JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Jinbi JIN

Computation of étale cohomology on curves in single exponential time

Tome 32, n° 2 (2020), p. 311-354.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2020__32_2_311_0>

Journal de Théorie des Nombres
de Bordeaux **32** (2020), 311–354

Computation of étale cohomology on curves in single exponential time

par Jinbi JIN

Résumé. Dans ce texte, on décrit un algorithme calculant, pour une courbe lisse et connexe X sur un corps k et un faisceau localement constant de groupes abéliens de torsion inversible dans k, le premièr groupe de cohomologie étale $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$ et le premièr groupe de cohomologie étale à support propre $\mathrm{H}^1_c(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$ comme ensembles de torseurs.

La complexité arithmétique de cet algorithme est exponentielle en $n^{\log n}$, $p_a(X)$, et $p_a(\mathcal{A})$, où $p_a(X)$ est le genre arithmétique de la complétion normale de X sur k, $p_a(\mathcal{A})$ est le genre arithmétique de la complétion normale de la courbe Y répresentant le faisceau $\mathcal{A}$, et n est le degré de Y sur X.

L'algorithme passe par le calcul d'un schéma en groupoïdes classifiant les $\mathcal{A}$-torseurs étales avec quelques structures additionnelles rigidifiantes.

Abstract. In this paper, we describe an algorithm that, for a smooth connected curve X over a field k, a finite locally constant sheaf $\mathcal{A}$ on $X_{\text{ét}}$ of abelian groups of torsion invertible in k, computes the first étale cohomology $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$ and the first étale cohomology with proper support $\mathrm{H}^1_c(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$ as sets of torsors.

The complexity of this algorithm is exponential in $n^{\log n}$, $p_a(X)$, and $p_a(\mathcal{A})$, where $p_a(X)$ is the arithmetic genus of the normal completion of X, $p_a(\mathcal{A})$ is the arithmetic genus of the normal completion Y of the smooth curve representing $\mathcal{A}$, and n is the degree of Y over X.

The computation in this algorithm is done via the computation of a groupoid scheme classifying the $\mathcal{A}$-torsors with some extra rigidifying data.

1. Introduction

The motivating question for this paper is the following; this question is posed e.g. by Poonen, Testa, and van Luijk in [22].

Question 1.1. *Is there an algorithm that takes an algebraic variety X over a field k, and a positive integer n invertible in k, and computes* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-modules isomorphic to the étale cohomology groups* $\mathrm{H}^q(X_{k^{\mathrm{sep}},\text{ét}}, \mathbb{Z}/n\mathbb{Z})$ *for* $q = 0, 1, \ldots, 2\dim X$*?*

Manuscrit reçu le 20 novembre 2017, révisé le 2 septembre 2019, accepté le 3 juin 2020.
2020 *Mathematics Subject Classification.* 14F20, 14Q05, 14Q20.
Mots-clefs. Algebraic geometry, Algorithm, Curves, Étale cohomology.

We assume affine schemes of finite presentation over some base ring R to be given by generators and relations over R, and we assume X to be given by a gluing datum of affine varieties over k. The output will be given as a pair (l, X) of a Galois extension l/k and a finite $\mathrm{Gal}(l/k)$-set X. [5, Thm. finitude] guarantees that in the situation of this question, the groups $\mathrm{H}^q(X_{k^{\mathrm{sep}}, \text{ét}}, \mathbb{Z}/n\mathbb{Z})$ are indeed finite.

The existence of an algorithm as in the question computing the étale cohomology groups in time polynomial in n for a fixed variety over $\mathbb{Q}$ implies, via the Lefschetz trace formula [5, Rapport] and by the argument of [3, Thm. 15.1.1], the computation of the number of $\mathbb{F}_q$-points of some fixed finite type scheme X (over $\mathbb{Z}$) in time polynomial in $\log q$. Here, we note that the problem of computing $\#X(\mathbb{F}_q)$ has many efficient solutions in practice, see e.g. [14, 17, 19]; however, none of them run in time polynomial in the characteristic of the finite field. One other application of a positive answer to the question above is the computation of Néron–Severi groups by Poonen, Testa, and van Luijk in [22] using the computation of the étale cohomology groups.

Question 1.1 is already known to have a positive answer. In 2015, Poonen, Testa, and van Luijk, in the aforementioned article [22], showed that the étale cohomology groups are computable if X is a smooth, projective, geometrically irreducible variety over a field of characteristic 0. Later that year, Madore and Orgogozo [21] showed that they are computable for any variety over any field, and, assuming computations with constructible sheaves can be performed, with coefficient sheaf any constructible sheaf of abelian groups (of torsion invertible in the base field). However, both of these results are fundamentally merely computability results, without any bounds on the complexity, even for a fixed instance.

So a natural extension of Question 1.1 is (in addition to allowing more general coefficients) to also ask for explicit upper bounds for the complexity; beyond the classical case of smooth curves with constant coefficients, the author doesn't know of any such result. In this paper, we will describe an algorithm computing, for smooth connected curves, the first étale cohomology group (proper support or not) with coefficients in a finite locally constant sheaf of abelian groups (of torsion invertible in k), together with theoretical upper bounds for the complexity.

We will assume the field k is given together with black box field operations (see Section 3 for more details) and we measure the complexity only in the number of field operations performed. While this is a good approximation for the time complexity in case k is finite, for infinite k this is usually not the case because of coefficient size growth. Algorithms will be deterministic (except for the use of the black boxes); for an actual implementation of the algorithm to be presented, it may be more efficient in practice to use

randomised algorithms. Moreover, the choice of algorithms is motivated by their theoretical worst-case complexities; for an actual implementation, it may be significantly more efficient in practice to use different algorithms than the ones used in this paper.

With this in mind, let us state this paper's main theorem, deferring the description of the in- and output mainly to Section 4 and Section 9.

Theorem 1.2. *There exist an algorithm that takes as input a smooth connected curve X over k, and a (curve representing a) finite locally constant sheaf $\mathcal{A}$ of abelian groups of degree n over X with n invertible in k, and return as output $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, \mathcal{A}|_{X_{k^{\mathrm{sep}}}})$ (resp. $\mathrm{H}^1_c(X_{k^{\mathrm{sep}}}, \mathcal{A}|_{X_{k^{\mathrm{sep}}}})$) as $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-modules in a number of field operations exponential in $n^{\log n}$, $p_a(X)$, and $p_a(\mathcal{A})$, where p_a denotes the arithmetic genus of the normal completion.*

More precise (and slightly more general) versions of this theorem will be given in Section 6 and Section 9.

Acknowledgments. This paper is in part based on Chapter 3 of the author's dissertation, which was funded by the Netherlands Organisation for Scientific Research (project no. 613.001.110), and the author thanks his supervisors Bas Edixhoven and Lenny Taelman for their guidance during the author's PhD candidacy. The author also thanks the Max-Planck-Institut für Mathematik in Bonn for their support during the production of this paper, and the anonymous referee for providing many useful comments on this paper.

2. The idea and structure of the algorithm

Let X be a smooth connected curve over a field k, and let $\mathcal{G}$ be a finite locally constant sheaf of groups on X. Then the set $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, \mathcal{G}|_{X_{k^{\mathrm{sep}}}})$, resp. $\mathrm{H}^1_c(X_{k^{\mathrm{sep}}}, \mathcal{G}|_{X_{k^{\mathrm{sep}}}})$, is the set of isomorphism classes of $\mathcal{G}|_{X_{k^{\mathrm{sep}}}}$-torsors on $X_{k^{\mathrm{sep}}}$, resp. the set of isomorphism classes of $j_!\mathcal{G}|_{X_{k^{\mathrm{sep}}}}$-torsors on $\overline{X}_{k^{\mathrm{sep}}}$. Here, $j\colon X \to \overline{X}$ is the open immersion of X into its normal completion $\overline{X}$.

Remark 2.1. If $\mathcal{G}$ is a sheaf of abelian groups, a priori we have two possible definitions of $j_!\mathcal{G}$; one arising from viewing $j_!$ as the left adjoint of j^{-1} on the category of sheaves of groups, and one arising from viewing $j_!$ as the left adjoint of j^{-1} on the category of sheaves of abelian groups. Let us call these $j_!^G\mathcal{G}$ and $j_!^A\mathcal{G}$ for now. There is a natural map $j_!^G\mathcal{G} \to j_!^A\mathcal{G}$, which induces an isomorphism on stalks since j is an open immersion (and direct sums of zero, resp. one object in the category of groups and that of abelian groups have the same underlying sets). Hence $j_!^G\mathcal{G} = j_!^A\mathcal{G}$, so there is no confusion possible if we just write $j_!\mathcal{G}$ in this case, like we did above.

The global idea behind the algorithm of Theorem 1.2 is to give a description of our target objects, being the (isomorphism classes of) $\mathcal{G}|_{X_{k^{\mathrm{sep}}}}$-

(resp. $j_!\mathcal{G}|_{X_{k^{\mathrm{sep}}}}$-)torsors on $X_{k^{\mathrm{sep}}}$, that is susceptible to a parametrisation, and to compute and use this parametrisation to compute the first cohomology.

In this paper, we choose to describe all occurring curves over $X_{k^{\mathrm{sep}}}$ (which includes the torsors of which we wish to compute the set of isomorphism classes) in terms of vector bundles on $\mathbb{P}^1_{k^{\mathrm{sep}}}$; all vector bundles over $\mathbb{P}^1_{k^{\mathrm{sep}}}$ are isomorphic to finite direct sums of Serre twists, and we have a simple parametrisation of every Hom-set between two such vector bundles. We recall this in more detail in Section 4. To this end, we want to view the curve X as an open subscheme of a smooth proper curve $\overline{X}$, together with a finite, generically étale morphism $\overline{X} \to \mathbb{P}^1_k$ such that the complement of X in $\overline{X}$ is either empty or the pre-image of a single rational point on $\mathbb{P}^1_k$.

If k were perfect, then the construction of such a finite cover is classical, using the explicit computation of Riemann–Roch spaces, e.g. as in [15]. However, since we don't require the field k to be perfect, there are some technicalities that come up. Namely, the normal completion of X may not be smooth, and it may not admit a finite, generically étale morphism to P^1_k. We evade this problem by passing to a finite purely inseparable base change l of k; by the topological invariance of the small étale site there is a bijection between $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, \mathcal{G}|_{X_{k^{\mathrm{sep}}}})$ and $\mathrm{H}^1(X_{l^{\mathrm{sep}}}, \mathcal{G}|_{X_{l^{\mathrm{sep}}}})$ (and also a bijection between their proper support counterparts), and we use (and make explicit) this bijection in order to be in the desired situation.

Problem 2.2. *Given a field k, a smooth curve X over it, a finite, generically étale morphism from the smooth normal completion $\overline{X}$ to $\mathbb{P}^1_k$ such that $\overline{X} - X$ is either empty or the pre-image of a single rational point of $\mathbb{P}^1_k$, and a finite locally constant sheaf $\mathcal{G}$ of groups on X, compute $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, \mathcal{G}|_{X_{k^{\mathrm{sep}}}})$, resp. $\mathrm{H}^1_c(X_{k^{\mathrm{sep}}}, \mathcal{G}|_{X_{k^{\mathrm{sep}}}})$.*

For a more uniform treatment, we will actually consider the following, slightly more general problem.

Problem 2.3. *Suppose given a field k, a smooth proper curve $\overline{X}$ over it, and a finite, generically étale morphism $f\colon \overline{X} \to \mathbb{P}^1_k$. For $p = 0, \infty \in \mathbb{P}^1(k)$, suppose given a subset S_p of $\{p\}$. Let $X = \overline{X} - f^{-1}(S_\infty)$ and $U = X - f^{-1}(S_0)$, and let $j\colon U \to X$ be the inclusion. Then, given a finite locally constant sheaf $\mathcal{G}$ of groups on U, compute $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$.*

The two chosen rational points 0 and ∞ of $\mathbb{P}^1_k$ serve two distinct roles; we will use additional data above ∞ to encode smoothness of curves finite over $\overline{X}$ (that are étale over X), and we will use additional data above 0 to encode elements of $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$.

Note that taking $S_0 = \emptyset$ and $S_\infty = \{\infty\}$ in Problem 2.3 gives us the computation of the first étale cohomology in Problem 2.2 with the rational point ∞, and that taking $S_0 = \{0\}$ and $S_\infty = \emptyset$ in Problem 2.3 gives

us the computation of the first étale cohomology with proper support in Problem 2.2 with the rational point 0.

Finally, we reduce to the case in which $\mathcal{G}$ is constant by computing a finite Galois cover $g\colon Y \to X$ for which $g^{-1}\mathcal{G}$ is constant. The description of $\mathcal{G}$-torsors in terms of the constant sheaf $g^{-1}\mathcal{G}$ is given in Section 5. Therefore, after another base change along a finite purely inseparable field extension if necessary, we have reduced Problem 2.3 to the following.

Situation 2.4. We are given a field k, a finite group Γ, for $p = 0, \infty \in \mathbb{P}^1(k)$, a subset S_p of $\{p\}$, and a diagram

$$\begin{array}{ccccc}
V & \longrightarrow & Y & \longrightarrow & \overline{Y} \\
{\scriptstyle g}\downarrow & & \downarrow & & \downarrow \\
U & \xrightarrow{\;j\;} & X & \longrightarrow & \overline{X} \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{P}^1_k - S_0 - S_\infty & \longrightarrow & \mathbb{P}^1_k - S_\infty & \longrightarrow & \mathbb{P}^1_k
\end{array}$$

in which:

- all squares are cartesian;
- $\overline{X}$ and $\overline{Y}$ are smooth, proper, and finite and generically étale over $\mathbb{P}^1_k$;
- $g\colon V \to U$ is Galois with group Γ.

Moreover, we are given a finite locally constant sheaf $\mathcal{G}$ of groups on U such that $g^{-1}\mathcal{G}$ is constant, and denote by G its group of connected components; the Galois action of Γ on V induces an action of Γ on G by automorphisms.

Problem 2.5. *In Situation 2.4, compute* $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$.

The computational details of this reduction step to Situation 2.4 is described in Section 9.

The algorithm solving Problem 2.5 consists of two steps. The core step involves translating the definition of a $j_!\mathcal{G}$-torsor to a description purely in terms of morphisms of vector bundles on $\mathbb{P}^1_k$ and commutativity relations between them. The parametrisation described in Section 4 then allows us to readily translate that into an explicit description of a groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$, of which the most important property is that the $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set of geometric connected components of $\mathcal{U}$ is isomorphic to $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$ in a natural way. This is detailed in Section 6, and the correctness of this part of the algorithm is proved in Section 7; these two sections form the core of this paper.

After this, we finish by using effective Noether normalisation as in e.g. [7, §1] to compute the set of isomorphism classes of $j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}}$-torsors by computing representatives for each of the isomorphism classes. Details of this step are found in Section 8.

3. Preliminaries

In this paper we will mainly consider *generic field algorithms*; i.e. algorithms that take a finite number of bits and a finite number of a field k, which are only allowed to operate on the field elements through a number of black box operations, and, aside from the black box operations, are deterministic. The assumptions that follow here are essentially the assumptions as mentioned in [2, p. 1843, 1846].

First, we assume the constants 0 and 1 (in k) and the characteristic exponent p (in $\mathbb{Z}$) are given. Moreover, we assume the imperfectness degree p^e of k to be finite, and that $k^{1/p}/k$ is given explicitly as a finite k-algebra (i.e. as a k-vector space with given unit and multiplication table).

In this paper these black box operations are:

- $=$, which takes $x, y \in k$, and returns 1 if $x = y$, and 0 if $x \neq y$;
- $-$, which takes $x \in k$, and returns $-x$;
- $\cdot^{-1}$, which takes $x \in k$, and returns nothing if $x = 0$, and x^{-1} if $x \neq 0$;
- $+$, which takes $x, y \in k$, and returns $x + y$;
- $\times$, which takes $x, y \in k$, and returns xy;
- $\cdot^{1/p}$, which takes $x \in k$, and returns $x^{1/p} \in k^{1/p}$;
- F, which takes a polynomial $f \in k[x]$, and returns its factorisation into irreducibles in $k[x]$.

Remark 3.1. For any field finitely generated over a finite field or $\mathbb{Q}$, there are algorithms for each of the above black box operations, however, the most efficient implementations of the factorisation algorithm for finite fields are randomised.

To such a generic field algorithm we attach a number of functions (from the set of inputs to $\mathbb{N}$).

- The *bit-complexity* N_{bit}; for an input I, the number $N_{\mathrm{bit}}(I)$ is the number of bit-operations the algorithm performs when given I.
- The *arithmetic complexity* N_{ar}; for an input I, the number $N_{\mathrm{ar}}(I)$ is the number of black box operations the algorithm performs when given I.

We will usually not mention the bit-complexity of the algorithms in this paper; in all cases, the bit-complexity will be small compared to the arithmetic complexity. As is customary, as a measure of size for inputs, we take the pair (b, f), where b is the number of bits in the input, and f is the

number of field elements in the input; so for Φ a function from the set of inputs to $\mathbb{N}$, we will denote by $\Phi(b, f)$ the maximum of the $\Phi(I)$ with I ranging over all the inputs with at most b bits and f field elements.

We note that a lot of linear algebraic operations, like matrix addition, matrix multiplication, computation of characteristic polynomial, and by extension, reduced row echelon form, rank, kernels, images, quotients, etc. can all be performed in arithmetic complexity polynomial in the size of the input.

By [18, §7], the primary decomposition of a finite k-algebra A can also be computed in arithmetic complexity polynomial in $[A : k]$, and if k is perfect, the same holds for the computation of nilradicals. In fact, in our case [18, §7] computes an l-basis (and therefore a k-basis) for the nilradical of $A \otimes_k l$ (where $l = k^{1/p^{\lfloor \log_p [A:k] \rfloor}}$), and therefore also a k-basis for the nilradical of A, in arithmetic complexity polynomial in $[A : k]^{e+1}$.

Moreover, using the criteria that a reduced finite k-algebra A is separable if $[A : k] < p$, and if and only if A is spanned over k by t_i^p for t_i any k-basis for A, one can compute separable closures of k in finite field extensions l in arithmetic complexity polynomial in $[l : k]$, using the obvious recursive algorithm.

By [2, §1.1] we have algorithms which compute for a finite field extension l/k the extension $l^{1/p}/l$ and the operations listed above; aside from the computation of $l^{1/p}/l$, that of characteristic roots, which have arithmetic complexity polynomial in $[l : k]^{e+1}$, and that of factorisation, which has arithmetic complexity polynomial in $[l : k]^{e+1}$ and the degree of the polynomial to be factored, every operation has arithmetic complexity polynomial in $[l : k]$. Moreover, l has the same characteristic exponent and imperfectness degree as k.

