Computability of the étale Euler-Poincaré characteristic

Jin, J.

Computability of the étale Euler-Poincaré characteristic

Proefschrift

ter verkrijging van

de graad van Doctor aan de Universiteit Leiden

op gezag van Rector Magnificus prof. mr. C. J. J. M. Stolker
volgens besluit van het College voor Promoties

te verdedigen op woensdag 18 januari 2017
klokke 13:45 uur

door

Jinbi Jin

geboren op zondag 4 december 1988 te Almelo

Promotoren:

prof. dr. S. J. Edixhoven	Universiteit Leiden
prof. dr. L. D. J. Taelman	Universiteit van Amsterdam

Commissie:

prof. dr. C. Diem	Universität Leipzig
prof. dr. H. W. Lenstra	Universiteit Leiden
dr. F. Orgogozo	Université Paris-Saclay
prof. dr. B. de Smit	Universiteit Leiden
prof. dr. A. W. van der Vaart	Universiteit Leiden

Het werk in dit proefschrift is gefinancieerd door de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), projectnr. 613.001.110.

Table of contents

Introduction

A motivating question for this dissertation is the following open question, which is stated e.g. in the preface of Serre [36].

Question. *Given a finite type scheme X, does there exist an algorithm that takes as input a prime power q and outputs $\#X(\mathbb{F}_q)$ in time polynomial in* $\log q$*?*

If one fixes the prime p of which q is a power (or in other words, if one restricts to those finite type schemes of which the image in $\operatorname{Spec}\mathbb{Z}$ is a proper closed subscheme), then algorithms based on p-adic cohomology give a positive answer to this question. To name some results: in 2001, Kedlaya [24] gave an algorithm computing the number $\#X(\mathbb{F}_{p^n})$ in time polynomial in n in the case that X is a hyperelliptic curve over $\mathbb{F}_p$, and in 2008, Lauder and Wan [27] gave an algorithm for general varieties over $\mathbb{F}_p$. Neither of these are polynomial in $\log q$ if the characteristic is allowed to vary (or in other words, if X has an open dense image in $\operatorname{Spec}\mathbb{Z}$).

There is some recent progress in this area by Harvey [21] in 2014, who gave an algorithm computing $\#X(\mathbb{F}_q)$ for X such that $X_{\mathbb{Q}}$ is a hyperelliptic curve in *average polynomial time* in $\log q$; more precisely, he gives an algorithm computing the zeta function of X over all "good" p up to some positive integer N in time N times a polynomial in $\log N$; as the number of primes up to N is proportional to $\frac{N}{\log N}$ by the prime number theorem, the average time per prime p is polynomial in $\log N$. However, if one is only interested in $\#X(\mathbb{F}_q)$ for a specific prime power q, the complexity of this algorithm is still exponential in $\log q$.

Algorithms based on étale cohomology give a positive answer for a different class of finite type schemes. In 1985, Schoof [35] gave an algorithm computing $\#X(\mathbb{F}_q)$ for X such that $X_{\mathbb{Q}}$ is an elliptic curve, in time polynomial in $\log q$, and Pila [33] extended this in 1990 to the case of general curves. Both algorithms do this by computing the trace of the Frobenius endomorphism on the first étale cohomology of X.

To generalise these algorithms, one would like to have, for a finite type scheme X, an algorithm computing the *Euler-Poincaré characteristic with compact support* modulo the prime ℓ, denoted by $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$, in time polynomial in ℓ. This is the alternating sum of the étale cohomology groups with compact support, denoted by $H^q_c(X_{\mathbb{Q}^{\mathrm{sep}},\text{ét}}, \mathbb{Z}/\ell\mathbb{Z})$, in the Grothendieck group $K_0\big(\mathbb{Z}/\ell\mathbb{Z}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]\big)$ of finite $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules annihilated by ℓ. We explain at the end of Chapter 2 that the existence of such an algorithm is sufficient for a positive answer to the question.

In 2015, Poonen et al. [34] showed that the étale cohomology groups are computable if X is a smooth, projective, and geometrically irreducible variety over a

field k of characteristic 0. Later that year, Madore and Orgogozo [29] showed that the étale cohomology groups are computable for any variety X. However, both methods rely on an enumeration along an infinite set – in the case of Poonen et al. [34] it is the set of Čech cocycles that is enumerated along; in Madore and Orgogozo [29] the set enumerated along is a set of suitable coverings of the variety – and no upper bound on the complexities of the given algorithms is known.

In this dissertation, we will partially improve these results. The fields we will work over will be fields in which we can compute addition, multiplication, the additive and multiplicative inverses, and factorisations of univariate polynomials; we call such fields *factorial fields*; we will use the number of field operations as a measure of complexity. We defer the description of the in- and output to Chapter 1.

In general, we show that we can compute the Euler-Poincaré characteristic in *effectively bounded* time, i.e. in time bounded by a *primitive recursive* function in terms of the input; we recall the notion of a primitive recursive function in Chapter 1. More precisely, we have the following main theorem.

Theorem I. *There exists an algorithm that takes as input a factorial field k, a scheme X of finite type over k, and an integer n invertible in k, and outputs $\chi_!(X, \mathbb{Z}/n\mathbb{Z})$ as an element of $K_0\big(\mathbb{Z}/n\mathbb{Z}[\mathrm{Gal}(k^{\mathrm{sep}}/k)]\big)$ in an effectively bounded number of field operations.*

We state and prove a more general version in Chapter 2. The strategy we use there is to compute a stratification of the scheme X of finite type over k into locally closed subschemes that are compositions of "sufficiently nice" relative curves, which are a variant of the "fibrations élémentaires" that appear in SGA4.3 [1, Exp. XI, Sec. 3] for example. This will allow us to reduce to the following main theorem.

Theorem II. *There exists an algorithm that takes as input a factorial field k, a smooth curve $f\colon X \to \operatorname{Spec} k$ factoring through a finite locally free morphism $X \to U$ with $U \subseteq \mathbb{P}^1_k$ an open subscheme, and an integer n coprime to the characteristic of k, and outputs the sets*

$$H^0(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z}), H^1(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z}), H^2(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z}),$$
$$H^0_c(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z}), H^1_c(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z}), H^2_c(X_{k^{\mathrm{sep}},\acute{e}t}, \mathbb{Z}/n\mathbb{Z})$$

in an effectively bounded number of field operations.

We state and prove a more general version in Chapter 3. This computation is done by first computing $H^0(X_{k^{\mathrm{sep}},\text{ét}}, \mathbb{Z}/n\mathbb{Z})$, $H^1(X_{k^{\mathrm{sep}},\text{ét}}, \mathbb{Z}/n\mathbb{Z})$, using the geometric interpretations of their elements. More precisely, for the first cohomology we construct a moduli space of $\mathbb{Z}/n\mathbb{Z}$-torsors on X with some additional structure, such that its connected components correspond bijectively to the isomorphism classes of $\mathbb{Z}/n\mathbb{Z}$-torsors on $X_{k^{\mathrm{sep}}}$. After that, we use Poincaré duality to compute the remaining groups.

1 Effective algebraic geometry

In this chapter we describe the basics of computations in algebraic geometry. We start by explaining in Sections 1.1 to 1.4 the view on computability taken in this dissertation, before treating the basic constructions in algebraic geometry that we will need for the algorithm described in the later chapters.

1.1 Primitive recursive functions and computability

In order to algorithmically compute with mathematical objects, one first needs to be able to present these objects into some computational model. There are a number of classical such models, e.g. that of the *Turing machine*, the *random-access machine* (or *RAM*), and that of the *recursive functions*. We wish to be able to describe a theory of algorithms that are "bounded" in some way; this can be done the most naturally in the theory of recursive functions, in which we have a class of *primitive recursive functions*.

A modern treatment on (primitive) recursive functions can be found in most books on computability; the following treatment is based on that of Moret [31].

We will define the set of primitive recursive functions as a subset of $\coprod_{n=0}^{\infty} \mathbb{N}^{\mathbb{N}^n}$; note that $\mathbb{N}^{\mathbb{N}^0} = \mathbb{N}$.

Definition 1.1. The *base functions* are the following:

- the constant $0 \in \mathbb{N}$;
- the *successor function* $S\colon \mathbb{N} \to \mathbb{N}$, $x \mapsto x + 1$;
- for positive integers n, i such that $i \leq n$, the *projection function* $P_i^n\colon \mathbb{N}^n \to \mathbb{N}$ on the i-th coordinate.

Next, we define the two operations under which we want the set of primitive recursive functions to be closed.

Definition 1.2. Let $m, n \geq 0$ be integers, and let $g\colon \mathbb{N}^m \to \mathbb{N}$, $h_1, \ldots, h_m\colon \mathbb{N}^n \to \mathbb{N}$ be functions. Then the function $\sigma_{m,n}(g, h_1, \ldots, h_m)\colon \mathbb{N}^n \to \mathbb{N}$ given by

$$(x_1, \ldots, x_n) \mapsto g\big(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)\big)$$

is said to be obtained from $g, h_1, \ldots, h_n$ by *substitution*.

Note that in the edge case $m = 0$, the function $\sigma_{0,n}(g)$ is the constant function (from $\mathbb{N}^n$) with value g; in the other edge case $n = 0$, the function $\sigma_{m,0}(g, h_1, \ldots, h_m)$ is $g(h_1, \ldots, h_m) \in \mathbb{N}$.

Definition 1.3. Let n be a positive integer, and let $g\colon \mathbb{N}^{n-1} \to \mathbb{N}$ and $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ be functions. Then the function $\rho_n(g,h)\colon \mathbb{N}^n \to \mathbb{N}$ given recursively by

$$(x_1,\dots,x_n) \mapsto \begin{cases} g(x_2,x_3,\dots,x_n) & \text{if } x_1 = 0 \\ h\big(x_1-1,\rho_n(g,h)(x_1-1,x_2,\dots,x_n),x_2,\dots,x_n\big) & \text{if } x_1 > 0 \end{cases}$$

is said to be obtained from g,h by *primitive recursion*.

Now we can define the set of primitive recursive functions.

Definition 1.4. The set R_p of *primitive recursive functions* is the smallest subset of the set $\coprod_{n=0}^{\infty} \mathbb{N}^{\mathbb{N}^n}$ that contains the base functions, and such that

- for all non-negative integers m,n, and all $g\colon \mathbb{N}^m \to \mathbb{N}$, $h_1,\dots,h_m\colon \mathbb{N}^n \to \mathbb{N}$ such that $g,h_1,\dots,h_m \in R_p$, we have $\sigma_{m,n}(g,h_1,\dots,h_m) \in R_p$;
- for all positive integers n, and all functions $g\colon \mathbb{N}^{n-1} \to \mathbb{N}$, $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ such that $g,h \in R_p$, we have $\rho_n(g,h) \in R_p$.

An *algorithm* computing a certain primitive recursive function f is in this context an explicit expression of f in terms of the base functions, substitution, and primitive recursion.

Example 1.5. The function $d\colon \mathbb{N} \to \mathbb{N}$ given by $x \mapsto \max(x-1,0)$ is primitive recursive. An algorithm computing it is

$$\rho_1(0,P_1^2).$$

For any primitive recursive function $f\colon \mathbb{N} \to \mathbb{N}$ (together with an algorithm computing it), the function $i_f\colon \mathbb{N}\times\mathbb{N} \to \mathbb{N}$ defined by $(n,x) \mapsto f^n(x)$ is primitive recursive, and an algorithm computing i_f is given by

$$\rho_2\big(P_1^1,\sigma_{1,3}(f,P_2^3)\big).$$

Note that i_S is the addition map on $\mathbb{N}$.

Note that the primitive recursive functions form a strictly smaller class of functions than what are typically called *recursive* or *computable* functions. We get the usual notion back once we add the *unbounded minimisation operator*, and temporarily also consider partial functions $\mathbb{N}^n \to \mathbb{N}$.

Definition 1.6. Let $f\colon \mathbb{N}^{n+1} \to \mathbb{N}$ be a partial function. Then $\mu_f\colon \mathbb{N}^n \to \mathbb{N}$ is the partial function such that $\mu_f(x_1,\dots,x_n)$ is undefined whenever $f(y,x_1,\dots,x_n) \neq 0$ for all $y \in \mathbb{N}$, and such that $\mu_f(x_1,\dots,x_n) = y$ if $y \in \mathbb{N}$ is the minimal number such that $f(y,x_1,\dots,x_n) = 0$. We say that μ_f is obtained from f by *unbounded minimisation*.

This allows us to define the set of recursive functions.

Definition 1.7. The set R' of *partial recursive functions* is the smallest set of partial functions $\mathbb{N}^n \to \mathbb{N}$ (with varying n) that contains the base functions, and such that

- for all integers $m,n \geq 0$, and all partial functions $g\colon \mathbb{N}^m \to \mathbb{N}$ and all partial functions $h_1,\dots,h_m\colon \mathbb{N}^n \to \mathbb{N}$ with $g,h_1,\dots,h_m \in R'$, the partial function $\sigma_{m,n}(g,h_1,\dots,h_m)$ lies in R';

- for all integers $n > 0$, and all partial functions $g\colon \mathbb{N}^{n-1} \to \mathbb{N}$, $h\colon \mathbb{N}^{n+1} \to \mathbb{N}$ with $g, h \in R'$, we have $\rho_n(g,h) \in R'$;
- for all integers $n \geq 0$, and all partial functions $g\colon \mathbb{N}^{n+1} \to \mathbb{N}$ with $g \in R'$, we have $\mu_g \in R'$.

The set R of *recursive functions* is the subset of R' of total functions.

1.2 Explicitly given sets and maps

The following is essentially the theory of (primitive) recursive sets, as can be found in most books on computability, e.g. Moret [31]. We will view $\mathbb{N}$ as a pointed set with base point 0 in what follows; we will think of 0 as an "error code".

Definition 1.8. A *presentation* of a set X consists of an injective *presentation map* $\pi\colon X \to \mathbb{N} - \{0\}$ together with an algorithm computing the characteristic function $\chi_{\pi(X)}$ of $\pi(X)$. An *explicitly given set* is a pair (X, π_X) of a set and a presentation π_X of X.

Definition 1.9. Let $(X, \pi_X), (Y, \pi_Y)$ be explicitly given sets. A *presentation* of a map $f\colon Y \to X$ is an algorithm computing the unique function $\varphi\colon \mathbb{N} \to \mathbb{N}$ such that $\varphi(y) = 0$ for all $y \notin \pi_Y(Y)$, and such that the following diagram commutes.

$$\begin{array}{ccc} Y & \xrightarrow{\pi_Y} & \mathbb{N} \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle \varphi} \\ X & \xrightarrow[\pi_X]{} & \mathbb{N} \end{array}$$

An *explicitly given map* $Y \to X$ is a map $Y \to X$ together with a presentation.

We obtain a collection $\mathrm{Set}_!$ of explicitly given sets and explicitly given maps, which only becomes a category after we identify algorithms defining the same map (in other words, we forget the algorithm). There is a forgetful functor $\mathrm{Set}_! \to \mathrm{Set}$, which is faithful by definition, but not full (as not every function is primitive recursive).

Example 1.10. Let, for any non-empty set X and any $x \in X$, the set $\mathrm{Seq}_{\infty,x}(X)$ denote the set of sequences $(x_i)_{i=0}^{\infty}$ such that $x_i = x$ for all but finitely many i. We first give the *Gödel encoding* of $\mathrm{Seq}_{\infty,0}(\mathbb{N})$. Let $p_0 = 2, p_1, \dots$ denote the increasing enumeration of the prime numbers. Then the Gödel encoding $\pi\colon \mathrm{Seq}_{\infty,0}(\mathbb{N}) \to \mathbb{N}$ sending $(a_0, a_1, \dots)$ to $p_0^{a_0} p_1^{a_1} \cdots$ is a presentation of $\mathrm{Seq}_{\infty,0}(\mathbb{N})$.

Now let X be a non-empty explicitly given set, and $x \in X$ an element such that $\pi_X(x) = 1$. The map $X \to \mathbb{N}$, $x \mapsto \pi_X(x) - 1$ then induces a presentation $\mathrm{Seq}_{\infty,x}(X) \to \mathrm{Seq}_{\infty,0}(\mathbb{N}) \to \mathbb{N}$, which sends the constant sequence x to 1. This allows us to iterate this process, obtaining presentations for e.g. $\mathrm{Seq}_{\infty,x}\big(\mathrm{Seq}_{\infty,x}(X)\big)$, etc.

Moreover, let, for any non-empty set X, the set $\mathrm{Seq}(X)$ denote the set of finite sequences in X. We then have an injective map $\mathrm{Seq}(\mathbb{N}) \to \mathrm{Seq}_{\infty,0}(\mathbb{N})$ sending $(a_1, \dots, a_n)$ to $(n, a_1, \dots, a_n)$, which induces a presentation of $\mathrm{Seq}(\mathbb{N})$. If X is an explicitly given set, then as before, the map $X \to \mathbb{N}$, $x \mapsto \pi_X(x) - 1$ induces a presentation $\mathrm{Seq}(X) \to \mathrm{Seq}(\mathbb{N}) \to \mathbb{N}$.

1.3 Explicitly given fields and factorial fields

In this section we will give a definition of a factorial field, cf. e.g. Ayoub [2]. We first give a definition of explicitly given rings and fields.

Definition 1.11. An *explicitly given ring* is an explicitly given set R that is a ring, together with elements $0, 1 \in R$, the characteristic of R, and encodings of the maps $+, \cdot \colon R \times R \to R$, $- \colon R \to R$. An *explicitly given morphism* $R \to S$ of explicitly given rings is an explicitly given map that is also a morphism of rings. An *explicitly given field* is an explicitly given ring k that is a field, together with a presentation of the map $\cdot^{-1} \colon k - \{0\} \to k - \{0\}$.

Remark 1.12. Note that at times, elements of fields are more naturally given as equivalence classes of elements of some set, e.g. the case of a fraction field of an integral domain. Therefore it may be more desirable to accommodate for this and define an explicitly given ring or field as an explicitly given set R together with a primitive recursive equivalence relation on R and the usual operations (which are to satisfy the usual relations only up to equivalence). However, since bounded minimisation is primitive recursive, so is the (characteristic function of the) set of minimal representatives of each equivalence class and the map $R \to R$ sending each x to its corresponding minimal representative. Therefore we can construct from such R an explicitly given ring or field in the sense of the definition above, and we lose no generality.

Example 1.13. The fields $\mathbb{F}_q$ (for q a prime power) and $\mathbb{Q}$ can be given the structure of an explicitly given field. Suppose that k is an explicitly given field. Any finitely generated extension of k can be given the structure of an explicitly given field. The field $k(x_1, x_2, \dots)$ can be given the structure of an explicitly given field.

For an explicitly given ring R, we will give $R[x]$ the structure of an explicitly given ring. First, identify $R[x]$ with $\mathrm{Seq}_{\infty,0}(R)$ by identifying a polynomial $f = \sum_{i=0}^{\infty} a_i x^i$ with the sequence $(a_i)_{i=0}^{\infty}$. Since we have obvious algorithms to compute addition, multiplication, and additive inverse, we get the structure of an explicitly given ring on $R[x]$. By iterating this process, one gets a structure of an explicitly given ring on the polynomial ring $R[x_1, \dots, x_n]$ as well.

Since we now have a presentation of polynomials and therefore also of finite sequences thereof, we can now introduce the notion of a polynomial factorisation algorithm.

Definition 1.14. A *factorial field* is an explicitly given field k, together with a presentation of a map $k[x] - \{0\} \to \mathrm{Seq}(k[x])$ sending f to a tuple $(f_1, \dots, f_n)$ such that $f = f_1 \cdots f_n$ and every f_i is irreducible.

Example 1.15. Any finitely generated extension of $\mathbb{F}_q$ (for q a prime power) or $\mathbb{Q}$ can be given the structure of a factorial field.

There exist explicitly given fields for which polynomial factorisation is not computable, see Fröhlich and Shepherdson [12].

1.4 Remarks on "algorithms" and "complexity"

First note that the notion of algorithm given above is not a very convenient notion to work with. However, there is a different way of describing primitive recursive functions which may be a bit more amenable, namely as so-called *loop programs* (see e.g. Handley and Wainer [20, Sec. 1]). Roughly speaking, these are algorithms using only finite loops of precomputed length (so no recursion is allowed a priori). Of course, as many algorithms use recursion, this is still a bit too restrictive in practice. In practice, we will also allow recursion if the total number of recursive calls for a single instance can be bounded by a precomputed number; it is possible to rewrite such recursively defined functions as a loop of a precomputed length. This allows us to discuss algorithms much more informally, and we will usually do so.

Note moreover that while the notion of explicitly given (or factorial) field described above is suitable for a notion of computability, it doesn't admit a good notion of *arithmetic complexity*, i.e. the number of field operations needed to compute a function (as a function in the input); as the field operations are assumed to be primitive recursive, they can be described in terms of base functions, the notion of a number of field operations isn't even well-defined! While the notion of an arithmetic complexity can be formalised, see e.g. Diem [10, Sec. 1.6.4] for RAMs, we will use the term informally, viewing the field operations of an explicitly given or factorial field as primitive operations.

Finally, note that in the definition of a factorial field, we have included a primitive recursive univariate factorisation algorithm, but in practice, some efficient such algorithms use randomisation, but halt with probability 1 and with the correct output, i.e. they are *Las Vegas* algorithms. Therefore algorithms involving factorisation should be viewed as Las Vegas algorithms in general. Other than that, we will usually ignore the difference between Las Vegas and deterministic algorithms.

1.5 Algebra over explicitly given fields

As stated in the previous section, we will be a lot less formal with algorithms from now on.

1.5.1 Vector spaces

We present a finite-dimensional vector space over k (with given basis) by its dimension, and a k-linear map from a vector space of dimension m to a vector space of dimension n by its $n \times m$-matrix with respect to the given bases.

If vector spaces V and V' have bases $(e_1, e_2, \dots, e_m)$ and $(e'_1, e'_2, \dots, e'_{m'})$, respectively, then we will assume their direct sum $V \oplus V'$ to be equipped with the basis $(e_1, e_2, \dots, e_m, e'_1, e'_2, \dots, e'_{m'})$, and their tensor product $V \otimes V'$ to be equipped with the basis $(e_i \otimes e'_{i'})_{i=1,i'=1}^{m,m'}$, with the lexicographical order on the indices. This has the additional advantage that if we have three vector spaces V, V', V'' with given bases, that then the natural isomorphisms $(V \otimes V') \otimes V'' \cong V \otimes (V' \otimes V'')$, $k \otimes V \cong V \cong V \otimes k$, and $(V \oplus V') \otimes V'' \cong (V \otimes V'') \oplus (V' \otimes V'')$ preserve the induced bases.

We present a subspace of dimension m of a given vector space of dimension n by an $n \times m$-matrix in reduced row echelon form. Therefore, by Gaussian elimination,

we can compute kernels and images of linear maps, in a number of field operations polynomially bounded by the dimensions of the source and target. Moreover, we can compute the quotient of a vector space by a subspace, and therefore we can compute cokernels of linear maps as well, also in a number of field operations polynomially bounded by the dimensions of the source and target.

1.5.2 Finitely generated algebras

We present an ideal I of $k[x_1, \ldots, x_m]$ by a finite set of generators $f_1, \ldots, f_s$. An algebra of finite type over k then is given by a non-negative integer m, and an ideal of $k[x_1, \ldots, x_m]$.

We present an element f of $k[x_1, \ldots, x_m]/I$ by an element of $f + I$ in $k[x_1, \ldots, x_m]$; note that sums and products of elements can be computed, and that equality of two elements can be tested using Gröbner basis algorithms. A k-algebra morphism $k[x_1, \ldots, x_m]/I \to k[y_1, \ldots, y_n]/J$ is given by the images of the x_i, under the condition that the generators of I map to 0 (which can be tested by the above). Moreover, compositions of morphisms can be computed, and equality of two morphisms can be tested using Gröbner basis algorithms.

We will consider more properties in Section 1.7.

1.5.3 Finite algebras

We describe two ways to present a finite k-algebra.

One way to present a finite k-algebra A is the *vector space presentation*, namely by its underlying vector space over k, together with the inclusion $\iota\colon k \to A$ and the multiplication map $\mu\colon A \otimes A \to A$; these are to be such that the following diagrams commute:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu \otimes \mathrm{id}_A} & A \otimes A \\ {\scriptstyle \mathrm{id}_A \otimes \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array} \qquad \begin{array}{ccc} A & \xrightarrow{\iota \otimes \mathrm{id}_A} & A \otimes A \\ {\scriptstyle \mathrm{id}_A \otimes \iota}\downarrow & & \downarrow{\scriptstyle \mu} \\ A \otimes A & \xrightarrow[\mu]{} & A \end{array}$$

and we present a morphism $A \to B$ of finite k-algebras by its underlying k-linear map; this map must be such that the following diagrams commute.

$$\begin{array}{ccc} A \otimes A & \xrightarrow{f \otimes f} & B \otimes B \\ {\scriptstyle \mu}\downarrow & & \downarrow{\scriptstyle \mu} \\ A & \xrightarrow[f]{} & B \end{array} \qquad \begin{array}{ccc} & k & \\ {\scriptstyle \iota}\swarrow & & \searrow{\scriptstyle \iota} \\ A & \xrightarrow[f]{} & B \end{array}$$

One other way to present a finite k-algebra is by the quotient of $k[x_1, \ldots, x_m]$ by a zero-dimensional ideal; in this case the morphisms are presented by morphisms of k-algebras. We claim that these two ways are equivalent; i.e. that we can transform one presentation into the other primitive recursively. We will only work this out for the objects, leaving the morphisms to the reader.

First suppose that we are given A as a vector space together with maps $\iota\colon k \to A$ and $\mu\colon A \otimes A \to A$, and let $(t_1, \ldots, t_m)$ be the given basis of A. Then A is isomorphic

to $k[t_1, \ldots, t_m]/I$, where I is generated by $t_i t_j - \mu(t_i \otimes t_j)$ and $1 - \iota(1)$. Note that this is done in a number of field operations polynomially bounded in $\dim_k A$.

Conversely, assume that we are given a zero-dimensional ideal $I \subseteq k[x_1, \ldots, x_m]$ such that $A = k[x_1, \ldots, x_m]/I$. Then we can compute from a Gröbner basis of I a k-basis for A consisting of monomials, and we can compute the multiplication and inclusion maps with respect to this basis using division with remainder with respect to the Gröbner basis. Note that this involves computing Gröbner basis of zero-dimensional ideals, which can theoretically be done in a number of field operations exponentially bounded in the number of given generators of the ideal, see Dickenstein et al. [9].

We now list a number of properties that can be decided algorithmically. We start with the property of being étale over k.

Proposition 1.16. *There exists an algorithm that takes as input an explicitly given field k and a finite k-algebra A, and decides whether A is étale over k, in a number of field operations polynomially bounded in* $\dim_k A$.

Proof. Note that A is étale over k if and only if the *trace form* $A \to \mathrm{Hom}_k(A, k)$ given by $a \mapsto \big(b \mapsto \mathrm{Tr}(ab)\big)$ is invertible. Since we can compute the trace form and the determinant thereof in a number of field operations bounded polynomially in $\dim_k A$, we get the desired result. □

To decide whether a finite k-algebra A is local, we use the following result.

Proposition 1.17 (Khuri-Makdisi [25, Sect. 7])**.** *There exists an algorithm that takes as input a factorial field k and a finite k-algebra A, and returns an isomorphism $\prod_i A_i \cong A$ with all A_i finite local k-algebras, in a number of field operations polynomially bounded in* $\dim_k A$.

Corollary 1.18. *There exists an algorithm that takes as input a factorial field k and a finite k-algebra A, and decides whether A is local, in a number of field operations polynomially bounded in* $\dim_k A$.

Since for a finite k-algebra, being étale and local is equivalent to being a finite separable field extension of k, we also get the following.

Corollary 1.19. *There exists an algorithm that takes as input a factorial field k and a finite k-algebra A, and decides whether A is a finite separable field extension of k, in a number of field operations polynomially bounded in* $\dim_k A$.

Finally, we can decide whether a finite k-algebra is a finite Galois (field) extension of k.

Proposition 1.20. *There exists an algorithm that takes as input a factorial field k and a finite separable field extension l over k, and outputs the Galois closure of l over k, in a number of field operations exponentially bounded in* $\dim_k l$.

Proof. Decompose $l \otimes l = \prod_i l_i$. Then note that each l_i is a separable field extension of l, and that l is Galois if and only if every l_i is equal to l. Therefore replacing l iteratively by an l_i with maximal dimension (and using that the Galois closure of l over k has degree at most $[l : k]!$ over k) computes the Galois closure of l over k in a number of field operations exponentially bounded in $\dim_k l$. □

Corollary 1.21. *There exists an algorithm that takes as input a factorial field k and a finite k-algebra A, and decides whether A is a finite Galois (field) extension of k, in a number of field operations polynomially bounded in* $\dim_k A$.

Next, we compute the Galois group of a finite Galois extension of k.

Proposition 1.22. *There exists an algorithm that takes as input a factorial field k and a finite Galois extension l of k, and outputs* $\mathrm{Gal}(l/k)$.

Proof. We note that $\mathrm{Gal}(l/k)$ is the set of k-rational points of a finite algebraic subgroup of $\mathrm{GL}_{\dim_k l,k}$, which we can compute using Gröbner bases. □

Finally, given a finite Galois extension l of k with Galois group G, we can make Galois theory effective: given a subgroup H of G, we can compute l^H (as the intersection of the kernels of the k-linear maps $1-h$ for $h \in H$), and vice versa, given a subextension l' of l over k, we can compute $\mathrm{Gal}(l/l')$.

1.5.4 Galois sets

The following treatment is essentially that of Couveignes and Edixhoven [5, p.69–70].

Let G be the absolute Galois group of k; recall that it is a profinite group. There are two natural ways of presenting a finite continuous G-set. For the first one, note that the category of finite continuous G-sets is equivalent to the opposite of that of finite separable k-algebras; so we present a finite continuous G-set by a finite separable k-algebra, and we present a morphism $Y \to X$ of finite continuous G-sets by a morphism of finite separable k-algebras (in the opposite direction).

Alternatively, note that a finite continuous G-set is given by a finite set X, together with a continuous group morphism $G \to S(X)$, where $S(X)$ is the permutation group on X. Its kernel N is a closed subgroup of finite index, which corresponds to a finite Galois extension l over k, and the Galois set X is determined by the action of $\mathrm{Gal}(l/k)$ on X. This shows that we can present a finite continuous G-set by a tuple (l, X, α) of a finite Galois extension l over k, a finite set X, and an action α of $\mathrm{Gal}(l/k)$ on X.

We can extend the above to any finite number of finite continuous G-sets, to see that we can present a finite number of finite continuous G-sets by a tuple $\left(l, (X_i, \alpha_i)_i\right)$, such that every (l, X_i, α_i) presents a finite continuous G-set. In particular, we see that we can present a morphism of finite continuous G-sets by a finite Galois extension l over k, finite sets X, Y, actions α_X, α_Y of $\mathrm{Gal}(l/k)$ on X, Y, respectively, and a $\mathrm{Gal}(l/k)$-equivariant map $f\colon Y \to X$.

