange so that X and W have an empty intersection. $\square$

Theorem 4.8. *Let $R = W_{p,\infty}(k)$ where $k = \overline{\mathbf{F}}_p$. Let $X_d \subset \mathbf{P}_R^N$ be a smooth irreducible curve of degree d and suppose that $d > p$ then for every $n \geq 1$, $J_p^1(X)_n \to X_n$ admits an A_n-structure.*

Proof. Let $\lambda = \{l_0, \ldots, l_n\}$ as in Lemma 4.7. By change in coordinates we can assume without loss of generality that the $l_0, \ldots, l_n$ are the coordinate hyperplanes given by $l_i = V(X_i)$. Let $l'_0, \ldots, l'_n$ be the coordinate axes, Let U_i be the subset of X where the projection map to l'_i is ètale and $\varepsilon_i : U_i \to \mathbf{A}^1$ be the ètale projection. and let $\psi_i : J_p^1(U_i) \to \widehat{U}_i \widehat{\times} \widehat{\mathbf{A}}_R^1$ be the affine bundle chart of $\widehat{J}^1(X)$ associated to ε_i.

For each pair of lines $\Lambda_1, \Lambda_2 \in \lambda_1$ one can see that π_{Λ_1} and π_{Λ_2} factor through π_Λ where $\Lambda = \overline{\Lambda_1, \Lambda_2}$. Letting $U = X_{\Lambda_1} \cap X_{\Lambda_2}$ puts us in the hypotheses of Lemma 4.6. If ψ_1 and ψ_2 are the associated transition maps we have $\psi_{12} = (\psi_1 \circ \psi_2^{-1}) \otimes_R R_n \in A_n(U_{ij})$ for every $n \geq 1$ which proves our result. $\square$

4.4. **Steps 3 and 4: Reduction of an A_n-structure.** The following theorem allows us to reduce the structure group of the first p-jet space of a smooth curve X/R of genus $g \geq 2$.

Theorem 4.9. *Let X/R be a scheme and $\pi : E \to X$ an $\mathbf{A}_R^1$-bundle. Suppose that E_n/X_n admits A_n-structures. Let $[L_0] \in \mathrm{Pic}(X_0)$ be the class naturally associated to the $\mathrm{AL}_1(\mathcal{O}_{X_0})$-structure on E_0 as in Remark 1.12.*
   If $H^1(X_0, L_0^*) = 0$ then E_n admits an $\mathrm{AL}_1(\mathcal{O}_{X_n})$-structure.
   Here L_0^* denotes the dual of L_0.

Proof. Let $\psi_{ij}^{(n)} \in A_{n+1}(U_{ij})$ be the transition maps on a trivializing cover for E_n. We will prove that $\psi_{ij}^{(n)} \sim_{A_{n+1}} \widetilde{\psi}_{ij}^{(n)} \in \mathrm{AL}_1(\mathcal{O}_{X_n})$ by induction.

The base case with $n = 0$ is trivial since $\underline{\mathrm{Aut}}(\mathbf{A}_{R_n}^1) = \mathrm{AL}_1(\mathcal{O}_{X_0})$.

We will suppose now that $\psi_{ij}^{(n-1)} \in \mathrm{AL}_1(\mathcal{O}_{X_{n-1}})$ and construct some ψ_i's in $A_{n+1}(U_i)$ such that

$$\psi_i \psi_{ij}^{(n)} \psi_j^{-1} \in \mathrm{AL}_1(\mathcal{O}_{X_n}).$$

Let $2 \leq r \leq n+1$ and define $M_{n,r} \leq \underline{\mathrm{Aut}}(\mathbf{A}_{R_n}^1)$ so be the automorphisms of degree less than r of the form

$$\psi = a_0 + a_1 T + p^n(b_2 T^2 + \cdots + b_r T^r) \mod p^{n+1}.$$

Note that $\psi_{ij}^{(n)} \in M_{n,n+1}$ since $\psi_{ij}^{(n-1)} \in \mathrm{AL}_1(\mathcal{O}_{X_{n-1}})$ and $\psi_{ij}^{(n)} \equiv \psi_{ij}^{(n-1)} \mod p^n$.

We show now prove the following claim: For every $r \geq 2$ if $\psi_{ij}^{(n)} \in M_{n,r}$ then there exists some $\psi_{ij}'^{(n)} \in M_{n,r-1}$ such that

$$\psi_{ij}^{(n)} \sim_{M_{n,r}} \psi_{ij}'^{(n)} \text{ and } \psi_{ij}^{(n+1)} \equiv \psi_{ij}'^{(n)} \mod p^{n+1}.$$

(Note that when we get to $r = 2$ we will have shown the structure group on E_n can be reduced to $\mathrm{AL}_1(\mathcal{O}_{X_n})$.)

