JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Christophe LEVRAT

Computing the cohomology of constructible étale sheaves on curves

Tome 36, n° 3 (2024), p. 1085-1122.
https://doi.org/10.5802/jtnb.1309

© Les auteurs, 2024.

Cet article est mis à disposition selon les termes de la licence CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
http://creativecommons.org/licenses/by-nd/4.0/fr/

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **36** (2024), 1085–1122

Computing the cohomology of constructible étale sheaves on curves

par Christophe LEVRAT

Résumé. Nous présentons une expression explicite du complexe de cohomologie d'un faisceau constructible de groupes abéliens sur le site étale d'une courbe algébrique irréductible sur un corps algébriquement clos, dans le cas où la torsion du faisceau est inversible dans le corps. Cette expression fait intervenir uniquement des groupes finis, et est fonctorielle en la courbe et le faisceau. En particulier, nous montrons comment calculer l'action galoisienne sur ce complexe. Nous présentons également un algorithme qui calcule cette expression, et étudions sa complexité. Nous illustrons cet algorithme par plusieurs exemples.

Abstract. We present an explicit expression for the cohomology complex of a constructible sheaf of abelian groups on the small étale site of an irreducible curve over an algebraically closed field, when the torsion of the sheaf is invertible in the field. This expression only involves finite groups, and is functorial in both the curve and the sheaf. In particular, we explain how to compute the Galois action on this complex. We also present an algorithm which computes this complex and study its complexity. We illustrate this algorithm with several examples.

1. Introduction

Let X_0 be an algebraic curve over a field k. Let n be a positive integer invertible in k_0, and $\mathcal{F}_0$ be a constructible sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules on the (small) étale site of X_0. Denote by k a separable closure of k_0, by X the base change of X_0 to k, and by $\mathcal{F}$ the restriction of $\mathcal{F}_0$ to X. The étale cohomology complex $\mathrm{R}\Gamma(X, \mathcal{F})$ is equipped with an action of $\mathrm{Gal}(k|k_0)$. Given the curve X and a suitable explicit description of the sheaf $\mathcal{F}$, we are interested in computing a finite extension k_1 of k_0 and a complex of $(\mathbb{Z}/n\mathbb{Z})[\mathrm{Gal}(k_1|k_0)]$-modules which represents $\mathrm{R}\Gamma(X, \mathcal{F})$.

The computability of étale cohomology groups of torsion sheaves on schemes of finite type over algebraically closed fields was proved in 2014 by Poonen, Testa and van Luijk [16, Thm. 7.9] in characteristic zero, and by Madore and Orgogozo in arbitrary characteristic [11, Thm. 0.1]. However,

Manuscrit reçu le 10 juillet 2023, révisé le 4 juin 2024, accepté le 26 juin 2024.
2020 *Mathematics Subject Classification.* 14F20, 11G20, 11Y16.
Mots-clefs. étale cohomology, constructible sheaf, algebraic curve, algorithm, complexity.

the algorithms described in these articles are not efficient enough to be used in practice, and the only known result about their complexity is that Madore and Orgogozo's algorithm is primitive recursive [10, Prop. 4.1.9]. In the case of smooth curves, some more efficient algorithms are known. When X is a smooth projective curve, $\mathrm{H}^1(X, \mu_n)$ is canonically isomorphic to the n-torsion of $\mathrm{Pic}(X)$; two algorithms, one developed by Huang and Ierardi [8], the other by Couveignes [1], compute this group when the base field k_0 is finite. Jin's algorithm [9] computes $\mathrm{H}^1(X, \mathcal{F})$ where X is a smooth curve and $\mathcal{F}$ is locally constant.

In this paper, we consider the case where X_0 is an integral curve over a field, and $\mathcal{F}_0$ is a constructible sheaf (or even a complex of such sheaves) on X_0. We present an explicit expression for the cohomology complex $\mathrm{R}\Gamma(X, \mathcal{F})$ with the aforementioned Galois action, as well as an algorithm which computes this complex (under some classical computability assumptions on the field k_0). The latter makes use of an existing algorithm computing $\mathrm{H}^1(X, \mu_n)$, such as those mentioned above. We also provide complexity bounds for this method. In particular, in the case of locally constant sheaves on smooth projective curves over finite fields, the complexity of computing $\mathrm{H}^1(X, \mathcal{F})$ using this algorithm is lower than Jin's. In the case where the base field k_0 is finite, we present an idea that should allow us to reduce the complexity of this algorithm, and explain why this would be a crucial step towards developing a polynomial-time point counting algorithm for surfaces.

In Section 2, we investigate the properties of the minimal Galois cover of a scheme trivialising the $\mathbb{Z}/n\mathbb{Z}$-torsors on this scheme, as well as its construction in the case of curves. In Section 3, we explain how to compute the cohomology of a locally constant sheaf on a scheme of cohomological dimension at most 1. Section 4 contains the proof of the main theorem: an explicit expression of $\mathrm{R}\Gamma(X, -)$ when X is a curve over a field of cohomological dimension at most 1. We then present in Section 5 the algorithms used to compute the cohomology of a constructible sheaf on such a curve, as well as their complexity. We also describe the potential application of our algorithms to point counting on surfaces over finite fields. In Sections 6 and 7, we illustrate these algorithms in two situations.

Terminology. *Unless explicitly stated otherwise, the word* cover *denotes a surjective finite étale map. A* Galois cover *is always supposed to be connected.*

2. The cover trivialising $\mathbb{Z}/n\mathbb{Z}$-torsors

2.1. General construction and properties. Let n be a positive integer. We will denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Given a (discrete) Λ-module M, we will denote by $M^\vee$ its Λ-dual.

Lemma 2.1. *Let G be a locally compact topological group. Consider the abelian group Λ, with the trivial action of G. Suppose the continuous cohomology group $\mathrm{H}^1(G,\Lambda)$ is finite. There is a unique closed normal subgroup S of G such that G/S is isomorphic to the Λ-dual $\mathrm{H}^1(G,\Lambda)^\vee$ of $\mathrm{H}^1(G,\Lambda)$. Moreover, S is a characteristic subgroup of G.*

Proof. Define S as the closure in G of $G^n[G,G]$. This group S is a characteristic subgroup of G (i.e. stable by all continuous automorphisms) because G^n and $[G,G]$ are stable by automorphisms. Since Λ is an n-torsion abelian group, there is a canonical isomorphism

$$\mathrm{Hom}_{\mathrm{cont}}(G/S,\Lambda) \xrightarrow{\sim} \mathrm{Hom}_{\mathrm{cont}}(G,\Lambda) = \mathrm{H}^1(G,\Lambda).$$

Pontryagin duality [7, Thm. 7.63] applied to the locally compact abelian group G/S yields the following isomorphism:

$$\mathrm{Hom}_{\mathrm{cont}}(G/S,\Lambda)^\vee \xrightarrow{\sim} G/S.$$

Now let H be a closed normal subgroup of G such that G/H is isomorphic to $\mathrm{H}^1(X,\Lambda)^\vee$. It necessarily contains S since G/H is a Λ-module. Since G/S and G/H have the same finite cardinality, $H = S$. □

Corollary 2.2. *Let X be an integral noetherian scheme such that $\mathrm{H}^1(X,\Lambda)$ is finite. Up to isomorphism, there is a unique étale Galois cover $X^{\langle n\rangle}$ of X with automorphism group isomorphic to $\mathrm{H}^1(X,\Lambda)^\vee$.*

Proof. This follows immediately from Lemma 2.1, the canonical isomorphism

$$\mathrm{H}^1(\pi_1(X),\Lambda) \xrightarrow{\sim} \mathrm{H}^1(X,\Lambda)$$

and Grothendieck–Galois theory. □

From now on, given such a scheme X, we will always denote by $X^{\langle n\rangle}$ a Galois cover of X as in the previous corollary.

Proposition 2.3. *Let X be an integral noetherian scheme such that $\mathrm{H}^1(X,\Lambda)$ is finite. For any finitely generated Λ-module M, the morphism $\mathrm{H}^1(X,M) \to \mathrm{H}^1(X^{\langle n\rangle},M)$ is trivial.*

Proof. Recall that $X^{\langle n\rangle}$ corresponds to the open subgroup S of $\pi_1(X)$, which is the closure of the subgroup $\pi_1(X)^n[\pi_1(X),\pi_1(X)]$. Since M is n-torsion, any map $\pi_1(X) \to M$ is trivial on S, hence $\mathrm{Hom}(\pi_1(X),M) \to \mathrm{Hom}(\pi_1(X^{\langle n\rangle}),M)$ is trivial. □

2.2. Explicit construction in the case of curves. Let U be a smooth integral curve over a field k. Denote by K its function field. Let n be a positive integer invertible in k. Recall the following description of $\mathrm{H}^1(U,\mu_n)$ in terms of divisors on U.

Lemma 2.4. *The group* $\mathrm{H}^1(U,\mu_n)$ *is canonically isomorphic to the quotient of*

$$\{(D,f)\in \mathrm{Div}(U)\times K^\times \mid nD=\mathrm{div}(f)\}$$

by the subgroup of pairs $(\mathrm{div}(f),f^n)$ *with* $f\in K^\times$.

Proof. This follows immediately from the corresponding description in terms of invertible sheaves given in [17, 040Q]. □

We will denote by $[D,f]$ the class of the pair (D,f) in $\mathrm{H}^1(U,\mu_n)$. Now suppose that k is separably closed. Let X be the smooth compactification of U. Denote by g the genus of X. Consider the closed complement $Z=\{P_1,\dots,P_r\}$ of U in X. When $r=0$ the lemma above is the usual description of $\mathrm{H}^1(X,\mu_n)$ as the group of n-torsion points on the Jacobian of X. When $r\geqslant 1$, the Gysin sequence

$$0\longrightarrow \mathrm{H}^1(X,\mu_n)\longrightarrow \mathrm{H}^1(U,\mu_n)\longrightarrow \mathrm{H}^0(Z,\Lambda)\longrightarrow \Lambda\longrightarrow 0$$

shows that $\mathrm{H}^1(U,\mu_n)$ is a free Λ-module of rank $2g-1+r$. Consider a basis $([D_i,g_i])_{1\leqslant i\leqslant s}$ of $\mathrm{H}^1(U,\mu_n)$. For every integer $j\in\{1\dots s\}$, we denote by V_j the normalisation of U in $K(\sqrt[n]{g_1},\dots,\sqrt[n]{g_j})$, by ϕ_j the induced cover $U_j\to U$, and set $V=V_s$.

Proposition 2.5. *The cover* $\phi\colon V\to U$ *is isomorphic to* $U^{\langle n\rangle}\to U$.

Proof. First of all, each cover $V_i\to V_{i-1}$ is étale, because it is constructed by taking an n^{th} root of a function whose valuation at each point is a multiple of n. Let us check by induction on $j\in\{1,\dots,r\}$ that $V_j\to V_{j-1}$ is Galois with group $\mu_n(k)$. This is obviously true for $j=1$. For any $i\in\{1,\dots,j-1\}$ the extension $V_i=V_{i-1}(\sqrt[n]{g_i})$ of V_{i-1} is Galois with group $\mu_n(k)$ by the induction hypothesis. The Hochschild–Serre spectral sequence yields an exact sequence

$$0\longrightarrow \mathrm{H}^1(\mu_n(k),\Lambda)\longrightarrow \mathrm{H}^1(V_{i-1},\Lambda)\longrightarrow \mathrm{H}^1(V_i,\Lambda).$$

Therefore, the kernel of $\phi_i^\star\colon \mathrm{H}^1(U,\Lambda)\to \mathrm{H}^1(V_i,\Lambda)$ is the direct sum $\Lambda[D_1,g_1]\oplus\dots\oplus\Lambda[D_i,g_i]\simeq\Lambda^i$, and $[D_j,g_j]$ is not in the kernel; the order of $\phi_i^\star[D_j,g_j]$ in $\mathrm{H}^1(V_i,\mu_n)$ is still n. Thus, $V\to U$ is finite étale of order n^r. The field k being separably closed, the extension $k(V)$ of $k(U)$ is the splitting field of the polynomials $T^n-g_1,\dots,T^n-g_r$, so it is Galois. The morphism $V\to U$ is therefore an étale Galois cover. An element of the group $\mathrm{Aut}(V|U)$ is an automorphism defined by $(\sqrt[n]{g_1}\mapsto\zeta_1\sqrt[n]{g_1},\dots,\sqrt[n]{g_r}\mapsto\zeta_r\sqrt[n]{g_r})$, where the ζ_i are n^{th} roots of unity in k; the group $\mathrm{Aut}(V|U)$ is therefore canonically isomorphic to $\mathrm{Hom}_\Lambda(\mathrm{H}^1(U,\mu_n),\mu_n)=\mathrm{H}^1(U,\Lambda)^\vee$. Lemma 2.1 now ensures that V is isomorphic to $U^{\langle n\rangle}$. □

Remark 2.6. *We will often consider the following situation. Let* $V\to U$ *be an étale Galois cover of smooth integral curves over* k. *The cover*

$V^{\langle n\rangle} \to U$ is still Galois because $V^{\langle n\rangle} \to V$ is characteristic (i.e. if $V \to S$ is a Galois cover, $V^{\langle n\rangle} \to S$ is Galois as well). Sometimes, we will need to compute a subcover $V' \to V$ of $V^{\langle n\rangle}$ by taking n^{th} roots of functions $g_1, \dots, g_t$ generating a submodule of $\mathrm{H}^1(V, \mu_n)$. In that case, $V' \to U$ is still Galois if and only if the submodule generated by $g_1, \dots, g_t$ is stable under the action of $\mathrm{Aut}(V|U)$. This is the case for instance if we take the submodule of elements of $\mathrm{H}^1(V, \mu_n)$ defined over some subfield of k over which the elements of $\mathrm{Aut}(V|U)$ are also defined.

2.3. Ramification at infinity. Let U be an integral affine curve over an algebraically closed field k. Denote by X the smooth compactification of U. Let n be an integer invertible in k, and denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let us study the ramification at infinity of $U^{\langle n\rangle} \to U$, i.e. the ramification of the smooth compactification X' of $U^{\langle n\rangle}$ above the points $P_0, \dots, P_r$ of $X - U$. The map $\mathrm{H}^2_Z(X, \mu_n) \to \mathrm{H}^2(X, \mu_n)$ can be expressed, using the Gysin isomorphism $\mathrm{H}^0(Z, \Lambda) \to \mathrm{H}^2_Z(X, \mu_n)$ and the isomorphism $\mathrm{H}^2(X, \mu_n) \to \Lambda$, as the sum map $\mathrm{H}^0(Z, \Lambda) \to \Lambda$. A basis of its kernel is given by $(P_1 - P_0, \dots, P_r - P_0)$. Consider functions $g_1, \dots, g_r \in k(X)$ such that

$$\mathrm{div}(g_i) = nD_i + (P_i - P_0)$$

where $D_i \in \mathrm{Div}^0(X - \{P_0, \dots, P_r\})$. The cover $X' \to X^{\langle n\rangle}$ corresponds to the function field extension

$$k(X^{\langle n\rangle})(\sqrt[n]{g_1}, \dots, \sqrt[n]{g_r})$$

of $k(X^{\langle n\rangle})$. Let $i \in \{1 \dots r\}$. The extension $k(X^{\langle n\rangle})(\sqrt[n]{g_j}, j \neq i)$ of $k(X^{\langle n\rangle})$ yields a cover $Y_i \to X^{\langle n\rangle}$ which is unramified above P_i because $v_{P_i}(g_j) = 0$. The cover $X' \to Y_i$, however, is ramified at P_i; let Q_i be a preimage of P_i in Y_i. Since $v_{Q_i}(g_i) = 1$, the fibre X'_{Q_i} is isomorphic to $k[x]/(x^n)$, and the ramification index of $X' \to Y_i$ at any preimage of Q_i is n. Above P_i, there are exactly $\frac{1}{n}|\mathrm{H}^1(U, \Lambda)|$ points of X', each of with ramification index n. Let R_i be a preimage of Q_i in X'. The inertia subgroup $I_{R_i|P_i} \subset \mathrm{Aut}(U^{\langle n\rangle}|U)$ of R_i fits in the short exact sequence

$$0 \longrightarrow I_{R_i|Q_i} \longrightarrow I_{R_i|P_i} \longrightarrow I_{Q_i|P_i} \longrightarrow 0$$

(see [17, 0BU7]). As $I_{Q_i|P_i} = 0$, there are isomorphisms

$$I_{R_i|P_i} = I_{R_i|Q_i} = \mathrm{Aut}(X'|Y_i) \simeq \Lambda.$$

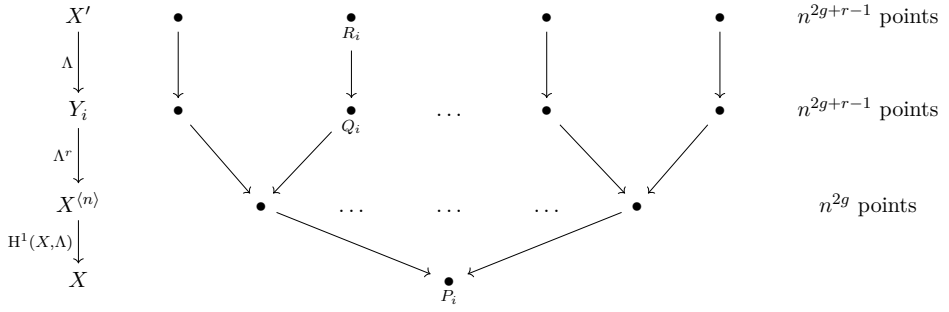

FIGURE 2.1. Ramification at infinity of the cover $U^{\langle n\rangle} \to U$

As a subgroup of $\mathrm{Aut}(U^{\langle n\rangle}|U)$, the group $I_{R_i|P_i}$ is generated by $\sqrt[n]{g_i} \mapsto \zeta\sqrt[n]{g_i}$, where ζ is a primitive n^{th} root of unity in k. The results regarding preimages and ramification indices also apply to P_0, which had been chosen arbitrarily. With the above notation, the subgroup $I_{R_0|P_0}$ is generated by the automorphism

$$(\sqrt[n]{g_1}, \ldots, \sqrt[n]{g_r}) \longmapsto (\zeta\sqrt[n]{g_1}, \ldots, \zeta\sqrt[n]{g_r}).$$

2.4. Cohomology of the ramification groups. Let n be a positive integer. Denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let us consider an étale Galois cover $V \to U$ of smooth integral curves over an algebraically closed field k of characteristic prime to n. Let K be the function field of U. Denote by X (resp. Y) the smooth compactification of U (resp. V). Set $G = \mathrm{Aut}(V|U)$. Let x be a closed point of $X - U$. Consider an inertia group $I \subset \mathrm{Gal}(K^{\mathrm{sep}}|K)$ at x, and one of its finite quotients $I_y \subset G$, which is the stabiliser in G of a closed point $y \in Y - V$ mapping to x. Denote by $P \lhd I$ and $P_y \lhd I_y$ the wild inertia subgroups. There are canonical isomorphisms [17, 09EE]

$$I/P \xrightarrow{\sim} \lim_{m\nmid p} \mu_m(k) \text{ and } I_y/P_y \xrightarrow{\sim} \mu_e(k)$$

where e is the ramification index of $Y \to X$ at y. From now on, we assume that n divides e. Let M be a $\Lambda[G]$-module.