Now consider the purely transcendental extension $k(x)/k$. We present its elements by pairs of polynomials; for $f, g \in k[x]$ we set the *height* of $\frac{f}{g}$ to be $h(\frac{f}{g}) = \max(\deg f, \deg g)$. Then note that for $k(x)/k$, we have $k(x)^{1/p} = k^{1/p}(x^{1/p})$ and therefore an obvious $k(x)$-basis for $k(x)^{1/p}$, and we can compute the listed operations for elements of $k(x)$ of height at most h in arithmetic complexity polynomial in $h(x)$. (Again, with the exceptions of characteristic roots, which has arithmetic complexity polynomial in $h(x)^{e+2}$ and polynomial factorisation, which has arithmetic complexity polynomial in $h(x)^{e+2}$ and the degree of the polynomial to be factored, see e.g. [16].)

As is customary, we will use the standard big-oh notation when bounding complexities; moreover, we will use $O(x, y)$ as a shorthand for $O\big(\max(x, y)\big)$.

4. Parametrising morphisms of modules

We first give a parametrisation of the set of morphisms between two vector bundles on $\mathbb{P}^1_k$ with k a field. To this end, we will use the following characterisation of isomorphism classes of vector bundles over $\mathbb{P}^1_k$.

Proposition 4.1 ([4]). *Let k be a field, and let $\mathcal{E}$ be a vector bundle on $\mathbb{P}^1_k$. Then there exists an up to permutation unique finite sequence $(a_i)_{i=1}^s$ of integers such that*

$$\mathcal{E} \cong \bigoplus_{i=1}^{s} \mathcal{O}_{\mathbb{P}^1_k}(a_i).$$

This motivates the following definition.

Definition 4.2. Let S be a scheme, and let a be a finite sequence of integers of length s. The *standard module of type a* on S is the $\mathcal{O}_{\mathbb{P}^1_S}$-module

$$\mathcal{O}_{\mathbb{P}^1_S}(a) = \bigoplus_{i=1}^{s} \mathcal{O}_{\mathbb{P}^1_S}(a_i).$$

So every vector bundle $\mathcal{E}$ over $\mathbb{P}^1_k$ is isomorphic to a standard module over k, say of type a; in this case, we simply say that $\mathcal{E}$ *has type a*.

Let, for finite sequences a, b of integers, of lengths s, t, respectively, $H_{a,b}$ define the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Set}$ sending S to $\mathrm{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\big(\mathcal{O}_{\mathbb{P}^1_S}(b), \mathcal{O}_{\mathbb{P}^1_S}(a)\big)$. Moreover, let $N(a,b) = \sum_{i=1,j=1}^{s,t} \max(a_i - b_j + 1, 0)$.

Then the functor $H_{a,b}$ is representable by $\mathbb{A}^{N(a,b)}$: in fact, as

$$\mathrm{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\big(\mathcal{O}_{\mathbb{P}^1_S}(b_j), \mathcal{O}_{\mathbb{P}^1_S}(a_i)\big) = \mathcal{O}(S)[x,y]_{a_i - b_j}$$

functorial in S, we get an identification

$$\begin{aligned}\mathrm{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}&\big(\mathcal{O}_{\mathbb{P}^1_S}(b), \mathcal{O}_{\mathbb{P}^1_S}(a)\big) \\ &= \big\{M \in \mathrm{Mat}_{s\times t}(\mathcal{O}(S)[x,y]) : M_{ij} \in \mathcal{O}(S)[x,y]_{a_i - b_j}\big\},\end{aligned}$$

and under this identification, all the relevant operations on morphisms of standard modules (i.e. identity map, composition, direct sum, tensor product, dual, exterior powers) correspond to their usual counterparts on matrices. In particular, if these operations are viewed as operations on the representing scheme $\mathbb{A}^{N(a,b)}$, then the degrees of the polynomials defining them are as expected.

To an element of $H_{a,b}(S)$, one way to give its fibre at $0 \in \mathbb{P}^1_S$ is by substituting $(0,1)$ for (x,y), and one way to give its fibre at $\infty \in \mathbb{P}^1_S$ is by substituting $(1,0)$ for (x,y). Moreover, a way to give the first infinitesimal neighbourhood at $\infty \in \mathbb{P}^1_S$ is by substituting $x = 1$ and setting $y^2 = 0$.

5. Torsors

A *curve* over a field k in this paper is a separated k-scheme of finite type, of pure dimension 1 over k.

Let $f\colon X \to \operatorname{Spec} k$ be a smooth connected curve over a field k, and let $\mathcal{G}$ be a finite locally constant étale sheaf of groups on an open subscheme U of X. In this section, we give, in abstract terms, a description of the category of $j_!\mathcal{G}$-torsors on X in terms of a finite étale Galois cover V of U trivisalising $\mathcal{G}$ (compare with Situation 2.4).

5.1. $j_!\mathcal{G}$-torsors and recollement. The main tool we will use in the description mentioned directly above is *recollement*, which we recall below.

Definition 5.1. Let X be a scheme, let $i\colon Z \to X$ be a closed immersion, and let $j\colon U \to X$ be its open complement.

Define the category $\mathrm{Sh}_{Z,U}(X_{\text{ét}})$ as follows. The set of objects of the category $\mathrm{Sh}_{Z,U}(X_{\text{ét}})$ is the set of triples $(\mathcal{F}_Z, \mathcal{F}_U, \phi)$ of a sheaf $\mathcal{F}_Z$ on $Z_{\text{ét}}$, a sheaf $\mathcal{F}_U$ on $U_{\text{ét}}$, and a morphism $\phi\colon \mathcal{F}_Z \to i^{-1}j_*\mathcal{F}_U$. For objects $(\mathcal{F}_Z, \mathcal{F}_U, \phi)$ and $(\mathcal{F}'_Z, \mathcal{F}'_U, \phi')$ of $\mathrm{Sh}_{Z,U}(X_{\text{ét}})$, the set of morphisms from $(\mathcal{F}_Z, \mathcal{F}_U, \phi)$ to $(\mathcal{F}'_Z, \mathcal{F}'_U, \phi')$ is the set of pairs (f_Z, f_U) of a morphism $f_Z\colon \mathcal{F}_Z \to \mathcal{F}'_Z$ and a morphism $f_U\colon \mathcal{F}_U \to \mathcal{F}'_U$ such that the following diagram commutes.

$$\begin{array}{ccc} \mathcal{F}_Z & \xrightarrow{f_Z} & \mathcal{F}'_Z \\ \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi'} \\ i^{-1}j_*\mathcal{F}_U & \xrightarrow[i^{-1}j_*(f_U)]{} & i^{-1}j_*\mathcal{F}'_U \end{array}$$

Theorem 5.2 (Recollement, e.g. [10, §5.4])**.** *Let X be a scheme, let $i\colon Z \to X$ be a closed immersion, and let $j\colon U \to X$ be its open complement.*

Then the functor $\mathrm{Sh}(X_{ét}) \to \mathrm{Sh}_{Z,U}(X_{ét})$ sending the sheaf $\mathcal{F}$ to the triple $(i^{-1}\mathcal{F}, j^{-1}\mathcal{F}, i^{-1}(\upsilon))$, where $\upsilon\colon \mathcal{F} \to j_*j^{-1}\mathcal{F}$ is the unit map of the adjoint pair (j^{-1}, j_*) of functors, is an equivalence of categories, and a quasi-inverse $\mathrm{Sh}_{Z,U}(X_{ét}) \to \mathrm{Sh}(X_{ét})$ is given by sending $(\mathcal{F}_Z, \mathcal{F}_U, \phi)$ to $i_*\mathcal{F}_Z \times_{i_*(\phi), i_*i^{-1}j_*\mathcal{F}_U, \upsilon} j_*\mathcal{F}_U$, where $\upsilon\colon j_*\mathcal{F}_U \to i_*i^{-1}j_*\mathcal{F}_U$ is the unit map of the adjoint pair (i^{-1}, i_*) of functors.

Note that the functor $i^{-1}j_*$ is left exact, hence commutes with finite limits.

Let us apply this to our category of torsors. So let $\mathcal{T}$ denote the category of $j_!\mathcal{G}$-torsors on $X_{\text{ét}}$, and let $\mathcal{T}_{Z,U}$ denote the category of which the objects are pairs $(\mathcal{F}, s)$ of a $\mathcal{G}$-torsor $\mathcal{F}$ on $U_{\text{ét}}$, and a section $s \in i^{-1}j_*\mathcal{F}(Z)$, and in which the morphisms $(\mathcal{F}, s) \to (\mathcal{F}', s')$ are the morphisms $f\colon \mathcal{F} \to \mathcal{F}'$ such that $i^{-1}j_*(f)$ sends s to s'.

Lemma 5.3. *Let X be a scheme, let $i\colon Z \to X$ be a closed immersion, and let $j\colon U \to X$ be its open complement. Let $\mathcal{G}$ be a sheaf of groups on $U_{\acute{e}t}$. The rule attaching to a $j_!\mathcal{G}$-torsor $\mathcal{F}$ on $X_{\acute{e}t}$ the pair $(j^{-1}\mathcal{F}, i^{-1}(\upsilon))$, where $\upsilon\colon \mathcal{F} \to j_*j^{-1}\mathcal{F}$ denotes the unit map of the adjoint pair (j^{-1}, j_*) of functors, defines an equivalence $\mathcal{T} \to \mathcal{T}_{Z,U}$ of categories.*

Proof. First, note that the sheaf $j_!\mathcal{G}$ is under recollement equivalent to the triple $(1, \mathcal{G}, 1)$.

Now giving a $j_!\mathcal{G}$-action ρ on a sheaf $\mathcal{F}$ on $X_{\text{ét}}$ is equivalent to giving $(i^{-1}\mathcal{F}, j^{-1}\mathcal{F}, i^{-1}(\upsilon))$ together with an action of $\mathcal{G}$ on $j^{-1}\mathcal{F}$; the commutativity of

$$\begin{array}{ccc} 1 \times i^{-1}\mathcal{F} & \xrightarrow{\rho_Z} & i^{-1}\mathcal{F} \\ \downarrow{\scriptstyle 1\times i^{-1}(\upsilon)} & & \downarrow{\scriptstyle i^{-1}(\upsilon)} \\ i^{-1}j_*\mathcal{G} \times i^{-1}j_*j^{-1}\mathcal{F} & \xrightarrow[i^{-1}j_*(\rho_U)]{} & i^{-1}j_*j^{-1}\mathcal{F} \end{array}$$

is automatic since both ρ_Z and $i^{-1}j_*(\rho_U)$ are group actions. (Of course, one can also deduce this equivalence by noting that a morphism $j_!\mathcal{G} \to \underline{\mathrm{Aut}}(\mathcal{F})$ is equivalent to a morphism $\mathcal{G} \to j^{-1}\underline{\mathrm{Aut}}(\mathcal{F}) = \underline{\mathrm{Aut}}(\mathcal{F}_U)$.)

Now $\mathcal{F}$ is a $j_!\mathcal{G}$-torsor if and only if the map $j_!\mathcal{G} \times \mathcal{F} \to \mathcal{F} \times \mathcal{F}$ given on local sections by $(g, s) \mapsto (s, gs)$ is an isomorphism, and $\mathcal{F}$ locally has a section. This is equivalent to the following.

- $i^{-1}\mathcal{F}$ is the terminal sheaf on $Z_{\text{ét}}$; therefore $i^{-1}(\upsilon)$ is an element of $i^{-1}j_*\mathcal{F}(Z)$, and it follows that the given rule indeed defines a functor;
- $j^{-1}\mathcal{F}$ is a $\mathcal{G}$-torsor on $U_{\text{ét}}$,

so the given rule defines an equivalence, as desired. □

5.2. Pushforward and normalisation. Next, we consider a description of the pushforward of a finite locally constant sheaf along certain open immersions. This is mostly well-known, but the author doesn't know of a reference, so proofs are included here for completeness.

Recall that, for a scheme X, the category of sheaves on $X_{\text{ét}}$ is equivalent to that of algebraic spaces étale over X. Quasi-inverses are given by the functor sending an algebraic space étale over X to its functor of points, and the functor sending a sheaf on $X_{\text{ét}}$ to its *espace étalé*. By descent, finite locally constant sheaves on $X_{\text{ét}}$ are precisely those of which the espace étalé is a finite étale X-scheme.

Proposition 5.4. *Let X be a scheme, and let $j\colon U \to X$ be a quasi-compact open immersion such that the normalisation of X in U is X. Let $\mathcal{F}$ be a finite locally constant sheaf on $U_{\acute{e}t}$, or equivalently, a finite étale U-scheme. Let $\overline{\mathcal{F}}$ be the normalisation of X in $\mathcal{F}$. Then for all étale X-schemes T, we have $j_*\mathcal{F}(T) = \overline{\mathcal{F}}(T)$ functorial in T.*

Proof. First of all, note that we may restrict ourself to étale X-schemes T that are affine, and therefore to quasi-compact separated étale X-schemes T. So let T be an étale quasi-compact separated X-scheme. Let $\overline{T}$ be the normalisation of X in T, and let $\overline{U \times_X T}$ be the normalisation of X in $U \times_X T$. Then $j_*\mathcal{F}(T) = \mathcal{F}(U \times_X T)$, and we have a map $\mathcal{F}(U \times_X T) \to \overline{\mathcal{F}}(\overline{U \times_X T})$. Since for every Y-morphism $\overline{U \times_X T} \to \overline{\mathcal{F}}$, the composition with $U \times_X T \to \overline{U \times_X T}$ factors through $\mathcal{F}$ (as $\mathcal{F}$ is a finite étale X-scheme), it follows that $\mathcal{F}(U \times_X T) = \overline{\mathcal{F}}(\overline{U \times_X T})$.

Now note that since normalisation commutes with smooth base change (see e.g. [23, Tag 082F]), it follows that the normalisation of T in $U \times_X T$ is simply T. Therefore $\overline{U \times_X T} \to \overline{T}$ is an isomorphism, and we have $\overline{\mathcal{F}}(\overline{U \times_X T}) = \overline{\mathcal{F}}(\overline{T}) = \overline{\mathcal{F}}(T)$, as desired. □

Corollary 5.5. *Let X be a scheme, and let $j\colon U \to X$ be a quasi-compact open immersion such that the normalisation of X in U is X. Then for all finite sets F, we have $j_*F = F$.*

Lemma 5.6. *Let k be a field, let X be a k-scheme of finite type, and let $j\colon U \to X$ be an open immersion such that the normalisation of X in U is X. Let $\mathcal{F}$ be a finite locally constant sheaf on $U_{ét}$, or equivalently, a finite étale U-scheme. Then $j_*\mathcal{F}$ is representable by an étale, quasi-compact, separated X-scheme.*

Proof. First note that by [5, Thm. finitude] $j_*\mathcal{F}$ is constructible, i.e. of finite presentation as an X-space.

Note that $\mathcal{F}$ is finite locally constant, so $\mathcal{F} \times \mathcal{F}$ is the disjoint union of the diagonal and its complement, inducing a morphism $\mathcal{F} \times \mathcal{F} \to \mathbb{Z}/2\mathbb{Z}$ such that the equaliser with the constant map with value 0 is the diagonal. Applying the left exact functor j_* to this gives a morphism $j_*\mathcal{F} \times j_*\mathcal{F} \to j_*(\mathbb{Z}/2\mathbb{Z}) = \mathbb{Z}/2\mathbb{Z}$ such that the equaliser with the constant map with value 0 is the diagonal. Therefore $j_*\mathcal{F}$ is separated as an X-space.

It follows by [23, Tag 03XX] that $j_*\mathcal{F}$ is representable by an étale, quasi-compact, separated X-scheme. □

Lemma 5.7. *Let k be a field, let X be a k-scheme of finite type, and let $j\colon U \to X$ be an open immersion such that the normalisation of X in U is X. Let $\mathcal{F}$ be a finite locally constant sheaf on $U_{ét}$, or equivalently, a finite étale U-scheme. Let $\overline{\mathcal{F}}$ be the normalisation of X in $\mathcal{F}$. Then $\overline{\mathcal{F}}$ is the normalisation of X in $j_*\mathcal{F}$.*

Proof. First note that we have a canonical morphism $j_*\mathcal{F} \to \overline{\mathcal{F}}$ corresponding to the identity section of $j_*\mathcal{F}$. Let $j_*\mathcal{F} \to Y \to X$ be a factorisation with $Y \to X$ integral. As $\overline{\mathcal{F}}$ is the normalisation of X in $\mathcal{F}$, it follows that

there exists a unique morphism $\overline{\mathcal{F}} \to Y$ such that the diagram

$$\begin{array}{ccc} \mathcal{F} & \longrightarrow & \overline{\mathcal{F}} \\ \downarrow & \swarrow & \downarrow \\ Y & \longrightarrow & X \end{array}$$

commutes. We show that this morphism also makes the diagram

$$\begin{array}{ccc} j_*\mathcal{F} & \longrightarrow & \overline{\mathcal{F}} \\ \downarrow & \swarrow & \\ Y & & \end{array} \tag{5.1}$$

commute. Let T be an étale quasi-compact separated X-scheme, and consider the following diagram.

$$\begin{array}{ccc} j_*\mathcal{F}(T) & \longrightarrow & \overline{\mathcal{F}}(T) \\ \downarrow & \swarrow & \\ Y(T) & & \end{array}$$

As the normalisations of X in T and $U \times_X T$ are equal, as in the proof of Proposition 5.4, the commutativity of this diagram is equivalent to the commutativity of the following one.

$$\begin{array}{ccc} \mathcal{F}(U \times_X T) & \longrightarrow & \overline{\mathcal{F}}(U \times_X T) \\ \downarrow & \swarrow & \\ Y(U \times_X T) & & \end{array}$$

It follows that the commutativity of (5.1) holds when restricted to $X_{\text{ét}}$.

Therefore, applying this to the identity section on $j_*\mathcal{F}$, it follows that (5.1) itself commutes. □

By Zariski's Main Theorem, we have the following.

Corollary 5.8. *The canonical morphism $j_*\mathcal{F} \to \overline{\mathcal{F}}$ is an open immersion identifying $j_*\mathcal{F}$ with the étale locus of $\overline{\mathcal{F}}$ over X.*

Proof. The étale locus V of $\overline{\mathcal{F}}$ over X is open in $\overline{\mathcal{F}}$ and étale over X, therefore factors through $j_*\mathcal{F}$. By maximality of V we get $j_*\mathcal{F} = V$. □

5.3. Galois actions on finite locally constant sheaves. Let X be a scheme, and let Γ be a group acting on X. Then recall that a Γ-*sheaf* on $X_{\text{ét}}$ is a sheaf $\mathcal{F}$ on $X_{\text{ét}}$ of which the espace étalé is a Γ-equivariant X-space.