For $r \geq 2$ define $\tau_r : M_{n,r} \to \mathcal{O}_{X_0}$ by

$$\tau_r(\psi) = \frac{b_r(\psi)}{a_1(\psi)} \mod p.$$

Now if $\widetilde{\psi} = \widetilde{a}_0 + \widetilde{a}_1 T + p^n(\widetilde{b}_2 T^2 + \cdots + \widetilde{b}_r T^r) \in M_{n,r}$ is another element we have

$$\tau_r(\psi \circ \widetilde{\psi}) = \frac{a_1 \widetilde{b}_r + b_r \widetilde{a}_1}{\widetilde{a}_1 a_1} = \tau_r(\psi)\widetilde{a}_1^{r-1} + \tau_r(\widetilde{\psi}).$$

This shows τ_r is a group cocycle with respect to the action of $M_{n,r}$ on $\mathcal{O}_{X_0}$ (which factors through the quotient $M_{n,r} \to \mathrm{AL}_1(\mathcal{O}_{X_0}) = \mathcal{O}_{X_0} \rtimes \mathcal{O}_{X_0}^\times \to \mathcal{O}_{X_0}^\times$, and $\mathcal{O}_{X_0}^\times$ acts on $\mathcal{O}_{X_0}$ via multiplication after raising an element to the $(r-1)$-st power.

The group cocycle τ_r induces a group homomorphism $\sigma_r : M_{n,r} \to \mathcal{O}_{X_0}^\times \ltimes \mathcal{O}_{X_0}$ given by

$$\sigma_r : \psi \mapsto (a_1(\psi)^{r-1} \mod p, \tau_r(\psi)).$$

Note that this is indeed a group homomorphism:

$$(a_1^{r-1}, \tau_r(\psi)) * (\widetilde{a}_1^{r-1}, \tau_r(\widetilde{\psi})) = (a_1^{r-1}\widetilde{a}_1^{r-1}, \tau_r(\psi)\widetilde{a}_1^{r-1} + \tau_r(\widetilde{\psi})) = ((a_1\widetilde{a}_1)^{r-1}, \tau_r(\psi \circ \widetilde{\psi})).$$

Let (m_{ij}, a_{ij}) be the image of the cocycle $\psi_{ij}^{(n)}$ under the map σ_r. Note that

$$(1,0) = (m_{ij}, a_{ij})(m_{jk}, a_{jk})(m_{ki}, a_{ki}) = (m_{ij}m_{jk}m_{ki})(a_{ij}m_{jk}m_{ki} + a_{kj}m_{ki} + a_{ki})$$

The condition on the a_{ij}'s is a really a condition for a cocycle with values in line bundles: Let L_0 is a line bundle on X_0 with trivializations

$$L_0(U_i) = \mathcal{O}(U_i)v_i$$

where

$$v_j = m_{ij}v_i.$$

Suppose $s_{ij} \in L_0(U_{ij})$ defines a cocycle and define a_{ij} by

$$s_{ij} = a_{ij}v_j.$$

Then we have

$$0 = s_{ij} + s_{jk} + s_{ki} = a_{ij}m_{ij}v_i + a_{jk}m_{ik}v_i + a_{ki}v_i.$$

If follows then that since $(m_{ij}, a_{ij})) \in \mathcal{O}_{X_0}^\times \ltimes \mathcal{O}_{X_0}$ define a cocycle then the collection

$$s_{ij} := a_{ij}v_j^* \in L^*(U_{ij})$$

define a cocycle in L^*.

By hypothesis $H^1(X_0, L_0^*)$ is trivial (a simple Riemann-Roch computation) and we have

$$s_{ij} = s_i - s_j$$

for some collection $s_i \in L_0^*(U_i)$. Define $a_i \in \mathcal{O}_{X_0}(U_i)$ by

$$s_i = a_iv_i^*, \quad i \in I.$$

This gives

$$s_i - s_j = (a_im_{ij}a_k)v_j^*$$

so

$$a_{ij} = a_im_{ij} - a_j$$

or

$$-a_im_{ij} + a_{ij} + a_j = 0.$$

In terms of Čech cochains on $\mathcal{O}_{X_0}^\times \ltimes \mathcal{O}_{X_0}$ this means

$$(1, a_i)(m_{ij}, a_{ij})(1, a_j) = (m_{ij}, -a_im_{ij} + a_{ij} + a_j) = (m_{ij}, 0).$$