Proposition 2.7. *In the situation described above, the canonical maps*

$$\tau_{\leqslant 1}\,\mathrm{R}\Gamma(I_y/P_y, M^{P_y}) \longrightarrow \mathrm{R}\Gamma(I/P, M^P) \longrightarrow \mathrm{R}\Gamma(I, M)$$

are quasi-isomorphisms.

Proof. Let σ denote a pro-generator of I/P, and σ_y its image in I_y/P_y. The actions of σ and σ_y on M are equal. Set $N_y = \sum_{i=1}^{e} \sigma_y^i$. The usual results

on the cohomology of (pro)-cyclic groups [18, Calc. 6.2.1] [5, Prop. 8.1.4] show that the map on the left hand side is:

$$\begin{array}{ccc} \mathrm{R}\Gamma(I/P, M^P) & = & M^P \xrightarrow{\sigma-\mathrm{id}} M^P \longrightarrow 0 \\ \uparrow & & \| \quad\quad \uparrow \quad\quad \uparrow \\ \tau_{\leqslant 1}\,\mathrm{R}\Gamma(I_y/P_y, M^{P_y}) & = & M^P \xrightarrow{\sigma_y-\mathrm{id}} \ker(N_y) \longrightarrow 0 \end{array}$$

Since n divides e, the action of N_y on M is trivial and $\ker(N_y) = M^P$, which shows that the map above is a quasi-isomorphism. The fact that the map on the right hand side is a quasi-isomorphism is shown in [5, Prop. 8.1.4] as well. □

The following lemma shows how to explicitly construct the inverse of the map on the left hand side as a morphism of complexes; it will be used in Theorem 4.5. We denote by $\mathrm{Hom}_{\mathrm{cr}}$ the groups of crossed homomorphisms: given a group G and a G-module M, $\mathrm{Hom}_{\mathrm{cr}}(G, M)$ is the group of maps $f\colon G \to M$ such that for all $g, h \in G$, $f(gh) = f(g) + g \cdot f(h)$.

Lemma 2.8. *The canonical map* $\mathrm{Hom}_{\mathrm{cr}}(I_y/P_y, M^{P_y}) \to \mathrm{Hom}_{\mathrm{cr}}(I_y, M)$ *has a section.*

Proof. Let $u\colon I_y \to M$ be a crossed homomorphism. Consider the commutative diagram

$$\begin{array}{ccccc} I_y & \xrightarrow{u} & M & \xrightarrow{q} & M_{P_y} \\ \downarrow & & \uparrow & \nearrow_{\alpha} & \\ I_y/P_y & \dashrightarrow & M^{P_y} & & \end{array}$$

and set $f = q \circ u$. For all $x \in P_y$ and $g \in I_y$, the definition of M_{P_y} ensures that $f(xg) = f(x) + q(x \cdot u(g)) = f(x) + f(g)$. Hence, for any $x \in P_y$, $f(x^{|P_y|}) = |P_y| f(x)$ is zero ; since multiplication by $|P_y|$ is an automorphism of M, this means that $f(x) = 0$. Therefore, there is a quotient map $\overline{f}\colon I_y/P_y \to M_{P_y}$. Set $\overline{u} = \alpha^{-1} \circ \overline{f}\colon I_y/P_y \to M^{P_y}$. The map $u \mapsto \overline{u}$ is clearly linear. Moreover, $\overline{u}$ is still a crossed homomorphism since $\overline{u}(\bar{g}_1\bar{g}_2) = \alpha^{-1} f(g_1 g_2) = \alpha^{-1} f(g_1) + q(g_1 \cdot \alpha^{-1} u(g_2))$. The I_y-linearity of $\alpha^{-1} q$ concludes. □

2.5. A similar cover with Galois action. Let k_0 be a perfect field, and k be an algebraic closure of k_0. Let n be an integer invertible in k. Denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let V_0 be a geometrically integral smooth curve over k_0. As usual, the base change $- \times_{k_0} k$ will be denoted by removing the subscript $_0$. We wish to compute a (connected) characteristic cover V_0' of V_0 such that the map $\mathrm{H}^1(V, \Lambda) \to \mathrm{H}^1(V', \Lambda)$ is trivial. In the case where V is connected and the elements of $\mathrm{H}^1(V, \mu_n)$ are defined over k_0,

the cover $V^{\langle n\rangle}$ constructed in the previous sections comes from k_0, and we are done. However, this is not the case in general. The construction below is a refinement of the simple idea of computing the Galois orbit of $V^{\langle n\rangle}$.

Construction of V_0'. The function field of Y_0 is of the form $k_0(x)[y]/(f)$, with $f \in k(x)[y]$. Denote by k_1 the algebraic closure of k_0 in $k_0(x)[y]/(f)$; since k_0 is perfect, k_1 is a separable extension. Let V_1 be a connected component of V. Let $([D_1, g_1], \dots, [D_r, g_r])$ be a basis of $\mathrm{H}^1(V_1, \mu_n)$ as in Lemma 2.4. Denote by k_2 the minimal extension of k_0 over which the g_i are defined. Let L be the Galois closure of the extension of k_0 generated by k_1, k_2 and $\mu_n(k)$. Let α be a primitive element of the extension $L|k_1$, and $m \in k_1[t]$ its minimal polynomial. For $i \in \{1 \dots r\}$, write $g_i = g_i'(\alpha, x, y)$ with $g_i' \in k_0(x)[t, y]/(m(t), f(x, y))$. Let $V_0' \to V_0$ be the normalisation of V_0 in the function field $k_0(\alpha, x, y)(\sqrt[n]{g_1'}, \dots, \sqrt[n]{g_r'})$. The curve V' is isomorphic to the $\mathrm{Gal}(L|k_0)$-orbit of $V_1^{\langle n\rangle}$; it has $[L : k_0]$ connected components, and the map $\mathrm{H}^1(V, \Lambda) \to \mathrm{H}^1(V', \Lambda)$ is trivial.

Note that since the degree of $V_0' \to (V_0 \times_{k_1} L)$ is n^r and that of $V_0 \times_{k_1} L \to V_0$ is $[L : k_1]$, the degree of $V_0' \to V_0$ is $n^r[L : k_1]$.

Proposition 2.9. *The cover $V_0' \to V_0$ is characteristic, i.e. if V_0 is an étale Galois cover of a curve U_0, then $V_0' \to U_0$ is still Galois.*

Proof. Consider the situation where V_0 is an étale Galois cover of a smooth integral k_0-curve U_0. Here is how to explicitly compute the automorphism group of $V_0 \to U_0$. The map $V_0' \to V_0$ has degree $n^r[L : k_1]$. Using the notations above, set $z_i = \sqrt[n]{g_i'}$. The elements of $\mathrm{Aut}(k_0(V_0')|k_0(V_0))$ are defined by $t \mapsto \sigma(t), z_i \mapsto \zeta_i z_i$ where $\sigma \in \mathrm{Gal}(L|k_1)$ and $\zeta_i \in \mu_n(L)$. There are $\deg(V_0' \to V_0) = n^r[L : k_1]$ such automorphisms since $\mu_n(k) \subset L$, hence the cover $V_0' \to V_0$ is Galois. Let us now compute the automorphism group of $V_0' \to U_0$. Its elements are defined by

$$(t, x, y, z_1, \dots, z_r) \longmapsto (\sigma(t), x', y', z_1', \dots, z_r')$$

where $\sigma \in \mathrm{Gal}(L|k_0)$, the pair (x', y') is the image of (x, y) under a U_0-automorphism of V_0 whose image in $\mathrm{Gal}(k_1|k_0)$ is the same as that of σ, and the elements $z_i' \in k_0(V_0')$ satisfy $z_i'^n = \phi(g_i')$. As expected, there are $\deg(V_0'|U_0) = n^r[L : k_1] \deg(V_0 \to U_0)$ elements in $\mathrm{Aut}(V_0'|U_0)$, and $V_0' \to U_0$ is Galois. □

Remark 2.10. *If need be, the Galois extension L of k_0 may be chosen to be a little larger, for instance to make sure that the points at infinity of the curve V' are defined over L. This does not affect any of the previous proofs.*

3. Schemes of cohomological dimension 1

Let n be a positive integer, and $\Lambda = \mathbb{Z}/n\mathbb{Z}$. Let X be an integral noetherian scheme, and $\bar{\eta}$ be a generic geometric point of X.

Proposition 3.1. *Let $\mathscr{L}$ be a finite locally constant sheaf of $\mathbb{Z}/n\mathbb{Z}$-modules on X. Let $Y \to X$ be an étale Galois cover such that $\mathscr{L}|_Y$ is constant and the morphism*

$$\mathrm{H}^1(X, \mathscr{L}) \longrightarrow \mathrm{H}^1(Y, \mathscr{L}|_Y)$$

is trivial. Then the morphism

$$\tau_{\leqslant 1}\, \mathrm{R}\Gamma(\mathrm{Aut}(Y|X), \mathscr{L}_{\bar{\eta}}) \longrightarrow \tau_{\leqslant 1}\, \mathrm{R}\Gamma(X, \mathscr{L})$$

is a quasi-isomorphism.

Proof. Let G be the automorphism group of $Y \to X$. The associated Hochschild–Serre spectral sequence yields the following short exact sequence:

$$0 \longrightarrow \mathrm{H}^1(G, \mathscr{L}_{\bar{\eta}}) \longrightarrow \mathrm{H}^1(X, \mathscr{L}) \longrightarrow \mathrm{H}^0(G, \mathrm{H}^1(Y, \mathscr{L}|_Y))$$

Hence the map $\mathrm{H}^1(G, \mathscr{L}_{\bar{\eta}}) \to \mathrm{H}^1(X, \mathscr{L})$ is an isomorphism, and

$$\mathrm{R}\Gamma(G, \mathscr{L}_{\bar{\eta}}) \longrightarrow \mathrm{R}\Gamma(X, \mathscr{L})$$

yields isomorphisms on cohomology groups in degree 0 and 1. □

Remark 3.2. *If in addition X has cohomological dimension 1 then*

$$\tau_{\leqslant 1}\, \mathrm{R}\Gamma(\mathrm{Aut}(Y|X), \mathscr{L}_{\bar{\eta}}) \longrightarrow \mathrm{R}\Gamma(X, \mathscr{L})$$

is a quasi-isomorphism.

Remark 3.3. *Here is how to construct a cover Y as in the proposition, provided that $\mathrm{H}^1(W, \Lambda)$ is finite. Pick an étale Galois cover $W \to X$ such that $\mathscr{L}|_W$ is a constant sheaf. Set $Y = W^{\langle n \rangle}$: since $Y \to W$ is characteristic, the cover $Y \to X$ is still Galois, and Proposition 2.3 ensures that $\mathrm{H}^1(X, \mathscr{L}) \to \mathrm{H}^1(Y, \mathscr{L}|_Y)$ is trivial.*

Given a profinite group H, we will denote by $P_H(\Lambda)$ the usual projective resolution (sometimes called *bar resolution*) of the trivial $\Lambda[\![H]\!]$-module Λ.

Proposition 3.4. *Suppose X is of cohomological dimension 1. Let $\mathscr{L} = [\mathscr{L}^0 \to \mathscr{L}^1 \to \cdots \to \mathscr{L}^s]$ be a complex of finite locally constant sheaves of Λ-modules on X, and Y be an étale Galois cover of X such that each map $\mathrm{H}^1(X, \mathscr{L}^i) \to \mathrm{H}^1(Y, \mathscr{L}^i|_Y)$ is trivial. Write $G = \mathrm{Aut}(Y|X)$. Consider the double complex $B^{\bullet,\bullet}$ defined by $B^{i,j} = \mathrm{Hom}_{\Lambda[G]}(\tau_{\geqslant -1} P_G^{-j}(\Lambda), \mathscr{L}^i_{\bar{\eta}})$. Then $\mathrm{R}\Gamma(X, \mathscr{L})$ is represented by the total complex $\mathrm{Tot}\, B^{\bullet,\bullet}$.*

Proof. We wish to compute

$$\mathrm{R}\Gamma(X,\mathscr{L}) = \mathrm{R}\Gamma(\pi_1(X),\mathscr{L}_{\bar{\eta}}) = \mathrm{RHom}_{\Lambda[\![\pi_1(X)]\!]}(\Lambda,\mathscr{L}_{\bar{\eta}}),$$

which is represented by the complex

$$\mathrm{Hom}^{\bullet}_{\Lambda[\![\pi_1(X)]\!]}(P_\pi(\Lambda),\mathscr{L}_{\bar{\eta}}) = \mathrm{Tot}(A^{\bullet,\bullet})$$

where $A^{i,j} = \mathrm{Hom}_{\Lambda[\![\pi_1(X)]\!]}(P^{-j}_{\pi_1(X)}(\Lambda),\mathscr{L}^i_{\bar{\eta}})$. The map $B^{\bullet,\bullet} \to A^{\bullet,\bullet}$ induced by the quotient map $\pi_1(X) \to G$ defines a morphism between the spectral sequence associated to these quotients. Recall that for each $i \in \{1 \dots s\}$, the map

$$\tau_{\leqslant 1}\,\mathrm{Hom}_{\Lambda[G]}(P_G(\Lambda),\mathscr{L}^i_{\bar{\eta}}) \longrightarrow \mathrm{Hom}_{\Lambda[\![\pi_1(X)]\!]}(P_{\pi_1(X)}(\Lambda),\mathscr{L}^i_{\bar{\eta}})$$

is a quasi-isomorphism. Since the functor $\mathrm{Hom}(-,\mathscr{L}^i_{\bar{\eta}})$ is left exact,

$$\mathrm{Hom}_{\Lambda[G]}(\tau_{\geqslant -1}P_G(\Lambda),\mathscr{L}^i_{\bar{\eta}}) = \tau_{\leqslant 1}\,\mathrm{Hom}_{\Lambda[H]}(P_G(\Lambda),\mathscr{L}^i_{\bar{\eta}}).$$

Hence the map $B^{\bullet,\bullet} \to A^{\bullet,\bullet}$ defines, on each column, a quasi-isomorphism of complexes. It therefore induces an isomorphism between the first pages of the corresponding spectral sequences (for the upward orientation) associated to $B^{\bullet,\bullet}$ and $A^{\bullet,\bullet}$: in position (i,j), it is the isomorphism $\mathrm{H}^j(H,\mathscr{L}^i_{\bar{\eta}}) \to \mathrm{H}^j(\pi_1(X),\mathscr{L}^i_{\bar{\eta}})$ for $j \leqslant 1$, and $0 \to \mathrm{H}^j(\pi_1(X),\mathscr{L}^i_{\bar{\eta}}) = 0$ otherwise. Therefore, the map between the abutments of these two spectral sequences is an isomorphism, i.e. the map $\mathrm{Tot}(B^{\bullet,\bullet}) \to \mathrm{Tot}(A^{\bullet,\bullet})$ is a quasi-isomorphism. □

4. Explicit computation of RΓ of a (possibly singular) curve

In this section, we are going to describe how to compute the cohomology of a complex of constructible sheaves on a curve. Let k_0 be a field, and k be a separable closure of k_0. Consider a geometrically irreducible curve X_0 over k_0, and its base change X over k. We are allowed to make the following additional assumptions, which do not alter the computed cohomology complex.

- The field k_0 is perfect, hence k is algebraically closed: the perfect closure k_0^{pf} of k_0 being a purely inseparable extension, the base change $- \times_{k_0} k_0^{\mathrm{pf}}$ induces an isomorphism on cohomology.
- The curve X is reduced: being a universal homeomorphism, the map $X_{\mathrm{red}} \to X$ induces an isomorphism on cohomology.
- The curve X has at worst multicross singularities [17, 0C1P]: the seminormalisation map $X^{\mathrm{sn}} \to X$ being a universal homeomorphism [17, 0EUS], it induces an isomorphism on cohomology, so we may assume X is seminormal. Since a seminormal curve over an algebraically closed field has at worst multicross singularities [2, §2, Cor. 1], we may assume this is the case for X.

