HAL open science

Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe

Christophe Levrat

To cite this version:

Christophe Levrat. Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe. Géométrie algébrique [math.AG]. Sorbonne Université, 2022. Français. NNT : 2022SORUS294 . tel-03884543

HAL Id: tel-03884543

https://theses.hal.science/tel-03884543v1

Submitted on 5 Dec 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

École doctorale de Sciences Mathématiques de Paris Centre

Thèse de doctorat

Discipline : Mathématiques

présentée par

Christophe Levrat

Calcul effectif de la cohomologie des faisceaux constructibles sur le site étale d'une courbe

---

dirigée par David Madore et Fabrice Orgogozo

Soutenue le 30 septembre 2022 devant le jury composé de :

M. Xavier Caruso	Université de Bordeaux	rapporteur
M. Alain Couvreur	INRIA Saclay	examinateur
M. Bruno Kahn	Sorbonne Université	président
M. Davide Lombardo	Università di Pisa	rapporteur
M. David Madore	Télécom Paris	directeur
M. Fabrice Orgogozo	Sorbonne Université	directeur
M. Hugues Randriam	ANSSI & Télécom Paris	examinateur

Institut de mathématiques de Jussieu-
Paris Rive gauche. UMR 7586.
Boîte courrier 247
4 place Jussieu
75 252 Paris Cedex 05

Sorbonne Université
École doctorale de Sciences
Mathématiques de Paris Centre.
4 place Jussieu
75 252 Paris Cedex 05

„Sie meinen“, fragte Lukas, „Sie werden gar nicht kleiner, wenn Sie näher kommen? Und Sie sind auch nicht wirklich so riesengroß, wenn Sie weit entfernt sind, sondern es sieht nur so aus?“
„Sehr richtig“, antwortete Herr Tur Tur. „Deshalb sagte ich; ich bin ein Scheinriese.“

Michael Ende, *Jim Knopf und Lukas der Lokomotivführer*

Résumé/Abstract

(FR) Cette thèse porte sur la représentation algorithmique des faisceaux constructibles de groupes abéliens sur le site étale d'une variété sur un corps algébriquement clos, ainsi que sur le calcul effectif de leur cohomologie lorsque leur torsion est inversible dans le corps. Nous décrivons trois représentations de ces faisceaux sur les courbes lisses ou nodales, ainsi que des algorithmes permettant d'effectuer un certain nombre d'opérations (noyaux et conoyaux de morphismes, images directes et réciproques, Hom interne et produit tensoriel) sur ces faisceaux. Nous présentons un algorithme de calcul du complexe de cohomologie d'un faisceau localement constant constructible sur une courbe lisse ou nodale X, et en déduisons une description explicite du foncteur $\mathrm{R}\Gamma(X,-)\colon \mathrm{D}^b_c(X,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{D}^b_c(\mathbb{Z}/n\mathbb{Z})$, fonctorielle en le schéma X et le complexe constructible considéré. En particulier, si X et le faisceau $\mathcal{F}$ proviennent par changement de base d'un sous-corps parfait, nous décrivons l'action de Galois sur le complexe $\mathrm{R}\Gamma(X,\mathcal{F})$ calculé. Nous donnons des bornes explicites sur le nombre d'opérations effectuées par l'algorithme calculant $\mathrm{R}\Gamma(X,\mathcal{F})$. Nous donnons également une description explicite des cup-produits dans la cohomologie des faisceaux localement constants constructibles sur les courbes projectives lisses. Enfin, nous indiquons comment déduire de ces algorithmes une façon de calculer la cohomologie d'un faisceau constant sur une surface lisse fibrée sur la droite projective.

Mots-clés : cohomologie étale, cohomologie galoisienne, géométrie algébrique effective, courbe algébrique, complexité.

(ENG) This thesis deals with the algorithmic representation of constructible sheaves of abelian groups on the étale site of a variety over an algebraically closed field, as well as the explicit computation of their cohomology. We describe three representations of such sheaves on curves with at worst nodal singularities, as well as algorithms performing various operations (kernels and cokernels of morphisms, pullback and pushforward, internal Hom and tensor product) on these sheaves. We present an algorithm computing the cohomology complex of a locally constant constructible sheaf on a smooth or nodal curve, which in turn allows us to give an explicit description of the functor $\mathrm{R}\Gamma(X,-)\colon \mathrm{D}^b_c(X,\mathbb{Z}/n\mathbb{Z}) \to \mathrm{D}^b_c(\mathbb{Z}/n\mathbb{Z})$. This description is functorial in the scheme X and the given complex of constructible sheaves. In particular, if X and the sheaf $\mathcal{F}$ are obtained by base change from a subfield, we describe the Galois action on the complex $\mathrm{R}\Gamma(X,\mathcal{F})$. We give precise bounds on the number of operations performed by the algorithm computing $\mathrm{R}\Gamma(X,\mathcal{F})$. We also give an explicit description of cup-products in the cohomology of locally constant constructible sheaves over smooth projective curves. Finally, we show how to use these algorithms in order to compute the cohomology groups of a constant sheaf on a smooth surface fibered over the projective line.

Keywords : étale cohomology, Galois cohomology, effective algebraic geometry, algebraic curve, complexity.

Remerciements

Ces quelques pages seront sans aucun doute les plus lues de tout ce manuscrit. Ce sont les seules à être écrites à la première personne du singulier, et c'est à partir d'elles que les chercheurs qui ne me connaissent pas se feront une image de moi. Par contre, pour vous qui me connaissez, qui m'avez accompagné pendant ces trois ans, ce n'est pas de moi qu'elles parlent, mais de vous. Ce sont ces pages, également, qui occuperont ceux qui en auront assez de faire semblant d'écouter attentivement pendant la soutenance. Ne vous inquiétez pas, elles sont faites pour : si vous lisez ces lignes à 15h05 alors que j'ai commencé à parler à 15h, dites-vous que d'autres sont en train de faire la même chose, et que je l'aurais peut-être fait aussi si je n'étais pas occupé à soutenir ma thèse.

Le jury Tout d'abord, je voudrais remercier les chercheurs qui m'ont fait l'honneur de s'intéresser à mon travail. Merci à Xavier Caruso, Alain Couvreur, Bruno Kahn, Davide Lombardo et Hugues Randriam d'avoir accepté de faire partie de mon jury. En particulier, je tiens à remercier Xavier Caruso et Davide Lombardo d'avoir lu mon manuscrit avec attention et suggéré de nombreuses corrections qui ont grandement amélioré la qualité des pages qui suivent. Merci à Alain Couvreur d'avoir toujours répondu à mes questions avec un sourire qui se lisait même dans les mails, et à Bruno Kahn pour sa présence et ses conseils bienveillants pendant ces trois années.

Les directeurs David et Fabrice, je ne peux pas assez vous remercier pour votre encadrement pendant ces trois années. J'ai beaucoup appris à vos côtés, sur les maths, sur la recherche, et aussi sur mes propres qualités et défauts. Vous avez été présents tous les deux tout au long de ma thèse, et vous ne m'avez pas laissé tomber à une période où d'autres doctorants ont perdu tout contact avec leurs directeurs. Vous avez su me parler dans les moments où j'étais en difficulté, et avez été optimistes pour moi dans les moments où je ne l'étais plus. Vous m'avez toujours communiqué votre envie que je réussisse, et j'ai fini par réussir ! En bref : merci, vous avez carrément géré.

Les autres chercheurs Je tiens à remercier Matthieu Rambaud, qui m'a fait découvrir avec enthousiasme le monde de la recherche il y a maintenant plus de quatre ans, et qui m'offre désormais un avenir dans ce monde : merci d'avoir pris de mes nouvelles pendant ces trois années, et merci de croire en moi. Je remercie également tous les autres chercheurs qui ont répondu à mes questions au cours de cette thèse : Christophe Ritzenthaler, Emmanuel Hallouin, Henri Lombardi... Sur cette liste figure en particulier le regretté Bas Edixhoven, dont une conjecture a inspiré certains des travaux de cette thèse.

Les enseignants et les enseignés La thèse, ce n'est heureusement pas que de la recherche ! Sinon, on deviendrait bien vite bien vieux. Merci à Maxime Wolff pour ses précieux conseils sur la gestion du temps consacré à l'enseignement en début de thèse, à Frédéric Paugam qui m'a permis d'enseigner des choses que je n'aurais jamais cru avoir la chance d'expliquer à qui que ce soit, et à Adrien Deloro pour ses encouragements, mais aussi son humour. Merci enfin à tous les étudiants qui se sont intéressés de près ou de loin aux choses que j'ai eu le plaisir de leur enseigner. J'espère que vous aussi, un jour, aurez la chance d'écrire des remerciements.

Le SdT Je remercie également mes camarades de l'organisation du Séminaire des Thésards. Aux permanents, Romain, Bram et Sébastien, merci pour votre soutien, votre motivation, et vos efforts pour avoir la carte du labo. Aux doctorants, merci pour ces rendez-vous (quasi-)hebdomadaires et ces discussions passionnantes. Raphaël, tu devrais aussi figurer plus bas, mais je te règle ton compte tout de suite : merci pour ta façon d'être franche et sincère, pour ton humour mais aussi ta capacité à survivre à tous ces exposés de géométrie algébrique. Je ne sais pas si tu te souviens d'une conversation qu'on a eue en sortant du 2bis l'hiver dernier : elle m'avait beaucoup rassuré. Antoine S, merci pour ta passion et ton investissement dans le fonctionnement du séminaire, et pour les conversations constructives sur les problèmes qu'on a pu rencontrer dans nos thèses respectives. Arnaud V, merci pour ta bienveillance, et pour le rôle que tu as joué dans mon intégration dans le monde des doctorants il y a maintenant trois ans.

Mes enseignants Faire des mathématiques, c'est avant tout avoir de jolies images en tête. Je tiens à remercier tous ceux qui m'ont fait découvrir ces images, à commencer par Charles Vix et ses belles courbes, ainsi que Pascal Guelfi et ses tôles ondulées. Merci à Gautier Hanna qui m'a emmené à mon premier séminaire il y a déjà plus de six ans. Merci également à Nicolas Perrin qui m'a donné le goût de l'algèbre commutative et la géométrie algébrique, à Mohamed Krir qui m'a appris à faire des calculs concrets sur des courbes (je trouvais ça inutile à l'époque, qu'est-ce que je pouvais être ignorant), et à Benoît Stroh qui m'a donné par son enseignement fantastique l'envie irrésistible de suivre le M2 de Jussieu.

Les doctorants Tout d'abord, je tiens à remercier mes camarades de bureau : Guido, qui est arrivé à Jussieu le même jour que moi et m'a enrôlé dans un groupe de travail quelques jours plus tard, et Arnaud E, qui même après son déménagement est encore venu me parler presque tous les matins pour me faire découvrir des maths fascinantes. Je vous souhaite toute la réussite au monde pour le grand avenir auquel vous êtes promis. La salle de convivialité du cinquième étage a vu passer des dizaines de doctorants pendant ces trois années, et je voudrais tous les remercier pour les conversations intéressantes que nous avons eues. Au début, il y avait la vieille garde : en particulier, Sylvain et ses innombrables histoires de voyages, grand Mathieu et ses conseils avisés sur l'enseignement, Jean-Michel avec sa prononciation soviétique de la lettre h et son goût du poivre... De ma génération, je tiens d'abord à remercier Grace pour son soutien et sa compréhension dans toutes les situations. Des cours de crypto de l'UVSQ à la fin de thèse en passant par l'enseignement à Jussieu, ta présence a toujours été synonyme de joie et de bienveillance. Merci aussi à Haowen, pas seulement pour les découvertes culinaires, mais surtout pour tous les moments de bavardage ! Germain, merci de m'avoir fait réviser le Erlkönig malgré moi, et de m'avoir montré qu'on pouvait trouver partout autour de soi des choses à compter et à appeler machinbidulèdre. Jacques, merci de m'avoir fait découvrir avec ferveur les délires du monde fascinant de la naturopathie ; et même si je ne joue plus à ce jeu, j'ai toujours trouvé une familiarité réconfortante dans tes descriptions des actualités de League of Legends. Maxime, merci de faire une forme de géométrie algébrique que j'ai parfois l'impression de comprendre ! Enfin, merci à tous les autres habitants du couloir pour chaque conversation et chaque rigolade : Xavier, Ilias, Alexandre, Benoît, petit Mathieu, Mahya, Anna F, petit et grand Thomas, Christina, Perla, Thibaut, Thibault,

Vadim, Raphaël, Sebastian, Antoine T, Chenyu, Fabrizio, Gabriel, Mathieu H, Adrien, Anna RS, Eva, Thiago, Nelson.

Les amis d'avant ou d'ailleurs La thèse, c'est beaucoup de travail, et le travail le plus important consiste à survivre à tout ce travail. Merci à vous tous pour chaque soirée, chaque repas, chaque après-midi de jeux, chaque bavardage, chaque message de soutien. Je voudrais rappeler à chacune et chacun d'entre vous un bon souvenir que nous avons partagé pendant ces trois années.

— Ceux de TPS : Alexandra, David, Guillaume et Camille, Issam, Léna... merci de m'avoir intégré à votre groupe d'amis à tel point que je crois moi-même avoir vu J***** danser sur une table du Fouaille après un cocktail champagne-café. D,I,L, vous souvenez de notre pique-nique sur les quais de Seine après la première vague ? Je travaillais à l'époque sur un document détaillant ce qui est maintenant résumé dans l'annexe B.2. A,C,G,I,L, vous vous souvenez de l'anniv de l'une d'entre nous dans un bar en sous-sol, puis un très bon resto avec en dessert une tartine très addictive ? Je travaillais sur la section II.7.2 cette semaine-là.

— Celle qui parle luxembourgeois : Ánh-Lise, merci d'avoir bien voulu rester amie avec un piéton. Merci pour tes mots rassurants il y a un an et demi quand j'étais coincé. Quand on se revoit, rien n'a changé, et c'est génial, et je te remercie pour ça aussi ! Tu te souviens du jour d'hiver où on a pris un café place Stan avec nos mecs ? C'était la dernière année d'insouciance collective. Je travaillais à cette époque sur les algorithmes de décomposition primaire de la section B.2.

— Ceux du DAp : merci à Bertrand et Sylvie, à Stéphane et Magda, ainsi qu'à Tatyana pour leur accueil chaleureux dans un monde qui n'était pas le mien au départ. En plus d'être des gens super sympa, on mange bien avec vous. Vous vous souvenez de la journée chachlik ? Qu'est-ce que c'était bon ! Je travaillais à cette époque de l'année sur la proposition C.3.9.