Let X be a connected scheme, let Γ be a finite group, and let $f\colon Y \to X$ be a finite étale connected Galois cover with Galois group Γ. Note that

pullback of sheaves defines an equivalence from the category of sheaves on $X_{\text{ét}}$ to that of Γ-sheaves on $Y_{\text{ét}}$. A quasi-inverse is given in terms of sheaves by sending $\mathcal{F}$ to the sheaf of Γ-invariants of $f_*\mathcal{F}$; in terms of espaces étalés, it sends an algebraic space Z étale over Y to the quotient $\Gamma\backslash Z$.

If $\mathcal{G}$ is a finite locally constant sheaf of groups on $X_{\text{ét}}$ such that $f^{-1}\mathcal{G}$ is constant, let G be the group of connected components of $f^{-1}\mathcal{G}$, and note that Γ acts on G by automorphisms. Therefore we see that a finite locally constant sheaf on $X_{\text{ét}}$ with $\mathcal{G}$-action corresponds to a Γ- and G-equivariant finite étale Y-scheme.

Let us now apply this to the following situation (compare with Situation 2.4).

Situation 5.9. Let k be a field. Suppose we have a finite group Γ, and a diagram of schemes of finite type over k

$$\begin{array}{ccccc} V & \xrightarrow{j'} & Y & \xleftarrow{i'} & W \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle h} \\ U & \xrightarrow[j]{} & X & \xleftarrow[i]{} & Z \end{array}$$

where U and X are connected, g is finite étale Galois with Galois group Γ, Y is the normalisation of X in V, $W = Y \times_X Z$, and j is the open complement of i. Let $\mathcal{G}$ be a finite locally constant sheaf of groups on $\mathcal{U}$ such that $g^{-1}\mathcal{G}$ is constant, say with group of connected components G.

Let $\mathcal{T}_{Z,U}$ be as in the previous section, and let $\mathcal{T}^{\Gamma}_{W,Y}$ be the category of which the objects are pairs $(\mathcal{F}, s)$ of a Γ-equivariant G-torsor $\mathcal{F}$ on $Y_{\text{ét}}$, and a Γ-equivariant section $s \in (i')^{-1}\mathcal{F}(W)$, and in which the morphisms $(\mathcal{F}, s) \to (\mathcal{F}', s')$ are the Γ-equivariant morphisms $f\colon \mathcal{F} \to \mathcal{F}'$ such that $(i')^{-1}(f)$ sends s to s'.

Lemma 5.10. *In Situation 5.9, the rule attaching to a pair $(\mathcal{F}, s)$ of a $\mathcal{G}$-torsor $\mathcal{F}$ and a section $s \in i^{-1}j_*\mathcal{F}(Z)$ the pair $(j'_*g^{-1}\mathcal{F}, s)$ defines an equivalence $\mathcal{T}_{Z,U} \to \mathcal{T}^{\Gamma}_{W,Y}$ of categories.*

Proof. First note that giving a $\mathcal{G}$-torsor $\mathcal{F}$ on $U_{\text{ét}}$ is equivalent to giving the Γ-equivariant G-torsor $g^{-1}\mathcal{F}$ on $V_{\text{ét}}$. Moreover, giving the section $s\colon Z \to i^{-1}j_*\mathcal{F}$ is the same as giving a Γ-invariant section $Z \to i^{-1}j_*g_*g^{-1}\mathcal{F} = i^{-1}f_*j'_*g^{-1}\mathcal{F} = h_*(i')^{-1}j'_*g^{-1}\mathcal{F}$, where the last step uses proper base change. This is the same as giving a Γ-equivariant section $W \to (i')^{-1}j'_*g^{-1}\mathcal{F}$.

Now $j'_*g^{-1}\mathcal{F}$ is a Γ-equivariant G-pseudotorsor which étale locally has a section, i.e. a Γ-equivariant G-torsor. Therefore giving the pair $(g^{-1}\mathcal{F}, s)$ is equivalent to giving $(j'_*g^{-1}\mathcal{F}, s)$, as desired. □

6. Computation of a groupoid scheme

In this section, we describe the core of our algorithm. (Though the core of this paper isn't the part of the algorithm described in this section, but rather its correctness.)

First, recall the following situation (Situation 2.4).

Situation 6.1. We are given a field k, a finite group Γ, for $p = 0, \infty \in \mathbb{P}^1(k)$, a subset S_p of $\{p\}$, and a diagram

$$\begin{array}{ccccc} V & \longrightarrow & Y & \longrightarrow & \overline{Y} \\ {\scriptstyle g}\downarrow & & \downarrow & & \downarrow \\ U & \xrightarrow{\quad j \quad} & X & \longrightarrow & \overline{X} \\ \downarrow & & \downarrow & & \downarrow \\ \mathbb{P}^1_k - S_0 - S_\infty & \longrightarrow & \mathbb{P}^1_k - S_\infty & \longrightarrow & \mathbb{P}^1_k \end{array}$$

in which:

- all squares are cartesian;
- $\overline{X}$ and $\overline{Y}$ are smooth, proper, and finite and generically étale over $\mathbb{P}^1_k$;
- $g\colon V \to U$ is Galois with group Γ.

Moreover, we are given a finite locally constant sheaf $\mathcal{G}$ of groups on U such that $g^{-1}\mathcal{G}$ is constant, and denote by G its group of connected components; the Galois action of Γ on V induces an action of Γ on G by automorphisms.

Then our algorithm proceeds by first reducing to Situation 2.4, and computing $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$ in Situation 2.4.

The core of our algorithm then is the computation of a groupoid k-scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ that satisfies the following properties.

- Both morphisms $\mathcal{R} \to \mathcal{U}$ are smooth and have geometrically connected fibres.
- Both $\mathcal{R}$ and $\mathcal{U}$ are affine and of finite type over k.
- There exists a functor from the category $\mathcal{U}(S)$ to the category of $j_!\mathcal{G}|_{U_S}$-torsors, functorial in the k-scheme S, that is an equivalence if S is the spectrum of a perfect field extension of k.

These conditions will imply that the set $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}})$ of geometric connected components of $\mathcal{U}$ is, as a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set, isomorphic to $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$. The proof of this is the subject of Section 7. We will also derive complexity bounds for this part of our algorithm.

As for how we represent Situation 2.4 and the output groupoid:

- As stated in Section 3, we will construct a generic field algorithm, so the representation of field elements, and all algorithms for the

"basic" operations are assumed to be given, and are used as black boxes.

- Finite locally free curves over $\mathbb{P}^1_k$ are given in terms of the description in Section 4, i.e. as standard modules together with the structure of a ring.
- Finite groups are given by their multiplication tables and finite group actions on finite locally free curves are given by a sequence of automorphisms.

Note that we haven't explained yet how to decide whether such an input is valid, but the characterisations in this section and the introduction of the next section will allow us to do so. The output groupoid will be given using generators and relations for their underlying coordinate rings.

We briefly recall the strategy outlined in Section 2 for the computation of the target groupoid k-scheme, but with slightly more details. This strategy is to translate the concept of a $j_!\mathcal{G}$-torsor (and isomorphisms between two of them) on $X_{\text{ét}}$ to a description purely in terms of linear maps between vector bundles on $\mathbb{P}^1_k$ and commutativity relations between them. Since we have a parametrisation of sets of morphisms between two such vector bundles as an affine space (Section 4), this will readily translate into a presentation of our groupoid scheme that satisfies the desired properties.

As a first step, let us describe, for a field extension l of k, the category $\mathcal{T}(l)$ of $j_!\mathcal{G}$-torsors on $(X_l)_{\text{ét}}$ more closely. By Lemma 5.10, $\mathcal{T}(l)$ is equivalent to that of Γ-equivariant G-torsors on $(Y_l)_{\text{ét}}$, together with a Γ-equivariant section from $\overline{Y_l} \times_{\mathbb{P}^1_l} S_0$. (We note that in case $S_0 = \emptyset$, the empty morphism is Γ-equivariant.) By taking normal completions, we obtain the following.

Proposition 6.2. *Let l be a perfect field extension of k. Then the category $\mathcal{T}(l)$ is equivalent to that of finite locally free $\mathbb{P}^1_l$-schemes T, smooth over l, together with a Γ-equivariant G-action, a Γ-equivariant morphism $T \to \overline{Y_l}$ and a Γ-equivariant section $\overline{Y_l} \times_{\mathbb{P}^1_l} S_0 \to T \times_{\mathbb{P}^1_l} S_0$, such that $T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is a G-torsor on $(Y_l)_{ét}$; here, the morphisms are the Γ-equivariant, G-equivariant morphisms of $\overline{Y_l}$-schemes.*

So aside from the conditions "smooth over l" and "$T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is a G-torsor on $(Y_l)_{\text{ét}}$", the data in the description above can readily be expressed in terms of morphisms of vector bundles on $\mathbb{P}^1_l$, and the relations in the description above can be easily expressed in terms of commutativity relations between these morphisms.

Example 6.3. As an example, we work out the equations of some of the commutativity relations mentioned above, in terms of the parametrisation given in Section 4. In the context of Situation 2.4, we take $\overline{X} = \mathbb{P}^1$, $S_0 = \{0\}$, $S_\infty = \{\infty\}$, Γ trivial, and for $\mathcal{G}$ the constant group sheaf with group $\mathbb{Z}/2\mathbb{Z}$. Moreover, we will restrict ourselves to describing (some of

the) equations for torsors of which the underlying $\mathcal{O}_{\mathbb{P}^1}$-module is a standard module of type $(0,-1)$.

Let k be a field. We will write $\mathcal{O} = \mathcal{O}_{\mathbb{P}^1_k}$ throughout this example. We first consider the space of algebra structures on a standard module of type $a = (0,-1)$. Note that an algebra structure is given by a unit morphism

$$\iota \in \mathrm{Hom}_{\mathcal{O}}(\mathcal{O}, \mathcal{O} \oplus \mathcal{O}(-1))$$

and a multiplication morphism

$$\mu \in \mathrm{Hom}_{\mathcal{O}}((\mathcal{O} \oplus \mathcal{O}(-1)) \otimes (\mathcal{O} \oplus \mathcal{O}(-1)), \mathcal{O} \oplus \mathcal{O}(-1))$$

satisfying the usual relations. Under the identification of Section 4, ι is equivalent to a pair (ι_1, ι_2) with $\iota_1 \in \mathcal{O}(\mathbb{P}^1_k) = k$ and $\iota_2 \in \mathcal{O}(-1)(\mathbb{P}^1_k) = \{0\}$, or equivalently, an element $\iota_{10} \in k$. Note that ι_1 and ι_{10} define the same element of k; however, we will view ι_1 as a homogeneous polynomial of degree 0, and ι_{10} as its unique coefficient.

Similarly, μ is equivalent to a tuple $(\mu_{ijk})_{i,j,k=1}^2$ with

$$\mu_{ijk} = \sum_{\alpha=0}^{a_k-a_i-a_j} \mu_{ijk\alpha} x^{a_k-a_i-a_j-\alpha} y^\alpha \in \mathcal{O}(a_k - a_i - a_j) = k[x,y]_{a_k-a_i-a_j},$$

which is equivalent to a 12-tuple

$$(\mu_{1110}, \mu_{1210}, \mu_{1211}, \mu_{1220}, \mu_{2110}, \mu_{2111}, \mu_{2120}, \mu_{2210}, \mu_{2211}, \mu_{2212}, \mu_{2220}, \mu_{2221})$$

of elements of k.

We now consider the relations. Commutativity of μ is easily expressed by the relations $\mu_{ijk} = \mu_{jik}$ for all i,j,k, giving non-trivial relations

$$\begin{aligned} \mu_{1210} &= \mu_{2110}, \\ \mu_{1211} &= \mu_{2111}, \\ \mu_{1220} &= \mu_{2120}. \end{aligned}$$

Working out the condition that ι is a left unit for μ yields the relations $\mu_{1ij}\iota_1 = 0$ if $i \neq j$ and $\mu_{1ii}\iota_1 = 1$, which gives the non-trivial relations

$$\begin{aligned} \mu_{1110}\iota_{10} &= 1, \\ \mu_{1210} = \mu_{1211} &= 0, \\ \mu_{1220}\iota_{10} &= 1, \end{aligned}$$

and therefore by commutativity also the relations

$$\begin{aligned} \mu_{2110} = \mu_{2111} &= 0, \\ \mu_{2120}\iota_{10} &= 1, \end{aligned}$$

Finally, the associativity of μ amounts to the relations

$$\mu_{i1l}\mu_{jk1} + \mu_{i2l}\mu_{jk2} = \mu_{1kl}\mu_{ij1} + \mu_{2kl}\mu_{ij2}$$

for all i, j, k, l. This doesn't give any new relations on the μ_{ijkl}. One way of seeing this, is the following. Note that over the function field $k(x)$ of $\mathbb{P}^1$, the induced symmetric $k(x)$-bilinear map $m\colon k(x)^2 \times k(x)^2 \to k(x)^2$ has a unit e, and for any $z \in k(x)^2$ linearly independent of e, any choice of $m(z,z) = az + be$ makes $k(x)$ isomorphic to $k(x)[\alpha]/(\alpha^2 - a\alpha - b)$. Hence for any choice of $\iota_1 \neq 0, \mu_{221}, \mu_{222}$, the resulting map μ is already associative.

Next, we add the structure of a $\mathbb{Z}/2\mathbb{Z}$-action on the resulting algebra, which is simply an $\mathcal{O}$-linear map $\rho\colon \mathcal{O} \oplus \mathcal{O}(-1) \to \mathcal{O} \oplus \mathcal{O}(-1)$ compatible with the algebra structure and such that ρ^2 is the identity. In the same way as before, we see that giving ρ is equivalent to giving

$$\rho_{ij} = \sum_{\alpha=0}^{a_j - a_i} \rho_{ij\alpha} x^{a_j - a_i - \alpha} y^\alpha \in k[x,y]_{a_j - a_i},$$

i.e. to a 4-tuple $(\rho_{110}, \rho_{210}, \rho_{211}, \rho_{220})$ of elements of k.

The identity $\rho^2 = \mathrm{id}$ gives us relations $\rho_{1j}\rho_{i1} + \rho_{2j}\rho_{i2} = 0$ for all i, j such that $i \neq j$, and $\rho_{1i}\rho_{i1} + \rho_{2i}\rho_{i2} = 1$ for all i. Working this out, we get

$$\begin{aligned} \rho_{110}^2 = \rho_{220}^2 &= 1, \\ \rho_{210}(\rho_{110} + \rho_{220}) &= 0, \\ \rho_{211}(\rho_{110} + \rho_{220}) &= 0. \end{aligned}$$

Finally, we consider the compatibility of ρ with the algebra structure. First, the condition $\rho\iota = \iota$ gives us the relation $\rho_{11}\iota_1 = \iota_1$, or equivalently, the relation $\rho_{110} = 1$. The condition $\mu \circ (\rho \otimes \rho) = \rho\mu$ gives us the relations

$$\mu_{11k}\rho_{i1}\rho_{j1} + \mu_{12k}\rho_{i1}\rho_{j2} + \mu_{21k}\rho_{i2}\rho_{j1} + \mu_{22k}\rho_{i2}\rho_{j2} = \rho_{1k}\mu_{ij1} + \rho_{2k}\mu_{ij2} \tag{6.1}$$

for all i, j, k. Of these relations, we see that only the relations for $i = j = 2$, being

$$\begin{aligned} \mu_{111}\rho_{21}^2 &= \rho_{21}\mu_{222}, \\ \mu_{122}\rho_{21}\rho_{22} + \mu_{212}\rho_{22}\rho_{21} + \mu_{222}\rho_{22}^2 &= \rho_{22}\mu_{222} \end{aligned}$$

(which are simplified a bit), cannot be obtained from previously mentioned relations. Comparing coefficients, we obtain the following equations:

$$\begin{aligned} \mu_{1110}\rho_{210}^2 &= \rho_{210}\mu_{2220}, \\ 2\mu_{1110}\rho_{210}\rho_{211} &= \rho_{210}\mu_{2221} + \rho_{211}\mu_{2220}, \\ \mu_{1110}\rho_{211}^2 &= \rho_{211}\mu_{2221}, \\ \mu_{1220}\rho_{210} + \mu_{2120}\rho_{210} + \mu_{2220}\rho_{220} &= \mu_{2220}, \\ \mu_{1220}\rho_{211} + \mu_{2120}\rho_{211} + \mu_{2221}\rho_{220} &= \mu_{2221}. \end{aligned}$$

Note that in this small example, we already get quite a lot of equations. It may be more enlightening to write out 6.1 in a more general form in

terms of the coefficients $\rho_{ij\lambda}, \mu_{ijk\lambda}$, which is given by the equations

$$\sum_{a,b} \sum_{\alpha+\beta+\gamma=\lambda} \mu_{abk\alpha}\rho_{ia\beta}\rho_{jb\gamma} = \sum_{a} \sum_{\alpha+\beta=\lambda} \rho_{ak\alpha}\mu_{ija\beta}$$

for all i, j, k, λ (where $\lambda = 0, 1, \ldots, a_k - a_i - a_j$).

6.1. Torsors. Let us first consider the condition "$T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is a G-torsor on $(Y_l)_{\text{ét}}$". To this end, we first express the condition "T is finite locally free over $\mathbb{P}^1_l$ of constant rank", using the fibre of Y_l above $0 \in \mathbb{P}^1_l$; this is not automatic as we didn't assume $\overline{Y}$ to be geometrically connected.

Lemma 6.4. *Let S be a scheme, let X be a finite locally free $\mathbb{P}^1_S$-scheme that is smooth over S. Let Y be an X-scheme that is finite locally free over $\mathbb{P}^1_S$, such that $Y \times_{\mathbb{P}^1_S} 0$ is finite locally free over $X \times_{\mathbb{P}^1_S} 0$ of constant rank n. Then Y is a finite locally free X-scheme of constant rank n.*

Proof. We can check fibrewise on S that $X \times_{\mathbb{P}^1_S} 0$ intersects all components of X, from which our claim follows. □

Since finite locally free modules over an Artinian ring are free, we have the following.

