LIFTED TORSORS OF LIFTS OF THE FROBENIUS ON ALGEBRAIC CURVES

TAYLOR DUPUY

Abstract. We prove that the sheaf of local formal lifts of the Frobenius on p-adic algebraic curves of sufficiently large genus has the structure of a torsor under some line bundle. We show that this torsor structure is not unique and describe all such line bundles and torsor structures explicitly. This lifts a well-known torsor structure exploited in the works of (say) Buium, Deligne-Illusie, Mochizuki and Ogus-Vologodsky.

Contents

1. Introduction 2
1.1. Motivation for Theorem 1.6 2
1.2. The statement of Theorem 1.6 5
1.3. The geometry of Theorem 1.6 7
1.4. Proof strategies 8
Acknowledgements 8
2. Wittferential algebra 9
2.1. p-derivations 9
2.2. First p-jet ring 9
2.3. Data of p-derivations 10
3. p-Jets 12
3.1. p-jet spaces 13
3.2. Remarks on p-formal schemes 14
3.3. Examples 14
4. Proof of Theorem 1.6 15
4.1. Step 1: Affine bundle structures 15
4.2. Step 2: Existence and uniqueness of an A_n-structure 16
4.3. Steps 3 and 4: Reduction of an A_n-structure 26
5. How many torsor structures are there? 28
5.1. Frame bundles and torsors 28
5.2. Amalgamated products 28
5.3. Preparations for the Steenrod theorem 29
5.4. Proof of Theorem 1.10 30
6. Geometry of group cocycles and moduli of reductions 34
6.1. Affine linear structures and torsor structures 34
6.2. Geometry of group cocycles 36
6.3. The moduli of torsor structures of lifts of the Frobenius modulo p^3 41
References 42

2000 *Mathematics Subject Classification.* Primary 11G99, Secondary 14G40.

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. Motivation for Theorem 1.6. Theorem 1.6, which is our main theorem, is about lifting known "arithmetic Kodaira-Spencer" constructions in characteristic p to characteristic zero. Subsections 1.1.1–1.1.5 provide motivation and background for Theorem 1.6. The expert reader may wish to skip directly to section 1.2.

1.1.1. *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.

1.1.2. *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 $W_{p,\infty}(k)$ is a 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 $\widehat{\mathbf{Z}_p^{ur}} = \widehat{\mathbf{Z}_p[\zeta; \zeta^n = 1, p \nmid n]}$, the p-adic completion of the maximal unramified extension of the p-adic integers. All of these 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 where for a ring A we have $W_{p,1}(A) = A \times A$ as sets with addition and multiplication rules given by

$$\begin{aligned}(x_0,x_1)(y_0,y_1) &= (x_0y_0, x_0^p y_1 + y_0^p x_1 + p x_1 y_1),\\ (x_0,x_1)+(y_0,y_1) &= (x_0+y_0, x_1+y_1+C_p(x_0,y_0)),\end{aligned}$$

where

$$C_p(S,T) = \frac{S^p + T^p - (S+T)^p}{p} \in \mathbf{Z}[S,T].$$

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.

1.1.3. *p-derivations and lifts of the Frobenius.* Let A be a ring and B be an A-algebra. Let p be a prime number. 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

$$\begin{aligned}\delta(a+b) &= \delta(a) + \delta(b) + C_p(a,b),\\ \delta(ab) &= \delta(a)b^p + a^p\delta(b) + p\delta(a)\delta(b),\\ \delta(1) &= 0,\end{aligned}$$

where $C_p(S,T)$ is as above. 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-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 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].

1.1.4. *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 $\delta_i - \delta_j$ gives a well-defined map
$$(\delta_i - \delta_j) : \mathcal{O}(U_{ij})_0 \to \mathcal{O}(U_{ij})_0,$$
which is a derivation of 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
$$\mathrm{DI}_0 : p\text{-Der}(R_1 \to R_0) \to H^1(X_0, FT_{X_0}).$$
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 $p\text{-Der}(\mathcal{O}_{X_1} \to \mathcal{O}_{X_0})$ is a torsor under FT_{X_0}. We will say more about this in section 2. The sheaf of p-derivations is representable, it is called the first p-jet space of a curve modulo p, and it will be denoted by $J^1_p(X)_0$. This torsor appears in 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 [DI87, Theorem 2.1] where the class $\mathrm{DI}_0(X)$ is denoted by $c = [h_{ij}]$. The class can also be seen in [DI87, Remark 2.2.iii] and [DI87, Theorem 3.5]. In [DI87, section 3], using a certain stack of splittings of a certain sheaf, they proof that Deligne-Illusie classes classify lifts of varieties modulo p^2.
2. In [Moc96, Chapter II, section 1, Theorem 1.1] 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 in [Ols07].

1.1.5. *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 **rth 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.

1.2. The statement of Theorem 1.6.

The following theorem lifts the situation in section 1.1.4.

Theorem 1.6 (Lifted Torsors of Lifts of the Frobenius)**.** *Let $R = W_{p,\infty}(\bar{\mathbf{F}}_p)$. Let X/R be the p-formal completion of a smooth projective curve of genus $g > 2$ defined over* Spf R*. Suppose in addition that the prime $p > 3g - 3$. There exists a line bundle $FT_X \to X$ such that $J_p^1(X)$ has the structure of a torsor under FT_X. Also, this FT_X and this torsor structure are non-unique.*

Theorem 1.6 is proved in section 4.3. Remarks on the proof can be found at the end of the introduction in section 1.4. We will now give an obstruction/deformation theoretic formulation of Theorem 1.6 which indicate what sort of geometry goes into the proof.

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

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

Theorem 1.7 (Obstruction/Deformation Theoretic Formulation of Theorem 1.6)**.** *Let $X \subset \mathbf{P}_R^N$ be a smooth projective curve.*

(1) *We have the following inductive procedure for finding torsor structures:*
- *Suppose $J_p^1(X)_{n-1}$ admits a torsor structure under some $FT_{X_{n-1}}$. There exists a sheaf of abelian groups $\mathcal{B}_n$ and cohomology classes* $\mathrm{obs}(X_{n+1}) \in$ *$H^1(X_n, \mathcal{B}_n)$ which is an obstruction to $J_p^1(X)_n$ admitting the structure of a torsor under a line bundle FT_{X_n} (which is not unique).*

- *In the case $n=0$ this structure is the well-known torsor of lifts of the Frobenius modulo p^2 where FT_{X_n} is the sheaf of Frobenius derivations and $\mathcal{B}_0 = F_{X_0}^*\Omega^1_{X_0}$.*

(2) *If the obstruction vanishes the isomorphism classes of pairs (FT_{X_n}, ρ_n) of line bundles FT_{X_n} together with torsor actions*

$$\rho_n : J^1_p(X)_n \times FT_{X_n} \to J^1_p(X)_n$$

are themselves a torsor under $H^0(X_n, \mathcal{B}_n)$.

(3) *In the case of curves satisfying $(*)$ the obstruction vanishes at each stage.*

In the case that the obstruction vanishes for some $n \geq 0$, after fixing a line bundle and torsor structure (FT_{X_n}, ρ_n) we define a **Deligne-Illusie** class

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

to be the cohomology class associated to the torsor structure. When $n=0$ we have $\mathrm{DI}_0(\rho_0) = \mathrm{DI}_0(X)$ where $\mathrm{DI}_0(X)$ is defined as in section 1.1.4.

Remark 1.8. The classes $\mathrm{DI}_0(X)$ are known to exist for smooth X/R of arbitrary dimension. The lifted classes are known to exists for abelian varieties. Buium refers 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 that

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

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 the Serre dual of the recipient space one can obtain arithmetic differential equations (wittferential equations) in the coefficients of the variety which are zero precisely when the variety admits a lifts of the Frobenius. In the case that the variety under consideration is an elliptic curve, there is only one differential equation and it is a differential modular form (in the sense of Buium) which cuts out canonical lifts on modular curves. See [BP09, Section 3.9] for an appearence in an application and [Bui00] for more on differential modular forms.

The following remark explains the connections of these classes to absolute geometry.

Remark 1.9. (1) The category of Λ_p-**Schemes** $\mathsf{Sch}_R^{\Lambda_p}$ (resp $\mathsf{Sch}_{R_n}^{\Lambda_p}$) is the category where objects are schemes X/R (resp X_n/R_n) with a lifts of the Frobenius on R (resp R_n) and morphisms are morphisms of schemes over R (resp 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 $- \otimes_{\Lambda_p} R_n$).

The significance of this category for us is the following: in view of being able to define torsor structures on higher order reductions of p-jet spaces one has the following equivalence of statements:

(a) $\mathrm{DI}_n(X_n) = 0$ in $H^1(X_n, FT_{X_n})$
(b) $J_p^1(X)_n \cong FT_{X_n}$ as a torsors under FT_{X_n}.
(c) 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]

This equivalence can be viewed as an arithmetic analog of Theorem 1.1 which is what motivates much of the theory.

(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 the algebro-geometric categories from say [Lor12],[TV09] or others mentioned in [PL09]. Such a construction could be interesting.

(3) A result of Raynaud [Ray83] shows 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 "nonisotrivial" in our setting.

1.3. **The geometry of Theorem 1.6.** The remainder of the paper is devoted to clearing up questions that arise out of proving Theorem 1.6. In particular one may ask:

(1) On what choices do the AL_1-structures in Theorem 1.6 depend?
(2) On what choices do the line bundles FT_{X_n} depend? Are they unique up to isomorphism?
(3) To what extent are $H^1(X_n, FT_{X_n})$ and the class inside it well-defined?
(4) Are the Deligne-Illusie classes parametrized by an easily describable canonical object?

The first, second and third questions are essentially the same and can be answered by developing the theory principal bundles in the category of fppf sheaves. After answering these questions we turn to the theory of algebraic stacks to answer Question 4.

These first questions can be answered by proving an "arithmetic Steenrod Theorem" together with the "yoga of fiber bundles". Here is the statement of the Theorem:

Theorem 1.10 (Arithmetic Steenrod Theorem)**.** *Let P be a principal G-bundle. Let* $\mathrm{Aut}(P)$ *denote the G-bundle automorphisms of P. Let $G' \subset G$ be a closed subgroup scheme. Let $P \to P/G'$ be the associated fibration.*

(1) *All the sections of $G'\backslash P' \to X$ give rise to G'-reductions of P.*
(2) *We have the following correspondence*

$$\{\ G'\text{-reductions of } P\ \}/(\mathit{isom}) \leftrightarrow \Gamma(X, P\backslash G')/\mathrm{Aut}(P).$$

Remark 1.11. Steenrod stated his theorem for topological spaces and we present the proof here for sheaves since we could nice find a suitable reference. We first learned about this approach from [Hir78, chapter 3] where it is partially treated for right actions in the category of algebraic varieties over $\mathbf{C}$. We found more details in [Bal09] and [Sor00] although these reference disagreed in some places (compare [Sor00, Lemma 2.2.3] and [Bal09, Remark 2.12, page 4] with Theorem 1.10). Because we can't find a complete reference for this theorem we give a full proof.

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

Question 4 is answered by the following theoremTheorem 1.10:

Theorem 1.12 (Moduli of Torsor Structures)**.** *Let X/R be a curve of genus $g \geq 2$. Suppose that $p > 3g-3$ and fix Σ_n an A_n-structure. The torsor/line bundle structures on $J^1_p(X)_n$ are parametrized by an algebraic stack $\mathcal{M}_{X_n}(\Sigma_n, \mathrm{AL}_{1,R_n})$ defined in Definition 6.8.*

This is proved in section 5.4 of the text. We found the notes [Sor00] particularly useful in this context and have adapted its notation for our purposes.