— Ceux de la L3 : Camille et Florian, et Florian aussi, on ne se voit largement pas autant qu'on s'apprécie, et je voudrais vous remercier pour tous les bons moments passés ensemble. Vous vous souvenez sûrement de nos parties de billard et de mes difficultés à manger un cornet de glace, mais est-ce que vous vous souvenez de la fois où on s'est vus à Longwy il y a maintenant près de trois ans, et vous m'avez bien éclaté à TowerFall ? À cette époque, j'essayais de comprendre les algorithmes de normalisation de l'annexe B.2.

— Celles des vacances mais pas que : Clémence et Mélanie, merci pour toutes les belles soirées de concert, de veille ou de retour de voyage. Est-ce que vous vous souvenez encore du premier midi à La Rochelle ? On avait bu de la Guignette sur la terrasse de notre appart, y avait du soleil et les terrasses venaient de rouvrir après 6 mois de fermeture ! La semaine d'avant, j'avais travaillé sur le contenu de la remarque 5.2.4.

— Ceux avec lesquels on n'a toujours pas joué au Cowboy Bebop : Gauthier et Mathilde, merci pour votre bonne humeur pendant les soirées passées à jouer à des jeux plus ou moins coopératifs. Vous vous souvenez de la dernière fois qu'on s'est vus ? C'était il y a quelques semaines, et en jouant à Galerapagos, Gauthier, tu as dit "Ta Ferrari n'est pas là ?" quand Mathilde a tiré la carte des clés de voiture, et ça a ouvert tout un monde de souvenirs pour moi. À ce moment-là, je travaillais sur une correction de la section III.4.5.

— Ceux qui ont vu naître AK : Gham, Ladié, Sulu, Tris. Merci de m'avoir supporté à l'époque où j'étais insupportable, merci d'être resté en contact ces dernières années, merci pour cette alliance devenue amitié. Vous vous souvenez de notre visio sur Messenger pendant le confinement ? On comparait un peu nos situations, et on était tous un peu dans la même. Je travaillais à l'époque sur la section II.2.1.

— Mes co-stagiaires d'un bel été : Isabella, Sarah, merci d'être toujours aussi vivantes et drôles et gentilles avec moi, et de m'avoir montré comment on finit une thèse. Isa, tu te souviens du jour

très très chaud où on est allés manger des glaces chez Pozzetto avec M et on n'avait pas assez de serviettes et y en avait partout sur la table ? Je venais d'avoir le financement pour la thèse, et vous deux, vous aviez déjà presque survécu à la première année. Je lisais à l'époque un livre sur le contenu du chapitre I. Sarah, tu te souviens de notre conversation derrière le Turing au mois de mai ? Il faisait beau et tu m'as ramené au RER et on était trop contents de s'être revus. J'étais en pleine rédaction de la section IV.1 à ce moment-là.

— Celui qui m'a fait découvrir le goulasch au tofu : Julien, merci d'avoir pris le temps de t'intéresser à ce jeune groupe de stagiaires qui était à Saclay pendant que tu rédigeais ta thèse, et d'avoir été depuis un ami fidèle et une source de très bons conseils cinématographiques. Tu te souviens de la fois où je suis venu te voir à Rennes, et tu m'as emmené dans une crêperie pompeuse avec des verres à vin gigantesques et des vraies serviettes dans les toilettes ? Tu savais que ça retiendrait mon attention, et je me rappelle toute cette journée comme si c'était hier. C'était le dernier jeudi avant le début de mon contrat de thèse, et je lisais à l'époque un livre sur le contenu de la section I.1.3.

— Celui qui met ses courses dans une poche : Marc, merci pour ta gentillesse, ta générosité, pour tous les déplacements que tu as faits pour venir nous voir. Tu te souviens de ta venue en décembre dernier, quand on est tombés par hasard sur une exposition de meubles Prisunic dans le Marais ? La semaine d'avant, j'avais travaillé sans succès sur ce qui est maintenant la section V.3.5.

— Celui que j'ai rencontré derrière un McDo : Marouane, tu es la seule personne qu'on puisse croiser plusieurs fois par hasard dans et autour de la fac, et je te remercie pour cette présence constante et pour toutes nos conversations stimulantes. Tu te souviens de la fois où t'es venu dans mon bureau tôt le matin pour parler de pronostics concernant l'euro de foot ? Je travaillais à l'époque sur la section III.3.4.

— Celles des petits écoliers : Mathilde et Sandrine, merci pour votre gentillesse et votre bienveillance à toute épreuve, pour nos réunions pleines de joie et de bonne humeur. Est-ce que vous vous souvenez de notre pique-nique sur les quais au mois de mai, et de l'embrouille sur les tranches de jambon ? Je rédigeais cette semaine-là la section IV.1.

— Celui qui a tout relu : Pascal, merci infiniment pour cet effort aussi conséquent que désintéressé. Tu te souviens de la fois en octobre 2019 où on s'est vus au Baker Street, et tu m'as donné des conseils précieux pour parler de quelque chose d'important à des gens qui m'importent ? J'essayais à l'époque de comprendre les algorithmes de normalisation évoqués dans l'annexe B.2.

— Le meilleur ami de mon enfance : Pierre, merci pour ton enthousiasme et ton énergie, et pour tout l'allemand que tu as retenu ! Tu te souviens du soir il y a environ un an où on a bu un verre près de la fac, et avant que Nicolas nous rejoigne, c'était la première fois depuis des lustres qu'on se voyait juste tous les deux ? On était assis en terrasse aux Rattrapages, on se racontait nos vies et on était juste super contents. La semaine en question, je travaillais sur l'annexe C.

— Celui qui m'a appris alors que j'étais censé lui apprendre : Quentin C, merci pour ta bonne humeur, ta philosophie, ta générosité. Merci de m'avoir laissé essayer de t'expliquer un peu de maths pendant deux ans, et d'être quand même devenu mon ami ! Tu te souviens de la soirée fin avril où tu nous as apporté une plante et tu m'as bien battu à FIFA ? Cette plante s'appelle maintenant Romy, et elle se porte très bien. Je rédigeais à ce moment-là le chapitre II.

— Celui qui avait un trait vert sur sa télé : Quentin R, merci d'abord pour deux dessins qui figurent dans cette thèse et pour lesquels tu refuses que je te remercie plus que ça. Merci aussi pour ton soutien dans toute cette aventure, et pour tes expressions qui me font toujours bien rigoler. Et puis merci d'être persuadé que je vais réussir quand je suis persuadé que je vais échouer. Tu te souviens encore de ta soutenance il y a un an ? T'avais fait une vidéo pour expliquer aux gens comment accéder à la salle, et c'était vachement bien pensé. C'était un jeudi après-midi, et le matin, j'avais corrigé des choses dans la section IV.4.

— Celui qui a connu Tigre Bois : Thomas, il y a tellement de choses pour lesquelles je dois te remercier dans ma vie que je ne vais pas tout étaler ici. Mais bien sûr, merci pour ton soutien presque quotidien, merci pour ta gentillesse, et merci de ne pas trop mal supporter les buts marqués au premier poteau. Est-ce que tu te souviens du vendredi soir juste avant mon déménagement, il y a un peu plus d'un an et demi ? J'étais très stressé parce que ma thèse n'avançait pas, et tu avais fait ton possible pour me rassurer. Ce jour-là, je me cassais les dents sur la suite de la section V.3.3.

— Celui que je n'ai pas vu, mais entendu, et que je veux remercier quand même : Tristan, merci d'être plus jeune et en même temps plus et moins sage que moi ! Un jour, on visitera le château de Fougeret ensemble.

— Celui que je n'ai ni vu, ni entendu, mais lu, et qui aime le BK même si ce dernier devient un peu décevant : Rodolphe, merci pour ta bienveillance en toute circonstance, et merci de me rappeler fréquemment des souvenirs qui risqueraient de disparaître de nos mémoires si on ne les réactivait pas de temps en temps.

— Ceux avec lesquels on n'a pas trop parlé de la thèse mais que je veux citer quand même, et avec chacun desquels on a fait au moins une raclette que je veux leur rappeler : merci à Kevin et Romain, à Martial et Tiago, à Thibault et Yann pour les belles soirées.

La famille J'en ai une géniale. C'est trop privé, je n'en dirai pas plus sur le sujet !

Le meilleur pour la fin Nicolas, merci pour tout ce qu'il y a de beau dans la vie ; ça y est, j'ai fini aussi, et je n'y serais pas arrivé sans toi.

Table des matières

Introduction **xiii**

I Cohomologie étale et groupe fondamental **1**
I.1 Morphismes étales et groupe fondamental . . . 1
I.2 Le topos étale . . . 4
I.3 Torseurs, H^1 et fibrés en droites . . . 9
I.4 Groupe fondamental et faisceaux lisses . . . 11
I.5 Les grands théorèmes . . . 15
I.6 Cohomologie à support dans un fermé . . . 18
I.7 Cohomologie à support compact . . . 19
I.8 Formule des traces et comptage de points . . . 20

II Revêtements et cohomologie des courbes **21**
II.1 Groupe fondamental des courbes . . . 21
II.2 Groupe de Picard et variété jacobienne . . . 27
II.3 Groupe de Picard des courbes nodales . . . 30
II.4 Cohomologie des faisceaux constants sur les courbes . . . 34
II.5 Cohomologie à support dans un fermé . . . 41
II.6 Revêtements cycliques de courbes . . . 44
II.7 Un revêtement caractéristique . . . 48

III Algorithmique des faisceaux constructibles **57**
III.1 Faisceaux lisses . . . 57
III.2 Images directes de faisceaux lisses . . . 59
III.3 Faisceaux constructibles sur les courbes lisses . . . 61
III.4 Opérations sur les faisceaux dans la représentation ($\sqcup$) . . . 68
III.5 Un exemple détaillé . . . 74
III.6 Faisceaux constructibles sur les courbes nodales . . . 75
III.7 Constructions sur les surfaces . . . 76

IV Calculabilité de la cohomologie et algorithmes existants **79**
IV.1 Calculabilité : l'algorithme de Madore et Orgogozo . . . 79
IV.2 L'algorithme de Couveignes . . . 86
IV.3 L'algorithme de Huang et Ierardi . . . 88
IV.4 L'algorithme de Jin . . . 96
IV.5 Aspects pratiques . . . 105

V Calcul effectif de la cohomologie **107**
V.1 Scindage explicite des suites exactes courtes . . . 109

V.2 Faisceaux constants sur les courbes affines . . . 109
V.3 Cohomologie des faisceaux lisses . . . 113
V.4 Cup-produits dans la cohomologie des faisceaux lisses . . . 124
V.5 Cohomologie des faisceaux constructibles : calcul du H^1 . . . 127
V.6 Calcul de $\mathrm{R}\Gamma(X,-)\colon \mathrm{D}^b_c(X,\Lambda) \to \mathrm{D}^b_c(\Lambda)$ . . . 128

VI Cohomologie des surfaces **139**
VI.1 Pinceaux de Lefschetz . . . 139
VI.2 Trivialisation des images directes dérivées . . . 140
VI.3 Calcul de la cohomologie de μ_n sur une surface . . . 141
VI.4 Algorithme et indications sur le calcul de sa complexité . . . 144

VII Problèmes ouverts **147**

Annexes **148**

A Corps calculables **149**
A.1 Corps calculables et complexité . . . 149
A.2 Polynômes . . . 151
A.3 Extensions de corps . . . 153

B Schémas de type fini sur un corps **157**
B.1 Schémas et morphismes . . . 157
B.2 Bases de Gröbner et applications . . . 158
B.3 Construction de familles d'hyperplans . . . 159
B.4 Recherche de points . . . 161
B.5 Restriction de Weil . . . 164

C Algorithmique des courbes **167**
C.1 Représentations des courbes lisses . . . 167
C.2 Produit fibré de courbes intègres lisses . . . 171
C.3 Diviseurs et espaces de Riemann-Roch . . . 172
C.4 Fonction zêta et comptage de points . . . 176

Bibliographie **179**

Introduction

Contexte

Cette thèse porte sur des méthodes explicites de calcul de groupes de cohomologie étale. Les prérequis à la compréhension de cette introduction et de la suite du manuscrit sont présentées dans le chapitre I. Soit n un entier. Soit k un corps de caractéristique première à n. Les catégories dérivées des faisceaux de $\Lambda \coloneqq \mathbb{Z}/n\mathbb{Z}$-modules sur les k-schémas de type fini sont munies des six opérations $f^\star$, $\mathrm{R}f_\star$, $\mathrm{R}f_!$, $\mathrm{R}f^!$, $\otimes^L_\Lambda$, $\mathrm{R}\underline{\mathrm{Hom}}_\Lambda$ définies par Grothendieck. La condition raisonnable de finitude sur les faisceaux est la constructibilité : un faisceau de Λ-modules sur un schéma noethérien X est dit constructible si X admet une stratification telle que le faisceau soit un système local sur chaque strate. Les faisceaux constructibles sont les objets noethériens de la catégorie des faisceaux de Λ-modules sur X. Un résultat majeur dû à Grothendieck, Artin, Deligne et plus récemment Gabber pour la formulation la plus générale [ILO, XIII, Th. 1.1.1], affirme que pour des schémas noethériens quasi-excellents sur lesquels n est inversible, la constructibilité est stable par les six opérations.