4.1. Cohomology with support in a 0-dimensional subscheme. Let k be an algebraically closed field. Let n be an integer invertible in k, and $\Lambda = \mathbb{Z}/n\mathbb{Z}$. Let X be an integral curve over k. Consider a nonempty closed zero-dimensional subscheme $i\colon Z \to X$, and its open complement $j\colon U \to X$. Let $\mathrm{R}\Gamma_Z(X,-)$ denote cohomology with support in Z. Since $\mathrm{R}\Gamma_Z(X,-) = \bigoplus_{z\in Z} \mathrm{R}\Gamma_z(X,-)$, we consider a single point $z \in Z$ and focus on computing $\mathrm{R}\Gamma_z(X,-)$.

Lemma 4.1. *Let $\mathscr{L}$ be a finite locally constant sheaf on U.*

- $\mathrm{H}^0_z(X, j_!\mathscr{L}) = \mathrm{H}^0_z(X, j_\star\mathscr{L}) = \mathrm{H}^1_z(X, j_\star\mathscr{L}) = 0$
- $\mathrm{H}^1_z(X, j_!\mathscr{L}) = \mathrm{H}^0(z, i^\star j_\star\mathscr{L})$
- $\mathrm{H}^2_z(X, j_!\mathscr{L}) = \mathrm{H}^2_z(X, j_\star\mathscr{L})$
- *For all $i \geqslant 3$, $\mathrm{H}^i_z(X, j_!\mathscr{L}) = \mathrm{H}^i_z(X, j_\star\mathscr{L}) = 0$.*

Proof. Since $\mathrm{H}^0(X, j_\star\mathscr{L}) \to \mathrm{H}^0(X - z, j_\star\mathscr{L})$ is an isomorphism and $\mathrm{H}^1(X, j_\star\mathscr{L}) \to \mathrm{H}^1(X - z, j_\star\mathscr{L})$ is always a monomorphism, the long exact sequence for cohomology with support associated to $j_\star\mathscr{L}$ shows that $\mathrm{H}^0_z(X, j_\star\mathscr{L}) = \mathrm{H}^1_z(X, j_\star\mathscr{L}) = 0$. Moreover, for any $j \geqslant 3$, the groups $\mathrm{H}^{j-1}(X - z, j_\star\mathscr{L})$ and $\mathrm{H}^j(X, \mathscr{L})$ are trivial, hence $\mathrm{H}^j_z(X, j_\star\mathscr{L}) = 0$. Recall that $\mathrm{H}^i_z(X, i_\star -) = \mathrm{H}^i(z, -)$. The long exact sequence of $\mathrm{H}^i_z(X,-)$ associated to the short exact sequence

$$0 \longrightarrow j_!\mathscr{L} \longrightarrow j_\star\mathscr{L} \longrightarrow i_\star i^\star j_\star\mathscr{L} \longrightarrow 0$$

shows that $\mathrm{H}^0_z(X, j_!\mathscr{L}) = 0$, $\mathrm{H}^1_z(X, j_!\mathscr{L}) = \mathrm{H}^0(z, i^\star j_\star\mathscr{L})$ and also $\mathrm{H}^2_z(X, j_!\mathscr{L}) = \mathrm{H}^2_z(X, j_\star\mathscr{L})$. The groups $\mathrm{H}^i_z(X, j_!\mathscr{L})$ are also trivial as soon as $i \geqslant 3$. □

Let us now compute the group $\mathrm{H}^2_z(X, j_!\mathscr{L}) = \mathrm{H}^2_z(X, j_\star\mathscr{L})$. From now on, we assume X to have only multicross singularities. Let $z_1, \ldots, z_r$ be the preimages of z in the normalisation $\widetilde{X}$ of X. Denote by X_z the strict henselisation of X at z. It contains one closed point z', as well as r minimal primes $z'_1, \ldots, z'_r$. Set $U_z \coloneqq U \times_X X_z$. Consider the following cartesian diagram.

$$\begin{array}{ccccc} U_z & \xrightarrow{j'} & X_z & \xleftarrow{i'} & z' \\ \downarrow{\scriptstyle g'} & & \downarrow{\scriptstyle g} & & \downarrow \\ U & \xrightarrow{j} & X & \xleftarrow{i} & z \end{array}$$

The following proof is given in [14, II, Prop. 1.1] in the special case of smooth curves.

Lemma 4.2. *Let $\mathcal{F}$ be a sheaf on U_z. For every nonnegative integer q, the group $\mathrm{H}^q(X_z, j'_!\mathcal{F})$ is trivial.*

Proof. The assertion holds for $q = 0$ since $\mathrm{H}^0(X_z, j'_!\mathcal{F})$ is the kernel of the map $\mathrm{H}^0(X_z, j'_\star\mathcal{F}) \to \mathrm{H}^0(X_z, i'_\star i'^\star j_\star\mathcal{F})$, which is simply the identity map of

$\mathrm{H}^0(U_z, \mathcal{F})$. Let us first show that for any injective sheaf J on U_z, the sheaf $j'_!\mathcal{F}$ on X is acyclic. To this end, we are going to prove that

$$0 \longrightarrow j'_!J \longrightarrow j'_\star J \longrightarrow i'_\star i'^\star j'_\star J \longrightarrow 0$$

is an injective resolution of $j'_!J$; the long exact sequence associated to this short exact sequence then shows that $\mathrm{H}^q(X_z, j'_\star J) = 0$ for any $q \geqslant 1$. Fix separable closures of $k(z'_1), \dots, k(z'_r)$, and denote by $I_1, \dots, I_r$ the associated Galois groups. The functor $i^\star j_\star$ may be rewritten as follows:

$$\begin{aligned} \mathrm{Mod}_{I_1} \times \cdots \times \mathrm{Mod}_{I_r} &\longrightarrow \mathrm{Ab} \\ (M_1, \dots, M_r) &\longmapsto M_1^{I_1} \times \cdots \times M_r^{I_r} \end{aligned}$$

This functor admits a left adjoint, which sends an abelian group M to $(M, \dots, M)$ with trivial $(I_1, \dots, I_r)$-action. Since this left adjoint is exact, $i'^\star j'_\star$ sends injectives to injectives. The functors $i'_\star$ and $j'_\star$ also send injectives to injectives, therefore the short exact sequence above is an injective resolution of $j'_!J$. We are now ready to prove the result. Let $\mathcal{F}$ be a sheaf on U_z, and let $J^\bullet$ be an injective resolution of $\mathcal{F}$. Then $j'_!J^\bullet$ is an acyclic resolution of $j'_!\mathcal{F}$, and $\mathrm{H}^q(X_z, j'_!\mathcal{F})$ is the q^{th} cohomology group of the complex $\Gamma(X_z, j'_!J^\bullet)$. The latter group is the image of $\mathcal{F}$ under the q^{th} right derived functor of $\Gamma(X_z, j'_!-)$, which is zero as proven above. □

Let $\nu\colon \widetilde{X} \to X$ be the normalisation map. Set $\widetilde{z} \coloneqq z \times_X \widetilde{X}$.

Proposition 4.3. *Let $\mathscr{L}$ be a finite locally constant sheaf on U. The map*

$$\mathrm{R}\Gamma_z(X, j_\star\mathscr{L}) \longrightarrow \mathrm{R}\Gamma_{\widetilde{z}}(\widetilde{X}, \nu^\star j_\star\mathscr{L})$$

is a quasi-isomorphism.

Proof. Denote by $\eta_1, \dots, \eta_r$ the generic points of the strict henselisations of $\widetilde{X}$ at the preimages $z_1, \dots, z_r$ of z in $\widetilde{X}$. Denote by $\widetilde{X_z}$ the normalisation of the strict henselisation of X at z. The normalisation of U_z is

$$U_z \times_{X_z} \widetilde{X_z} = U \times_X (\widetilde{X}_{z_1} \sqcup \cdots \sqcup \widetilde{X}_{z_r}) = \eta_1 \sqcup \cdots \sqcup \eta_r$$

and since normalisation is birational, the map

$$\eta_1 \sqcup \cdots \sqcup \eta_r \longrightarrow U_z$$

is an isomorphism. Lemma 4.1 shows that it suffices to prove that

$$\mathrm{H}^2_z(X, j_\star\mathscr{L}) \longrightarrow \mathrm{H}^2_{\widetilde{z}}(\widetilde{X}, \nu^\star j_\star\mathscr{L}) = \mathrm{H}^2_{z_1}(\widetilde{X}, \nu^\star j_\star\mathscr{L}) \times \cdots \times \mathrm{H}^2_{z_r}(\widetilde{X}, \nu^\star j_\star\mathscr{L})$$

is an isomorphism. Let us compute $\mathrm{H}^2_z(X, j_\star\mathscr{L})$. By excision, there is a canonical isomorphism

$$\mathrm{H}^2_z(X, j_\star\mathscr{L}) \xrightarrow{\sim} \mathrm{H}^2_{z'}(X_z, g^\star j_!\mathscr{L}) = \mathrm{H}^2_{z'}(X_z, j'_!g'^\star\mathscr{L}).$$

The long exact sequence in cohomology with support on z' for the sheaf $j'_!g'^\star\mathscr{L}$ reads:

$$\mathrm{H}^1(X_z, j'_!g'^\star\mathscr{L}) \longrightarrow \mathrm{H}^1(U_z, g'^\star\mathscr{L}) \longrightarrow \mathrm{H}^2_{z'}(X_z, j'_!g'^\star\mathscr{L}) \longrightarrow \mathrm{H}^2(X_z, j'_!g'^\star\mathscr{L}).$$

Lemma 4.2 ensures that the map

$$\mathrm{H}^1(U_z, g'^\star\mathscr{L}) \longrightarrow \mathrm{H}^2_{z'}(X_z, j'_!g'^\star\mathscr{L})$$

is an isomorphism. Since the scheme U_z is the coproduct of the points $z'_1, \dots, z'_r$, the group $\mathrm{H}^1(U_z, g'^\star\mathscr{L})$ is simply $\mathrm{H}^1(z'_1, \mathscr{L}_{z'_1}) \times \cdots \times \mathrm{H}^1(z'_r, \mathscr{L}_{z'_r})$. On the other hand, for $t \in \{1 \dots r\}$, $\mathrm{H}^2_{z_t}(\widetilde{X}, \nu^\star j_\star\mathscr{L})$ is isomorphic to $\mathrm{H}^1(\eta_t, \mathscr{L}_{\eta_t})$, and the map

$$\mathrm{H}^1(z'_t, \mathscr{L}_{z'_t}) \longrightarrow \mathrm{H}^1(\eta_t, \mathscr{L}_{\eta_t})$$

is simply the isomorphism induced by $\eta_t \xrightarrow{\sim} z'_t$. □

Denote by K the function field of X, and by K^{sep} a separable closure of K.

Corollary 4.4. *For each point $z \in Z \times_X \widetilde{X}$, choose a place of K^{sep} above z and denote by I_z the corresponding inertia group. The one-term complex*

$$0 \longrightarrow 0 \longrightarrow \bigoplus_{z \in Z \times_X \tilde{X}} \mathrm{H}^1(I_z, M) \longrightarrow 0 \longrightarrow \cdots$$

represents $\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})$.

Proof. This is merely rephrasing Proposition 4.3 using the fact that only H^2_z is nonzero, which was proven in Lemma 4.1. □

4.2. Cohomology of constructible sheaves. Let k be an algebraically closed field. Let n be an integer invertible in k. Denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let X be an integral curve with multicross singularities over k. Denote by $\nu\colon \widetilde{X} \to X$ its normalisation. Let $\mathcal{F}^\bullet = [\mathcal{F}^0 \to \cdots \to \mathcal{F}^t]$ be a complex of constructible sheaves of Λ-modules on X. This section aims to give an explicit description of the cohomology complex $\mathrm{R}\Gamma(X, \mathcal{F})$.

Let $j\colon U \to X$ be the inclusion of a regular open affine subscheme of X on which every sheaf $\mathcal{F}^s$ is locally constant. Let $i\colon Z \to X$ be the inclusion of its closed complement with the reduced subscheme structure. Set $\mathscr{L}^\bullet \coloneqq j^\star\mathcal{F}^\bullet$, and $M^\bullet \coloneqq \mathscr{L}^\bullet_{\bar{\eta}}$. Let $V \to U$ be an étale Galois cover such that:

- each sheaf $\mathscr{L}^s|_V$, $s \in \{0, \dots, t\}$ is constant;
- each map $\mathrm{H}^1(U, \mathscr{L}^s) \to \mathrm{H}^1(V, \mathscr{L}^s|_V)$, $s \in \{0, \dots, t\}$ is trivial;
- the ramification index of $V \to U$ above every point of $\widetilde{X} - U$ is divisible by n.

Denote by G the group $\mathrm{Aut}(V|U)$. Let $\widetilde{Z}$ be the preimage of Z in $\widetilde{X}$. Given $\tilde{z} \in \widetilde{Z}$, denote by $I_{\tilde{z}} \subset G$ its inertia group, and by $P_{\tilde{z}} \triangleleft I_{\tilde{z}}$ its wild inertia subgroup. For each integer $s \in \{0, \dots, t\}$, let $\phi^s \colon \mathcal{F}^s \to j_\star \mathscr{L}^s$ be the adjunction unit. Denote by ∂_M the transition maps of the complex $M^\bullet$, by $\partial_{\mathcal{F}}$ those of $\mathcal{F}^\bullet$, and by ∂_G the coboundary maps in the cochain complex representing group cohomology with respect to the group G; in particular, given an element m in a G-module, $\partial_G(m)$ is the crossed homomorphism $g \mapsto g \cdot m - m$. The remainder of this section will be dedicated to the proof of the following result.

Theorem 4.5. *In this situation,* $\mathrm{R}\Gamma(X, \mathcal{F}^\bullet)[1] \in \mathrm{D}^b_c(\Lambda)$ *is represented by the cone of the following morphism of complexes, whose terms are indexed by* $s \geqslant 0$*:*

$$\begin{array}{c} \cdots \longrightarrow M^s \oplus \mathrm{Hom}_{\mathrm{cr}}(G, M^{s-1}) \oplus \bigoplus_{z \in Z} \mathcal{F}^s_z \oplus \bigoplus_{\tilde{z} \in \tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M^{s-2}_{P_{\tilde{z}}}) \longrightarrow \cdots \\ \downarrow \\ \cdots \longrightarrow \bigoplus_{\tilde{z} \in \tilde{Z}} \left(M^s \oplus \mathrm{Hom}_{\mathrm{cr}}(I_{\tilde{z}}/P_{\tilde{z}}, M^{s-1}_{P_{\tilde{z}}}) \oplus \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M^{s-2}_{P_{\tilde{z}}}) \right) \longrightarrow \cdots \end{array}$$

Here, $(a, b, c_z, d_{\tilde{z}})$ *is sent to* $(a - \phi_z(c), \mathrm{res}^{I_z}_G(b), d)$ *where* $z = \nu(\tilde{z})$ *and* $\mathrm{res}^{I_z}_G$ *denotes the composite map*

$$\mathrm{Hom}_{\mathrm{cr}}(G, M^s) \longrightarrow \mathrm{Hom}_{\mathrm{cr}}(I_z, M)^s \longrightarrow \mathrm{Hom}_{\mathrm{cr}}(I_z/P_z, M^s_{P_z})$$

defined in Lemma 2.8. Then the transition map of the top complex is $(a, b, c_z, d_{\tilde{z}}) \mapsto (\partial_M(a), \partial_M(b) + (-1)^s \partial_G(a), \partial_{\mathcal{F}}(c_z), \partial_M(d_{\tilde{z}}) + (-1)^s \mathrm{res}^{I_z}_G(b))$. *The transition map of the bottom complex is* $(a, b, c) \mapsto (\partial_M(a), \partial_M(b) + (-1)^s \partial_G(a), \partial_M(c) + (-1)^s \partial_G(b))$.

Corollary 4.6. *When computing the cohomology of a single constructible sheaf* $\mathcal{F}$ *on* X *with generic geometric fibre* M*, the complex* $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ *is the cone of the following morphism of complexes:*

$$\begin{array}{ccccc} (\bigoplus_{z \in Z} \mathcal{F}_z) \oplus M & \xrightarrow{(0, \partial_G)} & \mathrm{Hom}_{\mathrm{cr}}(G, M) & \xrightarrow{(\mathrm{res}^{I_{\tilde{z}}}_G)_{\tilde{z}}} & \bigoplus_{\tilde{z} \in \tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) \\ \downarrow{\scriptstyle ((\phi_z - \mathrm{id})_{\tilde{z} \to z})_z} & & \downarrow{\scriptstyle (\mathrm{res}^{I_{\tilde{z}}}_G)_{\tilde{z}}} & & \downarrow{\scriptstyle \mathrm{id}} \\ \bigoplus_{\tilde{z} \in \tilde{Z}} M & \xrightarrow{\partial_{I_z}} & \bigoplus_{\tilde{z} \in \tilde{Z}} \mathrm{Hom}_{\mathrm{cr}}(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) & \longrightarrow & \bigoplus_{\tilde{z} \in \tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) \end{array}$$

Proof of the theorem. The functors $j_\star, j^\star, i_\star, i^\star$ can be extended to the (non-derived) category of complexes of constructible sheaves on X. These functors will allow us to compute $\mathrm{R}\Gamma(X, \mathcal{F}^\bullet)$ in the following way: first consider a short exact sequence involving $\mathcal{F}^\bullet$ in this category of complexes of constructible sheaves on X, then compute the associated distinguished triangle in $\mathrm{D}^b_c(\Lambda)$.