Corollary 6.5. *Let l be a perfect field extension of k. Then the category of finite locally free $\overline{Y_l}$-schemes of constant rank is equivalent to that of finite locally free $\mathbb{P}^1_l$-schemes T together with a morphism $T \to \overline{Y_l}$ and an $\mathcal{O}(\overline{Y_l} \times_{\mathbb{P}^1_l} 0)$-basis for $\mathcal{O}(T \times_{\mathbb{P}^1_l} 0)$ (morphisms in this category are simply morphisms of $\overline{Y_l}$-schemes).*

Next, we want to express the condition "$T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is étale over Y_l" in terms of vector bundles on $\mathbb{P}^1_l$. To this end, we will use the *transitivity of the discriminant*.

First, we recall the definitions of the *discriminant* and the *norm* of a finite locally free morphism $Y \to X$. Recall that, for a finite locally free morphism $Y \to X$ of schemes, we view $\mathcal{O}_Y$ as a (finite locally free) $\mathcal{O}_X$-algebra.

Definition 6.6. Let $f\colon Y \to X$ be a finite locally free morphism of schemes of constant rank, and let μ be the multiplication map $\mathcal{O}_Y \otimes_{\mathcal{O}_X} \mathcal{O}_Y \to \mathcal{O}_Y$. The *trace form* τ_f of f is the morphism $\mathcal{O}_Y \to \mathcal{H}om_{\mathcal{O}_X}(\mathcal{O}_Y, \mathcal{O}_X)$ corresponding to the composition $\mathrm{Tr}_f \mu\colon \mathcal{O}_Y \otimes_{\mathcal{O}_X} \mathcal{O}_Y \to \mathcal{O}_X$. The *discriminant* Δ_f of f is the determinant (over $\mathcal{O}_X$) of the trace form τ_f.

Definition 6.7 (cf. [9])**.** Let $f\colon Y \to X$ be a finite locally free morphism of schemes of constant rank, and let $\mathcal{L}$ be a line bundle on Y. The *norm* $\mathrm{N}_f \mathcal{L}$ of $\mathcal{L}$ is the line bundle

$$\mathcal{H}om_{\mathcal{O}_X}(\det_{\mathcal{O}_X} f_*\mathcal{O}_Y, \det_{\mathcal{O}_X} f_*\mathcal{L}).$$

Let $f\colon Y \to X$ be a finite locally free morphism of schemes of constant rank, and let $\mathcal{E}$ and $\mathcal{F}$ be finite locally free $\mathcal{O}_Y$-modules of the same constant rank. By [6, Eq. 7.1.1] and the fact that norms (of line bundles) commute with tensor products and duals (see [12, §6.5] and [9, Prop. 3.3]), we see that there is a unique isomorphism

$$\mathcal{H}om_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E}, \det_{\mathcal{O}_X}\mathcal{F}) = \mathcal{H}om_{\mathcal{O}_X}(\mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E}, \mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{F})$$

satisfying the following properties.

- It is compatible with base change by open immersions.
- For any isomorphism $\alpha\colon \mathcal{F} \to \mathcal{E}$, we have induced isomorphisms

  $$\mathcal{H}om_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E}, \det_{\mathcal{O}_X}\mathcal{F}) \to \mathcal{E}nd_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E})$$

  and

  $$\mathcal{H}om_{\mathcal{O}_X}(\mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E}, \mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{F}) \to \mathcal{E}nd_{\mathcal{O}_X}(\mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E}).$$

  Therefore they induce isomorphisms

  $$\mathcal{I}som_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E}, \det_{\mathcal{O}_X}\mathcal{F}) \to \mathcal{A}ut_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E}) = \mathbb{G}_{m,X}$$

  and

  $$\mathcal{I}som_{\mathcal{O}_X}(\mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E}, \mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{F}) \to \mathcal{A}ut_{\mathcal{O}_X}(\mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E}) = \mathbb{G}_{m,X}.$$

  These isomorphisms are equal under the given identification.

Therefore, we have the following.

Corollary 6.8. *Let $f\colon Y \to X$ be a finite locally free morphism of schemes of constant rank, and let $\mathcal{E}$ be a finite locally free $\mathcal{O}_Y$-module of constant rank r. Then*

$$\det_{\mathcal{O}_X}\mathcal{E} = \mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{E} \otimes_{\mathcal{O}_X} (\det_{\mathcal{O}_X}\mathcal{O}_Y)^{\otimes r}$$

$$\mathcal{H}om_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{E}, \mathcal{O}_X) = \mathrm{N}_f \det_{\mathcal{O}_Y}\mathcal{H}om_{\mathcal{O}_Y}(\mathcal{E}, \mathcal{O}_Y) \otimes_{\mathcal{O}_X} \left(\mathcal{H}om_{\mathcal{O}_X}(\det_{\mathcal{O}_X}\mathcal{O}_Y, \mathcal{O}_X)\right)^{\otimes r}$$

Using the two identifications above, we may now state the transitivity of the discriminant. A proof can be found in e.g. [20, §4.1].

Theorem 6.9 (Transitivity of the discriminant)**.** *Let $f\colon Y \to X$ and $g\colon Z \to Y$ be finite locally free morphisms of schemes of constant rank, and suppose that g has rank r. Then*

$$\Delta_{fg} = \mathrm{N}_f \Delta_g \otimes \Delta_f^{\otimes r}.$$

Corollary 6.10. *Let $f\colon Y \to X$ and $g\colon Z \to Y$ be finite locally free morphisms of schemes of constant rank, and suppose that g has rank r. Then g is étale if and only if we have $\det_{\mathcal{O}_X}\mathcal{O}_Z \cong (\det_{\mathcal{O}_X}\mathcal{O}_Y)^{\otimes r}$ and Δ_{fg} and $\Delta_f^{\otimes r}$ differ by a unit.*

Therefore we have the following.

Proposition 6.11. *Let l be a perfect extension of k. Then the category of finite étale $\overline{Y_l}$-schemes is equivalent to the full subcategory of that of finite locally free $\overline{Y_l}$-schemes T of constant rank (say r) such that $\det_{\mathcal{O}_{\mathbb{P}^1_l}} \mathcal{O}_T \cong (\det_{\mathcal{O}_{\mathbb{P}^1_l}} \mathcal{O}_{\overline{Y_l}})^{\otimes r}$ and $\Delta_{T/\mathbb{P}^1_l}$ and $\Delta^{\otimes r}_{\overline{Y_l}/\mathbb{P}^1_l}$ differ by a unit.*

Note that the condition on the determinants is simply a condition on the types of the standard modules over l isomorphic to $\mathcal{O}_T$ and $\mathcal{O}_{\overline{Y_l}}$, so if $S_\infty = \emptyset$, this gives an expression of the desired form. If $S_\infty = \infty$, then we use the following instead.

Proposition 6.12. *Let l be a perfect extension of k, and assume that $S_\infty = \infty$. Then the category of finite locally free $\overline{Y_l}$-schemes étale over Y_l is equivalent to the full subcategory of that of finite locally free $\overline{Y_l}$-schemes T of constant rank (say r) such that $\Delta_{T/\mathbb{P}^1_l}$ and $\Delta^{\otimes r}_{\overline{Y_l}/\mathbb{P}^1_l}$ differ by a unit times a power of y.*

Proof. It suffices to show that for integers a, b, a map $\phi\colon \mathcal{O}_{\mathbb{P}^1_l}(b) \to \mathcal{O}_{\mathbb{P}^1_k}(a)$ is an isomorphism when restricted to $\mathbb{A}^1_l$ if and only if it is given by multiplication by sy^{a-b} with $s \in l^\times$. Since y becomes invertible after restricting to $\mathbb{A}^1_l$, it follows that if ϕ is multiplication by sy^{a-b}, then $\phi|_{\mathbb{A}^1_l}$ is an isomorphism. Conversely, ϕ is multiplication by some $f \in l[x,y]_{a-b}$, which after restriction becomes the multiplication by $f(x,1)$ map $l[x] \to l[x]$. Since this map is an isomorphism, $f(x,1)$ must be an invertible constant in $l[x]$, i.e. $f = sy^{a-b}$ for some $s \in l^\times$. □

We are almost ready to express the condition "$T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is a G-torsor on $(Y_l)_{\text{ét}}$" in terms of vector bundles on $\mathbb{P}^1_l$.

Lemma 6.13. *Let $f\colon Y \to X$ be a morphism of schemes, and let G be a finite group acting on Y/X. Then Y is a G-torsor on X if and only if f is flat, surjective, locally of finite presentation, and G acts freely and transitively on geometric fibres.*

Proof. The necessity of the condition is clear. Hence suppose that f is flat, surjective, locally of finite presentation, and G acts freely and transitively on geometric fibres. Then for any geometric point $\overline{x}$ of S, $Y_{\overline{x}}$ is the trivial G-torsor, hence étale. As the property of being étale is fpqc local on the base, it follows that all fibres of f are étale, and since f is flat and locally of finite presentation, it follows that f is finite étale.

Now consider the morphism $\phi\colon G \times Y \to Y \times_X Y$ of finite étale Y-schemes given on the functor of points by $(g, y) \mapsto (gy, y)$, where the occurring schemes are viewed as Y-schemes via the projection on the second coordinate. Then ϕ is itself finite étale surjective, and as $G \times Y$ and $Y \times_X Y$ have the same rank over Y, it follows that ϕ is an isomorphism. After base

change with itself, it admits a section, so as f is finite étale, it also follows that Y is a G-torsor, as desired. □

Lemma 6.14. *Let $f\colon Y \to X$ be a finite étale morphism of schemes of constant rank n, and let G be a finite group of order n acting on Y/X. Then the locus in X where f is a G-torsor is open and closed in X.*

Proof. Consider the locus U in $Y \times_X Y$ on which the morphism $G \times Y \to Y \times_X Y$ given on the functor of points by $(g, y) \mapsto (gy, y)$ is an isomorphism (i.e. where the rank is equal to 1). It is an open and closed subset of $Y \times_X Y$ as this morphism is finite étale. As the rank of f is equal to n, the X-locus where the same morphism is an isomorphism is the image of U in X, and hence is open and closed as well. This locus equals the X-locus where f is a G-torsor, as desired. □

Therefore we have the following.

Corollary 6.15. *Let l be a perfect extension of k. Then the category of finite locally free G-equivariant $\overline{Y_l}$-schemes T such that $T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is a G-torsor on $(Y_l)_{ét}$ is equivalent to the category of finite locally free G-equivariant $\overline{Y_l}$-scheme T such that $T \times_{\mathbb{P}^1_l} (\mathbb{P}^1_l - S_\infty)$ is étale, and such that $T \times_{\mathbb{P}^1_l} 0$ is a G-torsor on $(\overline{Y_l} \times_{\mathbb{P}^1_l} 0)_{ét}$.*

Since in the description of finite locally free $\overline{Y_l}$-schemes T, an $\mathcal{O}(\overline{Y_l} \times_{\mathbb{P}^1_l} 0)$-basis for $\mathcal{O}(T \times_{\mathbb{P}^1_l} 0)$ occurred, in terms of which we can express the condition that $T \times_{\mathbb{P}^1_l} 0$ is a G-torsor on $(\overline{Y_l} \times_{\mathbb{P}^1_l} 0)_{\text{ét}}$.

6.2. Smoothness at ∞. Finally, we consider the condition "T is smooth over l". If $S_\infty = \emptyset$, then this follows automatically from T having to be étale over $\overline{Y_l}$, so assume that $S_\infty = \infty$. As $T \times_{\mathbb{P}^1_l} \mathbb{A}^1_l$ has to be étale over Y_l, it suffices to consider the condition "T is smooth over l at $T \times_{\mathbb{P}^1_l} \infty$".

To this end, assume that we have a scheme S, a positive integer r, and the structure of an algebra $\mathcal{A}$ on $\mathcal{O}_S^r$, given by, for the standard basis $e_1, \ldots, e_r$ on $\mathcal{O}_S^r$, $e_i e_{i'} = \sum_j \mu_{jii'} e_j$ and $1 = \sum_j \epsilon_j e_j$. Then the relative differentials $\Omega_{\mathcal{A}/\mathcal{O}_S}$ over S are generated by the $\mathrm{d}e_j$, with relations $e_{i'}\,\mathrm{d}e_i + e_i\,\mathrm{d}e_{i'} - \sum_j \mu_{jii'}\,\mathrm{d}e_j = 0$ for all i, i' and $\sum_j \epsilon_j\,\mathrm{d}e_j = 0$. Therefore we get a canonical presentation $\omega_{\mathcal{A}/\mathcal{O}_S}\colon \mathcal{A}^{r^2+1} \to \mathcal{A}^r$ of the $\mathcal{A}$-module $\Omega_{\mathcal{A}/\mathcal{O}_S}$, which is compatible with base change.

Proposition 6.16. *Let l be any extension of k. The category of finite locally free $\mathbb{P}^1_l$-schemes T smooth over l at $T \times_{\mathbb{P}^1_l} \infty$ is equivalent to that of finite locally free $\mathbb{P}^1_l$-schemes T, together with morphisms*

$$i\colon \mathcal{O}_{T \times_{\mathbb{P}^1_l} \infty^{(2)}} \to O^{2r}_{T \times_{\mathbb{P}^1_l} \infty^{(2)}}, \qquad j\colon O^{2r}_{T \times_{\mathbb{P}^1_l} \infty^{(2)}} \to O^{(2r)^2+2}_{T \times_{\mathbb{P}^1_l} \infty^{(2)}}$$

of $O_{T\times_{\mathbb{P}^1_l}\infty^{(2)}}$-modules such that the morphism $(\omega_{O_{T\times_{\mathbb{P}^1_l}\infty^{(2)}}/l} \oplus i)j$ is the identity on $O^{2r}_{T\times_{\mathbb{P}^1_l}\infty^{(2)}}$; the morphisms in the latter category are simply the morphisms of $\mathbb{P}^1_l$-schemes.

Proof. We will first show that T is smooth over l at $T\times_{\mathbb{P}^1_l}\infty$ if and only there exist i and j as in the proposition.

Write B for the ring of global sections of $T\times_{\mathbb{P}^1_l}(\mathbb{P}^1_l - 0)$, and note that it is a finite locally free $l[y]$-algebra. Then $T\times_{\mathbb{P}^1_l}\infty^{(2)} = \operatorname{Spec} B/y^2B$. First suppose that there exist morphisms

$$i\colon (B/y^2B) \to (B/y^2B)^{2r}, \qquad j\colon (B/y^2B)^{2r} \to (B/y^2B)^{(2r)^2+2}$$

such that for the canonical presentation

$$\omega_{(B/y^2B)/l}\colon (B/y^2B)^{(2r)^2+1} \to (B/y^2B)^{2r}$$

of $\Omega_{(B/y^2B)/l}$ as a (B/y^2B)-module, we have $(\omega_{(B/y^2B)/l} \oplus i)j = \mathrm{id}$. It immediately follows that $\Omega_{(B/y^2B)/l}$ is generated by one element as B/y^2B-module.

Conversely, if $\Omega_{(B/y^2B)/l}$ is generated by one element, we let i be a morphism from (B/y^2B) to $(B/y^2B)^{2r}$ sending 1 to (a lift of) a generator of $\Omega_{(B/y^2B)/l}$. Hence $(\omega_{(B/y^2B)/l}\oplus i)$ is a surjective morphism to a free B/y^2B-module, so it has a section j, as desired.

It remains to show that $\Omega_{(B/y^2B)/l}$ is generated as a B/y^2B-module by one element if and only if T is smooth over l at all points lying over $\infty \in \mathbb{P}^1_l$. Note that we have an isomorphism

$$\Omega_{B/l}\otimes_B (B/yB) \to \Omega_{(B/y^2B)/l}\otimes_{B/y^2B}(B/yB),$$

and that by Nakayama's lemma, the right hand side (and therefore the left hand side) is generated as a B/yB-module by one element if and only if $\Omega_{(B/y^2B)/l}$ is generated as a B/y^2B-module by one element. Therefore, again by Nakayama's lemma, there exists some $f \in 1 + yB$ such that $\Omega_{B/l}\otimes_B B_f$ is generated as a B_f-module by one element. So the left hand side is a B/yB-module generated by one element if and only if there exists a neighbourhood of $T\times_{\mathbb{P}^1_l}\infty$ that is smooth over l, which holds if and only if T is smooth over l at all points lying over $\infty \in \mathbb{P}^1_l$.

So now we have a forgetful functor from the category of finite locally free $\mathbb{P}^1_l$-schemes T together with morphisms i and j as in the proposition, to that of finite locally free $\mathbb{P}^1_l$-schemes T smooth over l at $T\times_{\mathbb{P}^1_l}\infty$, which is essentially surjective by the above, and fully faithful by construction. □

6.3. Bounds on types. In order to construct a groupoid scheme with the desired properties using the above, we first need to bound the number of possible types.

Lemma 6.17. *Let S be a scheme, let a be a finite sequence of integers, let X be a finite locally free $\mathbb{P}^1_S$-scheme of which the underlying $\mathcal{O}_{\mathbb{P}^1_S}$-modules is standard of type a, and suppose that X has geometrically reduced fibres over S. Then a is non-positive (i.e. all of its elements are non-positive).*

Proof. By taking a geometric fibre if necessary, we assume without loss of generality that S is the spectrum of an algebraically closed field k. Let $X_1, \ldots, X_t$ be the connected components of X. Then there exist finite sequences $a_1, \ldots, a_t$ such that for all i, the algebra $\mathcal{O}_{X_i}$ is of type a_i. These have the property that their concatenation is equal to a up to a permutation. Hence we assume without loss of generality that X is connected. In this case X is a reduced curve over S, so $\mathcal{O}_X(\mathbb{P}^1_S) = \mathcal{O}_X(X) = \mathcal{O}_S(S) = k$, where π is the structure morphism of X, so we deduce that a is non-positive. □

Remark 6.18. Of course, the converse is not true; a counterexample is the $\mathcal{O}_{\mathbb{P}^1_k}$-module $\mathcal{O}_{\mathbb{P}^1_k} \oplus \mathcal{O}_{\mathbb{P}^1_k}(-1)\epsilon$ with multiplication given by $\epsilon^2 = 0$.

In Situation 2.4, let l be a perfect extension of k, and let T be the normal completion of a $j'_!G$-torsor on $(Y_l)_{\text{ét}}$. Let a be the type of $\mathcal{O}_Y$, let b be the type of $\mathcal{O}_T$, and let s, t be their respective lengths. Then by the above, both a and b are non-negative. As the degree of the finite locally free morphism $T \to Y_l$ is equal to $\#G$, we see that $t = s \cdot \#G$. Moreover, if $S_\infty = \emptyset$, then by Corollary 6.10, we have $\sum_j b_j = \#G \cdot \sum_i a_i$; so up to permutation, we only have finitely many possibilities for b. So suppose that $S_\infty = \infty$.