Supposons k algébriquement clos. Soit X un schéma de type fini sur k. Le résultat précédent implique que pour tout faisceau constructible $\mathcal{F}$ de Λ-modules sur X, les groupes de cohomologie $\mathrm{H}^i(X, \mathcal{F})$ sont finis. De plus, ils sont nuls dès que $i > 2\dim X$. Un morphisme $f\colon Y \to X$ de k-schémas induit par fonctorialité un morphisme $\mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(Y, f^\star\mathcal{F})$. De même, si X provient par changement de base d'un schéma sur un sous-corps parfait k_0, $\mathrm{R}\Gamma(X, \mathcal{F})$ est muni d'une action de $\mathrm{Gal}(k|k_0)$. À défaut de pouvoir calculer les six opérations explicitement, un objectif atteignable est le calcul d'un complexe représentant $\mathrm{R}\Gamma(X, \mathcal{F})$, ou au moins des groupes $\mathrm{H}^i(X, \mathcal{F})$, d'une façon qui permette de représenter ces morphismes de fonctorialité. Si X est une courbe projective lisse connexe et $\mathcal{F}$ est constant, les groupes $\mathrm{H}^i(X, \mathcal{F})$ sont bien connus ; en particulier, $\mathrm{H}^1(X, \mu_n)$ est le groupe des points de n-torsion de la variété jacobienne de X. Si X est de dimension $d > 1$, les deux techniques de calcul usuelles procèdent par fibration et récurrence sur la dimension. D'une part, pour les variétés projectives, un pinceau de Lefschetz permet d'obtenir une fibration

$$\tilde{X} \to \mathbb{P}^1$$

où $\tilde{X}$ est un éclatement de X. D'autre part, les bons voisinages d'Artin permettent d'obtenir une fibration en courbes affines

$$X \to X_{d-1} \to \cdots \to X_1$$

où X_i est de dimension i. Si les suites spectrales associées à ces fibrations permettent assez rapidement de majorer le rang des $\mathrm{H}^j(X, \mathcal{F})$, voire le calculer pour des petites valeurs de j, elles ne fournissent

toutefois pas immédiatement une description de ces groupes permettant de calculer les morphismes de fonctorialité évoqués ci-dessus.

La calculabilité des groupes $\mathrm{H}^i(X, \Lambda)$ a été démontrée par Poonen, Testa et van Luijk en 2015 dans le cas où k est de caractéristique nulle [PTv15, Th. 7.9]. Une preuve en caractéristique quelconque a été donnée quelques mois plus tard par Madore et Orgogozo [MO15, Th. 0.1]. Ces deux articles décrivent en détail des algorithmes permettant effectivement de calculer les $\mathrm{H}^i(X, \mathbb{Z}/n\mathbb{Z})$, mais ne donnent pas de borne sur le nombre d'opérations effectuées par ces algorithmes, qui paraissent en outre trop inefficaces pour être utilisés dans la pratique. À l'autre bout du spectre, Huang et Ieradi [HI98, Th. 1] et plus tard Couveignes [Cou09, Th. 1] ont décrit des algorithmes calculant explicitement des classes de diviseurs sur une courbe projective lisse formant une base de la n-torsion de la jacobienne de cette courbe, avec des bornes de complexité très précises. Nous nous sommes intéressés au calcul du foncteur $\mathrm{R}\Gamma(X, -)$, lorsque X est une courbe lisse ou nodale, et donnons des bornes explicites sur la complexité du calcul.

Lorsque X provient par changement de base d'un corps fini $\mathbb{F}_q$, le calcul des $\mathrm{H}^i(X, \Lambda)$ permet également, par l'intermédiaire de la formule des traces, de compter les $\mathbb{F}_q$-points de X. En particulier, un algorithme de calcul de $\mathrm{H}^i(X, \Lambda)$ de complexité polynomiale en n et $\log q$ permet de calculer le cardinal de $X(\mathbb{F}_q)$ en un nombre d'opérations polynomial en $\log q$. Dans le cas où X est une courbe, l'algorithme probabiliste de Huang et Ierardi atteint cette complexité. Dans le cas où X est une surface, l'existence d'un tel algorithme a été conjecturée par Couveignes et Edixhoven dans [EC11, Epilogue] ; il y est suggéré d'employer une fibration de Lefschetz. Une grande partie du travail de cette thèse a été motivée par cette conjecture.

Contributions

Soient k_0 un corps parfait et k une clôture algébrique de k_0. Soit n un entier premier à la caractéristique de k. Notons Λ l'anneau $\mathbb{Z}/n\mathbb{Z}$. Soit X_0 une courbe lisse géométriquement intègre sur k_0. Notons $X = X_0 \times_{k_0} k$.

Représentations des faisceaux constructibles sur les courbes Nous décrivons trois représentations algorithmiques possibles des faisceaux constructibles sur X : par les générateurs ou cogénérateurs classiques de la catégorie des faisceaux constructibles, et par recollement relativement à un ouvert de lissité. Nous décrivons des algorithmes (de complexité élémentaire en les entrées) permettant de passer d'une représentation à une autre. Pour la représentation par recollement, qui est la plus adaptée aux calculs de cohomologie effectués par la suite, nous présentons des algorithmes calculant les opérations suivantes sur les faisceaux :

- noyau et conoyau de morphismes ;
- somme directe, produit tensoriel, Hom interne ;
- tiré en arrière, poussé en avant par des morphismes entre courbes lisses.

Nous adaptons également cette représentation par recollement au cas des courbes nodales.

Construction de revêtements galoisiens de courbes Nous montrons comment, à partir d'un algorithme calculant la n-torsion de la jacobienne de la compactification lisse de la normalisée de X, calculer explicitement un revêtement caractéristique X_2 de X de groupe $\mathrm{H}^1(X, \Lambda)^\vee$, ainsi qu'un revêtement caractéristique de X_0 de groupe $\mathrm{H}^1(X_0, \Lambda)^\vee$. Nous construisons également, à partir de X_2, un revêtement caractéristique $X_{2,0}$ de X_0 tel que $X_{2,0} \times_{k_0} k \to X$ trivialise les Λ-torseurs sur X. Une adaptation de ces constructions au cas des courbes nodales est également présentée. La notation X_2 trouve son origine dans le fait que lorsque n est un nombre premier ℓ, le revêtement $X_2 \to X$ correspond au quotient du complété pro-ℓ de $\pi_1(X)$ par le groupe numéro 2 de la série de Frattini descendante (pour plus de détails, voir [MO15, §3.1]).

Calculabilité de la cohomologie sur les variétés Après l'avoir passé en revue, ainsi que d'autres algorithmes de calcul de la cohomologie, nous montrons que l'algorithme de Madore et Orgogozo, qui calcule les groupes de cohomologie d'un faisceau constant sur un schéma de type fini sur k, est de complexité primitivement récursive dès que le schéma en entrée est lisse.

Cohomologie des faisceaux constructibles sur les courbes Soit $\mathcal{F}_0$ un faisceau constructible de Λ-modules sur X_0, lisse sur un ouvert affine non vide U_0, de complémentaire fermé réduit Z_0. Notons M sa fibre générique géométrique. Notons X, U, Z, V les changements de base respectifs de X_0, U_0, Z_0, V_0 à k et $\mathcal{F} = (\mathcal{F}_0)|_X$. Soit $V \to U$ un revêtement (étale connexe) galoisien trivialisant $\mathcal{F}|_U$. Soit $V_2 \to V$ le revêtement décrit ci-avant. Nous décrivons des méthodes efficaces de calcul de ces différents objets et du groupe $G \coloneqq \mathrm{Aut}(V_2|U)$. La courbe affine U est un $K(\pi, 1)$: la cohomologie de $\mathcal{F}$ sur U est la cohomologie galoisienne du $\pi_1(U)$-module M. Notons $C^{12}(G, M)$ le groupe des morphismes croisés $G \to M$.

Proposition a. (5.3.1) Le morphisme canonique

$$[M \to C^{12}(G, M)] = \tau_{\leqslant 1} \mathrm{R}\Gamma(G, M) \to \mathrm{R}\Gamma(U, \mathcal{F})$$

est un quasi-isomorphisme.

Pour chaque point $z \in Z$, notons I_z le groupe d'inertie d'un point de la compactification lisse de V_2 au-dessus de z, et P_z le groupe d'inertie sauvage correspondant. Soit $\phi_z \colon \mathcal{F}_z \to M^{I_z} \subseteq M^{P_z} \xrightarrow{\sim} M_{P_z}$ le morphisme de recollement en z composé avec l'isomorphisme canonique $M^{P_z} \xrightarrow{\sim} M_{P_z}$. Ici, les indices (resp. exposants) désignent les modules des coinvariants (resp. invariants) sous les groupes en question, et l'isomorphisme $M^{P_z} \xrightarrow{\sim} M_{P_z}$ associe à un élément de M invariant sous P_z sa classe dans le quotient M_{P_z}. Le morphisme ϕ_z fait partie des données définissant $\mathcal{F}$. Nous construisons dans le lemme 2.1.15 une section au morphisme d'inflation $C^{12}(I_z/P_z, M^{P_z}) \to C^{12}(I_z, M)$.

Théorème b. (5.0.1) Le cône du morphisme de complexes suivant représente $\mathrm{R}\Gamma(X, \mathcal{F})[1]$.

$$\begin{tikzcd}
M \oplus \bigoplus_{z \in Z} \mathcal{F}_z \arrow[r, "(\partial_G, 0)"] \arrow[d, "\bigoplus_{z \in Z} (\mathrm{id} - \phi_z)"] & C^{12}(G, M) \arrow[r] \arrow[d, "\bigoplus_z \mathrm{res}^G_{I_z}"] & \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
\bigoplus_{z \in Z} M_{P_z} \arrow[r, "\bigoplus_z \partial_{I_z}"] & \bigoplus_{z \in Z} C^{12}(I_z/P_z, M_{P_z}) \arrow[r] & \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] & 0
\end{tikzcd}$$

Lorsque V provient de k_0, le complexe obtenu est naturellement muni d'une action de $\mathrm{Gal}(k|k_0)$. Nous donnons également une variante de ce résultat permettant, à partir de la donnée d'un revêtement $V_0 \to U_0$ qui trivialise $\mathcal{F}_0$, de calculer l'action de $\mathrm{Gal}(k|k_0)$ sur $\mathrm{R}\Gamma(X, \mathcal{F})$. De plus, nous adaptons ce résultat au calcul de $\mathrm{R}\Gamma(X, \mathscr{K})$, où $\mathscr{K}$ est un complexe de faisceaux constructibles. Enfin, lorsque $k_0 = \mathbb{F}_q$, nous étudions la complexité de l'algorithme construisant ce complexe, basé sur des algorithmes existants de calcul de points de n-torsion dans la jacobienne d'une courbe.

Théorème c. (5.6.3) Notons g le genre de X, et r le nombre de points à l'infini de U. Soit d le degré de $V \to U$. Soit m un entier tel que M et les fibres de $\mathcal{F}$ en les points de $X - U$ soient des quotients de Λ^m. Il existe un algorithme probabiliste (Las Vegas) qui calcule un complexe de $\Lambda[\mathrm{Gal}(k|k_0)]$-modules représentant $\mathrm{R}\Gamma(X, \mathcal{F})$ en

$$\mathcal{P}(d, g, n, r, m, \log q)^{2^{O(d(g+r))}}$$

opérations dans $\mathbb{F}_q$, où $\mathcal{P}$ est un polynôme. Si V admet un modèle plan à singularités ordinaires de degré $O(g)$, cette complexité devient

$$\mathcal{P}(d, g, n, r, m, \log q)^{O\left((d(g+r))^2\right)}.$$

Calcul de cup-produits Supposons X projective de genre non nul. Soit $Y \to X$ un revêtement galoisien de X de degré divisible par n. Nous donnons une description alternative du H^2 d'un faisceau lisse sur X qui permet de calculer les cup-produits $\mathrm{H}^1 \times \mathrm{H}^1 \to \mathrm{H}^2$. Soient Y_2 le revêtement de Y de groupe $\mathrm{H}^1(Y, \Lambda)^\vee$, et Y_3 le revêtement de Y_2 de groupe $\mathrm{H}^1(Y_2, \Lambda)^\vee$. Notons $G_2 = \mathrm{Aut}(Y_2|X)$ et $G_3 = \mathrm{Aut}(Y_3|X)$.

Proposition d. (5.4.1) Pour tout faisceau lisse $\mathcal{F}$ de Λ-modules sur X trivialisé par Y de fibre M, le morphisme

$$\mathrm{im}(\mathrm{H}^2(G_2, M) \to \mathrm{H}^2(G_3, M)) \to \mathrm{H}^2(\pi_1(X), \mathcal{F})$$

est un isomorphisme.

Théorème e. (5.4.4) Soient $\mathcal{F}$ et $\mathcal{G}$ deux faisceaux lisses de Λ-modules sur X trivialisés par Y, de fibres respectives M et N. Le cup-produit

$$\mathrm{H}^1(X, \mathcal{F}) \times \mathrm{H}^1(X, \mathcal{G}) \to \mathrm{H}^2(X, \mathcal{F} \otimes \mathcal{G})$$

est réalisé par la composée

$$\mathrm{H}^1(G_2, M) \times \mathrm{H}^1(G_2, N) \xrightarrow{\cup} \mathrm{H}^2(G_2, M \otimes N) \to \mathrm{im}(\mathrm{H}^2(G_2, M \otimes N) \to \mathrm{H}^2(G_3, M \otimes N)).$$

Cohomologie des faisceaux constants sur les surfaces En appliquant la procédure prévue dans [EC11, Epilogue], nous indiquons comment appliquer les algorithmes précédents au calcul de la cohomologie de Λ sur une surface projective lisse sur k fibrée sur $\mathbb{P}^1$ par un pinceau de Lefschetz.

Organisation du manuscrit

Le chapitre I rappelle les définitions et théorèmes célèbres de la cohomologie étale. Il permettra au lecteur peu familier avec ces notions de trouver l'ensemble des résultats utilisés dans la suite du manuscrit, et pourra aisément être laissé de côté par le lecteur expert.

Le chapitre II recense des résultats classiques sur la cohomologie et les revêtements des courbes lisses, et leurs analogues moins connus concernant les courbes nodales. En particulier, il contient la construction et l'étude d'un revêtement caractéristique utilisé dans la suite.

Le chapitre III est consacré à la description des diverses représentations explicites des faisceaux constructibles de groupes abéliens sur une courbe lisse ou nodale, ainsi qu'aux algorithmes servant à passer d'une représentation à une autre. Nous y décrivons un certain nombre d'opérations sur ces faisceaux dans une représentation par recollement relativement à un ouvert de la courbe sur lequel le faisceau est lisse.

Les algorithmes existants pour le calcul de la cohomologie sont décrits dans le chapitre IV. Tout d'abord, nous résumons l'algorithme de Madore et Orgogozo qui calcule la cohomologie d'un faisceau sur une variété quelconque, et montrons qu'il est primitivement récursif dans le cas particulier des variétés lisses. L'algorithme de Huang et Ierardi et l'algorithme de Couveignes permettent de calculer la cohomologie d'un faisceau constant sur une courbe projective lisse ; nous expliquons comment adapter l'un et l'autre au calcul de la division par n dans le groupe de Picard de la courbe. Ces deux algorithmes serviront de base à nos méthodes de calcul. Enfin, nous décrivons la méthode de Jin servant à calculer la cohomologie d'un faisceau lisse sur une courbe lisse.