Let $\psi_i = T - p^n a_i T^t$ be elements of $M_{n,r}(U_i)$. We have

$$\sigma_r(\psi_i \circ \psi_{ij} \circ \psi_j^{-1}) = (m_{ij}, 0)$$

which implies that $\psi_i \circ \psi_{ij} \circ \psi_j \in M_{n,r-1}$. Hence we have that for all $r \geq 2$ and all $\psi_{ij}^{(n)} \in M_{n,r}$ there exists some $\psi_{ij}^{(n)} \in M_{n,r-1}$ such that $\psi_{ij}^{(n)} \sim_{M_{n,r}} \psi_{ij}'^{(n)}$ and $\psi_{ij}^{(n+1)} \equiv \psi_{ij}'^{(n)} \mod p^{n+1}$. This completes the proof. $\qquad \square$

To complete the proof of the Main theorem we apply Theorem 4.9 to E being the first p-jet space of a curve together with its A_n-structure given in section 4.3

Proof of Main Theorem. Consider the A_n-structure on $J_p^1(X)_n$ coming from Theorem 4.8. We apply theorem 4.9 so that $L_0 = FT_{X_0}$ – by Riemann-Roch we have $H^1(X_0, L_0^*) = 0$ are we are in the hypotheses of Theorem 4.9. $\qquad \square$

References

[Bor11] J. Borger. The basic geometry of witt vectors. ii: Spaces. *Mathematische Annalen*, 351(4):877–933, 2011.

[BP09] A. Buium and B. Poonen. Independence of points on elliptic curves arising from special points on modular and shimura curves, ii: local results. *Compositio Mathematica*, 145(03):566–602, 2009.

[Bui94] A. Buium. *Differential algebra and Diophantine geometry*. Hermann Paris, 1994.

[Bui95] A. Buium. Differential characters of abelian varieties over p-adic fields. *Inventiones Mathematicae*, 122(1):309–340, 1995.

[Bui96] A. Buium. Geometry of p-jets. *Duke Mathematical Journal*, 82(2):349–367, 1996.

[Bui00] A. Buium. Differential modular forms. *Journal fur die Reine und Angewandte Mathematik (Crelle)*, 520:95–168, 2000.

[Bui05] A. Buium. *Arithmetic differential equations*, volume 118. Amer Mathematical Society, 2005.

[DI87] P. Deligne and L. Illusie. Relèvements modulop 2 et décomposition du complexe de de rham. *Inventiones Mathematicae*, 89(2):247–270, 1987.

[Haz09] M. Hazewinkel. Witt vectors. part 1. *Handbook of algebra*, 6:319–472, 2009.

[Joy85] A. Joyal. δ-anneaux et vecteurs de witt. *CR Math. Rep. Acad. Sci. Canada*, 7(3):177–182, 1985.

[Kat89] Kazuya Kato. Logarithmic structures of fontaine-illusie. *Algebraic Analysis, Geometry and Number Theory*, pages 191–224, 1989.

[Lor12] O. Lorscheid. The geometry of blueprints: Part i: Algebraic background and scheme theory. *Advances in Mathematics*, 229(3):1804–1846, 2012.

[LS03] François Loeser and Julien Sebag. Motivic integration on smooth rigid varieties and invariants of degenerations. *Duke Mathematical Journal*, 119(2):315–344, 2003.

[Moc96] S. Mochizuki. A theory of ordinary p-adic curves. *Research Institute For Mathematical Sciences Kyoto University*, 32:957–1151, 1996.

[Ols07] MARTIN Olsson. Tangent spaces and obstruction theories. In *Notes from his lectures at the MSRI workshop on deformation theory and moduli in algebraic geometry*. Citeseer, 2007.

[OV07] Arthur Ogus and Vadim Vologodsky. Nonabelian hodge theory in characteristic p. *Publications mathématiques*, 106(1):1–138, 2007.

[PL09] J.L. Peña and O. Lorscheid. Mapping f_1-land: An overview of geometries over the field with one element. *Arxiv preprint arXiv:0909.0069*, 2009.

[Ray83] M. Raynaud. Around the mordell conjecture for function fields and a conjecture of serge lang. *Algebraic Geometry*, pages 1–19, 1983.

[TV09] B. Toën and M. Vaquié. Au-dessous de spec. *Journal of K-theory: K-theory and its Applications to Algebra, Geometry, and Topology*, 3(03):437–500, 2009.

E-mail address: dupuy@math.ucla.edu