Computability of the étale Euler-Poincaré characteristic

Jin, J.

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. □

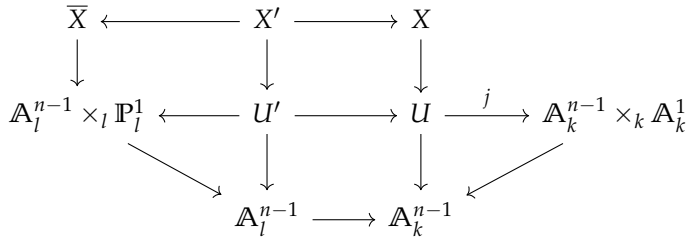
2.1.2 Smooth completions of curves

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

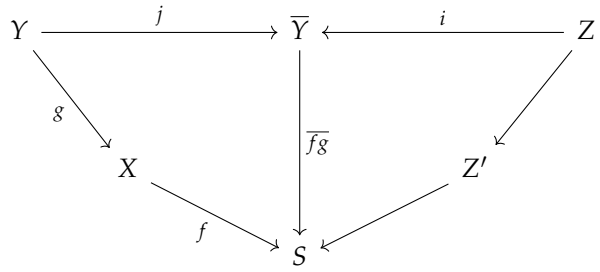
$$\operatorname{Hom}_{\mathbb{F}_3[t]}\left(\mathbb{F}_3[t, t^{-\frac{1}{2}}], A\right) \to \operatorname{Hom}_{\mathbb{F}_3[t^{\frac{1}{3}}]}\left(\mathbb{F}_3[t^{\frac{1}{6}}], A \otimes_{\mathbb{F}_3[t]} \mathbb{F}_3[t^{\frac{1}{3}}]\right)$$

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.