Nous présentons dans le chapitre V des méthodes de calcul de la cohomologie des faisceaux constructibles sur une courbe X lisse ou nodale. Le cas le plus simple, traité en premier, est celui des faisceaux constants, qui se résume à des calculs dans la jacobienne de la (compactification lisse de la normalisation de la) courbe. Vient ensuite le cas des faisceaux lisses, qui se ramène à des calculs de cohomologie galoisienne. Une section est alors consacrée aux calculs de cup-produits dans la cohomologie de ces

faisceaux. Enfin, le calcul de la cohomologie des faisceaux constructibles et des complexes d'iceux s'effectue par recollement, en s'appuyant sur le cas des faisceaux lisses. Nos résultats fournissent un calcul explicite du foncteur

$$\mathrm{R}\Gamma(X, -)\colon \mathrm{D}_c^b(X, \mathbb{Z}/n\mathbb{Z}) \to \mathrm{D}_c^b(\mathbb{Z}/n\mathbb{Z})$$

où n est un entier inversible sur X. Tous ces calculs sont fonctoriels en X et en le faisceau étudié ; nous donnons des bornes de complexité précises sur les algorithmes présentés.

Le chapitre VI est dédié au calcul de la cohomologie des surfaces projectives lisses. Nous montrons comment la méthode classique de fibration en courbes au moyen d'un pinceau de Lefschetz peut être utilisée en conjonction avec nos algorithmes sur les courbes pour calculer la cohomologie d'un faisceau constant sur une surface, et ainsi compter les points sur cette surface si elle provient d'un corps fini.

Les annexes contiennent des compléments de nature algorithmique. L'annexe A fournit des précisions sur les différentes classes de complexité ainsi que sur la notion de corps calculable, et rappelle la complexité des opérations classiques dans les anneaux de polynômes. L'annexe B détaille la représentation des variétés algébriques utilisée par les algorithmes, et résume les opérations classiques en géométrie algébrique effective. Enfin, les algorithmes spécifiques aux courbes ainsi que leur complexité sont présentés dans l'annexe C.

CHAPITRE I

Cohomologie étale et groupe fondamental

Ce premier chapitre recense les définitions des objets manipulés par la suite, ainsi que les principaux résultats de la cohomologie étale utilisés dans la suite de ce texte. Afin de rendre la lecture plus abordable et citer plus rapidement des théorèmes importants, ces résultats ne sont pas présentés dans l'ordre habituel de leur démonstration. Le lecteur averti pourra passer directement au chapitre suivant.

Nous supposons connus les résultats classiques d'algèbre homologique, en particulier la construction des catégories et foncteurs dérivés. Une introduction brève et efficace à ces notions se trouve dans [Tho01], et une introduction plus complète dans [Yek19].

Avertissement Dans ce chapitre, le terme *schéma* signifiera *schéma noethérien*. Tous les schémas rencontrés dans la suite de cette thèse seront effectivement noethériens.

I.1 Morphismes étales et groupe fondamental

I.1.1 Morphismes étales

Définition 1.1.1. Un morphisme de schémas $f\colon Y \to X$ est dit étale en un point y de Y s'il est plat et non ramifié en y. Il est dit étale s'il est étale en tout point de Y. Nous noterons $X_{\text{ét}}$ la catégorie dont les objets sont les couples (Y, f) où $f\colon Y \to X$ est un morphisme étale, et les morphismes $(Y, f) \to (Y', f')$ sont les morphismes de schémas $\phi\colon Y \to Y'$ tels que $f' \circ \phi = f$. Nous noterons Fét_X la sous-catégorie de $X_{\text{ét}}$ formée des X-schémas finis étales, appelés revêtements étales.

Exemple 1.1.2.

1. Toute immersion ouverte est étale.
2. L'immersion d'un fermé strict d'un schéma connexe n'est jamais étale.
3. Soient A un anneau et $h \in A[t]$. Soit $g \in A[t]$ un polynôme unitaire tel que g' soit inversible dans $A[t, h^{-1}]/(g)$. Alors le morphisme

$$\operatorname{Spec} A[t, h^{-1}]/(g) \to \operatorname{Spec} A$$

est étale. Un morphisme de cette forme est appelé morphisme étale standard.

4. Si k'/k est une extension galoisienne de corps et X est un schéma sur k alors le morphisme $X_{k'} \to X$ est étale.
5. Si k est un corps et n est un entier inversible dans k, l'endomorphisme de $\mathbb{G}_m = \operatorname{Spec} k[t, t^{-1}]$ défini par $t \mapsto t^n$ est étale.
6. Si E est une courbe elliptique sur un corps k et n est un entier inversible dans k alors la multiplication par n est un endomorphisme étale de E.
7. Le morphisme $\operatorname{Spec} k[x, y]/(y - x^2) \to \operatorname{Spec} k[y]$ donné par $(x, y) \mapsto y$ est plat, mais ramifié au point $(0, 0)$.
8. Soit $X = \operatorname{Spec} k[x, y]/(y^2 - x^2(x + 1))$ la cubique nodale, et soit $\nu\colon \mathbb{A}^1 \to X$ le morphisme de normalisation donné par $t \mapsto (t^2 - 1, t^3 - t)$. Le morphisme ν est non ramifié dès que la caractéristique de k est différente de 3, mais n'est pas plat.

Il existe de nombreuses caractérisations équivalentes de l'étalitude d'un morphisme (voir p. ex. [Stacks, 02GU]). L'une des plus explicites est la suivante.

Proposition 1.1.3. Soit $f\colon Y \to X$ un morphisme de schémas. Le morphisme f est étale en $y \in Y$ si et seulement s'il existe un ouvert affine $V = \operatorname{Spec} B$ de Y contenant y, un ouvert affine $U = \operatorname{Spec} A$ de X contenant $f(y)$ et une présentation

$$A = B[x_1 \dots x_n]/(f_1 \dots f_n)$$

tels que $\det(\partial f_i/\partial x_j) \in B_y^\times$.

L'étalitude d'un morphisme de variétés a une interprétation géométrique très simple.

Proposition 1.1.4. [Mil13, Prop. 2.9] Soit $f\colon Y \to X$ un morphisme de variétés sur un corps algébriquement clos k. Le morphisme f est étale si et seulement si, pour chaque point fermé y de Y, le morphisme induit entre les cônes tangents $\mathrm{TC}_{f(y)} X \to \mathrm{TC}_y Y$ est un isomorphisme.

Voici quelques propriétés classiques des morphismes étales.

Proposition 1.1.5. [Stacks, 02GN,02GO,03WT]

1. Un morphisme étale est ouvert.
2. La composée de morphismes étales est étale.
3. Tout changement de base d'un morphisme étale est étale.
4. Soient $f\colon Y \to X$ et $g\colon X \to S$ des morphismes de schémas. Si g et $g \circ f$ sont étales alors f l'est également.

I.1.2 Revêtements galoisiens

Définition 1.1.6. Soit X un schéma connexe. Un revêtement galoisien de X est un morphisme fini étale $f\colon Y \to X$, où Y est connexe, tel que le groupe d'automorphismes $\operatorname{Aut}(Y|X)$ agisse transitivement sur les fibres géométriques de f.

Remarque 1.1.7. Comme un morphisme fini est fermé et un morphisme étale est ouvert, tout revêtement galoisien d'un schéma connexe est surjectif.

Le lemme suivant montre en quoi cette notion généralise celle d'extension galoisienne de corps ; en particulier, une extension finie k'/k est galoisienne si et seulement si le morphisme $\operatorname{Spec} k' \to \operatorname{Spec} k$ est un revêtement galoisien.

Lemme 1.1.8. [Stacks, 03SF] Un morphisme fini étale de schémas $f\colon Y \to X$ est galoisien si et seulement si le groupe $\mathrm{Aut}(Y|X)$ est d'ordre $\deg(f)$.

Comme pour les extensions de corps, il y a une notion de clôture galoisienne.

Définition 1.1.9. Soit $f\colon Y \to X$ un morphisme fini étale, où X est un schéma connexe. Un morphisme $g\colon Z \to Y$ tel que la composée $Z \to X$ soit un revêtement galoisien est appelé clôture galoisienne de f si tout autre X-morphisme d'un revêtement galoisien de X vers Y se factorise par g.

$$\begin{tikzcd} Z \arrow[r, "g"] & Y \arrow[r] & X \\ & M \arrow[ul, dashed, "\exists!"] \arrow[u] \arrow[ur, "\mathrm{gal}"'] & \end{tikzcd}$$

Proposition 1.1.10. [Sza09, Prop. 5.3.9] La clôture galoisienne existe et est unique à isomorphisme près ; si $\bar{x}$ est un point géométrique de X, de préimages les points géométriques $\bar{y}_1, \ldots, \bar{y}_d$ de Y, la clôture galoisienne de f est la composante connexe dans $Y \times_X \cdots \times_X Y$ (d facteurs) de $(\bar{y}_1, \ldots, \bar{y}_d)$.

I.1.3 Groupe fondamental

Soit X un schéma connexe. Soit $\bar{x}$ un point géométrique de X. Rappelons que $\mathrm{Fét}_X$ désigne la catégorie des X-schémas finis étales.

Définition 1.1.11. Le groupe fondamental $\pi_1(X, \bar{x})$ de X en $\bar{x}$ est le groupe des automorphismes du foncteur fibre $\mathrm{Fib}_{\bar{x}}\colon \mathrm{Fét}_X \to \mathrm{Set}, Y \mapsto Y_{\bar{x}}$.

Considérons la catégorie cofiltrante $I_{X,\bar{x}}$ des couples $(f_Y\colon Y \to X, \bar{y})$, où $f_Y\colon Y \to X$ est un revêtement galoisien (connexe) et y est un point géométrique de Y vérifiant $\bar{x} = f_Y \circ \bar{y}$. Un morphisme de tels couples est un morphisme de X-schémas compatible avec les points géométriques.

Proposition 1.1.12. [Sza09, Prop. 5.4.6] Le foncteur $\mathrm{Fib}_{\bar{x}}$ est pro-représenté par $\lim_{Y \in I_{X,\bar{x}}^{\mathrm{op}}} Y$, c'est-à-dire que pour tout X-schéma étale $Z \to X$, le morphisme

$$\begin{array}{rcl} \mathrm{colim}_{(f_Y, \bar{y}) \in I_{X,\bar{x}}^{\mathrm{op}}} \mathrm{Hom}_X(Y, Z) & \longrightarrow & \mathrm{Fib}_{\bar{x}}(Z) \\ f & \longmapsto & f(\bar{y}) \end{array}$$

est un isomorphisme. Le groupe $\pi_1(X, \bar{x})$ est isomorphe à $\lim_{(Y,\bar{y}) \in I_{X,\bar{x}}^{\mathrm{op}}} \mathrm{Aut}(Y|X)^{\mathrm{op}}$. C'est en particulier un groupe profini.

Lemme 1.1.13. Soit $(Y, \bar{y})$ un objet de $I_{X,\bar{x}}$. Il y a une suite exacte de groupes profinis :

$$1 \to \pi_1(Y, \bar{y}) \to \pi_1(X, \bar{x}) \to \mathrm{Aut}(Y|X)^{\mathrm{op}} \to 1.$$

Démonstration. Pour tout $(Y', \bar{y}') \in I_{Y,\bar{y}}$, la clôture galoisienne de $Y' \to X$ se factorise par $Y' \to Y$. Par conséquent, si J désigne la sous-catégorie de $I_{Y,\bar{y}}$ des $(Y', \bar{y}')$ tels que $Y' \to X$ soit galoisienne, $\pi_1(Y, \bar{y})$ est encore isomorphe à $\lim_{(Y',\bar{y}') \in J^{\mathrm{op}}} \mathrm{Aut}(Y'|Y)^{\mathrm{op}}$. Comme J est encore une sous-catégorie de $I_{X,\bar{x}}$, ceci définit une injection $\pi_1(Y, \bar{y}) \to \pi_1(X, \bar{x})$, qui est le noyau de $\pi_1(X, \bar{x}) \to \mathrm{Aut}(Y|X)^{\mathrm{op}}$. $\square$

Le théorème central de la théorie de Galois-Grothendieck est le suivant.

Théorème 1.1.14. [Sza09, Th. 5.4.2] Le foncteur $\mathrm{Fib}_{\bar{x}}$ induit une équivalence entre $\mathrm{Fét}_X$ et la catégorie des ensembles finis munis d'une action à gauche continue de $\pi_1(X, \bar{x})$. Cette équivalence fait correspondre les revêtements galoisiens de X aux quotients finis de $\pi_1(X, \bar{x})$.

Exemple 1.1.15. 1. Soit k_0 un corps. Soit k_0^{sep} une clôture séparable de k_0. Notons $\bar{\eta}$ le point géométrique correspondant de $\operatorname{Spec} k_0$. Alors

$$\pi_1(\operatorname{Spec} k_0, \bar{\eta}) = \operatorname{Gal}(k_0^{\mathrm{sep}}|k_0).$$

2. Soit k un corps algébriquement clos de caractéristique nulle. Alors il n'y a pas de revêtement étale non trivial de $\mathbb{A}_k^n$, et

$$\pi_1(\mathbb{A}_k^n, \bar{\eta}) = \pi_1(\mathbb{P}_k^n, \bar{\eta}) = 0.$$

De même qu'en topologie, le choix du point-base $\bar{x}$ est indispensable à la fonctorialité de π_1. Soit $f\colon Y \to X$ un morphisme de schémas connexes. Soit $\bar{y}$ un point géométrique de Y d'image $\bar{x}$. Notons $B_{Y\to X} = - \times_X Y\colon \text{Fét}_X \to \text{Fét}_Y$ le foncteur de changement de base. Alors $\mathrm{Fib}_{\bar{x}} = \mathrm{Fib}_{\bar{y}} \circ B_{Y\to X}$, ce qui induit un morphisme de groupes $f_\star\colon \pi_1(Y, \bar{y}) \to \pi_1(X, \bar{x})$. Tout comme en topologie, le point-base n'a aucune influence sur la structure du groupe fondamental.

Proposition 1.1.16. [Sza09, Cor. 5.5.2] Soit $\bar{x}'$ un autre point géométrique de X. Il y a un isomorphisme $\pi_1(X, \bar{x}) \to \pi_1(X, \bar{x}')$, unique à un automorphisme intérieur de $\pi_1(X, \bar{x})$ près.