1.4. **Proof strategies.** We now make some remarks on the proofs of Theorems 1.6 and Theorem 1.12.

Remark 1.13 (Strategy of Theorem 1.6)*.* To prove that $J^1_p(X)_n$ has the structure of a torsor under some lift of FT_{X_0}, it suffices to show that $J^1_p(X)_n$ admits an AL_1-structure. Here are the 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 an 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 role 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 if $J^1_p(X)_n$ admits an $A_{n,d}$-structure then 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 4.2. The third and fourth steps are done simultaneously in section 4.3 and uses a "pairing" between group and Čech cohomology.

Remark 1.14 (Strategy of Theorem 1.10)*.* In this theorem we prove a variant of "Steenrod's Theorem" for fppf sheaves. This uses existence of limits in the category of fppf sheaves and technical computations. The main difficulty here was finding the correct setting in which to do this.

Remark 1.15 (Strategy of Theorem 1.12)*.* In an abstraction of our setup for 1.6 (with the requisite groups and group cocycles), we study the sections from Steenrod's theorem from a scheme-theoretic perspective. It turns out that the quotient in Steenrod's theorem is a quotient of scheme by a group scheme action and hence can be represented by an algebraic stack.

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.

While working on this paper the author was supported by MSRI in 2014, and by the European Reseach Council under the European Union's Seventh Framework Programme (FP7/2007-2013)/ ERC Grant agreement no. 291111/MODAG.

.

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

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

2. Wittferential algebra

In this section we gather material from [Bui95], [Bui96] and [Bui05] in a form that will be conventient for reference later. The expert reader may wish to skip this section.

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

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

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

Let A be a ring and $a \in A$. Recall that we have a well-defined morphism $\left[\frac{1}{a}\right] : aA \to A/\operatorname{ann}(a)$, where $\operatorname{ann}(a)$ denotes the annihilator ideal of a. This is used in what follows.

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 $\delta(x) = (\phi(x) - x^p)/p$.

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

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

Proof reference. The proofs are omitted. We refer to reader to [Bui96, section 1.3] for further discussion. □

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

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

where (relations) are generated by

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

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

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,

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

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

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

where $\dot{x} = (\dot{x}_1, \dots, \dot{x}_n)$ and $\dot{f} = (\dot{f}_1, \dots, \dot{f}_r)$. Here $(\dot{f}_1), \dots, (\dot{f}_r) \in R[x, \dot{x}]$ are computed using (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

$$\begin{tikzcd} A \arrow[r, "\delta"] \arrow[dr, "\delta_{p,1}"'] & B & . \\ & A_{p,1} \arrow[u, "u_\delta"'] & \end{tikzcd}$$

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

Proof reference. [Bui96, section 1.4]. □

2.3. **Data of p-derivations.**

Lemma 2.7. *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 $A \to B$.*
2. *An action $\rho : A \to W_{p,1}(B)$ (meaning a morphism of rings such that $(\pi_1)_B \circ g) = f : A \to B$ the algebra map.*
3. *A morphism of A-algebras $A_{p,1} \to B$.*

Proof. The equivalence between morphisms from the Jet ring and p-derivations can be found essentially in [Bui96, Lemma 1.6]. Since being flat is equivalent to multiplication by p being injective, one uses the relation $\delta(x) = (\phi(x) - x^p)/p$ to show that lifts of the Frobenius and p-derivations are equivalent. □

The following example describes the target of p-derivations and factorization of ring homomorphisms when A and B are not flat over R.

Example 2.8. 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

$$\begin{tikzcd} A_{p,1} \arrow[r, "u"] & B \\ A \arrow[u] & \end{tikzcd}$$

[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

This induces $A \to B$. Suppose we are given an algebra structure $f : A \to B$. Suppose $A = A/p^{n+1}$. 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

$$\begin{tikzcd}
A_{p,1} \arrow[r, "u"] & B & , \\
A \arrow[u] \arrow[r, "\pi_1^*"] & A/p^n \arrow[u] &
\end{tikzcd}$$

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

Theorem 2.9. *Let A be a p-torsion free ring and ϕ a lift of the Frobenius on A inducing a lift of the Frobenius on $A_n = A/p^{n+1}$. 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

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

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

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

We leave it to the reader to verify that this makes sense. In doing so, it is useful to now that when $A_n = B/p^{n+1}$ where B is p-torsion free then

$$\begin{aligned}
\mathrm{ann}_A(p^j) &\cong p^{n-j}A, \\
A/\mathrm{ann}_A(p^j) &\cong A/p^{n-j},
\end{aligned}$$

and hence we have maps $[1/p] : pA_n \to A_{n-1}$. □

Theorem 2.10. *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. □

Lemma 2.11. *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 étale 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 and these ideas go back to Seidenberg. We prove a stronger result from which our result follows a fortiori.

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

$$\begin{tikzcd} A \arrow[r] \arrow[d, "\alpha"] & B \arrow[d, "\beta"] \\ C \arrow[r] & C/I \end{tikzcd} \quad , \quad I^2 = 0, \tag{2.3}$$

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

$$\begin{tikzcd} A \arrow[d] \arrow[dr] & \\ W_{p,1}(C') \arrow[r] & C' \end{tikzcd} \quad ,$$

there exists a diagram

$$\begin{tikzcd} B \arrow[d] \arrow[dr] & \\ W_{p,1}(C') \arrow[r] & C' \end{tikzcd}$$

lifting the previous. We apply the infinitesimal lifting criterion (equation (2.3)) with the following choices:

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

Here $V_p(W_{p,1})$ denotes the kernel of the map $W_{p,1} \to \mathrm{id}$. □

3. p-Jets

References for this section include [Bui05], [Bui96] and [Bui95]. We present the material here for convenience. We summarize the results of this section:

1. The functors $X \circ W_{p,r}$ are represented by schemes $J_p^r(X)$ called p-jet spaces when X is defined over R_n.
2. Suppose $X/R = W_{p,\infty}(\bar{\mathbf{F}}_p)$ is flat. Then local sections of the map $(\pi_1)_n : J_p^1(X)_n \to X_n$ induce local p-derivations (equivalently local lifts of the Frobenius) on X_n and conversely.
3. If X/R is flat then $J_p^r(X_n) = J_p^r(X)_{n-r}$, in particular $J_p^1(X_n) = J_p^1(X)_{n-1}$.

3.1. **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:

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

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

Example 3.1. When $X = \operatorname{Spec}(A)$ 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

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

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. Bad localization behavior can be observed in the p-derivation rule for fractions

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

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.

Theorem 3.3 ([Bui96] section 1.4)**.** *Let $R = W_{p,\infty}(k)$ where k is perfect of characteristic p.*

(1) *Let X/R be a flat scheme. The functor $J_p^r(X)_n := X_{n+r+1} \circ W_{p,r}$ over X_n, is representable.*
(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 π_r.

Remark 3.4. Borger in [Bor11]] proves the following more difficult theorem: let $X/\mathbf{Z}$ be any scheme. The functor $J_p^r(X) := X \circ W_{p,r}$ is representable in the category of schemes over $\mathbf{Z}$.

Theorem 3.5. *Let X/R be a scheme which is flat over R. Let n, m, r, s be natural numbers.*

(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},*

$$J_p^m(X)_{n-m} \xrightarrow{(\pi_{r+s,s})_{n-r-s}} J_p^s(X)_{n-m} \ .$$

This is a morphism of schemes over R_{n-m}.

(2) *The sheaf of local sections*

$$\begin{tikzcd} J_p^1(X)_m \arrow[r, "\pi_1"] & X_n \arrow[l, bend right, "s"'] \end{tikzcd}$$

represents the sheaf of p-derivations (equivalently local lifts of the Frobenius)

$$\delta : \mathcal{O}(X_{n+1}) \to \mathcal{O}(X_n) = \mathcal{O}(X_{n+1})/p^{n+1}.$$

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

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

The first part of the proposition follows from an explicit description of the ideals given previously (Theorem 2.3). The second part follows from the characterization of lifts of the Frobenius on rings of the form $A_n = B/p^{n+1}$ (c.f. (2.10)). □

3.2. **Remarks on 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

$$\begin{tikzcd} & \vdots \arrow[d] & \vdots \arrow[d] & \\ \cdots \arrow[r] & J_p^r(X)_n \arrow[r] \arrow[d] & J_p^r(X)_{n-1} \arrow[r] \arrow[d] & \cdots \\ \cdots \arrow[r] & J_p^r(X)_n \arrow[r] \arrow[d] & J_p^r(X)_{n-1} \arrow[r] \arrow[d] & \cdots \\ & \vdots & \vdots & \end{tikzcd}$$

The p-formal schemes $\widehat{J_p^r}(X) := \operatorname{colim}_n \widehat{J_p^r}(X)_n$ used by Buium (in say [Bui05]) behave nicely. Officially the limit should be taken as in [Sta14, TagOAI6, Definition 68.5.9] (also see [Sta14, TagOAIT, Lemma 68.8.1] to see this limit is a formal scheme and [Sta14, TagOAIT, Remark 68.8.3] to see why this limit and the limit from EGA coincide.) 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 3.6. Let $R = W_{p,\infty}(k)$ where k is a perfect field of characteritic p. Let $X = \operatorname{Spec}(R[x]/(f))$ (using multi-index notation). In the category of R-schemes, there are no sections s of

$$\begin{tikzcd} J_p^1(X)_0 \arrow[r, equal] & J_p^1(X_1) \arrow[r, "\pi_1"'] & X_1 \arrow[l, bend right, "s"'] \end{tikzcd} ,$$

since 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 3.7. Let $R = W_{p,\infty}(\mathbf{F}_p)$. Write

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

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

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

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

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

4. Proof of Theorem 1.6

The following sections prove Theorem 1.6.

4.1. **Step 1: Affine bundle structures.**

Definition 4.1. Let $X \in \mathsf{Sch}_B$. An **étale coordinate chart** of X is pair (U, ε) consisting of and open subset $U \subset X$ together with with an étale morphism $\varepsilon : U \to \mathbf{A}_B^{\dim_B(X)}$.

Recall that any smooth scheme $X/B = R$ of relative dimension d admits étale coordinate atlas by affine opens, i.e. there is a cover by affine opens $(U_i \to X)_{i \in I}$ and étale maps $f_i : U_i \to \mathbf{A}^d_R$.

The following lemma shows that étale coordinate charts induce $\mathbf{A}^1$-bundle trivializations of the first jet space.

Lemma 4.2 ([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 $\widehat{J}^1_p(X) \cong \widehat{X} \widehat{\times}_Y \widehat{J}^1_p(Y)$.*
2. *If $f : X \to \mathbf{A}^d_R$ is étale then there exist an isomophism $\psi_f : \widehat{J}^1_p(X) \cong \widehat{X} \widehat{\times} \widehat{\mathbf{A}}^d_R$*

Definition 4.3. We call ψ_f from part 2 of Lemma 4.2 the **induced trivialization**.

Remark 4.4. If $X = \mathrm{Spec}\, A$ and $f^* : R[T_1, \dots, T_n] \to A$ is étale then $\mathcal{O}(J^1(X)) = \mathcal{O}(X)[\dot{T}_1, \dots, \dot{T}_n]\widehat{\ }$. Here we have identified the étale parameters T_i with their image under f^*.

Remark 4.5. We have $J^1_p(Y)_n = (\pi_1^{-1})_n(Y_n)$ if $Y \hookrightarrow X$ is an open immersion R-schemes when X is flat over R.