Consider the following short exact sequence of complexes of constructible sheaves on X:

$$0 \longrightarrow \mathcal{F}^\bullet \longrightarrow j_\star\mathscr{L}^\bullet \oplus i_\star i^\star\mathcal{F}^\bullet \longrightarrow i_\star\mathcal{Q}^\bullet \longrightarrow 0$$

where $\mathcal{Q}^\bullet \coloneqq i^\star j_\star\mathscr{L}^\bullet$. Here, the first map is just the sum of the two adjunction maps $\mathcal{F}^\bullet \to j_\star j^\star\mathcal{F}^\bullet$ and $\mathcal{F}^\bullet \to i_\star i^\star\mathcal{F}^\bullet$, and the second map is the difference of the adjunction maps $j_\star\mathscr{L} \to i_\star i^\star j_\star\mathscr{L}$ and $i_\star i^\star\mathcal{F}^\bullet \to i_\star i^\star j_\star j^\star\mathcal{F}^\bullet$. The object $\mathrm{R}\Gamma(X,\mathcal{F}^\bullet)[1]$ of $\mathrm{D}^b_c(\Lambda)$ is the cone of the morphism

$$\mathrm{R}\Gamma(X, j_\star\mathscr{L}^\bullet) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathcal{F}^\bullet) \longrightarrow \mathrm{R}\Gamma(X, i_\star\mathcal{Q}^\bullet).$$

Computing $\mathbf{R\Gamma(}X, j_\star\mathscr{L}\mathbf{)}$**.** The following distinguished triangle in $\mathrm{D}^b_c(X,\Lambda)$ [17, 09XP]:

$$\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L}^\bullet) \longrightarrow \mathrm{R}\Gamma(X, j_\star\mathscr{L}^\bullet) \longrightarrow \mathrm{R}\Gamma(U, \mathscr{L}^\bullet) \xrightarrow{+1}$$

shows that $\mathrm{R}\Gamma(X, j_\star\mathscr{L}^\bullet)[1]$ is the cone of $\mathrm{R}\Gamma(U,\mathscr{L}^\bullet) \to \mathrm{R}\Gamma_Z(X, j_\star\mathscr{L}^\bullet)[1]$. Let us now turn to the computation of $\mathrm{R}\Gamma(U,\mathscr{L}^\bullet)$ and $\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L}^\bullet)$. According to Proposition 3.4, $\mathrm{R}\Gamma(U,\mathscr{L}^\bullet)$ is represented by the total complex associated to the double complex

$$\begin{array}{ccccccc}
\mathrm{Hom}_{\mathrm{cr}}(G, M^0) & \longrightarrow & \mathrm{Hom}_{\mathrm{cr}}(G, M^1) & \longrightarrow & \mathrm{Hom}_{\mathrm{cr}}(G, M^2) & \longrightarrow & \cdots \\
\uparrow & & \uparrow & & \uparrow & & \\
M^0 & \longrightarrow & M^1 & \longrightarrow & M^2 & \longrightarrow & \cdots
\end{array}$$

which is

$$M^0 \longrightarrow M^1 \oplus \mathrm{Hom}_{\mathrm{cr}}(G, M^0) \longrightarrow M^2 \oplus \mathrm{Hom}_{\mathrm{cr}}(G, M^1) \longrightarrow \cdots$$

For each integer $s \in \{0,\dots,t\}$, $\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L}^s)$ is represented by the one-term complex

$$\bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{H}^2_{\tilde{z}}(X, \nu^\star j_\star\mathscr{L}^s)[-2]$$

according to Lemma 4.1. By Corollary 4.4 and Proposition 2.7, $\mathrm{H}^2_{\tilde{z}}(X, \nu^\star j_\star\mathscr{L}^s) = \mathrm{H}^1(I_{\tilde{z}}, M^s) = \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M^s_{P_{\tilde{z}}})$. It follows that $\mathrm{R}\Gamma(X, j_\star\mathscr{L}^\bullet)$ is represented by the complex

$$\begin{aligned}
M^0 &\xrightarrow{(\partial^0_M, \partial^0_G)} M^1 \oplus \mathrm{Hom}_{\mathrm{cr}}(G, M^0) \\
&\xrightarrow{(\partial^1_M, \partial^0_G - \partial^0_M, \mathrm{res}^{I_{\tilde{z}}}_G)} M^2 \oplus \mathrm{Hom}_{\mathrm{cr}}(G, M^1) \oplus \bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}, M^0) \longrightarrow \cdots
\end{aligned}$$

Representing $\mathbf{R\Gamma(}X, i_\star i^\star \mathcal{F}^\bullet\mathbf{)}$**.** For all $s \in \{0, \dots, t\}$, $\mathrm{R\Gamma}(X, i_\star i^\star \mathcal{F}^s)$ is simply represented by the one-term complex $\mathrm{H}^0(Z, \mathcal{F}^s)[0]$. Therefore $\mathrm{R\Gamma}(X, i_\star i^\star \mathcal{F}^\bullet)$ is represented by the complex

$$\bigoplus_{z\in Z} \mathcal{F}^0_z \longrightarrow \bigoplus_{z\in Z} \mathcal{F}^1_z \longrightarrow \bigoplus_{z\in Z} \mathcal{F}^2_z \longrightarrow \cdots$$

whose differentials are those of $\mathcal{F}^\bullet$.

Representing $\mathbf{R\Gamma(}X, i_\star \mathcal{Q}^\bullet\mathbf{)}$**.** We know that

$$\mathrm{R\Gamma}(X, i_\star \mathcal{Q}^s) = \mathrm{R\Gamma}(X, i_\star i^\star j_\star \mathscr{L}^s)$$

is represented by the one-term complex $\bigoplus_{z\in\tilde{Z}} \mathrm{H}^0(I_z, M^s)$ concentrated in degree zero. However, in order to be able to express the map $\mathrm{R\Gamma}_Z(X, j_\star\mathscr{L}) \to \mathrm{R\Gamma}(X, i_\star \mathcal{Q}^s)$ as a morphism of complexes, we will write $\mathrm{R\Gamma}(X, i_\star \mathcal{Q}^s)$ as the following three-term complex:

$$\bigoplus_{\tilde{z}\in\tilde{Z}} M^s \longrightarrow \bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{Hom}_{\mathrm{cr}}(I_{\tilde{z}}/P_{\tilde{z}}, M^s_{P_{\tilde{z}}}) \longrightarrow \bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M^s_{P_{\tilde{z}}})$$

whose first differential is the one sending $(m^s_{\tilde{z}})_{\tilde{z}}$ to $(g_{\tilde{z}} \mapsto (g_{\tilde{z}} \cdot m^s_{\tilde{z}} - m^s_{\tilde{z}}))_{\tilde{z}}$, and the second one is the usual quotient map. By the same arguments as above, $\mathrm{R\Gamma}(X, i_\star \mathcal{Q}^\bullet)$ is thus represented by the complex

$$\begin{aligned}\bigoplus_{\tilde{z}\in\tilde{Z}} M^0 &\longrightarrow \bigoplus_{\tilde{z}\in\tilde{Z}} (M^1 \oplus \mathrm{Hom}_{\mathrm{cr}}(I_{\tilde{z}}/P_{\tilde{z}}, M^0_{P_{\tilde{z}}})) \\ &\longrightarrow \bigoplus_{\tilde{z}\in\tilde{Z}} (M^2 \oplus \mathrm{Hom}_{\mathrm{cr}}(I_{\tilde{z}}/P_{\tilde{z}}, M^1_{P_{\tilde{z}}}) \oplus \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M^0_{P_{\tilde{z}}})) \longrightarrow \cdots\end{aligned}$$

Putting everything together. We have now computed each term of the morphism of complexes

$$\mathrm{R\Gamma}(X, j_\star \mathscr{L}^\bullet) \oplus \mathrm{R\Gamma}(X, i_\star i^\star \mathcal{F}^\bullet) \longrightarrow \mathrm{R\Gamma}(X, i_\star \mathcal{Q}^\bullet)$$

whose cone is $\mathrm{R\Gamma}(X, \mathcal{F}^\bullet)$. The morphism itself is the difference of the two adjunction maps. □

Remark 4.7. *A cover $V \to U$ as in the theorem may be computed in the following way: consider an étale Galois cover $W \to U$ such that each $\mathscr{L}^i|_W$ is constant, and set $V = W^{\langle n\rangle}$. While $W^{\langle n\rangle}$ is the canonical choice, we may for complexity reasons choose any of its subcovers that still satisfy the three required properties listed above. Here is one example of such a subcover. The action of* $\mathrm{Gal}(k|k_0)$ *on* $\mathrm{H}^1(U, \mathscr{L}^\bullet)$ *factors through a finite quotient* $\mathrm{Gal}(k_1|k_0)$*. The image of* $\mathrm{H}^1(U, \mathscr{L}^\bullet)$ *in* $\mathrm{H}^1(W, \Lambda)$ *is still defined over k_1, and we may construct a Galois subcover of $W^{\langle n\rangle} \to U$ by taking n^{th} roots only of functions that are defined over k_1. This will be used in the case of finite fields in Section 5.6.*

4.3. Computing the Galois action. Let k_0 be a perfect field, let k be an algebraic closure of k_0 and $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$. Consider a curve X_0 over k_0. For the sake of simplicity, we consider a single sheaf $\mathcal{F}_0$ on X_0. The general case of complexes of sheaves is handled in the same way. Let $X = X_0 \times_{k_0} k$ and $\mathcal{F} = \mathcal{F}_0|_X$. This section is dedicated to the description of a complex of $\Lambda[\mathfrak{G}_0]$-modules representing $\mathrm{R}\Gamma(X, \mathcal{F})$. Let U_0 be an affine open subset of X_0 on which $\mathcal{F}$ is locally constant, and $W_0 \to U_0$ be a Galois cover such that $\mathcal{F}_0|_{W_0}$ is constant. Let Z_0 be the reduced closed complement of U_0 in X_0. Denote by U, W, Z their base changes to k. Consider the cover $V = W^{\langle n \rangle}$, and the complex representing $\mathrm{R}\Gamma(X, \mathcal{F})$ computed above using V.

The easy case: when W_0 has a rational point w_0. In that case, W is connected. The terms of $\mathrm{R}\Gamma(X, \mathcal{F})$ consist of cohomology groups of $G = \mathrm{Aut}(V|U)$ or I_z/P_z, where z is a closed point at infinity of U, with values in (a suitable quotient of) M. Understanding the action of $\mathfrak{G}_0$ on G is straightforward: let $\overline{w}$ be a geometric point of W whose image in W is w_0, let $\overline{u}$ be its image in U and $\overline{v}$ a preimage of $\overline{w}$ in $V = W^{\langle n \rangle}$. The group $\mathfrak{G}_0$ acts on $\pi_1(W, \overline{w}) \subset \pi_1(U, \overline{u})$ by functoriality, and since $W^{\langle n \rangle} \to W$ is characteristic, this action restricts to $\pi_1(V, \overline{v})$. Moreover, for $z \in X(k_0)$, the group $\mathfrak{G}_0$ acts naturally on I_z/P_z, which is canonically isomorphic to $\mu_e(k)$, where e is the ramification index of $V^{\langle n \rangle} \to U$ above z. Finally, the group M^{P_z} does not depend on the choice of preimage of Z in the compactification of $V^{\langle n \rangle}$. For a point z defined over an extension k_1 of k_0, we need to consider its Galois orbit T: then $\mathfrak{G}_0$ acts naturally on $\bigoplus_{t \in T} \mathrm{R}\Gamma(I_t/P_t, M^{P_t})$, where the preimages of t whose inertia groups we compute have been chosen in the same $\mathfrak{G}_0$-orbit. These considerations allow us to compute the action of $\mathfrak{G}_0$ on each of the terms of the complex representing $\mathrm{R}\Gamma(X, \mathcal{F})$.

The general case. In general, W need not be connected, and the function field $k_0(W_0)$ may contain a finite nontrivial Galois extension of k_0. Section 2.5 shows how to construct a Galois cover $V_0 \to U_0$ whose function field contains a sufficiently large Galois extension L of k_0 over which the elements of $\mathrm{H}^1(W, \mu_n)$ as well as the points at infinity of $V \coloneqq V_0 \times_{k_0} k$ are defined. This ensures that any closed point of the smooth compactification of V_0 above a point of Z_0 is exactly L. Consider a connected component V_c of V. The group $G_c \coloneqq \mathrm{Aut}(V_c|U) = \ker(\mathrm{Aut}(V_0|U_0) \to \mathrm{Gal}(L|k_0))$ is the stabiliser of V_c in $G \coloneqq \mathrm{Aut}(V_0|U_0)$. Set $M_0 = \mathrm{H}^0(V_0, \mathcal{F}_0)$ and $M = \mathrm{H}^0(V, \mathcal{F})$; then M is the induced representation $\mathrm{ind}_{G_c}^{G}(M_0)$, and Shapiro's lemma [15, Thm. 4.19] shows that the map

$$\tau_{\leqslant 1}\, \mathrm{R}\Gamma(G_c, M_0) \longrightarrow \tau_{\leqslant 1}\, \mathrm{R}\Gamma(G, M)$$

in $\mathrm{D}_c^b(\Lambda)$ is a quasi-isomorphism. As an abelian group, $M = M_0^d$ where d is the number of connected components of V. The group $\mathfrak{G}_0$ acts naturally on M as it does on set the connected components of V, in a way that is

compatible with its action on G. This allows to compute the action of $\mathfrak{G}_0$ on $\tau_{\leqslant 1}\mathrm{R}\Gamma(G,M)$. Let $z\in Z_0$ be a closed point with residue field k_1. Let v be a preimage of z in V_0. Denote by $T\coloneqq\{\tau(z),\tau\in\mathrm{Gal}(k_1|k_0)\}$ the $\mathfrak{G}_0$-orbit of z. For each $\tau\in\mathrm{Gal}(k_1|k_0)$, consider a preimage v_τ of $\tau(z)$ in V_0; we choose the v_τ to be in the same $\mathfrak{G}_0$-orbit. Let $D_\tau\triangleleft G$ be the decomposition group of v_τ. The map $D_\tau\to\mathrm{Gal}(L'|k_0)$ is surjective, and its kernel is the inertia group I_τ of v_τ, so that $M=\mathrm{ind}_{I_\tau}^{D_\tau}M_0$. Shapiro's lemma now ensures that

$$\mathrm{R}\Gamma(D_\tau,M)=\mathrm{R}\Gamma(I_\tau,M_0)=\mathrm{R}\Gamma(I_\tau/P_\tau,M_0^{P_\tau})$$

in $\mathrm{D}_c^b(\Lambda)$. The group $\mathfrak{G}_0$ acts naturally on the complex $\bigoplus_\tau\mathrm{R}\Gamma(D_\tau,M)$, whose cohomology groups are $\mathrm{H}^0(T,j_\star\mathcal{F}|_U)$ and $\mathrm{H}^2_T(X,j_\star\mathcal{F}|_U)$. Using these notations, $\mathrm{R}\Gamma(X,\mathcal{F})[1]$ is isomorphic in $\mathrm{D}_c^b(\Lambda[\mathfrak{G}_0])$ to the cone of the following morphism of complexes:

$$\begin{array}{ccccccccc}
0\to M\oplus\bigoplus_T\mathrm{H}^0(T,\mathcal{F}) & \xrightarrow{(\partial_G,0)} & \mathrm{Hom}_{\mathrm{cr}}(G,M) & \longrightarrow & \bigoplus_T\bigoplus_\tau\mathrm{H}^1(I_\tau/P_\tau,M_{P_\tau})\to 0\\
\downarrow{\scriptstyle\bigoplus_{T,\tau}(\mathrm{res}^G_{I_\tau}-\phi_z)} & & \downarrow{\scriptstyle\bigoplus_{T,\tau}\mathrm{res}^G_{I_\tau}} & & \downarrow{\scriptstyle\mathrm{id}}\\
0\longrightarrow\bigoplus_T\bigoplus_\tau M_{P_\tau} & \xrightarrow{\bigoplus_z\partial_{I_\tau}} & \bigoplus_T\bigoplus_\tau\mathrm{Hom}_{\mathrm{cr}}(I_\tau/P_\tau,M_{P_\tau}) & \to & \bigoplus_T\bigoplus_\tau\mathrm{H}^1(I_\tau/P_\tau,M_{P_\tau})\to 0
\end{array}$$

where T runs through the $\mathfrak{G}_0$-orbits in Z, and τ runs through the k_0-automorphisms of the residue field of the closed points of T.

4.4. Functoriality over $\mathrm{Spec}\,k$. Consider a morphism $\phi\colon X'\to X$ of integral curves over an algebraically closed field k. As usual, let n be an integer invertible in k, and denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let $\mathcal{F}$ be a constructible sheaf of Λ-modules on X. Here is how to compute a morphism of complexes of Λ-modules representing $\mathrm{R}\Gamma(X,\mathcal{F})\to\mathrm{R}\Gamma(X',\phi^\star\mathcal{F})$. Let U be an affine open subset of X on which $\mathcal{F}$ is locally constant. Let $W\to U$ be an étale Galois cover such that $\mathcal{F}|_W$ is constant, and $W'\to U'$ be the Galois closure of a connected component of $W\times_X X'$. Consider the Galois covers $V=W^{\langle n\rangle}\to W$ and $V'=(W')^{\langle n\rangle}\to W'$. Given the construction of V and V', the map $\mathrm{H}^1(W,\mu_n)\to\mathrm{H}^1(W',\mu_n)$ defines a map $V'\to V$.

By elementary Galois theory, there is a map $\mathrm{Aut}(V'|U')\subseteq\mathrm{Aut}(V'|U)\to\mathrm{Aut}(V|U)$. For each point $z\in X-U$, choose a preimage z_V of z in the smooth compactification of V. For each preimage z' of z in X', consider a preimage z'_V of z' in the smooth compactification of V' whose image in V is z_V. Consider the inertia groups $P_V\triangleleft I_V\subseteq\mathrm{Aut}(V|U)$ of z_V and $P_{V'}\triangleleft I_{V'}\subseteq\mathrm{Aut}(V'|U')$ of z'_V. The map $\mathrm{Aut}(V'|U')\to\mathrm{Aut}(V|U)$ induces for each choice of z,z',z_V,z'_V a map $I_{V'}/P_{V'}\to I_V/P_V$. The functoriality of the bar resolution thus allows to compute the maps $\mathrm{R}\Gamma(\mathrm{Aut}(V'|U'),M)\to\mathrm{R}\Gamma(\mathrm{Aut}(V|U),M)$ and $\mathrm{R}\Gamma(I_V/P_V,M^{P_V})\to\mathrm{R}\Gamma(I_{V'}/P_{V'},M^{P_{V'}})$ that are needed to compute the morphism of complexes representing $\mathrm{R}\Gamma(X,\mathcal{F})\to\mathrm{R}\Gamma(X',\phi^\star\mathcal{F})$.