Nous pourrons donc nous permettre l'abus de notation consistant, lorsque X est intègre, à noter $\pi_1(X)$ le groupe $\pi_1(X, \bar{\eta})$, où $\bar{\eta}$ est un point générique géométrique de X. Dans le cas où X est de surcroît normal, le groupe $\pi_1(X)$ est le groupe de Galois d'une extension de son corps des fonctions.

Proposition 1.1.17. [Sza09, Prop. 5.4.9] Soit X un schéma normal intègre de corps des fonctions K. Soient $\bar{\eta} = \operatorname{Spec} \bar{K} \to X$ un point générique géométrique de X, et K^{sep} la clôture séparable de K dans $\bar{K}$. Désignons par K_X la composée dans K^{sep} des sous-extensions L/K telles que la normalisation de X dans L soit étale sur X. Alors K_X est une extension galoisienne de K, et le groupe $\operatorname{Gal}(K_X|K)$ est canoniquement isomorphe à $\pi_1(X, \bar{\eta})$.

Théorème 1.1.18. [SGA1, IX, Th. 6.1] Soient k_0 un corps, et k une clôture algébrique de k_0. Soit k_0^{sep} la clôture séparable de k_0 dans k. Soit X_0 un k_0-schéma de type fini géométriquement intègre. Notons $X \coloneqq X_0 \times_{k_0} k$. Soit $\bar{x}\colon \operatorname{Spec} k \to X$ un point géométrique de X. Le morphisme $X \to X_0$ induit une suite exacte de groupes profinis

$$1 \to \pi_1(X, \bar{x}) \to \pi_1(X_0, \bar{x}) \to \operatorname{Gal}(k_0^{\mathrm{sep}}|k) \to 1.$$

I.2 Le topos étale

Introduite par Grothendieck dans les années 1960, la théorie des sites et des topos permet de généraliser la théorie usuelle des faisceaux définis sur la topologie de Zariski d'un schéma. Elle permet de considérer des topologies contenant beaucoup plus d'ouverts que la topologie de Zariski, et donne lieu à des théories cohomologiques plus fines, comme la cohomologie étale.

I.2.1 Sites

Définition 1.2.1. Soit $\mathcal{C}$ une catégorie. Une prétopologie sur $\mathcal{C}$ est la donnée d'un ensemble $\operatorname{Couv}(\mathcal{C})$ de familles de morphismes $(u_i\colon U_i \to U)_{i\in I}$ dans $\mathcal{C}$, appelées familles couvrantes, vérifiant les propriétés suivantes.

1. Si $V \to U$ est un isomorphisme dans $\mathcal{C}$ alors $(V \to U) \in \operatorname{Couv}(\mathcal{C})$.
2. Si $(U_i \to U)_{i\in I} \in \operatorname{Couv}(\mathcal{C})$ et pour tout $i \in I$, $(V_{ij} \to U_i)_{j\in J_i} \in \operatorname{Couv}(C)$ alors $(V_{ij} \to U)_{i,j} \in \operatorname{Couv}(C)$.

3. Si $(U_i \to U)_{i\in I} \in \mathrm{Couv}(\mathcal{C})$ et $V \to U$ est un morphisme dans $\mathcal{C}$ alors les produits fibrés $U_i \times_U V$ existent et $(U_i \times_U V \to V)_{i\in I} \in \mathrm{Couv}(\mathcal{C})$.

Une catégorie munie d'une prétopologie sera appelée un site.

Cette terminologie courante diffère de celle employée dans [$\mathrm{SGA4}_1$], où un site est défini comme une catégorie munie d'une *topologie*. Ceci n'a aucune incidence sur la suite.

Définition 1.2.2. Soit X un schéma.

1. Un recouvrement de Zariski de X est la donnée d'une famille d'ouverts de Zariski $(U_i)_{i\in I}$ de X telle que $X = \bigcup_{i\in I} U_i$. Le site de Zariski de X est la catégorie des ouverts de X munie de la prétopologie dont les familles couvrantes sont les recouvrements de Zariski.
2. Un recouvrement étale de X est la donnée d'une famille $(u_i \colon U_i \to X)_{i\in I}$ d'éléments de $X_{\text{ét}}$ telle que $\bigcup_i u_i(U_i) = X$. Le (petit) site étale sur X est la catégorie $X_{\text{ét}}$ munie de la prétopologie dont les familles couvrantes sont les recouvrements étales. Le gros site étale sur X est la catégorie des X-schémas, munie de la prétopologie dont les familles couvrantes sont les recouvrements étales.

I.2.2 Faisceaux et topos

Soit $\mathcal{C}$ un site. Afin de traiter le sujet des topos en toute généralité et en évitant de rencontrer des problèmes ensemblistes, il est nécessaire de fixer en amont un univers $\mathcal{U}$ [$\mathrm{SGA4}_1$, I, §0] et ne considérer que des $\mathcal{U}$-sites [$\mathrm{SGA4}_1$, II, Def. 3.0.2]. Si la catégorie sous-jacente à $\mathcal{C}$ est une catégorie de schémas de type fini sur un schéma fixé, ce qui est le cas du petit site étale sur un schéma, ces complications peuvent être ignorées (voir par exemple la discussion dans [Mil80, II, §2, p.57]).

Définition 1.2.3. Un préfaisceau sur $\mathcal{C}$ est un foncteur $\mathcal{C}^{\mathrm{op}} \to \mathrm{Set}$. Un préfaisceau $\mathcal{F}$ sur $\mathcal{C}$ est appelé un faisceau si pour tout $U \in \mathcal{C}$ et toute famille couvrante $(U_i \to U)_{i\in I}$, la suite

$$\mathcal{F}(U) \to \prod_{i\in I} \mathcal{F}(U_i) \rightrightarrows \prod_{i,j\in I} \mathcal{F}(U_i \times_U U_j)$$

est exacte. La catégorie des faisceaux sur un site est appelée topos.

On définit de la même façon les (pré)faisceaux de groupes, groupes abéliens, anneaux, modules... sur $\mathcal{C}$. Nous noterons $\mathrm{Ab}(\mathcal{C})$ la catégorie des faisceaux de groupes abéliens sur $\mathcal{C}$. Soit X un schéma. Soit Λ un anneau commutatif. Nous noterons également $\mathrm{Ab}(X)$ (resp. $\mathrm{Mod}_\Lambda(X)$) la catégorie des faisceaux de groupes abéliens (resp. de Λ-modules) sur le site $X_{\text{ét}}$.

Remarque 1.2.4.

1. [$\mathrm{SGA4}_1$, II, Th. 3.4] Comme pour la topologie de Zariski, il existe un foncteur de faisceautisation, adjoint à gauche du foncteur d'oubli de la catégorie des faisceaux sur $\mathcal{C}$ vers la catégorie des préfaisceaux sur $\mathcal{C}$.
2. Comme dans la topologie de Zariski, les opérations usuelles sur les préfaisceaux de groupes abéliens (noyau, conoyau, produit, somme directe, produit tensoriel) sont définies en effectuant les opérations concernées sur les groupes de sections. Les opérations correspondantes sur les faisceaux sont obtenues à partir de celles-ci par faisceautisation.

Exemple 1.2.5. Soit G un groupe. Vu comme un groupoïde à un objet, il définit un site $\mathcal{C}_G$. La catégorie des G-ensembles est équivalente au topos des faisceaux sur $\mathcal{C}_G$.

Définition 1.2.6. Soient A, B deux topos. Un morphisme de topos $A \to B$ est la donnée d'un couple de foncteurs $(u^\star, u_\star)$ où $u^\star \colon B \to A$ commute aux limites finies et $u_\star \colon A \to B$ est adjoint à droite à $u^\star$.

La catégorie des faisceaux de groupes abéliens sur $\mathcal{C}$ est abélienne et admet suffisamment d'injectifs [SGA4$_1$, II, Prop. 6.7]. Lorsque $\mathcal{C}$ est le site étale d'un schéma X, nous noterons $\mathrm{D}(X)$ sa catégorie dérivée, et $\mathrm{D}^b(X)$ la sous-catégorie pleine de $\mathrm{D}(X)$ constituée des objets K tels que $\mathrm{H}^i K$ soit non nul seulement pour un nombre fini d'entiers i. Le foncteur des sections globales

$$\Gamma(\mathcal{C}, -)\colon \mathrm{Ab}(\mathcal{C}) \to \mathrm{Ab}$$

associe à un faisceau $\mathcal{F}$ le groupe des morphismes de préfaisceaux d'ensembles du préfaisceau trivial $U \mapsto \{\star\}$ vers $\mathcal{F}$; dans le cas particulier où le site $\mathcal{C}$ admet un objet final X, $\Gamma(\mathcal{C}, \mathcal{F}) = \mathcal{F}(X)$. Ce foncteur est exact à gauche mais pas à droite ; son foncteur dérivé est noté $\mathrm{R}\Gamma(\mathcal{C}, -)$, et les groupes de cohomologie associés sont les $\mathrm{H}^i(\mathcal{C}, -) = \mathrm{R}^i\Gamma(\mathcal{C}, -)$. Pour tout schéma X, nous noterons encore $\mathrm{R}\Gamma(X, -)\colon \mathrm{D}(X) \to \mathrm{D}(X)$ le foncteur $\mathrm{R}\Gamma(X_{\text{ét}}, -)$.

I.2.3 Opérations sur les faisceaux

Définition 1.2.7. Soit $f\colon Y \to X$ un morphisme de schémas. Il donne lieu aux foncteurs suivants.

1. Le foncteur image directe $f_\star\colon \mathrm{Ab}(Y) \to \mathrm{Ab}(X)$. Pour tout faisceau $\mathcal{F} \in \mathrm{Ab}(Y)$, $f_\star\mathcal{F}$ est le faisceau $U \mapsto \mathcal{F}(U \times_X Y)$ sur Y.
2. Le foncteur image directe à support propre $f_!\colon \mathrm{Ab}(Y) \to \mathrm{Ab}(X)$. Pour tout faisceau $\mathcal{F} \in \mathrm{Ab}(Y)$, le faisceau $f_!\mathcal{F}$ est le sous-faisceau de $f_\star\mathcal{F}$ dont les sections sur $U \to X$ sont les $s \in f_\star\mathcal{F}(U)$ dont le support (c'est-à-dire le plus petit fermé sur le complémentaire duquel faisceau est nul) est propre sur U.
3. Le foncteur image inverse $f^\star$. Pour tout faisceau $\mathcal{G} \in \mathrm{Ab}(X)$, $f^\star\mathcal{G}$ est le faisceautisé du préfaisceau $U \mapsto \operatorname{colim}_V \mathcal{F}(V)$ sur X, où la colimite porte sur les $V \to X$ étales tels que la composée $U \to X$ se factorise par $V \to X$. En particulier, si f est étale, il s'agit simplement de la restriction de $\mathcal{F}$ au site étale de Y.

Le foncteur $f^\star$ est adjoint à gauche de $f_\star$. Le foncteur $f^\star$ est exact, et le foncteur $f_\star$ est exact à gauche ; il est également exact à droite lorsque le morphisme f est fini [Mil80, II, Cor. 3.6].

Soit $\mathcal{F} \in \mathrm{Ab}(X)$. Étant donné un point géométrique $\bar{x}\colon \operatorname{Spec} k \to X$, la fibre $\mathcal{F}_{\bar{x}}$ est définie comme étant $\Gamma(\operatorname{Spec} k, \bar{x}^\star\mathcal{F})$. Un morphisme de faisceaux $\mathcal{F} \to \mathcal{G}$ est un monomorphisme (resp. épi, resp iso) si et seulement si pour tout point géométrique $\bar{x}$ de X, le morphisme induit $\mathcal{F}_{\bar{x}} \to \mathcal{G}_{\bar{x}}$ en est un.

I.2.4 Exemples de faisceaux

Soit X un schéma. Donnons quelques exemples de faisceaux sur le site étale de X. Le premier est le faisceau structural de X, qui à $U \in X_{\text{ét}}$ associe $\mathcal{O}_U(U)$; nous le noterons encore $\mathcal{O}_X$. De même, le préfaisceau $U \mapsto \mathrm{Hom}_X(U, Y)$ représenté par un X-schéma Y est un faisceau.

Définition 1.2.8. Soit A un groupe abélien. Le faisceau constant associé à A, noté $\underline{A}_X$ ou simplement A, est le faisceautisé du préfaisceau $U \mapsto A$ ayant pour morphismes de restriction id_A. Son groupe de sections sur $U \in X_{\text{ét}}$ est $\underline{A}_X(U) = A^{\pi_0(U)}$, où $\pi_0(U)$ est l'ensemble des composantes connexes de U. Un faisceau sur X est dit constant s'il est isomorphe à un faisceau de cette forme.

Remarque 1.2.9. Le foncteur faisceau constant est adjoint à gauche du foncteur des sections globales $\Gamma(X, -)\colon \mathcal{F} \mapsto \mathcal{F}(X)$.

Exemple 1.2.10. Le groupe multiplicatif $\mathbb{G}_{m,X}$, représenté par $\operatorname{Spec} \mathbb{Z}[t, t^{-1}] \times_{\mathbb{Z}} X$, associe à $U \in X_{\text{ét}}$ le groupe $\Gamma(U, \mathcal{O}_U)^\times$. Le groupe additif $\mathbb{G}_{a,X}$, représenté par $\operatorname{Spec} \mathbb{Z}[t] \times_{\mathbb{Z}} X$, associe à $U \in X_{\text{ét}}$ le groupe $\Gamma(U, \mathcal{O}_U)$. Soit n un entier. Le morphisme $[n]\colon \mathbb{G}_m \to \mathbb{G}_m$ défini par $t \mapsto t^n$ est un morphisme

de schémas en groupes, et son noyau est $\mu_n = \operatorname{Spec} \mathbb{Z}[t]/(t^n - 1) \times_{\mathbb{Z}} X$. Le faisceau représenté par μ_n est

$$\mu_{n,X} \colon U \mapsto \{x \in \Gamma(U, \mathcal{O}_U) \mid x^n = 1\}.$$

Remarquons que si X est un schéma sur un corps k qui contient les racines n-ièmes de l'unité, le choix d'une telle racine $\zeta \in \mu_n(k)$ détermine un isomorphisme de faisceaux $\mathbb{Z}/n\mathbb{Z} \to \mu_n$.