Lemma 6.19. *Let S be a scheme, let a be a finite sequence of integers, and let X be finite locally free $\mathbb{P}^1_S$-scheme such that $\mathcal{O}_X$ is a standard module over S of type a, where a has length s, and such that X is smooth over S. Then X is a family of curves over S of Euler characteristic $s + \sum_i a_i$.*

Proof. It suffices to check this on geometric fibres, so we may assume that S is the spectrum of an algebraically closed field k. Then

$$\begin{aligned}
&\dim_k \mathrm{H}^0(X, \mathcal{O}_X) - \dim_k \mathrm{H}^1(X, \mathcal{O}_X) \\
&\qquad = \dim_k \mathrm{H}^0\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1_k}(a)\right) - \dim_k \mathrm{H}^1\left(\mathbb{P}^1_k, \mathcal{O}_{\mathbb{P}^1_k}(a)\right) \\
&\qquad = \sum_i (1 + a_i) \\
&\qquad = s + \sum_i a_i.
\end{aligned}$$

□

Proposition 6.20. *Let S be a scheme, and let $Y \to X$ be a morphism of finite locally free $\mathbb{P}^1_S$-schemes, with $\mathcal{O}_X$ and $\mathcal{O}_Y$ standard modules over S of respective types a and b, which have respective lengths s, t. Let G be a finite group of order invertible in S acting on Y over X, such that $Y \times_{\mathbb{P}^1_S} \mathbb{A}^1_S$ is a G-torsor over $X \times_{\mathbb{P}^1_S} \mathbb{A}^1_S$. Then*

$$\sum_j b_j \geq \#G \sum_i a_i - \tfrac{1}{2}t.$$

Proof. It suffices to check this on geometric fibres, so we may assume that S is the spectrum of an algebraically closed field k. As G acts transitively on Y over X, and the order of G is invertible in k, it follows that Y is tamely ramified over X. Therefore the ramification degree of Y over X is at most t, as $Y \times_{\mathbb{P}^1_k} \mathbb{A}^1_k$ is étale over $X \times_{\mathbb{P}^1_k} \mathbb{A}^1_k$, and Y has degree t over $\mathbb{P}^1_k$. So by the Riemann–Hurwitz formula, we have

$$-2t - 2\sum_j b_j \leq -2\tfrac{t}{s}s - 2\tfrac{t}{s}\sum_i a_i + t,$$

as desired (note that $t = s \cdot \#G$). □

So therefore, also in the case that $S_\infty = \infty$, we see that there are only finitely many possibilities for the type b of T.

6.4. Complexity. Now we see that, in Situation 2.4, the description of the category of $j_!\mathcal{A}$-torsors on $X_{\text{ét}}$ in terms of vector bundles on $\mathbb{P}^1_k$ gives, for each of the (finitely many) possibilities for the type b, a groupoid scheme $\mathcal{R}_b \rightrightarrows \mathcal{U}_b$ of which $\mathcal{R}_b$ and $\mathcal{U}_b$ are (explicitly given) closed subschemes of some $\mathbb{A}^N_k$. Let $\mathcal{R} = \coprod_b \mathcal{R}_b$ and $\mathcal{U} = \coprod_b \mathcal{U}_b$.

We now have an algorithm which, given Situation 2.4, computes $\mathcal{R}$ and $\mathcal{U}$ simply by writing out all equations attached to the relations occurring in this section. We call this algorithm the *core algorithm*. The remainder of this section will be devoted to bounding the complexity of the core algorithm, or in this case equivalently, the size of the output of this algorithm. We will in the following restrict ourselves to the case in which $S_0 = \{0\}$ and $S_\infty = \{\infty\}$; the bounds we obtain in this case will also hold in the other cases.

Let us start by introducing the parameters in terms of which the complexity bound is computed. Let a be the type of $\overline{Y}$, say of length s, and write $\gamma = \sum_i -a_i$. Note that by Lemma 6.19, $\gamma = s - 1 + p_a(\overline{Y})$, where p_a denote the arithmetic genus. Also note that $\#\Gamma \leq s$, so by Corollary 6.23 below, the number of field elements needed to give Situation 2.4 is polynomial in s, γ, and $\#G$.

Let us now bound the number of possible types b that can occur as the type of an object of $\mathcal{U}$.

Proposition 6.21. *The logarithm of the number of b that can occur as the type of an object of $\mathcal{U}$ is $O\big(s \cdot \#G \log(s\gamma \cdot \#G)\big)$.*

Proof. For convenience, write $N = \lceil \#G(\frac{1}{2}s + \gamma) \rceil$.

By Lemma 6.17, a possible type b must be non-positive. By Proposition 6.20, a possible type b must satisfy $\sum_j -b_j \leq \#G(\frac{1}{2}s+\gamma)$. Such a type corresponds to a unique tuple $(c_0, \ldots, c_N)$ of non-negative integers with $\sum_{k=0}^N c_k = t$ and $\sum_{k=0}^N k c_k \leq N$ by setting c_k to be the number of $-b_j$ equal to k. The number of tuples satisfying the first of these conditions is $\binom{N+t}{t} \leq (N+t)^t$. □

Next, we will bound the size of $\mathcal{R}_b$, i.e. for the given closed immersion $\mathcal{R}_b \to \mathbb{A}_k^N$, the number N, the number of polynomials generating the defining ideal, and the degree of these polynomials. Note that bounds for $\mathcal{R}_b$ will also hold for $\mathcal{U}_b$. To this end, note that we have the following trivial bound.

Lemma 6.22. *Let a and b be finite sequences of non-positive integers, of lengths s and t, respectively. Then* $\dim_k \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{O}_{\mathbb{P}^1_k}(a), \mathcal{O}_{\mathbb{P}^1_k}(b)) \leq st + t\sum_i(-a_i)$.

Corollary 6.23. *Let a be a finite sequence of non-positive integers, of length s. Then*

$$\dim_k \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{O}_{\mathbb{P}^1_k}, \mathcal{O}_{\mathbb{P}^1_k}(a)) \leq s + \sum_i(-a_i)$$

$$\dim_k \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{O}_{\mathbb{P}^1_k}(a), \mathcal{O}_{\mathbb{P}^1_k}(a)) \leq s^2 + s\sum_i(-a_i)$$

$$\dim_k \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{O}_{\mathbb{P}^1_k}(a)^{\otimes 2}, \mathcal{O}_{\mathbb{P}^1_k}(a)) \leq s^3 + 2s^2\sum_i(-a_i)$$

$$\dim_k \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}(\mathcal{O}_{\mathbb{P}^1_k}(a)^{\otimes 3}, \mathcal{O}_{\mathbb{P}^1_k}(a)) \leq s^4 + 3s^3\sum_i(-a_i).$$

Therefore, working out everything, which is straightforward but tedious, gives the following.

Proposition 6.24. *For the given closed immersion $\mathcal{R}_b \to \mathbb{A}_k^N$, we have $N = O(s^4(\#G)^4\gamma)$, its defining ideal is given by $O(s^4(\#G)^4\gamma)$ polynomials, which have degree at most $s \cdot \#G$.*

Note that a polynomial ring in N variables has $\binom{N+d}{d}$ monomials of degree at most d; so by the proposition above, we see that the size of the output is

$$\exp\Big(O\big(s \cdot \#G \log(s\gamma \cdot \#G)\big)\Big).$$

Now that we have bounds for the sizes of $\mathcal{R}$ and $\mathcal{U}$, we now turn to the degrees of the defining polynomials of the morphisms defining the structure of a groupoid scheme.

Recall for this that points of $\mathcal{R}_b$ are given by two objects of $\mathcal{U}_b$, together with an $\mathcal{O}_{\mathbb{P}^1}$-linear map connecting the two objects. So the source and target maps $\mathcal{R}_b \to \mathcal{U}_b$ are induced by projections between their ambient affine spaces. Therefore the affine k-scheme $\mathcal{R}_b \times_{\mathcal{U}_b} \mathcal{R}_b$ of finite type is given by $O(s^4(\#G)^4\gamma)$ variables, $O(s^4(\#G)^4\gamma)$ relations of degree at most $s \cdot \#G$. Moreover, the composition map $\mathcal{R}_b \times_{\mathcal{U}_b} \mathcal{R}_b \to \mathcal{R}_b$ forgets the middle object and composes the two $\mathcal{O}_{\mathbb{P}^1}$-linear maps, so it is given by polynomials of degree at most 2.

Theorem 6.25. *The core algorithm computes the groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ given Situation 2.4 as input, and has arithmetic complexity*

$$\exp\Big(O\big(s \cdot \#G \log(s\gamma \cdot \#G)\big)\Big).$$

Proof. Simply note that every individual coefficient can be computed in arithmetic complexity bounded by a fixed polynomial in $s, \gamma, \#G$. □

7. Connected components of $\mathcal{U}$

Recall the following situation (Situation 2.4).

Situation 7.1. We are given a field k, a finite group Γ, for $p = 0, \infty \in \mathbb{P}^1(k)$, a subset S_p of $\{p\}$, and a diagram

$$\begin{array}{ccccc}
V & \longrightarrow & Y & \longrightarrow & \overline{Y} \\
{\scriptstyle g}\downarrow & & \downarrow & & \downarrow \\
U & \xrightarrow{\ j\ } & X & \longrightarrow & \overline{X} \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{P}^1_k - S_0 - S_\infty & \longrightarrow & \mathbb{P}^1_k - S_\infty & \longrightarrow & \mathbb{P}^1_k
\end{array}$$

in which:

- all squares are cartesian;
- $\overline{X}$ and $\overline{Y}$ are smooth, proper, and finite and generically étale over $\mathbb{P}^1_k$;
- $g\colon V \to U$ is Galois with group Γ.

Moreover, we are given a finite locally constant sheaf $\mathcal{G}$ of groups on U such that $g^{-1}\mathcal{G}$ is constant, and denote by G its group of connected components; the Galois action of Γ on V induces an action of Γ on G by automorphisms.

In Section 6, as the core part of our algorithm, we computed a groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ as a disjoint union of groupoid schemes $\mathcal{R}_b \rightrightarrows \mathcal{U}_b$, and postulated the following properties of it.

- Both morphisms $\mathcal{R} \to \mathcal{U}$ are smooth and have geometrically connected fibres.
- Both $\mathcal{R}$ and $\mathcal{U}$ are affine and of finite type over k.
- There exists a functor from the category $\mathcal{U}(S)$ to the category of $j_!\mathcal{G}|_{U_S}$-torsors, functorial in the k-scheme S, that is an equivalence if S is the spectrum of a perfect field extension of k.

By the construction of Section 6, we see that $\mathcal{R} \rightrightarrows \mathcal{U}$ satisfy the latter two properties. In this section, we will prove the first property, and show that these properties imply that the set $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}})$ of geometric connected components of $\mathcal{U}$ is, as a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set, isomorphic to $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$.

7.1. Smoothness and geometric connectedness of fibres. The first property above will follow from the following.

Proposition 7.2. *Fix a finite sequence b of integers. In Situation 2.4, let $\mathcal{R}_b \rightrightarrows \mathcal{U}_b$ be the groupoid scheme attached to b defined in Section 6.4. Then the two morphisms $\mathcal{R}_b \to \mathcal{U}_b$ are smooth and have geometrically irreducible fibres, and every isomorphism class in $\mathcal{U}_{b,k^{\mathrm{alg}}}$ has the same dimension.*

Proof. Let a be the type of the underlying $\mathbb{P}^1_k$-vector bundle of $\overline{Y}$, and s its length, and let t be the length of b. Denote the morphisms $\mathcal{R}_b \rightrightarrows \mathcal{U}_b$ by α_b, ω_b, with α_b sending a morphism to its source, and with ω_b sending a morphism to its target. For this, it suffices to show that for all $x \in \mathcal{U}_b(k^{\mathrm{alg}})$, the geometric fibre H of α_b above x is irreducible, since the image $\omega_b(H)$ in $\mathcal{U}_{b,k^{\mathrm{alg}}}$ is by definition the isomorphism class of x.

Note that, for any k^{alg}-scheme S, giving an isomorphism with fixed source (say with underlying $\overline{Y}_S$-scheme T) in the groupoid $\mathcal{R}_b(S) \rightrightarrows \mathcal{U}_b(S)$ is, by transport of structure, the same as giving:

- an $\mathcal{O}_{\mathbb{P}^1_S}$-linear automorphism of $\mathcal{O}_{\mathbb{P}^1_S}(b)$;
- an $\mathcal{O}_{\overline{Y}_S \times_{\mathbb{P}^1_S} 0}$-linear automorphism of $\mathcal{O}^{\#A}_{\overline{Y}_S \times_{\mathbb{P}^1_S} 0}$;
- if $S_\infty = \infty$, morphisms

$$i\colon \mathcal{O}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}} \to O^{2\#A}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}}, \qquad j\colon O^{2\#A}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}} \to O^{(2\#A)^2+2}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}}$$

such that $(\omega_{T \times_{\mathbb{P}^1_S} \infty^{(2)}/S} \oplus i)j = \mathrm{id}$.

In case $S_\infty = \emptyset$, we obtain an obvious isomorphism $H \to H_1 \times H_2$, and in case $S_\infty = \{\infty\}$, we obtain an obvious map $H \to H_1 \times H_2 \times H_3$, where

- H_1 is the functor sending a k^{alg}-scheme S to $\mathrm{Aut}_{\mathcal{O}_{\mathbb{P}^1_S}}(\mathcal{O}_{\mathbb{P}^1_S}(b))$;

- H_2 is the functor sending a k^{alg}-scheme S to $\mathrm{Aut}_{\mathcal{O}_{\overline{Y}_S \times_{\mathbb{P}^1_S} 0}}(\mathcal{O}^{\#G}_{\overline{Y}_S \times_{\mathbb{P}^1_S} 0})$;
- H_3 is the functor sending a k^{alg}-scheme S to the subset of

$$\mathrm{Hom}_{\mathcal{O}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}}}(\mathcal{O}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}}, \mathcal{O}^{2 \cdot \#G}_{T \times_{\mathbb{P}^1_S} \infty^{(2)}})$$

of i such that $\omega_{T \times_{\mathbb{P}^1_S} \infty^{(2)}} \oplus i$ is surjective.

First note that using the description of standard modules, we easily see that H_1 is representable by a finite product of factors of the form $\mathbb{G}_{m,k}$ and $\mathbb{A}^1_k$, so therefore by a smooth, irreducible k^{alg}-scheme. Moreover, note that H_2 is isomorphic to the functor sending a k^{alg}-scheme S to $\mathrm{Hom}_S(\overline{Y}_S \times_{\mathbb{P}^1_S} 0, \mathrm{GL}_{\#G,S})$, which, as $\mathcal{O}_{\overline{Y}_S \times_{\mathbb{P}^1_S} 0}$ is finite free over $\mathcal{O}_S$ with a given basis functorial in S, is representable by a non-empty open subscheme of $\mathbb{A}^{s(\#G)^2}_{k^{\mathrm{alg}}}$. Hence H_2 is a smooth, irreducible k^{alg}-scheme as well. Similarly, we see that H_3 is representable by a non-empty open subscheme of $\mathbb{A}^{4t \cdot \#G}_{k^{\mathrm{alg}}}$, and therefore by a smooth, irreducible k^{alg}-scheme.

Finally, we show that H is a smooth, irreducible k^{alg}-scheme. We do this by showing that H is Zariski locally on $H_1 \times H_2 \times H_3$ isomorphic to $H_1 \times H_2 \times H_3 \times \mathbb{A}^N_{k^{\mathrm{alg}}}$ for some fixed N.

First note that we have a morphism $H_3 \to \mathbb{A}^M_{k^{\mathrm{alg}}}$ of k^{alg}-schemes, which is given on the functor of points by sending $i \in H_3(S)$ to the corresponding $4t \cdot \#G \times (2t(2 \cdot \#G)^2 + 4t)$-matrix with coefficients in $\mathcal{O}(S)$, with respect to the basis subordinate to both the standard bases and the given k-basis of $T \times_{\mathbb{P}^1_k} \infty^{(2)}$, so that $M = 4t^2((2 \cdot \#G)^3 + 4 \cdot \#G)$. So let $i \in H_3(k^{\mathrm{alg}})$, and view it as a $4t \cdot \#G \times (2t(2 \cdot \#G)^2 + 4t)$-matrix over k^{alg}. As this matrix corresponds to a surjective map of k^{alg}-vector spaces, there is a $4t \cdot \#G \times 4t \cdot \#G$-minor which is invertible. Let $U \subseteq \mathbb{A}^M_{k^{\mathrm{alg}}}$ be the locus on which this minor is invertible, and let V be the inverse image of U in H_3; V is an open neighbourhood of i.

Now let $j \in H_3(V)$ be the open inclusion. By construction, the kernel of $\omega_{T \times_{\mathbb{P}^1_V} \infty^{(2)}} \oplus j$ is free over $\mathcal{O}_V$. Since an $\mathcal{O}_{T \times_{\mathbb{P}^1_V} \infty^{(2)}}$-linear section of this map is well-defined up to a unique tuple of elements from this kernel, it follows that the inverse image of $H_1 \times H_2 \times V$ in H is isomorphic to $H_1 \times H_2 \times V \times \mathbb{A}^N_{k^{\mathrm{alg}}}$ for some fixed N that is independent of the choices made. Hence H is a smooth, irreducible k^{alg}-scheme, as desired.

Finally note that the dimension of H only depends on the type b, and that the induced morphism $H \to \mathcal{U}_{b,k^{\mathrm{alg}}}$ has finite fibres, so every isomorphism class in $\mathcal{U}_{b,k^{\mathrm{alg}}}$ has the same dimension. □

7.2. Stacks of torsors. We now set out to prove that the three properties mentioned in the introduction of this section imply that the set $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}})$ of geometric connected components of $\mathcal{U}$ is, as a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set, isomorphic to $\mathrm{H}^1(X_{k^{\mathrm{sep}}}, j_!\mathcal{G}|_{U_{k^{\mathrm{sep}}}})$, in a more general setting, which we will formulate in the language of stacks in the next subsection. Before that, in this subsection, we will prove a lemma on the fppf stack of torsors under a finite group that we will need.

Let S be a scheme. A *topologically finite étale* S-scheme T is a morphism $T \to S$ that factors as a composition $T \to T' \to S$ with $T' \to S$ finite étale and $T \to T'$ a universal homeomorphism.

Let $f\colon X \to S$ be a proper smooth curve, let $i\colon Y \to X$ be a closed immersion, topologically finite étale over S, and let $j\colon U \to X$ denote its open complement. Write $h = fi$ and $g = fj$. Let G be a finite group; if Y is non-empty, we also assume that the order of G is invertible on S.