Using Section 1.5.3, we see that these two presentations can be converted into one another in a straightforward way; if A is a finite separable k-algebra, and $A = \prod_i l_i$ is a decomposition of A into fields, then a corresponding triple is (l, X, α) where l is the Galois closure of the compositum of the l_i and the set X is $\coprod_i \mathrm{Hom}_k(l_i, l)$ together with the natural $\mathrm{Gal}(l/k)$-action on the $\mathrm{Hom}_k(l_i, l)$; conversely, if (l, X, α) is a presentation of a finite continuous G-set, then decompose X into $\mathrm{Gal}(l/k)$-orbits X_i, compute for each i a stabiliser G_i of a point of X_i (which is well-defined up to inner automorphisms), and set $A = \prod_i l^{G_i}$.

1.5.5 Multivariate and absolute factorisation

Recall that a factorial field is an explicitly given field together with an algorithm for *univariate* polynomial factorisation. However, using a trick attributed to Kronecker in van der Waerden [37, Sec. 42], one can easily reduce multivariate polynomial factorisation to univariate polynomial factorisation; this uses an number of field operations exponential in the degree of the polynomial to be factored.

Next, we consider *absolute factorisation*, i.e. given a polynomial $f \in k[x_1, \ldots, x_m]$, find the factorisation of f over the algebraic closure of k. Note that this factorisation is defined over a finite extension l of k. By Chistov [4, Sec. 1.3], absolute factorisation can be reduced to ordinary multivariate polynomial factorisation in a number of field operations which is polynomial in the degree of the polynomial to be factored.

It follows that any factorial field admits an algorithm computing absolute factorisations of polynomials in $k[x_1, \ldots, x_m]$.

1.6 Curves over explicitly given fields

Let k be an explicitly given field. In this section we describe two ways to describe $\mathbb{P}^1_k$-vector bundles, one of which is more or less classical, essentially going back to Dedekind and Weber [6] (another reference is Diem [10]), and an alternative one better suited for our purposes. We can then describe curves together with a finite locally free morphism to $\mathbb{P}^1_k$ as vector bundles on $\mathbb{P}^1_k$ with an algebra structure.

1.6.1 Vector bundles via function fields

The following is a slight generalisation and alteration of the idea described in Diem [10, Sect. 2.5.4.2].

The basic idea here is to describe a vector bundle $\mathcal{E}$ on $\mathbb{P}^1_k$ by $(\mathcal{E}_\eta, \mathcal{E}(U_0), \mathcal{E}(U_1))$, where $\eta \in \mathbb{P}^1_k$ is the generic point, and U_0, U_1 are the standard affine open subsets of $\mathbb{P}^1_k$. Here we view the $\mathcal{E}(U_i)$ as subsets of $\mathcal{E}_\eta$. The rule attaching to $\mathcal{E}$ a triple as above is a functor, the target category of which we describe below. There, we will identify $\mathcal{O}_{\mathbb{P}^1_k,\eta}, \mathcal{O}_{\mathbb{P}^1_k}(U_0), \mathcal{O}_{\mathbb{P}^1_k}(U_1)$ with $k(x), k[x], k[x^{-1}]$, respectively.

Consider the category $\mathcal{L}(k)$ defined as follows. The objects of $\mathcal{L}(k)$ are tuples (V, V_0, V_1), where V is a finite dimensional vector space over $k(x)$, say of dimension m, and V_0 (resp. V_1) is a free $k[x]$-submodule (resp. $k[x^{-1}]$-submodule) of V of rank m, such that V_0 and V_1 generate the same $k[x, x^{-1}]$-submodule of V. The morphisms $(V, V_0, V_1) \to (W, W_0, W_1)$ in $\mathcal{L}(k)$ are the morphisms $V \to W$ that map V_i into W_i for $i \in \{0, 1\}$.

Note that the functor from the category of vector bundles on $\mathbb{P}^1$ to $\mathcal{L}(k)$ defined by

$$\mathcal{E} \mapsto (\mathcal{E}_\eta, \mathcal{E}(U_0), \mathcal{E}(U_1)).$$

is an equivalence of categories.

By expanding the definition of the objects and morphisms of $\mathcal{L}(k)$ in terms of matrices, we see that $\mathcal{L}(k)$ (hence also the category of vector bundles on $\mathbb{P}^1_k$) is equivalent to the category $\mathcal{P}'(k)$ (of presentations of finite locally free $\mathcal{O}_{\mathbb{P}^1_k}$-modules) defined below.

The objects of $\mathcal{P}'(k)$ are tuples (m, B_0, B_1), where m is a non-negative integer and $B_0, B_1 \colon k(x)^m \to k(x)^m$ are $k(x)$-linear isomorphisms, the columns of the matrices of which generate the same $k[x, x^{-1}]$-submodules of $k(x)^m$, i.e. the matrix of $B_0 B_1^{-1}$ has entries in $k[x, x^{-1}]$. (Matrices are always taken with respect to the standard bases.)

Now consider two objects (m, B_0, B_1) and (n, C_0, C_1) of $\mathcal{P}'_1(k)$. The morphisms in $\mathcal{P}'(k)$ from (m, B_0, B_1) to (n, C_0, C_1) are the $k(x)$-linear maps $f \colon k(x)^m \to k(x)^n$, such that the $k[x]$-submodule generated by the columns of the matrix of B_0 is mapped into that of C_0, and such that the $k[x^{-1}]$-submodule generated by the columns of the matrix of B_1 is mapped into that of C_1. In other words, we have that the matrices of $C_0^{-1} f B_0$, resp. $C_1^{-1} f B_1$ have entries in $k[x]$, resp. $k[x^{-1}]$.

Note that the tensor product $(m, B_0, B_1) \otimes (m', B_0', B_1')$ of two objects in $\mathcal{P}'(k)$ is given by $(mm', B_0 \otimes B_0', B_1 \otimes B_1')$, and that the tensor product of two morphisms $f \colon (m, B_0, B_1) \to (n, C_0, C_1)$ and $f' \colon (m', B_0', B_1') \to (n', C_0', C_1')$ is given by $f \otimes f'$ (as $k(x)$-linear map $k(x)^{mm'} \to k(x)^{nn'}$). Moreover, $\otimes$ is associative and the (identity morphism on) the object $(0, 0, 0)$ is neutral for $\otimes$.

1.6.2 Vector bundles via Dedekind-Weber splitting

There is an alternative way to present vector bundles on $\mathbb{P}^1_k$. The following theorem (commonly attributed to Grothendieck) describes all isomorphism classes of vector bundles on $\mathbb{P}^1_k$.

Theorem 1.23 (Dedekind and Weber [6])**.** *Let k be a field, and let $\mathcal{E}$ be a finite locally free $\mathcal{O}_{\mathbb{P}^1_k}$-module. Then there exists a (up to permutation unique) finite sequence of integers $(a_i)_{i=1}^s$ such that $\mathcal{E} \cong \bigoplus_{i=1}^s \mathcal{O}_{\mathbb{P}^1_k}(a_i)$.*

Write, for a finite sequence $a = (a_i)_{i=1}^s$ of integers, $\mathcal{O}_{\mathbb{P}^1_k}(a)$ for the $\mathcal{O}_{\mathbb{P}^1_k}$-module $\bigoplus_{i=1}^s \mathcal{O}_{\mathbb{P}^1_k}(a_i)$. We will use the "linear algebra" of such objects to describe the category of finite locally free $\mathcal{O}_{\mathbb{P}^1_k}$-algebras. Since for all finite sequences a, b of integers, we have

$$\begin{aligned}\operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}\big(\mathcal{O}_{\mathbb{P}^1_k}(a), \mathcal{O}_{\mathbb{P}^1_k}(b)\big) &= \bigoplus_{i,j} \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_k}}\big(\mathcal{O}_{\mathbb{P}^1_k}(a_i), \mathcal{O}_{\mathbb{P}^1_k}(b_j)\big) \\ &= \bigoplus_{i,j} \mathcal{O}_{\mathbb{P}^1_k}(b_j - a_i)(\mathbb{P}^1_k),\end{aligned}$$

we see that giving a morphism $\mathcal{O}_{\mathbb{P}^1_k}(a) \to \mathcal{O}_{\mathbb{P}^1_k}(b)$ is the same as giving an element of

$$\operatorname{Mat}_{b,a}(k) = \{M \in \operatorname{Mat}_{t \times s}\big(k[x, y]\big) : M_{ji} \in k[x, y]_{b_j - a_i}\},$$

where s and t are the respective lengths of the sequences a and b.

Therefore the category of vector bundles on $\mathbb{P}^1_k$ is equivalent to the category $\mathcal{P}(k)$ of which the objects are finite sequences of integers, and in which the set of morphisms from a finite sequence a to a finite sequence b is given by $\operatorname{Mat}_{b,a}(k)$ (with composition given by matrix multiplication).

Next, we describe tensor products in $\mathcal{P}(k)$. For two finite sequences a, a' of integers the sequence $a \oplus a'$ is the set $\{a_i + a'_{i'}\}_{i,i'}$ together with the order on the index

set given by the lexicographical order on pairs (i, i'), so that there is an isomorphism $\mathcal{O}_{\mathbb{P}^1_k}(a \oplus a') \cong \mathcal{O}_{\mathbb{P}^1_k}(a) \otimes \mathcal{O}_{\mathbb{P}^1_k}(a')$. Moreover, the tensor product of two morphisms can be computed by viewing morphisms as matrices with entries in $k(x, y)$.

1.6.3 Converting presentations

We now describe explicit quasi-inverse equivalences between $\mathcal{P}(k)$ and $\mathcal{P}'(k)$.

First we describe the functor $F\colon \mathcal{P}(k) \to \mathcal{P}'(k)$. For an object a of $\mathcal{P}(k)$, i.e. a finite sequence of integers, we set $F(a)$ to be the triple

$$\Big(\bigoplus_i \mathcal{O}_{\mathbb{P}^1_k}(a_i)_\eta, B_0, B_1\Big),$$

where we identify $\mathcal{O}_{\mathbb{P}^1_k}(a_i)_\eta$ with $k(x)$ by identifying y with 1, and where B_0 is the identity matrix, and where B_1 is the diagonal matrix of which the i-th entry is x^{a_i}. The given identification of $\mathcal{O}_{\mathbb{P}^1_k}(a_i)_\eta$ with $k(x)$ also immediately gives a description of F on morphisms.

Next, we describe its quasi-inverse $G\colon \mathcal{P}'(k) \to \mathcal{P}(k)$. Suppose that we have an object (m, B_0, B_1) of $\mathcal{P}'(k)$. Then the method of e.g. Görtz and Wedhorn [16, Lem. 11.50], see also Hess [22, Sec. 4], gives an algorithm to compute a basis $C = \{C_i\}$ of $k(x)^m$ over k such that C generates the same $k[x]$-submodule as B_0, and a sequence of integers a of length s such that $x^{a_i}C_i$ spans the same $k[x^{-1}]$-submodule of $k(x)^m$ as B_1. In this case, we set $G(m, B_1, B_2) = a$.

Next, if we have a morphism $\varphi\colon (m, B_0, B_1) \to (n, C_0, C_1)$ in $\mathcal{P}'(k)$, we consider their corresponding sequences of integers a, b, and the matrix M of the corresponding k-linear map $k(x)^m \to k(x)^n$ with respect to the $k(x)$-bases given above. By definition of a morphism, the entries of this matrix lie in $k[x]$, and in fact, the degree of the (j, i)-entry is at most $b_j - a_i$. Let M' be the matrix in $k[x, y]$ obtained from M by replacing each entry $M_{ji}(x)$ by $a_{ji}(x/y)y^{b_j - a_i}$. Then $G(\varphi)$ is given by M'.

By construction, the following is now clear.

Proposition 1.24. *The functors F and G defined above are quasi-inverse equivalences.*

1.7 Commutative algebra over explicitly given fields

In this section, we consider certain constructions in commutative algebra. We present k-algebras of finite type as in Section 1.5.2.

1.7.1 Localisations

For an element $f \in k[x_1, \dots, x_m]$ and an ideal I of $k[x_1, \dots, x_m]$, the localisation $\big(k[x_1, \dots, x_m]/I\big)_f$ of $k[x_1, \dots, x_m]$ is given by the morphism

$$k[x_1, \dots, x_m]/I \to k[x_1, \dots, x_m, x_{m+1}]/\big(I + (x_{m+1}f - 1)\big)$$

sending x_i to x_i (for $i = 1, 2, \dots, m$).

1.7.2 Equality of radicals of ideals

Given two ideals I, J of $k[x_1, \ldots, x_m]$, we can test algorithmically whether their radicals are equal using an effective Nullstellensatz, like the following theorem by Kollár.

Theorem 1.25 (Kollár [26, Cor. 1.7])**.** *Let k be a field, and let $f_1, \ldots, f_s \in k[x_1, \ldots, x_m]$ and let d be the maximum of 3 and their degrees. Then for all $h \in \sqrt{(f_1, \ldots, f_s)}$ there exist a positive integer $t \leq 2d^m$ and $g_1, \ldots, g_s \in k[x_1, \ldots, x_m]$ such that*

$$h^t = g_1 f_1 + \cdots + g_s f_s$$

with $\deg g_i f_i \leq (1 + \deg h) 2d^m$.

In fact, if we weaken the condition in the last line to $\deg g_i f_i \leq (1 + 2d^m \deg h) 2d^m$, then we can take $t = 2d^m$. Therefore checking whether a polynomial lies in the radical of some ideal of $k[x_1, \ldots, x_m]$ boils down to solving a large system of linear equations.

1.7.3 Tensor products

Let $A = k[x_1, \ldots, x_m]/I$, $B = k[y_1, \ldots, y_n]/J$, $C = k[z_1, \ldots, z_p]/K$. Let $\varphi\colon A \to B$ and $\psi\colon A \to C$ be morphisms of k-algebras. Then the tensor product $B \otimes_A C$ is given by

$$\frac{k[x_1, \ldots, x_m, y_1, \ldots, y_n, z_1, \ldots, z_p]}{I + J + K + \big(\varphi(x_1) - x_1, \ldots, \varphi(x_m) - x_m, \psi(x_1) - x_1, \ldots, \psi(x_m) - x_m\big)}$$

together with the obvious morphisms $B \to B \otimes_A C$ and $C \to B \otimes_A C$.

1.7.4 Other algorithms

We list some more algorithms we will make use of, namely those for *Noether normalisation* and *primary decomposition*.

Theorem 1.26 (Nagata [32])**.** *There exists an algorithm that takes as input an explicitly given field k and a k-algebra A of finite type, and outputs an injective integral morphism $k[x_1, \ldots, x_m] \to A$ in an effectively bounded number of field operations.*

Theorem 1.27 (Gianni et al. [15])**.** *There exists an algorithm that takes as input a factorial field k and an ideal $I \subseteq k[x_1, \ldots, x_m]$, and outputs a primary decomposition of I in an effectively bounded number of field operations.*

Remark 1.28. We remark that the algorithm by Gianni et al. [15] a priori is not primitive recursive because of the use of an unbounded search at two points, namely Proposition 3.7 and Proposition 8.2. Fortunately, in the case that we need, this can be amended, as explained below.

First, the unbounded search in Proposition 3.7 collapses, as we only need the case that $p = 0$. Moreover, we note that the crucial step in Proposition 8.2 in the case that we need, is the following: given ideals I, J of $k[x_1, \ldots, x_n]$ and $s \in k[x_1, \ldots, x_n]$, compute a positive integer m such that $s^m J \subseteq I$ if one exists. This can be done primitive recursively by first computing $I : J$ (using Gröbner bases) and then checking if $s \in \sqrt{I : J}$, using an effective Nullstellensatz like the one by Kollár [26] mentioned above.

Moreover, replacing every occurrence of a factorisation in their algorithm by an absolute factorisation will give an algorithm computing an *absolute* primary decomposition (i.e. a primary decomposition over $\bar{k}$) instead.

1.8 Schemes of finite type over a field

1.8.1 Affine schemes

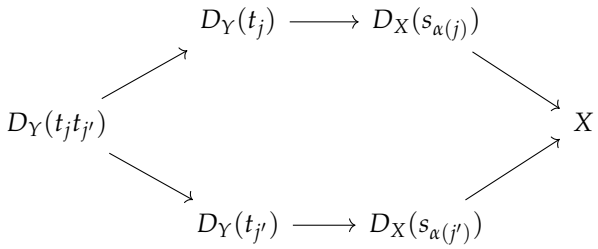
The category of affine schemes of finite type over a field k is just the opposite of the category of k-algebras of finite type, so we present an affine scheme X of finite type over k by its ring $\mathcal{O}(X)$ of global sections, and a morphism $Y \to X$ of affine schemes of finite type over k by the morphism $\mathcal{O}(X) \to \mathcal{O}(Y)$ of k-algebras. For an affine scheme X and $s \in \mathcal{O}(X)$, we will denote by $D_X(s)$ the standard open subscheme of X defined by s.

Note that we can compute fibre products of affine schemes.

1.8.2 Quasi-affine schemes

We present a quasi-affine scheme U of finite type over k by an affine scheme X of finite type over k, together with a finite sequence $s_1, \ldots, s_m \in \mathcal{O}(X)$ of elements generating an ideal defining the complement of U in X. Note that we can view an affine scheme X as a quasi-affine scheme presented by $(X, 1)$. We can test algorithmically whether two such presentations define the same open subscheme of a fixed scheme X, since this boils down to checking that two ideals have the same radical.

Suppose the quasi-affine schemes U and V are presented by tuples $(X, s_1, \ldots, s_m)$ and $(Y, t_1, \ldots, t_n)$, respectively. A morphism $V \to U$ with respect to the given presentations is then given by a map $\alpha\colon \{1, \ldots, n\} \to \{1, \ldots, m\}$ and morphisms $D_Y(t_j) \to D_X(s_{\alpha(j)})$ such that the following diagram commutes for all j and j' in $\{1, \ldots, n\}$.



Note that for any morphism $f\colon V \to U$ where $U \subseteq X$ and $V \subseteq Y$ are open subschemes with X and Y affine and of finite type over k, there exist presentations of U and V such that f can be given with respect to those presentations.

We want to be able to compute compositions of composable morphisms and test whether two morphisms are equal. To this end, we first explain how to compute the fibre product of two quasi-affine schemes.

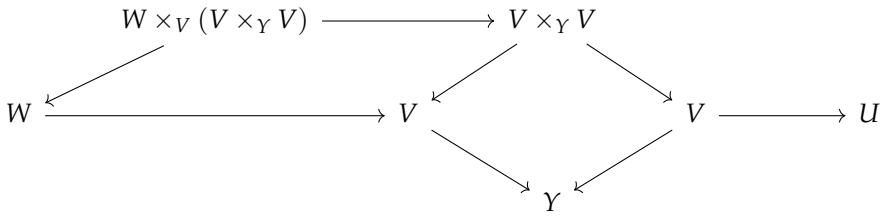
Suppose that the quasi-affine schemes U, V, W are given by tuples $(X, s_1, \ldots, s_m)$, $(Y, t_1, \ldots, t_n)$, $(Z, u_1, \ldots, u_p)$, respectively, and let $V \to U$ and $W \to U$ be morphisms with respect to the given presentations. Then by the classical construction of fibre

products of schemes, we see that $V \times_U W$ is given by

$$(Y \times_X Z, t_j u_k)$$

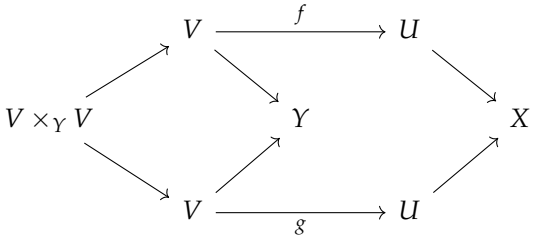
(with (j,k) running through all pairs such that the images of j and k in $\{1,\dots,m\}$ are the same). We have obvious projection morphisms $V \times_U W \to V$ and $V \times_U W \to W$ with respect to the given presentations.

Now let U, V, W be quasi-affine schemes, and let $f\colon V \to U$ and $g\colon W \to V$ be morphisms. Suppose that V is given as an open subscheme of the affine scheme Y, and view the presentations of V used for f and g as morphisms $V \to Y$ of quasi-affine schemes. We can then compute the composition fg using the following diagram, in which we do not simplify the expression $V \times_Y V$ as both factors are in general given by distinct presentations.

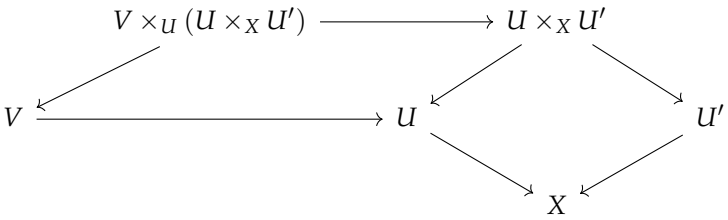


The composition fg then is the morphism $W \times_V (V \times_Y V) \to U$ in the diagram above.

In a similar vein, if U and V are quasi-affine schemes, given as open subschemes, of the affine schemes X and Y, respectively, and $f, g\colon V \to U$ are morphisms, then we can test whether $f = g$ since this is the case if and only if the following diagram commutes.



Finally, suppose that U, U' are both open subschemes of an affine scheme X, that V is an open subscheme of an affine scheme Y, and that $f\colon V \to U$ is a morphism of schemes. We can test whether the image of f is contained in U' by considering the diagram



and testing that $V \times_U (U \times_X U')$ (which is given as an open subscheme of the scheme $Y \times_X X = Y$) is the same as V. Moreover, we see that if the image of f is contained in U', then the diagram above gives a way to compute a presentation of the induced morphism $V \to U'$.

1.8.3 Presentations of schemes

A scheme of finite type over k is presented by gluing data:

- affine schemes $X_1, \dots, X_m$ of finite type over k;
- for all $i, j \in \{1, \dots, m\}$ an open subscheme $X_{ij} \subseteq X_i$ such that $X_{ii} = X_i$ for all $i \in \{1, \dots, m\}$;
- for all $i, j \in \{1, \dots, m\}$ a morphism $\varphi_{ji} \colon X_{ij} \to X_{ji}$ of quasi-affine schemes, such that φ_{ii} is the identity on X_i for all $i \in \{1, \dots, m\}$, and such that the *cocycle condition* holds, i.e.:
  for all $i, j, k \in \{1, \dots, m\}$, the image of $X_{ij} \times_{X_i} X_{ik}$ under φ_{ji} is contained in X_{jk}, and the diagram

$$\begin{array}{ccc} X_{ij} \times_{X_i} X_{ik} & \xrightarrow{\varphi_{ji}} & X_{ji} \times_{X_j} X_{jk} \\ & {\scriptstyle \varphi_{ki}} \searrow \quad \swarrow {\scriptstyle \varphi_{kj}} & \\ & X_{ki} \times_{X_k} X_{kj} & \end{array}$$

  is commutative.

We will denote such a presentation by the shorthand $(X_1, \dots, X_m)$.

Note that the cocycle condition for $i = k$ implies that $\varphi_{ji} = \varphi_{ij}^{-1}$ for all i, j in $\{1, \dots, m\}$ and that the induced morphism $\varphi_{ji} \colon X_{ij} \times_{X_i} X_{ik} \to X_{ji} \times_{X_j} X_{jk}$ is an isomorphism for all $i, j, k \in \{1, \dots, m\}$.

A morphism $(Y_1, \dots, Y_n) \to (X_1, \dots, X_m)$ of presentations of schemes of finite type over k is given by a map $\alpha \colon \{1, \dots, n\} \to \{1, \dots, m\}$, morphisms $f_j \colon Y_j \to X_{\alpha(j)}$, and morphisms $f_{jj'} \colon Y_{jj'} \to X_{\alpha(j)\alpha(j')}$ compatible with gluing data. More precisely, the following diagrams commute for all $j, j' \in \{1, \dots, n\}$.

$$\begin{array}{ccc} Y_{jj'} & \xrightarrow{f_{jj'}} & X_{\alpha(j)\alpha(j')} \\ \downarrow & & \downarrow \\ Y_j & \xrightarrow[f_j]{} & X_{\alpha(j)} \end{array} \qquad \begin{array}{ccc} Y_{jj'} & \xrightarrow{f_{jj'}} & X_{\alpha(j)\alpha(j')} \\ {\scriptstyle \varphi_{j'j}}\downarrow & & \downarrow{\scriptstyle \varphi_{\alpha(j')\alpha(j)}} \\ Y_{j'j} & \xrightarrow[f_{j'j}]{} & X_{\alpha(j')\alpha(j)} \end{array}$$

First note that we can algorithmically determine whether two morphisms of presentations of schemes define the same morphism between the schemes that they present, by the following.

Lemma 1.29. *Let $f, g \colon (Y_1, \dots, Y_n) \to (X_1, \dots, X_m)$ be morphisms between presentations of schemes (with α, β the corresponding maps on indices). Then they define the same morphism of schemes if and only if the following holds: for all $j \in \{1, \dots, n\}$, the projections*

$Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ and $Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ are isomorphisms and the compositions $Y_j \to Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)}$ and $Y_j \to Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)}$ of the respective inverses and the projections are equal.

Proof. In this proof, we will identify the $X_i, X_{ii'}, Y_j, Y_{jj'}$ with the open subschemes of the schemes they define.

First suppose that f, g define the same morphism of schemes. Then, for all j, the image of Y_j lies in $X_{\alpha(j)}$ and $X_{\beta(j)}$, and therefore in $X_{\alpha(j)\beta(j)}$. Hence the projections $Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ and $Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ are isomorphisms. Moreover, the morphism $Y_j \to X_{\alpha(j)\beta(j)}$ induced by f_j now is the composition

$$Y_j \to Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)},$$

and the one induced by g_j is the composition

$$Y_j \to Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)},$$

so these two must be equal.

Conversely, suppose that the projection morphisms $Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ and $Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to Y_j$ are isomorphisms for all $j \in \{1, \dots, n\}$, and that the compositions

$$Y_j \to Y_j \times_{X_{\alpha(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)}$$

and

$$Y_j \to Y_j \times_{X_{\beta(j)}} X_{\alpha(j)\beta(j)} \to X_{\alpha(j)\beta(j)}$$

of the respective inverses and the projections are equal. The first condition implies that the image of every Y_j under both f and g lies in $X_{\alpha(j)\beta(j)}$, and the second condition then implies that the resulting morphisms $Y_j \to X_{\alpha(j)\beta(j)}$ are equal. Since the Y_j cover Y, it follows that f and g define the same morphism of schemes. □

Note that we can also compute algorithmically compositions of morphisms of presentations of schemes. Moreover, if $(X_1, \dots, X_m)$, $(Y_1, \dots, Y_n)$, $(Z_1, \dots, Z_p)$ are presentations of schemes X, Y, Z, respectively, and $(Y_1, \dots, Y_n) \to (X_1, \dots, X_m)$ and $(Z_1, \dots, Z_p) \to (X_1, \dots, X_m)$ are morphisms of presentations, then the construction of fibre products of schemes gives a way to compute a presentation of the fibre product $Y \times_X Z$.

Next, we describe presentations of open subschemes of schemes. Let X be a scheme, presented as $(X_1, \dots, X_m)$. Then an open subscheme U of X is presented by a tuple $(U_1, \dots, U_n)$ together with a map $\alpha\colon \{1, \dots, n\} \to \{1, \dots, m\}$ and standard open subschemes $U_j \to X_{\alpha(j)}$ for all $j \in \{1, \dots, n\}$.

The corresponding description of U as a scheme is then given by the additional data of the intersections, which can be computed as the open subscheme

$$U_{jj'} = (U_j \times_{X_{\alpha(j)}} X_{\alpha(j)\alpha(j')}) \times_{U_j} \varphi_{j'j}^{-1}(U_{j'} \times_{X_{\alpha(j')}} X_{\alpha(j')\alpha(j)})$$

of U_j, together with the isomorphisms $U_{jj'} \to U_{j'j}$ induced by $\varphi_{j'j}^{-1}$. We then have an obvious morphism $U \to X$ given with respect to the given presentations.

Note that we can test algorithmically whether $U = X$ by testing that for all i in $\{1, \ldots, m\}$, the union in the affine scheme X_i over all $j \in \{1, \ldots, n\}$ of the open subschemes $\varphi^{-1}_{\alpha(j)i}(U_j \times_{X_{\alpha(j)}} X_{\alpha(j)i})$ is X_i itself.

Let us call a presentation of such an open subscheme $U = X$ of X a *refinement*; these present the identity morphism on X. Now note that with the same methods as in the case of quasi-affine schemes, if two morphisms $Z \to Y$ and $Y \to X$ are given, together with a chain of refinements connecting the target of the former to the source of the latter, one can compute the composition $Z \to X$. Moreover, again with the same methods as in the case of quasi-affine schemes, if two morphisms $Y \to X$ are given, together with a chain of refinements connecting the targets, and one connecting the sources, one can test whether these two morphisms are equal.

1.8.4 Finite étale morphisms of schemes

Let $(X_1, \ldots, X_m)$ be a presentation of a scheme X. Then we present a finite étale X-scheme (or equivalently, a finite locally constant sheaf on $X_{\text{ét}}$) by a descent datum w.r.t. the open cover $\{X_i \to X\}$; more precisely, by the following data:

- for all $i \in \{1, \ldots, m\}$ a finite étale morphism $Y_i \to X_i$;
- for all $i, j \in \{1, \ldots, m\}$ a morphism $\psi_{ji} \colon Y_i \times_{X_i} X_{ij} \to Y_j \times_{X_j} X_{ji}$ lying over the morphism $\varphi_{ji} \colon X_{ij} \to X_{ji}$,

such that ψ_{ii} is the identity on Y_i for all i and such that the *cocycle condition* holds, i.e. for all $i, j, k \in \{1, \ldots, m\}$ the following diagram commutes

$$\begin{array}{ccc} Y_i \times_{X_i} X_{ij} \times_{X_i} X_{ik} & \xrightarrow{\psi_{ji}} & Y_j \times_{X_j} X_{ji} \times_{X_j} X_{jk} \\ & {\scriptstyle \psi_{ki}} \searrow \quad \swarrow {\scriptstyle \psi_{kj}} & \\ & Y_k \times_{X_k} X_{ki} \times_{X_k} X_{kj} & \end{array}$$

Note that a presentation as above in particular defines a (presentation) of a scheme Y, and a morphism $Y \to X$ with respect to the given presentations. A morphism $Z \to Y$ of finite étale X-schemes is therefore simply a commutative triangle

$$\begin{array}{ccc} Z & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

2 Euler-Poincaré characteristic of varieties

Let Λ be a finite ring that is injective as a Λ-module; the conditions here are used to apply Poincaré duality, at the end of Chapter 3. The main example we are interested in is $\Lambda = \mathbb{Z}/n\mathbb{Z}$. For a scheme X, let $\Lambda\text{-Mod}(X_{\text{ét}})$ denote the category of sheaves of (left) Λ-modules on $X_{\text{ét}}$, and let $\Lambda\text{-Mod}_c(X_{\text{ét}})$ denote the full subcategory of $\Lambda\text{-Mod}(X_{\text{ét}})$ of constructible sheaves of (left) Λ-modules. Let $D_\Lambda(X_{\text{ét}})$ and $D_{\Lambda,c}(X_{\text{ét}})$ denote the corresponding bounded derived categories.

For each morphism $f\colon Y \to X$ of separated schemes of finite type over a field, we have a triangulated morphism $Rf_!\colon D_{\Lambda,c}(Y_{\text{ét}}) \to D_{\Lambda,c}(X_{\text{ét}})$, and therefore an induced group morphism $\chi_{f!}(Y,-)\colon K_0\big(\Lambda\text{-Mod}_c(Y_{\text{ét}})\big) \to K_0\big(\Lambda\text{-Mod}_c(X_{\text{ét}})\big)$ between their Grothendieck groups, called the *(relative) Euler-Poincaré characteristic*. If X is the spectrum of the (context-dependent) base field, we will usually omit the morphism f from the notation; note that in this case $\chi_!(Y,\mathcal{M})$ is the alternating sum of the $H^q_c(Y_{k^{\text{sep}}},\mathcal{M})$.