Proposition 1.2.11. [SGA4$_3$, IX, 3.2 et 3.5] Soit n un entier inversible sur X. Il y a une suite exacte dans $\mathrm{Ab}(X)$, appelée suite exacte de Kummer :

$$0 \to \mu_{n,X} \to \mathbb{G}_{m,X} \xrightarrow{[n]} \mathbb{G}_{m,X} \to 0.$$

Supposons X de caractéristique un nombre premier p. Il y a une suite exacte dans $\mathrm{Ab}(X)$, appelée suite exacte d'Artin-Schreier :

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathbb{G}_{a,X} \xrightarrow{t \mapsto t^p - t} \mathbb{G}_{a,X} \to 0.$$

Définition 1.2.12.

1. Un faisceau sur X est dit localement constant s'il existe un recouvrement étale $(U_i \to X)_{i \in I}$ tel que pour tout i, la restriction de $\mathcal{F}$ au site étale de U_i soit un faisceau constant.
2. Un faisceau $\mathcal{F}$ sur X est dit constructible si X est réunion finie de parties localement fermées sur lesquelles $\mathcal{F}$ est localement constant à fibres finies.
3. Soit Λ un anneau noethérien. Un faisceau de Λ-modules sur X sera dit lisse s'il est localement constant et constructible, c'est-à-dire localement constant et à fibres finies.

Nous noterons $\mathrm{D}^b_c(X)$ la sous-catégorie triangulée pleine de $\mathrm{D}^b(X)$ des objets K tels que tous les faisceaux $\mathrm{H}^i K$ soient constructibles. De même, nous noterons $\mathrm{D}^b_c(\Lambda)$ la catégorie dérivée bornée des Λ-modules de type fini.

Voici quelques exemples de faisceaux abéliens constructibles sur X.

- le faisceau représenté par un X-schéma étale [Stacks, 03S8.(1)] ;
- si $f \colon Y \to X$ est un morphisme étale, le faisceau $f_! \Lambda$ [Stacks, 03S8.(3)] ;
- si $i \colon Z \to X$ est une immersion fermée et $\mathcal{F}$ est un faisceau constructible sur Z, le faisceau gratte-ciel $i_\star \mathcal{F}$.

Remarquons que ce dernier point fournit un exemple de faisceau constructible qui n'est pas représentable par un X-schéma étale ; en effet, un tel schéma aurait une image ouverte dans X, et donc des sections locales non nulles en tout point d'un ouvert de X.

I.2.5 Anneaux locaux pour la topologie étale

L'équivalent des anneaux locaux pour la topologie étale sont les anneaux henséliens.

Définition 1.2.13. Un anneau local $(A, \mathfrak{m}, k)$ est dit hensélien si pour tout $f \in A[t]$ et toute racine $a_0 \in k$ de $\bar{f} \in k[t]$ telle que $\bar{f}'(a_0) \neq 0$, il existe $a \in A$ tel que $\bar{a} = a_0$ et $f(a) = 0$. Il est dit strictement hensélien si le corps résiduel k est séparablement clos.

Proposition 1.2.14. [EGA 4$_4$, Prop. 18.8.8] Soit $(A, \mathfrak{m}, k)$ un anneau local. Il existe un anneau local strictement hensélien $(A^{hs}, \mathfrak{m}^{hs}, k^{hs})$ muni d'un morphisme d'anneaux locaux $i^{hs} \colon A \to A^{hs}$ tel que tout morphisme d'anneaux locaux de A vers un anneau strictement hensélien $(A', \mathfrak{m}', k')$ se factorise par A^{hs}, et que cette factorisation est unique si l'on impose le morphisme de corps résiduels $k^{hs} \to k'$. Le couple (A^{hs}, i^{hs}) est appelé hensélisé strict de A.

Soit X un schéma. Soit $\bar{x} \colon \operatorname{Spec} k \to X$ un point géométrique de X. Un voisinage étale de $\bar{x}$ est un morphisme étale $u \colon U \to X$ tel que $\bar{x}$ se factorise par u. La colimite des $\Gamma(U, \mathcal{O}_U)$, où U parcourt les voisinages étales de X, est alors le hensélisé strict de l'anneau local $\mathcal{O}_{X,x}$. Nous noterons $X_{\bar{x}}$ le schéma $\operatorname{Spec} \mathcal{O}^{hs}_{X,x}$; il est muni d'un morphisme canonique $X_{\bar{x}} \to X$.

I.2.6 Recollement

Soit X un schéma. Soit $j\colon U \to X$ une immersion ouverte. Soit $i\colon Z \to X$ une immersion fermée dont l'image est le complémentaire de l'image de U dans X. Définissons une catégorie $\mathcal{C}_{U,Z}$ de la façon suivante. Ses objets sont les triplets $(\mathcal{F}_U, \mathcal{F}_Z, \phi)$ où $\mathcal{F}_U \in \mathrm{Ab}(U)$, $\mathcal{F}_Z \in \mathrm{Ab}(Z)$ et $\phi\colon \mathcal{F}_Z \to i^\star j_\star \mathcal{F}_U$. Les morphismes $(\mathcal{F}_U, \mathcal{F}_Z, \phi) \to (\mathcal{F}'_U, \mathcal{F}'_Z, \phi')$ sont les couples de morphismes $(\psi_U\colon \mathcal{F}_U \to \mathcal{F}'_U, \psi_Z\colon \mathcal{F}_Z \to \mathcal{F}'_Z)$ tels que le diagramme suivant soit commutatif.

$$\begin{tikzcd} \mathcal{F}_Z \arrow[r, "\psi_Z"] \arrow[d, "\phi"] & \mathcal{F}'_Z \arrow[d, "\phi'"] \\ \mathcal{F}_U \arrow[r, "\psi_U"] & \mathcal{F}'_U \end{tikzcd}$$

Remarquons que pour tout faisceau $\mathcal{F}$ sur X, l'adjonction $j^\star \dashv j_\star$ fournit un morphisme

$$\phi_{\mathcal{F}}\colon \mathcal{F} \to j_\star j^\star \mathcal{F}.$$

Proposition 1.2.15. [Mil80, II, Th. 3.10] Le foncteur $\mathrm{Ab}(X) \to \mathcal{C}_{U,Z}$ qui à un faisceau $\mathcal{F}$ associe $(j^\star\mathcal{F}, i^\star\mathcal{F}, \phi_{\mathcal{F}})$ et à un morphisme $f\colon \mathcal{F} \to \mathcal{F}'$ associe $(j^\star f, i^\star f)$ est une équivalence de catégories. Un quasi-inverse est donné par $(\mathcal{F}_U, \mathcal{F}_Z, \phi) \mapsto \mathcal{F}$, où $\mathcal{F}$ est défini par le diagramme cartésien suivant :

$$\begin{tikzcd} \mathcal{F} \arrow[r] \arrow[d] & i_\star \mathcal{F}_Z \arrow[d, "i_\star\phi"] \\ j_\star \mathcal{F}_U \arrow[r, "i^\star \dashv i_\star"'] & i_\star i^\star j_\star \mathcal{F}_U \end{tikzcd}$$

Définition 1.2.16. L'équivalence de catégories précédente permet de définir les foncteurs

$$j_!\colon \mathrm{Ab}(U) \to \mathrm{Ab}(X),\ \mathcal{F} \mapsto (\mathcal{F}, 0, 0)$$

et

$$i^!\colon \mathrm{Ab}(X) \to \mathrm{Ab}(Z),\ (\mathcal{F}_U, \mathcal{F}_Z, \phi) \mapsto \ker(\phi).$$

Remarque 1.2.17. Le foncteur $j_!$ coïncide avec le foncteur image directe à support propre défini précédemment.

Proposition 1.2.18. Les foncteurs $i_\star, i^\star, i^!, j_\star, j_!, j^\star$ vérifient les adjonctions

$$i^\star \dashv i_\star \dashv i^!$$

et

$$j_! \dashv j^\star \dashv j_\star.$$

Les foncteurs $i^\star, i_\star, j^\star, j_!$ sont exacts. Les foncteurs $i^!$ et $j_\star$ sont exacts à gauche. Pour tout faisceau $\mathcal{F}$ de groupes abéliens sur X, il y a des suites exactes courtes

$$0 \to j_! j^\star \mathcal{F} \to \mathcal{F} \to i_\star i^\star \mathcal{F} \to 0$$

et

$$0 \to i_\star i^! \mathcal{F} \to \mathcal{F} \to j_\star j^\star \mathcal{F}.$$

I.3 Torseurs, H^1 et fibrés en droites

I.3.1 Torseurs et premier groupe de cohomologie

Soit $\mathcal{C}$ un site. Soit $\mathcal{G}$ un faisceau en groupes abéliens sur $\mathcal{C}$.

Définition 1.3.1. Un faisceau $\mathcal{F}$ sur $\mathcal{C}$ est un $\mathcal{G}$-torseur s'il est muni d'une action à gauche $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ qui est localement (pour la topologie de $\mathcal{C}$) isomorphe à l'action par translation $\mathcal{G} \times \mathcal{G} \to \mathcal{G}$.

Soit $\mathcal{G} \to \mathcal{I}$ un monomorphisme de $\mathcal{G}$ vers un faisceau injectif. Alors le morphisme

$$\mathrm{H}^0(\mathcal{C}, \mathcal{I}/\mathcal{G}) \to \mathrm{H}^1(\mathcal{C}, \mathcal{G})$$

est surjectif. Soit $c \in \mathrm{H}^1(\mathcal{C}, \mathcal{G})$: il est l'image d'un élément $c' \in \mathrm{H}^0(\mathcal{C}, \mathcal{I}/\mathcal{G})$. Considérons le faisceau $\mathcal{F}' \subset \mathcal{I}$ des antécédents de c'.

Proposition 1.3.2. [Stacks, 03AJ] L'application $\mathcal{F} \mapsto \mathcal{F}'$ définit une bijection canonique entre l'ensemble $\mathrm{H}^1(\mathcal{C}, \mathcal{G})$ et l'ensemble des classes d'isomorphisme de $\mathcal{G}$-torseurs sur $\mathcal{C}$.

Définition 1.3.3. Soient $\mathcal{F}_1, \mathcal{F}_2$ deux faisceaux sur $\mathcal{C}$ munis d'une action à gauche de $\mathcal{G}$. Le produit contracté $\mathcal{F}_1 \wedge^{\mathcal{G}} \mathcal{F}_2$ est le quotient du faisceau $\mathcal{F}_1 \times \mathcal{F}_2$ par la relation d'équivalence définie par $(g \cdot f_1, f_2) = (f_1, g \cdot f_2)$.

Si $\mathcal{T}_1$ et $\mathcal{T}_2$ sont deux $\mathcal{G}$-torseurs, le produit contracté $\mathcal{T}_1 \wedge^{\mathcal{G}} \mathcal{T}_2$ est encore un $\mathcal{G}$-torseur ; le produit contracté définit une loi de groupe sur l'ensemble des classes d'isomorphisme de $\mathcal{G}$-torseurs sur X, qui correspond à la loi de groupe sur $\mathrm{H}^1(\mathcal{C}, \mathcal{G})$ via la bijection ci-dessus [Mil80, III.4, Rem. 4.8(b)].

I.3.2 Torseurs sur le site étale

Soit X un schéma.

Définition 1.3.4.

1. Soit G un X-schéma en groupes. Soit T un X-schéma muni d'une action à droite de G. On dit que T est un G-torseur sur X si $T \to X$ est étale et surjectif, et si le morphisme $G \times_X T \to T \times_X T, (g, t) \mapsto (t, tg)$ est un isomorphisme.
2. Soit G un groupe abélien. Un faisceau $\mathcal{F}$ sur X est un G-torseur si c'est un torseur sous le faisceau constant associé à G. Un X-schéma T est un G-torseur si c'est un torseur sous le X-schéma en groupes $G \times X$.

Le résultat de représentabilité élémentaire suivant suffira dans notre cas.

Proposition 1.3.5. [Fu15, Prop. 5.7.18] Soit X un schéma. Soit G un schéma en groupes séparé étale de présentation finie sur X. Le foncteur de Yoneda $T \mapsto h_T$ induit une équivalence de catégories entre la catégorie des X-schémas qui sont des G-torseurs et la catégorie des faisceaux sur X qui sont des h_G-torseurs.

Les torseurs sous un groupe fini généralisent les revêtements galoisiens.

Lemme 1.3.6. [Sza09, Prop. 5.3.16] Soit X un schéma. Soit G un groupe fini. Les G-torseurs connexes sur X sont les revêtements galoisiens de X de groupe G.

Remarque 1.3.7 (Fonctorialité)**.** Voici comment se décrivent différents morphismes en termes de torseurs.

- Étant donné un morphisme de faisceaux de groupes abéliens $u \colon \mathcal{F} \to \mathcal{G}$ sur X, le morphisme $u_\star \colon \mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(X, \mathcal{G})$ obtenu par fonctorialité de $\mathrm{H}^1(X, -)$ associe à un $\mathcal{F}$-torseur $\mathcal{T}$ le $\mathcal{G}$-torseur $\mathcal{T} \wedge^{\mathcal{F}} \mathcal{G}$, où $\mathcal{F}$ agit sur $\mathcal{G}$ via $f \cdot g = u(f) + g$.

- Étant donné un morphisme de schémas $\phi\colon Y \to X$, le morphisme $\phi^\star\colon \mathrm{H}^1(X,\mathcal{F}) \to \mathrm{H}^1(Y, f^\star\mathcal{F})$ associe à un $\mathcal{F}$-torseur $\mathcal{T}$ le $\phi^\star\mathcal{F}$-torseur $\phi^\star\mathcal{T}$.
- Étant donné une suite exacte de faisceaux de groupes abéliens sur X

$$0 \to \mathcal{F} \xrightarrow{u} \mathcal{G} \xrightarrow{v} \mathcal{H} \to 0$$

  le morphisme canonique $\partial\colon \mathrm{H}^0(X,\mathcal{H}) \to \mathrm{H}^1(X,\mathcal{F})$ est construit de la façon suivante [SGA4$\frac{1}{2}$, Cycle, 1.1.4]. À une section globale $s \in \mathrm{H}^0(X,\mathcal{H})$, il associe le faisceau

$$v^{-1}s\colon U \mapsto \{t \in \mathcal{G}(U) \mid v_U(t) = s|_U\}.$$

  La structure de $\mathcal{F}$-torseur sur $\partial s := v^{-1}s$ est donnée par $f \cdot t = u(f) + t$.

Mentionnons enfin un résultat qui servira par la suite, concernant la restriction des torseurs.