Definition 4.6. Let X be a smooth projective curve. Let $\varepsilon_1, \varepsilon_2 : U \to \mathbf{A}^1_R$ be two étale coordinate charts. We will say that ε_1 and ε_2 are **compatible** and write $\varepsilon_1 \sim \varepsilon_2$ if and only if $\psi_{\varepsilon_1} \sim_{A_n} \psi_{\varepsilon_2}$.

Consider now, X as an embedded curve: $\varphi : X \to \mathbf{P}^N$. We will say that $H_1 \sim H_2$ if the associated étale projectsions are compatible: $\varepsilon_{H_1} \sim \varepsilon_{H_2}$.

Remark 4.7. The relation of compatibility, $\sim$, is an equivalence relation.

Lemma 4.8. *Let $\mathbf{G}(1,N)$ denote the Grassmannian of lines in $\mathbf{P}^N$.*

1. *For $H \subset \mathbf{G}(1,N)$, there exists some $U_H \subset \mathbf{G}(1,N)$ open such that for all $H' \in U_H(R)$ we have $\varepsilon_H \sim \varepsilon_{H'}$.*

(2) *Suppose* $\mathbf{P}^{N_1} \times \mathbf{P}^{N_2} \to \mathbf{P}^{N_3}$*, with* $N_3 = (N_1+1)(N_2+1) - 1$*. For all* $H \subset \mathbf{P}^{N_1}$ *there exists some* $H' \subset \mathbf{P}^{N_3}$ *such that* $\varepsilon_H \sim \varepsilon_{H'}$ *with respect to their embeddings.*

(3) *Suppose that* Σ_1 *and* Σ_2 *are* A_n*-structures induced from embeddings* $\varphi_1 : X \to \mathbf{P}^{N_1}$ *and* $\varphi_2 : X \to \mathbf{P}^{N_2}$*. Then* $\Sigma_1 = \Sigma_2$*.*

Proof. Variation of an étale parameter gives a family of equations $f(x_1, \widetilde{x}_2, t) = 0$ where t is a coordinate for $\mathbf{G}(1,N)$. The condition for incompatibility of the associated parameter x_1 and $\widetilde{x}_2$ is given by

$$\frac{\partial f}{\partial x_1} \equiv \frac{\partial f}{\partial \widetilde{x}_2} \equiv 0 \mod p.$$

This defines a proper closed subset of $\mathbf{G}(1,N)$.

The Segre embedding $\mathbf{P}^{N_1} \times \mathbf{P}^{N_2} \to \mathbf{P}^{(N_1+1)(N_2+1)-1}$ is given by $([x_i],[y_i]) \mapsto [x_i y_j]$. The image has coordinates $[z_{ij}]$ and is characterized by the vanishing of 2×2 minors. Fixing a line in $\mathbf{P}^{N_1}$ then fixing a fiber induces an identical projection: the restriction to $Z_{ij} = 0$ for $i \neq N_2$ and replacing $[y_j]$ with $[z_{N_2 j}]$ in the equations defining H_2 in $\mathbf{P}^{N_2}$ give us our hyperplane which induces the same projection as ε_{H_2}.

Using the notation as in part 1, let $H_1 \subset \mathbf{P}^{N_1}$ and $H_2 \subset \mathbf{P}^{N_2}$ be hyperplanes. Let $N_3 = (N_1+1)(N_2+1) - 1$ and $H_1', H_2' \subset \mathbf{P}^{N_3}$ be such that $\varepsilon_{H_1} \cong \varepsilon_{H_1'}$ and $\varepsilon_{H_2} \cong \varepsilon_{H_2'}$ as per part 2. Consider now $U_{H_1'}$ and $U_{H_2'}$ open subset of $\mathbf{G}(1,N_3)$ as in part 1. Both of these are nonempty by the existence of the structures Σ_1 and Σ_2. Since the interesection of two nonempty open set is open we are done. □

4.2. Step 2: Existence and uniqueness 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

$$A_n := \{a_0 + a_1 T + pa_2 T^2 + \cdots + p^{n-1} a_n T^n : a_1 \in \mathcal{O}_{X_n}^\times, a_i \in \mathcal{O}_{X_n}\} \subset \underline{\mathrm{Aut}}(\mathbf{A}^1_{R_{n-1}}).$$

Proposition 4.9. $A_n \subset \underline{\mathrm{Aut}}(\mathbf{A}^1_{R_{n-1}})$ *is a subgroup. Also, it is a group scheme over* R_{n-1} *given by*

$$A_n = \operatorname{Spec} R_{n-1}[a_0, a_1, \frac{1}{a_1}, pa_2, \ldots, p^{n-1}a_n].$$

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

$$\begin{aligned} f(T) &= a_0 + a_1 T + pa_2 T^2 + \cdots + p^{n-1} a_n T^n, \\ g(T) &= b_0 + b_1 T + pb_2 T^2 + \cdots + p^{n-1} b_n T^n \end{aligned}$$

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

If is sufficient to show that every term in

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

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 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

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

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 4.10 (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 $\psi_U : J^1_p(U) \to \widehat{U} \widehat{\times} \widehat{\mathbf{A}}^1$ 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 $\mathcal{O}^1(U) = O(U)[\dot{y}]^{\hat{}}$ and $\mathcal{O}^1(V) = \mathcal{O}(V)[\dot{x}]^{\widehat{p}}$. This means we have

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

[5] see Lemma 4.2

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

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

where for a polynomial $g(x) = a_0 + a_1 x + \cdots + a_n x^n$ 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

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

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

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

Since

$$\begin{aligned} pB^{-3}A^2C &= p\frac{(R + {f^{\phi}}_x(x^p,y^p)\dot{x})^2 {f^{\phi}}_{yy}(x^p,y^p)}{2{f^{\phi}}_y(x^p,y^p)^3} \\ AB^{-1} &= \frac{1}{{f^{\phi}}_y(x^p,y^p)}[R + {f^{\phi}}_x(x^p,y^p)\dot{x} + p{f^{\phi}}_{xx}(x^p.y^p)\dot{x}^2/2 \\ &\quad -p\frac{{f^{\phi}}_{xy}(x^p,y^p)\dot{x}}{{f^{\phi}}_y(x^p,y^p)}(R + {f^{\phi}}_x(x^p,y^p)\dot{x})] \end{aligned}$$

we get

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

where

$$\begin{aligned} \alpha &= -\frac{R}{{f^{\phi}}_y(x^p,y^p)} + p\frac{R^2{f^{\phi}}_y y(x^p,y^p)}{2{f^{\phi}}_y(x^p,y^p)^3} \\ \beta &= -\frac{-{f^{\phi}}_x(x^p,y^p)}{{f^{\phi}}_y(x^p,y^p)} + p\frac{{f^{\phi}}_{xy}(x^p,y^p)R}{{f^{\phi}}_y(x^p,y^p)^2} + \frac{pR{f^{\phi}}_x(x^p,y^p){f^{\phi}}_y y(x^p,y^p)}{{f^{\phi}}_y(x^p,y^p)^3}, \\ \gamma &= -\frac{{f^{\phi}}_{xx}(x^p,y^p)}{2{f^{\phi}}_y(x^p,y^p)} + \frac{{f^{\phi}}_{xy}(x^p,y^p){f^{\phi}}_x(x^p,y^p)}{{f^{\phi}}_y(x^p,y^p)^2} + \frac{{f^{\phi}}_x(x^p,y^p)^2{f^{\phi}}_{yy}(x^p,y^p)}{2{f^{\phi}}_y(x^p,y^p)^3}. \end{aligned}$$

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

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

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

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

so that its general term takes the form

$$p^{d-1} a^d_{i,j} \dot{x}^i (a_0 + a_1\dot{x} + p a_2 \dot{x}^2 + \cdots + p^{n-2} a_{n-1}\dot{x}^{n-1})^j.$$

We expand this general term further to get

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

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 $kf_k(S,T) \equiv 0 \mod p$ for $k = 1,\ldots,d$. If $p \nmid k$ this means that $f_k(S,T) = 0$ which tells us that

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

Note in particular that

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

□

The following remark gives our conventions for projections to and from linear subspaces of projective spaces.

Remark 4.11 (remarks on projections). By a decomposition of $\mathbf{P}^n$ (over R) we will mean a collection of linear forms $\lambda = \{l_0, \dots, l_n\}$ in general position together with its associated linear subspaces. For $0 \leq d \leq n$ 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 étale onto its image.

Lemma 4.12. *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 étale 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 $\pi(x_1, \dots, x_r, \dots, x_n) = (x_1, \dots, x_r)$ and curves of the form $X = \operatorname{Spec} \ R[x_1, \dots, x_n]/(f_1, \dots, f_e)$.

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 $f = (f_1, \dots, f_e)$ with respect to the variables $(x_{r+1}, \dots, x_n)$ evaluated at a.

We use the following two facts:

(1) The condition on π being étale 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 étale 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 étaleness by property 1.

The second property is a special case of the first. □

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

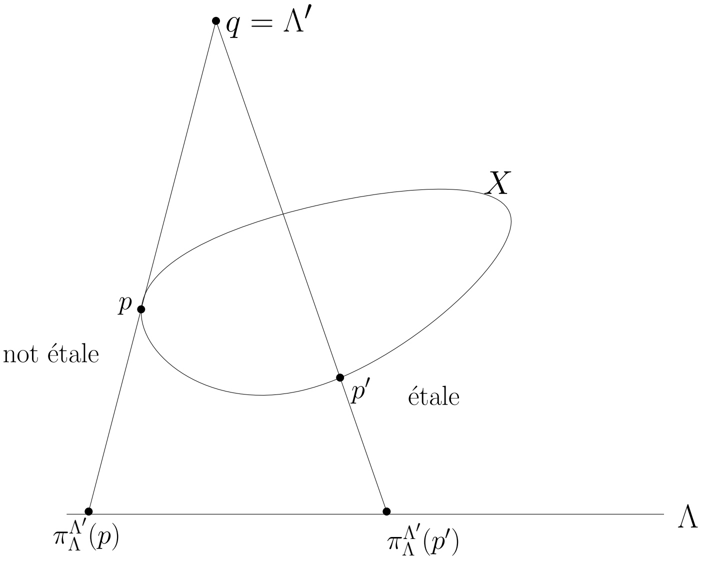

Figure 1. A projection in to Λ with center Λ'.

Lemma 4.13. *Let $X \subset \mathbf{P}^n_R$ be a smooth irreducible curve of degree $d < p$. Let π_1 and π_2 be projections onto lines in $\mathbf{P}^2_R \subset \mathbf{P}^n_R$ where the centers of projections do not intersect X.*

Let $\varepsilon_1, \varepsilon_2 : U \to \mathbf{A}^1_R$ 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 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.