4.5. Cohomology of curves over a field of cohomological dimension 1. Consider a perfect field k_0 of cohomological dimension 1 such that $\mathrm{H}^1(k_0, \mathbb{Z}/n\mathbb{Z})$ is finite, e.g. a finite field or the fraction field of a strictly henselian local DVR. Let n be an integer invertible in k_0. Denote by Λ the ring $\mathbb{Z}/n\mathbb{Z}$. Let X_0 be an integral curve over k_0, and $\mathcal{F}_0^\bullet$ be a complex of constructible sheaves of Λ-modules on X_0. Denote by k the algebraic closure of k_0, by $\mathfrak{G}_0$ the Galois group $\mathrm{Gal}(k|k_0)$ and by $X, \mathcal{F}$ the respective base changes of $X_0, \mathcal{F}_0$ to k. Theorem 4.5 shows how to compute a complex $M^\bullet$ of $\mathfrak{G}_0$-modules representing $\mathrm{R}\Gamma(X, \mathcal{F}^\bullet)$. Recall that

$$\mathrm{R}\Gamma(X_0, \mathcal{F}_0^\bullet) = \mathrm{R}\Gamma(\mathfrak{G}_0, \mathrm{R}\Gamma(X, \mathcal{F}^\bullet)).$$

We described in Section 3 how to determine a complex representing this object. Let k_1 be a Galois extension of k such that the action of $\mathfrak{G}_0$ on $\mathrm{R}\Gamma(X, \mathcal{F}^\bullet)$ factors through $\mathrm{Gal}(k_1|k_0)$. Consider the extension $k_1^{\langle n \rangle}$ of k_0 with Galois group $\mathrm{H}^1(k_1, \Lambda)^\vee$, and the Galois group $G = \mathrm{Gal}(k_1^{\langle n \rangle}|k_0)$. Then $\mathrm{R}\Gamma(X_0, \mathcal{F}_0)$ is represented by the total complex associated to the double complex $B^{i,j} = \mathrm{Hom}_{\Lambda[G]}(\tau_{\geqslant -1} P_G^{-j}(\Lambda), M^i)$, where P_G is the usual projective resolution of Λ as a $\Lambda[G]$-module.

Remark 4.8. *The same method also applies in theory to the general case where* $\mathrm{H}^1(k_0, \Lambda)$ *is infinite, using continuous group cohomology and* $\Lambda[\![G]\!]$*-modules; one particularly interesting case to consider would be when* k_0 *is the function field of a curve over an algebraically closed field. However, to go any further in practical computations, one is quickly confronted with the issue of computing a generating set of* $\mathrm{H}^1(k_0, \mathbb{Z}/n\mathbb{Z}) \simeq k_0^\times/(k_0^\times)^n$.

5. Algorithmic aspects

In this whole section, n is a positive integer and Λ denotes the ring $\mathbb{Z}/n\mathbb{Z}$.

5.1. Representing curves and sheaves.

Representing curves. A smooth projective curve over a field k_0 is defined by a (possibly singular) plane model given by a polynomial in two variables. When working with a closed subscheme of a smooth curve, we may always suppose that its image in the plane model is nonsingular. Such a closed subscheme is defined by equations; an open subscheme is defined by its closed complement. A morphism of smooth curves is given by a morphism of plane models, i.e. by two polynomials in two variables. The only time we need to work with rational points is when considering the geometric points in a given closed subscheme Z_0 of the curve; in that case, we may replace k_0 with a finite extension over which these points are defined. This extension has degree bounded by the number r of geometric points in Z_0, and passing to this extension has no impact on the complexity estimates

given below, which are all at least polynomial in r. A curve X with multicross singularities is defined by its normalisation $\widetilde{X}$, as well as the subsets of points of $\widetilde{X}$ that have the same singular image in X; again, we suppose that these subsets of $\widetilde{X}$ have a nonsingular image in the plane model.

Representing sheaves. Let X be a smooth curve over an algebraically closed field k of characteristic prime to n. A constructible sheaf of Λ-modules on the étale site of X will be described by the following gluing data, which defines it uniquely [13, II, Thm. 3.10]:

- a closed 0-dimensional subscheme Z of X, defined by an equation;
- a finite locally constant sheaf $\mathscr{L}$ on the open complement U of Z, defined by a Galois cover $V \to U$ and the action of the group $G = \mathrm{Aut}(V|U)$ on the Λ-module $M = \mathrm{H}^0(V, \mathscr{L})$;
- for each point $z \in Z$, the Λ-module $\mathcal{F}_z$ defined by generators and relations;
- for each point $z \in Z$, the gluing morphism $\phi_z \colon \mathcal{F}_z \to (j_\star \mathscr{L})_z = \mathrm{H}^0(I_z, M)$, where $I_z \subset G$ is the stabiliser of a preimage of z in V.

This data also allows to represent morphisms and direct sums of sheaves in a very straightforward manner, as well as to compute tensors products and Hom-sheaves; see [10, §III.4] for more details. While this representation of constructible sheaves might not be the first that comes to mind, it is well suited to our computation of cohomology groups. The usual ways of defining constructible sheaves (as cokernel of $f_!\Lambda \to g_!\Lambda$ with f, g étale or kernel of $f_\star\Lambda \to g_\star\Lambda$ with f, g finite) also admit an algorithmic representation, which can be converted into this one (see [10, §III.3]).

5.2. Computing the cohomology of $\boldsymbol{\mu_n}$: existing algorithms. Our methods rely on existing algorithms which, given a smooth integral curve X over an algebraically closed field k of characteristic prime to n, compute $\mathrm{H}^1(X, \mu_n)$. Recall that we need to be able to compute it even for affine curves, which can prove to be a bit trickier than in the projective case.

The most efficient algorithm computing $\mathrm{H}^1(X, \mu_n)$, developed by Couveignes, only applies to projective curves over finite fields, and actually requires prior knowledge of the characteristic polynomial of the Frobenius endomorphism of X; since it makes use of some properties of the Frobenius and the group structure of $\mathrm{Pic}^0(X)[n]$, adapting it to the cohomology of affine curves, or of curves over other types of fields does not seem easy. Given a curve of genus g over $\mathbb{F}_q$, described by an ordinary plane model of degree d, it computes $\mathrm{Pic}^0(X)(\mathbb{F}_q)[n]$ in time polynomial in $d, g, \log q, n$ [1, Thm. 1].

While it was also first described only for projective curves over finite fields, Huang and Ierardi's method [8] applies to more general settings.

Their algorithm constructs an affine scheme whose points correspond to divisors D such that nD is the divisor of a rational function, and then finds a point in each irreducible component of this scheme, which is enough to find a representative of every n-torsion class in $\mathrm{Pic}^0(X)$. This strategy readily adapts to the computation of division by n in $\mathrm{Pic}^0(X)$, thus allowing to compute the cohomology of μ_n on an open subset of X. It is also independent of the chosen base field. The complexity of their algorithm, computed when the base field is $\mathbb{F}_q$, is polynomial in $n^g, n^d, \log q$ [10, Prop. 4.3.3].

In the remainder of this article, we will denote by $\mathsf{H1Const}(k_0, n, d, g, r)$ or simply $\mathsf{H1Const}(X, n)$ the complexity of the computation of $\mathrm{H}^1(X, \mu_n)$, where X is a smooth integral curve of genus g over k, given by a degree d polynomial in $k_0[x, y]$, with r points at infinity. We will also denote by $\mathsf{Root}(\mathsf{k_0}, \mathsf{n}, \mathsf{d})$ the complexity of computing an n^{th} root of an element in a degree d extension of k_0.

5.3. Computing in $\mathbf{H^1}(\boldsymbol{X}, \boldsymbol{\mu_n})$. Let U be a smooth integral curve over an algebraically closed field k of characteristic prime to n. Let X be the smooth compactification of U. Let n be an integer invertible in k, and Λ be the ring $\mathbb{Z}/n\mathbb{Z}$. Denote by $P_0, \ldots, P_r$ the points of $X - U$. Recall that the elements of $\mathrm{H}^1(U, \mu_n)$ are equivalence classes $[D, f]$ of pairs where f is a rational function on U such that $\mathrm{div}_U(f) = nD$. The class $[D, f]$ is trivial in $\mathrm{H}^1(U, \mu_n)$ precisely when f is an n^{th} power. The sum $[D, f] + [D', f']$ is defined by $[D + D', ff']$.

Here is how to compute the coordinates of an element of $\mathrm{H}^1(U, \mu_n)$ in a given basis using the Weil pairing, as is done in the projective case in [1, §8]. The Weil pairing

$$e_n \colon \mathrm{H}^1(U, \mu_n) \times \mathrm{H}^1_c(U, \mu_n) \longrightarrow \mu_n$$

is nondegenerate. In this context,

$$\mathrm{H}^1_c(U, \mu_n) = \frac{\{(D, f) \in \mathrm{Div}(U) \times k(X)^\times \mid nD = \mathrm{div}(f), f(P_0) = \cdots = f(P_r) = 1\}}{\{(D, f^n) \text{ where } f(P_0) = \cdots = f(P_r) = 1\}}$$

sits in the short exact sequence

$$0 \longrightarrow \frac{\mu_n(k)^r}{\mu_n(k)} \longrightarrow \mathrm{H}^1_c(U, \mu_n) \longrightarrow \mathrm{H}^1(X, \mu_n) \longrightarrow 0$$

and may be computed in the following way. Choose a primitive n^{th} root of unity $\zeta \in k$. For each $i \in \{1 \ldots r\}$, consider a function $g_i \in k(X)$ such that $g_i(P_0) = \zeta^{-1}$, $g_i(P_i) = \zeta$, and $g_i(P_j) = 1$ for all $j \neq 0, i$. Then $([\mathrm{div}(g_1), g_1^n], \ldots, [\mathrm{div}(g_r, g_r^n])$ is a basis of the image of $\mu_n(k)^r/\mu_n(k)$ in $\mathrm{H}^1_c(U, \mu_n)$. The Weil pairing is computed as usual: given $v = [D, f] \in$

$\mathrm{H}^1(U,\mu_n)$ and $w = [E,g] \in \mathrm{H}^1_c(U,\mu_n)$ where f and g are suitably normalised,

$$e_n(v,w) = \frac{f(E)}{g(D)}.$$

Algorithm 1: CoordinatesInBasis

Data: Smooth integral curve U over alg. closed field k, smooth compactification X of U
The points $P_0,\dots,P_r$ of $X-U$
Positive integer n invertible in k
Basis $B = (v_1,\dots,v_{2g+r})$ of $\mathrm{H}^1(U,\mu_n)$, where
$v_i = (D_i, f_i) \in \mathrm{Div}(U) \times K^\times$ and $([v_1],\dots,[v_{2g}])$ is a basis of $\mathrm{H}^1(X,\mu_n)$
Element $v_0 \in \mathrm{H}^1(U,\mu_n)$ represented by $(D_0,f_0) \in \mathrm{Div}(U)\times K^\times$
Primitive n^{th} root of unity $\zeta \in k$
Result: Coordinates $(\alpha_1,\dots,\alpha_{2g+r}) \in \Lambda^{2g+r}$ of v w.r.t. B
Function $h \in k(X)^\times$ such that $f = h^n f_1^{\alpha_1}\dots f_{2g+r}^{\alpha_{2g+r}}$

---

for $i \in \{1\dots r\}$ **do**
  Compute function f_i such that $f_i(P_0) = \zeta^{-1}$, $f_i(P_i) = \zeta$, and $f_i(P_j) = 1$ for $j \neq 0, i$
  Set $v_{1-i} := (\mathrm{div}(g_i), g_i^n)$
end
Compute matrix $M = e_n(v_i,v_j)_{0\leqslant i\leqslant 2g+r,\,1-r\leqslant i\leqslant 2g} \in \mathrm{Mat}_{(2g+r+1)\times(2g+r)}(\mu_n(k))$
Compute an element $(1,-\alpha_1,\dots,-\alpha_{2g}) \in \ker(M)$: then $v_0 = \sum_i \alpha_i v_i$ in $\mathrm{H}^1(U,\mu_n)$
Compute Riemann–Roch space L of $D_0 - \sum_i \alpha_i D_i$
Pick $h \in L$: then $D_0 - \sum_i \alpha_i D_i = \mathrm{div}(h^{-1})$
Compute n^{th} root $c \in k$ of $f_0 h^n \prod_i f_i^{-\alpha_i} \in k$
return $\alpha_1,\dots,\alpha_{2g+r} \in \Lambda$ and function $ch \in k(X)^\times$

Lemma 5.1. *Suppose all of the divisors $D_0,\dots,D_{2g+r}$ are given as difference of two effective divisors of degree $\leqslant m$, and the curve X is given by a plane model of degree d. This algorithm returns the coordinates of v in time* $\mathrm{Poly}(d,m,g,r) + \mathsf{Root}\left(k_0, n, n^{(2g+r)^2}\right)$.

Proof. Computing the functions f_i using Lagrange interpolation, as well as the matrix M using the definition above, is straightforward. The kernel of M is computed using standard linear algebra techniques over Λ (using the isomorphism $\mu_n(k) \to \Lambda$ given by $\zeta \mapsto 1$), which run in polynomial time in the size of M. □

5.4. Construction of $V^{\langle n\rangle}$. Let k be an algebraically closed field of characteristic prime to n. Let X be an integral smooth projective curve over k, and U an affine open subscheme of X. Let V be an étale Galois cover of U. The following algorithm computes the cover $V^{\langle n\rangle} \to V$ defined in Section 2.1, as well as the group $\mathrm{Aut}(V^{\langle n\rangle}|U)$.

Algorithm 2: nTorsCover

Data: Galois cover $V \to U$ of smooth integral curves over alg. closed field k
Generating set S of $\mathrm{Aut}(V|U)$
Integer n invertible in k
Result: Generating set of $\mathrm{Aut}(V^{\langle n\rangle}|U)$

Compute basis $[D_i, f_i]_{1\leqslant i\leqslant s}$ of $\mathrm{H}^1(V, \mu_n)$ (see Section 5.2)
for $\sigma \in S$ **do**
  for $i \in \{1 \dots s\}$ **do**
    Compute $\sigma^\star(D_i, f_i)$
    Compute $h, \alpha_1, \dots, \alpha_s$ such that $\sigma^\star f_i = h_i^n f_1^{\alpha_1} \dots f_s^{\alpha_s}$ using Algorithm 1
  end
  Define $\rho_\sigma \colon (x, y) \mapsto \sigma(x, y), z_j \mapsto h_j z_1^{\alpha_1} \dots z_s^{\alpha_s}$
end
for $i \in \{1 \dots s\}$ **do**
  Define $\phi_i \colon (x, y) \mapsto (x, y), z_i \mapsto \zeta z_i, (z_j)_{j\neq i} \mapsto (z_j)_{j\neq i}$
end
return $\{\rho_\sigma\}_{\sigma\in S} \cup \{\phi_i\}_{1\leqslant i\leqslant s}$

Proposition 5.2. *If U has r points at infinity and V is given by an ordinary plane model of degree d, Algorithm 2 computes a generating set of* $\mathrm{Aut}(V^{\langle n\rangle}|U)$ *in*

$$\mathsf{H1Const}(k_0, n, d, (2g + r)[V : U], r[V : U])$$

elementary operations.

Proof. The genus of V is bounded by $(2g + r)[V : U]$. The complexity of computing the coordinates of the pullback of the divisors is polynomial-time in $n, [V : U](2g + r), d$, hence dominated by that of computing a basis of $\mathrm{H}^1(V, \mu_n)$. □

Here is how, once $G^{\langle n\rangle} = \mathrm{Aut}(V^{\langle n\rangle} \to U)$ has been computed, to compute the preimages of points of X in the smooth compactification of $V^{\langle n\rangle}$, as well as their inertia group. This is done by considering a suitable explicit model of $V^{\langle n\rangle}$. Recall that the function field of $V^{\langle n\rangle}$ is obtained from that of V by adjoining n^{th} roots of functions $f_1, \dots, f_t \in k(V)$. Write $f_i = \frac{g_i}{h_i}$, where

$g_i, h_i \in k[x,y]$. Denote by Z (resp. W, resp. $W^{\langle n\rangle}$) the sets of points at infinity of U (resp. V, resp. $V^{\langle n\rangle}$). Consider a point $z \in Z$, and a preimage w of z in W. Replacing f_i with $h_i^n f_i$ if necessary, we may suppose $h_i(w) \neq 0$. Then the affine curve given by the equation of V and $h_i z_i^n - g_i$ contains n^{t-1} preimages of w, which are nonsingular. Given one of these preimages w, the inertia subgroup I_w can be computed simply by evaluating the elements of $G^{\langle n\rangle}$ at w.