Lemme 1.3.8. Soit $j\colon U \to X$ une immersion ouverte. Soit $\mathcal{F}$ un faisceau de groupes abéliens sur U. Alors le morphisme de restriction $\mathrm{H}^1(X, j_\star\mathcal{F}) \to \mathrm{H}^1(U,\mathcal{F})$ est injectif.

Démonstration. Soit $\mathcal{T}$ un $j_\star\mathcal{F}$-torseur sur X tel qu'il y ait un isomorphisme de $j^\star j_\star\mathcal{F} = \mathcal{F}$-torseurs $\phi\colon j^\star\mathcal{T} \to j^\star j_\star\mathcal{F}$. Comme tout morphisme de torseurs est un isomorphisme, il suffit d'exhiber un morphisme de $j_\star\mathcal{F}$-torseurs $\mathcal{T} \to j_\star\mathcal{F}$, ce qui est simple : la composée

$$\mathcal{T} \to j_\star j^\star\mathcal{T} \xrightarrow{j_\star\phi} j_\star j^\star j_\star\mathcal{F} \simeq j_\star\mathcal{F}$$

convient. En effet, le diagramme

$$\begin{tikzcd}
j_\star\mathcal{F} \times \mathcal{T} \arrow[r] \arrow[d] & j_\star j^\star j_\star\mathcal{F} \times j_\star j^\star\mathcal{T} \arrow[r] \arrow[d] & j_\star j^\star j_\star\mathcal{F} \times j_\star j^\star j_\star\mathcal{F} \arrow[r] \arrow[d] & j_\star\mathcal{F} \times j_\star\mathcal{F} \arrow[d] \\
\mathcal{T} \arrow[r] & j_\star j^\star\mathcal{T} \arrow[r] & j_\star j^\star j_\star\mathcal{F} \arrow[r] & j_\star\mathcal{F}
\end{tikzcd}$$

est commutatif. □

I.3.3 Torseurs sous $\mathbb{G}_m$ et μ_n

Soit X un schéma. Fixons un entier naturel non nul n. Dans un premier temps, nous allons considérer les torseurs sous $\mathbb{G}_m$ et μ_n sur X. Ils admettent une description en termes de faisceaux inversibles sur X. Remarquons qu'un faisceau inversible pour la topologie étale sur X définit par restriction un faisceau inversible pour la topologie de Zariski. Réciproquement, un $\mathcal{O}_X$-module inversible $\mathcal{L}$ pour la topologie de Zariski définit un $\mathcal{O}_X$-module dont les sections sur $(U \xrightarrow{u} X) \in X_{\text{ét}}$ sont données par $\Gamma(U, u^\star_{Zar}\mathcal{L})$ [Stacks, 03DV]. Ceci définit une équivalence entre les catégories de $\mathcal{O}_X$-modules inversibles pour les topologies de Zariski et étale ; il n'y a donc pas lieu de faire une distinction entre les deux.

Proposition 1.3.9. [Stacks, 040D] Étant donné un faisceau inversible $\mathcal{L}$ sur X, le faisceau sur $X_{\text{ét}}$

$$\underline{\mathrm{Isom}}(\mathcal{O}_X, \mathcal{L})\colon U \mapsto \mathrm{Isom}_U(\mathcal{O}_U, \mathcal{L}_U)$$

est un $\mathbb{G}_m$-torseur. Le morphisme $\mathcal{L} \mapsto \underline{\mathrm{Isom}}(\mathcal{O}_X, \mathcal{L})$ définit un isomorphisme $\operatorname{Pic} X \to \mathrm{H}^1(X, \mathbb{G}_m)$ fonctoriel en X. L'isomorphisme inverse associe à un $\mathbb{G}_m$-torseur $\mathcal{T}$ le faisceau inversible $\mathcal{T} \wedge^{\mathbb{G}_m} \mathcal{O}_X$.

Considérons désormais la catégorie $\mathcal{C}$ dont les objets sont les couples $(\mathcal{L}, \alpha)$, où $\mathcal{L}$ est un faisceau inversible sur X et $\alpha\colon \mathcal{L}^{\otimes n} \xrightarrow{\sim} \mathcal{O}_X$ est une trivialisation de $\mathcal{L}^{\otimes n}$. Un morphisme entre deux couples $(\mathcal{L}, \alpha), (\mathcal{L}', \alpha')$ est défini comme étant un morphisme $\phi\colon \mathcal{L} \to \mathcal{L}'$ tel que le diagramme

$$\begin{tikzcd} \mathcal{L}^{\otimes n} \arrow[r, "\alpha"] \arrow[d, "\phi"'] & \mathcal{O}_X \arrow[d, "\mathrm{id}"] \\ \mathcal{L}'^{\otimes n} \arrow[r, "\alpha'"] & \mathcal{O}_X \end{tikzcd}$$

soit commutatif. Soit S l'ensemble des classes d'isomorphisme de tels couples. Le produit tensoriel $(\mathcal{L}, \alpha) \otimes (\mathcal{L}', \alpha') \coloneqq (\mathcal{L} \otimes \mathcal{L}', \alpha \otimes \alpha')$ définit une loi de groupe sur S, d'élément neutre $(\mathcal{O}_X, \mathrm{id})$.

Proposition 1.3.10. [Stacks, 040Q] Étant donné un objet $(\mathcal{L}, \alpha)$ de $\mathcal{C}$, le faisceau

$$\mathcal{T}_{\mathcal{L}}\colon U \mapsto \mathrm{Isom}_{\mathcal{C}}((\mathcal{O}_U, 1), (\mathcal{L}|_U, \alpha|_U))$$

sur $X_{\text{ét}}$ est un μ_n-torseur. L'application $\mathcal{L} \mapsto \mathcal{T}_{\mathcal{L}}$ définit un isomorphisme de groupes $S \to \mathrm{H}^1(X, \mu_n)$ fonctoriel en X.

I.4 Groupe fondamental et faisceaux lisses

I.4.1 Faisceaux lisses et π_1-modules

Soient X un schéma et $\bar{x}$ un point géométrique de X. Soit Λ un anneau fini.

Proposition 1.4.1. [Fu15, Prop. 5.8.1.(i)] Soit $\mathcal{F}$ un faisceau à fibres finies sur X. Le faisceau $\mathcal{F}$ est localement constant si et seulement s'il est représenté par un revêtement étale de X. S'il l'est, il existe un morphisme fini étale surjectif $f\colon Y \to X$, avec Y connexe, tel que $f^\star\mathcal{F}$ soit constant.

En d'autres termes, le foncteur de Yoneda $Y \mapsto h_Y$ définit une équivalence entre la catégorie $\mathrm{Fét}_X$ des revêtements étales de X et la catégorie des faisceaux localement constants constructibles sur X. Nous connaissons déjà une autre catégorie équivalente à $\mathrm{Fét}_X$: celle des $\pi_1(X, \bar{x})$-modules. Nous serons intéressés par le cas particulier des faisceaux de Λ-modules ; le résultat s'énonce alors de la façon suivante.

Proposition 1.4.2. [SGA1, V, Th. 4.1] Le foncteur fibre en $\bar{x}$ définit une équivalence de catégories entre la catégorie des faisceaux lisses de Λ-modules sur X et la catégorie des $\pi_1(X, \bar{x})$-modules de type fini munis d'une structure de Λ-module qui commute à l'action de $\pi_1(X, \bar{x})$.

Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X. La proposition précédente montre qu'il est uniquement déterminé par la donnée du $\pi_1(X, \bar{x})$-ensemble $\mathcal{F}_{\bar{x}}$. Un faisceau localement constant $\mathcal{T}$ sur X muni d'une action à droite de $\mathcal{F}$ s'identifie alors au groupe $\mathcal{T}_{\bar{x}}$, muni d'une action à droite de $\mathcal{F}_{\bar{x}}$ et d'une action continue à gauche de $\pi_1(X, \bar{x})$, qui sont compatibles au sens où pour tous $s \in \pi_1(X, \bar{x}), t \in T_{\bar{x}}$ et $f \in \mathcal{F}_{\bar{x}}$:

$$s(t \cdot f) = (st) \cdot (sf).$$

Le faisceau $\mathcal{T}$ est un $\mathcal{F}$-torseur si et seulement si $\mathcal{T}_{\bar{x}}$ est un $\mathcal{F}_{\bar{x}}$-torseur dans la catégorie des $\pi_1(X, \bar{x})$-ensembles [SGA1, XI, §5, p231]. Il s'en déduit un isomorphisme canonique, fonctoriel en $\mathcal{F}$:

$$\begin{array}{ccc} \mathrm{H}^1(X, \mathcal{F}) & \xrightarrow{\sim} & \mathrm{H}^1(\pi_1(X, \bar{x}), \mathcal{F}_{\bar{x}}) \\ \mathcal{T} & \mapsto & \mathcal{T}_{\bar{x}}. \end{array}$$

Opérations sur les faisceaux lisses Soit $f\colon Y \to X$ un revêtement galoisien de schémas connexes. Fixons des points géométriques $\bar{x}, \bar{y}$ de X et Y tels que $\bar{x} = f \circ \bar{y}$. Si $\mathcal{F}$ est un faisceau lisse de groupes abéliens sur X de fibre $\mathcal{F}_{\bar{x}} = M$, le faisceau lisse $f^\star\mathcal{F}$ a pour fibre $\mathcal{F}_{\bar{y}} = M$. L'adjoint à droite de $f^\star$ est $f_\star$, qui correspond donc à l'adjoint à droite du foncteur d'oubli $\mathrm{Mod}_{\pi_1(X,\bar{x})} \to \mathrm{Mod}_{\pi_1(Y,\bar{y})}$, qui est la co-induction. Dans les catégories de revêtements étales de X et de Y, il correspond à la restriction de Weil $R_{Y\to X}$ (voir annexe B.5). Le tableau suivant résume la situation :

Revêtements étales	Faisceaux lisses	π_1-modules
$- \times_X Y$	$f^\star$	oubli $M \mapsto M$
$R_{Y\to X}$	$f_\star$	$\mathrm{coind}_{\pi_1(X,\bar{x})}^{\pi_1(Y,\bar{y})}$

Revêtement trivialisant minimal Soit X un schéma. Soit $\bar{x}$ un point géométrique de X. Soit Λ un anneau noethérien. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X, correspondant à un $\pi_1(X,\bar{x})$-module M. Notons $\mathfrak{S}$ le groupe de monodromie associé : c'est l'image de $\pi_1(X,\bar{x})$ dans $\mathrm{Aut}_\Lambda(M)$. Soit H le noyau du morphisme $\pi_1(X,\bar{x}) \to M$. Il correspond à un revêtement galoisien $X_{\min} \to X$ de groupe d'automorphismes $\pi_1(X,\bar{x})/H \xrightarrow{\sim} \mathfrak{S}$; ce revêtement est minimal pour la propriété de trivialiser $\mathcal{F}$.

I.4.2 G-faisceaux et descente galoisienne

Définition 1.4.3. Soient X un schéma, $\mathcal{F}$ un faisceau sur X, et G un groupe d'automorphismes de X. Une action de G sur $\mathcal{F}$ est une famille d'isomorphismes $(\phi_g\colon \mathcal{F} \to g_\star\mathcal{F})_{g\in G}$ telle que $\phi_{e_G} = \mathrm{id}_\mathcal{F}$ et que pour tous $g, h \in G$, le diagramme

$$\begin{tikzcd} \mathcal{F} \arrow[r, "\phi_g"] \arrow[d, "\phi_{gh}"'] & g_\star\mathcal{F} \arrow[d, "g_\star\phi_h"] \\ (gh)_\star\mathcal{F} \arrow[r, "\sim"] & g_\star h_\star\mathcal{F} \end{tikzcd}$$

où la ligne du bas est l'isomorphisme canonique, soit commutatif. Un faisceau $\mathcal{F}$ muni d'une action de G sera appelé G-faisceau. Un morphisme de G-faisceaux est un morphisme de faisceaux compatible à l'action de G.

Considérons pour la suite un revêtement galoisien $f\colon Y \to X$ de groupe G. Si $\mathcal{F}$ est un faisceau sur X, alors le faisceau $f^\star\mathcal{F}$ est muni d'une action de G. Étant donné un élément $g \in G$, la composition du morphisme d'adjonction $f^\star\mathcal{F} \to g_\star g^\star f^\star\mathcal{F}$ avec l'isomorphisme canonique $g_\star g^\star f^\star\mathcal{F} \to g_\star(f \circ g)^\star\mathcal{F} = g_\star f^\star\mathcal{F}$ fournit un morphisme $f^\star\mathcal{F} \to g_\star f^\star\mathcal{F}$.

Proposition 1.4.4. [Stacks, 0GEZ, 0CDQ] Le foncteur $\mathcal{F} \mapsto f^\star\mathcal{F}$ définit une équivalence entre la catégorie des faisceaux sur X et la catégorie des G-faisceaux sur Y. Un quasi-inverse de ce foncteur est donné par $\mathcal{F} \mapsto (f_\star\mathcal{F})^G$.

Soit $\mathcal{G}$ un faisceau de groupes abéliens sur X. Notons $\mathcal{G}'$ le G-faisceau $f^\star\mathcal{G}$. Soit $\mathcal{F}$ un $\mathcal{G}$-torseur sur X. Le G-faisceau $\mathcal{F}' := f^\star\mathcal{F}$ est encore un $\mathcal{G}'$-torseur sur Y ; le morphisme $\mathcal{G}' \times \mathcal{F}' \to \mathcal{F}'$ est un morphisme de $\mathcal{G}$-faisceaux, au sens où le diagramme suivant est commutatif pour tout $g \in G$:

$$\begin{tikzcd} \mathcal{G}' \times \mathcal{F}' \arrow[r] \arrow[d] & \mathcal{F}' \arrow[d] \\ g_\star\mathcal{G}' \times g_\star\mathcal{F}' \arrow[r] & g_\star\mathcal{F}' \end{tikzcd}$$

Réciproquement, soit $\mathcal{F}'$ un G-faisceau sur Y muni d'une action de $\mathcal{G}'$ qui en fait un $\mathcal{G}'$-torseur. Soit $\mathcal{F}$ le faisceau $(f_\star\mathcal{F}')^G$ sur X ; il vérifie $f^\star\mathcal{F} = \mathcal{F}'$. Le morphisme $\mathcal{G}' \times \mathcal{F}' \to \mathcal{F}'$ descend en un morphisme $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ si et seulement si l'action de $\mathcal{G}'$ sur $\mathcal{F}'$ est G-équivariante au sens ci-dessus.