Let $\mathcal{T}$ denote the fppf stack of G-torsors on $U_{\text{ét}}$; i.e. its objects are pairs $(T, \mathcal{F})$ of an S-scheme T and a G-torsor $\mathcal{F}$ on $(U \times_S T)_{\text{ét}}$, and the morphisms $(T, \mathcal{F}) \to (T', \mathcal{F}')$ are the pairs of a morphism $\phi\colon T \to T'$ and an isomorphism $\phi^{-1}\mathcal{F}' \to \mathcal{F}$. We show that $\mathcal{T}$ has a representable and finite étale diagonal, or equivalently, the relevant Isom-sheaves are representable by finite étale schemes.

Without loss of generality, and to ease notation a bit, we will only consider the Isom-sheaves on S. More precisely, let $\mathcal{F}$ and $\mathcal{F}'$ be G-torsors on $U_{\text{ét}}$, and let $\mathcal{I}$ denote the sheaf on $(\mathrm{Sch}/U)_{\mathrm{fppf}}$ sending $\phi\colon T \to U$ to the set $\mathrm{Isom}_T(\phi^{-1}\mathcal{F}, \phi^{-1}F')$ of isomorphisms of G-torsors. We denote by $g_{\mathrm{big},*}$ the big pushforward functor $(\mathrm{Sch}/U)_{\mathrm{fppf}} \to (\mathrm{Sch}/S)_{\mathrm{fppf}}$.

Lemma 7.3. *The sheaf $g_{big,*}\mathcal{I}$ on $(\mathrm{Sch}/S)_{fppf}$ is representable by a finite étale S-scheme.*

Proof. By [23, Tag 0D01, 0D1A], the fppf sheaf $g_{\mathrm{big},*}\mathcal{I}$ is representable by an algebraic space, locally of finite presentation over S, since both $\mathcal{F}$ and $\mathcal{F}'$ are representable by finite étale algebraic spaces over U. Moreover, we easily see that it is formally étale over S, therefore étale over S. Hence it is representable by the espace étalé of $(g_{\mathrm{big},*}\mathcal{I})|_{S_{\text{ét}}} = g_*(\mathcal{I}|_{U_{\text{ét}}})$.

Now we note that $\mathcal{I}|_{U_{\text{ét}}}$ is a G-torsor on $U_{\text{ét}}$, so its pushforward under g is finite locally constant by [13, Exp. XIII; Prop. 1.14, Thm. 2.4]; this uses the additional assumption on the order of G if Y is non-empty. Hence $g_{\mathrm{big},*}\mathcal{I}$ is representable by a finite étale S-scheme. □

In addition, let Γ be a finite group acting on G, and on X over S, such that Y (and therefore U) is stable under Γ, and let $k\colon Z \to U$ be a closed immersion stable under Γ, and let $l\colon V \to U$ be its open complement.

Let $\mathcal{T}'$ denote the fppf stack of Γ-equivariant $l_!G$-torsors on $U_{\text{ét}}$; i.e. its objects are pairs $(T, \mathcal{F})$ of an S-scheme T and a Γ-equivariant $l_!A$-torsor

$\mathcal{F}$ on $(U \times_S T)_{\text{ét}}$, and the morphisms $(T, \mathcal{F}) \to (T', \mathcal{F}')$ are the pairs of a morphism $\phi\colon T \to T'$ and a Γ-equivariant isomorphism $\phi^{-1}\mathcal{F}' \to \mathcal{F}$. We show that $\mathcal{T}'$ too has a representable and finite étale diagonal.

Again, without loss of generality, we will only consider the relevant Isom-sheaves on S. Let $\mathcal{F}$ and $\mathcal{F}'$ be Γ-equivariant $l_!\mathcal{G}$-torsors on $U_{\text{ét}}$, and let $\mathcal{I}'$ denote the sheaf on $(\mathrm{Sch}/U)_{\text{fppf}}$ sending $\phi\colon T \to U$ to the set of Γ-invariant isomorphisms $\phi^{-1}\mathcal{F} \to \phi^{-1}\mathcal{F}'$ of $l_!G$-torsors.

Corollary 7.4. *The sheaf $g_{big,*}\mathcal{I}'$ on $(\mathrm{Sch}/S)_{fppf}$ is representable by a finite étale S-scheme.*

Proof. By the last step in the proof of Lemma 5.10, we see that we can write $g_{\text{big},*}\mathcal{I}'$ as a finite limit of finite étale S-schemes, which therefore is finite étale over S as well. □

7.3. Connected components. We first reformulate the context of the computations of Section 6, using the language of stacks.

Let $\mathcal{T}$ be the stack on $(\mathrm{Sch}\,/X)_{\text{fppf}}$ of $\mathcal{G}$-torsors, resp. the stack on $(\mathrm{Sch}\,/\overline{X})_{\text{fppf}}$ of $j_!\mathcal{G}$-torsors; note that this stack is presented by the groupoid scheme $\mathcal{G} \to X$, resp. $j_!\mathcal{G} \to \overline{X}$. Let f be the structure morphism $X \to \operatorname{Spec} k$, resp. the structure morphism $\overline{X} \to \operatorname{Spec} k$, and let p denote the morphism from the big étale topos to the small étale topos for which p_* is the restriction to the small site. Note that for this p, the functor p^{-1} is the espace étalé functor. Let $f_{\text{big},*}$ and $f_{\text{small},*}$ denote the big and small pushforward, respectively.

We then have a stack $f_{\text{small},*}p_*\mathcal{T} = p_*f_{\text{big},*}\mathcal{T}$ on $(\operatorname{Spec} k)_{\text{ét}}$, to which we can attach the sheaf $\pi_0(f_{\text{small},*}p_*\mathcal{T})$ on $(\operatorname{Spec} k)_{\text{ét}}$, and a morphism $f_{\text{small},*}p_*\mathcal{T} \to \pi_0(f_{\text{small},*}p_*\mathcal{T})$ of stacks on $(\operatorname{Spec} k)_{\text{ét}}$. The Galois set to be computed now corresponds to the sheaf $\pi_0(f_{\text{small},*}p_*\mathcal{T})$ on $(\operatorname{Spec} k)_{\text{ét}}$, or in other words, to the étale k-scheme $p^{-1}\pi_0(f_{\text{small},*}p_*\mathcal{T})$.

In the previous subsection, we have shown that the diagonal of $f_{\text{big},*}\mathcal{T}$ is representable and finite étale, which simply means that for any k-scheme S and any two objects X, Y of $f_{\text{big},*}\mathcal{T}(S)$, the sheaf $\mathrm{Hom}_{f_{\text{big},*}\mathcal{T}(S)}(X, Y)$ on $(\mathrm{Sch}\,/k)_{\text{ét}}$ is representable by a finite étale S-scheme.

In Section 6, we have computed a groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ with $\mathcal{R}$ and $\mathcal{U}$ affine schemes of finite type over k, together with an obvious (non-explicit) morphism $[\mathcal{U}/\mathcal{R}] \to f_{\text{big},*}\mathcal{T}$ of stacks on $(\mathrm{Sch}\,/k)_{\text{ét}}$. There, we also show that $p^{-1}p_*[\mathcal{U}/\mathcal{R}] \to p^{-1}f_{\text{small},*}p_*\mathcal{T}$ is an equivalence (after some purely inseparable base change, but we ignore this technical point for now), and that the morphisms $\mathcal{R} \rightrightarrows \mathcal{U}$ are smooth and have geometrically irreducible fibres.

Hence we are (after some purely inseparable base change) in the situation of the following proposition.

Proposition 7.5. *Let $\mathcal{T}$ be a stack on $(\mathrm{Sch}/k)_{fppf}$ of which the diagonal is representable and finite étale. Let $\mathcal{R} \rightrightarrows \mathcal{U}$ be a groupoid scheme such that both morphisms $\mathcal{R} \to \mathcal{U}$ are smooth and have geometrically connected fibres, and such that $\mathcal{R}$ and $\mathcal{U}$ are of finite type over k. Let $[\mathcal{U}/\mathcal{R}] \to \mathcal{T}$ be a morphism of stacks on $(\mathrm{Sch}/k)_{fppf}$ such that $p^{-1}p_*[\mathcal{U}/\mathcal{R}] \to p^{-1}p_*\mathcal{T}$ is an equivalence, or in other words, such that for each separable extension l/k, the functor $[\mathcal{U}/\mathcal{R}](l) \to \mathcal{T}(l)$ is an equivalence. Then the map $\mathcal{U}(k^{\mathrm{sep}}) \to \pi_0(\mathcal{T})(k^{\mathrm{sep}})$ is a $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant surjection, and factors through an isomorphism $\pi_0(\mathcal{U}) \to \pi_0(\mathcal{T})$.*

If in addition the morphisms $\mathcal{R} \to \mathcal{U}$ have geometrically irreducible fibres, then the connected components of $\mathcal{U}_{k^{\mathrm{sep}}}$ are irreducible.

Proof. First note that the equivalence $p^{-1}p_*[\mathcal{U}/\mathcal{R}] \to p^{-1}p^*\mathcal{T}$ induces a surjective $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant map $U(k^{\mathrm{sep}}) \to \pi_0(\mathcal{T})(k^{\mathrm{sep}})$.

Let $\bar{x} \in \mathcal{U}(k^{\mathrm{sep}})$ and let $j\colon U \to \mathcal{U}_{k^{\mathrm{sep}}}$ be the open immersion of the connected component U containing $\bar{x}$ into $\mathcal{U}_{k^{\mathrm{sep}}}$. Moreover, let $f\colon U \to \operatorname{Spec} k^{\mathrm{sep}}$ denote the structure morphism, and let $p\colon \mathcal{U}_{k^{\mathrm{sep}}} \to \mathcal{U}$ be the projection morphism. Let $\mathcal{Y} \in \mathcal{U}(\mathcal{U})$ denote the "universal object"; i.e. the object corresponding to the identity map on $\mathcal{U}$.

Define $Y_1 = j^{-1}p^{-1}\mathcal{Y}, Y_2 = f^{-1}\bar{x}^{-1}\mathcal{Y} \in \mathcal{U}(U)$, and consider their images in $\operatorname{Ob}\mathcal{T}(U)$. Then $\mathrm{Isom}_{\mathcal{T}(U)}(Y_1, Y_2)$ is representable by a finite étale U-scheme by assumption.

Moreover, it is surjective as by construction $\mathrm{Hom}_{\mathcal{T}(U)}(Y_1, Y_2)(\bar{x})$ is non-empty and U is connected. Hence for any point $\overline{x'} \in \mathcal{U}(k^{\mathrm{sep}})$, the set $\mathrm{Hom}_{\mathcal{T}(U)}(Y_1, Y_2)(\overline{x'})$ is non-empty as well. Therefore we see that the morphism $\mathcal{U}(k^{\mathrm{sep}}) \to \pi_0(\mathcal{T})(k^{\mathrm{sep}})$ factors through a surjective $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant map $\pi_0(\mathcal{U})(k^{\mathrm{sep}}) \to \pi_0(\mathcal{T})(k^{\mathrm{sep}})$. In other words, the morphism $\pi_0(\mathcal{U}) \to \pi_0(\mathcal{T})$ of sheaves on $(\operatorname{Spec} k)_{\text{ét}}$ is surjective.

Denote the morphisms $\mathcal{R} \to \mathcal{U}$ by α and ω. As α and ω have geometrically connected fibres, it follows that the morphism $\pi_0(\mathcal{U}) \to \pi_0(\mathcal{T})$ is an isomorphism; if $\bar{x}, \bar{x}' \in \mathcal{U}(k^{\mathrm{sep}})$ are isomorphic, then $\bar{x}' \in \alpha(\omega^{-1}(\bar{x}))$, hence $\bar{x}, \bar{x}'$ lie in the same geometric connected component of $\mathcal{U}$.

Finally, if α and ω have geometrically irreducible fibres, then the same argument implies that every geometric connected component of $\mathcal{U}$ is irreducible. □

As a corollary, we see that in Proposition 7.5 any set X of points $\operatorname{Spec} l_i \to \mathcal{U}$ (with l_i/k finite algebraic) such that every connected component of $\mathcal{U}$ contains a point X induces a finite cover of $\pi_0(\mathcal{T})$. We describe in Section 8 how to use such a set X to compute $\pi_0(\mathcal{T})$.

Corollary 7.6. *There is a canonical bijection from $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}})$ to the set of isomorphism classes of $\mathcal{G}$-torsors on $X_{k^{\mathrm{sep}}}$. Moreover, all $\mathcal{U}_b$ are equidimensional.*

8. Geometric points and first cohomology

Next, we will use the groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ to compute $\mathrm{H}^1(X_{\text{ét}}, j_!\mathcal{G})$. We will do this in a slightly more general situation, namely the following (compare with the conditions of Proposition 7.5).

Situation 8.1. Let k be a field, let $\mathcal{R} \rightrightarrows \mathcal{U}$ be a groupoid scheme in which the morphisms $\mathcal{R} \to \mathcal{U}$ are smooth with geometrically irreducible fibres, and with $\mathcal{R}$,$\mathcal{U}$ affine and equidimensional, given by at most r polynomials (which are of degree at most d) in at most N variables. Let $\mathcal{T}$ be a stack on $(\mathrm{Sch}\,/k)_{\text{fppf}}$ with representable and finite étale diagonal, and let $[\mathcal{U}/\mathcal{R}] \to \mathcal{T}$ be a morphism such that $p^{-1}p_*[\mathcal{U}_{k^{\mathrm{perf}}}/\mathcal{R}_{k^{\mathrm{perf}}}] \to p^{-1}p_*\mathcal{T}_{k^{\mathrm{perf}}}$ is an equivalence. Here, for any field k, $p\colon (\mathrm{Sch}\,/k)_{\text{fppf}} \to (\mathrm{Spec}\,k)_{\text{ét}}$ denotes the change-of-site morphism for which p_* is the restriction.

Let us, for a finite reduced k-algebra A, denote by $A^\dagger$ the separable closure of k in A. Moreover, if A is a finite product $\prod_i k_i$ of fields, denote by A^{perf} the product $\prod_i k_i^{\mathrm{perf}}$. Suppose we are in Situation 8.1. Then to any morphism $x\colon \mathrm{Spec}\,l \to \mathcal{U}$ with l/k finite, we can attach an induced morphism $\mathrm{Spec}\,l^{\mathrm{perf}} \to \mathcal{U}$. This in turn induces a morphism $\mathrm{Spec}\,l^{\mathrm{perf}} \to p^{-1}p_*\mathcal{T}_{k^{\mathrm{perf}}}$, which is étale as both $\mathrm{Spec}\,l^{\mathrm{perf}}$ and $p^{-1}p_*\mathcal{T}_{k^{\mathrm{perf}}}$ are étale over $\mathrm{Spec}\,k^{\mathrm{perf}}$. We hence get a morphism $\mathrm{Spec}\,l^\dagger \to p^{-1}p_*\mathcal{T}$.

We prove a couple of lemmas regarding this construction.

Lemma 8.2. *In Situation 8.1, let $\{x_i\colon \mathrm{Spec}\,l_i \to \mathcal{U}\}$ be a family of points on $\mathcal{U}$. Then the image of $\coprod_i \mathrm{Spec}\,l_i \to \mathcal{U}$ intersects every geometric connected component of $\mathcal{U}$ if and only if $\coprod_i \mathrm{Spec}\,l_i^\dagger \to p^{-1}p_*\mathcal{T}$ is surjective.*

Proof. We note that the image of $\coprod_i \mathrm{Spec}\,l_i \to \mathcal{U}$ intersects every geometric connected component if and only if the image of $\coprod_i \mathrm{Spec}\,l_i^{\mathrm{perf}} \to \mathcal{U}$ does so. This is equivalent to $\coprod_i \mathrm{Spec}\,l_i^{\mathrm{perf}} \to p^{-1}p_*\mathcal{T}_{k^{\mathrm{perf}}}$ being surjective, i.e. to $\coprod_i \mathrm{Spec}\,l_i^\dagger \to p^{-1}p_*\mathcal{T}$ being surjective. □

Lemma 8.3. *In Situation 8.1, let $x\colon \mathrm{Spec}\,l \to \mathcal{U}$ and $y\colon \mathrm{Spec}\,m \to \mathcal{U}$ be two points on $\mathcal{U}$. Let A be the coordinate ring of $\alpha^{-1}x \times_{\mathcal{R}} \omega^{-1}y$. Then $A^\dagger$ is the coordinate ring of $\mathrm{Spec}\,l \times_{p^{-1}p_*\mathcal{T}} \mathrm{Spec}\,m$.*

Proof. Let $x'\colon \mathrm{Spec}\,l^{\mathrm{perf}} \to \mathcal{U}$ and $y'\colon \mathrm{Spec}\,m^{\mathrm{perf}} \to \mathcal{U}$. Then A^{perf} is the coordinate ring of $\alpha^{-1}x' \times_{\mathcal{R}} \omega^{-1}y' = \mathrm{Spec}\,l^{\mathrm{perf}} \times_{p^{-1}p_*\mathcal{T}_{k^{\mathrm{perf}}}} \mathrm{Spec}\,m^{\mathrm{perf}}$, so $A^\dagger$ is the coordinate ring of $\mathrm{Spec}\,l^\dagger \times_{p^{-1}p_*\mathcal{T}} \mathrm{Spec}\,m^\dagger$, being the unique finite k-subalgebra of A^{perf} of which the base change to k^{perf} is A^{perf}. □

So in Situation 8.1, by finding enough points on $\mathcal{U}$, one can construct a presentation of the stack $p^{-1}p_*\mathcal{T}$, which then can be used to compute π_0 of this. Let us do so explicitly below.

Proposition 8.4. *Algorithm 8.5 takes as input Situation 8.1 and computes a finite set X of morphisms $x_i\colon \operatorname{Spec} l_i \to \mathcal{U}$ with l_i/k finite, such that the induced map $\coprod_i \operatorname{Spec} l_i \to \pi_0(p_*\mathcal{T})$ is surjective. Moreover, it does so in arithmetic complexity*

$$\exp\Big(O(N^2\log(d), eN\log(d), \log(r))\Big)$$

Algorithm 8.5. Compute a Noether normalisation $\nu\colon \mathcal{U} \to \mathbb{A}^{\dim \mathcal{U}}$ using e.g. [7, §1]. Note that this also works for finite fields, but only after a base change to a finite field extension; so for finite fields, one needs to keep track of the Galois action as well.