In this chapter and the next, we prove the following.

Theorem 2.1. *There exists an algorithm that takes as input a morphism $f\colon X \to S$ of finite type, with S the spectrum of a factorial field k, a finite ring Λ of order coprime to the characteristic of k that is injective as a Λ-module, and a finite locally constant sheaf $\mathcal{M}$ of (left) Λ-modules, and outputs $\chi_!(X,\mathcal{M}) \in K_0\big(\Lambda\text{-Mod}_c(S_{ét})\big)$ in an effectively bounded number of field operations.*

In this chapter we will reduce to the case of a curve. More precisely, we assume for now the existence of the following algorithm (and that it is correct and halts in effectively bounded time), and come back to it in Chapter 3. (In fact, in Chapter 3 we will consider a slightly more general situation.)

Algorithm 2.2. *Suppose that given as input is a diagram*

$$\begin{array}{ccc} X & \xrightarrow{g} & U \\ & & \downarrow j \\ & & \mathbb{P}^1_k \end{array} \xrightarrow{\pi} \operatorname{Spec} k$$

where g is finite étale, j is a standard open immersion, k is an absolutely factorial field, together with a finite ring Λ of order coprime to the characteristic of k that is injective as a Λ-module, and a finite locally constant sheaf $\mathcal{M}$ of Λ-modules on $X_{ét}$. Write $f = \pi j g$.

Output: $R^0 f_!\mathcal{M}$, $R^1 f_!\mathcal{M}$, $R^2 f_!\mathcal{M}$.

The main idea of the reduction to the case of curves is to make the following classical results explicit.

(1) *Topological invariance of the small étale site (*SGA1 *[19, Exp. IX, 4.10]):* If the morphism $f\colon X' \to X$ is a universal homeomorphism (e.g. a finite locally free purely inseparable morphism), then the pullback functor
$$f^{-1}\colon \Lambda\text{-}\mathrm{Mod}(X_{\text{ét}}) \to \Lambda\text{-}\mathrm{Mod}(X'_{\text{ét}})$$
and the pushforward functor
$$f_*\colon \Lambda\text{-}\mathrm{Mod}(X'_{\text{ét}}) \to \Lambda\text{-}\mathrm{Mod}(X_{\text{ét}})$$
are quasi-inverse equivalences.

(2) If $i\colon Z \to X$ is a closed immersion into X with complement $j\colon U \to X$, then
$$\chi_!(X, \mathcal{M}) = \chi_!(U, j^{-1}\mathcal{M}) + \chi_!(Z, i^{-1}\mathcal{M}).$$

(3) If $g\colon Z \to Y$ and $f\colon Y \to X$ are morphisms of schemes, then we have $Rf_!Rg_! = R(fg)_!$ as functors from $D_{\Lambda,c}(Z_{\text{ét}}) \to D_{\Lambda,c}(X_{\text{ét}})$.

Let us first make some remarks on how we plan to use these results.

The intended usage of (2) should be clear; though we do remark that (2) guarantees that the computation can be done using only finite locally constant sheaves, since every constructible sheaf $\mathcal{M} \in \Lambda\text{-}\mathrm{Mod}_c(X_{\text{ét}})$ on a scheme X admits a stratification of X into locally closed subschemes, on all of which $\mathcal{M}$ is finite locally constant. This also allows us to extend the definition of $\chi_!(X, \mathcal{M})$ to all finite type schemes over k, in a well-defined way.

A consequence of (1) is that if $f\colon X' \to X$ is a finite locally free purely inseparable morphism and X, X' are separated schemes of finite type over a field, then we have
$$\chi_!(X, \mathcal{M}) = \chi_!(X', f^{-1}\mathcal{M}) \qquad \chi_!(X', \mathcal{M}') = \chi_!(X, f_*\mathcal{M}')$$
for all $\mathcal{M} \in \Lambda\text{-}\mathrm{Mod}_c(X_{\text{ét}})$ and $\mathcal{M}' \in \Lambda\text{-}\mathrm{Mod}_c(X'_{\text{ét}})$. This allows us to perform computations "up to universal homeomorphisms".

The Grothendieck spectral sequence applied to (3) gives us, for all morphisms $g\colon Z \to Y$, $f\colon Y \to X$ between separated schemes of finite type over a field and $\mathcal{M} \in \Lambda\text{-}\mathrm{Mod}_c(Z_{\text{ét}})$, the identity
$$\chi_{fg!}(Z, \mathcal{M}) = \chi_{f!}\big(Y, \chi_{g!}(Z, \mathcal{M})\big).$$
We will use this to inductively compute the Euler-Poincaré characteristic, using fibrations similar to that in Artin [1, Exp. XI, Sec. 3].

Finally, if we are to utilise Algorithm 2.2, we want to have a sufficient condition for a relative curve $f\colon X \to S$ between schemes of finite type over a field and a finite locally constant sheaf $\mathcal{M}$ to have finite locally constant $R^p f_!\mathcal{M}$; this is the subject of Section 2.3.

2.1 Generic computations on families

In this section, we consider several problems of the following form; given a morphism $f\colon Y \to X$ of affine schemes of finite type over a factorial field k with X integral, say with generic point η, such that $Y_\eta \to \eta$ has some property P, compute a

non-empty open subscheme U of X and a closed subscheme Z of X with complement U such that $f^{-1}(U) \to U$ has property P.

A simple example that will be useful for us is the following. Given a generically smooth morphism $f\colon Y \to X$ of affine schemes of finite type over a factorial field k with X integral, compute a non-empty open subscheme $U \subseteq X$ such that $f^{-1}(U)$ is smooth over U, and a complement Z of U in X.

In this case this computation is straightforward; we compute the inverse image in $\mathcal{O}(X)$ of the Jacobian ideal in $\mathcal{O}(Y)$, pick a non-zero element h of it, and we set $U = D_X(h)$ and $Z = V_X(h)$.

2.1.1 Decompositions of finite morphisms

Recall that any reduced finite algebra A over a field k is isomorphic to one of the form $l_1 \times \cdots \times l_n$ with the l_i finite field extensions of k, and that for all l_i we have a factorisation $k \to k_i \to l_i$ with k_i the separable closure of k in l_i.

We want to replicate this generically in a relative setting, i.e. given a generically finite morphism $f\colon Y \to X$ from an affine reduced scheme Y to an affine integral scheme X of finite type over a factorial field k, we want to compute a non-empty open affine subscheme $U \subseteq X$ for which $f^{-1}(U)$ decomposes as $V_1 \sqcup \ldots \sqcup V_n$ where each V_i is integral and admits a factorisation $V_i \to U_i \to U$ with V_i finite locally free and purely inseparable over U_i and U_i finite étale over U. In fact, the computation will also give an $\mathcal{O}(U_i)$-basis of $\mathcal{O}(V_i)$ and a $\mathcal{O}(U)$-basis of $\mathcal{O}(U_i)$.

We start by computing generically an $\mathcal{O}(X)$-basis of $\mathcal{O}(Y)$; for convenience, say that an *explicitly free* morphism is a finite locally free morphism $Y \to X$ (between affine schemes of finite type over k) such that $\mathcal{O}(Y)$ is free as an $\mathcal{O}(X)$-module, together with an $\mathcal{O}(X)$-basis for $\mathcal{O}(Y)$.

Algorithm 2.3. *Suppose that given as input is a generically finite morphism $f\colon Y \to X$ of affine schemes of finite type over k with X integral and Y reduced. We assume that $\mathcal{O}(Y)$ is given as $\mathcal{O}(X)[y_1, \ldots, y_n]/(g_1, \ldots, g_t)$.*

Output: $\big(f^{-1}(U) \to U, f^{-1}(Z)\big)$, where $U \subseteq X$ is a non-empty standard open subscheme such that $f^{-1}(U) \to U$ is explicitly free, and where Z is a closed subscheme of X with complement U.

- Compute a reduced Gröbner basis $(g'_1, \ldots, g'_{t'})$ of $(g_1, \ldots, g_t)$ in the polynomial ring $K(X)[y_1, \ldots, y_n]$ together with identities $g'_{i'} = \sum_i a_{i'i} g_i$ with $a_{i'i}$ in $K(X)[y_1, \ldots, y_n]$, such that every $g'_{i'}$ is monic.
- Using division with remainder, compute identities $g_i = \sum_{i'} b_{ii'} g'_{i'}$ with $b_{ii'}$ in $K(X)[y_1, \ldots, y_n]$.
- Let $K(Y) = \mathcal{O}(Y) \otimes_{\mathcal{O}(X)} K(X)$; let $B \subseteq K(Y)$ be the set of monomials in the y_i that are not divisible by any leading monomial of a $g'_{i'}$; this is a $K(X)$-basis of $K(Y)$.
- Let h be a non-zero element in $\mathcal{O}(X)$ that is a multiple of every denominator occurring in some $a_{i'i}$ or $b_{ii'}$.
- Set $U = D_X(h)$ and $Z = V_X(h)$.
- **Output** $f^{-1}(U) \to U$ (together with the $K(X)$-basis B), the scheme $f^{-1}(Z)$, and **halt**.

Proposition 2.4. *Algorithm 2.3 is correct and halts in an effectively bounded number of field operations.*

Proof. By construction of h we have $(g'_1, \ldots, g'_{t'}) = (g_1, \ldots, g_t)$ in $\mathcal{O}(U)[y_1, \ldots, y_n]$, and since we have chosen the $g'_{i'}$ to be monic, it follows that the $K(X)$-basis of $\mathcal{O}(Y) \otimes_{\mathcal{O}(X)} K(X)$ that is computed is an $\mathcal{O}(U)$-basis of $\mathcal{O}\big(f^{-1}(U)\big)$. □

We also have the following (one-dimensional) variant of this step.

Algorithm 2.5. *Suppose that given as input is a morphism $X \to \mathbb{A}^1_S$ of affine schemes of finite type over k with S integral and X reduced. We assume that X is generically over S finite locally free over $\mathbb{A}^1_S$, and that $\mathcal{O}(X)$ is given as $\mathcal{O}(S)[x][y_1, \ldots, y_n]/(g_1, \ldots, g_t)$.*

Output: $\big(f^{-1}(U) \to \mathbb{A}^1_U, f^{-1}(Z)\big)$, where $f\colon X \to S$ is the structure morphism, $U \subseteq S$ is a non-empty standard open subscheme such that $f^{-1}(U) \to \mathbb{A}^1_U$ is explicitly free, and where Z is a closed subscheme of X with complement U.

- Compute a reduced Gröbner basis $(g'_1, \ldots, g'_{t'})$ of $(g_1, \ldots, g_t)$ in the polynomial ring $K(S)[x][y_1, \ldots, y_n]$ together with identities $g'_{i'} = \sum_i a_{i'i} g_i$ with $a_{i'i} \in K(S)[x][y_1, \ldots, y_n]$, such that every $g'_{i'}$ has leading term (with respect to the y_i) of the form $h'_{i'} y_1^{e_1} \cdots y_n^{e_n}$ with $h'_{i'} \in K(S)[x]$ monic. This can be done with respect to any monomial ordering for which $y_1, \ldots, y_n > x^e$ for all positive integers e.
- Let h' be a non-zero element of $K(X)[x]$ that is a multiple of every $h'_{i'}$.
- Using division with remainder, compute identities $g_i = \sum_{i'} a'_{ii'} g'_{i'}$ with $a'_{ii'}$ in $K(S)[x][y_1, \ldots, y_n]$.
- Let $K(X) = \mathcal{O}(X) \otimes_{\mathcal{O}(S)[x]} K(S)[x]$; let $B \subseteq K(X)$ be the set of monomials in the y_i that are not divisible by any leading term of a $g'_{i'}$; let $B_{h'} \subseteq K(X)$ be the set of monomials in the y_i that are not divisible by any leading monomial of a $g'_{i'}$; then $B_{h'}$ is linearly independent over $K(S)[x]$, and $B_{h'} \cdot K(S)[x] \supseteq h'K(X)$.
- Compute a $K(S)[x]$-basis of the image of the multiplication-by-h'-map from $K(X)$ to $B_{h'} \cdot K(S)[x]$, and therefore a $K(S)[x]$-basis $c_1, \ldots, c_s$ of $K(X)$.
- Write $B = \{b_1, \ldots, b_r\}$ and compute for all j an identity $b_j = \sum_{j'} a''_{jj'} c_{j'}$ with $a''_{jj'} \in K(S)[x]$.
- Let h be a non-zero element in $\mathcal{O}(S)$ that is a multiple of every denominator occurring in some $a_{i'i}$, $a'_{ii'}$, $a''_{jj'}$, $h'_{i'}$, or $c_{j'}$.
- Set $U = D_S(h)$ and $Z = V_S(h)$.
- **Output** $f^{-1}(U) \to U$ (together with the $K(S)[x]$-basis C), the scheme $f^{-1}(Z)$, and **halt**.

Proposition 2.6. *Algorithm 2.5 is correct and halts in an effectively bounded number of field operations.*

Proof. By construction of h we have that $(g'_1, \ldots, g'_{t'}) = (g_1, \ldots, g_t)$ in the polynomial ring $\mathcal{O}(U)[x][y_1, \ldots, y_n]$, that $c_1, \ldots, c_s$ is defined over $\mathcal{O}(U)$, and that $c_1, \ldots, c_s$ is a $\mathcal{O}(U)[x]$-basis $\mathcal{O}\big(f^{-1}(U)\big)$. □

Now we can perform the construction of the decomposition.

Algorithm 2.7. *Suppose that given as input is an explicitly free morphism $f\colon Y \to X$ of affine schemes of finite type over k with X integral and Y reduced.*

Output: $\big((V_i \to U_i \to U)_i, f^{-1}(Z)\big)$, where $U \subseteq X$ is a standard open subscheme such that $f^{-1}(U) = \coprod_i V_i$, such that $V_i \to U_i$ is finite purely inseparable and explicitly free, $U_i \to U$ is finite étale and explicitly free, and where Z is a closed subscheme of X with complement U.

- Compute, in terms of the given basis, a $K(X)$-basis B of $K(Y)$ subordinate to a decomposition $K(Y) = \prod_i L_i$ together with factorisations $K(X) \to K_i \to L_i$, where the L_i are finite field extensions of $K(X)$, and K_i is the separable closure of $K(X)$ in L_i.
- Let d be the determinant of B and let Δ_i be the discriminant of $K_i/K(X)$.
- Let $h \in \mathcal{O}(X)$ be an element that is a multiple of:
  - every denominator occurring in B;
  - the numerator and the denominator of d;
  - the numerator and the denominator of every Δ_i.
- Set $U = D_X(h)$ and $Z = V_X(h)$
- **Output** the decomposition over U induced by the basis B of $K(Y)$, the scheme $f^{-1}(Z)$, and **halt**.

Proposition 2.8. *Algorithm 2.7 is correct and halts in an effectively bounded number of field operations.*

Proof. By construction. □

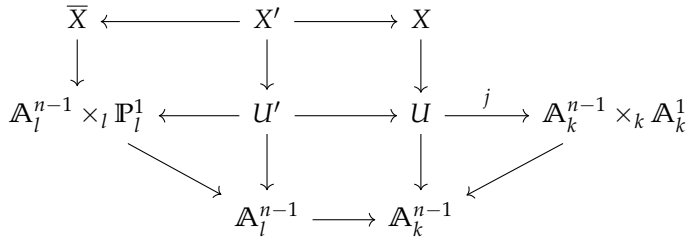
2.1.2 Smooth completions of curves

Another construction that we want to perform generically in a relative setting, is the following one.

Given a finite étale and explicitly free morphism $X \to U$, with U a standard affine non-empty open subscheme of $\mathbb{A}^1_k$, compute a finite purely inseparable extension l over k and a smooth curve $\overline{X}$, finite locally free over $\mathbb{P}^1_l$, such that $X_l = U_l \times_{\mathbb{P}^1_l} \overline{X}$; note that $\overline{X}$ is necessarily the normal completion of X_l over l (i.e. the unique proper normal curve over l with function field that of X_l). In general we cannot take $l = k$, as the following standard example (see e.g. Görtz and Wedhorn [16, Ex. 6.22]) shows.

Example 2.9. Let k be a non-perfect field of odd characteristic p, and let $\alpha \in k$ be an element that is not a p-th power in k. Let $U = \operatorname{Spec} k[x, 1/(x^p - \alpha)]$ and let $X = \operatorname{Spec} k[x, y, 1/(x^p - \alpha)]/(y^2 - x^p + \alpha)$. Then $X \to U$ is finite étale, and induces a finite locally free morphism from the normal completion $\overline{X}$ of X to $\mathbb{P}^1_k$. Above $\mathbb{A}^1_k$, the curve $\overline{X}$ is $\operatorname{Spec} k[x, y]/(y^2 - x^p + \alpha)$, which is not smooth at the point $(y, x^p - \alpha)$. So $\overline{X}$ is not smooth.

We explain how to perform this construction, simultaneously for the absolute and the relative setting. The situation is the following. We are given the right half of the following diagram.



Here, X is finite étale and explicitly free over U, and j is a standard open immersion. We wish to complete the diagram in such a way that all squares are cartesian, that $\overline{X} \to \mathbb{A}_l^{n-1} \times_l \mathbb{P}_l^1$ is generically over $\mathbb{A}_l^{n-1}$ finite locally free, that $\overline{X} \to \mathbb{A}_l^{n-1}$ is generically smooth, that the complement of X' in $\overline{X}$ is generically finite over $\mathbb{A}_l^{n-1}$, and that $\mathbb{A}_l^{n-1} \to \mathbb{A}_k^{n-1}$ is finite locally free purely inseparable.

We remark that we work here with open subschemes of $\mathbb{A}_k^n$ as base schemes; this is motivated by the future use of Noether normalisation in the computation.

Note we that we can perform computations over the perfect closure k^{perf} of a field k within the field k itself, using the fact that the Frobenius automorphism $k^{\mathrm{perf}} \to k^{\mathrm{perf}}$ induces an isomorphism $k^{1/p} \to k$; any finite set of elements of k^{perf} lies in some k^{1/p^e}, and we can keep track of this by keeping track of the integer e.

As an example, we describe the computation of radicals over k^{perf} using only computations in k, using the method of Matsumoto [30].

Example 2.10. Suppose that an ideal I of $k[x_1, \ldots, x_m]$ is given, and assume that k has characteristic p. We wish to compute the radical J of $\overline{k} \otimes I$ in $\overline{k}[x_1, \ldots, x_m]$. Note that by Theorem 1.25 (which is Kollár [26, Cor. 1.7]), we can compute a positive integer e such that if $h \in J$, then $h^{p^e} \in \overline{k} \otimes I$. This also shows that J is defined over k^{1/p^e}.

Denote by $\varphi\colon k^{\mathrm{perf}}[x_1, \ldots, x_m] \to k^{\mathrm{perf}}[x_1, \ldots, x_m]$ the morphism that raises all coefficients to the p-th power. Then note that by the above, $\varphi^e(J) \cap k[x_1, \ldots, x_m]$ is the radical of $\varphi^e|_{k[x_1,\ldots,x_m]}(I)$, which we compute in the usual way.

Returning to the problem at hand, note that a normal proper curve over a perfect field is automatically smooth, and it is defined by a finite number of elements of k^{perf}. Therefore we are done if we have a normalisation algorithm for proper curves over perfect fields, and in which each step commutes with taking the Frobenius automorphism on k^{perf}. Roughly speaking, any deterministic algorithm proceeding constructively should suffice; a more specific example would be that of Diem [10, Sect. 2.7]. Therefore we have the following.

Corollary 2.11. *There exists an algorithm that takes as input a proper curve X over a factorial field k together with a finite locally free morphism $X \to \mathbb{P}_{k'}^1$, computes a finite purely inseparable extension l over k, a smooth proper curve Y over k, and the normalisation map $Y \to X_l$ (over $\mathbb{P}_l^1$), in an effectively bounded number of field operations.*

In case of a function field of the form $k(x_1, \ldots, x_{n-1})$, we can even take the extension to be of the form $l(x_1^{1/q}, \ldots, x_{n-1}^{1/q})$ with l a finite purely inseparable extension of k. This gives rise to the following.

Algorithm 2.12. *Suppose that given as input is a finite étale and explicitly free morphism $X \to U$ of affine schemes of finite type over k with $U \subseteq \mathbb{A}^n_k$ a non-empty standard affine open subscheme.*

Output: $(V \to \mathbb{A}^{n-1}_k, \overline{X}_0 \to \mathbb{A}^1_V, \overline{X}_1 \to \mathbb{A}^1_V, Z \to X)$*, where:*

- $V \to \mathbb{A}^{n-1}_k$ *factors as* $V \to S \to \mathbb{A}^{n-1}_k$ *with* $V \to S$ *a standard open immersion and* $S \to \mathbb{A}^{n-1}_k$ *finite locally free purely inseparable, such that* $S \to \operatorname{Spec} k$ *factors through a smooth morphism* $S \to \operatorname{Spec} l$ *with* l *a finite purely inseparable field extension of* k*;*
- $\overline{X}_0, \overline{X}_1$ *are schemes, finite locally free over the standard open cover of* $\mathbb{P}^1_V$ *that coincide with* X *on* $U \times_{\mathbb{A}^n_k} \mathbb{A}^1_V$ *and that define a scheme smooth over* V*;*
- Z *is a complement of* $X \times_{\mathbb{A}^{n-1}_k} V$ *in* $X \times_{\mathbb{A}^{n-1}_k} S$*.*

(So $Z \to X$ is the composition of a finite locally free purely inseparable morphism and a closed immersion.)

- Compute a field extension of $k(x_1, \ldots, x_{n-1})$ of the form $L = l(x_1^{1/q}, \ldots, x_{n-1}^{1/q})$ with l a finite purely inseparable extension of k, such that the normal completion of the fibre of X above $\operatorname{Spec} L$ is smooth, using Corollary 2.11; let A_0 denote the resulting finite free $L[x_n]$-algebra with basis $u_1, \ldots, u_s$, and let A_1 denote the resulting finite free $L[x_n^{-1}]$-algebra with basis $v_1, \ldots, v_s$.
- Compute a multiple $h \in l[x_1^{1/q}, \ldots, x_{n-1}^{1/q}]$ of every denominator occurring:
  - in a coefficient of 1 and the $u_i u_j$ as linear combinations of $u_1, \ldots, u_s$;
  - in a coefficient of 1 and the $v_i v_j$ as linear combinations of $v_1, \ldots, v_s$

  (in other words, the equations defining A_0 and A_1 over L).
- Let S be the $\mathbb{A}^{n-1}_k$-scheme $\operatorname{Spec} l[x_1^{1/q}, \ldots, x_{n-1}^{1/q}]$, and let V' be $D_S(h)$.
- Let A_0' be the finite free $l[x_1^{1/q}, \ldots, x_{n-1}^{1/q}, 1/h, x_n]$-algebra defined by the same equations as A_0.
- Similarly, let A_1' be the finite free $l[x_1^{1/q}, \ldots, x_{n-1}^{1/q}, 1/h, x_n^{-1}]$-algebra defined by the same equations as A_1.
- Let V be the intersection of the open subschemes of V' obtained by applying Algorithm 2.5 to the subschemes of $\operatorname{Spec} A_0'$ (resp. $\operatorname{Spec} A_1'$) defined by the Jacobian ideals.
- Compute the complement Z of $X \times_{\mathbb{A}^{n-1}_k} V$ in $X \times_{\mathbb{A}^{n-1}_k} S$.
- **Output** $V \to \mathbb{A}^{n-1}_k$, $\operatorname{Spec} A_0' \times_{\mathbb{A}^1_S} \mathbb{A}^1_V \to \mathbb{A}^1_V$, $\operatorname{Spec} A_1' \times_{\mathbb{A}^1_S} \mathbb{A}^1_V \to \mathbb{A}^1_V$, and $Z \to X$, and **halt**.

Proposition 2.13. *Algorithm 2.12 is correct and halts in an effectively bounded number of field operations.*

Proof. Note that as A_0 and A_1 are smooth over L, the function field of V', it follows that the Jacobian ideals of A_0' and A_1' over $l[x_1^{1/q}, \ldots, x_{n-1}^{1/q}, 1/h]$ generically define the empty scheme, so the locus V computed is the locus in V' where both $\operatorname{Spec} A_0'$ and $\operatorname{Spec} A_1'$ are smooth. The rest follows by construction. □

2.2 The (relative) 0-dimensional case

Let us now consider the computation of the Euler-Poincaré characteristic in the relative zero-dimensional case. First, we relate pushforwards of sheaves along a finite locally free morphism f to Weil restrictions (see e.g. Bosch et al. [3, Sec. 7.6]) along f.

Lemma 2.14. *Let $f\colon Y \to X$ be a finite locally free morphism of schemes, and let $\mathcal{F}$ be a finite locally constant sheaf on $Y_{ét}$, viewed as its representing finite étale Y-scheme. Then $f_*\mathcal{F}$ is represented by the Weil restriction $\operatorname{Res}_X^Y \mathcal{F}$ of $\mathcal{F}$ to X.*

Proof. Using the functor of points, it is easy to see that $\operatorname{Res}_X^Y \mathcal{F}$ is formally étale and locally of finite presentation over X, therefore étale. It follows that it also represents the functor $X_{ét}^{\mathrm{op}} \to \mathrm{Set}$ given by $U \mapsto \operatorname{Hom}_Y(Y \times_X U, \mathcal{F})$, i.e. it represents $f_*\mathcal{F}$. □

So the computation of pushforwards of sheaves along a finite locally free morphism $f\colon Y \to X$ amounts to a computation of a Weil restriction along f; in the case that we are also given a $\mathcal{O}(X)$-basis of $\mathcal{O}(Y)$, this computation is well-known in our situation, but we include it here for completeness.

Algorithm 2.15. *Suppose that given on input is an effective field k, a finite type k-algebra A, a finite free A-algebra B, together with an A-basis $t_1, \dots, t_n$ of B, and let $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$. Moreover, suppose that given on input is a finite locally constant sheaf $\mathcal{F}$ on $Y_{ét}$, given as a finite locally free B-algebra by $B[x_1, \dots, x_m]/(f_1, \dots, f_s)$.*

Output: the pushforward of $\mathcal{F}$ along $Y \to X$.

- Let x_{ij} be variables for $i \in \{1, \dots, m\}$, $j \in \{1, \dots, n\}$.
- Compute the set I of coefficients of all

$$f_k\left(\sum_j x_{1j}t_j, \dots, \sum_j x_{mj}t_j\right)$$

  with respect to the A-basis $t_1, \dots, t_j$ of B.
- Return (the spectrum of) $A[x_{ij}]/I$.

From the given construction of $\operatorname{Res}_X^Y \mathcal{F}$, it is also clear how to construct, given a morphism $S \to \operatorname{Res}_X^Y \mathcal{F}$ of X-schemes, the corresponding morphism $S \times_X Y \to \mathcal{F}$.

Remark 2.16. If $f\colon Y \to X$ is finite étale, then $\operatorname{Res}_X^Y \mathcal{F}$ is finite étale over X; this is Bosch et al. [3, Prop. 7.6.5(f)], but can now also be seen as a consequence of proper smooth base change. If $f\colon Y \to X$ is a universal homeomorphism, then by topological invariance of the small étale site, $\operatorname{Res}_X^Y \mathcal{F}$ is finite étale over X.

Note that Res_X^Y in general does not send finite Y-schemes to finite X-schemes; an example is given by $X = \operatorname{Spec} \mathbb{F}_3[t]$, $Y = \operatorname{Spec} \mathbb{F}_3[t^{\frac{1}{3}}]$, $Z = \operatorname{Spec} \mathbb{F}_3[t^{\frac{1}{6}}]$; then we obtain $\operatorname{Res}_X^Y Z = \operatorname{Spec} \mathbb{F}_3[t, t^{-\frac{1}{2}}]$ using Algorithm 2.15 applied to the $\mathbb{F}_3[t]$-basis $1, t^{\frac{1}{3}}, t^{\frac{2}{3}}$ of $\mathbb{F}_3[t^{\frac{1}{3}}]$, and the functorial bijection

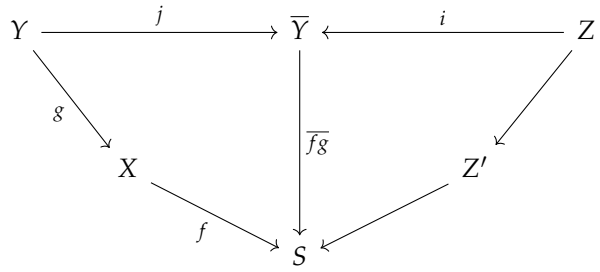
$$\operatorname{Hom}_{\mathbb{F}_3[t]}\left(\mathbb{F}_3[t, t^{-\frac{1}{2}}], A\right) \to \operatorname{Hom}_{\mathbb{F}_3[t^{\frac{1}{3}}]}\left(\mathbb{F}_3[t^{\frac{1}{6}}], A \otimes_{\mathbb{F}_3[t]} \mathbb{F}_3[t^{\frac{1}{3}}]\right)$$

is given by $f \mapsto (t^{\frac{1}{6}} \mapsto f(t^{-\frac{1}{2}})t^{\frac{2}{3}})$.

2.3 Higher derived images along relative curves

We show that under certain circumstances, the higher derived images of finite locally constant sheaves of Λ-modules are finite locally constant. We first define the condition needed, this is a variant of the notion of a *fibration élémentaire* of SGA4.3 [1, Exp. XI, Sec. 3].

Definition 2.17. Let $f\colon X \to S$ be a smooth curve between separated schemes of finite type over a field k, and let $\mathcal{M} \in \Lambda\text{-Mod}_c(X_{\text{ét}})$ be finite locally constant. Then f is said to be an *$\mathcal{M}$-elementary fibration* if there exists a commutative diagram



such that:

- j is an open immersion,
- i is a closed immersion with complement j,
- g is finite étale Galois (with respect to some finite group Γ),
- $\overline{fg}$ is smooth and proper,
- $Z \to Z'$ is finite locally free purely inseparable,
- $Z' \to S$ is finite étale,
- $g^{-1}\mathcal{M}$ is constant.

We can now state this section's main result precisely, as follows; we say that an object M of $D_{\Lambda,c}(X_{\text{ét}})$ (for a scheme X) has *finite locally constant cohomology* if $H^i(M)$ is finite locally constant for all i.

Theorem 2.18. *Let $f\colon X \to S$ be a smooth morphism of separated schemes of finite type over a field k, and let $\mathcal{M} \in \Lambda\text{-Mod}_c(X_{ét})$ be finite locally constant. Suppose that f is an $\mathcal{M}$-elementary fibration. Then $Rf_!\mathcal{M}$ has finite locally constant cohomology.*

We first include the following homological algebra lemma.

Lemma 2.19. *Let X be a scheme, and let*

$$\mathcal{M}_1 \longrightarrow \mathcal{M}_2 \longrightarrow \mathcal{M}_3 \longrightarrow \mathcal{M}_4 \longrightarrow \mathcal{M}_5$$

be an exact sequence in $\Lambda\text{-Mod}(X_{ét})$ Suppose that $\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_4, \mathcal{M}_5$ are finite locally constant. Then so is $\mathcal{M}_3$.