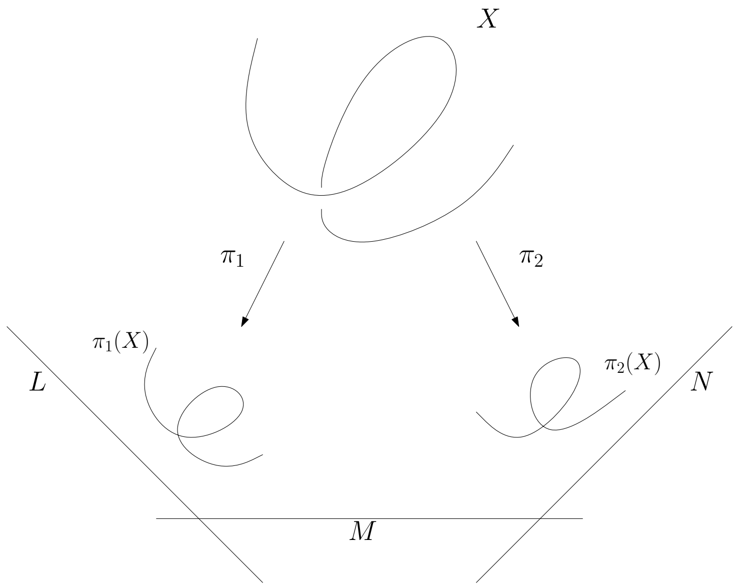

Figure 2. A curve $X \subset \mathbf{P}^N$ with two projections onto $\Lambda_1 = \overline{L, M}$ and $\Lambda_2 = \overline{M, N}$ both isomorphic to $\mathbf{P}^2$. The étale projections $\varepsilon_L, \varepsilon_M$ and ε_N to the lines L, M and N which induce the trivializations on the $J^1(X)$ factor through the projections π_1 and π_2

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

$$\begin{tikzcd}
R[S,T] \arrow[r, "\sigma"] \arrow[d, "\alpha"] & B \arrow[d] \\
R[S,T]/p \arrow[r, "\sigma_0"] & B/p.
\end{tikzcd}$$

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

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 étale projections

[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 $(f) = (f_i)$.

(Lemma 4.12)

$$\begin{aligned}&\frac{\partial f}{\partial p} + f^{\phi}{}_x(x^p,y^p)\dot{x} + f^{\phi}{}_y(x^p,y^p)\dot{y}\\ &+\frac{p}{2}(f^{\phi}{}_{xx}(x^p,y^p)\dot{x}^2 + 2f^{\phi}{}_{xy}(x^p,y^p)\dot{x}\dot{y} + f^{\phi}{}_{yy}(x^p,y^p)\dot{y}^2 \equiv 0 \mod p^2\end{aligned}$$

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 étale 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 (Lemma 4.10) to establish

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

for each $n \geq 2$. □

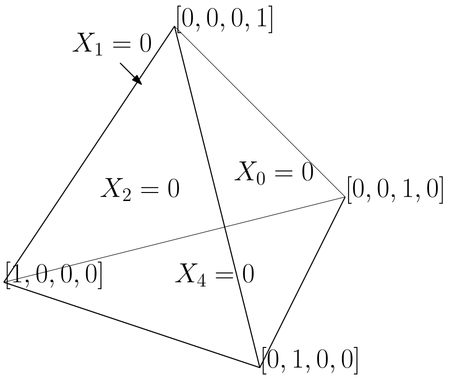

Figure 3. A picture of $\mathbf{P}^3$ with its standard decomposition.

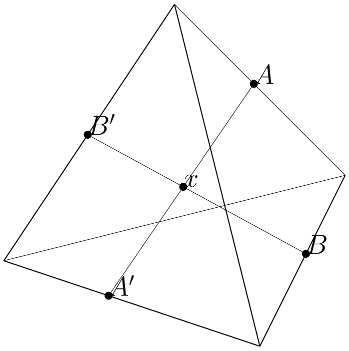

Figure 4. If there exists some point x such that T_xX is equal $L(\Lambda', \Lambda, P)$ for all $\Lambda \in \lambda_2$ then we would have $\overline{AA'} = \overline{B'B}$. The situation looks very bad in this simple case.

Lemma 4.14. *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 $\pi_\Lambda : X_\Lambda \to \mathbf{A}^1_R \subset \mathbf{P}^1_R$ étale onto its image. (cf section 4.11).*

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

$$\pi_\Lambda^{\Lambda'} : X \to \Lambda \cong \mathbf{P}^1 \text{ or } \mathbf{P}^2$$

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 4.2 and 4.2 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 $X \subset \mathbf{P}^N_{\bar{\mathbf{F}}_p}$ 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 ($\bar{\mathbf{F}}_p$ is an infinite field) we can arrange so that X and W have an empty intersection. □

Theorem 4.15. *Let $R = W_{p,\infty}(k)$ where $k = \overline{\mathbf{F}}_p$. Let $X_d \subset \mathbf{P}^N_R$ be a smooth irreducible curve of degree d and suppose that $d > p$ then for every $n \geq 1$, $J^1_p(X)_n \to X_n$ admits an A_n-structure.*

Remark 4.16. Lemma 4.8 part gives uniqueness of the A_n-structure.

Proof. Let $\lambda = \{l_0, \dots, l_n\}$ as in Lemma 4.14. By change in coordinates we can assume without loss of generality that the $l_0, \dots, l_n$ are the coordinate hyperplanes given by $l_i = V(X_i)$. Let $l_0', \dots, l_n'$ be the coordinate axes, Let U_i be the subset of X where the projection map to l_i' is étale and $\varepsilon_i : U_i \to \mathbf{A}^1$ be the étale 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 4.13. 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. □

4.3. **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 4.17. *Let X/R be a scheme and $\pi : E \to X$ an $\mathbf{A}^1_R$-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* **??**.

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 $\underline{\mathrm{Aut}}(\mathbf{A}^1_{R_n}) = \mathrm{AL}_1(\mathcal{O}_{X_0})$.

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 $M_{n,r} \leq \underline{\mathrm{Aut}}(\mathbf{A}^1_{R_n})$ to be the automorphisms of degree less than or equal to 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 $\psi_{ij}^{(n)} \sim_{M_{n,r}} \psi'^{(n)}_{ij}$ and $\psi_{ij}^{(n+1)} \equiv \psi'^{(n)}_{ij} \mod p^{n+1}$. This completes the proof. □

To complete the proof of the Main theorem we apply Theorem 4.17 to E being the first p-jet space of a curve together with its A_n-structure given in section 4.2

Proof of Theorem 1.6. Consider the A_n-structure on $J^1_p(X)_n$ coming from Theorem 4.15. We apply theorem 4.17 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 4.17. □

5. How many torsor structures are there?

In this section we lay the ground work for proof of Theorem 1.10 and Theorem 1.12. This section culminates in the proof of Theorem 1.10.

5.1. **Frame bundles and torsors.** The standard references for torsors on the étale site of a scheme is [Mil80, chapter III, section 4.]. One should also consult [Sko01, Chapter 2, Definition 2.2.1].

By a left **principal G-bundle**, we will mean fiber bundle over X with fiber G and structure group G where the transition maps are given by right multiplication. We define G-torsors over X as in [Sko01, Chapter 2, Definition 2.2.1]. All torsors are assumed to be locally trivial. The yoga of Fiber bundles and Principal bundles can be found in [Neu09, section 1.1], [Bre10, Example 1.5] or [Bal09].

It is a standard fact that the category of left G-torsors on X is equivalent to the category of left principal G-bundles [Mil80, III, section 4, Proposition 4.1]. We will denote the category by $B_X(G)$. Since principal fiber bundles, torsors and fiber bundles with G-structures are all equivalent we will take morphisms of each of these objects to be the morphism of the associated G-torsor of frames. All of these objects are classified by elements of $H^1(X, G)$. (See [Sta14, Tag0497] for a proof for arbitrary sites. A reference for the statement is [Bre10, pg 2]. Also, note that SGA 4.5 only does abelian torsors!)

5.2. **Amalgamated products.**

Definition 5.1. Let L be a left G-space over X. Let R be a right G-space over X. We define the **amalgamated product** via of L and R by $R\times^G L := (R\times_X L)/G$ Where the right action on the product is defined by $((x,y),g)) \mapsto (xg, g^{-1}y)$.

Remark 5.2. (1) There are two ways to take amalgamated products. Some authors prefer right amalgamation (see [Bre10, section 1.2], [Hir78, pg 44], [Bal09, Remark 2.2]) and some authors prefer left amalgamation (see [Mit01, beginning of chapter 3]). It doesn't matter if you quotient by a left or right action: define the **(left) amalgamated product**

$$R\times_G L := G\backslash(R\times_X L)$$

where the left action on $R\times_X L$ is given by

$$(g,(x,y)) \mapsto (xg^{-1}, gy).$$

One can check that $R\times_G L \cong R\times^G L$.

(2) Let P' be a left G'-space. We give $G\times^{G'} P' = P'(G)$ the structure of a left G-space given by $g\cdot[g_0,p'] = [gg_0,p']$. Note that this is not that action $g\cdot[g_0,p'] = [g_0g^{-1},p']$. This was extends the G'-action on P'. This can give rise to confusion.

5.3. **Preparations for the Steenrod theorem.**

Definition 5.3. Let S be a scheme. Let $G' \subset G$ be a closed immersion of affine group schemes over S. We say that $G' \subset G$ has the **Steenrod property** if the quotient map

$$q : G \to G' \backslash G = Y$$

is a left principal G'-bundle on Y and the map $q : G \to G' \setminus G$ is a universal categorical quotient [vdGM07, Definition 4.5 (iv)].

Quotients in the category of fppf sheaves are automatically universal quotients [vdGM07, 4.30, page 62] hence it will be convenient to embed all schemes into the category of sheaves on $(\mathsf{Sch}_S)_{fppf}$ the big fppf site of the category Sch_S.

Lemma 5.4. *Work with big fppf sheaves. Let $Y := G' \setminus G$. Let $G'_Y = G' \times Y$ with the Y-map being the canonical projection. Let $\pi : G \to Y$ be the canonical quotient map. The left action of G'_Y on G over Y, gives G the structure of a G'_Y-torsors over Y.*

Proof. Observe that $(G'_Y \times_Y G)(T) = G'(T) \times G(T)$ so we can consider the action of $G'(T)$ fiber by fiber. For each $\overline{x} \in G'(T) \backslash G(T)$ the action $G'(T) \times \pi_T^{-1}(\overline{x}) \to \pi_T^{-1}(\overline{x})$ is clearly faithful and full. The commutativity of the diagram

$$\begin{tikzcd}
G'(T) \times G(T) \arrow[rr] \arrow[dr] & & G(T) \arrow[dl] \\
& (G' \backslash G)(T) &
\end{tikzcd}$$

gives us an action $G'_Y \times_Y G \to G$ over Y which as presheaves is a torsor. Sheafifying preserves the torsor structure.

□

Remark 5.5.
1. In the category of (big fppf)-sheaves the map $q : G \to G' \backslash G$ has a G' worth of elements in each fiber. There is an action of G' on each of the fibers.
2. The principal bundle condition is equivalent to the existence of a cover of $(U_i \to G' \backslash G)_{i \in I}$ such that $q : G \to G' \backslash G$ has sections $s_i : U_i \to G$ such that $\sigma \circ s_i = \mathrm{id}_{U_i}$.

For the remainder of this section we will assume $G' \subset G$ has the Steenrod property.

The following is to be taken in the category of algebraic spaces.