Then set $R = \mathcal{O}(\nu^{-1}(0))$. Compute a k-basis for R using a Gröbner basis computation for the ideal defining R. Compute the primary decomposition of R and for each local factor S of R, compute the composition of $\mathcal{O}(\mathcal{U}) \to R$, $R \to S$, and $S \to S^{\mathrm{red}}$.

Proof. First note that, as $\mathcal{U}$ is equidimensional, every geometric connected component maps surjectively to $\mathbb{A}^{\dim \mathcal{U}}$. Hence R is the ring of global sections of a closed subscheme of $\mathcal{U}$ that intersects every geometric connected component, so this procedure indeed computes a set X as desired. It remains to prove the claims on the arithmetic complexity.

By [7, §1; §3] (for Noether normalisation and the zero-dimensional Gröbner basis computation, respectively), R can be computed as finite k-algebras in arithmetic complexity

$$\exp\Big(O(N^2\log(d), \log(r))\Big).$$

Let us bound the k-vector space dimension of the R. First note that $\mathcal{U} \leq N$. Therefore R is given by at most N generators, and by relations that are of degree at most d. Hence

$$\dim_k R = \exp\Big(O(N\log(d))\Big).$$

So by the methods of [18, §7], we see that the primary decomposition of R can be computed in arithmetic complexity

$$\exp\Big(O(N\log(d))\Big).$$

Moreover, for each of the local factors, the degree of the purely inseparable extension l/k to be taken doesn't exceed $(\dim_k R)^e$, as the degree of the polynomials to be factored doesn't exceed $\dim_k R$. It then follows by that the maps $R \to S^{\mathrm{red}}$ can be computed in arithmetic complexity

$$\exp\Big(O((e+1)N\log(d))\Big).$$

as $\dim_k(S \otimes_k l) \leq (\dim_k R)^{e+1}$. □

Proposition 8.6. *Algorithm 8.7 takes as input Situation 8.1,* $x\colon \operatorname{Spec} l \to \mathcal{U}$*, and* $y\colon \operatorname{Spec} m \to \mathcal{U}$ *and computes the finite* k*-scheme* $\alpha^{-1}x \times_{\mathcal{R}} \omega^{-1}y$ *in arithmetic complexity*

$$\exp\Big(O\big(N_{x,y}^2 \log(d_{x,y}), \log(r)\big)\Big),$$

where $N_{x,y} = \max(N, \log[l:k], \log[m:k])$ *and* $d_{x,y} = \max(d, [l:k], [m:k])$.

Algorithm 8.7. We first compute for l and m a "small" set of generators. Start by setting $X = F = \emptyset$. For s in a k-basis for l, compute $k[X][s] \subseteq l$ and the minimal polynomial f of s over $k[X] \subseteq l$, and then, if f is linear, do nothing, otherwise add s to X and f to F. Write $l = k[X]/(F)$ afterwards, and repeat this for m.

Now compute x, y in terms of the "small" descriptions of l and m obtained above, and compute $\alpha^{-1}x \times_{\mathcal{R}} \omega^{-1}y$. Finally, compute a k-basis for its coordinate ring via Gröbner bases, and the unit and multiplication table with respect to this basis.

Proof. Note that in the first step, we write l (resp. m) using $O(\log[l:k])$ (resp. $O(\log[m:k])$) generators and relations, of degree at most $[l:k]$ (resp. $[m:k]$). Moreover, $\mathcal{U}$ and $\mathcal{R}$ are given by at most N generators and r relations, of degree at most d. Therefore $\alpha^{-1}x \times_{\mathcal{R}} \omega^{-1}y$ is given by $O\big(\log[l:k], \log[m:k], N\big)$ generators, $O\big(\log[l:k], \log[m:k], N, r\big)$ relations, of degree at most $\max\big([l:k], [m:k], d\big)$. Hence the arithmetic complexity follows from [7, §3] in the same way as before. □

As a corollary, using Lemma 8.2 and Lemma 8.3, we have the following.

Corollary 8.8. *There exists an algorithm that takes Situation 8.1 as input and computes a diagram*

$$\begin{array}{ccc} Y^\dagger & \rightrightarrows & X^\dagger \\ & & \uparrow \\ & & X \\ & & \downarrow \\ & & \mathcal{U} \end{array}$$

with $X^\dagger, Y^\dagger$ *finite étale over* k*,* $Y^\dagger \rightrightarrows X^\dagger$ *a presentation for* $p^{-1}p_*\mathcal{T}$*,* $X \to X^\dagger$ *a finite purely inseparable morphism between finite* k*-schemes, and* $X \to \mathcal{U}$ *having image intersecting every geometric connected component of* $\mathcal{U}$*, in arithmetic complexity*

$$\exp\Big(O\big((e+1)N^3 \log(d)^3, \log(r)\big)\Big).$$

In the corollary above, we can assume that if U, V are two distinct connected components of $X^\dagger$, then $\alpha^{-1}U \times_{Y^\dagger} \omega^{-1}V$ is empty, since whenever we encounter distinct connected components U, V for which $\alpha^{-1}U \times_{Y^\dagger} \omega^{-1}V$ is not empty, then we may simply omit one of U, V. It follows that the groupoid scheme $Y^\dagger \rightrightarrows X^\dagger$ is a finite disjoint union of groupoid schemes $Y_i^\dagger \rightrightarrows X_i^\dagger$ with finite étale arrows in which each X_i is the spectrum of a finite separable field extension of k. Therefore the problem of computing $\pi_0(p^{-1}p_*\mathcal{T})$ reduces to computing π_0 of each of these groupoid schemes.

The following lemma suggests how to compute π_0 in this case.

Lemma 8.9. *Let S be a connected scheme, and let $Y \rightrightarrows X$ be groupoid scheme over S with X and Y finite étale S-schemes. Then the image R of $Y \to X \times_S X$ is an étale equivalence relation on X, and $\pi_0([X/Y]) = X/R$.*

Proof. This is trivial once we view X and Y as finite $\pi_1(S)$-sets. □

Corollary 8.10. *Algorithm 8.11 takes a groupoid scheme $Y \rightrightarrows X$ over k with X and Y finite étale k-schemes, and outputs $\pi_0([X/Y])$ in arithmetic complexity polynomial in the degrees of X and Y over k.*

Algorithm 8.11. Let l, B be the respective coordinate rings of X, Y, and let $A = l \otimes_k l$. Let $A = \prod_i A_i$ be the primary decomposition of A; since A is separable over k, all A_i are fields.

Compute the morphism $A \to B$, and compute the set I of indices i for which the induced map $A_i \to B$ is non-zero. Set $A_I = \prod_{i \in I} A_i$. Compute the morphisms $l \to A_I$ sending $s \in l$ to $s \otimes 1$ and $1 \otimes s$, respectively, and return their equaliser k'.

Proof. Note that, since $\operatorname{Spec} A_I$ is the image of Y in $X \times_{\operatorname{Spec} k} X$ by construction, $\operatorname{Spec} k'$ is the coequaliser of the two morphisms $\operatorname{Spec} A_I \to X$ constructed, in other words, it is the quotient of X by the étale equivalence relation $\operatorname{Spec} A_i$ on X, as desired. □

Applying the above to the groupoid scheme obtained in Section 6, we get the following.

Corollary 8.12. *There exists an algorithm that takes as input Situation 2.4 and computes a finite étale k-scheme representing $\mathrm{H}^1(X_{k^{\mathrm{sep}},ét}, j_!\mathcal{G})$ in arithmetic complexity*

$$\exp\Big(O\big((e+1)s^{12}(\#G)^{12}\gamma^3 \log(s \cdot \#G)^3\big)\Big).$$

In order to be able to compute additional structures on $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!\mathcal{G})$, it will turn out to be useful to compute this set as a finite $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set, together with some additional structure. The first step in this is to compute a finite Galois extension l/k such that the Galois action on $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!\mathcal{G})$ factors through $\mathrm{Gal}(l/k)$. This is done in the standard recursive way.

Lemma 8.13. *Algorithm 8.14 takes as input a finite separable k-algebra A, and computes the minimal Galois extension l/k such that $A\otimes_k l$ is a product of copies of l, in arithmetic complexity polynomial in* $(\dim_k A)!$. *If* $\operatorname{Spec} A$ *is the underlying scheme of a group scheme over k, then the arithmetic complexity is*

$$\exp\Big(O\big(\log(\dim_k A)^2\big)\Big).$$

Algorithm 8.14. Set $A' = A$, and compute a primary decomposition $A' = \prod_i A'_i$. Set $l = k$. While the number of factors is not $\dim_k A$, choose A'_i of maximal dimension, and set $A' = A' \otimes_l A'_i$, $l = A'_i$, and compute a primary decomposition $A' = \prod_i A'_i$. Return l.

Corollary 8.15. *There exists an algorithm that takes as input a finite separable k-algebra A, and computes the corresponding finite* $\operatorname{Gal}(k^{\mathrm{sep}}/k)$*-set in arithmetic complexity polynomial in* $(\dim_k A)!$ *(or*

$$\exp\Big(O\big(\log(\dim_k A)^2\big)\Big)$$

if $\operatorname{Spec} A$ *is the underlying scheme of a group scheme over k).*

Now by base change to l, we get the following.

Corollary 8.16. *There exists an algorithm that takes as input Situation 2.4 and computes:*

- *a finite Galois extension l/k such that the* $\operatorname{Gal}(k^{\mathrm{sep}}/k)$*-action on the finite set* $\mathrm{H}^1(X_{k^{\mathrm{sep}},\acute{e}t}, j_!\mathcal{G})$ *factors through* $\operatorname{Gal}(l/k)$*,*
- *the finite* $\operatorname{Gal}(l/k)$*-set* $\mathrm{H}^1(X_{k^{\mathrm{sep}},\acute{e}t}, j_!\mathcal{G})$*,*
- *for each $h \in \mathrm{H}^1(X_{k^{\mathrm{sep}},\acute{e}t}, j_!\mathcal{G})$, a finite extension l_h/l and a morphism* $\operatorname{Spec} l_h \to \mathcal{U}$ *representing h,*

in arithmetic complexity

$$\exp\Big(O\big((e+1)s^{12}(\#G)^{12}\gamma^3\log(s\cdot\#G)^3, (e+1)\log[l:k]\big)\Big).$$

9. Reductions and applications

In the previous sections, we assumed normal proper curves to be presented as finite locally free $\mathbb{P}^1_k$-schemes as described in Section 4. Alternatively, normal proper connected curves can be presented using their function fields, as a finite extension of $k(x)$, and in this case, we will present morphisms between normal proper connected curves by morphisms between their function fields.

Passing from the presentation as finite locally free $\mathbb{P}^1_k$-scheme to that as a finite extension of $k(x)$ is simple: given a finite locally free $\mathbb{P}^1_k$-scheme X with type a of length s, one can compute the finite $k(x)$-algebra $k(X)$ corresponding to it in arithmetic complexity polynomial in s and $\sum_i -a_i$, simply

by, in the conventions of Section 4, substituting $y = 1$ in the multiplication table and unit defining $\mathcal{O}_X$; this computation is functorial in X.

Conversely, given a finite field extension A of $k(x)$ of degree d defined by elements of height at most h, one can compute $\alpha_1, \ldots, \alpha_n \in A$ such that $A = k(x, \alpha_1, \ldots, \alpha_n)$, and, for all i, minimal polynomials for α_{i+1} over $k(x, \alpha_1, \ldots, \alpha_i)$ in arithmetic complexity polynomial in d, h, using the methods of [1]; note that $n \leq \log_2 d$, and the minimal polynomials have degree at most d, and their coefficients have height at most d^3h. By multiplying by suitable polynomials in $k[x]$, one can make each α_{i+1} have a minimal polynomial of which the coefficients lie in $k[x, \alpha_1, \ldots, \alpha_i]$, in arithmetic complexity polynomial in d, h; the minimal polynomials in this case will have x-degree at most d^5h. Therefore we obtain a $k[x]$-order in A consisting of products of the α_i. Similarly, we can compute a $k[x^{-1}]$-order in A, in arithmetic complexity polynomial in d and h.

Then, by [8, §2.7] (which we can apply since we are able to compute nilradicals of finite k-algebras) one can compute the corresponding maximal orders over $k[x]$ and $k[x^{-1}]$ in arithmetic complexity polynomial in d^{e+1} and h. Moreover, they define the same $k[x, x^{-1}]$-submodule of A, so it follows from [11, Lem. 11.50] that one can compute a sequence (a_i) of integers, and bases (b_i) and (c_i) of the respective maximal orders such that $b_i = x^{a_i} c_i$ for all i, and therefore a presentation of the normal proper connected curve as a finite locally free $\mathbb{P}^1_k$-scheme, in arithmetic complexity polynomial in d^{e+1} and h as well.

In fact, as the computation of nilradicals of finite k-algebras as described in Section 3 proceeds by first computing the nilradical of the base change to k^{perf}, it follows that one can compute a purely inseparable extension l of k and a *smooth* proper connected curve with function field $k(x)l$ in arithmetic complexity polynomial in d^{e+1} and h; we will refer to this as the construction of a *smooth completion*.

As for functoriality, given a morphism $K \to L$ of function fields, with K given as a finite $k(x)$-algebra, and L as a finite $k(y)$-algebra, one can compute a $k(x)$-basis of L (and therefore a K-basis of L) by successively computing a $k(x)$-basis of $k(x, y)$ and a $k(x, y)$-basis of L; with respect to this $k(x)$-basis of L, the computation given above is functorial.

Remark 9.1. The above gives us an algorithm for the computation of the normalisation (over k and over k^{perf}) of a finite locally free $\mathbb{P}^1_k$-scheme of type a of length s, in arithmetic complexity polynomial in s^{e+1} and $\sum_i -a_i$; for the type a' (of length s') of the resulting normal proper curve, we have $s = s'$ and $\sum_i -a'_i \leq \sum_i -a_i$.

To present divisors on proper normal curves, we will mainly use the so-called *free ideal presentation*. Roughly speaking, in this presentation, divisors on a proper normal curve X are given as formal sums of closed

points of X, which in turn are given by maximal ideals of $\mathcal{O}_X$. For more details on this and other related presentations, see e.g. [15], or [8, Ch. 2] for a more detailed exposition. For the purposes of this paper, we simply note that we can compute images and pre-images of closed points of a morphism of proper normal curves in arithmetic complexity polynomial in the size of the input.

Now an arbitrary normal curve X will be presented by the product of the function fields of its connected components, and the finite complement of X in its normal completion $\overline{X}$; as a measure for the size of an affine curve, we take the $k(x)$-degree of the corresponding $k(x)$-algebra, an upper bound h for the height of the elements of $k(x)$ defining this algebra, the number of closed points in $\overline{X} - X$, and the maximum degree of these closed points over k. Morphisms $Y \to X$ between normal curves will be presented by morphisms between their normal completions, such that for every closed point in the complement of X in $\overline{X}$ there is a closed point of Y in $\overline{Y}$ lying over it.

9.1. Topological invariance of the small étale site. In our reduction to Situation 2.4, we will make use of finite locally free, purely inseparable morphisms between normal proper curves and the *topological invariance of the small étale site*, which states that for a universal homeomorphism $f\colon Y \to X$, the functors f_* and f^{-1} are quasi-inverse functors between $\mathrm{Sh}(X_{\text{ét}})$ and $\mathrm{Sh}(Y_{\text{ét}})$. Given a finite locally free, purely inseparable morphism $f\colon Y \to X$ between normal proper connected curves, we will make this explicit for étale sheaves representable by étale separated X-schemes (resp. Y-schemes), i.e. by normal curves.

For $\mathcal{F}$ an étale sheaf representable by an étale and separated X-scheme, the pullback is simply $Y \times_X \mathcal{F}$, which clearly can be computed in arithmetic complexity polynomial in the size of the input.

Proposition 9.2. *Algorithm 9.3 takes a finite locally free, purely inseparable morphism $f\colon Y \to X$ between normal proper connected curves, and a normal curve $\mathcal{F}$, étale over Y, and computes $f_*\mathcal{F}$, in arithmetic complexity polynomial in the size of the input.*

Algorithm 9.3. Write K, L, for the function fields of X, Y, respectively, let $\mathcal{F}$ be an étale and separated Y-scheme (with normal completion $\overline{\mathcal{F}}$), and let B denote its corresponding L-algebra. Let A be the Weil restriction of B from L to K. Compute the L-algebra isomorphism $A \otimes_K L \to B$, and therefore a morphism $A \to B$. Let $\overline{\mathcal{F}}'$ denote the corresponding normal proper curve, and $\overline{\mathcal{F}} \to \overline{\mathcal{F}}'$ be the corresponding morphism. Output $\overline{\mathcal{F}}'$ together with the image of the complement of $\mathcal{F}$ in $\overline{\mathcal{F}}$.

Proof. The output is correct since the output $\mathcal{F}'$ needs to satisfy $\mathcal{F}' \times_X Y = \mathcal{F}$, and since taking Weil restrictions sends finite separable L-algebras to finite separable K-algebras, and is left adjoint to base changing from K to L. □

9.2. Presentation of torsors. In Section 9 we have given the complexity of our algorithm computing the first cohomology as a Galois-*set*. In case the input group sheaf is abelian, the first cohomology also has the structure of an abelian group. In this subsection, we explain how to compute this structure. So write in Situation 2.4 $\mathcal{A} = \mathcal{G}$ and $A = G$, which are both abelian.

Note that in Situation 2.4, we have a second presentation of a $j_!\mathcal{A}$-torsor on $X_{k^{\mathrm{sep}},\text{ét}}$ (the first being as a geometric point on the groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ constructed in the previous section). First, any $j_!\mathcal{A}$-torsor is representable by an étale separated X-scheme and therefore by a normal curve, so we can present a $j_!\mathcal{A}$-torsor T by a normal curve together with the group action $j_!\mathcal{A} \times_X T \to T$. In fact, $j_!\mathcal{A}$ is representable by the disjoint union of X (acting as the zero section) and $\mathcal{A} - 1$ (which is finite étale over U). We indicate how to pass between these presentations.

Starting with $x \in \mathcal{U}(l)$, we let k' be the separable closure of k in l. Note that x defines a Γ-equivariant A-torsor $\overline{T}$ on $\overline{Y}_{l,\text{ét}}$ together with a Γ-equivariant section $\overline{Y} \times_{\mathbb{P}^1_k} S_0 \to \overline{T}$. Using the function field presentations, one can then compute quotients under Γ using linear algebra, which gives us a $j_!\mathcal{A}$-torsor T on $X_{l,\text{ét}}$. Therefore we can compute the corresponding $j_!\mathcal{A}$-torsor on $X_{k',\text{ét}}$ in arithmetic complexity polynomial in $s^{e+1}, (\#A)^{e+1}, \gamma^{e+1}, [l:k]^{e+1}$.