Proof. By SGA4.3 [1, Prop. IX.2.1], $\mathcal{M} \in \Lambda\text{-Mod}(X_{\text{ét}})$ is finite locally constant if and only if for all geometric points x_0, x_1 of X with x_0 a specialisation of x_1, the specialisation map $\mathcal{M}_{x_0} \to \mathcal{M}_{x_1}$ is an isomorphism. Considering for all geometric

points x_0, x_1 of X with x_0 a specialisation of x_1, the diagram

$$\begin{array}{ccccccccc} \mathcal{M}_{1,x_0} & \longrightarrow & \mathcal{M}_{2,x_0} & \longrightarrow & \mathcal{M}_{3,x_0} & \longrightarrow & \mathcal{M}_{4,x_0} & \longrightarrow & \mathcal{M}_{5,x_0} \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\ \mathcal{M}_{1,x_1} & \longrightarrow & \mathcal{M}_{2,x_1} & \longrightarrow & \mathcal{M}_{3,x_1} & \longrightarrow & \mathcal{M}_{4,x_1} & \longrightarrow & \mathcal{M}_{5,x_1}, \end{array}$$

shows that we are done by the Five Lemma. □

Corollary 2.20. *Let X be a scheme, and let $M, N, P \in D_{\Lambda,c}(X_{ét})$ be vertices of a triangle*

$$M \longrightarrow N \longrightarrow P \longrightarrow M[1].$$

If M and N have finite locally constant cohomology, then so does P.

Corollary 2.21. *Let X be a scheme, and let $E_{r\geq r_0}^{p,q}$ be a first-quadrant spectral sequence in $\Lambda\text{-}\mathrm{Mod}(X_{ét})$ converging to H^{p+q}. If all $E_{r_0}^{p,q}$ are finite locally constant, then so are all H^i.*

Now the proof of Theorem 2.18 follows from the following two lemmas.

Lemma 2.22. *Consider the following commutative diagram of schemes*

$$\begin{array}{ccccc} X & \xrightarrow{j} & \overline{X} & \xleftarrow{i} & Z \\ & \searrow^{f} & \downarrow{\scriptstyle \overline{f}} & \swarrow & \\ & & S & & \end{array}$$

where $\overline{f}$ is proper and smooth, j is an open immersion, and i is a closed immersion. Suppose moreover that $\overline{f}i$ is a composition $Z \to Z' \to S$ with $Z \to Z'$ finite locally free purely inseparable, and $Z' \to S$ finite étale. Let M be a finite Λ-module. Then $Rf_!M$ has finite locally constant cohomology.

Proof. Note that we have a canonical exact sequence

$$0 \longrightarrow j_!M \longrightarrow M \longrightarrow i_*M \longrightarrow 0.$$

Applying $R\overline{f}_*$ to it gives the triangle

$$Rf_!M \longrightarrow R\overline{f}_*M \longrightarrow R(\overline{f}i)_*M \longrightarrow (Rf_!M)[1].$$

As $\overline{f}$ is proper and smooth, it follows that $R\overline{f}_*M$ has finite locally constant cohomology, and as $\overline{f}i$ is the composition of a finite étale morphism and a universal homeomorphism, it follows that $R(\overline{f}i)_*M$ has finite locally constant cohomology. So by Corollary 2.20, it follows that $Rf_!M$ has finite locally constant cohomology as well, as desired. □

Lemma 2.23. *Let $g\colon Y \to X$ be a finite étale Galois morphism of schemes with Galois group Γ, and let $f\colon X \to S$ be a morphism of separated schemes of finite type over a field k. Let $\mathcal{M} \in \Lambda\text{-}\mathrm{Mod}_c(X_{ét})$ such that $R(fg)_!g^{-1}\mathcal{M}$ has finite locally constant cohomology. Then $Rf_!\mathcal{M}$ has finite locally constant cohomology.*

Proof. We employ some abuse of notation. Let i_Γ denote both the functor from $\Lambda[\Gamma]\text{-}\mathrm{Mod}_c(X_{\text{ét}})$ to $\Lambda\text{-}\mathrm{Mod}_c(X_{\text{ét}})$ and the one from $\Lambda[\Gamma]\text{-}\mathrm{Mod}_c(S_{\text{ét}})$ to $\Lambda\text{-}\mathrm{Mod}_c(S_{\text{ét}})$ sending $\mathcal{M}$ to the sheaf $\mathcal{M}^\Gamma$ of Γ-invariants. Note that $Ri_\Gamma\mathcal{M}$ has finite locally constant cohomology for any finite locally constant sheaf $\mathcal{M}$, and that we have $Ri_\Gamma Rg_!g^{-1}\mathcal{M} = R(i_\Gamma g_* g^{-1})\mathcal{M}$ (see e.g. Fu [13, Sec. 9.1]). Moreover, we have the identity $Ri_\Gamma Rf_! = Rf_! Ri_\Gamma$, so

$$Ri_\Gamma R(fg)_! g^{-1} = Ri_\Gamma Rf_! Rg_* g^{-1} = Rf_! R(i_\Gamma g_* g^{-1}) = Rf_!.$$

The corresponding Grothendieck spectral sequence is the *Hochschild-Serre spectral sequence*

$$E_2^{p,q} = \mathcal{H}^p(\Gamma, R^q f_! g_! g^{-1}\mathcal{M}) \Rightarrow R^{p+q} f_!\mathcal{M},$$

so by Corollary 2.21 it follows that $Rf_!\mathcal{M}$ has finite locally constant cohomology. □

As a corollary, we give an algorithm computing the pushforward along a smooth curve admitting an elementary fibration.

Algorithm 2.24. *Suppose that given as input is a curve $f\colon X \to S$ with S irreducible, smooth, and affine and $\mathcal{M} \in \Lambda\text{-}\mathrm{Mod}_c(X_{\text{ét}})$ on X. Assume that f admits an $\mathcal{M}$-elementary fibration.*

Output: a non-empty open standard subscheme $U \subseteq S$, a complement Z of $f^{-1}U$, and $R^i f_!\mathcal{A}|_U$ for $i = 0, 1, 2$.

- Compute the generic fibre Y_i of $R^i f_!\mathcal{A}$ over S as (the spectrum of) a finite free $K(S)$-algebra with basis $t_1, \ldots, t_s$.
- Compute a multiple $h \in \mathcal{O}(S)$ of every denominator occurring in the equations defining Y_i, and of the discriminant of Y_i over $K(S)$.
- **Output** $U = D_S(h)$, and for each i the finite étale U-scheme defined by the same equations as Y_i, together with the Λ-module structure, and **halt**.

Proposition 2.25. *Algorithm 2.24 is correct.*

Proof. We have established above that $R^i f_!\mathcal{A}$ over is S is finite locally constant, hence representable by a finite étale S-scheme. So once we have computed the generic fibre, the scheme is just the normalisation of S in $K(Y_i)$; which shows that there is a unique finite étale S-scheme with generic fibre Y_i. As the algorithm computes a finite étale U-scheme with generic fibre Y_i, it must be the finite étale U-scheme representing $R^i f_!\mathcal{A}|_U$. □

2.4 The algorithm

The main idea of the algorithm that follows will be to factor any finite type k-scheme (locally in the constructible topology, and up to universal homeomorphisms) into elementary fibrations, when given a finite locally constant sheaf on it. Note that we can (locally) compute pushforwards along universal homeomorphisms using Algorithm 2.15, and that we can compute higher direct images along elementary fibrations using Algorithm 2.24.

We will formulate the algorithm recursively. For clarity of exposition, we will not explicitly write out the partitioning of X into an open and a closed subscheme and

the recursive calls corresponding to them; instead we will indicate them by the word "generic" (or variations thereof).

Algorithm 2.26 (EPC)**.** *Suppose that given as input is a finite type k-scheme X, a finite ring Λ of order coprime to the characteristic of k that is injective as a Λ-module, and a finite locally constant sheaf $\mathcal{M}$ on X of Λ-modules.*

Output: $\chi_!(X, \mathcal{M})$.

- If X is not given as an affine scheme, say given by $(X_1, \dots, X_m)$ with $m \geq 2$, then **output** $\mathrm{EPC}(X_1, \mathcal{M}|_{X_1}) + \mathrm{EPC}(X - X_1, \mathcal{M}|_{X-X_1})$ and **halt**.
- If X is not reduced, then **output** $\mathrm{EPC}(X^{\mathrm{red}}, \mathcal{M}|_{X^{\mathrm{red}}})$ and **halt**.
- Compute a finite morphism $X \to \mathbb{A}_k^n$ by Noether normalisation.
- If $n = 0$, **output** the pushforward of $\mathcal{A}$ using Section 2.2, and **halt**.
- Compute generically a decomposition $X \to X' \to \mathbb{A}_k^n$ with $X' \to \mathbb{A}_k^n$ finite étale, $X \to X'$ is finite locally free purely inseparable using Section 2.1.1.
- If $n = 1$, let f be the structure morphism $X \to \operatorname{Spec} k$, **output** the alternating sum $R^0 f_! \mathcal{M} - R^1 f_! \mathcal{M} + R^2 f_! \mathcal{M}$ using the black box Algorithm 2.2, and **halt**.
- Compute a finite étale Galois morphism $g\colon Y \to X$ such that Y is connected and $g^{-1}\mathcal{M}$ is constant, say with value M.
- Compute generically a finite purely inseparable extension l over k, a finite locally free purely inseparable morphism $\mathbb{A}_l^{n-1} \to \mathbb{A}_k^{n-1}$, and a smooth completion $\overline{Y}$ of $Y \times_{\mathbb{A}_k^{n-1}} S$ as in Algorithm 2.12, with complement a composition of a finite étale morphism and a finite locally free purely inseparable morphism using Section 2.1.1.
- Compute the pullback $\mathcal{M}'$ of $\mathcal{M}$ along the projection $X \times_{\mathbb{A}_k^{n-1}} \mathbb{A}_l^{n-1} \to X$.
- Compute generically the higher direct images $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2$ of $\mathcal{M}'$ along the morphism $X \times_{\mathbb{A}_k^{n-1}} \mathbb{A}_l^{n-1} \to \mathbb{A}_l^{n-1}$ using Algorithm 2.24.
- Compute the pushforward $\mathcal{P}_0, \mathcal{P}_1, \mathcal{P}_2$ of $\mathcal{N}_0, \mathcal{N}_1, \mathcal{N}_2$, respectively along the morphism $\mathbb{A}_l^{n-1} \to \mathbb{A}_k^{n-1}$ using Section 2.1.1.
- **Output** $\mathrm{EPC}(\mathbb{A}_k^{n-1}, \mathcal{P}_0) - \mathrm{EPC}(\mathbb{A}_k^{n-1}, \mathcal{P}_1) + \mathrm{EPC}(\mathbb{A}_k^{n-1}, \mathcal{P}_2)$ and **halt**.

Proposition 2.27. *Algorithm 2.26 is correct and halts in effectively bounded time.*

Proof. Correctness follows by construction, taking into account the dévissage techniques mentioned in the beginning of this chapter, and Section 2.3. Moreover, it halts in effectively bounded time, as each step does, and as the total number of steps is bounded exponentially in the dimension of X; each recursive call reduces the dimension of X by 1, and the number of such calls per loop is bounded by a constant. □

2.5 Application: Counting points on varieties

In this section, we describe how to reduce the computation of the number $\#X(\mathbb{F}_q)$ of $\mathbb{F}_q$-points of a finite type scheme X to the computation of $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ for primes ℓ. More precisely, we prove the following proposition.

Proposition 2.28. *Let X be a finite type scheme. There exists an algorithm that takes as input a prime power q and a prime ℓ coprime to q, and outputs $\#X(\mathbb{F}_q) \bmod \ell$ in effectively bounded time, which for fixed ℓ is polynomial in $\log q$.*

If there exists an algorithm that takes as input a prime ℓ, and computes $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ in time polynomial in ℓ, then there exists an algorithm as above with complexity polynomial in ℓ and $\log q$.

Corollary 2.29. *Let X be a finite type scheme. If there exists an algorithm that takes as input a prime ℓ, and computes $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ in time polynomial in ℓ, then there exists an algorithm that takes as input a prime power q and outputs $\#X(\mathbb{F}_q)$ in time polynomial in $\log q$.*

Proof. We use the same trick that is used also in Schoof [35] to compute the number of $\mathbb{F}_q$-points of elliptic curves in time polynomial in $\log q$. Note that we have a trivial upper bound for $\#X(\mathbb{F}_q)$ that is polynomial in q; we assume that X is given by gluing data, so that we have an open cover $\{X_1, \dots, X_m\}$ of affine schemes, given as closed subschemes of $\mathbb{A}^n$ for some fixed n. Hence we have a trivial upper bound $\#X(\mathbb{F}_q) \leq mq^n$. Therefore we can apply the aforementioned trick of computing the number $\#X(\mathbb{F}_q)$ modulo $mq^n + 1$, by using the Chinese Remainder Theorem and computing $\#X(\mathbb{F}_q)$ modulo ℓ for a finite set of primes such that $\prod_\ell \ell \geq mq^n + 1$; by the prime number theorem, we can take a set of primes that are bounded polynomially in $\log q$. □

We will mainly focus on the proof of the second part of Proposition 2.28. So let X be a finite type scheme, and suppose that there exists an algorithm that takes as input a prime ℓ, and outputs $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ in time polynomial in ℓ. We describe how to compute in time polynomial in $\log q$ the number $\#X(\mathbb{F}_q)$ of $\mathbb{F}_q$-points of X under this assumption.

Note that X itself is not part of the input of the algorithm to be constructed, so we can allow ourselves any amount of extra data that only depends on X. We start by describing this data.

Recall that the *Grothendieck group of finite type schemes* is the quotient of the free abelian group generated by the isomorphism classes of finite type schemes by the subgroup generated by the following:

- $[X'] - [X]$ for every universal homeomorphism $X' \to X$;
- $[X] - [U] - [Z]$ for every closed subscheme $Z \subseteq X$ with complement U.

By the standard dévissage techniques for étale cohomology, we see that the étale Euler-Poincaré characteristic $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ only depends on the class of X in the Grothendieck group.

By generically factoring finite type schemes into relative curves, using the same techniques as in the previous sections, we see that the following holds.

Proposition 2.30. *Let X be a finite type scheme. Then there exist finite type schemes X_i that either are proper smooth over $\operatorname{Spec}\mathbb{F}_p$ for some prime p, or proper smooth over $\operatorname{Spec}\mathbb{Z}[1/N]$ for some N squarefree, and integers a_i such that $[X] = \sum_i a_i[X_i]$.*

Let S_X denote the set of primes that either occur in some $\mathbb{F}_p$, or as a divisor of some N. We will assume that an expression of the form $[X] = \sum_i a_i[X_i]$ for X as in

Proposition 2.30 is given, and let $f_i\colon X_i \to \operatorname{Spec}\mathbb{Z}$ be the structure morphism; the finite set S_X can then be easily computed from it.

We will now use the *Lefschetz trace formula* to compute $\#X(\mathbb{F}_q)$ modulo ℓ in time polynomial in ℓ. First, note that we have the following.

Proposition 2.31. *For all primes $p \neq \ell$ such that $p \notin S_X$, we have*

$$\chi_!(X_{\mathbb{F}_p}, \mathbb{Z}/\ell\mathbb{Z})(\mathbb{F}_p^{\mathrm{sep}}) = \chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})(\mathbb{Q}^{\mathrm{sep}})$$

in $K_0(\mathbb{Z}/\ell\mathbb{Z})$.

Proof. Let N be the product of ℓ and all primes in S_X. Note that

$$\begin{aligned}\chi_!(X_{\mathbb{Z}[1/N]}, \mathbb{Z}/\ell\mathbb{Z}) &= \sum_i a_i \chi_!(X_{i,\mathbb{Z}[1/N]}, \mathbb{Z}/\ell\mathbb{Z}) \\ &= \sum_i a_i \sum_q (-1)^q R^q (f_{i,\mathbb{Z}[1/N]})_!(\mathbb{Z}/\ell\mathbb{Z})\end{aligned}$$

is a sum of finite locally constant sheaves of $\mathbb{Z}/\ell\mathbb{Z}$-modules on $\operatorname{Spec}\mathbb{Z}[1/N]$ by proper smooth base change, and the result follows. □

Next, we recall the definition of the trace.

Definition 2.32. Let k be a field, let Λ be a (not necessarily commutative) k-algebra, let $\lambda \in \Lambda$, and let M be a Λ-module that is finite as a k-module. Then the *trace* $\operatorname{Tr}(\lambda; M) \in k$ is the trace (as k-linear map) of the endomorphism $M \to M$ given by multiplication by λ.

Note that for any short exact sequence

$$0 \longrightarrow M \longrightarrow N \longrightarrow P \longrightarrow 0$$

of Λ-modules that are finite over k, we have $\operatorname{Tr}(\lambda; N) = \operatorname{Tr}(\lambda; M) + \operatorname{Tr}(\lambda; P)$. Therefore we have well-defined traces of elements of the corresponding Grothendieck groups as well. Moreover, we have $\operatorname{Tr}(\lambda\mu; M) = \operatorname{Tr}(\mu\lambda; M)$ for all $\lambda, \mu \in \Lambda$ and Λ-modules M that are finite over k.

Theorem 2.33 (Lefschetz trace formula, SGA4.5 [7, Rapport, Thm. 4.10])**.** *Let X be a $\mathbb{F}_p$-scheme of finite type, and let $F \in \operatorname{Gal}(\mathbb{F}_p^{\mathrm{sep}}/\mathbb{F}_p)$ denote the Frobenius morphism $x \mapsto x^p$. Then*

$$\#X(\mathbb{F}_{p^n}) = \operatorname{Tr}\big(F^{-n}; \chi_!(X_{\mathbb{F}_p}, \mathbb{Z}/\ell\mathbb{Z})\big).$$

Remark 2.34. The theorem cited is more general; in the notation there, we take K and Λ equal to $\mathbb{Z}/\ell\mathbb{Z}$. Moreover, the notion of trace used here is different from the notion of trace used in SGA4.5 [7], but by the theory of Frobenii, the numbers are the same (see also SGA4.5 [7, Rapport, Sec. 1.8]).

We now indicate, following the proof of Theorem 15.1.1 in Couveignes and Edixhoven [5] how to use this to compute $\#X(\mathbb{F}_q)$ modulo ℓ.

Let π denote the étale fundamental group of $\operatorname{Spec}\mathbb{Z}[1/N]$ at some base point. Then we have morphisms $\operatorname{Gal}(\mathbb{F}_p^{\mathrm{sep}}/\mathbb{F}_p) \to \pi$ and $\operatorname{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q}) \to \pi$ (corresponding to the morphisms $\operatorname{Spec}\mathbb{F}_p \to \operatorname{Spec}\mathbb{Z}[1/N]$ and $\operatorname{Spec}\mathbb{Q} \to \operatorname{Spec}\mathbb{Z}[1/N]$, respectively) that are well-defined up to inner automorphisms. Moreover, the latter morphism is surjective, so the Frobenius morphism in $\operatorname{Gal}(\mathbb{F}_p^{\mathrm{sep}}/\mathbb{F}_p)$ defines a conjugacy

class in $\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})$, and we find that for any element in this conjugacy class, its trace on $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ (in $K_0\big(\mathbb{Z}/\ell\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})]\big)$) is equal to the trace of Frobenius on $\chi_!(X_{\mathbb{F}_p}, \mathbb{Z}/\ell\mathbb{Z})$ (in $K_0\big(\mathbb{Z}/\ell\mathbb{Z}[\mathrm{Gal}(\mathbb{F}_p^{\mathrm{sep}}/\mathbb{F}_p)]\big)$).

Algorithm 2.35 (see also Couveignes and Edixhoven [5, Thm. 15.1.1])**.** *Suppose that given as input are primes $p \neq \ell$ such that $p \notin S_X$, and a positive integer n.*

Output: $\#X(\mathbb{F}_{p^n}) \mod \ell$

- Compute $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ as a finite sum $\sum_i a_i M_i$ with $a_i \in \mathbb{Z}$ and M_i a finite $\mathbb{Z}/\ell\mathbb{Z}[\mathrm{Gal}(\mathbb{Q}^{\mathrm{sep}}/\mathbb{Q})]$-module.
- For each M_i, let K_i be a finite Galois extension of $\mathbb{Q}$ over which M_i is given as a finite $\mathrm{Gal}(K_i/\mathbb{Q})$-module on which $\mathrm{Gal}(K_i/\mathbb{Q})$ acts faithfully.
- Let A_i be the ring of integers of K_i, let $\overline{A_i} = A_i/pA_i$, and compute a decomposition $\overline{A_i} = \prod_j \overline{A_{ij}}$ of $\overline{A_i}$ into finite field extensions $\overline{A_{ij}}$ of $\mathbb{F}_p$.
- By enumerating all elements of $\mathrm{Gal}(K_i/\mathbb{Q})$, find an element $F_i \in \mathrm{Gal}(K_i/\mathbb{Q})$ acting on some $\overline{A_{ij}}$ as Frobenius.
- **Output** $\sum_i a_i \operatorname{Tr}\big(F_i^{-n}; M_i\big)$, and **halt**.

Proposition 2.36. *If Algorithm 2.35 uses in its first step an algorithm that takes as input a prime ℓ and outputs $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ in time polynomial in ℓ, then Algorithm 2.35 is correct and halts in time polynomial in ℓ,* $\log p$*, and n.*

Proof. Correctness follows by construction.

For the bound on the complexity, note that the assumption that $\chi_!(X_{\mathbb{Q}}, \mathbb{Z}/\ell\mathbb{Z})$ can be computed in time polynomial in ℓ implies that the number of M_i, their dimensions over $\mathbb{Z}/\ell\mathbb{Z}$, the size (i.e. the logarithm of the absolute value) of the coefficients of A_i over $\mathbb{Z}$, and the orders of the groups $\mathrm{Gal}(K_i/\mathbb{Q})$ are all polynomially bounded in ℓ. Moreover, the reduction of the A_i modulo p can be done in time polynomial over $\log p$, so we see that the endomorphism F_i^n of M_i can be computed in time polynomial in ℓ, $\log p$, and n, and therefore its trace as well. □

As a corollary, we obtain a proof of Proposition 2.28, and therefore, under the assumption that there exists an algorithm that takes as input a prime ℓ and outputs $\chi_!(X, \mathbb{Z}/\ell\mathbb{Z})$ in time polynomial in ℓ, a positive answer to the question stated in the introduction.

3 Cohomology of smooth curves

The goal of this chapter is to describe an algorithm for Algorithm 2.2. A key ingredient is the fact that, for a finite étale Galois morphism $g\colon X' \to X$ of smooth curves with Galois group Γ, we can make the equivalence between the category of finite étale Γ-schemes over X' and the category of finite étale schemes over X explicit. Note that under this equivalence, a finite étale group scheme on X corresponds to a Γ-equivariant group scheme on X'. We will use this to reduce to the following situation.

Let $f\colon X \to \operatorname{Spec} k$ be a smooth connected curve, let Γ, G be finite groups such that Γ acts on X and on G by automorphisms. Consider the stack $\mathcal{T} = \mathcal{T}^G_{\Gamma,X}$ over k of Γ-equivariant G-torsors on X over k. We then construct a groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$, together with a morphism of the corresponding fppf prestack $[\mathcal{U}/\mathcal{R}] \to \mathcal{T}$ such that $\mathcal{U}(\bar{k}) \to \mathcal{T}(\bar{k})$ induces a $\operatorname{Gal}(k^{\mathrm{sep}}/k)$-equivariant bijection $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}}) \to \mathcal{T}(k^{\mathrm{sep}})/\cong$. To this end, we only require a few properties.

Proposition 3.1. *Let $\mathcal{T}$ be a separated étale algebraic stack over a field k. Let $\mathcal{R} \rightrightarrows \mathcal{U}$ be a groupoid scheme such that $\mathcal{R}$ and $\mathcal{U}$ are affine and of finite type over k. Let $[\mathcal{U}/\mathcal{R}] \to \mathcal{T}$ be a morphism of fppf prestacks such that for all perfect field extensions l of k, the functor $[\mathcal{U}/\mathcal{R}](l) \to \mathcal{T}(l)$ is an equivalence, and such that the isomorphism classes in $\mathcal{U}(\bar{k})$ are connected.*

Then the map $\mathcal{U}(\bar{k}) \to \operatorname{Ob}\mathcal{T}(k^{\mathrm{sep}})/\cong$ is a $\operatorname{Gal}(k^{\mathrm{sep}}/k)$-equivariant map that is surjective, and factors through a $\operatorname{Gal}(k^{\mathrm{sep}}/k)$-equivariant bijection $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}}) \to \operatorname{Ob}\mathcal{T}(k)/\cong$.

If in addition the isomorphism classes in $\mathcal{U}(\bar{k})$ are irreducible, then the connected components of $\mathcal{U}_{k^{\mathrm{sep}}}$ are irreducible.

Proof. The surjectivity of the map $\mathcal{U}(\bar{k}) \to \operatorname{Ob}\mathcal{T}(k^{\mathrm{sep}})/\cong$ and its compatibility with the Galois action is clear from the identity $\operatorname{Gal}(k^{\mathrm{sep}}/k) = \operatorname{Gal}(\bar{k}/k^{\mathrm{perf}})$ and the assumption that $[\mathcal{U}/\mathcal{R}](l) \to \mathcal{T}(l)$ is an equivalence for every perfect field extension l of k, so let us show that the map factors through $\pi_0(\mathcal{U}_{\bar{k}})$.

Let $\bar{x} \in \mathcal{U}(\bar{k})$ and let $j\colon U \to \mathcal{U}_{\bar{k}}$ be the open immersion of the connected component U containing $\bar{x}$ into $\mathcal{U}_{\bar{k}}$. Moreover, let $f\colon U \to \operatorname{Spec}\bar{k}$ denote the structure morphism, and let $i\colon U_{\bar{k}} \to U$ 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 $Y_1 = j^{-1}i^{-1}\mathcal{Y}, Y_2 = f^{-1}\bar{x}^{-1}\mathcal{Y} \in \mathcal{U}(U)$, and consider their images in $\operatorname{Ob}\mathcal{T}(U)$. Then the Hom-sheaf $\operatorname{Hom}_{\mathcal{T}(U)}(Y_1, Y_2)$ is representable by a finite étale U-scheme as $\mathcal{T}$ is separated and étale over k.

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 $\overline{x'} \in \mathcal{U}(\bar{k})$, the set $\mathrm{Hom}_{\mathcal{T}(U)}(Y_1, Y_2)(\overline{x'})$ is non-empty as well. Therefore the morphism $\mathcal{U}(\bar{k}) \to \mathrm{Ob}\,\mathcal{T}(\bar{k})/\cong$ factors through a surjective $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant map $\pi_0(\mathcal{U}_{\bar{k}}) \to \mathrm{Ob}\,\mathcal{T}(\bar{k})/\cong$. Note that the source of this map is equal to $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}})$ as $\mathrm{Spec}\,\bar{k} \to \mathrm{Spec}\,k^{\mathrm{sep}}$ is a universal homeomorphism, and that the target of this map is $\mathrm{Ob}\,\mathcal{T}(k^{\mathrm{sep}})/\cong$ as $\mathcal{T}$ is étale over k.

As the map $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}}) \to \mathrm{Ob}\,\mathcal{T}(k^{\mathrm{sep}})/\cong$ is surjective and isomorphism classes in $\mathcal{U}(k^{\mathrm{sep}})$ are connected (and therefore are disjoint unions of connected components of $\mathcal{U}(k^{\mathrm{sep}})$), it follows that map $\pi_0(\mathcal{U}_{k^{\mathrm{sep}}}) \to \mathrm{Ob}\,\mathcal{T}(k^{\mathrm{sep}})/\cong$ is bijective. Finally, if the isomorphism classes in $\mathcal{U}(k^{\mathrm{sep}})$ are irreducible, then it follows from this that connected components of $\mathcal{U}_{k^{\mathrm{sep}}}$ must be irreducible as well. □

In particular, since in our case $\mathcal{T}$ is a separated étale algebraic stack over k, we see that as soon as we construct an explicit groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ satisfying the conditions of Proposition 3.1, we have a proof of the finiteness of $\mathrm{Ob}\,\mathcal{T}(k^{\mathrm{sep}})/\cong$ as $\pi_0(\mathrm{Ob}\,\mathcal{X}_{k^{\mathrm{sep}}})$ is finite.

We give a rough description of the construction of such a groupoid scheme in the case in which X is projective; the affine case is then reduced to this one. We fix a finite locally free morphism $\pi\colon X \to \mathbb{P}^1_k$ (such that Γ acts on $X/\mathbb{P}^1_k$), and we note that for a k-scheme S, giving a Γ-equivariant G-torsor on X_S is equivalent to giving

- a finite locally free $\mathcal{O}_{\mathbb{P}^1_S}$-algebra $\mathcal{O}_Y$, together with compatible actions of the finite groups Γ and G,
- a morphism $\varphi\colon \pi_*\mathcal{O}_X \to \mathcal{O}_Y$ that is Γ-equivariant and G-equivariant for the trivial action of G on $\pi_*\mathcal{O}_X$,

such that φ corresponds to a G-torsor on X; in particular, $\mathcal{O}_Y$ is finite, étale, and of constant rank $\#G$ as an $\pi_*\mathcal{O}_X$-algebra. The desired groupoid scheme $\mathcal{R} \rightrightarrows \mathcal{U}$ then is one in which $\mathcal{U}$ has a moduli interpretation in terms of the objects above.

This chapter is roughly divided into four parts. In the first part, we set up a language for "universal linear algebra over $\mathbb{P}^1$". In the second part (starting from Section 3.7) and the third part (starting from Section 3.13), we use this in order to describe a groupoid scheme with the desired properties, in the projective and affine case, respectively. Finally, we then use this description in the last part (starting from Section 3.17) to compute $R^q f_*$ and $R^q f_!$ for $q = 0, 1, 2$.

3.1 Category schemes

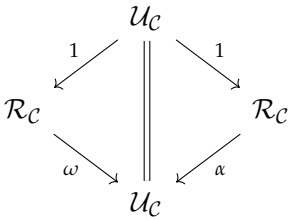
In our construction of the desired groupoid scheme, categories that are not groupoids will arise naturally. Therefore we will need the notion of a *category scheme*, which is (for the cognoscenti) an internal category (see e.g. Johnstone [23, Sec. B.2.3]) in the category of schemes over a fixed base scheme. We work out what this means below.

Definition 3.2. Let S be a scheme. A *category scheme* $\mathcal{C}$ over S consists of:

- S-schemes $\mathcal{R}_\mathcal{C}, \mathcal{U}_\mathcal{C}$ (the *scheme of morphisms*, resp. *scheme of objects*);
- S-morphisms $\alpha, \omega\colon \mathcal{R}_\mathcal{C} \to \mathcal{U}_\mathcal{C}$ (the *source*, resp. *target* morphisms);
- an S-morphism $1\colon \mathcal{U}_\mathcal{C} \to \mathcal{R}_\mathcal{C}$ (the *unit* morphism);
- an S-morphism $\circ\colon \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} \to \mathcal{R}_\mathcal{C}$ (the *composition* morphism),

such that the following diagrams commute.