Lemma 5.6. *Let $G' \subset G$ have the Steenrod property. Let $(\pi : E \to X) \in B_G(X)$. Let $q : E \to Y := G' \backslash E$ be a universal categorical quotient. We have $(q : E \to Y) \in B_{G'}(Y)$.*

Proof. It is enough to show that there exists a cover $(Y_j \to Y)_{j \in J}$ and trivializations $E_{Y_j} \cong Y_j \times G'$ which are isomorphisms of left G'_{Y_j}-spaces. There exists a cover by $(U_i \to X)_{i \in I}$ such that $E_{U_i} \cong U_i \times G$ as left G_{U_i}-spaces. Since $Y = G' \backslash E$ is a categorical quotient we have that

$$Y_{U_i} \cong G'_{U_i} \backslash E_{U_i} \cong G'_{U_i} \backslash G_{U_i}$$

and we have the diagram

$$\begin{tikzcd}
E_{U_i} \arrow[r] \arrow[d] & U_i \times G \arrow[d, "\mathrm{id}_{U_i} \times \sigma"] \\
Y_{U_i} \arrow[r] & U_i \times G'\backslash G
\end{tikzcd}$$

By the Steenrod property there exist a cover $(W_k \to G'\backslash G)_{k \in K}$ such that $\sigma : G \to G'\backslash G'$ trivializes as a G'-bundle. In other words, there exists isomorphisms

$$\psi_k : G_{W_k} \cong W_k \times G' \tag{5.1}$$

as left G'_{W_k}-spaces. Base-changing the trivializations ψ_k by the maps U_i trivialize the map $\mathrm{id}_{U_i} \times \sigma$ giving

$$(Y_j \to Y)_{j \in J} = (U_i \times W_k \to Y)_{(i,k) \in I \times K}$$

as the desired trivializing cover. □

Lemma 5.7. *The map $\rho : Y \to X$ is a $(G'\backslash G)$-bundle with G-structure. The (nonfaithful) representation in the giving the structure $G \to \mathrm{Aut}(G' \setminus G)$ takes g to the automorphism given by right multiplication by g^{-1}.*

Proof. Since $\pi : E \to X$ is a left principal G-bundle there exists a cover $(U_i \to X)_{i \in I}$ and trivializations $\psi_i : E_{U_i} \to U_i \times G$ such that the transition maps ψ_{ij} are given by right multiplication. [7] Using the fact $q : E \to G'\backslash E = Y$ is a categorical quotient we have

$$Y_{U_i} = (G'\backslash E)_{U_i} \cong U_i \times (G'\backslash G),$$

and we see that the transitions between trivializations are given by right multiplication by elements of $G_{U_{ij}}$. □

5.4. **Proof of Theorem 1.10.** We will now state Steenrod's theorem concerning the reduction of structure group F-fiber bundles $J \to X$ with structure group G.

Given a principal G-bundle P we get the associated F-fiber bundle with structure group G by taking $F \times^G P$. Given a F-fiber bundle with structure group G, we map to the sheaf of trivializations.

Under this correspondence the structure group of the principal bundle P reduces $G' \leq G$ if and only if the structure group of the F-fiber bundle reduces if and only if there is an element of $\xi' \in H^1(X, G')$ which maps to $\xi = \mathrm{cl}(J) \in H^1(X, G)$ under the natural map induced by $G' \to G$.

We can now describe how to get reductions of principal fiber bundles with structure group G. Let $\pi : P \to X$ be such a left G-torsor. Here we quotient our left G-torsor P by the subgroup $G' \leq G$ we are interested in to get

$$Q := G'\backslash P.$$

This gives us a factorization of the map $\pi : P \to X$ from the principal bundle to the base space as a map to the quotient $q : P \to G'\backslash P = Q$ then a map to the base

[7] This is equivalent to ψ_i being an isomorphisms of left G_{U_i}-spaces.

$\pi' : Q \to X$:

$$\begin{tikzcd}
P \arrow[dd, "\pi"'] \arrow[dr, "q"] & . \\
& G'\backslash P = Q \arrow[dl, "\rho"] \\
X &
\end{tikzcd}$$

The map q from the original principal bundle P to the quotient $Q = P/G$ turns out to be a principal G'-bundle over Q for the subgroup $G' \leq G$ we were considering. When viewing P as a principal G'-bundle over Q we use the notation P_Q. It turns out that one can parametrize all reductions as sections of Q modulo automorphisms:

Theorem 5.8 (Steenrod's Theorem). *In the category* $\mathrm{Shv}((\mathsf{Sch}_S)_{fppf})$ *fix the following:*

- $G' \subset G$ *inclusion of subgroups*
- $P = (\pi : P \to X) \in B_G(X)$
- $Q := G'\backslash P \cong G'\backslash G \times^G P$
- $P_Q = (q : P \to Q) := G'\backslash P \times^G P \in B_{G'}(Q)$

Let $\rho : Q \to X$ *fit into the diagram*

$$\begin{tikzcd}
P \arrow[d, "\pi"] \arrow[dr, "q"] & . \\
X & Q = G'\backslash P \arrow[l, "\rho"]
\end{tikzcd}$$

The following statements hold:

(1) P_Q *is a* G'*-reduction of* $\rho^* P_X$*. More precisely, the pair* (P_Q, φ) *where*

$$\varphi : G \times^{G'} P_Q \to \rho^* P_X$$

$$\varphi([g, e]) = [g \cdot e, q(e)].$$

makes (P_Q, φ) *a* G'*-reduction of* $\rho^* P_X$*.*

(2) *If* $s \in \Gamma(X, Q)$ *then* $s^*(P_Q) \in B_X(G')$ *and there exists and isomorphism of* G*-torsors* $\alpha = \alpha_s : G' \times^G s^*(P_Q) \to P$ *making* $s^* P_Q$ *are* G'*-reduction of* P*.*

(3) *All reductions* (P', φ) *of* P *to structure group* G *are isomorphic to reductions coming from pullbacks of sections of* $Q = G'\backslash P$*. In fact, the associated* $(P', \varphi) \mapsto s_\varphi \in \Gamma(X, Q)$ *is canonical.*

(4) *Let* $s_1, s_2 \in \Gamma(X, Q)$*. Let* $P_1 = s_1^* P_Q$ *and* $P_2 = s_2^* P_Q$ *be the associated reductions.*

$$P_1 \cong_{B_X G'} P_2 \iff \exists \alpha \in \mathrm{Aut}(P_X), {}^{\alpha}s_1 = s_2.$$

Proof. Since we are working with sheaves we may check everything on the level of points.

(1) We just need to check that the map alpha defines a morphism of left G-torsors. First observe that the action on the amalgamated product is $g \cdot$

$[g_0, e] = [gg_0, e]$. Next observe that the action of G on $P_Q = \rho^* P_X = P \times_X Q$ is given by $g \cdot (e, y) = (ge, y)$. We now consider the map

$$\alpha : [g_0, e] \mapsto (g_0 e, q(e)).$$

We show that the map alpha in fact lands in P_Y:

$$\pi(g_0 e) = \rho(q(e)) = \pi(e).$$

We show that α is well-defined: we only need to check that $\alpha([g_0 g', (g')^{-1} e]) = \alpha([g_0, e])$ for each g' in G'. This follows from

$$\begin{aligned} \alpha([g_0 g', (g')^{-1} e]) &= (g_0 g' (g')^{-1} e, q(g_0 g' (g')^{-1} e)) \\ &= (g_0 e, q(g_0 e)) \\ &= (g_0 e, q(e)) \\ &= \alpha([g_0, e]). \end{aligned}$$

We show that α is G-equivariant: recall that

$$g \cdot [g_0, e] := [gg_0, e],$$
$$g \cdot (e, y) := (ge, y).$$

We have

$$\begin{aligned} \alpha(g \cdot [g_0, e]) &= \alpha([gg_0, e]) \\ &= [gg_0 e, q(e)] \\ &= g \cdot (g_0 e, q(e)) \\ &= g \cdot \alpha([g_0, e]). \end{aligned}$$

Since any morphism of G-torsors is an isomorphism we are done.

(2) We will prove that the G'-bundle $s^* P_Q$ comes with a natural isomorphism

$$\varphi = \varphi_s : G \times^{G'} s^* P_Q \to P_X$$

making it a G'-reduction of P_X. The proof is the following string of equalities:

$$\begin{aligned} P_X &= (\rho \circ s)^* P_X \\ &\cong s^*(\rho^* P_X) \\ &= s^*(G \times^{G'} P_Q) \\ &= G \times^{G'} s^* P_Q. \end{aligned}$$

The last line follows from [Mit01, Proposition 3.6] which states that base change and amalgamated product commute for F-bundles with G-structures. [8]

(3) To every reduction (P', φ) there is a canonical section s of $\rho : Q \to X$ and an isomorphism $P' \cong s^* P_Q$ of G'-bundles.
- Take the G'-equivariant map $f = f_\varphi$ defined by the composition[9]

$$P' \to P'(G) = G \times^{G'} P' \to^{\varphi} P,$$
$$p' \mapsto [1, p'] \mapsto \varphi([1, p']).$$

[8] Let $(p : E \to B) \in \mathsf{Bun}(F; G)/B$. Let $f : B' \to B$. $f^*(P \times^G F) \cong (f^* P) \times^G F$.

[9] The left action of G on $G \times^{G'} P'$ is given by $g \cdot [g_0, p'] = [gg_0, p']$. The morphism $\varphi : P' \to G \times^{G'} P'$ is G'-equivariant $\varphi(g' \cdot p') = [1, g'p'] = [g', p'] = g' \cdot \varphi(p')$.

- Take the quotient by G' and descend f to a map

$$X \cong G' \backslash P' \to G' \backslash P = Q,$$

which gives our section s.

It remains exhibit a canonical isomorphism of G'-bundles $\alpha : P' \cong s^* P_Q$. Note that s fits into the fiber diagram.

$$\begin{tikzcd}
P' \arrow[r, "f_\varphi"] \arrow[d, "q'"', "G'"] & P \arrow[d, "G'"] \\
X = G' \backslash P' \arrow[r, "s"] & G' \backslash P =: Q
\end{tikzcd} \tag{5.2}$$

We claim the map

$$\alpha := q' \times_Q f_\varphi : P' \to s^* P_Q = X \times_{s,Q} P_Q$$

does the trick. It is enough to show a morphism of G' spaces.

From the pullback diagram (5.2) there is clearly a morphism $P' \to s^* P_Q$ of schemes. Observe the following:

- The map f_φ is G'-equivariant.
- The G'-action on $s^* P_Q$ comes from the G'-action on P_Q by base change.
- α which is the base change of f_φ and hence is G'-equivariant. This proves α is a G'-morphism of torsors and hence gives us the desired isomorphism.

(4) The forward direction is the "easy" one: given a section, one can show that the pullback by the section and the pullback by an acted one section are isomorphic.

Let (P'_1, φ_1) and (P'_2, φ_2) be two reductions of P to structure group G'. Suppose that we have an isomorphism of G'-bundles $\alpha : P'_1 \to P'_2$. Let s_1 and s_2 be the canonically associated sections of (P'_1, φ_1) and (P'_2, φ_2). We claim that there exists an automorphism $\gamma = \gamma_\alpha$ such that $s_1 = \gamma \circ s_2$.

We first how to explain how to get an automorphism from two sections $\alpha : P'_1 \to P'_2$: Consider the diagram

$$\begin{tikzcd}
P'_1(G) \arrow[rr, "G \times^{G'} \alpha"] \arrow[dr, "\varphi_1"'] & & P'_2(G) \arrow[dl, "\varphi_2"] \\
& P &
\end{tikzcd}$$

which when you follow around backwards from P gives you the automorphism $\gamma = \gamma_\alpha$:

$$\gamma = \varphi_2 \circ (G \times^{G'} \alpha) \circ \varphi_1^{-1}.$$

We now have a G'-equivariant diagram:

$$\begin{tikzcd}
P_1' \arrow[r, "\alpha"] \arrow[d, "f_{\varphi_1}"] & P_2' \arrow[d, "f_{\varphi_2}"] \\
P_1'(G) \arrow[d, "\varphi_1"'] & P_2'(G) \arrow[d, "\varphi_2"] \\
P \arrow[r, "\gamma_\alpha"] & P
\end{tikzcd},$$

Where we are using notation from the proof of Lemma 5.8 (3). From the proof of Lemma 5.8 (3), we know that taking the G'-quotient of this diagram gives

$$\begin{tikzcd}
& X \arrow[dl, "s_{\varphi_2}"'] \arrow[dr, "s_{\varphi_1}"] & \\
G'\backslash P \arrow[rr, "\gamma"] & & G'\backslash P
\end{tikzcd},$$

which proves our result.