Conversely, let T be a $j_!\mathcal{A}$-torsor on $X_{k',\text{ét}}$ with k'/k separable. Pull T back to a Γ-equivariant G-torsor on $Y_{k',\text{ét}}$, together with Γ-equivariant section $Y_{k'} \times_{\mathbb{P}^1_k} S_0 \to Y_{k'}$, and compute a smooth completion. Now some linear algebra suffices to compute the additional data (see Section 6.1 and Section 6.2) required to obtain a point of $\mathcal{U}(k^{\mathrm{alg}})$ in arithmetic complexity polynomial in $s^{e+1}, (\#A)^{e+1}, \gamma^{e+1}, [k':k]^{e+1}$.

Therefore, using this, Corollary 8.16 and Proposition 8.6, we have the following.

Corollary 9.4. *Algorithm 9.5 takes as input Situation 2.4 (but with $\mathcal{A} = \mathcal{G}$ a sheaf of abelian groups, so that $A = G$ is abelian) and computes the* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-module* $\mathrm{H}^1(X_{k^{\mathrm{sep}},ét}, j_!\mathcal{A})$ *in arithmetic complexity*

$$\exp\Big(O((e+1)^3 s^{16} (\#A)^{16} \gamma^4 \log(s\#A)^3)\Big).$$

Algorithm 9.5. It remains to compute addition of classes of $j_!\mathcal{A}$-torsors on $X_{k^{\mathrm{sep}},\text{ét}}$. For this, it suffices to note that if T_1, T_2 are $j_!\mathcal{A}$-torsors on $X_{k',\text{ét}}$ with k'/k separable, then the sum of the classes of T_1 and T_2 in

$\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!\mathcal{A})$ is given by the quotient of $T_1 \times_{X_{k'}} T_2$ by the $j_!\mathcal{A}$-action given by $a(t_1, t_2) = (at_1, a^{-1}t_2)$; compute this using linear algebra over $k'(x)$, and find the element in $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!\mathcal{A})$ isomorphic to it using Algorithm 8.7.

Proof. It remains to find an upper bound for $\log[l : k]$. Note that the cardinality of the set $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!\mathcal{A})$ is

$$\exp\Big(O\big(s^8(\#A)^8\gamma^2\log(s\#A), es^4(\#A)^4\gamma\log(s\#A)\big)\Big)$$

by Proposition 8.4. As this set is an abelian group, it follows that

$$\log[l : k] = O\big((e+1)^2 s^{16}(\#A)^{16}\gamma^4\log(s\#A)^2\big),$$

from which the arithmetic complexity follows. □

9.3. Reduction to Situation 2.4. We will now indicate how to reduce to Situation 2.4 for "most" smooth connected curves X over k, non-empty open subschemes U of X, and finite locally constant sheaves $\mathcal{A}$ on $U_{\text{ét}}$. We would like to use explicit computation of Riemann–Roch spaces as in [15] to compute a suitable cover of X over $\mathbb{P}^1_k$, however, this requires the curve to be given as a generically étale finite locally free $\mathbb{P}^1_k$-scheme (or equivalently, a separating element for the function field of X must be given).

Proposition 9.6. *Algorithm 9.7 takes as input a normal proper connected curve X over k of type a, and computes a finite purely inseparable extension l/k, a finite locally free purely inseparable morphism $X' \to X$ of degree at most $[X : \mathbb{P}^1_k]^{e+2}$, and a generically étale finite locally free morphism $X' \to \mathbb{P}^1_l$ of degree at most $[X : \mathbb{P}^1_k]$, in arithmetic complexity polynomial in $\sum_i -a_i$ and $[X : \mathbb{P}^1_k]^{e+2}$.*

Algorithm 9.7. By computing the separable closure K' of $k(x)$ in K, compute the minimal p-power q such that $f^q \in K'$ for all $f \in K$. Let $L = K \cdot k^{1/q}(x^{1/q})$, which is the reduction of $K \otimes_{k(x)} k^{1/q}(x^{1/q})$, and output $l = k^{1/q}$ and $x^{1/q}$, together with a K-basis of L.

Proof. We note that q is bounded from above by $[K : k(x)]$, and that therefore L can be computed in arithmetic complexity polynomial in $\sum_i -a_i$ and $[K : k(x)]^{e+2}$. □

Proposition 9.8. *Algorithm 9.9 takes as input a smooth connected curve X generically étale over $\mathbb{P}^1_k$, given by its normal completion $\overline{X}$, a finite set $\{Q_1, \dots, Q_t\}$ of closed points of $\overline{X}$, and an open immersion $j\colon U \to X$, given by a finite set $\{P_1, \dots, P_s\}$ of closed points of X, and computes a finite locally free morphism $\pi\colon X \to \mathbb{P}^1_k$ with $\pi^{-1}(\infty) = \{Q_1, \dots, Q_t\}$ and $\pi^{-1}(0) \supseteq \{P_1, \dots, P_s\}$ in arithmetic complexity polynomial in the size of the input.*

Algorithm 9.9. Write $Z_0 = \sum_{i=1}^{s} P_i$, $Z_\infty = \sum_{j=1}^{t} Q_j$, and let g be the genus of X. Let m be the smallest integer such that $m(t-1) - s > 2g - 2$ and $2^m > t$. Using [15], compute a k-basis B for $\mathcal{O}_X(-Z_0 + mZ_\infty)$, and compute the subspaces $\mathcal{O}_X(-Z_0 + mZ_\infty - mQ_j)$ for $j = 1, \ldots, t$. Find a linear combination $f = \sum_{b \in B} \epsilon_b b$ with $\epsilon_b \in \{0, 1\}$ for all $b \in B$ such that f is not in any of the $\mathcal{O}_X(-Z_0 + mZ_\infty - mQ_j)$ for $j = 1, \ldots, t$.

Compute a minimal polynomial for f over $k(x)$, and write it as a minimal polynomial for x over $k(f)$, and compute successively a $k(f)$-basis for $k(x, f)$ and a $k(f)$-basis for $k(X)$. Output the corresponding map $X \to \mathbb{P}^1_k$.

Proof. Note that by choice of m, we see that $\mathcal{O}_X(-Z_0 + mZ_\infty - mQ_j)$ has dimension $\#B - m$, so f ranges over a set of $2^{\#B}$ elements, of which at most $t2^{\#B-m}$ lie in one of the given subspaces. By choice of m, we have $t2^{\#B-m} < 2^{\#B}$, so there exists such f not lying in any of the given subspaces. □

In particular, if either $U = X$ or $X = \overline{X}$, then we can get a finite locally free morphism $\overline{X} \to \mathbb{P}^1_k$ with U and X inverse images of $\mathbb{P}^1_k$, $\mathbb{P}^1_k - 0$, or $\mathbb{P}^1_k - \infty$. Therefore, using smooth completions, we now have an obvious reduction to Situation 2.4, and therefore the following corollary, which in turn implies Theorem 1.2.

Corollary 9.10. *Let $S_0 \in \{\emptyset, 0\}$ and $S_\infty \in \{\emptyset, \infty\}$. There is an algorithm that takes a finite locally free $\mathbb{P}^1_k - S_\infty$-scheme X, smooth over k, and a finite étale commutative group scheme $\mathcal{A}$ over $U = X \times_{\mathbb{P}^1_k} (\mathbb{P}^1_k - S_0 - S_\infty)$, and computes the* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-module* $\mathrm{H}^1(X_{k^{\mathrm{sep}},ét}, j_!\mathcal{A})$ *in arithmetic complexity exponential in e, $[X : \mathbb{P}^1_k - S_\infty]$, $[\mathcal{A} : U]^{\log[\mathcal{A}:U]}$, γ_X, and $\gamma_\mathcal{A}$. Here, γ_X (resp. $\gamma_\mathcal{A}$) is $\sum_i -a_i$, where a is the type of the normal completion of X (resp. $\mathcal{A}$).*

Proof. We need to prove that the size of the cover $\overline{Y}$ constructed is polynomial in $[X : \mathbb{P}^1_k - S_\infty]$, $[\mathcal{A} : U]^{\log[\mathcal{A}:U]}$, γ_X, and $\gamma_\mathcal{A}$. Recall that $\overline{Y}$ is constructed by setting $X' = X$, $\mathcal{A}' = \mathcal{A}$ and then repeatedly base changing $\mathcal{A}'/X'$ to a non-trivial connected component of $\mathcal{A}'$.

For each such base change, let a be the type of $\mathcal{A}'$, let a' be the type of the chosen connected component of $\mathcal{A}'$, and let a'' be the type of their fibre product $\mathcal{A}''$ over X. Note that as then $\mathcal{O}_{\mathbb{P}^1_k}(a')$ is a direct summand of $\mathcal{O}_{\mathbb{P}^1_k}(a)$, we have $\max_j -a'_j \leq \max_i -a_i$. Moreover, as $\mathcal{O}_{\mathbb{P}^1_k}(a) \otimes_{\mathcal{O}_{\mathbb{P}^1_k}} \mathcal{O}_{\mathbb{P}^1_k}(a')$ surjects onto $\mathcal{O}_{\mathbb{P}^1_k}(a'')$, it follows that $\max_k -a''_k \leq \max_{i,j} -a_i - a'_j \leq 2\max_i -a_i$. Since $\log_2[\mathcal{A} : U]$ such base changes suffice for the construction of a finite locally free X-scheme of which the normalisation is $\overline{Y}$, it follows that for the type b of $\overline{Y}$, its length t is at most $[X : \mathbb{P}^1_k - S_\infty][\mathcal{A} : U]^{\log_2[\mathcal{A}:U]}$, and $\sum_j -b_j \leq t \max_j b_j \leq t[\mathcal{A} : U]\gamma_\mathcal{A}$.

The result now follows from Corollary 9.4. □

9.4. Application to computation for constructible sheaves. In this section, we will indicate how to compute $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$ for X a smooth connected curve and $\mathcal{A}$ an arbitrary constructible sheaf of abelian groups, of torsion invertible in k, under the following assumptions. We will assume a presentation of constructible sheaves (and morphisms between them) to be given, with respect to which one can perform certain operations. These operations are:

- one can compute finite direct sums of constructible sheaves;
- one can compute kernels and cokernels of morphisms;
- for a constructible sheaf $\mathcal{A}$, one can compute a non-empty open subscheme U of X such that $\mathcal{A}|_U$ is finite locally constant;
- for a closed immersion $i\colon Z \to X$ and its open complement $j\colon U \to X$, one can compute the functors $i^{-1}, i_*, i^!, j_!, j^{-1}, j_*$ and the corresponding units and counits of adjunction; given $\mathcal{A}_Z$ on $Z_{\text{ét}}$, $\mathcal{A}_U$ on $U_{\text{ét}}$, and $\phi\colon \mathcal{A}_Z \to i_* j^{-1} \mathcal{A}_U$, one can compute the corresponding constructible sheaf on $X_{\text{ét}}$.

In theory, one should be able to give such a presentation using recollement (as done in Section 5 for $j_!\mathcal{A}$-torsors), but we will not work this out in this paper.

So suppose X is a smooth connected curve, and $\mathcal{A}$ is a constructible sheaf of abelian groups on $X_{\text{ét}}$, of torsion invertible in k. Let U be a non-empty open subscheme for which $\mathcal{A}|_U$ is finite locally constant. Use Algorithm 9.7 and Algorithm 9.9 to find l/k finite purely inseparable, $V \subseteq U_l$ open and a finite locally free morphism $\overline{X}_l \to \mathbb{P}^1_l$ such that V and X_l are finite locally free over their images in $\mathbb{P}^1_l$. Write $j\colon V \to X_l$ for the inclusion, and write $i\colon Z \to X_l$ for its closed complement.

Compute the canonical short exact sequence

$$0 \to j_! j^{-1}\mathcal{A} \to \mathcal{A} \to i_* i^{-1}\mathcal{A} \to 0,$$

and the morphism

$$\delta(i,j)\colon \mathrm{H}^0(X_{k^{\mathrm{sep}},\text{ét}}, i_* i^{-1}\mathcal{A}) \to \mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_! j^{-1}\mathcal{A})$$

which sends a section of $i^{-1}\mathcal{A}$ to the constructible sheaf defined by $j^{-1}\mathcal{A}$ on $V_{\text{ét}}$, 0 on $Z_{\text{ét}}$, and the section of $i^{-1}j_*j^{-1}\mathcal{A}$ obtained from the given section of $i^{-1}\mathcal{A}$ by composition with $i^{-1}\mathcal{A} \to i^{-1}j_*j^{-1}\mathcal{A}$. Then, as we have $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, i_* i^{-1}\mathcal{A}) = 0$, we see that $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A}) = \operatorname{coker} \delta(i,j)$.

This is independent of the choice of (i,j) in the following sense. If $j'\colon V' \to X_l$ and $i'\colon Z' \to X_l$ are given, with $V' \subseteq V$ and a given morphism $Z \to Z'$ over X_l, then we can compute a commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & j'_!(j')^{-1}\mathcal{A} & \longrightarrow & \mathcal{A} & \longrightarrow & i'_*(i')^{-1}\mathcal{A} & \longrightarrow & 0 \\
 & & \downarrow & & \| & & \downarrow & & \\
0 & \longrightarrow & j_! j^{-1}\mathcal{A} & \longrightarrow & \mathcal{A} & \longrightarrow & i_* i^{-1}\mathcal{A} & \longrightarrow & 0
\end{array}$$

a commutative diagram

$$\begin{array}{ccc} \mathrm{H}^0(X_{k^{\mathrm{sep}},\text{ét}}, i'_*(i')^{-1}\mathcal{A}) & \longrightarrow & \mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j'_!(j')^{-1}\mathcal{A}) \\ \downarrow & & \downarrow \\ \mathrm{H}^0(X_{k^{\mathrm{sep}},\text{ét}}, i_*i^{-1}\mathcal{A}) & \longrightarrow & \mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, j_!j^{-1}\mathcal{A}) \end{array}$$

and therefore the morphism $\operatorname{coker}\delta(i',j') \to \operatorname{coker}\delta(i,j)$ corresponding to the identity map on $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A})$.

In the same way, we see that for constructible sheaves $\mathcal{A}, \mathcal{B}$ on $X_{\text{ét}}$, and a morphism $\mathcal{A} \to \mathcal{B}$, we can compute the induced morphism $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A}) \to \mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{B})$, and that for a morphism $f\colon Y \to X$ of smooth connected curves, we can compute the pullback $\mathrm{H}^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathcal{A}) \to \mathrm{H}^1(Y_{k^{\mathrm{sep}},\text{ét}}, f^{-1}\mathcal{A})$.

References

[1] S. J. Berkowitz, "On computing the determinant in small parallel time using a small number of processors", *Inf. Process. Lett.* **18** (1984), p. 147-150.

[2] A. Chistov, "Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time", *J. Sov. Math.* **34** (1986), no. 4, p. 1838-1882, Translated from *Zap. Nauchn. Sem. S.-Petersburg*, 137:124–188, 1984.

[3] J.-M. Couveignes & S. J. Edixhoven (eds.), *Computational aspects of modular forms and Galois representations*, Annals of Mathematics Studies, vol. 176, Princeton University Press, 2011.

[4] R. Dedekind & H. Weber, "Theorie der algebraischen Funktionen einer Veränderlichen", *J. Reine Angew. Math.* (1882).

[5] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, vol. 569, Springer, 1977.

[6] ———, "Le déterminant de la cohomologie", in *Current trends in arithmetical algebraic geometry*, Contemporary Mathematics, vol. 67, American Mathematical Society, 1987, p. 93-177.

[7] A. Dickenstein, N. Fitchas, M. Giusti & C. Sessa, "The membership problem for unmixed polynomial ideals is solvable in single exponential time", *Discrete Appl. Math.* **33** (1991), p. 73-94.

[8] C. Diem, "On arithmetic and the discrete logarithm problem in class groups of curves", 2008, Habilitation thesis.

[9] D. Ferrand, "Un foncteur norme", *Bull. Soc. Math. Fr.* **126** (1998), p. 1-49.

[10] L. Fu, *Étale cohomology theory*, 2nd revised ed., Nankai Tracts in Mathematics, vol. 14, World Scientific, 2015.

[11] U. Görtz & T. Wedhorn, *Algebraic geometry I. Schemes. With examples and exercises*, Advanced Lectures in Mathematics, Vieweg+Teubner, 2010.

[12] A. Grothendieck, "Éléments de Géométrie Algébrique II. Etude globale élémentaire de quelques classes de morphismes", *Publ. Math., Inst. Hautes Étud. Sci.* **8** (1961), p. 5-222.

[13] ———, *Revêtements étales et groupe fondamental (SGA1)*, Lecture Notes in Mathematics, vol. 224, Springer, 1971.

[14] D. Harvey, "Counting points on hyperelliptic curves in average polynomial time", *Ann. Math.* **179** (2014), no. 2, p. 783-803.

[15] F. Hess, "Computing Riemann–Roch spaces in algebraic function fields and related topics", *J. Symb. Comput.* **33** (2002), no. 4, p. 425-445.

[16] E. Kaltofen, "Polynomial-time reductions from multivariate to bi- and univariate integral polynomial factorization", *SIAM J. Comput.* **14** (1985), no. 2, p. 469-489.

[17] K. S. Kedlaya, "Counting points on hyperelliptic curves using Monsky–Washnitzer cohomology", *J. Ramanujan Math. Soc.* **16** (2001), no. 4, p. 323-338.

[18] K. Khuri-Makdisi, "Asymptotically fast group operations on Jacobians of general curves", https://arxiv.org/abs/math/0409209v2, 2004.
[19] A. Lauder & D. Wan, "Counting points on varieties over finite fields of small characteristic", in *Algorithmic Number Theory*, Mathematical Sciences Research Institute Publications, vol. 44, Cambridge University Press, 2008.
[20] M. Lieblich, "Galois representations arising from p-divisible groups", PhD Thesis, Harvard University, 2000.
[21] D. A. Madore & F. Orgogozo, "Calculabilité de la cohomologie étale modulo ℓ", *Algebra Number Theory* **9** (2015), no. 7, p. 1647-1739.
[22] B. Poonen, D. Testa & R. van Luijk, "Computing Néron–Severi groups and cycle class groups", *Compos. Math.* **151** (2015), no. 4, p. 713-734.
[23] Stacks Project Authors, "Stacks Project", 2014, http://stacks.math.columbia.edu.

Jinbi Jin
The Netherlands
E-mail: jinbijin@jinbijin.nl