- (source and target of unit)



- (source and target of composition)

$$\begin{array}{ccccc} \mathcal{R}_\mathcal{C} & \xleftarrow{\pi_1} & \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} & \xrightarrow{\pi_2} & \mathcal{R}_\mathcal{C} \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\circ} & & \downarrow{\scriptstyle\alpha} \\ \mathcal{U}_\mathcal{C} & \xleftarrow[\omega]{} & \mathcal{R}_\mathcal{C} & \xrightarrow[\alpha]{} & \mathcal{U}_\mathcal{C} \end{array}$$

- (unit)

$$\begin{array}{ccccc} \mathcal{R}_\mathcal{C} & \xrightarrow{(1\omega,\mathrm{id})} & \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} & \xleftarrow{(\mathrm{id},1\alpha)} & \mathcal{R}_\mathcal{C} \\ & \searrow^{\mathrm{id}} & \downarrow{\scriptstyle\circ} & \swarrow_{\mathrm{id}} & \\ & & \mathcal{R}_\mathcal{C} & & \end{array}$$

- (associativity)

$$\begin{array}{ccc} \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} & \xrightarrow{(\circ,\mathrm{id})} & \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} \\ {\scriptstyle(\mathrm{id},\circ)}\downarrow & & \downarrow{\scriptstyle\circ} \\ \mathcal{R}_\mathcal{C} \times_{\alpha,\omega} \mathcal{R}_\mathcal{C} & \xrightarrow{\quad\circ\quad} & \mathcal{R}_\mathcal{C} \end{array}$$

We will use the notation $\mathrm{Ob}\,\mathcal{C}$ instead of $\mathcal{U}_\mathcal{C}$ if we view it as a scheme of objects. We also define the corresponding notion of a functor.

Definition 3.3. Let S be a scheme, and let $\mathcal{C}$ and $\mathcal{D}$ be category schemes. A *functor* $F\colon \mathcal{C} \to \mathcal{D}$ consists of S-morphisms $\mathcal{R}_F\colon \mathcal{R}_\mathcal{C} \to \mathcal{R}_\mathcal{D}$ and $\mathcal{U}_F\colon \mathcal{U}_\mathcal{D} \to \mathcal{U}_\mathcal{D}$ such that the following diagrams (representing respectively the compatibility of F with source and target, unit, and composition) commute.

$$\begin{array}{ccc} \mathcal{R}_\mathcal{C} & \xrightarrow{\mathcal{R}_F} & \mathcal{R}_\mathcal{D} \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\omega} \\ \mathcal{U}_\mathcal{C} & \xrightarrow[\mathcal{U}_F]{} & \mathcal{U}_\mathcal{D} \end{array} \qquad \begin{array}{ccc} \mathcal{R}_\mathcal{C} & \xrightarrow{\mathcal{R}_F} & \mathcal{R}_\mathcal{D} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ \mathcal{U}_\mathcal{C} & \xrightarrow[\mathcal{U}_F]{} & \mathcal{U}_\mathcal{D} \end{array}$$

$$\begin{array}{ccc} \mathcal{U}_\mathcal{C} & \xrightarrow{\mathcal{U}_F} & \mathcal{U}_\mathcal{D} \\ 1\downarrow & & \downarrow 1 \\ \mathcal{R}_\mathcal{C} & \xrightarrow{\mathcal{R}_F} & \mathcal{R}_\mathcal{D} \end{array}$$

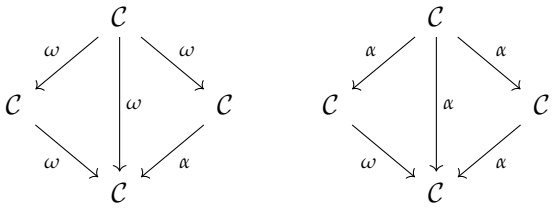
$$\begin{array}{ccc} \mathcal{R}_{\mathcal{C}} \times_{\alpha,\omega} \mathcal{R}_{\mathcal{C}} & \xrightarrow{\mathcal{R}_F \times \mathcal{R}_F} & \mathcal{R}_{\mathcal{D}} \times_{\alpha,\omega} \mathcal{R}_{\mathcal{D}} \\ {\scriptstyle \circ}\downarrow & & \downarrow{\scriptstyle \circ} \\ \mathcal{R}_{\mathcal{C}} & \xrightarrow[\mathcal{R}_F]{} & \mathcal{R}_{\mathcal{D}} \end{array}$$

An equivalent way to describe a category scheme is as follows; this uses the alternative description of a category given in e.g. Gelfand and Manin [14, Ex. II.1.1].

Definition 3.4. Let S be a scheme. A *single-sorted category scheme* consists of:

- an S-scheme $\mathcal{C}$;
- S-morphisms $\alpha, \omega \colon \mathcal{C} \to \mathcal{C}$ (the *source*, resp. *target* morphisms);
- an S-morphism $\circ \colon \mathcal{C} \times_{\alpha,\omega} \mathcal{C} \to \mathcal{C}$ (the *composition* morphism),

such that the following diagrams (representing respectively the relations regarding the source and target of the unit, the source and target of the composition, the unit morphism, and associativity) commute.



$$\begin{array}{ccccc} \mathcal{C} & \xleftarrow{\pi_1} & \mathcal{C} \times_{\alpha,\omega} \mathcal{C} & \xrightarrow{\pi_2} & \mathcal{C} \\ {\scriptstyle \omega}\downarrow & & \downarrow{\scriptstyle \circ} & & \downarrow{\scriptstyle \alpha} \\ \mathcal{C} & \xleftarrow[\omega]{} & \mathcal{C} & \xrightarrow[\alpha]{} & \mathcal{C} \end{array}$$

$$\begin{array}{ccccc} \mathcal{C} & \xrightarrow{(\omega,\mathrm{id})} & \mathcal{C} \times_{\alpha,\omega} \mathcal{C} & \xleftarrow{(\mathrm{id},\alpha)} & \mathcal{C} \\ & {\scriptstyle \mathrm{id}}\searrow & \downarrow{\scriptstyle \circ} & \swarrow{\scriptstyle \mathrm{id}} & \\ & & \mathcal{C} & & \end{array}$$

$$\begin{array}{ccc} \mathcal{C} \times_{\alpha,\omega} \mathcal{C} \times_{\alpha,\omega} \mathcal{C} & \xrightarrow{(\circ,\mathrm{id})} & \mathcal{C} \times_{\alpha,\omega} \mathcal{C} \\ {\scriptstyle (\mathrm{id},\circ)}\downarrow & & \downarrow{\scriptstyle \circ} \\ \mathcal{C} \times_{\alpha,\omega} \mathcal{C} & \xrightarrow{\circ} & \mathcal{C} \end{array}$$

The term *single-sorted* refers to the fact that this notion of a category uses only one "type", namely that of morphisms. We now define functors for this notion of category scheme.

Definition 3.5. Let S be a scheme, and let $\mathcal{C}$ and $\mathcal{D}$ be single-sorted category schemes over S. A *functor* $F\colon \mathcal{C} \to \mathcal{D}$ is a morphism of schemes such that the following diagrams (representing the compatibility of F with source and target, and with composition, respectively) commute.

$$\begin{array}{ccc} \mathcal{C} & \xrightarrow{F} & \mathcal{D} \\ {\scriptstyle\omega}\downarrow & & \downarrow{\scriptstyle\omega} \\ \mathcal{C} & \xrightarrow[F]{} & \mathcal{D} \end{array} \qquad \begin{array}{ccc} \mathcal{C} & \xrightarrow{F} & \mathcal{D} \\ {\scriptstyle\alpha}\downarrow & & \downarrow{\scriptstyle\alpha} \\ \mathcal{C} & \xrightarrow[F]{} & \mathcal{D} \end{array}$$

$$\begin{array}{ccc} \mathcal{C} \times_{\alpha,\omega} \mathcal{C} & \xrightarrow{F\times F} & \mathcal{D} \times_{\alpha,\omega} \mathcal{D} \\ {\scriptstyle\circ}\downarrow & & \downarrow{\scriptstyle\circ} \\ \mathcal{C} & \xrightarrow[F]{} & \mathcal{D} \end{array}$$

Note that we obtain a category Cat_S of category schemes over S, as well as a category Cat'_S of single-sorted category schemes over S. In order to avoid confusion with the category Cat of small categories, we will never drop the base scheme S from the notation. By construction, we have the following.

Proposition 3.6. *The functor* $\mathrm{Cat}_S \to \mathrm{Cat}'_S$ *sending an object* $(\mathcal{U}, \mathcal{R}, \alpha, \omega, 1, \circ)$ *to the object* $(\mathcal{R}, 1\alpha, 1\omega, \circ)$ *is an equivalence and has as quasi-inverse the functor* $\mathrm{Cat}'_S \to \mathrm{Cat}_S$ *sending an object* $(\mathcal{C}, \alpha, \omega, \circ)$ *to* $(E, \mathcal{C}, \alpha, \omega, i, \circ)$*, where* $i\colon E \to \mathcal{C}$ *is the equaliser of* α *and* ω*.*

Proof. By construction. □

Finally, using the Yoneda lemma, one also has descriptions of category schemes in terms of the functor(s) of points. We will use all of these descriptions interchangably from now on.

3.2 The category scheme of standard modules

We start to carry out the program outlined in the introduction of this chapter by constructing an affine category scheme of finite type over k modeling the category of vector bundles on $\mathbb{P}^1_k$, presented as in Section 1.6.2. Its objects over a k-scheme S will be of the following kind. Let $\mathrm{Seq} = \mathrm{Seq}(\mathbb{Z})$ denote the set of all finite sequences of integers.

Definition 3.7. Let S be a scheme, and let $a = (a_i)_{i=1}^s \in \mathrm{Seq}$ be a finite sequence of integers. The *standard module of type* a over S is the $\mathcal{O}_{\mathbb{P}^1_S}$-module

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

Let $\mathcal{S} \subseteq \mathrm{Seq}$. A *locally standard module of type in* $\mathcal{S}$ is an $\mathcal{O}_{\mathbb{P}^1_S}$-module $\mathcal{E}$ such that there exists a locally constant map $q\colon S \to \mathcal{S}$ such that $\mathcal{E}|_{q^{-1}(a)} = \mathcal{O}_{\mathbb{P}^1_{q^{-1}(a)}}(a)$ for all $a \in \mathcal{S}$.

So, as mentioned before, Theorem 1.23 states that every vector bundle over $\mathcal{O}_{\mathbb{P}^1_k}$ for a field k is isomorphic to a locally standard module over k. In the remainder of this section, we define the category scheme of locally standard modules, together with some additional ("linear algebraic") structure we will be using in later constructions. Our choice of base scheme will be $\operatorname{Spec}\mathbb{Z}$; this doesn't cause any loss of generality, and will be easier on the notation.

3.2.1 Construction

We construct the category scheme of locally standard modules over k as a disjoint union of affine schemes of finite type over k, which we describe first. To this end, we identify, for a scheme S, the scheme $\mathbb{P}^1_S$ with $\operatorname{Proj}_S \mathcal{O}_S[x,y]$, and for all integers n, the $\mathcal{O}_S$-module $\mathcal{O}_{\mathbb{P}^1_S}(n)(\mathbb{P}^1_S)$ with $\mathcal{O}_S[x,y]_n$, the degree n part of $\mathcal{O}_S[x,y]$.

Definition 3.8. Let $\mathcal{S} \subseteq \mathrm{Seq}$. The *category scheme* $\mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}}$ *of locally standard modules of type in* $\mathcal{S}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ that sends a scheme S to the category of locally standard modules of type in $\mathcal{S}$.

We show that this functor is representable, so that it indeed is a category scheme. To this end, we introduce an auxiliary functor.

Definition 3.9. Let $a, b \in \mathrm{Seq}$. The functor $\mathrm{Mod}^{\mathrm{st}}_{b,a}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Set}$ that sends a scheme S to the set of $\mathcal{O}_{\mathbb{P}^1_S}$-linear maps $\mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$.

Lemma 3.10. *Let* $a, b \in \mathrm{Seq}$. *The functor* $\mathrm{Mod}^{\mathrm{st}}_{b,a}$ *is representable by* $\mathbb{A}_k^{N(b,a)}$ *where* $N(b,a) = \sum_{\sigma,\tau} \max(0, b_\tau - a_\sigma + 1)$.

The proof of Lemma 3.10 follows from the following. Note that for all schemes S, we have

$$\begin{aligned}\operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(a), \mathcal{O}_{\mathbb{P}^1_S}(b)\right) &= \bigoplus_{i,j} \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(a_i), \mathcal{O}_{\mathbb{P}^1_S}(b_j)\right), \\ &= \bigoplus_{i,j} \mathcal{O}_{\mathbb{P}^1_S}(b_j - a_i)(\mathbb{P}^1_S);\end{aligned}$$

so therefore we obtain an identification

$$\operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(a), \mathcal{O}_{\mathbb{P}^1_S}(b)\right) = \left\{ M \in \operatorname{Mat}_{t,s}\left(\mathcal{O}_S(S)[x,y]\right) : M_{ji} \in \mathcal{O}_S(S)[x,y]_{b_j - a_i} \right\},$$

where s and t are the lengths of a and b, respectively.

Note that this is an $\mathcal{O}(S)$-module admitting an $\mathcal{O}(S)$-basis given by, for all i, j, and $\lambda \in \{0, 1, \ldots, b_j - a_i\}$, the $t \times s$-matrix $E_{ji\lambda}$ that has zeroes everywhere except for the (j,i) entry, which is $x^\lambda y^{b_j - a_i - \lambda}$ (taking the lexicographical order for triples (j,i,λ)). The result follows.

We therefore get the representability of $\mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}}$ as a consequence.

Proposition 3.11. *Let* $\mathcal{S} \subseteq \mathrm{Seq}$. *The functor* $\mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}}$ *is representable by the category scheme* $(\mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}}, \alpha, \omega, \circ)$, *where*

- $\mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}} = \coprod_{a,b \in \mathcal{S}} \mathrm{Mod}^{\mathrm{st}}_{b,a}$;

- $\alpha\colon \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}} \to \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\alpha_{b,a} = \alpha|_{\operatorname{Mod}^{\mathrm{st}}_{b,a}}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{a,a}$$
is the constant morphism with value the identity matrix;
- $\omega\colon \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}} \to \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\omega_{b,a} = \omega|_{\operatorname{Mod}^{\mathrm{st}}_{b,a}}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{b,b}$$
is the constant morphism with value the identity matrix;
- $\circ\colon \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}} \times_{\alpha,\omega} \operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\circ_{c,b,a} = \circ|_{\operatorname{Mod}^{\mathrm{st}}_{c,b} \times \operatorname{Mod}^{\mathrm{st}}_{b,a}}\colon \operatorname{Mod}^{\mathrm{st}}_{c,b} \times \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{c,a}$$
is the morphism given by matrix multiplication.

If $\mathcal{S}$ is finite, then $\operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ is affine and of finite type.

Proof. By definition, the functor $\operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ is the Zariski sheafification of the functor $\coprod_{b,a\in\mathcal{S}} \operatorname{Mod}^{\mathrm{st}}_{b,a}$. It follows that $\operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ is representable by $\coprod_{b,a\in\mathcal{S}} \operatorname{Mod}^{\mathrm{st}}_{b,a}$. Moreover, for all schemes S we have by construction that the maps $\alpha(S)$, $\omega(S)$, and $\circ(S)$ coincide with the source, target, and composition maps on the category of locally standard modules of type in $\mathcal{S}$.

Finally, if $\mathcal{S}$ is finite, then $\operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ is a finite disjoint union of affine schemes of finite type, therefore affine and of finite type itself. □

Corollary 3.12. *For all $a \in \mathrm{Seq}$, the scheme $\operatorname{Ob}\operatorname{Mod}^{\mathrm{st}}_{\{a\}}$ is representable by $\operatorname{Spec}\mathbb{Z}$.*

Let $\mathcal{S} \subseteq \mathrm{Seq}$. The functor $\operatorname{Ob}\operatorname{Mod}^{\mathrm{st}}_{\mathcal{S}}$ is representable by $\coprod_{a\in\mathcal{S}} \operatorname{Ob}\operatorname{Mod}^{\mathrm{st}}_{\{a\}}$.

Note that by construction, for any field k, the category of k-points of $\operatorname{Mod}^{\mathrm{st}}$ is equal to the category $\mathcal{P}(k)$ of Section 1.6.2.

Expanding everything in terms of the basis $\{E_{ji\lambda}\}$ of $\operatorname{Mat}_{b,a}$ described above, we find that the following an explicit description of $\operatorname{Mod}^{\mathrm{st}}_1$.

Formulary 3.13. Let $a, b, c \in \mathrm{Seq}$ be of lengths s, t, u, respectively. Then
$$\operatorname{Mod}^{\mathrm{st}}_{b,a} = \operatorname{Spec}\mathbb{Z}[x_{ji\lambda} : 1 \le j \le t, 1 \le i \le s, 0 \le \lambda \le b_j - a_i].$$
The morphisms $\alpha_{b,a}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{a,a}$ and $\omega_{b,a}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{b,b}$ are given in terms of the coordinate rings by
$$x_{ji\lambda} \mapsto \begin{cases} 1 & \text{if } i = j \text{ (so } \lambda = 0); \\ 0 & \text{otherwise.} \end{cases}$$
The morphism $\circ_{c,b,a}\colon \operatorname{Mod}^{\mathrm{st}}_{c,b} \times \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{c,a}$ is given in terms of the coordinate rings by
$$x_{ki\lambda} \mapsto \sum_{j=1}^{t} \sum_{(\lambda_1,\lambda_2)} x_{kj\lambda_1} \otimes x_{ji\lambda_2},$$
where (λ_1, λ_2) runs through all pairs of integers with the properties $\lambda_1 + \lambda_2 = \lambda$, $0 \le \lambda_1 \le c_k - b_j$, and $0 \le \lambda_2 \le b_j - a_i$.

3.2.2 Direct sums

We describe direct sums in $\mathrm{Mod}^{\mathrm{st}}$. For a scheme S, and $a, a' \in \mathrm{Seq}$ of lengths s, s', respectively, we identify the direct sum $\mathcal{O}_{\mathbb{P}^1_S}(a) \oplus \mathcal{O}_{\mathbb{P}^1_S}(a')$ with $\mathcal{O}_{\mathbb{P}^1_S}(aa')$, where aa' is the concatenation of a and a'. Using this identification, we obtain a functor $\oplus\colon \mathrm{Mod}^{\mathrm{st}} \times \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ of categories, sending for all schemes S a pair $(M, M') \in \mathrm{Mod}^{\mathrm{st}}(S) \times \mathrm{Mod}^{\mathrm{st}}(S)$ to $M \oplus M'$.

Lemma 3.14. *The functor* $\oplus\colon \mathrm{Mod}^{\mathrm{st}} \times \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ *is the morphism such that*

$$\oplus_{b,b',a,a'} = \oplus|_{\mathrm{Mod}^{\mathrm{st}}_{b,a} \times \mathrm{Mod}^{\mathrm{st}}_{b',a'}}\colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \times \mathrm{Mod}^{\mathrm{st}}_{b',a'} \to \mathrm{Mod}^{\mathrm{st}}_{bb',aa'}$$

sends, for any scheme S*, the pair* $(M, M') \in \mathrm{Mod}^{\mathrm{st}}_{b,a}(S) \times \mathrm{Mod}^{\mathrm{st}}_{b',a'}(S)$ *to the direct sum* $M \oplus M'\colon \mathcal{O}_{\mathbb{P}^1_S}(b) \oplus \mathcal{O}_{\mathbb{P}^1_S}(b') \to \mathcal{O}_{\mathbb{P}^1_S}(a) \oplus \mathcal{O}_{\mathbb{P}^1_S}(a')$.

Expanding this in the same way as in Formulary 3.13, we find the following.

Formulary 3.15. Let $a, b, a', b' \in \mathrm{Seq}$, of lengths s, t, s', t', respectively. Notation is as in Formulary 3.13. The morphism $\oplus_{b,b',a,a'}\colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \times \mathrm{Mod}^{\mathrm{st}}_{b',a'} \to \mathrm{Mod}^{\mathrm{st}}_{bb',aa'}$ is given in terms of the coordinate rings by

$$x_{j,i,\lambda} \mapsto \begin{cases} x_{j,i,\lambda} \otimes 1 & \text{if } 1 \le i \le s \text{ and } 1 \le j \le t; \\ 1 \otimes x_{j-t,i-s,\lambda} & \text{if } s+1 \le i \le s+s' \text{ and } t+1 \le j \le t+t'; \\ 0 & \text{otherwise.} \end{cases}$$

3.2.3 Tensor products and duals

We describe tensor products in $\mathrm{Mod}^{\mathrm{st}}$. If S is a scheme, $a, a' \in \mathrm{Seq}$, then we identify the tensor product $\mathcal{O}_{\mathbb{P}^1_S}(a) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(a')$ with $\bigoplus_{i,i'} \mathcal{O}_{\mathbb{P}^1_S}(a_i + a'_{i'})$, together with the lexicographical ordering on the pairs (i, i').

Let us therefore introduce the notation $a \oplus a'$ for the finite sequence $(a_i + a'_{i'})_{i,i'}$ together with the lexicographical ordering on the pairs (i, i'). The identification above now gives us a functor $\otimes\colon \mathrm{Mod}^{\mathrm{st}} \times \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ of category schemes, sending for all schemes S a pair $(M, M') \in \mathrm{Mod}^{\mathrm{st}}(S) \times \mathrm{Mod}^{\mathrm{st}}(S)$ to $M \otimes M'$.

Lemma 3.16. *The functor* $\otimes\colon \mathrm{Mod}^{\mathrm{st}} \times \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ *is the morphism such that*

$$\otimes_{b,b',a,a'} = \otimes|_{\mathrm{Mod}^{\mathrm{st}}_{b,a} \times \mathrm{Mod}^{\mathrm{st}}_{b',a'}}\colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \times \mathrm{Mod}^{\mathrm{st}}_{b',a'} \to \mathrm{Mod}^{\mathrm{st}}_{b \oplus b', a \oplus a'}$$

sends, for any scheme S*, the pair* $(M, M') \in \mathrm{Mod}^{\mathrm{st}}_{b,a}(S) \times \mathrm{Mod}^{\mathrm{st}}_{b',a'}(S)$ *to the tensor product* $M \otimes M'\colon \mathcal{O}_{\mathbb{P}^1_S}(b) \otimes \mathcal{O}_{\mathbb{P}^1_S}(b') \to \mathcal{O}_{\mathbb{P}^1_S}(a) \otimes \mathcal{O}_{\mathbb{P}^1_S}(a')$.

Note that the tensor product is associative, and that the neutral element with respect to the tensor product is $\mathcal{O}_{\mathbb{P}^1_S} = \mathcal{O}_{\mathbb{P}^1_S}(0_1)$, where 0_1 is the zero sequence of length 1.

Next, note that for any scheme S and any objects $\mathcal{E}, \mathcal{E}' \in \mathrm{Ob}\,\mathrm{Mod}^{\mathrm{st}}(S)$, we have an isomorphism $\Sigma(\mathcal{E}, \mathcal{E}')\colon \mathcal{E} \otimes \mathcal{E}' \to \mathcal{E}' \otimes \mathcal{E}$. This defines a morphism Σ from the scheme $\mathrm{Ob}\,\mathrm{Mod}^{\mathrm{st}} \times \mathrm{Ob}\,\mathrm{Mod}^{\mathrm{st}}$ to $\mathrm{Mod}^{\mathrm{st}}$.

Lemma 3.17. *The morphism* $\Sigma\colon \operatorname{Ob}\operatorname{Mod}^{\mathrm{st}} \times \operatorname{Ob}\operatorname{Mod}^{\mathrm{st}} \to \operatorname{Mod}^{\mathrm{st}}$ *is the morphism such that*

$$\Sigma_{a,a'} = \Sigma|_{\operatorname{Ob}\operatorname{Mod}^{\mathrm{st}}_{\{a\}} \times \operatorname{Ob}\operatorname{Mod}^{\mathrm{st}}_{\{a'\}}} : \operatorname{Spec}\mathbb{Z} \to \operatorname{Mod}^{\mathrm{st}}_{a'\oplus a, a\oplus a'}$$

is given by the isomorphism $\mathcal{O}_{\mathbb{P}^1}(a) \otimes \mathcal{O}_{\mathbb{P}^1}(a') \to \mathcal{O}_{\mathbb{P}^1}(a') \otimes \mathcal{O}_{\mathbb{P}^1}(a)$ *switching the two factors.*

Finally, for a scheme S and $a \in \mathrm{Seq}$, we write $\mathcal{O}_{\mathbb{P}^1_S}(a)^\vee = \mathcal{H}om_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(a), \mathcal{O}_{\mathbb{P}^1_S}\right)$, which we identify with $\mathcal{O}_{\mathbb{P}^1_S}(-a)$, where $-a$ is the sequence $(-a_i)_i$. Using this identification, we get a dualisation functor ${}^\vee\colon (\operatorname{Mod}^{\mathrm{st}})^{\mathrm{op}} \to \operatorname{Mod}^{\mathrm{st}}$ sending, for a scheme S, a morphism $M \in \operatorname{Mod}^{\mathrm{st}}(S)$ to $M^\vee$. This dualisation is compatible with tensor products.

Lemma 3.18. *The functor* ${}^\vee\colon (\operatorname{Mod}^{\mathrm{st}})^{\mathrm{op}} \to \operatorname{Mod}^{\mathrm{st}}$ *is the morphism such that*

$${}^\vee{}_{b,a} = {}^\vee|_{(\operatorname{Mod}^{\mathrm{st}})^{\mathrm{op}}_{b,a}} : \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{-a,-b}$$

sends, for any scheme S*, the morphism* $M \in \operatorname{Mod}^{\mathrm{st}}_{b,a}(S)$ *to its dual* $M^\vee$*.*

Remark 3.19. We have, for every scheme S and for all $a, b, c \in \mathrm{Seq}$, identifications

$$\begin{aligned}\operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(b) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(c), \mathcal{O}_{\mathbb{P}^1_S}(a)\right) &= \bigoplus_{i,j,k} \mathcal{O}_{\mathbb{P}^1_S}(a_i - b_j - c_k)(\mathbb{P}^1_S) \\ &= \operatorname{Hom}_{\mathcal{O}_{\mathbb{P}^1_S}}\left(\mathcal{O}_{\mathbb{P}^1_S}(c), \mathcal{O}_{\mathbb{P}^1_S}(a) \otimes \mathcal{O}_{\mathbb{P}^1_S}(b)^\vee\right),\end{aligned}$$

that preserve matrices (as tuples with the lexicographical order on the index set). This identification identifies the trace map $\mathcal{O}_{\mathbb{P}^1_S}(a) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(a)^\vee \to \mathcal{O}_{\mathbb{P}^1_S}$ with the identity map $\mathcal{O}_{\mathbb{P}^1_S}(a)^\vee \to \mathcal{O}_{\mathbb{P}^1_S}(a)^\vee$.

Consider the tuple[1] $(\operatorname{Mod}^{\mathrm{st}}, \otimes, {}^\vee, \Sigma, \mathcal{O}_{\mathbb{P}^1})$. Expanding everything in the same way as in Formulary 3.13, we find the following.

Formulary 3.20. Let $a, b, a', b' \in \mathrm{Seq}$ be of lengths s, t, s', t', respectively. Notation is as in Formulary 3.13. Write for convenience

$$\begin{aligned}\operatorname{Mod}^{\mathrm{st}}_{b\oplus b', a\oplus a'} = \operatorname{Spec}\mathbb{Z}[x_{(j,j')(i,i')\lambda} : 1 \le j \le t, 1 \le j' \le t', 1 \le i \le s,\\ 1 \le i' \le s', 0 \le \lambda \le b_j + b'_{j'} - a_i - a'_{i'}].\end{aligned}$$

The morphism $\otimes_{b,b',a,a'}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \times \operatorname{Mod}^{\mathrm{st}}_{b',a'} \to \operatorname{Mod}^{\mathrm{st}}_{b\oplus b', a\oplus a'}$ is given in terms of the algebras by

$$x_{(j,j')(i,i')\lambda} \mapsto \sum_{(\lambda_1,\lambda_2)} x_{ji\lambda_1} \otimes x_{j'i'\lambda_2},$$

where (λ_1, λ_2) runs through all integers such that $\lambda_1 + \lambda_2 = \lambda, 0 \le \lambda_1 \le b_j - a_i$, and $0 \le \lambda_2 \le b'_{j'} - a'_{i'}$. The morphism ${}^\vee{}_{b,a}\colon \operatorname{Mod}^{\mathrm{st}}_{b,a} \to \operatorname{Mod}^{\mathrm{st}}_{-a,-b}$ is given in terms of the algebras by

$$x_{ji\lambda} \mapsto x_{ij\lambda}.$$

[1] This tuple, together with Remark 3.19, gives $\operatorname{Mod}^{\mathrm{st}}(S)$ the structure of a strict rigid symmetric monoidal category for all schemes S.

The morphism $\Sigma_{a,a'} \in \mathrm{Mod}^{\mathrm{st}}_{a'\oplus a, a\oplus a'}(\operatorname{Spec}\mathbb{Z})$ is given by

$$x_{i_2' i_2 i_1 i_1'} \mapsto \begin{cases} 1 & \text{if } i_1 = i_2 \text{ and } i_1' = i_2'; \\ 0 & \text{otherwise.} \end{cases}$$

The object $\mathcal{O}_{\mathbb{P}^1} \in \mathrm{Mod}^{\mathrm{st}}_{1,0_1,0_1}(\operatorname{Spec}\mathbb{Z})$ (where 0_1 is the zero sequence of length 1) is given by

$$x_{000} \mapsto 1.$$

3.2.4 Exterior powers

Fix a positive integer n. We describe the n-th exterior power on $\mathrm{Mod}^{\mathrm{st}}$, using the following.

Lemma 3.21. *Let S be a scheme, let $a, b \in \mathrm{Seq}$ be of lengths s, t, respectively, and let n be a positive integer. Then the multilinear alternating map*

$$\bigwedge\colon \mathcal{O}_{\mathbb{P}^1_S}(a)^n \to \sum_{I\subseteq\{1,2,\ldots,s\},\#I=n} \mathcal{O}_{\mathbb{P}^1_S}\Big(\sum_{i\in I} a_i\Big)$$

mapping, locally on sections,

$$e \mapsto \left(\sum_{\pi} \operatorname{sgn}(\iota^{-1}\pi) \prod_{k=1}^{n} e_{k\pi(k)}\right)_{I\subseteq\{1,2,\ldots,s\},\#I=n}$$

is the n-th exterior power of $\mathcal{O}_{\mathbb{P}^1_S}(a)$. Here, π runs through the set of bijections from $\{1,2,\ldots,n\}$ to I and $\iota\colon \{1,2,\ldots,n\} \to I$ is the unique order-preserving bijection.

Moreover, the n-th exterior power $\bigwedge^n \varphi\colon \bigwedge^n \mathcal{O}_{\mathbb{P}^1_S}(a) \to \bigwedge^n \mathcal{O}_{\mathbb{P}^1_S}(b)$ of a $\mathcal{O}_{\mathbb{P}^1_S}$-linear map $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$, is given by the matrix indexed by subsets $I \subseteq \{1,2,\ldots,s\}$ and $J \subseteq \{1,2,\ldots,t\}$ of size n of which the (J,I)-entry is the $n \times n$-minor of φ (viewed as a $t \times s$-matrix with entries in $\mathcal{O}_S(S)[x,y]$) corresponding to I and J.

Therefore, if we, for $a \in \mathrm{Seq}$ of length s, write $\bigwedge^n a = (\sum_{i\in I} a_i)_{I\subseteq\{1,2,\ldots,s\},\#I=n}$, where we take the lexicographical order on the set of subsets I of $\{1,2,\ldots,s\}$, then we can identify $\bigwedge^n \mathcal{O}_{\mathbb{P}^1_S}(a)$ with $\mathcal{O}_{\mathbb{P}^1_S}(\bigwedge^n a)$. This defines a morphism of schemes $\bigwedge^n\colon \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ sending for any scheme S the morphism $M \in \mathrm{Mod}^{\mathrm{st}}(S)$ to $\bigwedge^n M$.