□

Remark 5.9. Let $i : G' \to G$ denote the inclusion map. In terms of cohomology we have $\xi' = \mathrm{cl}(\pi) \in H^1(X, G)$ and $\xi' = \mathrm{cl}(q : E \to Q) \in H^1(Q, G')$ then

$$is^*\xi' = \xi.$$

6. Geometry of group cocycles and moduli of reductions

6.1. **Affine linear structures and torsor structures.** In this section we want to describe to what extent AL_n-structures on affine bundles determine torsors under vector bundles. First there is the obvious: given an AL_n-structure on an affine bundle we can define a torsor structure on the level of points by subtracting two sections in the affine coordinates. Because of affine linearity, this gives a well-defined torsor structure under some vector bundle. One may wonder: what is the vector bundle associated to this torsor structure? Well, this is the vector bundle pieced together from transition maps determined by the "linear" part of the "affine linear" transition. One way expressing the vector bundle is by saying it is a vector bundle E with trivializations $\varphi_i : E|U_i \to \mathcal{O}^n|U_i$ such that the transitions φ_{ij} are the image of the cocycle associated to the affine linear structure under the map $\mathrm{AL}_n \to \mathrm{GL}_n$.

This establishes that AL_n-structures give torsors under line bundles, but how well-defined is this process? For example does an AL_n-structure determine the torsor structure up to isomorphism? We first fix what we mean by a "torsor structure".

Definition 6.1. A **group-torsor pair** will be a triple (E, J, ρ) consisting of two sheaves (in whatever topology you want) E, and J where E is a sheaf of locally free $\mathcal{O}_X$-modules together with a morphism of sheaves $\rho : E \times J \to J$ giving a full and faithful action of E on J. A morphism of group-torsor pairs will be a morphism locally free sheaves $E_1 \to E_2$ such together with an equivariant morphisms $J_1 \to J_2$. This category will be denoted by $\mathsf{GTPAIRS}$.

I want to describe now the extent to which the AL_n-cocycle determines the group torsor structure. The correct way to do this appears to be in terms of "Descent Data" for the group-torsor pair on the underlying affine bundles.

Definition 6.2. We define the category of $DD(\mathcal{U}, E, J)$ for affine bundles E and J. Objects will be pairs (ψ_i, φ_i) consisting of an AL_n-atlas $(\psi_i : E_{U_i} \to U_i \times \mathbf{A}^r)$ for J and a GL_n-atlas $(\varphi_i : E_{U_i} \to \mathbf{G}^r_{a,U_i})$ for E such that $\varphi_{ij}(v) = B_{ij}v$ and $\psi_{ij}(t) = a_{ij} + B_{ij}t$. Isomorphisms will be a collections $(a_i + B_it) \in C^0(\mathcal{U}, \mathrm{AL}_n)$. The collection $(a_i + B_it)$ will be viewed as a morphism $(\psi_i, \varphi_i) \to (\psi_i', \varphi_i')$ where ψ_i' and φ_i' are given by $\psi_i' = (a_i + B_it) \circ \psi_i$ and $\varphi_i' = B_i \cdot \varphi_i$.

One would hope to make a statement like "the functor from group-torsor pairs on underlying vector bundles to descent data on underlying vector bundles is an equivalence of categories". This seems to be too silly. However, there is a functor from descent data to group-torsor pairs with the property that every isomorphism of descent data induces the identity of the group torsor pair.

Lemma 6.3. *There is a functor from*

$$\text{construct} : DD(\mathcal{U}, E, J) \to \mathsf{GTPAIRS}$$

defined such that every isomorphism of descent data induces the identity of the group-torsor pair.

Proof. We describe how to construct a group torsor pair up to isomorphism. Let e_1 and e_2 be local sections of J. Fix a collection of trivializations $\Psi = (\psi_i)$. Consider the division map $-_\Psi$ defined by

$$e_1 -_\Psi e_2 := \psi_i^{-1}(\psi_i(e_1) - \psi_i(e_2)). \tag{6.1}$$

(1) The division map is well-defined: It suffices to look at two trivializations ψ_1 and ψ_2. Observe that

$$\begin{aligned} \psi_1(e_1) - \psi_1(e_2) \quad &\mapsto^{\varphi_{21}} \quad L_{g_{21}}(\psi_1(e_1) - \psi_1(e_2)) \\ &= \quad L_{g_{21}}\psi(e_1) + \beta_{21} - (L_{g_{21}}\psi_1(e_2) + \beta_{21}) \\ &= \quad \psi_2(e_1) - \psi_2(e_2), \end{aligned}$$

so the division map is well-defined. The action is faithful because it is locally.

(2) The action is $-_{(\psi_i)}$ independent of the choice of trivialization: Let $(b_i, g_i) \in C^0(\mathcal{U}, \mathrm{AL}_r)$ and (ψ_i) a collection of AL_n- compatible trivializations. One verifies that

$$e_1 -_{(b_i,g_i)\cdot(\psi_i)} e_2 = e_1 -_{(\psi_i)} e_2$$

directly on the nose (c.f. Definition 6.1 and the fact that the ψ_i's induce local isomorphisms of the pairs $(E|U_i, J|U_i)$ and $(E|U_i, \mathcal{O}^r|U_i)$).

(3) We claim the group-torsor pair (E, J) associated to the isomorphism class of (ψ_i, φ_i) is unique. We need to show that after acting on a pair (ψ_i, φ_i) by an element $(b_i, g_i)_{i \in I} \in Z^1(\mathcal{U}, \mathrm{AL}_n)$ diagonally we get the same group-torsor pair. First observe that the vector bundle doesn't change since modifying (φ_i) just gives a different set of trivializations. The rest follows from what has previously been stated.

□

Now that we have answered this question we can ask how this construction of torsors relates to the well-known "torsors are classified by $H^1(E)$" statement. Here we view an E-cocycle as objects of a category and coboundaries as morphisms between them. We will call this category $DD(\mathcal{U}, E)$. To setup a correspondence between appropriate AL_n-structures and elements of $H^1(E)$ we need to forget a little bit about the category $DD(\mathcal{U}, E, J)$ previously constructed . To do this we construct a new category $DD'(\mathcal{U}, E, J)$ whose objects are pairs (a_{ij}, φ_i) where ($\varphi_i : E|U_i \to \mathcal{O}^n|U_i$) is a GL_n-structure on E and (a_{ij}, φ_{ij}) is a AL_n-cocycle (here we used the canonical isomorphism $\mathrm{AL}_n \cong \mathbf{G}_a^n \rtimes \mathrm{GL}_n$) and morphisms between these guys will again be elements of $C^0(\mathrm{AL}_n)$ where we regard (a_i, B_i) as a morphisms $(a_{ij}, \varphi_i) \to (a'_{ij}, \varphi'_i)$ where

$$a'_{ij} = a_i + B_i a_{ij} - \varphi_{ij} B_j^{-1} a_j,$$
$$\varphi'_i = B_i \cdot \varphi_i.$$

The above discussion can be summarized by stating that there are a series of functors encoding cohomology of group-torsor pairs in categories, each with decreasing complexity:

$$DD(\mathcal{U}, E, J) \to DD'(\mathcal{U}, E, J) \to Z^1(\mathcal{U}, \mathbf{G}_a^n \rtimes \mathrm{GL}_n).$$

The intermediate category has the following property:

Lemma 6.4. *The map $\Upsilon : DD'(\mathcal{U}, E, J) \to Z^1(\mathcal{U}, E)$ defined by $\Upsilon(a_{ij}, \varphi_i) = (\varphi_i(a_{ij}))$ sends isomorphisms to isomorphisms and is essentially surjective.*

Proof. We first check how Υ behaves under morphisms (modification by coboundaries). To do this we factor a coboundary (a_i, b_i) as $(a_i, 1)(0, b_i)$ and look at the action of the boundaries $(1, b_i)$ and $(a_i, 1)$ separately. We claim that the action under $(1, b_i)$ leaves the map fixed and the action of $(1, b_i)$ modifies the image by a cocycle. We first show that this map sends isomorphisms to isomorphisms.

To show essential surjectivity, we need to show that every element of the target is isomorphic to some image. A computation with cocycles shows that $Z^1(\mathcal{U}, \mathrm{AL}_r)_{(\varphi_{ij})} \to Z^1(\mathcal{U}, E)$ given by $(a_{ij}, \varphi_{ij}) \mapsto \varphi_i^{-1}(a_{ij})$ is a bijection — here, $Z^1(\mathcal{U}, \mathrm{AL}_r)_{(\varphi_{ij})}$ denotes the inverse image of the cocycle $(\varphi_{ij}) \in Z^1(\mathcal{U}, \mathrm{GL}_n)$ in $Z^1(\mathcal{U}, \mathrm{AL}_n)$ where the map is the natural one induced by the quotient $\mathrm{AL}_n \cong \mathcal{O}^n \rtimes \mathrm{GL}_n \to \mathrm{GL}_n$. We also know that the map $Z^1(\mathcal{U}, \mathrm{AL}_r)_{(\varphi_{ij})} \to DD'(\mathcal{U}, E, J)$ given by $(s_{ij}) \mapsto (\varphi_i^{-1}(s_{ij}), \varphi_{ij})$ is essentially surjective (since every trivialization can be modified to a "standard one"). □

6.2. **Geometry of group cocycles.** This section should be viewed as giving a geometric interpretation of Theorem 1.7.

Fix an F-fiber bundle $\pi : J \to X$ with G-structure Σ. We can say more about the reductions of the structure group in the following special situation:

- There exists a linear right action of G on some abelian group A and a right group cocycle $\tau : G \to A$ such that $G' = \ker(\tau)$.

Given the extra condition, we fix some more notation: we let $\overline{G} = G$ be the quotient through which the action of G on A factors and let $\Phi_\tau : G \to \bar{G} \ltimes A$ be the group homomorphism associated to τ.

First we give a remark in elementary group theory that we will use later

Remark 6.5. Let $G', G'' \subset G$ be subgroups.

(1) $G'G'' = G$ and $G' \cap G'' = 1$ makes the representation of elements as $\alpha\beta$ with $\alpha \in G'$ and $\beta \in G''$ unique. For $[\alpha\beta] \in G' \backslash G$ we have $[\alpha\beta] = [\beta]$ and the representative is unique.

(2) Suppose the exact sequence

$$\begin{tikzcd} 1 \arrow[r] & G'' \arrow[r, "j"] & G \arrow[r, "p"] & G' \arrow[r] & 1 \end{tikzcd}$$

is split by $s : G' \to G$. Using the splitting, identity G' as a subgroup $G' \subset G$. Under these conditions $G' \cap G'' = 1$ and $G'G'' = 1$.