Algorithm 3: InertiaGroup

Data: Galois cover $V \to U$ of smooth integral curves over alg. closed field k, with smooth compactification $Y \to X$ Integer n invertible in k
Group $\mathrm{Aut}(V^{\langle n\rangle}|U)$ and basis $(D_i, f_i = \frac{g_i}{h_i})_{1\leqslant i\leqslant s}$ of $\mathrm{H}^1(V, \mu_n)$
Point z in compactification of U, preimage w of z in compactification of V
Result: Preimage $w^{\langle n\rangle}$ of w in compactification of $V^{\langle n\rangle}$
Generating set of inertia group $I^{\langle n\rangle} \subset \mathrm{Aut}(V^{\langle n\rangle}|U)$ of $w^{\langle n\rangle}$

---

for $i \in \{1 \dots s\}$ **do**
  if $h_i(w) = 0$ **then**
    $g_i \leftarrow h_i^{n-1} g_i, h_i \leftarrow 1$
  end
  Compute root t_i of $h_i(z)T^n - g_i(z) \in k[T]$
end
Set $w^{\langle n\rangle} = (w, t_1, \dots, t_s) \in \operatorname{Spec} Y[z_1, \dots, z_n]/(h_i z_i^n - g_i)$
$I^{\langle n\rangle} \coloneqq \{\sigma \in G^{\langle n\rangle} \mid \sigma(w^{\langle n\rangle}) = w^{\langle n\rangle}\}$
return $w^{\langle n\rangle}, I^{\langle n\rangle}$

Lemma 5.3. *Algorithm 3 returns a preimage $w^{\langle n\rangle}$ of w in the smooth compactification of $V^{\langle n\rangle}$ and its stabiliser in*

$$[V:U]\left((n^{2g+r} + (2g+r)\mathsf{Root}\left(k_0, n, n^{([V:U](2g+r))^2}\right)\right)$$

elementary operations.

Proof. Computing $w^{\langle n\rangle}$ requires $[V:U](2g+r)$ computations of n^{th} roots in k. Computing $I^{\langle n\rangle}$ requires $[V:U]n^{2g+r}$ function evaluations. □

5.5. Computation of RΓ. Let k_0 be a perfect field of characteristic prime to n, and k be an algebraic closure of k_0. Let X_0 be an integral curve over k_0 with ordinary singularities, and $X = X_0 \times_{k_0} k$. Consider a complex $\mathcal{F}_0^\bullet = [\mathcal{F}_0^0 \to \dots \to \mathcal{F}_0^t]$ of constructible sheaves of $\mathbb{Z}/n\mathbb{Z}$-modules on X_0, and set $\mathcal{F}^\bullet \coloneqq (\mathcal{F}_0)^\bullet|_X$. Let U be a smooth open affine subscheme of X such that $\mathcal{F}^\bullet|_U$ is a complex of locally constant sheaves. Let r be the number of points of $X - U$. Let $V \to U$ be an étale Galois cover such

that, for each integer $i \in \{0 \dots t\}$, the sheaf $\mathcal{F}^i|_U$ is constant. Denote by G the automorphism group of $V \to U$. The following algorithm computes the cohomology complex $\mathrm{R}\Gamma(X, \mathcal{F}^\bullet)$ described in Theorem 4.5.

Algorithm 4: RGamma

Data: Integral curve X over alg. closed field k
Integer n invertible in k
Constructible sheaf complex $\mathcal{F}^\bullet$ on X as described in Section 5.1:
affine open $U \subset X$ where each $\mathcal{F}^i$ is locally constant,
Galois cover $V \to U$ which trivialises $\mathscr{L}^\bullet := \mathcal{F}^\bullet|_U$,
Galois group $\mathrm{Aut}(V|U)$ and inertia subgroups $I_z \subset G$ for $z \in X - U$,
generic fibres M^i of $\mathcal{F}^i$ with action of $\mathrm{Aut}(V|U)$,
fibres $\mathcal{F}^i_z$ for $z \in X - U$,
adjunction units $\phi^i_z \colon \mathcal{F}^i_z \to (M^i)^{I_z}$.
Result: Complex of Λ-modules representing $\mathrm{R}\Gamma(X, \mathcal{F})$

Compute $\mathrm{Aut}(V^{\langle n \rangle}|U)$ using Algorithm 2
Compute inertia subgroups $I'_z \subset \mathrm{Aut}(V^{\langle n \rangle}|U)$ using Algorithm 3
Using linear algebra, compute $\mathrm{Hom}_{\mathrm{cr}}(\mathrm{Aut}(V^{\langle n \rangle}|U), M^i)$ and $\mathrm{Hom}_{\mathrm{cr}}(I'_z, M^i)$ for $z \in X - U$
Compute the morphism $\Psi \colon \mathrm{R}\Gamma(X, i_\star i^\star \mathcal{F}^\bullet) \oplus \mathrm{R}\Gamma(X, j_\star \mathscr{L}^\bullet) \to \mathrm{R}\Gamma(X, i_\star i^\star j_\star \mathscr{L}^\bullet)$ of Theorem 4.5
return $\mathrm{Cone}(\Psi)[-1]$

Theorem 5.4. *Let m be an integer such that M and the fibres $\mathcal{F}^i_z$, $z \in Z$, $i \in \{0 \dots t\}$ are given by at most m generators. Denote by d the degree of an ordinary plane model of V. Algorithm 4 computes a complex of Λ-modules representing $\mathrm{R}\Gamma(X, \mathcal{F})$ in*

$$\mathsf{H1const}(k_0, n, d, [V:U](2g+r)) + \mathrm{Poly}\left((n^{[V:U](2g+r))^2}, m, t\right) + [V:U](2g+r)\mathsf{Root}\left(k_0, n, n^{([V:U](2g+r))^2}\right)$$

elementary operations. When $k_0 = \mathbb{F}_q$, this number is bounded by

$$\mathrm{Poly}\left(n^{([V:U](2g+r))^2}, n^d, m, \log q, t\right).$$

Proof. This is just putting together the complexities of the previous algorithms, taking into account that the computation of modules of crossed homomorphisms is done using linear algebra over Λ. In order to bound the number in the case of a finite field, we use the complexity of Huang and Ierardi's algorithm to compute $\mathrm{H}^0(V, \mu_n)$. □

Remark 5.5. *The only existing algorithm computing* $\mathrm{H}^1(X,\mathcal{F})$ *when* $\mathcal{F}$ *is locally constant is Jin's algorithm; its complexity is exponential in* $|M|^{\log|M|}$ [9, Thm. 1.2]*, to which the complexity of our algorithm compares favourably.*

5.6. Improving complexity when k_0 is finite. Here we consider the case where $k_0=\mathbb{F}_q$ is a finite field, X_0 is a smooth curve over k_0, and $\mathcal{F}_0$ is a constructible sheaf of $\mathbb{F}_\ell$-vector spaces on X_0, where ℓ is a prime not dividing q. Let U_0 be an open subset of X_0 on which $\mathcal{F}_0$ is locally constant. Denote by $V_0\to U_0$ an étale Galois cover such that $\mathcal{F}_0|_{V_0}$ is constant with fibre M. For simplicity, we assume V_0 to be geometrically connected; if it were not, the field extension $\mathbb{F}_Q$ defined below should be replaced by its compositum with the field extension defined in Section 2.5. Write $m=\dim_{\mathbb{F}_\ell}(M)$. Denote by $k=\overline{\mathbb{F}_q}$ an algebraic closure of k_0, and by X,U,V the base changes of X_0,U_0,V_0 to k. Denote by g_X the genus of X and by r the number of points of $X-U$.

Lemma 5.6. *Set* $D=|\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)|$ *and* $Q=q^D$*. Consider a basis* $(D_1,f_1),\dots,(D_s,f_s)$ *of the* $\mathbb{F}_\ell$*-vector space* $\mathrm{H}^1(V,\mu_\ell)(\mathbb{F}_Q)$*, that is, the subspace of elements of* $\mathrm{H}^1(V,\mu_\ell)$ *invariant under the action of* $\mathrm{Gal}(k|\mathbb{F}_Q)$*. Denote by* $V_D^{\langle\ell\rangle}$ *the étale Galois cover of* V *defined by the function field extension* $k(V)(\sqrt[\ell]{f_1},\dots,\sqrt[\ell]{f_s})$*. The map* $\mathrm{H}^1(U,\mathcal{F}|_U)\to\mathrm{H}^1(V_D^{\langle\ell\rangle},\mathcal{F}|_{V_D^{\langle\ell\rangle}})$ *is trivial.*

Proof. We know that the action of $\mathrm{Gal}(k|k_0)$ factors through a finite quotient $\mathrm{Gal}(k_1|k_0)$, where $[k_1:k_0]$ divides $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{H}^1(U,\mathcal{F}))$. Recall the prime-to-$p$ fundamental group of U is generated by at most $2g+r$ elements. Now $\mathrm{H}^1(U,\mathcal{F})$ is a quotient of $\mathrm{Hom}_{\mathrm{cr}}(\pi_1(U)^{(p')},M)$; its dimension as an $\mathbb{F}_\ell$-vector space is bounded above by $m(2g_X+r)$. Therefore, $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{H}^1(U,\mathcal{F}))$ injects into $\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)$. Note that since ℓ divides $Q-1$, the field $\mathbb{F}_Q$ contains a primitive ℓ^{th} root of unity ζ, and the isomorphism $\mathrm{H}^1(V,\mathbb{F}_\ell)\to\mathrm{H}^1(V,\mu_\ell)$ defined by $1\mapsto\zeta$ is $\mathrm{Gal}(k|\mathbb{F}_Q)$-equivariant. Since the U-automorphisms of V are defined over $\mathbb{F}_q$, the set $\mathrm{H}^1(V,\mu_\ell)(\mathbb{F}_Q)$ is stable under the action of $\mathrm{Aut}(V|U)$, and $V'\to U$ is still Galois. The construction of $V_D^{\langle\ell\rangle}$ ensures that $\mathrm{H}^1(V,\mathbb{F}_\ell)(\mathbb{F}_Q)\to\mathrm{H}^1(V_D^{\langle\ell\rangle},\mathbb{F}_\ell)$ is trivial. The m copies of $\mathcal{F}|_V\simeq\mathbb{F}_\ell^m$ being stable under the action of $\mathrm{Gal}(k|k_0)$, the map

$$\mathrm{H}^1(U,\mathcal{F})\longrightarrow\mathrm{H}^1(V_D^{\langle\ell\rangle},\mathcal{F})\xrightarrow{\sim}\mathrm{H}^1(V_D^{\langle\ell\rangle},\mathbb{F}_\ell)^m$$

factors through $\mathrm{H}^1(V,\mathbb{F}_\ell)(\mathbb{F}_Q)^m$, and is also trivial. □

Hence, we may use $V_D^{\langle\ell\rangle}$ instead of $V^{\langle\ell\rangle}$ in Algorithm 4. Note that $D\leqslant\ell^{(m(2g+r))^2}$.

Computing $\mathbf{H^1(V,\mathbb{F}_\ell)(\mathbb{F}_Q)}$**.** This group is isomorphic to $\mathrm{H}^1(V,\mu_\ell)(\mathbb{F}_Q)$. Denote by $\overline{V}$ the smooth projective curve containing V, and by $J_{\overline{V}}$ its Jacobian. Consider a basis $(D_i,f_i)_{1\leqslant i\leqslant s}$ of $\mathrm{H}^1(V,\mu_\ell)(\mathbb{F}_Q)$. Here, the D_i are divisors on V such that $\ell D_i=\mathrm{div}_V(f_i)$. The proof of Lemma 2.4 tells us that we may assume some of these pairs to form a basis of $J_{\overline{V}}[\ell](\mathbb{F}_Q)$. For the remaining ones, the elements $M_i\coloneqq \ell D_i-\mathrm{div}_{\overline{V}}(f_i)$ form a basis of the space of $\mathrm{Gal}(k|\mathbb{F}_Q)$-invariant elements of the kernel of the following map.

$$\begin{aligned}\mathrm{H}^0(\overline{V}-V,\mathbb{F}_\ell)&\longrightarrow \mathbb{F}_\ell\\ (\lambda_P)_{P\in\overline{V}-V}&\longmapsto \sum_P \lambda_P\end{aligned}$$

Finding the D_i amounts to dividing the M_i by ℓ in $J_{\overline{V}}$. Here is how to do this. Any element of $J(\mathbb{F}_Q)$ has order dividing $Q-1$. Write $Q-1=\ell^\alpha s$ with s prime to ℓ. Then $sM_i\in J[\ell^\alpha](\mathbb{F}_Q)$, and we may find in $J[\ell^{\alpha+1}](\mathbb{F}_Q)$ an element E_i such that $\ell E_i=sM_i$: to do this, compute $J[\ell^{\alpha+1}](\mathbb{F}_Q)$ and use linear algebra. Actually, given the definition of α, $J[\ell^{\alpha+1}](\mathbb{F}_Q)=J[\ell^\alpha](\mathbb{F}_Q)$. Considering integers u,v such that $u\ell+vs=1$, we have $M_i=\ell\cdot(uM_i+vE_i)$.

Complexity. Since $Q=q^D$ where $D=|\mathrm{GL}_{m(2g_X+r)}(\mathbb{F}_\ell)|$, the integers α and s can be computed easily. As soon as $q^{\ell-1}\neq 1 \mod \ell^2$, we know $q^{\ell-1}$ has order $\ell^{\alpha-1}$ in $(\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times$ and

$$\alpha-1\leqslant v_\ell(D)=\frac{(m(2g_X+r))(m(2g_X+r)-1)}{2}$$

which is polynomial in m,g_X,r. The complexity of computing $\mathrm{H}^1(V,\mu_\ell)(\mathbb{F}_Q)$ is dominated by the computation of $J[\ell^\alpha](\mathbb{F}_Q)$. Couveignes' algorithm computes $J[\ell^\alpha](\mathbb{F}_Q)$ in time polynomial in ℓ^α, the genus of $\overline{V}$ and $\log(Q)$, assuming the characteristic polynomial of the Q-Frobenius on V is known.

5.7. Potential application: point counting on surfaces. Let X_0 be a smooth projective surface over a finite field $k_0=\mathbb{F}_q$. Denote by k an algebraic closure of k_0, and set $X=X_0\times_{k_0}k$. Consider the problem of computing $|X(k_0)|$. The usual approach, as in Schoof's algorithm, is to compute this number modulo ℓ for enough primes ℓ up to $O(\log q)$.

The Lefschetz theorem reduces this question to computing the trace of the Frobenius on $\mathrm{H}^i(X,\mathbb{F}_\ell)$. The classical way of computing these groups, as in [13, §V.3], is by using a Lefschetz pencil, which yields a fibration $\pi\colon\widetilde{X}\to\mathbb{P}^1$, where $\widetilde{X}$ is a blowup of X at a finite number of points. Edixhoven conjectured in [3, Epilogue] that this strategy might allow us to compute $|X(k_0)|$ in time polynomial in $\log(q)$. Here is where we stand on this conjecture. The sheaf $\mathcal{F}\coloneqq \mathrm{R}^1\pi_\star\mathbb{F}_\ell$ is a constructible sheaf on the projective line. It is locally constant on the open subset U of $\mathbb{P}^1$ over which the fibres of π are smooth curves. For $z\in\mathbb{P}^1-U$, we know how to compute

$\mathrm{R}\Gamma(X_z, \mathbb{F}_\ell)$. Moreover, given an explicit description of $\mathcal{F}$, we know how to compute $\mathrm{R}\Gamma(\mathbb{P}^1, \mathcal{F})$. Denote by $X_{\overline{\eta}}$ the generic fibre of π, and by $g_{\overline{\eta}}$ its genus. A trivialising cover $V \to U$ of $\mathcal{F}|_U$ is given by the normalisation of U in an extension of K of $k(t)$ over which $\mathrm{Pic}(X_{\overline{\eta}})[\ell]$ is defined. The following data helps us estimate the complexity we need for the different steps of the algorithms:

- the degree $[K : k(t)]$ is smaller than $\ell^{4g_{\overline{\eta}}^2}$;
- the number $r = |\mathbb{P}^1 - U|$ only depends on π and not on ℓ;
- the genus g_V of V is bounded by $r\ell^{4g_{\overline{\eta}}^2}$.

Computing the whole cover $V^{\langle \ell \rangle}$ would be too costly. However, as suggested in Section 5.6, it is sufficient to compute a subcover $V_D^{\langle \ell \rangle}$ of $V^{\langle \ell \rangle}$ using only elements of $\mathrm{H}^1(V, \mu_\ell)$ defined over a degree $D = O(\ell^{4g_{\overline{\eta}}^2 r^2})$ extension $\mathbb{F}_Q$ of $\mathbb{F}_q$. Hence, if we could compute:

- $\mathrm{H}^1(X_{\overline{\eta}}, \mu_\ell)$ in time polynomial in ℓ and $\log(q)$,
- $\mathrm{H}^1(V, \mu_\ell)(\mathbb{F}_Q)$ in time polynomial in $\ell, \log Q$ and the genus of V,

then we should be able to compute the $\mathrm{H}^i(X, \mathcal{F})$ with their Frobenius action in time $\mathrm{Poly}(\ell, \log q)$. Mascot recently described an algorithm to deal with the first item of the list [12, Alg. 2.2] using p-adic approximation; however, parts of his method are not yet rigorous [12, Rk. 4.3].

For the moment, this is nothing more than wishful thinking: all existing algorithms to compute $\mathrm{H}^1(V, \mu_\ell)$, even for projective curves, have complexity exponential either in $\log(q)$ or in the genus of V. However, there is some hope. Harvey's algorithm [6, Thm. 1], which computes the zeta function of hyperelliptic curves, reaches an average polynomial-time complexity. Combined with Couveignes' algorithm and Section 5.6, this allows for an average polynomial-time complexity for the computation of $\mathrm{H}^1(V, \mu_\ell)(\mathbb{F}_Q)$ in the case where V is an open subset of a hyperelliptic curve.