Lemma 3.22. *The functor $\bigwedge^n\colon \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{st}}$ is the morphism of schemes such that*

$$\bigwedge^n_{b,a} = \bigwedge^n|_{\mathrm{Mod}^{\mathrm{st}}_{b,a}}\colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \to \mathrm{Mod}^{\mathrm{st}}_{\bigwedge^n b, \bigwedge^n a}$$

sends, for any scheme S, the morphism $M \in \mathrm{Mod}^{\mathrm{st}}_{b,a}(S)$ to its n-th exterior power $\bigwedge^n M$.

Working this out as in Formulary 3.13, we get the following.

Formulary 3.23. Let n be a positive integer, and let $a, b \in \mathrm{Seq}$ be of lengths s, t, respectively. Notation is as in Formulary 3.13. Write for convenience

$$\mathrm{Mod}^{\mathrm{st}}_{\bigwedge^n b, \bigwedge^n a} = \operatorname{Spec}\mathbb{Z}\Big[x_{JI\lambda} : I \subseteq \{1,2,\ldots,s\}, J \subseteq \{1,2,\ldots,t\}, \#I = \#J = n, \\ 0 \le \lambda \le \textstyle\sum_{j\in J} b_j - \sum_{i\in I} a_i\Big].$$

Then the morphism $\bigwedge^n_{b,a}\colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \to \mathrm{Mod}^{\mathrm{st}}_{\bigwedge^n b,\bigwedge^n a}$ is given by

$$x_{JI\lambda} \mapsto \sum_{\pi} \mathrm{sgn}(\iota^{-1}\pi) \sum_{\sum_i \lambda_i = \lambda} \prod_{i\in I} x_{\pi(i)i\lambda_i},$$

where π runs through the set of bijections $I \to J$, and $\iota\colon I \to J$ is the unique order-preserving bijection.

3.3 The category scheme of standard algebras

Definition 3.24. Let S be a scheme, let $a \in \mathrm{Seq}$, and let $\mathcal{S} \subseteq \mathrm{Seq}$. An *standard algebra of type a* (resp. *locally standard algebra of type in $\mathcal{S}$*) over S is an $\mathcal{O}_{\mathbb{P}^1_S}$-algebra of which the underlying $\mathcal{O}_{\mathbb{P}^1_S}$-module is standard of type a (resp. locally standard of type in $\mathcal{S}$).

Equivalently, for $a \in \mathrm{Seq}$, a standard algebra of type a is given by a multiplication map $\mu\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(a)$ and a unit map $\iota\colon \mathcal{O}_{\mathbb{P}^1_S} \to \mathcal{O}_{\mathbb{P}^1_S}(a)$, such that the following diagrams commute.

- (associativity)

$$\begin{array}{ccc}
\mathcal{O}(a)\otimes \mathcal{O}(a)\otimes \mathcal{O}(a) & \xrightarrow{\mu\otimes \mathrm{id}} & \mathcal{O}(a)\otimes \mathcal{O}(a) \\
\downarrow{\scriptstyle \mathrm{id}\otimes\mu} & & \downarrow{\scriptstyle \mu} \\
\mathcal{O}(a)\otimes \mathcal{O}(a) & \xrightarrow[\mu]{} & \mathcal{O}(a)
\end{array}$$

- (commutativity)

$$\begin{array}{ccc}
\mathcal{O}(a)\otimes \mathcal{O}(a) & \xrightarrow{\Sigma} & \mathcal{O}(a)\otimes \mathcal{O}(a) \\
& {\scriptstyle \mu}\searrow \quad \swarrow{\scriptstyle \mu} & \\
& \mathcal{O}(a) &
\end{array}$$

- (unit)

$$\begin{array}{ccc}
\mathcal{O}(a) & \xrightarrow{\iota\otimes \mathrm{id}} & \mathcal{O}(a)\otimes \mathcal{O}(a) \\
& {\scriptstyle \mathrm{id}}\searrow & \downarrow{\scriptstyle \mu} \\
& & \mathcal{O}(a)
\end{array}$$

With this description, we see that a morphism $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$ of standard algebras is a morphism of $\mathcal{O}_{\mathbb{P}^1_S}$-modules such that the following diagram commutes.

$$\begin{array}{ccc}
\mathcal{O}_{\mathbb{P}^1_S}(a) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow{\varphi\otimes\varphi} & \mathcal{O}_{\mathbb{P}^1_S}(b) \otimes_{\mathcal{O}_{\mathbb{P}^1_S}} \mathcal{O}_{\mathbb{P}^1_S}(b) \\
\downarrow{\scriptstyle \mu} & & \downarrow{\scriptstyle \mu} \\
\mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow[\varphi]{} & \mathcal{O}_{\mathbb{P}^1_S}(b) \\
\uparrow{\scriptstyle \iota} & & \uparrow{\scriptstyle \iota'} \\
\mathcal{O}_{\mathbb{P}^1_S} & = & \mathcal{O}_{\mathbb{P}^1_S}
\end{array}$$

Definition 3.25. Let $\mathcal{S} \subseteq \mathrm{Seq}$. The *category scheme* $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *of locally standard algebras with type in* $\mathcal{S}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ sending a scheme S to the category of locally standard algebras over S with type in $\mathcal{S}$.

We show that this functor is indeed representable, again using an auxiliary functor.

Definition 3.26. Let $a, b \in \mathrm{Seq}$. The functor $\mathrm{Alg}^{\mathrm{st}}_{b,a}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Set}$ sending a scheme S to the set of tuples $(\mu_b, \iota_b, \varphi, \mu_a, \iota_a)$ such that (μ_a, ι_a) defines a structure of an $\mathcal{O}_{\mathbb{P}^1_S}$-algebra on $\mathcal{O}_{\mathbb{P}^1_S}(a)$, (μ_b, ι_b) defines a structure of an algebra on $\mathcal{O}_{\mathbb{P}^1_S}(b)$, and $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$ is a morphism of $\mathcal{O}_{\mathbb{P}^1_S}$-algebras.

Lemma 3.27. *Let* $a, b \in \mathrm{Seq}$. *The functor* $\mathrm{Alg}^{\mathrm{st}}_{b,a}$ *is representable by an affine scheme of finite type.*

Proof. In fact, it is clear from the description of the category of standard algebras given above that $\mathrm{Alg}^{\mathrm{st}}_{b,a}$ is a subscheme of $\mathbb{A}_k^{N(b,b\otimes b)+N(b,0)+N(b,a)+N(a,a\otimes a)+N(a,0)}$. □

Corollary 3.28. *Let* $\mathcal{S} \subseteq \mathrm{Seq}$. *Then* $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is representable by the tuple* $(\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}, \alpha, \omega, \circ)$, *where*

- $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} = \coprod_{a,b\in\mathcal{S}} \mathrm{Alg}^{\mathrm{st}}_{b,a}$;
- $\alpha\colon \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} \to \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\alpha_{b,a} = \alpha|_{\mathrm{Alg}^{\mathrm{st}}_{b,a}}\colon \mathrm{Alg}^{\mathrm{st}}_{b,a} \to \mathrm{Alg}^{\mathrm{st}}_{a,a}$$
is given by $(\mu_b, \iota_b, \varphi, \mu_a, \iota_a) \mapsto (\mu_a, \iota_a, \mathrm{id}, \mu_a, \iota_a)$;
- $\omega\colon \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} \to \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\omega_{b,a} = \omega|_{\mathrm{Alg}^{\mathrm{st}}_{b,a}}\colon \mathrm{Alg}^{\mathrm{st}}_{b,a} \to \mathrm{Alg}^{\mathrm{st}}_{b,b}$$
is given by $(\mu_b, \iota_b, \varphi, \mu_a, \iota_a) \mapsto (\mu_b, \iota_b, \mathrm{id}, \mu_b, \iota_b)$;
- $\circ\colon \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} \times_{\alpha,\omega} \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} \to \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is the morphism such that*
$$\circ_{c,b,a} = \circ|_{\mathrm{Alg}^{\mathrm{st}}_{c,b} \times_{\alpha,\omega} \mathrm{Alg}^{\mathrm{st}}_{b,a}}\colon \mathrm{Alg}^{\mathrm{st}}_{c,b} \times_{\alpha,\omega} \mathrm{Alg}^{\mathrm{st}}_{b,a} \to \mathrm{Alg}^{\mathrm{st}}_{c,a}$$
is given by
$$(\mu_c, \iota_c, \psi, \mu_b, \iota_b) \circ (\mu_b, \iota_b, \varphi, \mu_a, \iota_a) = (\mu_c, \iota_c, \psi \circ \varphi, \mu_a, \iota_a).$$

If $\mathcal{S}$ *is finite, then* $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is affine and of finite type.*

Proof. By definition, the functor $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ is the Zariski sheafification of the disjoint union of the representable functors $\mathrm{Alg}^{\mathrm{st}}_{b,a}$ for $a, b \in \mathcal{S}$. Therefore it is representable by $\coprod_{a,b\in\mathcal{S}} \mathrm{Alg}^{\mathrm{st}}_{b,a}$. Moreover, for all schemes S we have by construction that the morphisms $\alpha(S), \omega(S), \circ(S)$ coincide with the source, target, and composition on the category of locally standard algebras of type in $\mathcal{S}$ over S.

If $\mathcal{S}$ is finite, then $\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ is a finite disjoint union of affine schemes of finite type and therefore is itself affine and of finite type. □

Note that the relative spectrum functor over $\mathbb{P}^1$ embeds, for all k-schemes S, the category $\mathrm{Alg}^{\mathrm{st}}(S)$ contravariantly and fully faithfully in the category of finite locally free $\mathbb{P}^1_S$-schemes. We will call the objects in the essential image *standard schemes*.

3.4 Group actions

We present finite groups by their multiplication tables.

Let Γ and G be multiplicatively written finite groups, with Γ acting by automorphisms on G. Then recall that a Γ-*equivariant G-action* on a set X consists of an action of Γ and of G on X, such that for all $\gamma \in \Gamma$, $g \in G$, and $x \in X$, we have $(\gamma g)x = \gamma\big(g(\gamma^{-1}x)\big)$. By the Yoneda lemma, this extends to arbitrary categories.

Example 3.29. The smallest example with non-trivial Γ-action on G and non-trivial action of G on X is the following; let $G = \mathbb{Z}/3\mathbb{Z}$, and let $\Gamma = \{\pm 1\}$ act on G via the unique non-trivial automorphism of G. Let $X = G$, together with the Γ-action. Then the regular action of G on X is Γ-equivariant.

One other way to describe this action is as $G = X = \mu_{3,\mathbb{R}}(\mathbb{C})$, and $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ acting on G and X by complex conjugation.

Definition 3.30. Let S be a scheme, let $a \in \mathrm{Seq}$, and let $\mathcal{S} \subseteq \mathrm{Seq}$. A *standard Γ-equivariant G-algebra of type a* (resp. *locally standard Γ-equivariant G-algebra of type in $\mathcal{S}$*) over S is a Γ-equivariant G-algebra over $\mathcal{O}_{\mathbb{P}^1_S}$ which is standard of type a (resp. locally standard of type in $\mathcal{S}$) as an $\mathcal{O}_{\mathbb{P}^1_S}$-module.

An equivalent description is the following.

Note that an action of Γ on a standard algebra is given by a set $\{\rho_\gamma\}$ of endomorphisms such that

- $\rho_1 = \mathrm{id}$;
- $\rho_\gamma \rho_{\gamma'} = \rho_{\gamma\gamma'}$ for all $\gamma, \gamma' \in \Gamma$.

A morphism $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$ between standard algebras that have a Γ-action is Γ-equivariant if and only if for all $\gamma \in \Gamma$ the following diagram commutes.

$$\begin{array}{ccc} \mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow{\varphi} & \mathcal{O}_{\mathbb{P}^1_S}(b) \\ {\scriptstyle\rho_\gamma}\downarrow & & \downarrow{\scriptstyle\rho_\gamma} \\ \mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow{\varphi} & \mathcal{O}_{\mathbb{P}^1_S}(b) \end{array}$$

Now a Γ-equivariant G-action on a standard Γ-algebra is given by a set $\{r_g\}$ of endomorphisms such that

- $r_1 = \mathrm{id}$;
- $r_g r_{g'} = r_{gg'}$ for all $g, g' \in G$;
- $r_{\gamma g} = \rho_\gamma r_g \rho_\gamma^{-1}$ for all $\gamma \in \Gamma$, $g \in G$.

A Γ-equivariant morphism $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(a) \to \mathcal{O}_{\mathbb{P}^1_S}(b)$ between standard Γ-equivariant G-algebras is G-equivariant if and only if for all $g \in G$ the following diagram commutes.

$$\begin{array}{ccc} \mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow{\varphi} & \mathcal{O}_{\mathbb{P}^1_S}(b) \\ {\scriptstyle r_g}\downarrow & & \downarrow{\scriptstyle r_g} \\ \mathcal{O}_{\mathbb{P}^1_S}(a) & \xrightarrow{\varphi} & \mathcal{O}_{\mathbb{P}^1_S}(b) \end{array}$$

Definition 3.31. Let $\mathcal{S} \subseteq \mathrm{Seq}$. The *category scheme* $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *of locally standard* Γ*-equivariant* G*-algebras of type in* $\mathcal{S}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ sending a scheme S to the category of locally standard Γ-equivariant G-algebras over S of type in $\mathcal{S}$.

As usual, we define the corresponding auxiliary functor in order to show that $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ is representable.

Definition 3.32. Let $a, b \in \mathrm{Seq}$. The functor $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{b,a}$ is the functor from $\mathrm{Sch}^{\mathrm{op}}$ to Set sending a scheme S to the set of $\big((r'_g), (\rho'_\gamma), \varphi, (r_g), (\rho_\gamma)\big)$ such that $\varphi \in \mathrm{Alg}^{\mathrm{st}}_{b,a}(S)$, the tuples (r_g) and (ρ_γ) define a Γ-equivariant G-action on the source of φ, and the tuples (r'_g) and (ρ'_γ) define a Γ-equivariant G-action on the target of φ.

Lemma 3.33. *Let* $a, b \in \mathrm{Seq}$. *The functor* $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{b,a}$ *is representable by an affine* k*-scheme of finite type.*

Proof. By construction, it is representable by a closed subscheme of $(\mathrm{Alg}^{\mathrm{st}}_{b,a})^{1+2e+2n}$. □

Corollary 3.34. *Let* $\mathcal{S} \subseteq \mathrm{Seq}$. *Then* $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is representable. If* $\mathcal{S}$ *is finite, then* $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ *is affine and of finite type.*

Note that for any finite group G we have $(G, 1)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} = (1, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$; in this case, we will use the notation $G\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$ instead. Moreover, we have $1\text{-}\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}} = \mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$.

As seen in the previous section, we have for every scheme S a fully faithful contravariant functor from $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}(S)$ into the category of Γ-equivariant G-schemes finite locally over $\mathbb{P}^1_S$; let us call objects in its essential image *standard* Γ*-equivariant* G*-schemes*.

3.5 Category schemes of free modules and algebras

We first consider the free modules over $\mathcal{O}_S$.

Definition 3.35. Let S be a scheme, let $\mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. A *component-locally free* $\mathcal{O}_S$*-module of rank in* $\mathcal{R}$ is an $\mathcal{O}_S$-module $\mathcal{E}$ such that there exists a locally constant map $q\colon S \to \mathcal{R}$ such that $\mathcal{E}|_{q^{-1}r} = \mathcal{O}^r_{q^{-1}r}$ for all $r \in \mathcal{R}$. A *component-locally free* $\mathcal{O}_S$*-module* is a component-locally free $\mathcal{O}_S$-module with rank in $\mathbb{Z}_{\geq 0}$.

We define the corresponding category scheme.

Definition 3.36. Let $\mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. The *category scheme* $\mathrm{Mod}^{\mathrm{free}}_{s,r}$ *of free modules of rank in* $\mathcal{R}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ sending a scheme S to the category of component-locally free $\mathcal{O}_S$-modules with rank in $\mathcal{R}$.

In order to show that $\mathrm{Mod}^{\mathrm{free}}_{\mathcal{R}}$ is indeed a category scheme, we could repeat the same strategy as in Section 3.2. Alternatively, we note that if we have a free module $\mathcal{O}_S^r$ on S, it pulls back to a standard module $\mathcal{O}^r_{\mathbb{P}^1_S}$ over S, giving a natural transformation $\mathrm{Mod}^{\mathrm{free}} \to \mathrm{Mod}^{\mathrm{st}}$ of functors $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ such that for all schemes S, the functor $\mathrm{Mod}^{\mathrm{free}}(S) \to \mathrm{Mod}^{\mathrm{st}}(S)$ is fully faithful, and has as essential image those objects of $\mathrm{Mod}^{\mathrm{st}}(S)$ that have as type a finite sequence of zeroes. Hence we have the following.

Proposition 3.37. *Let* $\mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. *Then* $\mathrm{Mod}^{\mathrm{free}}_{\mathcal{R}} = \mathrm{Mod}^{\mathrm{st}}_{\mathcal{S}}$, *where* $\mathcal{S}$ *is the set of finite sequences of zeroes with length in* $\mathcal{R}$.

Recall that $\mathrm{Mod}^{\mathrm{st}}$, and therefore $\mathrm{Mod}^{\mathrm{free}}$ as well, is a disjoint union of affine schemes. Let us introduce some notation for these affine schemes.

Definition 3.38. Let $r, s \in \mathbb{Z}_{\geq 0}$. Then the scheme $\mathrm{Mod}^{\mathrm{free}}_{s,r}$ is $\mathrm{Mod}^{\mathrm{st}}_{0_s,0_r}$, where $0_r, 0_s$ are the zero sequences of lengths r and s, respectively.

Proposition 3.39. *Let* $\mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. *Then* $\mathrm{Mod}^{\mathrm{free}}_{\mathcal{R}} = \coprod_{r,s \in \mathcal{R}} \mathrm{Mod}^{\mathrm{free}}_{s,r}$.

We do the same for the category scheme $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{st}}$.

Definition 3.40. Let Γ, G be finite groups, together with an action of Γ on G by automorphisms. A *component-locally free* Γ*-equivariant* G*-algebra over* $\mathcal{O}_S$ *of degree in* $\mathcal{D}$ is a Γ-equivariant G-algebra over $\mathcal{O}_S$ that is component-locally free as a $\mathcal{O}_S$-module.

Definition 3.41. Let $\mathcal{D} \subseteq \mathbb{Z}_{\geq 0}$. The *category scheme* $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}_{\mathcal{D}}$ *of component-locally free* Γ*-equivariant* G*-algebras of degree in* $\mathcal{D}$ is the functor $\mathrm{Sch}^{\mathrm{op}} \to \mathrm{Cat}$ sending a scheme S to the category of component-locally free Γ-equivariant G-algebras over $\mathcal{O}_S$ of degree in $\mathcal{D}$.

In the same way as before, we show the following.

Proposition 3.42. *Let* Γ, G *be finite groups, together with an action of* Γ *on* G *by automorphisms. The functor* $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}_{\mathcal{D}}$ *is representable by* $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{st}}_{\mathcal{S}}$, *where* $\mathcal{S}$ *is the set of sequences of zeroes of length in* $\mathcal{D}$.

Finally, we describe $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}$ as a disjoint union of affine schemes.

Definition 3.43. Let $d, e \in \mathbb{Z}_{\geq 0}$. Then the scheme $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}_{e,d}$ is $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{st}}_{0_e,0_d}$, where $0_d, 0_e \in \mathrm{Seq}$ are the zero sequences of lengths d and e, respectively.

Proposition 3.44. *Let* $\mathcal{D} \subseteq \mathbb{Z}_{\geq 0}$. *Then* $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}_{\mathcal{D}} = \coprod_{d,e \in \mathcal{D}} (\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}_{e,d}$.

As in the previous two sections, we have for all schemes S a fully faithful contravariant functor from $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{free}}(S)$ to the category of Γ-equivariant G-schemes finite locally free over S. We call the objects of its essential image the *component-locally free* Γ*-equivariant* G*-schemes*.

3.6 The slice category scheme

We treat this construction in general for clarity, although we only need it for the category schemes $(\Gamma, G)\text{-}\operatorname{Alg}^{\mathrm{st}}_{\mathcal{S}}$ and $(\Gamma, G)\text{-}\operatorname{Alg}^{\mathrm{free}}_{\mathcal{D}}$ from the previous section.

Definition 3.45. Let $\mathcal{C}$ be a category scheme over a scheme S, and let $X \in \operatorname{Ob}\mathcal{C}(S)$. Then the *slice category scheme* $\mathcal{C}_X$ *of* $\mathcal{C}$ *over* X is the functor $\operatorname{Sch}_S^{\mathrm{op}} \to \mathrm{Cat}$ sending an S-scheme T to the category $\mathcal{C}(T)_X$ of objects in $\mathcal{C}(T)$ with a morphism to X (or rather the image of X under $\mathcal{C}(S) \to \mathcal{C}(T)$).

Lemma 3.46. *Let $\mathcal{C}$ be a category scheme over a scheme S, and let $X \in \operatorname{Ob}\mathcal{C}(S)$. Then $\mathcal{C}_X$ is representable.*

Proof. Note that for any S-scheme T, a morphism in $\mathcal{C}_X(T)$ is given by a commutative triangle

$$\begin{array}{ccc} Z & \longrightarrow & Y \\ & \searrow \quad \swarrow & \\ & X & \end{array}$$

of morphisms in $\mathcal{C}(T)$. Therefore $\mathcal{C}_X$ is representable by a closed subscheme of $\mathcal{C}^3$. □

Note that if X is the terminal object of $\mathcal{C}(S)$, then $\mathcal{C}_X = \mathcal{C}$.

3.7 Torsors over smooth projective curves

Let k be a factorial field. Let Γ, G be finite groups, together with an action of Γ on G by automorphisms. Let $f\colon X \to \operatorname{Spec} k$ be a smooth projective curve, together with a given finite locally free morphism $X \to \mathbb{P}^1_k$, and an action of Γ on X over $\mathbb{P}^1_k$. Then note that X is (isomorphic to) an object of $(\Gamma, G)\text{-}\operatorname{Alg}^{\mathrm{st}}_k(k)$, say of type a. In the next few sections, we will construct a category scheme over k of Γ-equivariant G-torsors on X.

3.8 Fibre functors

Let $p = (0:1) \in \mathbb{P}^1_k(k)$, and let N be a positive integer. What we describe below will work for any $p \in \mathbb{P}^1_k(k)$ with some fixed pre-computation per finite sequence of integers – namely the expressions of a number of powers of x as linear combinations of powers of $x - a$ in $k[x]$. Since we do not need a lot of distinct points in the end (in fact we will only need two), we will restrict to the case $p = (0:1)$ (and by symmetry the case $p = (1:0)$ as well).

Denote for $N \geq 2$ by $p^{(N)}$ the $(N-1)$-th infinitesimal neighbourhood of p in $\mathbb{P}^1_k$; we set $p^{(1)} = p$, although we will usually omit the superscript (1) from the notation. Note that for any k-scheme S the pullback of the standard module of type a (with a a sequence of length s) along the closed immersion $p^{(N)}_S \to \mathbb{P}^1_S$ is as $\mathcal{O}_S$-module isomorphic to $(\mathcal{O}_S^N)^s$. Therefore, for any k-scheme S, the pullback of a locally standard module along $p^{(N)}_S \to \mathbb{P}^1_S$ is component-locally free.

Definition 3.47. Let N be a positive integer. The *fibre functors*

$$\Phi_{p^{(N)}} \colon \mathrm{Mod}^{\mathrm{st}} \to \mathrm{Mod}^{\mathrm{free}}, \qquad \Phi_{p^{(N)}} \colon (\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}} \to (\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{free}}$$

are the functors sending, for any scheme S, an object to its pullback along $p_S^{(N)} \to \mathbb{P}^1_S$.

We have the following description of $\Phi_{p^{(N)}}$.

Proposition 3.48. *Let N be a positive integer, and let $a, b \in \mathrm{Seq}$ be of lengths s and t, respectively. Then $\Phi_{p^{(N)},b,a} \colon \mathrm{Mod}^{\mathrm{st}}_{b,a} \to \mathrm{Mod}^{\mathrm{free}}_{Nt,Ns}$ sends, for any k-scheme S, the matrix $M \in \mathrm{Mat}_{b,a}(S)$ to the $Nt \times Ns$-matrix of which the $\big((j,j'),(i,i')\big)$-entry is the coefficient of $x^{j'-i'}$ in $M_{ji}(x,1)$.*

3.9 Finite flat covers

We now use the previous section to construct a category scheme of standard schemes that are finite locally over X of *constant* rank. The following criterion guarantees that any morphism $Y \to X$ of standard schemes is automatically finite locally free.

Lemma 3.49. *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 $\mathbb{P}^1_S$. Then Y is a finite locally free X-scheme.*

Proof. As X and Y are finite and of finite presentation over $\mathbb{P}^1_S$, Y is also finite and of finite presentation over X. Hence it suffices to show that Y is flat over X. By the fibre-wise criterion for flatness (see e.g. Görtz and Wedhorn [16, Cor. 14.25]), it suffices to prove that for all points $s \in S$, we have Y_s flat over X_s. Hence we assume without loss of generality that S is the spectrum of a field.

Let $y \in Y$ be a point, and let $x \in X$ and $p \in \mathbb{P}^1_S$ be their images. As X is smooth over S, the ring $\mathcal{O}_{X,x}$ is a torsion-free $\mathcal{O}_{\mathbb{P}^1_S,p}$-algebra, which is either a discrete valuation ring, or a field. As $\mathcal{O}_{Y,y}$ is finite free, hence torsion-free, over $\mathcal{O}_{\mathbb{P}^1_S,p}$, it follows that $\mathcal{O}_{Y,y}$ is torsion-free over $\mathcal{O}_{X,x}$ as well, hence flat. Hence Y is flat over X, as desired. □

We want to be able to check when (or otherwise enforce that) a morphism $Y \to X$ of standard schemes has constant rank. To this end, we use the following criterion.

Lemma 3.50. *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 $Y_{(0:1)}$ is finite locally free over $X_{(0:1)}$ 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 $X_{(0:1)}$ intersects all components of X, from which our claim follows. □

Finally, note that $X_{(0:1)}$ is finite over k, so any finite locally free $\mathcal{O}_{X_{(0:1)}}$-module is in fact free. This motivates the following.

Definition 3.51. Let $\mathcal{S} \subseteq \mathrm{Seq}$. The *category scheme* $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ *of standard finite flat covers of* X *of type in* $\mathcal{S}$ is the functor $\mathrm{Sch}_k^{\mathrm{op}} \to \mathrm{Cat}$ that sends a k-scheme S to the category in which the objects are triples $(\mathcal{O}_Y, n, B)$, where $\mathcal{O}_Y$ is an object of $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{st}}_{X,\mathcal{S}}(S)$, $n \geq 0$ is an integer, and $B\colon \mathcal{O}^n_{X_{(0:1)}} \to \mathcal{O}_{Y_{(0:1)}}$ is an isomorphism of $\mathcal{O}_{X_{(0:1)}}$-modules.

The functor $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ is indeed a category scheme.

Proposition 3.52. *Let* $\mathcal{S} \subseteq \mathrm{Seq}$. *Then* $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ *is representable. If* $\mathcal{S}$ *is finite, then* $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ *is affine and of finite type over* k.

Proof. Let S be a k-scheme, and let $(\mathcal{O}_Y, e, B)$ be an object of $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}(S)$. Note that for B, being an isomorphism of $\mathcal{O}_{X_{(0:1)}}$-modules is equivalent to being an $\mathcal{O}_S$-linear isomorphism such that the following diagram commutes.

$$\begin{array}{ccc}
\mathcal{O}_{X_{(0:1)}} \otimes \mathcal{O}^n_{X_{(0:1)}} & \xrightarrow{\mathrm{id}\otimes B} & \mathcal{O}_{X_{(0:1)}} \otimes \mathcal{O}_Y \\
\downarrow & & \downarrow \\
\mathcal{O}^n_{X_{(0:1)}} \otimes \mathcal{O}^n_{X_{(0:1)}} & & \mathcal{O}_Y \otimes \mathcal{O}_Y \\
{\scriptstyle\mu}\downarrow & & \downarrow{\scriptstyle\mu} \\
\mathcal{O}^n_{X_{(0:1)}} & \xrightarrow[B]{} & \mathcal{O}_Y
\end{array}$$

This establishes $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ as a closed subscheme of $(\Gamma, G)\text{-}\,\mathrm{Alg}^{\mathrm{st}}_{X,\mathcal{S}} \times (\mathrm{Mod}^{\mathrm{free}})^4$ (as we add the data of the isomorphism and its inverse of both the source and the target). □

3.10 Finite étale covers

We now construct a category subscheme of $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ of those objects that are étale over $\mathcal{O}_X$. The next criterion allows us to restrict our attention to non-positive sequences of integers, as finite étale covers of a smooth projective curve are again smooth and projective.

Lemma 3.53. *Let* S *be a scheme, let* $a \in \mathrm{Seq}$, *and let* X *be a standard scheme of type* a, *and such 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 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 3.54. Of course, the converse is not true; a counterexample is the $\mathcal{O}_{\mathbb{P}^1_k}$-module $\mathcal{O}_{\mathbb{P}^1_k} \oplus \mathcal{O}_{\mathbb{P}^1_k}(-1)\varepsilon$ with multiplication given by $\varepsilon^2 = 0$.

Now we need a criterion for a morphism $Y \to X$ of constant rank of standard schemes to be étale. 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 3.55. 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 $\operatorname{Tr}_f \mu\colon \mathcal{O}_Y \otimes_{\mathcal{O}_X} \mathcal{O}_Y \to \mathcal{O}_X$. The *discriminant* Δ_f of f is the determinant (over $\mathcal{O}_X$) of the trace form τ_f.

Definition 3.56 (cf. Ferrand [11])**.** 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 Deligne [8, Eq. 7.1.1] and the fact that norms (of line bundles) commute with tensor products and duals (see EGA2 [17, Sec. 6.5] and Ferrand [11, 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.

Therefore, we have the following.

Corollary 3.57. *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. Lieblich [28, Sec. 4.1].

Theorem 3.58 (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 3.59. *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.*

Definition 3.60. Let $\mathcal{R}$ be a set of non-negative integers. The *category scheme* $\mathrm{Et}^{\mathrm{proj}}_{X,\mathcal{D}}$ *of standard finite étale Γ-equivariant G-schemes over X with degree in $\mathcal{D}$* is the functor $\mathrm{Sch}_k^{\mathrm{op}} \to \mathrm{Cat}$ sending a k-scheme S to the subcategory of $\mathrm{Flat}^{\mathrm{proj}}_X(S)$ of finite étale morphisms $Y \to X$ of standard schemes over S, with degree in $\mathcal{D}$.

We show that $\mathrm{Et}^{\mathrm{proj}}_{X,\mathcal{D}}$ is indeed a category scheme.