(3) Let G, G' and G'' be as in 1 or 2. Write ψ uniquely as $\psi = \alpha_\psi \beta_\psi$ where $\alpha_\psi \in G'$ and $\beta_\psi \in G''$. Let $\tau : G \to G''$ be the map $\tau[\psi] = \beta_\psi$. Let G' act on the right of G'' by conjugation. This map is a group cocycle:

$$\alpha\beta\alpha'\beta' = \alpha\alpha'\beta^{\alpha'}\beta'$$

$$\beta^{\alpha'} = (\alpha')^{-1}\beta\alpha$$

$$\tau[\alpha\beta\alpha'\beta'] = \tau[\alpha\beta]^{\alpha'}\tau[\alpha'\beta']$$

(4) Let G, G' and G'' be as in 2. Consider $G' \ltimes G''$ with the rule:

$$(\alpha, \beta)(\alpha', \beta') = (\alpha\alpha', \beta^{\alpha'}\beta').$$

The map $G \to G'' \rtimes G'$ given by

$$\alpha\beta \mapsto (\alpha, \beta)$$

is an isomorphism (the map is injective and surjective and a group homomorphism). Observe that this map is just

$$\psi \mapsto (\alpha, \tau[\psi]).$$

Lemma 6.6. *Suppose $G', G'' \subset G$ and $G'G'' = G$ with $G' \cap G'' = 1$. Write $\psi = \alpha_\psi \beta_\psi$ and consider the cocycle $\tau : G \to G''$ given by $\psi \mapsto \beta_\psi$. Suppose G'' is a normal subgroup.*

(1) *The morphism of S-schemes $\rho_\tau : G'' \times G \to G''$ defined by*

$$\beta \star_\tau \psi = \beta^\psi * \tau[g],$$

is a right action.

(2) *$G' \backslash G \cong (G'', \star_\tau)$ as right G-sets.*

Proof. (1) We have

$$\begin{aligned} a \star (g_1 g_2) &= a^{g_1 g_2} + \tau[g_1 g_2] \\ &= a^{g_1 g_2} + \tau[g_1]^{g_2} + \tau[g_2] \\ &= (a^{g_1} + \tau[g_1])^{g_2} + \tau[g_2] \\ &= (a \star g_1) \star g_2. \end{aligned}$$

(2) The map $\tau : G \to (G'', \star)$ defined by $\psi = \alpha_\psi \beta_\psi \mapsto \beta_\psi$ is a morphism of right G-sets. First we establish a morphism: The map τ factors $\bar{\tau} : G' \backslash G \to (G'', \star)$ since $G' = \ker(\tau)$. The map $\bar{\tau}$ is a morphism of right G-sets. The map $\bar{\tau}$ is a bijection and the inverse map $(G'', \star) \to G' \backslash G$ defined by

$$\beta \mapsto [\beta] \in G' \backslash G$$

defines an inverse which shows the map is an isomorphism.

$$G' \backslash G \ni [\varphi] = [\alpha_\varphi \beta_\varphi] = [\beta_\varphi]$$

$$\begin{aligned} [\varphi]\cdot\psi &= [\beta_\varphi\alpha_\psi\beta_\psi] \\ &= [\beta_\varphi^{\alpha_\psi} * \beta_\psi] \end{aligned}$$

□

Often, there exists an isomorphism $\beta : G'\backslash G \cong (A, \rho_\tau)$ as right G-spaces.

Example 6.7. Let $G = A_2$,$G' = \mathrm{AL}_{1,R_1}$, $G'' = \{T + pc^2T^2\} \cong A = p\mathbf{G}_{a,R_1}$. We have $G = G'G''$ with G'' normal in G.

Fix the following notation:

$$\begin{aligned} (pc)^{\alpha+\beta T+\gamma cT^2} &= pc\beta \\ \tau_2(a+bT+pcT^2) &= p\frac{c}{b} \\ (pc)\star(\alpha+\beta T+p\gamma T^2) &= (pc)^{\alpha+\beta T+p\gamma T^2} + \tau_2[\alpha+\beta T+p\gamma T^2] \\ &= p(c\beta+\frac{\gamma}{\beta}) \end{aligned}$$

These groups satisfy the conditions of Lemma 6.6 and hence we will be able to show that $G'\backslash G \cong (G'', \star)$ as right G-spaces. We perform some of the computations in Lemma 6.6 to provide semantics.

- We first show that $[a+bT+pc^2] = [T+p\frac{c}{b}T^2]$. To see this let $f^{-1}(T) = a+bT$ and observe that

$$\begin{aligned} \psi_0(T) := a+bT+pcT^2 &\sim f(T)\circ(f^{-1}(T)+pcT^2) \\ &= T + \frac{1}{(f^{-1})'(T)}\cdot pcT^2 \\ &= T + p\frac{c}{b}T^2 \\ &= T + p\tau_2[\psi_0]T^2. \end{aligned}$$

  Note that such a representative is necessarily unique since $G'\cap G'' = 1_G$.
- We will show that the action of $\psi = \alpha+\beta T+p\gamma T^2 \in G$ on $[T+pcT^2] \in (G'\backslash G)$ is given by

$$[T+pcT^2]\circ(\alpha+\beta T+p\gamma T^2) = [T+p\left(\beta c+\frac{\gamma}{\beta}\right)T^2].$$

  Proof. The identity:

$$(T+pcT^2)\circ(\alpha+\beta T+p\gamma T^2) = (\alpha+pc\alpha^2)+(\beta+2pc\beta\alpha)T+p(\gamma+c\beta^2)T^2,$$

  plus the previous bullet. □

  Note that $c \mapsto \beta c+\frac{\gamma}{\beta}$ is independent of α and only depends on β modulo p. It is actually the same thing as $c\star\psi$
- The map τ_2 is the same thing as finding a representative for $G'\backslash G$ coming from $\{T+pcT^2\}\subset A_2$.

Definition 6.8. . Fix an F-fiber bundle $\pi : J \to X$ with G-structure Σ. Associate to π a Lax functor

$$\mathcal{M}_X(\Sigma, G') : (\mathsf{Sch}_S)^{op} \to \mathsf{Grpd}$$

defined for each $T \in \mathsf{Sch}_S$ by

$$\mathcal{M}_X(\Sigma, G')(T) = \{\ (\Sigma'_T, \varphi) : \Sigma'_T \in B_{X_T}(G'_T)\ ,\ \varphi_T : G_T \times^{G'_T} \Sigma'_T \to \Sigma_T\ \}. \tag{6.2}$$

The objects of this category of Frame bundles and morphisms are morphisms of G'-torsors (ignoring the reduction map φ).

Observe that $\mathcal{M}_X(\Sigma, G')$ takes values in groupoids. We will show that under our special circumstances our functor is representable.

Theorem 6.9. *Fix an F-fiber bundle $\pi : J \to X$ with G-structure Σ. Let A be an abelian sheaf with a right action of G. Let $\tau : G \to A$ be a cocycle for the right action. Suppose that $(G' \backslash G) \cong (A, \star_\tau)$ as right G-sets.*[10] *Suppose that the actions factor through $\overline{G}$.*

Let $\xi = \mathrm{cl}(\Sigma) \in H^1(X, G)$. Let $\overline{\xi} \in H^1(X, \bar{G})$ be the image of ξ under $G \to \bar{G}$. Let $\mathcal{A}$ be a twisted form of A associated to $\overline{\xi}$.

(1) *Let $Q = G' \backslash \Sigma$. The $(G' \backslash G)$-bundle $q : Q \to X$ has the structure of a torsor under $\mathcal{A}$.*
(2) *The cohomology class associated to the $\mathcal{A}$-torsor structure on $q : Q \to X$ is an obstruction to $\pi : J \to X$ having a reduction to structure group G'.*
(3) *The lax functor $\mathcal{M}_X(\Sigma, G')$ is represented by an algebraic stack over S.*

Proof. (1) The bundle map $q : Q \to X$ naturally has the structure of a $(G' \backslash G)$-fiber bundle with a G-structure on the $(G' \backslash G)$-fibers induced from the right multiplication G-structure $\pi : \Sigma \to X$.

The existence of the isomorphism of G-sets $\bar{\tau} : (G' \backslash G) \to (A, \star_\tau)$ essentially proves the theorem (see Lemma 6.6, part 6.2). We will now fill out some details:

First some setup: let $(U_i \to X)$ be a trivializing cover for $\pi : P \to X$. Let $\psi_i : \rho^{-1}(U_i) \to U_i \times (G' \backslash G)$ define a G-compatible $(G' \backslash G)$-atlas (where the G-action of the transitions is induced from the G-torsor structure on $\Sigma \to X$). To get A-local trivializations define $\overline{\psi}_i : \rho^{-1}(U_i) \to U_i \times A$ by

$$\overline{\psi}_i = \bar{\tau} \circ \psi_i.$$

The transition maps for the A-structure are given by $\overline{\psi}_{ij} = (* \mapsto * \star_\tau g_{ji}) = (* \mapsto * \star_0 (\overline{g}_{ji}, \tau(g_{ji})))$ where we used $\star_0 : A \times (\overline{G} \ltimes A) \to A$ to denote the action $x \star_0 (\bar{g}, \alpha) = x^{\bar{g}} + \alpha$. [11] This shows how the trivializations $\overline{\psi}_i$ induce a $(\overline{G} \ltimes A)$-structure.

The existence of the torsor structures on bundles with semi-direct product transition maps follows from general principals. Since it doesn't hurt to repeat explanations we give it again here: Let $\mathcal{A} \to X$ be a twisted form of A with trivializations $\varphi_i : \mathcal{A}_{U_i} \to A_{U_i}$ such that $\varphi_{ij} = R_{\overline{g}_{ji}}$ where $R : A \times \overline{G} \to A$ is the prescribed right action of $\overline{G}$ on A in the statement of the theorem. [12] As the transition maps respect the group structure on A, the twisted form $\mathcal{A}$ has the structure of an abelian group scheme. It is the twisted form of $\mathcal{A}$ classified by $[R_{\overline{g}_{ji}}] \in H^1(X, \mathrm{Aut}(A))$.

[10] c.f. Lemma 6.6 for conditions

[11] Observe the factorization $x \star_\tau g = x \star_0 (\bar{g}, \tau[g])$.

[12] Observe that $g \mapsto R_{g^{-1}}$ defines group homomorphism: $G \to \underline{\mathrm{Aut}}(A)$

We show now that Q is a torsor under $\mathcal{A}$. We define the torsor structure by a division map: for each open set U with trivialization $\psi : \rho^{-1}(U) \to U \times A$ define $d : Q \times Q \to \mathcal{A}$ by

$$d(s_1, s_2) := \psi^{-1}(\psi(s_1) - \psi(s_2)),$$

for $s_1, s_2 \in \Gamma(U, Q)$. Here, the addition rule of A is used on the right hand side and, because the transition maps are affine linear, $d(s_1, s_2)$ gives a well-defined section of $\mathcal{A}$. Furthermore, because of the sheaf property, the map d is well-defined for all open subsets.

(2) Let $\mathrm{cl}(\mathcal{Q}) = \xi \in H^1(X, \mathcal{A})$ be the class associated to the $\mathcal{A}$-torsor structure on Q. Lemma 5.8 part (4) says that reductions are equivalent to global sections of Q modulo equivalence. We know that $\xi = 0$ if and only if $\Gamma(X, Q)$ is not empty if and only if $Q \cong \mathcal{A}$ as left $\mathcal{A}$-torsors. Hence $\Gamma(X, Q)$ is naturally a torsor under $\mathcal{A}(X)$.

(3) If we suppose that $\Gamma(X, Q)$ is nonempty. The section s gives an isomorphism $\Gamma(X, Q) \to \mathcal{A}(X)$ of left $\mathcal{A}(X)$ sets given by $s' \mapsto s' - s$. By Lemma 5.8 part (4) we have a bijection

$$\mathrm{Aut}(P)\backslash\mathcal{A}(X) \to \mathcal{M}_X(\Sigma, G')(X)/\sim$$
$$[s] \mapsto [s^*\Sigma_Q]$$

Globalizing this construction gives $\mathcal{M} \cong \underline{\mathrm{Aut}}(P)\backslash\mathcal{A}$ as sheaves on X. Since $\underline{\mathrm{Aut}}(P)$ is represented by sections of the adjoint bundle, the quotient $\underline{\mathrm{Aut}}(P)\backslash\mathcal{A}$ is a group scheme quotient and hence exists as an algebraic stack.