6. First example: sheaves on subschemes of $\mathbb{P}^1$

6.1. The cover. Take $n = 2$. Let k_0 be a field of odd characteristic in which -1 is not a square. Consider the degree 2 (ramified) Galois cover

$$\begin{aligned} \overline{f} \colon \mathbb{P}^1 &\longrightarrow \mathbb{P}^1 \\ y &\longmapsto y^2 \end{aligned}$$

whose automorphism group is generated by $\tau \colon y \mapsto -y$. Set $U = \mathbb{P}^1 - \{0, 1, \infty\}$ and $V = f^{-1}U = \mathbb{P}^1 - \{0, \pm 1, \infty\}$, and consider the étale cover $f \colon V \to U$ induced by $\overline{f}$.

Computation of $V^{\langle n \rangle}$. The group $\mathrm{H}^1(V, \mu_2) \simeq \Lambda^3$ is generated by the divisor-function pairs $(0 - \infty, y), (1 - \infty, y - 1), (-1 - \infty, y + 1)$. The

cover $V^{\langle n\rangle} \to V$ with group $\mathrm{H}^1(V,\Lambda)^\vee$ corresponds to the field extension $k(\sqrt{y},\sqrt{y-1},\sqrt{y+1})/k(y)$. The corresponding cover of $\overline{V} = \mathbb{P}^1$ is the map

$$\begin{aligned}\operatorname{Proj} k[z_0,z_1,z_2,z_3]/(z_1^2-(z_0^2-z_3^2),z_2^2-(z_0^2+z_3^2)) &\longrightarrow \operatorname{Proj} k[y_0,y_1]\\ (z_0:z_1:z_2:z_3) &\longmapsto (z_0^2:z_3^2)\end{aligned}$$

which is ramified above $0,\pm1,\infty$.

***Computation of* $\mathbf{Aut}(V^{\langle n\rangle}|U)$.** The automorphism group $G := \mathrm{Aut}(V^{\langle n\rangle}|U)$ has order 16; in order to compute all of its elements, it suffices to compute a preimage of τ in $\mathrm{Aut}(V^{\langle n\rangle}|U)$. Such a preimage is given by $\gamma\colon (z_0:z_1:z_2:z_3) \mapsto (\sqrt{-1}z_0:\sqrt{-1}z_2:\sqrt{-1}z_1:z_3)$. Let

$$\begin{aligned}\sigma_1&\colon (z_0:z_1:z_2:z_3) \longmapsto (-z_0:z_1:z_2:z_3)\\ \sigma_2&\colon (z_0:z_1:z_2:z_3) \longmapsto (z_0:-z_1:z_2:z_3)\\ \sigma_3&\colon (z_0:z_1:z_2:z_3) \longmapsto (z_0:z_1:-z_2:z_3)\end{aligned}$$

be the obvious generators of $\mathrm{Aut}(V^{\langle n\rangle}|V) \lhd G$. Then $\gamma\sigma_2 = \sigma_3\gamma$ and $\gamma\sigma_3 = \sigma_2\gamma$, which implies that $\langle\sigma_2,\sigma_3\rangle$ is normal in G. It is easy to check that the composite map

$$\langle\gamma\rangle \longrightarrow G/\langle\sigma_2,\sigma_3\rangle$$

is an isomorphism; therefore,

$$G = \langle\sigma_2,\sigma_3\rangle \rtimes \langle\gamma\rangle.$$

6.2. Cohomology of a locally constant sheaf. The sheaf $\mathcal{F} := f_\star\Lambda$ is locally constant on U, trivialised by the cover $f\colon V \to U$ since $f^\star f_\star\Lambda \simeq \Lambda^2$. It corresponds to the $\mathrm{Aut}(V|U)$-module Λ^2, where the non-trivial element of $\mathrm{Aut}(V|U)$ exchanges the two copies of Λ. Since f is finite, $\mathrm{R}f_\star\Lambda = (f_\star\Lambda)[0]$ and there is a canonical isomorphism

$$\mathrm{R}\Gamma(U,f_\star\Lambda) = \mathrm{R}\Gamma(V,\Lambda).$$

We therefore expect to find

$$\mathrm{H}^1(U,\mathcal{F}) = \mathrm{H}^1(V,\Lambda) \simeq \Lambda^3.$$

***Computing* $\mathbf{R\Gamma(U,\mathcal{F})}$.** We know that $\mathrm{R}\Gamma(U,\mathcal{F})$ is represented by the following two-term complex:

$$\Lambda^2 \longrightarrow \mathrm{Hom}_{\mathrm{cr}}(G,\Lambda^2).$$

A crossed homomorphism $f\colon G \to \Lambda^2$ is determined by the images of $\sigma_1,\sigma_2,\sigma_3,\gamma$. Using the relations $\gamma\sigma_1 = \sigma_1\gamma$, $\gamma\sigma_2 = \sigma_3\gamma$ and $\gamma^2 = \sigma_1\sigma_2\sigma_3$, we see that such a map is uniquely determined by a tuple $(a,a_1,a_2,a_3) \in \Lambda^4$; the corresponding map f is defined by $f(\sigma_1) = (a_1,a_1)$, $f(\sigma_2) = (a_2,a_3)$,

$f(\sigma_3) = (a_3, a_2)$ and $f(\gamma) = (a, a + a_1 + a_2 + a_3)$. The principal crossed homomorphisms correspond to $(0,0,0,0)$ and $(1,0,0,0)$. Hence the complex above is isomorphic to

$$\begin{aligned} \Lambda^2 &\longrightarrow \Lambda^4 \\ (a,b) &\longmapsto (a+b,0,0,0) \end{aligned}$$

and its cohomology groups are Λ and Λ^3, as expected.

Computing the Galois action. The action of $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$ on $\mathrm{Aut}(Y|X)$ clearly factors through the quotient $\mathrm{Gal}(k_0(\sqrt{-1})|k_0)$. The latter group is generated by $\phi\colon \sqrt{-1} \mapsto -\sqrt{-1}$. The automorphism ϕ acts trivially on $\sigma_1, \sigma_2, \sigma_3$, and

$$\phi \cdot \gamma = \sigma_1\sigma_2\sigma_3\gamma\colon (z_0 : z_1 : z_2 : z_3) \longmapsto (-\sqrt{-1}z_0 : -\sqrt{-1}z_1 : -\sqrt{-1}z_2 : z_3).$$

The action of ϕ on Λ^2 is trivial, and its action on $\mathrm{Hom}_{\mathrm{cr}}(G, \Lambda^2) \simeq \Lambda^4$ is $(\phi \cdot f)(x) = \phi f(\phi^{-1}x) = f(\phi^{-1}x)$. Explicitly, since $\phi \cdot \gamma = \sigma_1\sigma_2\sigma_3\gamma$, this action is given by

$$\phi \cdot (a, a_1, a_2, a_3) = (a + a_1 + a_2 + a_3, a_1, a_2, a_3).$$

6.3. Ramification. The following illustrates Section 2.4 and provides a few results that will be used in the next example.

Ramification. Let Z, W, W' denote the sets of points at infinity of $U, V, V^{\langle n\rangle}$ respectively. The following table gives an overview of the situation.

Points in Z	0	1		∞
Preimages in W	0	-1	1	∞
Ramification	index 2	index 1	index 1	index 2
Preimages in W'	4 points	4 points	4 points	4 points
Ramification	index 4	index 2	index 2	index 4
A preimage in W'	$P_0 = (0, \sqrt{-1}, 1)$	$P_{-1} = (\sqrt{-1}, \sqrt{-2}, 0)$	$P_1 = (1, 0, \sqrt{2})$	$P_\infty = (1:1:1:0)$
Its inertia group	$\langle\gamma\sigma_2\rangle \simeq \mu_4(k)$	$\langle\sigma_3\rangle \simeq \mu_2(k)$	$\langle\sigma_2\rangle \simeq \mu_2(k)$	$\langle\gamma\rangle \simeq \mu_4(k)$

The canonical isomorphism $I_{P_0} \to \mu_4(k)$ can be described explicitly as follows. The function y is a uniformiser of $V^{\langle n\rangle}$ at $P_0 = (0, \sqrt{-1}, 1)$. The orbit of y under the action of $I_{P_0} = \langle\gamma\sigma_2\rangle$ is $\{\pm y, \pm\sqrt{-1}y\}$. Hence the set $\{\frac{\sigma(y)}{y}(P_0) \mid \sigma \in I_{P_0}\}$ is exactly $\mu_4(k)$, and the isomorphism I_{P_0} to $\mu_4(k)$ sends an element $\sigma \in I_{P_0}$ to $\frac{\sigma(y)}{y}(P_0)$.

The generator $\sqrt{-1}$ of $\mu_4(k)$ exchanges the two copies of Λ in $M = \Lambda^2$. The Λ-module of crossed homomorphisms $\mu_4(k) \to M$ is isomorphic to Λ^2, and $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(I_{P_0}, M)$ is represented by the following complex.

$$\begin{aligned} \Lambda^2 &\longrightarrow \Lambda^2 \\ (a,b) &\longmapsto (a+b, a+b) \end{aligned}$$

The group $\mathcal{F}_0 = \mathrm{H}^0(I_{P_0}, M)$ is generated by $(1,1)$, and $\mathrm{H}^2_0(X, j_\star\mathcal{F}) = \mathrm{H}^1(I_{P_0}, M)$ is generated by the class of $(0,1)$. The compuation of the complex $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(I_{P_\infty}, M)$ is done in the same way and yields the same result. The group I_{P_1} is canonically isomorphic to $\mu_2(k)$, and acts trivially on M. Therefore, $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(I_{P_1}, M)$ is represented by the following complex.

$$\begin{aligned} \Lambda^2 &\longrightarrow \Lambda^2 \\ (a,b) &\longmapsto 0 \end{aligned}$$

The computation for P_{-1} is the same and yields the same result.

6.4. Cohomology of a constructible sheaf. We still consider a field k_0 of odd characteristic, where -1 is not a square. Define $k_1 = k_0(\sqrt{-1})$. Let us now consider the ramified cover of projective curves $\bar{f}\colon \mathbb{P}^1 \to \mathbb{P}^1$ defined by f, and the sheaf $\mathcal{F} \coloneqq \bar{f}_\star\Lambda$ on $\mathbb{P}^1$. Since $\bar{f}$ is unramified outside $0, \infty$, the sheaf $\mathcal{F}$ is locally constant on the open subset $\mathbb{G}_m = \mathbb{P}^1 - \{0,\infty\}$, and $\mathscr{L} \coloneqq \mathcal{F}|_{\mathbb{G}_m}$ is trivialised by $\bar{f}|_{\mathbb{G}_m}\colon \mathbb{G}_m \to \mathbb{G}_m, y \mapsto y^2$. The cover $\mathbb{G}_m^{\langle n\rangle}$ is also $\mathbb{G}_m \to \mathbb{G}_m, z \mapsto z^2$, and the composite

$$\mathbb{G}_m^{\langle n\rangle} \longrightarrow \mathbb{G}_m \xrightarrow{f} \mathbb{G}_m$$

is given by $z \mapsto z^4$. Its automorphism group is $G = \langle \gamma\colon z \mapsto \sqrt{-1}z\rangle \simeq \mathbb{Z}/4\mathbb{Z}$, and the inertia subgroups at 0 and ∞ are both equal to G. Denote by j the inclusion $\mathbb{G}_m \to \mathbb{P}^1$. We have $(j_\star\mathscr{L})_0 = \Lambda$ and $(j_\star\mathscr{L})_\infty = \Lambda$. The adjunction units $\mathcal{F}_0 \to (j_\star\mathscr{L})_0$ and $\mathcal{F}_\infty \to (j_\star\mathscr{L})_\infty$ are the identity maps $\Lambda \to \Lambda$.

***Computing* $\mathbf{R\Gamma(\mathbb{G}_m, \mathscr{L})}$.** The crossed homomorphisms $G \to M = \mathscr{L}_{\bar{\eta}} \simeq \Lambda^2$ are uniquely determined by the image of $(a,b) \in \Lambda^2$ under γ. The usual cochain complex representing $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G, M) = \tau_{\leqslant 1}\,\mathrm{R}\Gamma(\mathbb{G}_m, \mathscr{L})$ is the following.

$$\begin{aligned} \Lambda^2 &\longrightarrow \mathrm{Hom}_{\mathrm{cr}}(G, \Lambda^2) \\ (a,b) &\longmapsto [\gamma \mapsto (a+b, a+b)] \end{aligned}$$

Therefore $\mathrm{H}^1(G, M)$ is isomorphic to Λ, and the kernel of the map $\Lambda^2 \to \mathrm{H}^1(G, M)$ sending a crossed homomorphism to its cohomology class is $\langle(1,1)\rangle$; this map can be rewritten as

$$\begin{aligned} \Lambda^2 &\longrightarrow \Lambda \\ (a,b) &\longmapsto a+b. \end{aligned}$$

***Computing* $\mathbf{R\Gamma(X, j_\star\mathscr{L})}$.** The element $\mathrm{R}\Gamma(X, j_\star\mathscr{L})[1] \in \mathrm{D}^b_c(X, \Lambda)$ is the cone of

$$\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G, M) \longrightarrow \mathrm{H}^1(I_0, M)[-1] \oplus \mathrm{H}^1(I_\infty, M)[-1] = \Lambda^2[-1].$$

Therefore, $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$ is represented by the complex

$$\Lambda^2 \longrightarrow \Lambda^2 \longrightarrow \Lambda^2$$

where both morphisms are given by $(a, b) \mapsto (a + b, a + b)$.

***Computing* $\mathbf{R\Gamma(X, \mathcal{F})}$.** Let us now turn to the computation of the map

$$\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(Z, i^\star\mathcal{F}) \longrightarrow \mathrm{R}\Gamma(Z, i^\star j_\star\mathscr{L}).$$

On the one hand, $\mathrm{R}\Gamma(Z, i^\star\mathcal{F}) = \mathrm{H}^0(Z, i^\star\mathcal{F})[0] = \mathcal{F}_0[0] \oplus \mathcal{F}_\infty[0]$. On the other hand, $\mathrm{R}\Gamma(Z, i^\star j_\star\mathscr{L})$ is represented by the complex

$$\Lambda^2 \oplus \Lambda^2 \xrightarrow{\alpha'} \Lambda^2 \oplus \Lambda^2 \xrightarrow{\beta'} \Lambda^2$$

where the arrows are given by $\alpha' \colon (a, b, c, d) \mapsto (a+b, a+b, c+d, c+d)$ and $\beta' \colon (a, b, c, d) \mapsto (a + b, c + d)$. Hence the map we were looking for is

$$\begin{array}{ccccc} \Lambda^4 & \xrightarrow{\alpha} & \Lambda^2 & \xrightarrow{\beta} & \Lambda^2 \\ \downarrow{\scriptstyle u} & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle \mathrm{id}} \\ \Lambda^4 & \xrightarrow{\alpha'} & \Lambda^4 & \xrightarrow{\beta'} & \Lambda^2 \end{array}$$

where, writing the upper left-hand side term as $\mathcal{F}_0 \oplus \mathcal{F}_\infty \oplus M$, the arrows are given by

- $u \colon (a, b, c, d) \mapsto (a + c, a + d, b + c, b + d)$
- $\alpha \colon (a, b, c, d) \mapsto (c + d, c + d)$
- $\beta \colon (a, b) \mapsto (a + b, a + b)$
- $v \colon (a, b) \mapsto (a, b, a, b)$
- $\alpha' \colon (a, b, c, d) \mapsto (a + b, a + b, c + d, c + d)$
- $\beta' \colon (a, b, c, d) \mapsto (a + b, c + d)$.

Computing the cone of this morphism and shifting by 1 yields the following complex, which represents $\mathrm{R}\Gamma(X, \mathcal{F})$.

$$\Lambda^4 \xrightarrow{\partial_0} \Lambda^6 \xrightarrow{\partial_1} \Lambda^6 \xrightarrow{\partial_2} \Lambda^2$$

- $\partial_0 \colon (a, b, c, d) \mapsto (c + d, c + d, a + c, b + c, a + d, b + d)$
- $\partial_1 \colon (a, b, c, d, e, f) \mapsto (a+b, a+b, a+c+d, b+c+d, a+e+f, b+e+f)$
- $\partial_2 \colon (a, b, c, d, e, f) \mapsto (a + c + d, b + e + f)$.

The cohomology groups of this complex are $\mathrm{H}^0 = \langle(1, 1, 1, 1)\rangle$, $\mathrm{H}^1 = 0$ and $\mathrm{H}^2 = \langle\overline{(1, 0, 1, 0, 0, 0)}\rangle \simeq \Lambda$. This result was to be expected: we have computed the cohomology of $(\mathbb{P}^1 \xrightarrow{x \mapsto x^2} \mathbb{P}^1)_\star\Lambda$, which is the cohomology of the constant sheaf Λ on $\mathbb{P}^1$.

Computing the Galois action. The action of $\mathrm{Gal}(k|k_0)$ on $\mathrm{R}\Gamma(X,\mathcal{F})$ factors through the quotient $\mathrm{Gal}(k_0(\sqrt{-1})|k_0)$ of $\mathrm{Gal}(k|k_0)$. Denote by $\sigma\colon \sqrt{-1} \mapsto -\sqrt{-1}$ the nontrivial element of $\mathrm{Gal}(k_0(\sqrt{-1})|k_0)$. The group $\mathrm{Gal}(k|k_0)$ acts on G by $\sigma\cdot\gamma = \gamma^3$, and trivially on M. Its action on $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G,M) = \Lambda^2 \to \Lambda^2$ is trivial on the first term, and $(a,b)\mapsto(b,a)$ on the second. In particular, it acts trivially on $\mathrm{H}^1(G,M) = \Lambda$. The action of σ on $\mathcal{F}_0, \mathcal{F}_\infty$ is also trivial. Hence the action of $\mathrm{Gal}(k|k_0)$ on the complex

$$\Lambda^4 \longrightarrow \Lambda^6 \longrightarrow \Lambda^6 \longrightarrow \Lambda^2$$

representing $\mathrm{R}\Gamma(X,\mathcal{F})$ is trivial on the first and last terms,

$$\sigma\cdot(a,b,c,d,e,f) = (b,a,c,d,e,f)$$

on the second term, and

$$\sigma\cdot(a,b,c,d,e,f) = (a,b,d,c,f,e)$$

on the third term. In particular, $\mathrm{Gal}(k|k_0)$ acts trivially on $\mathrm{H}^0(X,\Lambda)$ and $\mathrm{H}^2(X,\Lambda)$, as expected.