Proposition 3.61. *Let $\mathcal{D}$ be a set of non-negative integers. Then $\mathrm{Et}^{\mathrm{proj}}_{X,\mathcal{D}}$ is representable. If $\mathcal{D}$ is finite, then $\mathrm{Et}^{\mathrm{proj}}_{X,\mathcal{D}}$ is affine and of finite type over k.*

Proof. Let $\mathcal{S}$ be the set of non-positive sequences b of integers (of length t) such that

$$\frac{t}{s} = \frac{\sum_\tau b_\tau}{\sum_\sigma a_\sigma} \in \mathcal{D}.$$

Note that $\mathcal{S}$ is finite if $\mathcal{D}$ is finite. Then by Lemma 3.49, Lemma 3.53, and Corollary 3.59, the desired category scheme is the category scheme in which the objects are the objects $\mathcal{O}_Y$ of $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}}$ such that $\Delta_{\mathcal{O}_Y/\mathcal{O}_{\mathbb{P}^1}}$ and $\Delta^{\otimes \frac{t}{s}}_{\mathcal{O}_X/\mathcal{O}_{\mathbb{P}^1}}$ differ by a unit ε. This establishes $\mathrm{Et}^{\mathrm{proj}}_{X,\mathcal{D}}$ (explicitly if $\mathcal{D}$ is finite) as a closed subscheme of $\mathrm{Flat}^{\mathrm{proj}}_{X,\mathcal{S}} \times \mathbb{A}^4_k$ (as we add the data of the units and their inverses corresponding to the source and target). □

3.11 Torsors

We now identify the closed subscheme of $\mathrm{Et}^{\mathrm{proj}}_{X,n}$ consisting of (morphisms between) G-torsors. To this end, we first prove the following lemmas, in order to show that checking whether an object of $\mathrm{Et}^{\mathrm{proj}}_{X,n}$ is a G-torsor can essentially be done in the category scheme $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_X$.

Lemma 3.62. *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 $\varphi\colon \underline{G}_X \times_X Y \to Y \times_X Y$ 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 $\underline{G}_X \times_X Y$ 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 3.63. *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 $\underline{G}_X \times_X Y \to Y \times_X Y$ 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. □

Corollary 3.64. *Let S be a scheme, let $f\colon Y \to X$ be a finite étale morphism of $\mathbb{P}^1_S$-schemes, and let G be a finite group of order n acting on Y/X. Then Y is a G-torsor on X if and only if $Y_{(0:1)}$ is a G-torsor on $X_{(0:1)}$.*

Proof. Note that by Lemma 3.62 we may assume that S is the spectrum of a field, in which case it follows from Lemma 3.63 and the fact that $X_{(0:1)}$ intersects all components of X. □

Recall that for a k-scheme S, objects of $\mathrm{Et}^{\mathrm{proj}}_{X,n}(S)$ are "locally" of the form $(\mathcal{O}_Y, n, B)$, where $\mathcal{O}_Y$ is an object of $(\Gamma, G)\text{-}\mathrm{Alg}^{\mathrm{st}}_X(S)$, and B is an isomorphism $\mathcal{O}^n_{X_{0:1}} \to \mathcal{O}_{Y_{0:1}}$ of $\mathcal{O}_{X_{(0:1)}}$-modules.

Definition 3.65. Let X be a smooth projective curve together with an action of a finite group Γ that is a standard scheme over k, say of type a. Let G be a finite group of order n on which Γ acts by automorphisms. The *category scheme* $\mathrm{Tors}^{\mathrm{proj}}_X$ *of G-torsors on X* is the functor $\mathrm{Sch}^{\mathrm{op}}_k \to \mathrm{Cat}$ sending a k-scheme S to the full subcategory of $\mathrm{Et}^{\mathrm{proj}}_{X,n}(S)$ of G-torsors on X.

Proposition 3.66. *The functor $\mathrm{Tors}^{\mathrm{proj}}_X$ is representable by an affine category scheme of finite type over k.*

Proof. It suffices to express explicitly the condition that an object $(\mathcal{O}_Y, n, B)$ of $\mathrm{Et}^{\mathrm{proj}}_{X,n}$ is a G-torsor. By Corollary 3.64, this is equivalent to

$$\mathcal{O}_{Y_{(0:1)}} \otimes_{\mathcal{O}_{X_{(0:1)}}} \mathcal{O}_{Y_{(0:1)}} \to \mathcal{O}^n_{Y_{(0:1)}},\ y_1 \otimes y_2 \mapsto (gy_1y_2)_{g\in G}$$

being an isomorphism of $\mathcal{O}_{\mathbb{P}^1}$-modules. Note that we can compute the morphism from $\mathrm{Ob}\,\mathrm{Et}^{\mathrm{proj}}_{X,n}$ to $\mathrm{Alg}^{\mathrm{free}}_{X_{(0:1)}}$ sending an object $(\mathcal{O}_Y, n, B)$ to the following composition in $\mathrm{Alg}^{\mathrm{free}}_{X_{(0:1)}}$.

$$\begin{array}{ccccc} & & \mathcal{O}_{X_{(0:1)}}^{n^2} & & \\ & & \| & & \\ \mathcal{O}_{X_{0:1}}^{n} \otimes_{\mathcal{O}_{X_{(0:1)}}} \mathcal{O}_{X_{(0:1)}}^{n} & \xrightarrow{B\otimes B} & \mathcal{O}_{Y_{(0:1)}} \otimes_{\mathcal{O}_{X_{0:1}}} \mathcal{O}_{Y_{(0:1)}} & & \\ & & \downarrow & & \\ & & \mathcal{O}_{Y_{(0:1)}}^{n} & & \end{array}$$

This establishes $\mathrm{Tors}_X^{\mathrm{proj}}$ explicitly as a closed subscheme of $\mathrm{Et}_{X,n}^{\mathrm{proj}} \times (\mathrm{Alg}_{X_{(0:1)}}^{\mathrm{free}})^2$, by adding the data of the inverse of the morphism above for both the source and the target. □

3.12 The stack of G-torsors

We show that the category scheme $\mathrm{Tors}_X^{\mathrm{proj}}$ over k defines a presentation of the stack $\mathcal{T} = \mathcal{T}_{\Gamma,X}^{G}$ over k of Γ-equivariant G-torsors on X. More precisely, we show the following.

Theorem 3.67. *Let $[\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}} / \mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}}] \to \mathcal{T}$ be the functor sending for any k-scheme S, the object $T \in \mathrm{Ob}\,\mathrm{Tors}_X^{\mathrm{proj}}(S)$ to the underlying Γ-equivariant G-torsor on X. For all field extensions l of k, the functor $[\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}} / \mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}}](l) \to \mathcal{T}(l)$ is an equivalence. The isomorphism classes in $\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}}$ are irreducible. The stack $\mathcal{T}$ is the fppf stackification of $[\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}} / \mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}}]$.*

Therefore by Proposition 3.1 we have the following.

Corollary 3.68. *The map $\mathrm{Ob}\,\mathrm{Tors}_X^{\mathrm{proj}}(\bar{k}) \to \mathrm{Ob}\,\mathcal{T}(\bar{k})/\cong$ factors through a bijection $\pi_0(\mathrm{Ob}\,\mathrm{Tors}_{X,k^{\mathrm{sep}}}^{\mathrm{proj}}) \to \mathrm{Ob}\,\mathcal{T}(k^{\mathrm{sep}})/\cong$ that is $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant, and the connected components of $\mathrm{Ob}\,\mathrm{Tors}_{X,k^{\mathrm{sep}}}^{\mathrm{proj}}$ are irreducible.*

We will first show the following.

Theorem 3.69. *Let k be a field, let G be a finite group, let X be a smooth projective curve together with a finite locally free morphism $X \to \mathbb{P}^1$. Then for all k-schemes S and all étale G-torsors Y over X_S, the $\mathcal{O}_{\mathbb{P}^1_S}$-algebra $\mathcal{O}_Y$ is as an $\mathcal{O}_{\mathbb{P}^1_S}$-module fppf locally isomorphic to a standard module.*

Proof. Let S be a k-scheme, and let Y be an étale G-torsor over X_S. First note that we can reduce to the case that S is affine, and since Y is smooth over S, we can further reduce to the case that S is of finite type over k by Grothendieck [18, Prop. 17.7.8].

Let $s\colon \mathrm{Spec}\,\kappa(s) \to S$ be a closed point of S, so that $\kappa(s)$ is finite over k. Let Y_s/X_s denote the pullback of Y/X_S along $s\colon \mathrm{Spec}\,\kappa(s) \to S$. As Y_s is finite locally free over $\mathbb{P}^1_{\kappa(s)}$, we see that $\mathcal{O}_{Y_s}$ is a standard module. Consider the base change $S_{\kappa(s)}$ of S along $\mathrm{Spec}\,\kappa(s) \to \mathrm{Spec}\,k$.

Let $Y_1/X_{S_{\kappa(s)}}$ be the pullback of Y/X_S along $S_{\kappa(s)} \to S$, and let $Y_2/X_{S_{\kappa(s)}}$ be the pullback of Y_s/X_s along $S_{\kappa(s)} \to \operatorname{Spec}\kappa(s)$. Note that $\mathcal{O}_{Y_2}$ is isomorphic to a standard module by Theorem 1.23. Let $\mathcal{I}_{S_{\kappa(s)}}(Y_1, Y_2)$ denote the functor sending T to $\operatorname{Isom}_{X_T,G}(Y_{1,T}, Y_{2,T})$. By descent, it is representable by a finite étale $S_{\kappa(s)}$-scheme and $\mathcal{I}_{S_{\kappa(s)}}(Y_1, Y_2)(s) \neq \emptyset$. Therefore (finite) étale locally around s in $S_{\kappa(s)}$, we have $Y_1 \cong Y_2$. As $S_{\kappa(s)} \to S$ is an fppf cover, we deduce that the $\mathcal{O}_{\mathbb{P}^1_S}$-module $\mathcal{O}_Y$ is fppf locally isomorphic to a standard module over S. □

Corollary 3.70. *The stack $\mathcal{T}$ is the fppf stackification of $[\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}}/\mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}}]$.*

Proof. We show that for any k-scheme S and any Γ-equivariant G-torsor Y on X_S, the torsor Y is fppf locally on S an object of $\mathrm{Tors}_X^{\mathrm{proj}}$.

Let S be a k-scheme, and let Y be a Γ-equivariant G-torsor on X_S. Then by Theorem 3.69, fppf locally on S the $\mathcal{O}_{\mathbb{P}^1_S}$-module $\mathcal{O}_Y$ is a standard module, and $Y_{(0:1)}$ is a G-torsor on $X_{S,(0:1)}$, so étale locally on S the G-torsor $Y_{(0:1)}$ is isomorphic to $\coprod_{g\in G} X_{S,(0:1)}$. Therefore by construction of $\mathrm{Tors}_X^{\mathrm{proj}}$, it follows that $\mathcal{T}$ is the stackification of $[\mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}}/\mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}}]$, as desired. □

So in particular, the category scheme $\mathrm{Tors}_X^{\mathrm{proj}}$ defines a presentation of $\mathcal{T}$. We now show the following.

Proposition 3.71. *The stack $\mathcal{T}$ is algebraic, and is presented by $\mathrm{Tors}_X^{\mathrm{proj}}$.*

Proof. We show that the maps $\alpha, \omega\colon \mathcal{R}_{\mathrm{Tors}_X^{\mathrm{proj}}} \to \mathcal{U}_{\mathrm{Tors}_X^{\mathrm{proj}}}$ are smooth, so that $\mathcal{T}$ is algebraic. Recall to this end that $\mathrm{Tors}_X^{\mathrm{proj}}$ is a disjoint union of category schemes $\mathrm{Tors}_{X,b,b}^{\mathrm{proj}}$, where b runs through some finite subset of Seq. These category schemes are the category subschemes of $\mathrm{Tors}_X^{\mathrm{proj}}$ of those objects that are of type b. It therefore suffices to show that the morphisms $\alpha, \omega\colon \mathrm{Tors}_{X,b,b}^{\mathrm{proj}} \to \mathrm{Ob}\,\mathrm{Tors}_{X,b,b}^{\mathrm{proj}}$ are smooth for all b. To this end, we construct for all b a group scheme A over k, as follows.

Let A_1 be the $\mathcal{O}_{\mathbb{P}^1_k}$-automorphism scheme over k of $\mathcal{O}_{\mathbb{P}^1_k}(b)$, and let A_2 be the $\mathcal{O}_{X_{(0:1)}}$-automorphism scheme over k of $\mathcal{O}_{X_{(0:1)}}^{\#G}$. Let $A = A_1 \times_k A_2$. We show that A is smooth and geometrically irreducible. Of course, it suffices to show that both A_1 and A_2 are smooth and geometrically irreducible.

First consider A_1. Using the description of $\mathrm{Mod}^{\mathrm{st}}$, we easily see that A_1 is a product of factors of the form $\mathrm{GL}_{i,k^{\mathrm{sep}}}$ or $\mathbb{G}_{\mathrm{a},k^{\mathrm{sep}}}$, and therefore smooth and geometrically irreducible.

For A_2, we first note that A_2 is isomorphic to $\mathcal{H}om_k(X_{(0:1)}, \mathrm{GL}_{n,k})$. So we have an open immersion $A_2 \to \mathcal{H}om_k(X_{(0:1)}, \mathbb{A}^{n^2})$, and its target is as a scheme isomorphic to $\mathbb{A}^{d(\#G)^2}$, where d is the degree of $X_{(0:1)}$ over k. Hence A_2 is smooth and geometrically irreducible. We deduce that A is smooth and geometrically irreducible.

Note that $\mathrm{Ob}\,\mathrm{Tors}_{X,b,b}^{\mathrm{proj}}$ admits an obvious action of A, in other words, we have two maps suggestively denoted $\alpha, \omega\colon A \times_k \mathrm{Ob}\,\mathrm{Tors}_{X,b,b}^{\mathrm{proj}} \to \mathrm{Ob}\,\mathrm{Tors}_{X,b,b}^{\mathrm{proj}}$ given on functors

of points by $\alpha(g,t) = t$ and $\omega(g,t) = gt$. In fact, the morphism from $A \times \operatorname{Ob} \operatorname{Tors}^{\mathrm{proj}}_{X,b,b}$ to $\operatorname{Tors}^{\mathrm{proj}}_{X,b,b}$ sending (g,t) to the morphism $t \to gt$ induced by g is an isomorphism of schemes compatible with α and ω. This shows that both α and ω are smooth, as A is a smooth group scheme. □

We can now finish the proof of Theorem 3.67.

Proof of Theorem 3.67. By construction of $\operatorname{Tors}^{\mathrm{proj}}_X$ we see that it is fibred in groupoids and that there is an obvious fully faithful functor $\operatorname{Tors}^{\mathrm{proj}}_X \to \mathcal{T}$ of fibred categories.

We show that for any field extension l of k, any Γ-equivariant étale G-torsor over X_l is isomorphic to one arising from $\operatorname{Tors}^{\mathrm{proj}}_X(l)$. Recall that by construction, the category $\operatorname{Tors}^{\mathrm{proj}}_X(l)$ is equivalent to the category of Γ-equivariant, G-invariant finite étale morphisms $f\colon Y \to X_l$ of constant rank n, together with an A-linear isomorphism $\varphi\colon B \to \bigoplus_{g\in G} A$, and such that the G-equivariant A-algebra morphism $\psi\colon B \otimes_A B \to \bigoplus_{g\in G} B$, $b \otimes b' \mapsto (gbb')_{g\in G}$ is an isomorphism. In the above, B and A are the coordinate rings of the schemes $Y_{(0:1)}$ and $X_{l,(0:1)}$, respectively. Note that A and B are spectra of Artinian l-algebras. Hence it suffices to show that any such f admits such φ if and only if it is an étale G-torsor over X_l. But this follows easily from Corollary 3.64.

It remains to show that isomorphism classes in $\operatorname{Ob} \operatorname{Tors}^{\mathrm{proj}}_X(k^{\mathrm{sep}})$ are irreducible, but as the isomorphism classes are precisely the $A(k^{\mathrm{sep}})$-orbits by construction of $\operatorname{Tors}^{\mathrm{proj}}_X$, the result follows. □

3.13 Torsors over smooth affine curves

Let k be a factorial field. Let Γ, G be finite groups, together with an action of Γ on G by automorphisms. Let $f\colon X \to \operatorname{Spec} k$ be a smooth affine curve, together with a finite locally free morphism $X \to \mathbb{A}^1_k$ and an action of Γ on X over $\mathbb{A}^1_k$. Let $\overline{f}\colon \overline{X} \to \operatorname{Spec} k$ be the normal completion of X, and let $\overline{X} \to \mathbb{P}^1_k$ be the finite locally free morphism induced by $X \to \mathbb{A}^1_k$. Then $\overline{X}$ is (isomorphic to) an object of $(\Gamma, G)\text{-}\operatorname{Alg}^{\mathrm{st}}(k)$. In the next few sections, we construct a category scheme over k of torsors over X, or rather their completions over $\overline{X}$.

3.14 The differential morphism

First we find a criterion for a finite locally free $\mathbb{P}^1_k$-scheme to be smooth. We do this by constructing for each component-locally free algebra over a fixed one, its module of differentials, or rather a presentation thereof, functorially over the base. More precisely, we construct a morphism from $\operatorname{Ob} \operatorname{Alg}^{\mathrm{st}}_{\overline{X}}$ to a category scheme we define below. This category scheme is a fibred version of Definition 3.35.

We first define its objects.

Definition 3.72. Let S be a k-scheme, and let $\mathcal{O}_X$ be an object of $\operatorname{Alg}^{\mathrm{free}}(S)$. Let $\mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. A *component-locally free $\mathcal{O}_X$-module with rank in $\mathcal{R}$* is an $\mathcal{O}_X$-module $\mathcal{E}$ such

that there exists a locally constant map $q\colon S \to \mathcal{R}$ such that $\mathcal{E}_{q^{-1}r} = \mathcal{O}^r_{q^{-1}r \times_S X}$ for all $r \in \mathcal{R}$.

We define the corresponding category scheme.

Definition 3.73. Let $\mathcal{D}, \mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. The *category scheme* $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,\mathcal{R},\mathcal{D}}$ *of finite free modules of rank in* $\mathcal{R}$ *over finite free algebras of degree in* $\mathcal{D}$ is the functor $\operatorname{Sch}_k^{\text{op}} \to \operatorname{Cat}$ sending a k-scheme S to the fibred category of component-locally free modules over component-locally free algebras over S.

Equivalently, for any k-scheme S, the category $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,\mathcal{R},\mathcal{D}}(S)$ is the category in which the objects are pairs $(\mathcal{E}, \mathcal{O}_Y)$ of a component-locally free algebra $\mathcal{O}_Y$ and a component-locally free $\mathcal{O}_Y$-module $\mathcal{E}$, and in which the morphisms from $(\mathcal{E}, \mathcal{O}_Y)$ to $(\mathcal{F}, \mathcal{O}_Z)$ are pairs (ψ, φ) of a morphism $\varphi\colon \mathcal{O}_Y \to \mathcal{O}_Z$ and a φ-linear morphism $\psi\colon \mathcal{E} \to \mathcal{F}$.

We show that $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,\mathcal{R},\mathcal{D}}$ is representable, using an auxiliary functor.

Definition 3.74. Let $d, e, r, s \in \mathbb{Z}_{\geq 0}$. The functor $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,s,r,e,d}\colon \operatorname{Sch}_k^{\text{op}} \to \operatorname{Set}$ is the functor sending a k-scheme S to the set of pairs (ψ, φ) with $\varphi\colon \mathcal{O}_Y \to \mathcal{O}_Z$ in $\operatorname{Alg}^{\text{free}}_{e,d}$ and ψ a φ-linear map $\mathcal{O}_Y^r \to \mathcal{O}_Z^s$.

Lemma 3.75. *Let* $d, e, r, s \in \mathbb{Z}_{\geq 0}$. *Then* $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,s,r,e,d}$ *is representable by an affine scheme of finite type over* k.

Proof. Let S be a k-scheme. Then note that given an element $\varphi\colon \mathcal{O}_Y^r \to \mathcal{O}_Z^s$ of $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,s,r,e,d}$ is the same as giving r elements of $\big(\mathcal{O}_Z(S)\big)^s$, which is also the same as giving r elements of $\big(\mathcal{O}_S(S)\big)^{es}$. Hence $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,s,r,e,d}$ is representable by the affine scheme $\operatorname{Alg}^{\text{free}}_{k,e,d} \times_k \mathbb{A}^{ers}_k$. □

Corollary 3.76. *Let* $\mathcal{D}, \mathcal{R} \subseteq \mathbb{Z}_{\geq 0}$. *Then* $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,\mathcal{R},\mathcal{D}}$ *is representable. If* $\mathcal{D}$ *and* $\mathcal{R}$ *are finite, then it is affine and of finite type over* k.

Now we are in a position to construct, a morphism $\Omega\colon \operatorname{Ob}\operatorname{Alg}^{\text{free}}_k \to \operatorname{Mod}\operatorname{Alg}^{\text{free}}_k$ that sends a free algebra to a presentation of its module of differentials.

Let S be a k-scheme, and let $\mathcal{A} = (\mu, \varepsilon)$ be an object of $\operatorname{Alg}^{\text{free}}_d(S)$. The idea is to view $\mathcal{A}$ as $\mathcal{O}_S[t_1, t_2, \ldots, t_d]/I$, where I is the ideal generated by $t_i t_{i'} - \sum_j \mu_{jii'} t_j$ and $1 - \sum_j \varepsilon_j t_j$; so $\Omega_{\mathcal{A}/\mathcal{O}_S}$ is given as the $\mathcal{A}$-module with generators $\mathrm{d}t_i$ and relations $t_{i'}\,\mathrm{d}t_i + t_i\,\mathrm{d}t_{i'} - \sum_j \mu_{jii'}\,\mathrm{d}t_j = 0$ (for all $i, i' \in \{1, 2, \ldots, d\}$) and $-\sum_j \varepsilon_j\,\mathrm{d}t_j$. Set $\Omega(S)(\mathcal{A})$ to be the $\mathcal{A}$-linear map $\mathcal{A}^{d^2+1} \to \mathcal{A}^d$ corresponding to these relations, so that $\Omega_{\mathcal{A}/\mathcal{O}_S}$ is the cokernel of $\Omega(S)(\mathcal{A})$. This defines for all $d \in \mathbb{Z}$ a morphism $\Omega_d\colon \operatorname{Ob}\operatorname{Alg}^{\text{free}}_{k,d,d} \to \operatorname{Mod}\operatorname{Alg}^{\text{free}}_{k,d^2+1,d,d,d}$, and hence a morphism Ω from $\operatorname{Ob}\operatorname{Alg}^{\text{free}}_k$ to $\operatorname{Mod}\operatorname{Alg}^{\text{free}}_k$ that we call the *differential morphism*.

3.15 Finite flat covers

In this section, we construct from $\operatorname{Flat}^{\text{proj}}_X$ a category scheme such that for all field extensions l of k, the category of l-points is the category of finite flat covers of X_l such

that its normal completion $\overline{X_l}$ is smooth over l at points lying over $(1:0) \in \mathbb{P}^1(l)$. We do this by defining the following.

Definition 3.77. Let S be a k-scheme, and let Y be an object of $(\Gamma, G)\text{-}\operatorname{Alg}^{\mathrm{st}}_{\overline{X},b,b}(S)$, with b of length t. *Smoothness data at* ∞ on Y consists of

- a morphism $i\colon \mathcal{O}_{Y_{(1:0)^{(2)}}} \to \mathcal{O}^{2tn}_{Y_{(1:0)^{(2)}}}$ of $\mathcal{O}_{Y_{(1:0)^{(2)}}}$-modules;
- a morphism $j\colon \mathcal{O}^{2tn}_{Y_{(1:0)^{(2)}}} \to \mathcal{O}^{(2tn)^2+2}_{Y_{(1:0)^{(2)}}}$ of $\mathcal{O}_{Y_{(1:0)^{(2)}}}$-modules;

such that

$$\big((\Omega\Phi_{(1:0)^{(2)}}F)(Y) \oplus i\big)j = \mathrm{id}_{\mathcal{O}^{2tn}_{Y_{(1:0)^{(2)}}}}.$$

We check that this is the right notion for our purposes.

Lemma 3.78. *Let k be a field, let X be a finite locally free $\mathbb{P}^1_k$-scheme that is smooth over k, and let Y be a finite locally free X-scheme that is of degree t over $\mathbb{P}^1_k$. Then smoothness data at ∞ on Y exist if and only if Y is smooth at all points lying over $(1:0) \in \mathbb{P}^1(k)$.*

Proof. Write B for the ring of global sections of $Y - Y_{(0:1)}$, and note that it is a finite locally free $k[y]$-algebra. Then $Y_{(1:0)^{(2)}} = \operatorname{Spec} B/y^2B$. First suppose that smoothness data at ∞ on Y exist; i.e. there exist morphisms

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

such that for the presentation $\varphi\colon (B/y^2B)^{(2tn)^2+1} \to (B/y^2B)^{2tn}$ of $\Omega_{(B/y^2B)/k}$ as a (B/y^2B)-module given in Section 3.14, we have $(\varphi \oplus i)j = \mathrm{id}$. It then immediately follows that $\Omega_{(B/y^2B)/k}$ is generated by one element as B/y^2B-module.

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

It remains to show that $\Omega_{(B/y^2B)/k}$ is generated as a B/y^2B-module by one element if and only if Y is smooth over k at all points lying over $(1:0) \in \mathbb{P}^1(k)$. Note that we have an isomorphism

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

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 $\Omega_{(B/y^2B)/k}$ 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 $\Omega_{B/k} \otimes_B B_f$ 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 $Y_{(1:0)}$ that is smooth over k, which holds if and only if Y is smooth over k at all points lying over $(1:0) \in \mathbb{P}^1(k)$. □

Definition 3.79. Let $\mathcal{S} \subseteq \mathrm{Seq}$. The *category scheme* $\mathrm{Flat}^{\mathrm{aff}}_{\overline{X},\mathcal{S}}$ *of standard finite flat covers of X of type in $\mathcal{S}$* is the functor $\mathrm{Sch}^{\mathrm{op}}_k \to \mathrm{Cat}$ that sends a k-scheme S to the category

in which the objects are triples $(\mathcal{O}_Y, i, j)$ with $\mathcal{O}_Y$ an object of $\mathrm{Flat}^{\mathrm{proj}}_{\overline{X},\mathcal{S}}(S)$ and (i,j) smoothness data on Y at ∞.

As before, we have the following by construction.

Proposition 3.80. *Let $\mathcal{S} \subseteq \mathrm{Seq}$. Then $\mathrm{Flat}^{\mathrm{aff}}_{\overline{X},\mathcal{S}}$ is representable. If $\mathcal{S}$ is finite, then $\mathrm{Flat}^{\mathrm{aff}}_{X,\mathcal{S}}$ is affine and of finite type over k.*

3.16 Torsors

Definition 3.81. The *category scheme* $\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}$ *of finite étale Γ-equivariant G-torsors over X* is the functor $\mathrm{Sch}^{\mathrm{op}}_k \to \mathrm{Cat}$ sending a k-scheme S to the subcategory of $\mathrm{Flat}^{\mathrm{aff}}_{\overline{X}}(S)$ of objects Y (over $\mathbb{P}^1_S$) such that $\Delta_{Y/\mathbb{P}^1_S}$ and $\Delta^{\otimes \#G}_{\overline{X}_S/\mathbb{P}^1_S}$ differ by a unit times a power of y, and such that $Y - Y_{(1:0)}$ is a G-torsor over X.

We show that $\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}$ is a category scheme that is affine and of finite type over k. We first note that the condition that $\Delta_{Y/\mathbb{P}^1_S}$ and $\Delta^{\otimes \#G}_{\overline{X}_S/\mathbb{P}^1_S}$ is sufficient for an object of $\mathrm{Flat}^{\mathrm{aff}}_{\overline{X}}$ to be étale over X, and that over fields, it is also necessary. This follows from the following lemma.

Lemma 3.82. *Let S be a scheme, and let a and b be integers. Let $\mathbb{A}^1_S \subseteq \mathbb{P}^1_S$ be the complement of the section $(1:0)$, let $\varphi\colon \mathcal{O}_{\mathbb{P}^1_S}(b) \to \mathcal{O}_{\mathbb{P}^1_S}(a)$ be a $\mathcal{O}_{\mathbb{P}^1_S}$-linear map. If φ is multiplication by sy^{a-b} with $s \in \mathcal{O}_S(S)^\times$, then φ defines an isomorphism of $\mathcal{O}_{\mathbb{A}^1_S}$-modules. If S is the spectrum of a field, then φ defines an isomorphism of $\mathcal{O}_{\mathbb{A}^1_S}$-modules if and only if it is multiplication by sy^{a-b} with $s \in \mathcal{O}_S(S)^\times$.*

Proof. Since y becomes invertible after restricting to $\mathbb{A}^1_S$, it follows that if φ is multiplication by sy^{a-b}, then $\varphi|_{\mathbb{A}^1_S}$ is an isomorphism. Conversely, if S is the spectrum of a field l, then 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 $s \in l^\times$. □

Next, we want to bound the fibre-wise (classical) Euler characteristic of torsors, using the following lemmas.

Lemma 3.83. *Let $Y \to X$ be a finite locally free morphism of schemes, and let G be a finite group acting on Y over X. Then the locus on X where G acts transitively on Y over X is closed.*

Proof. Consider the morphism $\underline{G}_X \times_X Y \to Y \times_X Y$ given on the functor of points by $(g,y) \mapsto (gy,y)$. Let Z be the (topological) image of this morphism, and let V be its complement. As $Y \times_X Y$ is finite locally free over X, the image U of V is open, and the complement of U is the locus on X where G acts transitively on Y over X. □

Corollary 3.84. *Let S be a scheme, let $Y \to X$ be a finite locally free morphism of finite locally free $\mathbb{P}^1_S$-schemes that is étale over $X - X_{(1:0)}$, and let G be a finite group acting on Y over X. If G is a torsor on $Y_{(0:1)}$ over $X_{(0:1)}$, then G acts transitively on Y over X.*

Proof. This follows from Lemma 3.63 and Lemma 3.83. □

Lemma 3.85. *Let S be a scheme, let $a \in \mathrm{Seq}$, and let X be a standard scheme 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 $s + \sum_\sigma a_\sigma$.*

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

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

□

Proposition 3.86. *Let S be a scheme, and let $Y \to X$ be a morphism of standard schemes, with X of type a and with Y of type b, where a, b are of length s, t, respectively. Let G be a finite group of order invertible in S acting on Y over X, such that Y is a G-torsor over X. Then*

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

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 $Y - Y_{(1:0)}$ is étale over $X - X_{(1:0)}$, 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. □

Hence we have the following.

Proposition 3.87. *Then $\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}$ is representable by an affine k-scheme of finite type.*

Now write $\mathcal{T} = \mathcal{T}^G_{\Gamma, X}$.

Theorem 3.88. *Let $[\mathcal{U}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}} / \mathcal{R}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}}] \to \mathcal{T}^G_{\Gamma, X}$ sending for any k-scheme S the object T of $\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}(S)$ to the underlying Γ-equivariant G-torsor on X. For all perfect field extensions l over k, the functor $[\mathcal{U}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}} / \mathcal{R}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}}](l) \to \mathcal{T}(l)$ is an equivalence. The isomorphism classes in $\mathcal{U}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}}$ are irreducible.*

Proof. By construction, for all perfect field extensions l over k, the functor from $[\mathcal{U}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}} / \mathcal{R}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}}](l)$ to $\mathcal{T}(l)$ is an equivalence. We show that the isomorphism classes in $\mathcal{U}_{\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}}$ are irreducible.