□

Remark 6.10. This remark is documenting a failed method for constructing $\mathcal{M}_X(\Sigma, G')$. The author attempted the following to show the space of reductions was represented by an algebraic stack; we list the procedure in steps and explain its failure following the initial listing of steps:

(1) (take a quotient) Show that the quotient $Q := G'\backslash P$ is a represented by a an algebraic space over X.
(2) (construct a Hom-stack) Show that The hom-stack $H := \underline{\mathrm{Hom}}_X(X, Q)$ is represented by a Deligne-Mumford stack.
(3) (construct a group scheme of automorphisms) and show there exists a natural group scheme Γ associated to gauge group $\mathrm{Aut}(P)$ and a left action $\Gamma \times H \to H$.
(4) (take a quotient of a stack) Show that the quotient $\Gamma\backslash S$ exists as an algebraic stack and take it as our definition of $\mathcal{M}_X(\Sigma, G')$.

If these steps were all true then this would give a presentation of $\mathcal{M}$.

(1) (Quotienting by a group scheme is ok)
(2) (Constructing a Hom-stack is *NOT OK*) To apply [Nit05, pg 31 or Thm 6.6] or [Ols06, Theorem 1.1] for representability of $\underline{\mathrm{Hom}}_X(X, Q)$ one needs $Q \to X$ to be proper. In one of our application $S = X$ and $Q = A_2\backslash\Sigma_1$ and the morphism $Q \to X$ is often affine and not proper.
(3) (Converting to group scheme action is ok)
(4) (Quotienting an algebraic stack is ok) For the definition of a group action on groupoids see [Rom05, Definition 1.3]. By [Rom05, Theorem 4.1] If M is an algebraic stack which is finitely presented, G a flat group scheme which

is separated and finitely presented then M/G is an algebraic stack and $q : M \to M/G$ is a G-torsor (this implies q is representable, q is separated and q is finitely presented)

6.3. **The moduli of torsor structures of lifts of the Frobenius modulo p^3.** In this example we work out Theorem 6.9 for the principal bundle of the first p-jet space of a curve modulo p^2.

Theorem 6.11. *Let X/R be a smooth projective curve of genus g and let $p > 3g-3$. Let Σ_1 be the canonical A_2-structure on $J^1_p(X)_1$. The set of reductions to an AL_{1,R_1}-structure is in bijections with a quotient of a $(2p-1)(g-1)$ dimensional vector space.*

Remark 6.12. We were hoping that the above result would allow us to compute the dimension of $\mathcal{M}_{X_1}(\Sigma_1, \mathrm{AL}_{1,R_1})$ but this is not how stacky dimensions work.

The dimensions of local cohomology groups in the moduli problem have nothing to do with stack dimensions. This can be seen for example in the difference between the dimension of the Picard stack $[C/\mathbf{G}_m]$ (which is zero dimensional) and the Picard scheme which is g dimension if C is a curve of genus g.

We thank David Zureick-Brown for pointing this out to us.

Proof. We first fix some notation. Let $G = A_2$, $G' = \mathrm{AL}_{1,R_1}$ and $G'' = \{T + pcT^2\} \subset A_2$. Observe that $G'' \cong A := p\mathbf{G}_{a,R_1}$. Let $Q = (G'\backslash\Sigma_1)$. Let ρ be defined by the diagram:

$$\begin{tikzcd}
\Sigma_1 \arrow[dr, "q"] \arrow[dd, "\pi"] & \\
& (G'\backslash\Sigma_1) = Q \arrow[dl, "\rho"] \\
X &
\end{tikzcd}$$

The assertions beyond $\mathcal{A} = \Omega_{X_0}^{\otimes p}$ follow from elementary Riemann-Roch together with Lemma 5.8 part 4. We work on showing the torsor structure explicitly. The obstruction to being the trivial torsor vanishes and hence $\Gamma(X, Q)$ is parametrized by $\mathcal{A}(X)$. We also have $\dim_{R_0} \Gamma(X, Q) = \dim_{R_0} \mathcal{A}(X) = (2p-1)(g-1)$.

We will first show that $\rho : Q \to X$ has the structure of a torsor under a line bundle. We will then identify what the line bundle is.

Let $(U_i \to X_1)_{i\in I}$ be a trivializing atlas for the A_2-bundle of frames Σ_1 with trivializations $\xi_i : \Sigma_{U_i} \to (A_2)_{U_i}$. From the definition of the frame bundle we know that

$$\xi_i(\psi) := \psi \circ \psi_i^{-1}$$

where $\psi_i \in \Sigma_1(U_i)$ are trivializations of $J^1_p(X)_1$ with its given A_2-structure. Using the formula for ξ_i we may compute the transition maps: For $\varphi \in A_2(U_{ij})$ we have

$$\xi_{ij}(\varphi) = \xi_i \circ \xi_j^{-1}(\varphi) = \xi_i(\varphi \circ \psi_j) = \varphi \circ \psi_j \circ \psi_i^{-1} = R_{\psi_{ji}}(\varphi).$$

Here, R denotes the action of right multiplication. After quotienting by $G' = \mathrm{AL}_{1,R_1}$ we obtain the factorization

$$\begin{tikzcd}
\Sigma_1 \arrow[dr, "q"] \arrow[dd, "\pi"'] & . \\
& G'\backslash\Sigma_1 = Q \arrow[dl, "\rho"] \\
X &
\end{tikzcd}$$

The trivializations (ξ_i) of the left A_2-torsor Σ_1 induce A_2-compatible trivializations of the $(\mathrm{AL}_{1,R_1}\backslash A_2)$-fiber bundle (and hence an A_2-structure) since the quotient is a universal categorical quotient. Let us denote the induced trivializations by $\overline{\xi}_i$. The transition maps $\overline{\xi}_{ij}$ are also given by right multiplication by ψ_{ji}:

$$\overline{\xi}'_{ij} = R_{\psi_{ji}} : (\mathrm{AL}_{1,R_1}\backslash A_2)_{U_{ij}} \to (\mathrm{AL}_{1,R_1}\backslash A_2)_{U_{ij}}.$$

We now come to the torsor structure. Let $\tau : A_2 \to p\mathbf{G}_{a,R_1}$ be the right group cocycle defined by

$$\tau([a + bT + pcT^2]) \mapsto p\frac{c}{b}.$$

By Lemma 6.6 (2) $\tau : A_2 \to p\mathbf{G}_{a,R_1}$ induces an isomorphism right A_2-spaces $\bar{\tau} : (\mathrm{AL}_{1,R_1}\backslash A_2) \to (p\mathbf{G}_{a,R_1}, \star_\tau)$. The isomorphism of right A_2-spaces induces an isomorphism of schemes

$$Q \cong (\mathrm{AL}_{1,R_1}\backslash A_2) \times^{A_2} \Sigma_1 \xrightarrow{\bar{\tau}\times^{A_2}\Sigma_1} (p\mathbf{G}_{a,R_1}, \star_\tau) \times^{A_2} \Sigma_1 \ .$$

The isomorphism $\bar{\tau} \times^{A_2} \Sigma_1$ gives Q the structure of a $p\mathbf{G}_{a,R_1}$-bundle with an A_2-structure.

The $p\mathbf{G}_{a,R_1}$-atlas on Q is given by $\bar{\xi}'_i := \bar{\tau} \circ \bar{\xi}_i$. The transition maps $\bar{\xi}'_{ij} : U_{ij} \times p\mathbf{G}_{a,R_1} \to U_{ij} \times p\mathbf{G}_{a,R_1}$ are given by a right action: for $x \in p\mathbf{G}_{a,R_1}(U_{ij})$ we have

$$\bar{\xi}'_{ij}(x) = x \star \psi_{ji} = x^{\psi_{ji}} + \tau[\psi_{ji}].$$

Since $\bar{\xi}'_{ij}$ is a cocycle, and $\star$ is an AL_1-action we know that Q is a torsor.

It remains to identify $\mathcal{A}$. Let $\psi_{ij}(T) = a_{ij} + b_{ij}T + pc_{ij}T^2$. Recall that $[\bar{b}_{ij}] = \mathrm{cl}(F^*T_{X_0}) \in H^1(X_0, \mathcal{O}_{X_0})$ The formula

$$\bar{\xi}'_{ij}(x) = x^{\psi_{ji}} + \tau_2[\psi_{ji}] = xb_{ji} + \frac{c_{ji}}{b_{ji}}$$

implies that $\mathcal{A} \cong (F^*T_{X_0})^\vee$. Since the global sections are parametrized by $H^0(\mathcal{A})$ and the set of reductions is a quotient of $\mathcal{A}$ we the dimension of the set of reductions is bounded by the dimension of $H^0(\mathcal{A})$. □

References

[Bal09] V Balaji. Lectures on principal bundles. *Moduli Spaces and Vector Bundles*, 359:1, 2009.

[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.

[Bre10] Lawrence Breen. Notes on 1-and 2-gerbes. In *Towards higher categories*, pages 193–235. Springer, 2010.

[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. American Mathematical Society, 2005.

[DI87] P. Deligne and L. Illusie. Relèvements modulo p^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.

[Hir78] F. Hirzebruch. *Topological Methods in Algebraic Geometry*. Springer Science & Business Media, 1978.

[Joy85] A. Joyal. δ-anneaux et vecteurs de Witt. *Comptes rendus mathématiques de l'académie des sciences*, 7(3):177–182, 1985.

[Kat89] K. 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] F. Loeser and J. Sebag. Motivic integration on smooth rigid varieties and invariants of degenerations. *Duke Mathematical Journal*, 119(2):315–344, 2003.

[Mil80] James S Milne. *Etale Cohomology (PMS-33)*. Number 33. Princeton University Press, 1980.

[Mit01] S. A. Mitchell. Notes on principal bundles and classifying spaces. *Lecture Notes. University of Washington*, 2001.

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

[Neu09] F. Neumann. *Algebraic stacks and moduli of vector bundles*. IMPA, 2009.

[Nit05] N.A Nitsure. Construction of Hilbert and quot schemes. arXiv preprint math/0504590, 2005.

[Ols06] M. Olsson. Hom-stacks and restriction of scalars. *Duke Mathematical Journal*, pages 139–164, 2006.

[Ols07] M. Olsson. Tangent spaces and obstruction theories. In *Deformation theory and moduli in algebraic geometry (MSRI Notes)*. Citeseer, 2007.

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

[PL09] J.L. Peña and O. Lorscheid. Mapping F1-land: An overview of geometries over the field with one element. *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.

[Rom05] M. Romagny. Group actions on stacks and applications. pages 209–235, 2005.

[Sko01] A. Skorobogatov. *Torsors and rational points*. Number 144. Cambridge University Press, 2001.

[Sor00] C. Sorger. Lectures on moduli of principal G-bundles over algebraic curves. *ICTP Lecture Notes*, page 3, 2000.

[Sta14] The Stacks Project Authors. Stacks project. http://stacks.math.columbia.edu, 2014.

[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.

[vdGM07] G. van der Geer and B. Moonen. Abelian varieties. *Book in preparation*, page 71, 2007.

E-mail address: dupuy@math.huji.ac.il