7. Second example: sheaves on subschemes of an elliptic curve

The examples in this section illustrate a non-trivial case in which we can easily compute the cohomology of sheaves using (almost) only functions that are already available in current computer algebra systems: when the locally constant part of the sheaf is trivialised by a subscheme of a hyperelliptic curve.

7.1. The cover. Consider the finite field $k_0 = \mathbb{F}_{11}$, and the integer $n = 2$ invertible in k_0. Consider the field extension $\mathbb{F}_{121} = \mathbb{F}_{11}(a)$, where a generates the cyclic group $\mathbb{F}_{121}^\times$ and $a^2 + 7a + 2 = 0$. Denote by $\overline{E}$ the elliptic curve over $k = \overline{\mathbb{F}_{11}}$ defined by the affine Weierstrass equation $y^2 = (x-1)(x-2)(x-3)$. Let $\overline{C}$ be the genus 2 curve over k given by the affine equation $y^2 = (x^2-1)(x^2-2)(x^2-3)$. The curve $\overline{C}$ has two points at infinity ∞_+, ∞_- which do not lie on the affine open defined by this equation. Consider the degree 2 cover $\overline{f}\colon \overline{C} \to \overline{E}$ given by $(x,y)\mapsto(x^2,y)$. It is ramified at the affine points $P = (0,4)$ and $Q = (0,7)$ of $\overline{C}$, whose images in E are respectively $(0,4)$ and $(0,7)$. Denote by $C = \overline{C} - \{P,Q\}$ and $E = \overline{E} - \{\overline{f}(P), \overline{f}(Q)\}$ the affine curves obtained from $\overline{C}$ and $\overline{E}$ by removing the ramification locus. Denote by $f\colon C \to E$ the étale Galois cover induce by $\overline{f}$. Both curves C and E are obtained by base change from curves C_0 and E_0 defined over $k_0 = \mathbb{F}_{11}$.

Computing the Galois group of $C^{\langle n\rangle} \to E$ will allow us to determine the cohomology of any locally constant sheaf on E trivialised by f. First, we need to compute $\mathrm{H}^1(C,\mu_2)$. This is where we need to cheat a little since no algorithm performing this computation for a general curve has been

implemented yet (see Section 5.2 for existing algorithms); fortunately, $\overline{C}$ being a genus two curve, we have other means of finding a generating set for this group.

Computing $\mathbf{H^1(C, \mu_2)}$**.** Denote by

$$P_1^{\pm} = (\pm 1, 0), \qquad P_2^{\pm} = (\pm a^6, 0), \qquad P_3^{\pm} = (\pm 5, 0)$$

the points of C with y-coordinate 0. A basis of $\mathrm{Jac}(\overline{C})[2]$ is given by the classes of the divisors

$$D_1 \coloneqq P_1^+ - P_1^-, \quad D_2 \coloneqq P_2^+ - P_2^-, \quad D_3 \coloneqq P_2^+ - P_3^+, \quad D_4 \coloneqq P_1^+ - P_3^-.$$

The rational functions

$$f_1 \coloneqq \frac{x-1}{x+1}, \qquad f_2 \coloneqq \frac{x-a^6}{x+a^6}, \qquad f_3 \coloneqq \frac{x-a^6}{x-5}, \qquad f_4 \coloneqq \frac{x-1}{x+5}$$

all satisfy $2D_i = \mathrm{div}(f_i)$. Denote by D_5 the divisor $P - Q$, which is linearly equivalent to two times the divisor

$$\overline{D}_5 \coloneqq (a^{41}, a^{29}) + (-a^{41}, a^{29}) - (\infty_+ + \infty_-).$$

We found this divisor $\overline{D}_5$ using a brute-force search on $\mathrm{Jac}(\overline{C})(\mathbb{F}_{121})$; for hyperelliptic curves such as $\overline{C}$, this can also be done using division polynomials (see e.g. [4, Thm. C]). In the particular case where $n = 2$, division by 2 has even been explicitly described by Zarhin [19, Thm. 3.2]. The divisor of the rational function

$$f_5 = \frac{y + a^8 x^2 + 7}{x}$$

is $2\overline{D}_5 - D_5$. Therefore, an $\mathbb{F}_2$-basis of $\mathrm{H}^1(C, \mu_2)$ is given by

$$(D_1, f_1), \ldots, (D_4, f_4), (\overline{D}_5, f_5).$$

Computing $\mathbf{Aut}(\boldsymbol{C^{\langle n\rangle}|E})$**.** The cover $C^{\langle n\rangle} \to C$ with group $\mathrm{H}^1(C, \Lambda)^\vee$ is defined by its function field $k(C)(z_1, \ldots, z_5)$ where $z_i^2 = f_i$. Recall that we never need to compute a smooth model of $C^{\langle n\rangle}$. For reasons explained in Section 7.2, we choose to replace f_5 with $x^2 f_5$, which still yields the same function field. The group $G = \mathrm{Aut}(C^{\langle n\rangle}|E)$ has order 64; it contains the normal subgroup $H = \mathrm{Aut}(C^{\langle n\rangle}|C) \simeq (\mathbb{Z}/2\mathbb{Z})^5$ generated by the elements $\gamma_i \colon z_i \mapsto -z_i$. Let us now determine a preimage in G of the generator $\sigma \colon (x, y) \mapsto (-x, y)$ of $\mathrm{Aut}(C|E)$. First, we compute the divisors $\sigma^\star D_i$.

$$\begin{aligned}
\sigma^\star D_1 &= -D_1 \\
\sigma^\star D_2 &= -D_2 \\
\sigma^\star D_3 &= D_1 + D_3 + \mathrm{div}(h_3) \quad \text{where } h_3 = \tfrac{y}{x^3 + a^{58}x^2 + a^2 x + a^{54}} \\
\sigma^\star D_4 &= D_2 + D_4 + \mathrm{div}(h_4) \quad \text{where } h_4 = \tfrac{y}{x^3 + a^{80}x^2 + a^{103}x + a^{114}} \\
\sigma^\star D_5 &= D_5
\end{aligned}$$

Note that $\sigma^\star f_3 = h_3^2 f_1 f_3$, $\sigma^\star f_4 = h_4^2 f_2 f_4$ and $\sigma^\star f_5 = -f_5$. Since a^{30} is a square root of -1 in $\mathbb{F}_{121}$, the automorphism $\delta \in G$ given by

$$x \longmapsto -x, \quad y \longmapsto y, \quad z_1 \longmapsto \frac{1}{z_1}, \quad z_2 \longmapsto \frac{1}{z_2},$$
$$z_3 \longmapsto h_3(x,y) z_1 z_3, \quad z_4 \longmapsto h_4(x,y) z_2 z_4, \quad z_5 \longmapsto a^{30} z_5$$

is a preimage of σ. In particular, since

$$h_3(x,y)h_3(-x,y) = h_4(x,y)h_4(-x,y) = -1,$$

the automorphism δ^2 is given by

$$x \longmapsto x, \quad y \longmapsto y, \quad z_1 \longmapsto z_1, \quad z_2 \longmapsto z_2,$$
$$z_3 \longmapsto -z_3, \quad z_4 \longmapsto -z_4, \quad z_5 \longmapsto -z_5.$$

] Hence $\delta^2 = \gamma_3\gamma_4\gamma_5$ and the order of δ as an element of G is 4. Furthermore, $\delta\gamma_1 = \gamma_1\gamma_3\delta$ and $\delta\gamma_2 = \gamma_2\gamma_4\delta$. The elements $\gamma_3, \gamma_4, \gamma_5$ generate the center of G. Its commutator subgroup is $\langle \gamma_3 = [\gamma_1, \delta], \gamma_4 = [\gamma_2, \delta] \rangle$. Finally, let us compute the action of $\mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11}) = \langle \phi \colon a \mapsto 2a^{-1} \rangle$ on G, which can be done very easily since the elements of G are defined by their action on coordinates of points. Predictably, ϕ acts trivially on the γ_i; it also sends δ to $\gamma_5\delta$.

7.2. Ramification. Here is how to compute the preimages of the points P and Q in $C^{\langle n \rangle}$. We have computed its function field as $k(C^{\langle n \rangle}) = k(C)(z_1^2 - f_1, \ldots, z_5^2 - f_5)$, and would now like to compute an actual affine model of $C^{\langle n \rangle}$. For each $i \in \{1 \ldots 5\}$, write $f_i = \frac{g_i}{h_i}$. For P and Q to have easily computable preimages, we can replace f_i with $h_i^2 f_i$ when $h_i(P) = 0$ or $h_i(Q) = 0$. This is only the case for f_5, which now reads $x(y + a^8 x^2 + 7)$. The following affine curve is birational to $C^{\langle n \rangle}$:

$$\begin{aligned} \operatorname{Spec} k[x, y, z_1, \ldots, z_5]/ \quad & (y^2 - (x^2-1)(x^2-2)(x^2-3), \\ & (x+1)z_1^2 - (x-1), \\ & (x+a^6)z_2^2 - (x-a^6), \\ & (x-5)z_3^2 - (x-a^6), \\ & (x+5)z_4^2 - (x-1), \\ & z_5^2 - x(y + a^8 x^2 + 7)). \end{aligned}$$

The $\frac{1}{2}|\mathrm{H}^1(C, \mu_2)| = 16$ preimages of $P = (0, 4)$ in $C^{\langle n \rangle}$ are the points $(0, 4, \pm 1, \pm a^{30}, \pm 3a^3, \pm 3a^{30}, 0)$. The preimages of $Q = (0, 7)$ are the points $(0, 7, \pm 1, \pm a^{30}, \pm 3a^3, \pm 3a^{30}, 0)$. Choose two preimages $P_{C^{\langle n \rangle}} = (0, 4, 1, a^{30}, 3a^3, 3a^{30}, 0)$ and $Q_{C^{\langle n \rangle}} = (0, 7, 1, a^{30}, 3a^3, 3a^{30}, 0)$ of P and Q in this affine curve birational to $C^{\langle n \rangle}$, and denote by $P_E = (0, 4), Q_E = (0, 7)$ their respective images in E. The inertia group $I_{P_{C^{\langle n \rangle}}|P_E} \subset G$ has order

$|I_{P|P_E}| \cdot |I_{P_{C^{\langle n\rangle}|P}}| = 2 \times 2 = 4$; it is generated by δ. The same applies to $I_{Q_{C^{\langle n\rangle}|Q}} = \langle\delta\rangle$.

7.3. Cohomology of a locally constant sheaf on E. Consider the locally constant sheaf $\mathcal{F}$ on E trivialised by C, with generic fibre $M = \Lambda^3$, defined by the representation:

$$\begin{aligned} \mathrm{Aut}(C|E) &\longrightarrow \mathrm{GL}_3(\Lambda) \\ \sigma &\longmapsto \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{aligned}$$

Computations using Magma yield $\mathrm{H}^0(E,\mathcal{F}) \simeq \Lambda^2$ and $\mathrm{H}^1(E,\mathcal{F}) \simeq \Lambda^8$. More precisely, the 1-cocycles $c_1,\dots,c_8$ below form a basis of $\mathrm{H}^1(G,M)$; the null-cohomologous cocycle c' is the image of the 0-cocycle $(1\ 0\ 0) \in M$.

Cocycle c	$c(\gamma_1)$	$c(\gamma_2)$	$c(\gamma_3)$	$c(\gamma_4)$	$c(\gamma_5)$	$c(\delta)$
c_1	(1 0 0)	(0 0 0)	(1 0 1)	(0 0 0)	(0 0 0)	(0 0 1)
c_2	(0 1 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)
c_3	(0 0 1)	(0 0 0)	(1 0 1)	(0 0 0)	(0 0 0)	(0 0 1)
c_4	(0 0 0)	(1 0 0)	(0 0 0)	(1 0 1)	(0 0 0)	(0 0 1)
c_5	(0 0 0)	(0 1 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)
c_6	(0 0 0)	(0 0 1)	(0 0 0)	(1 0 1)	(0 0 0)	(0 0 1)
c_7	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(1 0 1)	(0 0 1)
c_8	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 1 0)
c'	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(0 0 0)	(1 0 1)

The action of $\phi \in \mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11})$ on $\mathrm{Hom}_{\mathrm{cr}}(G,M)$ only affects the element c_7 of this basis, sending it to $\phi^\star c_7 = c_7 + c'$. Its action on $\mathrm{H}^1(G,M)$ is therefore trivial.

Remark 7.1. *We now know that the action of* $\mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11})$ *on* $\mathrm{H}^1(E,\mathcal{F})$ *is trivial. Therefore, we could have chosen a subcover of* $C^{\langle n\rangle}$ *by first computing a basis of* $\mathrm{H}^1(C,\mu_2)(\mathbb{F}_{11})$ *and then taking* n^{th} *roots of the functions appearing in this basis. With the notations above, such a basis is given by* $(D_1,f_1),(D_2,f_2),(D_4,f_4),(D_3+\overline{D}_5,f_3f_5)$. *Set* $k(C') = k(C)(z_1,z_2,z_4,t_3)$ *where* $z_i^2 = f_i$ *and* $t_3^2 = f_3f_5$. *Using the previous notations* h_3,h_4, *a preimage of* $\sigma \in \mathrm{Aut}(C|E)$ *in* $\mathrm{Aut}(C'|E)$ *is the automorphism* δ *given by:*

$$x \longmapsto -x, \quad y \longmapsto y, \quad z_1 \longmapsto \frac{1}{z_1}, \quad z_2 \longmapsto \frac{1}{z_2}, \quad z_4 \longmapsto h_4(x,y)z_2z_4,$$
$$t_3 \longmapsto a^{30}h_3(x,y)t_3.$$

The group $\mathrm{Aut}(C'|E)$ *only has order 32, and one can check that the map*

$$\mathrm{R}\Gamma(\mathrm{Aut}(C'|E), M) \longrightarrow \mathrm{R}\Gamma(\mathrm{Aut}(C^{\langle n\rangle}|E), M)$$

is a quasi-isomorphism.

Acknowledgments. The author would like to thank David Madore and Fabrice Orgogozo for their continued help and support during his PhD thesis, whose main results led to the ones presented in this article. He is also grateful to the anonymous referee for their helpful questions and comments.

References

[1] J.-M. Couveignes, "Linearizing torsion classes in the Picard group of algebraic curves over finite fields", *J. Algebra* **321** (2009), no. 8, p. 2085-2118.

[2] E. D. Davis, "On the geometric interpretation of seminormality", *Proc. Am. Math. Soc.* **68** (1978), no. 1, p. 1-5.

[3] B. Edixhoven & J.-M. Couveignes (eds.), *Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujan's tau at a prime*, Annals of Mathematics Studies, vol. 176, Princeton University Press, 2011, xi+425 pages.

[4] E. Eid, "Efficient computation of Cantor's division polynomials of hyperelliptic curves over finite fields", *J. Symb. Comput.* **117** (2023), p. 68-100.

[5] L. Fu, *Etale Cohomology Theory*, 2nd rev. ed., Nankai Tracts in Mathematics, no. 14, World Scientific, 2015, ix+611 pages.

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

[7] K. H. Hofmann & S. A. Morris, *The structure of compact groups. A primer for the student – a handbook for the expert*, De Gruyter Studies in Mathematics, vol. 25, Walter de Gruyter, 2020, xxvii+1006 pages.

[8] M.-D. Huang & D. Ierardi, "Counting points on curves over finite fields", *J. Symb. Comput.* **25** (1998), no. 1, p. 1-21.

[9] J. Jin, "Computation of étale cohomology on curves in single exponential time", *J. Théor. Nombres Bordeaux* **32** (2020), no. 2, p. 311-354.

[10] C. Levrat, "Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe", PhD Thesis, Sorbonne Université (France), 2022.

[11] D. A. Madore & F. Orgogozo, "Calculabilité de la cohomologie étale modulo ℓ", *Algebra Number Theory* **9** (2015), no. 7, p. 1647-1739.

[12] N. Mascot, "Explicit computation of Galois representations occurring in families of curves", 2023, `https://arxiv.org/abs/2304.04701`.

[13] J. S. Milne, *Étale Cohomology*, Princeton Mathematical Series, no. 33, Princeton University Press, 1980, xiii+323 pages.

[14] ———, *Arithmetic Duality Theorems*, 2nd ed., BookSurge, 2006, First publ. by Academic Press, 1986, viii+339 pages.

[15] J. Neukirch, *Class Field Theory*, Springer, 2013, x+184 pages.

[16] B. Poonen, D. Testa & R. van Luijk, "Computing Néron–Severi groups and cycle class groups", *Compos. Math.* **151** (2015), no. 4, p. 713-734.

[17] The Stacks Project Authors, "Stacks Project", https://stacks.math.columbia.edu, 2018.

[18] C. A. Weibel, *An Introduction to Homological Algebra*, Cambridge Studies in Advanced Mathematics, no. 38, Cambridge University Press, 1994, xiv+450 pages.

[19] Y. G. Zarhin, "Division by 2 on odd-degree hyperelliptic curves and their Jacobians", *Izv. Math.* **83** (2019), no. 3, p. 501-520.

Christophe Levrat
INRIA Saclay
1 rue Honoré d'Estienne d'Orves
91120 Palaiseau, France
E-mail: christophe.levrat@math.cnrs.fr
URL: https://chrislevrat.perso.math.cnrs.fr/