Note that $\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}$ admits an obvious forgetful functor to $\mathrm{Flat}^{\mathrm{proj}}_{\overline{X}}$, and we show that the image of an isomorphism class of $\mathrm{Ob}\,\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}(\bar{k})$ is irreducible in the same way as in Theorem 3.67. Therefore it suffices to show that the non-empty geometric fibres of the morphism $\mathrm{Ob}\,\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}} \to \mathrm{Ob}\,\mathrm{Flat}^{\mathrm{proj}}_{\overline{X}}$ are irreducible. So let Y be an object of $\mathrm{Flat}^{\mathrm{proj}}_{\overline{X}}(\bar{k})$ in the image of this morphism, and write B for the ring of global sections of $Y - Y_{(0:1)}$.

Then for smoothness data (i, j) at ∞ for s we have that

- i is unique up to a unique element of $\operatorname{im}\varphi$, which is free over $\bar{k}$ and can therefore be parametrised by an affine space over $\bar{k}$;
- j is unique up to a unique $2n\#G$-tuple of $\ker(\varphi \oplus i)$, which again is free over $\bar{k}$ and can therefore be parametrised by an affine space over $\bar{k}$.

Hence the fibre over Y is irreducible, as desired. □

Therefore by Proposition 3.1, we have the following.

Corollary 3.89. *The induced map* $\mathrm{Ob}\,\mathrm{Tors}^{\mathrm{aff}}_{\overline{X}}(\bar{k}) \to \mathrm{Ob}\,\mathcal{T}(\bar{k})/\cong$ *factors through a bijection* $\pi_0(\mathrm{Ob}\,\mathrm{Tors}^{\mathrm{aff}}_{\overline{X},k^{\mathrm{sep}}}) \to \mathrm{Ob}\,\mathcal{T}(\bar{k})/\cong$ *that is* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-equivariant, and the connected components of* $\mathrm{Ob}\,\mathrm{Tors}^{\mathrm{aff}}_{\overline{X},k^{\mathrm{sep}}}$ *are irreducible.*

3.17 Computation of cohomology

We now use the previous sections to describe Algorithm 2.2, which, as we recall, takes as input a factorial field k, a finite ring Λ that is annihilated by an integer n that is invertible in k and that is injective as a Λ-module, a smooth connected curve $f\colon X \to \operatorname{Spec} k$ that is the composition of a finite étale morphism $X \to U$, an open immersion $U \to \mathbb{P}^1_k$ (given as the complement of the zero set of a single homogeneous polynomial), the structure morphism $\mathbb{P}^1_k \to \operatorname{Spec} k$, and a finite locally constant $\mathcal{M} \in \mathrm{Ob}\,\Lambda\text{-}\mathrm{Mod}_c(X_{\text{ét}})$, and outputs $R^0 f_!\mathcal{M}$, $R^1 f_!\mathcal{M}$, $R^2 f_!\mathcal{M}$. Moreover, we do so functorially in $\mathcal{M}$.

Note that we can construct a finite locally free morphism $X \to \mathbb{A}^1_k$ from these data if $U \neq \mathbb{P}^1_k$.

Algorithm 3.90. *Suppose that given as input is a factorial field k and a homogeneous polynomial $h \in k[x, y]$ of degree $d \geq 1$.*

Output: a finite locally free morphism $U = \mathbb{P}^1_k - V_{\mathbb{P}^1_k}(h) \to \mathbb{A}^1_k$.

- If $k = \mathbb{F}_q$, find the smallest integer $D \leq d!$ such that $x^{q^D} - x - 1$ and $h(x, 1)$ have no common zeroes, and **output** the morphism $U \to \mathbb{A}^1_k$ given by

$$(x : y) \mapsto \frac{(x^{q^D} - xy^{q^D-1} - y^{q^D})^d}{h(x, y)^{q^D}},$$

  and **halt**.

- If k is infinite, compute an $a \in k$ for which $h(a) \neq 0$, **output** the morphism $U \to \mathbb{A}^1_k$ given by
$$(x : y) \mapsto \frac{(x - ay)^d}{h(x, y)},$$
and **halt**.

Proposition 3.91. *Algorithm 3.90 is correct and halts in an effectively bounded number of field operations.*

Proof. In the case that $k = \mathbb{F}_q$, we have by construction that $\left((x^{q^D} - x - 1)^d, h^{q^D}\right)$ is the unit ideal in $k[x]$. In the case that k is infinite, there exists an $a \in k$ with $h(a) \neq 0$, which can be found by enumerating at most $d + 1$ elements of k, and we have that $\left((x - a)^d, h\right)$ is the unit ideal of $k[x]$. The morphism constructed can therefore in both cases be extended to a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$ such that the inverse image of $\{\infty\}$ is $Z_{\mathbb{P}^1_k}(h)$; as this morphism is finite locally free, so is the morphism constructed. □

3.18 Computation of $R^0 f_*$

Let us first describe how to compute pushforwards, functorially; it suffices to consider sheaves of sets. We will insist on giving our output as a set of sections, since this makes it easier to compare elements.

The computation of pushforwards is a special case of the following computation.

Algorithm 3.92. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, and finite étale X-schemes Y_1, Y_2.*

Output: $\mathrm{Hom}_{X_{k^{\mathrm{sep}}}}(Y_{1,k^{\mathrm{sep}}}, Y_{2,k^{\mathrm{sep}}})$ *as a finite* $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-set.*

- Compute a finite purely inseparable extension l of k such that the normal completions $\overline{X_l}$, $\overline{Y_{1,l}}$, $\overline{Y_{2,l}}$ of X_l, $Y_{1,l}$, $Y_{2,l}$, respectively, are smooth over l, using Algorithm 2.12.
- Compute the morphisms $\overline{Y_{1,l}} \to \overline{X_l}$ and $\overline{Y_{2,l}} \to \overline{X_l}$ in $\mathrm{Alg}^{\mathrm{st}}_l(l)$, so that $\overline{Y_{1,l}}$ and $\overline{Y_{2,l}}$ are objects of $\mathrm{Alg}^{\mathrm{st}}_{l,\overline{X_l}}(l)$.
- Set $H' = \omega^{-1}(\overline{Y_{2,l}}) \times_{\mathrm{Alg}^{\mathrm{st}}_{l,\overline{X_l}}} \alpha^{-1}(\overline{Y_{1,l}})$, set $H = \mathrm{Res}^l_k H'$, and compute a finite Galois extension k' of k such that $H_{k'}$ splits completely over k'.
- Set $l' = l \otimes k'$, and attach to every element of $H(k')$ the corresponding morphism $\overline{Y_{1,l'}} \to \overline{Y_{2,l'}}$.
- Attach to each such morphism $\overline{Y_{1,l'}} \to \overline{Y_{2,l'}}$ its restriction to $Y_{1,l'}$.
- **Output** the finite $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set obtained in this way, and **halt**.

Proposition 3.93. *Algorithm 3.92 is correct and halts in an effectively bounded number of field operations.*

Proof. We first show that H is finite étale over k. First note that H' is a finite l-scheme, since it is of finite type over l by definition, and for all field extensions m of l, we have $H'(m) = \mathrm{Hom}_{\overline{X_m}}(\overline{Y_{1,m}}, \overline{Y_{2,m}}) = \mathrm{Hom}_{X_m}(Y_{1,m}, Y_{2,m})$, which is finite as $Y_{1,m}$ and $Y_{2,m}$ are finite étale over X_m. Moreover, by the topological invariance of the small étale

site, we see that H' is formally étale and therefore étale. Hence $H = \mathrm{Res}_k^l H'$ is finite étale over k.

Now the proof follows from the fact that any morphism $Y_{1,l'} \to Y_{2,l'}$ must already be defined over k'. □

As $f_*\mathcal{F}$ corresponds to the $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set $\mathrm{Hom}_{X_{k^{\mathrm{sep}}}}(X_{k^{\mathrm{sep}}}, \mathcal{F}_{k^{\mathrm{sep}}})$, we see that computing pushforwards is a special case of Algorithm 3.92. Next, we consider functoriality in $\mathcal{F}$.

Algorithm 3.94. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, a morphism $\varphi\colon \mathcal{F} \to \mathcal{G}$ between finite locally constant sheaves $\mathcal{F}, \mathcal{G}$ on $X_{\acute{e}t}$.*

Output: the $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-equivariant map $f_*\varphi\colon f_*\mathcal{F} \to f_*\mathcal{G}$.

- Let l be a finite Galois extension of k such that $f_*\mathcal{F}, f_*\mathcal{G}$ split completely over l.
- **Output** the map sending a section $s\colon X_l \to \mathcal{F}_l$ to its composition with the morphism $\mathcal{F}_l \to \mathcal{G}_l$, and **halt**.

Remark 3.95. It follows that we can also compute $R^0 f_! \mathcal{F} = f_! \mathcal{F}$ for any finite locally constant sheaf $\mathcal{F}$ of pointed sets and any smooth curve $f\colon X \to \mathrm{Spec}\, k$ given as a finite locally free scheme over $\mathbb{A}^1_k$ or $\mathbb{P}^1_k$; if X is affine, then $f_!\mathcal{F}$ is simply the sheaf represented by $\mathrm{Spec}\, k$, and if X is projective, then $f_!\mathcal{F} = f_*\mathcal{F}$.

3.19 Computation of $R^1 f_*$

We now describe the computation of $R^1 f_*$; it suffices to do this functorially for sheaves of groups. As in the previous section, we insist on giving the elements of our output a geometric interpretation, namely as a set of representatives of isomorphism classes of torsors on $X_{k^{\mathrm{sep}}}$. In each of the algorithms in this section, the condition that $\mathcal{G}$ be of degree coprime to the characteristic can be dropped in the case that the curve X is projective.

We first describe an algorithm deciding whether two torsors on X are isomorphic over k^{sep}.

Algorithm 3.96. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, a finite locally constant sheaf $\mathcal{G}$ of groups on $X_{\acute{e}t}$ of degree coprime to the characteristic of k, finite separable extensions k_1, k_2 of k, and a $\mathcal{G}_{k_i}$-torsor T_i on X_{k_i} for $i = 1, 2$.*

Output: "yes" if $T_{1,k^{\mathrm{sep}}} \cong T_{2,k^{\mathrm{sep}}}$; otherwise nothing.

- Compute a finite étale Galois morphism $g\colon Y \to X$ with Galois group Γ and with Y connected, such that $g^{-1}\mathcal{G}$ is constant, say with fibre G (with Γ-action).
- Compute a finite purely inseparable extension l over $k_1 k_2$ such that the normal completions $\overline{Y_l}$, $\overline{T_{1,l}}$, $\overline{T_{2,l}}$ of Y_l, $T_{1,l}$, $T_{2,l}$, respectively, are smooth over l, using Algorithm 2.12.
- Set $\mathcal{T} = \mathrm{Tors}^{\mathrm{aff}}_{l,\overline{Y_l}}$ (or $\mathcal{T} = \mathrm{Tors}^{\mathrm{proj}}_{l,\overline{Y_l}}$ in the projective case).

- Using an absolute primary decomposition algorithm, compute a finite separable extension l' of l over which the connected components of $\mathrm{Ob}\,\mathcal{T}_{l^{\mathrm{sep}}}$ are defined.
- Compute $\overline{T_{1,l'}}$ and $\overline{T_{2,l'}}$ as objects of $\mathcal{T}_{l'}(l')$.
- If they do not belong to the same connected component of $\mathrm{Ob}\,\mathcal{T}_{l'}$, **halt**.
- Otherwise, **output** "yes" and **halt**.

Proposition 3.97. *Algorithm 3.96 is correct and halts in an effectively bounded number of field operations.*

Proof. By construction, the algorithm decides correctly whether $T_{1,\bar{k}} \cong T_{2,\bar{k}}$, but this is equivalent to $T_{1,k^{\mathrm{sep}}} \cong T_{2,k^{\mathrm{sep}}}$. □

We use this to compute $R^1 f_*$.

Algorithm 3.98. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, $\mathcal{G}$ a finite locally constant sheaf of groups on $X_{\acute{e}t}$ of degree coprime with the characteristic of k.*

Output: $R^1 f_* \mathcal{G}$ as a finite $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set of representatives of isomorphism classes of $\mathcal{G}_{k^{\mathrm{sep}}}$-torsors on $X_{k^{\mathrm{sep}}}$.

- Compute a finite étale Galois morphism $g\colon Y \to X$ with Galois group Γ and with Y connected, such that $g^{-1}\mathcal{G}$ is constant, say with fibre G (with Γ-action).
- Compute a finite purely inseparable extension l of k such that the normal completion $\overline{Y_l}$ of Y_l is smooth.
- Set $\mathcal{T} = \mathrm{Tors}^{\mathrm{aff}}_{l,\overline{Y_l}}$ (or $\mathcal{T} = \mathrm{Tors}^{\mathrm{proj}}_{l,Y_l}$ in the projective case).
- Using an absolute primary decomposition algorithm, compute a finite Galois extension l' of l over which the connected components of $\mathrm{Ob}\,\mathcal{T}_{l^{\mathrm{sep}}}$ are defined.
- Compute a finite extension l'' of l', and for every connected component of $\mathrm{Ob}\,\mathcal{T}_{l'}$ an l''-rational point on it; i.e. a Γ-equivariant G-torsor on $\overline{Y_{l''}}$.
- Attach to every such torsor its restriction to $Y_{l''}$, and then its quotient by Γ.
- Let k'' be the separable closure of k in l''.
- Let T denote the finite set of $\mathcal{G}$-torsors on $X_{k''}$ obtained this way.
- For every $t \in T$ and $\gamma \in \mathrm{Gal}(k''/k)$, find using Algorithm 3.96 $\gamma t \in T$ by enumeration.
- **Output** the finite $\mathrm{Gal}(k^{\mathrm{sep}}/k)$-set T, and **halt**.

Proposition 3.99. *Algorithm 3.98 is correct and halts in an effectively bounded number of field operations.*

Proof. This follows directly from Corollary 3.89 in the affine case, and from Corollary 3.68 in the projective case. □

Before considering functoriality in $\mathcal{G}$, we first consider quotients of finite étale morphisms by finite locally constant sheaves of groups on $X_{\acute{e}t}$.

Algorithm 3.100. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, a finite étale scheme Y over X, a finite locally constant sheaf $\mathcal{G}$ of groups on $X_{\acute{e}t}$ acting on Y.*

Output: the quotient of Y by the action of $\mathcal{G}$.

- Compute a finite étale Galois morphism $g\colon X' \to X$ with Galois group Γ and with Y connected, such that $g^{-1}\mathcal{G}$ is constant, say with fibre G (with Γ-action).
- Set $Y' = X' \times_X Y$.
- **Output** $\Gamma\backslash(G\backslash Y')$ and **halt**.

Hence we can compute $R^1 f_*$ functorially as follows.

Algorithm 3.101. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, $\varphi\colon \mathcal{G} \to \mathcal{H}$ a morphism of finite locally constant sheaves of groups on $X_{\acute{e}t}$ of degree coprime with the characteristic of k.*

Output: the $\mathrm{Gal}(k^{\mathrm{sep}}/k)$*-equivariant map $R^1\varphi\colon R^1 f_*\mathcal{G} \to R^1 f_*\mathcal{H}$.*

- Let l be a finite Galois extension of k such that $R^1 f_*\mathcal{G}$ and $R^1 f_*\mathcal{H}$ split completely over l.
- **Output** the map sending a $\mathcal{G}_l$-torsor $T \to X_l$ to a $\mathcal{H}_l$-torsor isomorphic to $\mathcal{H}_l \otimes_{\mathcal{G}_l} T = \mathcal{G}_l\backslash(\mathcal{H}_l \times_{X_l} T) \to X_l$ (where $\mathcal{G}$ acts by $g(h,t) = (hg^{-1}, gt)$), and **halt**.

Finally, if $\mathcal{G}$ is commutative, then $R^1 f_*\mathcal{G}$ is an abelian group, and we can compute its group structure.

Algorithm 3.102. *Suppose that given as input is a factorial field k, a finite locally free morphism $X \to \mathbb{A}^1_k$ (or $X \to \mathbb{P}^1_k$) with X a smooth connected curve over k, $\varphi\colon \mathcal{G} \to \mathcal{H}$ a morphism of finite locally constant sheaves of abelian groups on $X_{\acute{e}t}$ of degree coprime with the characteristic of k.*

Output: the addition map $R^1 f_*\mathcal{G} \times_k R^1 f_*\mathcal{G} \to R^1 f_*\mathcal{G}$.

- Let l be a finite Galois extension of k such that $R^1 f_*\mathcal{G}$ splits completely over l.
- **Output** the map sending a pair (T_1, T_2) of $\mathcal{G}_l$-torsors to a $\mathcal{G}_l$-torsor isomorphic to $T_1 \otimes_{\mathcal{G}_l} T_2 = \mathcal{G}_l\backslash(T_1 \times_{X_l} T_2)$ (where $\mathcal{G}_l$ acts by $g(t_1,t_2) = (t_1 g^{-1}, gt_2)$), and **halt**.

3.20 Poincaré duality

Note that we have now computed $R^0 f_!$, $R^0 f_*$, and $R^1 f_*$ of a smooth connected curve $f\colon X \to \operatorname{Spec} k$. We compute the rest using Poincaré duality; we recall its statement first.

Let Λ be a finite ring annihilated by $n \in \mathbb{Z}$, let X be a scheme, and let $\mathcal{M}$ be a finite locally constant sheaf of Λ-modules on $X_{\text{ét}}$. Then we denote the d-th Tate twist $\mathcal{M} \otimes_{\mathbb{Z}/n\mathbb{Z}} (\mu_n)^{\otimes d}$ of $\mathcal{M}$ by $\mathcal{M}(d)$; note that this doesn't depend the choice of the annihilator n, and that we can compute this if X is a smooth curve or the spectrum of a field. Write moreover $\mathcal{M}^\vee$ for $\mathcal{H}om(\mathcal{M}, \Lambda)$, which we can compute by Algorithm 3.92.

Theorem 3.103 (Poincaré duality, SGA4.3 [1, Exp. XVIII, Sec. 3.2.6])**.** *Let Λ be a finite ring that is injective as a Λ-module, let $f\colon X \to \operatorname{Spec} k$ be a smooth curve over a field, and let $\mathcal{M}$ be a finite locally constant sheaf of Λ-modules on $X_{\acute{e}t}$. Then for $q = 0, 1, 2$ we have $R^{2-q} f_*(\mathcal{M}^\vee(1)) = (R^q f_! \mathcal{M})^\vee$.*

In other words, we have the identities

$$R^1 f_! \mathcal{M} = \left(R^1 f_* \left(\mathcal{M}^\vee(1) \right) \right)^\vee$$
$$R^2 f_! \mathcal{M} = \left(f_* \left(\mathcal{M}^\vee(1) \right) \right)^\vee$$
$$R^2 f_* \mathcal{M} = \left(f_! \left(\mathcal{M}^\vee(1) \right) \right)^\vee.$$

Therefore we indeed have an algorithm as in Algorithm 2.2, as desired.

Bibliography

[1] M. Artin. *Théorie des topos et cohomologié étale des schémas (SGA4) vol. 3*, volume 305 of *Lecture Notes in Math.* Springer-Verlag, 1972.

[2] C. W. Ayoub. The decomposition theorem for ideals in polynomial rings over a domain. *J. Algebra*, 76:99–110, 1982.

[3] S. Bosch, W. Lütkebohmert, and M. Raynaud. *Néron models*, volume 21 of *Ergeb. Math. Grenzgeb. (3)*. Springer, 1990.

[4] A. Chistov. Algorithm of polynomial complexity for factoring polynomials and finding the components of varieties in subexponential time. *J. Math. Sci. (N. Y.)*, 34(4):1838–1882, 1986. Translated from *Zap. Nauchn. Sem. S.-Petersburg*, 137:124–188, 1984.

[5] J.-M. Couveignes and S. J. Edixhoven, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Ann. of Math. Stud.* Princeton Univ. Press, 2011.

[6] R. Dedekind and H. Weber. Theorie der algebraischen Funktionen einer Veränderlichen. *J. Reine Angew. Math.*, 1882.

[7] P. Deligne. *Cohomologie étale*, volume 569 of *Lecture Notes in Math.* Springer-Verlag, 1977.

[8] P. Deligne. Le déterminant de la cohomologie. *Comtemp. Math.*, 67:93–177, 1987.

[9] A. Dickenstein, N. Fitchas, M. Giusti, and C. Sessa. The membership problem for unmixed polynomial ideals is solvable in single exponential time. *Discrete Math. Appl.*, 33:73–94, 1991.

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

[11] D. Ferrand. Un foncteur norme. *Bull. Soc. Math. France*, 126:1–49, 1998.

[12] A. Fröhlich and J. C. Shepherdson. On the factorisation of polynomials in finite steps. *Math. Z.*, 62:331–334, 1955.

[13] L. Fu. *Étale cohomology theory*, volume 14 of *Nankai Tracts Math.* World Sci. Publ., 2015.

[14] S. I. Gelfand and Y. I. Manin. *Methods of Homological Algebra*. Springer Monogr. Math. Springer-Verlag, 2003.

[15] P. Gianni, B. Trager, and G. Zacharias. Gröbner bases and primary decomposition of polynomial ideals. *J. Symbolic Comput.*, 6:149–167, 1988.

[16] U. Görtz and T. Wedhorn. *Algebraic Geometry I*. Adv. Lectures Math. Vieweg+Teubner Verlag, first edition, 2010. ISBN 978-3-834-0676-5. doi: 10.1007/978-3-8348-9722-0.

[17] A. Grothendieck. Éléments de Géométrie Algébrique II. Etude globale élémentaire de quelques classes de morphismes. *Publ. Math. Inst. Hautes Études Sci.*, 8: 5–222, 1961.

[18] A. Grothendieck. Éléments de Géométrie Algébrique IV. Etude locale des schémas et des morphismes de schémas, quatrième partie. *Publ. Math. Inst. Hautes Études Sci.*, 32:5–361, 1967.

[19] A. Grothendieck. *Revêtements étales et groupe fondamental (SGA1)*, volume 224 of *Lecture Notes in Math.* Springer-Verlag, 1971.

[20] W. G. Handley and S. S. Wainer. Complexity of primitive recursion. In U. Berger and H. Schwichtenberg, editors, *Computational Logic*, volume 165 of *NATO Adv. Sci. Inst.*, pages 273–300, 1999.

[21] D. Harvey. Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2), 2014.

[22] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symbolic Comput.*, 33(4), 2002.

[23] P. T. Johnstone. *Sketches of an elephant: a topos theory compendium*, volume 43 of *Oxford Logic Guides*. Clarendon Press, 2002.

[24] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[25] K. Khuri-Makdisi. Asymptotically fast group operations on Jacobians of general curves. *arXiv NT/0409209v2*, 2004.

[26] J. Kollár. Sharp effective Nullstellensatz. *J. Amer. Math. Soc.*, 1(4):963–975, 1988.

[27] A. Lauder and D. Wan. Counting points on varieties over finite fields of small characteristic. In J. Buhler and P. Stevenhagen, editors, *Algorithmic Number Theory*, volume 44 of *MRSI Publications*. 2008.

[28] M. Lieblich. Galois representations arising from p-divisible groups, 2000.

[29] D. A. Madore and F. Orgogozo. Calculabilité de la cohomologie étale modulo ℓ. *Algebra Number Theory*, 9(7):1647–1739, 2015.

[30] R. Matsumoto. Computing the radical of an ideal in positive characteristic. *J. Symbolic Computation*, 32:263–271, 2001.

[31] B. M. E. Moret. *The theory of computation*. Addison Wesley Longman, Inc., 1998.

[32] M. Nagata. *Local rings*. Wiley-Interscience, 1962.

[33] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[34] B. Poonen, D. Testa, and R. van Luijk. Computing Néron-Severi groups and cycle class groups. *Compos. Math.*, 151(4):713–734, 2015.

[35] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44:483–494, 1985.

[36] J.-P. Serre. *Lectures on $N_X(p)$*, volume 11 of *Res. Notes Math.* A. K. Peters, 2011.

[37] B. L. van der Waerden. *Modern Algebra (English)*. Frederick Ungar Publishing Co., 1949.

Samenvatting

Dit proefschrift gaat, zoals de titel *"Berekenbaarheid van de étale Euler-Poincaré karakteristiek"* misschien al suggereert, over het algoritmisch berekenen van de *étale Euler-Poincaré karakteristiek*. Dit is gerelateerd aan het "snel tellen van oplossingen van vergelijkingen", in de volgende zin.

Neem variabelen $x_1, x_2, x_3, \ldots, x_n$. Een *polynoom* in deze variabelen is een uitdrukking verkregen uit deze variabelen en het getal 1 door optellen, aftrekken, of vermenigvuldigen. Bijvoorbeeld: $x_1, x_2, x_3, \ldots$ zijn alle zelf ook polynomen; ieder geheel getal is een polynoom (tel 1 een aantal keer bij 1 op, of trek 1 een aantal keer van 1 af); en om wat ingewikkeldere voorbeelden te noemen, $x_1 \cdot x_2 - 1$, $x_1^3 - 5x_1 + 8$, $x_3 + x_4 \cdot x_5^9$ zijn ook polynomen (zoals gebruikelijk staat x^i voor $x \cdot x \cdot \cdots \cdot x$ waarin x in totaal i keer voorkomt). Een *systeem van polynomen* is dan een collectie van polynomen.

Neem een priemgetal p. De oplossingen waarin we geïnteresseerd zijn, zijn de zogenaamde *modulo p oplossingen* van een polynoom; dit zijn collecties gehele getallen $(a_1, a_2, a_3, \ldots, a_n)$, alle van 0 tot en met $p - 1$, zodat wanneer er voor iedere variabele $x_1, x_2, x_3, \ldots, x_n$, respectievelijk $a_1, a_2, a_3, \ldots, a_n$ wordt gesubstitueerd, dat er dan een veelvoud van p uit komt. Evenzo, een *modulo p oplossing* van een systeem van polynomen is een collectie gehele getallen $(a_1, a_2, a_3, \ldots, a_n)$ dat een oplossing is van ieder polynoom in het systeem.

Bijvoorbeeld, neem $p = 3$ en $n = 1$, en bekijk het polynoom $x_1^3 - 5x_1 + 8$. Door voor x_1 de waarden 0, 1, 2, te substitueren, krijgen we het volgende tabel.

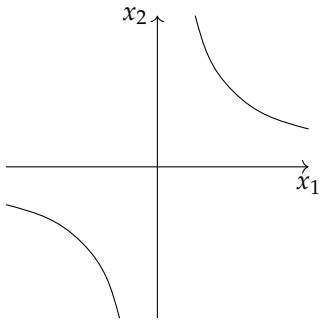
x_1	x_1^3	$x_1^3 - 5x_1 + 8$
0	0	8
1	1	4
2	8	6

We zien dus dat $x_1^3 - 5x_1 + 2$ als enige modulo 3 oplossing het getal 2 heeft; namelijk, 6 is het enige getal uit de rechterkolom dat een veelvoud is van 3.

Nu is het in principe makkelijk om het aantal modulo p oplossingen van een systeem van polynomen te tellen; men kan gewoon ieder van de p^n mogelijkheden af gaan, en van iedere mogelijkheid nagaan of het een modulo p oplossing is. Maar voor toepassingen in de cryptografie (denk aan bijv. internetversleuteling of je bankpas) neemt men priemgetallen van enkele honderden cijfers, en in zulke gevallen zou het te lang duren om alle mogelijkheden af te gaan, zelfs voor de sterkste supercomputer.

Om in dat soort gevallen nog steeds het aantal modulo p oplossingen te kunnen tellen, is een oplossing – die al daadwerkelijk wordt toegepast in het geval $n = 2$ en een "systeem" van één polynoom – het gebruiken van een formule voor het aantal modulo p oplossingen van een systeem van polynomiale vergelijkingen. In dit geval is de formule de zogenaamde *Lefschetz spoorformule*, die uitgedrukt is in de étale Euler-Poincaré karakteristiek behorende bij het systeem van polynomen.

We kunnen ook op een meer "meetkundige" manier naar (systemen van) polynomen kijken, door de *oplossingen* van systemen van polynomen te beschouwen; een oplossing is een collectie van getallen $(a_1, a_2, a_3, \ldots, a_n)$ zodat wanneer er voor iedere $x_1, x_2, x_3, \ldots, x_n$, respectievelijk $a_1, a_2, a_3, \ldots, a_n$ wordt gesubstitueerd, dat er dan 0 uit komt. We kunnen de oplossingen van systemen van polynomen dan visualiseren met behulp van een grafiek; voor het polynoom $x_1 \cdot x_2 - 1$ (met $n = 2$) hebben we bijvoorbeeld een grafiek van de volgende vorm.



De projectie van deze grafiek op de x_1-as bevat alle punten op de x_1-as behalve 0, en boven ieder ander punt van de x_1-as ligt er één punt van de grafiek. Met andere woorden, iedere punt van de x_1-as hoort óf bij een punt van de grafiek, óf is een oplossing van de vergelijking $x_1 = 0$, dus de twee polynomen $x_1 \cdot x_2 - 1$ (met $n = 2$) en $x_1 = 0$ (met $n = 1$) kunnen worden opgevat als een soort "meetkundige splitsing" van het polynoom 0 (met $n = 1$), en in dit geval is er een relatie tussen de bijbehorende étale Euler-Poincaré karakteristieken.

Er zijn meer van dit soort "meetkundige" relaties, en deze worden in dit proefschrift gebruikt om een algoritme te geven die de étale Euler-Poincaré karakteristiek van een systeem polynomen uitrekent.

Nawoord

Ik bedank:

- allereerst mijn promotoren Bas Edixhoven en Lenny Taelman voor hun begeleiding, en voor alle gesprekken en discussies, die altijd motiverend op mij werkten;
- Bas Edixhoven, Ronald van Luijk, David Madore, Lenny Taelman, en Olivier Wittenberg, voor de discussies na het mini-symposium in Leiden op 25 juni 2013;
- tenslotte Samuele Anni, Steven Berghout, Owen Biesel, Raymond van Bommel, Johan Bosman, Fokko van de Bult, Birgit van Dalen, Christophe Debry, Maarten Derickx, Remy van Dobben de Bruyn, Krzysztof Dorobisz, Dino Festi, Alberto Gioia, Albert Gunawan, David Holmes, Michiel Kosters, Peter Koymans, Abtien Javanpeykar, Ariyan Javanpeykar, Niels Langeveld, Junjiang Liu, Stefan van der Lugt, Ronald van Luijk, Julian Lyczak, Chloe Martindale, Djordjo Milovic, Maxim Mornev, Marin van Noord, Giulio Orecchia, Carlo Pagano, René Pannekoek, Quintijn Puite, Jan van Rijn, Mima Stanojkovski, Marco Streng, Frank Takes, Jonathan Vis, Erik Visse, Qijun Yan, Yan Zhao, Weidong Zhuang, Wouter Zomervrucht, Stefan Zwetsloot, en vele anderen, voor het leuker maken van de afgelopen $4\frac{1}{2}$ jaar.

Curriculum vitae

Jinbi Jin is geboren op zondag 4 december 1988, te Almelo.

Van 2000 tot en met 2006 volgde hij onderwijs aan het RKSG Marianum, van 2000 tot en met 2003 in Lichtenvoorde, en van 2003 tot en met 2006 in Groenlo, waar hij ook zijn VWO-diploma in juni 2006 heeft gehaald. Daarna heeft hij tot en met 2011 Wiskunde gestudeerd aan de Universiteit Leiden, waar hij in december 2011 zijn diploma heeft gehaald.

Sinds oktober 2016 is hij begonnen met een post-doc aan het Max Planck Instituut voor Wiskunde in Bonn, Duitsland.

Index