Corollaire 1.4.5. Soit $\mathcal{G}$ un faisceau de groupes abéliens sur X. Le foncteur $\mathcal{F} \mapsto f^\star\mathcal{F}$ définit une équivalence entre la catégorie des $\mathcal{G}$-torseurs sur X et celle des $f^\star\mathcal{G}$-torseurs sur Y munis d'une action de G telle que l'action de $f^\star\mathcal{G}$ soit G-équivariante.

I.4.3 Schémas $K(\pi, 1)$

Sur certains schémas, la cohomologie des faisceaux lisses est isomorphe à la cohomologie galoisienne de leur fibre : les schémas qui vérifient cette propriété sont appelés schémas $K(\pi, 1)$. Une étude détaillée de leurs propriétés se trouve par exemple dans [Ach15].

Soient X un schéma connexe et $\bar{x}$ un point géométrique de X. Soit ℓ un nombre premier inversible sur X. Notons $X_{\text{fét}}$ le topos fini étale associé à X, défini par la sous-catégorie pleine des X-schémas finis étales munie de la topologie étale. L'équivalence de catégories donnée par le théorème 1.1.14 définit un isomorphisme de topos entre $X_{\text{fét}}$ et le topos $B_{\pi_1(X,\bar{x})}$ des $\pi_1(X, \bar{x})$-ensembles finis continus.

Définition 1.4.6. Un faisceau d'ensembles $\mathcal{F}$ sur X est dit ℓ-monodromique s'il est localement constant constructible et si l'image de $\pi_1(X, \bar{x})$ dans $\mathrm{Aut}(\mathcal{F}_{\bar{x}})$ est un ℓ-groupe. Un faisceau de groupes $\mathcal{F}$ sur X est dit ℓ-monodromique si ses fibres sont des ℓ-groupes finis et s'il est ℓ-monodromique en tant que faisceau d'ensembles.

Notons encore $X_{\ell\text{ét}}$ le topos défini par la sous-catégorie pleine des schémas finis étales $Y \to X$ tels que le faisceau représenté par Y soit ℓ-monodromique. Considérons les morphismes de topos $\rho\colon X_{\text{ét}} \to X_{\text{fét}}$ et $\rho_\ell\colon X_{\text{ét}} \to X_{\ell\text{ét}}$ définis par la restriction des faisceaux aux sites définissant $X_{\text{fét}}$ et $X_{\ell\text{ét}}$. Notons enfin $\pi_1(X, \bar{x})^\ell$ le complété pro-ℓ de $\pi_1(X, \bar{x})$.

Définition 1.4.7. [AG15, Def. 9.21] Le schéma X est appelé un $K(\pi, 1)$ si pour tout entier n inversible sur X et tout faisceau $\mathcal{F}$ de $\mathbb{Z}/n\mathbb{Z}$-modules sur $X_{\text{fét}}$, le morphisme d'adjonction

$$\mathcal{F} \to \mathrm{R}\rho_\star(\rho^\star\mathcal{F})$$

est un isomorphisme.

Définition 1.4.8. [MO15, 1.4.4] Le schéma X est un $K(\pi, 1)$ pro-ℓ si pour tout faisceau abélien $\mathcal{F}$ de ℓ-torsion sur $X_{\ell\text{ét}}$, le morphisme d'adjonction

$$\mathcal{F} \to \mathrm{R}\rho_{\ell\star}(\rho_\ell^\star\mathcal{F})$$

est un isomorphisme.

Lemme 1.4.9. [MO15, 1.4.2] Le schéma X est un $K(\pi, 1)$ si et seulement si, pour tout entier n inversible sur X et tout faisceau lisse $\mathcal{F}$ de $\mathbb{Z}/n\mathbb{Z}$-modules, le morphisme

$$\mathrm{R}\Gamma(\pi_1(X, \bar{x}), \mathcal{F}_{\bar{x}}) \to \mathrm{R}\Gamma(X, \mathcal{F})$$

est un isomorphisme. Le schéma X est un $K(\pi, 1)$ pro-ℓ si et seulement si, pour tout faisceau abélien ℓ-monodromique $\mathcal{F}$ sur X, le morphisme

$$\mathrm{R}\Gamma(\pi_1(X, \bar{x})^\ell, \mathcal{F}_{\bar{x}}) \to \mathrm{R}\Gamma(X, \mathcal{F})$$

est un isomorphisme.

Si X est un $K(\pi,1)$, la cohomologie d'un faisceau lisse $\mathcal{F}$ sur X peut donc se calculer à l'aide de la cohomologie du $\pi_1(X,\bar{x})$-module $\mathcal{F}_{\bar{x}}$. Le résultat d'effaçabilité suivant fournit une condition suffisante pour qu'un schéma soit un $K(\pi,1)$.

Proposition 1.4.10. [Sti02, Prop. A.3.1] Soient X un schéma connexe et ℓ un nombre premier inversible sur X. Supposons que pour tout $i \geqslant 1$ et tout faisceau lisse $\mathcal{F}$ de torsion inversible sur X (resp. de $\mathbb{Z}/\ell\mathbb{Z}$-espaces vectoriels), il existe un revêtement $\phi_i \colon Y_i \to X$ galoisien (resp. galoisien de groupe un ℓ-groupe) tel que le morphisme $\mathrm{H}^i(X,\mathcal{F}) \to \mathrm{H}^i(Y_i,\phi_i^\star\mathcal{F})$ soit nul. Alors X est un $K(\pi,1)$.

Démonstration. Un ∂-foncteur cohomologique effaçable étant universel [Gro57, Prop. 2.2.1], il suffit de montrer que pour tout $i \geqslant 1$, le foncteur $\mathrm{H}^i(X,\rho^\star -) \colon B_{\pi_1(X,\bar{x})} \to \mathrm{Ab}$ est effaçable. Soit M un $\pi_1(X,\bar{x})$-module fini de torsion inversible sur X, et $\mathcal{F} = \rho^\star M$ le faisceau lisse associé. Soit $i \geqslant 1$. La condition de l'énoncé fournit un revêtement galoisien $\phi \colon Y \to X$ tel que $\mathrm{H}^i(X,\mathcal{F}) \to \mathrm{H}^i(Y,\phi^\star\mathcal{F})$ soit nul. Le morphisme $\mathcal{F} \to \phi_\star\phi^\star\mathcal{F}$ est injectif. Soit $\bar{y}$ un point géométrique de Y d'image $\bar{x}$. Le faisceau lisse $\phi_\star\phi^\star\mathcal{F}$ correspond au $\pi_1(X,\bar{x})$-module $N \coloneqq \mathrm{coind}_{\pi_1(X,\bar{x})}^{\pi_1(Y,\bar{y})} M$. Enfin, $\mathrm{H}^1(X,\phi_\star\phi^\star\mathcal{F}) = \mathrm{H}^1(Y,\mathcal{F})$ par exactitude de $\phi_\star$. Il y a donc une injection $M \to N$ dans $B_{\pi_1(X,\bar{x})}$ telle que $\mathrm{H}^1(X,\rho^\star M) \to \mathrm{H}^1(X,\rho^\star N)$ soit nulle. □

Remarque 1.4.11. Sur un corps algébriquement clos, pour tout entier $m \geqslant 1$, $\pi_1(\mathbb{P}^m) = 0$ [SGA1, XI, Prop. 1.1] mais $\mathrm{H}^2(\mathbb{P}^m,\Lambda) = \Lambda(-1)$ [Mil13, Example 16.3]. Par conséquent, $\mathbb{P}^m$ n'est pas un $K(\pi,1)$. Nous verrons dans la section II.6.3 qu'à l'exception de $\mathbb{P}^1$, les courbes lisses sont toutes des $K(\pi,1)$. Il existe également des résultats positifs en dimension quelconque, sur les corps finis : Achinger a montré [Ach17, Th. 1.1.1] que tout $\mathbb{F}_p$-schéma affine connexe est un $K(\pi,1)$.

Remarque 1.4.12. Si X est un $K(\pi,1)$ alors pour tout complexe K de $\pi_1(X,\bar{x})$-modules, le morphisme

$$\mathrm{R}\Gamma(\pi_1(X,\bar{x}),K) \to \mathrm{R}\Gamma(X,\rho^\star K)$$

est encore un isomorphisme. Notons $\mathscr{K} = \rho^\star K$. Considérons le morphisme entre les suites spectrales $E_{2,\pi}^{pq} \coloneqq \mathrm{H}^p(\pi,\mathrm{H}^q K)$ et $E_{2,X}^{pq} \coloneqq \mathrm{H}^p(X,\mathrm{H}^q \mathscr{K})$ données par [Stacks, 015J]. Il est un isomorphisme dès la deuxième page puisque X est un $K(\pi,1)$, et il induit donc des isomorphismes entre les aboutissements $\mathrm{H}^i(\pi,K) \to \mathrm{H}^i(X,\mathscr{K})$ par [Wei94, Th. 5.2.12]. Par conséquent, le morphisme $\mathrm{R}\Gamma(\pi,K) \to \mathrm{R}\Gamma(X,\mathscr{K})$ est un isomorphisme dans $\mathrm{D}_c^b(\Lambda)$.

I.4.4 Morphismes de restriction

Cette section recense quelques lemmes utiles par la suite.

Lemme 1.4.13. Soit U' un ouvert non vide d'un schéma U intègre normal. Notons $j \colon U' \to U$ l'inclusion. Si $\mathcal{F}$ est un faisceau constant de Λ-modules sur U' de fibre F alors $j_\star\mathcal{F}$ est constant sur U de fibre F.

Démonstration. Soit $f \colon T \to U$ un morphisme étale. Alors T est encore un schéma normal [Stacks, 025P]. Si T est connexe alors il est intègre [Stacks, 033M], et son ouvert $T \times_X U'$ (qui est non vide puisque U' est dense) est encore irréductible, donc connexe. Par conséquent, $j_\star\mathcal{F}(T) = F$. Les morphismes de restriction de $j_\star\mathcal{F}$ sont évidemment les mêmes que ceux de $\mathcal{F}$. □

Lemme 1.4.14. Soient U un schéma intègre normal, et U' un ouvert non vide de U. Notons $j \colon U' \to U$ l'inclusion. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur U. Alors le morphisme d'adjonction $\mathcal{F} \to j_\star j^\star\mathcal{F}$ est un isomorphisme.

Démonstration. Il existe un morphisme fini étale $p\colon V \to U$ qui trivialise $\mathcal{F}$, avec V un schéma intègre normal. Considérons le diagramme cartésien suivant.

$$\begin{tikzcd} V' \arrow[r, "j'"] \arrow[d, "q"'] & V \arrow[d, "p"] \\ U' \arrow[r, "j"] & U \end{tikzcd}$$

Alors V' est un ouvert non vide de V. Considérons le faisceau constant $F = j'^\star p^\star \mathcal{F}$. Par le lemme précédent, ${j'}_\star F$ est constant, et par conséquent le morphisme $p^\star \mathcal{F} \to {j'}_\star j'^\star p^\star \mathcal{F} = {j'}_\star q^\star j^\star \mathcal{F} = p^\star j_\star j^\star \mathcal{F}$ (par finitude de p) est un isomorphisme. Comme le morphisme p est fidèlement plat et quasi-compact, le foncteur $p^\star$ reflète les isomorphismes [EGA 4_2, Prop. 2.7.1], et par conséquent $\mathcal{F} \to j_\star j^\star \mathcal{F}$ est un isomorphisme. □

Corollaire 1.4.15. Soit X un schéma intègre normal. Soient $U' \subset U$ deux ouverts de Zariski non vides de X. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X. Le morphisme de restriction $\mathcal{F}(U) \to \mathcal{F}(U')$ est un isomorphisme.

I.5 Les grands théorèmes

I.5.1 Dimension cohomologique

Définition 1.5.1. Soit ℓ un nombre premier. La ℓ-dimension cohomologique d'un schéma X est le plus petit $j \in \mathbb{N} \cup \{\infty\}$ tel que pour tout faisceau abélien $\mathcal{F}$ de ℓ-torsion sur X et tout $i > j$, $\mathrm{H}^i(X, \mathcal{F}) = 0$. Elle sera notée $\mathrm{cd}_\ell(X)$. La dimension cohomologique de X est

$$\mathrm{cd}(X) \coloneqq \sup_\ell \mathrm{cd}_\ell(X) \in \mathbb{N} \cup \{\infty\}.$$

Proposition 1.5.2. [SGA4_3, X, Cor. 4.3] Soient p, ℓ deux nombres premiers distincts. Soient k_0 un corps de caractéristique p et X un schéma affine de type fini sur k_0. Alors

$$\mathrm{cd}_\ell(X) \leqslant \mathrm{cd}_\ell(k_0) + 2\dim(X)$$

et

$$\mathrm{cd}_p(X) \leqslant \dim(X) + 1.$$

Proposition 1.5.3. [SGA4_3, X, Th. 5.1] Soit X un schéma affine de type fini sur un corps k_0. Alors

$$\mathrm{cd}(X) \leqslant \dim(X) + \mathrm{cd}(k_0).$$

Remarque 1.5.4.

1. Lorsque X est le spectre d'un corps k_0, sa dimension cohomologique est la dimension cohomologique de k_0 pour la cohomologie galoisienne. En particulier, les corps de dimension cohomologique nulle sont les corps séparablement clos. Les corps finis ainsi que les corps de fonctions de courbes sur un corps algébriquement clos sont de dimension cohomologique 1.
2. Si X est une courbe sur un corps séparablement clos et $\mathcal{F}$ est un faisceau abélien de torsion sur X alors $\mathrm{H}^i(X, \mathcal{F}) = 0$ dès que $i \geqslant 3$. Si X est de surcroît affine, $\mathrm{H}^2(X, \mathcal{F})$ est également nul.

I.5.2 Invariance topologique

Nous nous intéresserons par la suite uniquement au calcul de la cohomologie de schémas réduits sur des corps parfaits ; les résultats suivants justifient ces restrictions.

Théorème 1.5.5. [SGA4$_2$, VIII, Th. 1.1] Soit $f\colon Y \to X$ un morphisme de schémas. Si f est un homéomorphisme universel alors les foncteurs $- \times_X Y\colon X_{\text{ét}} \to Y_{\text{ét}}$ et $f^\star\colon \operatorname{Ab}(X) \to \operatorname{Ab}(Y)$ qu'il induit sont des équivalences de catégories.

Supposons X de dimension cohomologique finie. Avec ces notations, pour tout $K \in \mathrm{D}^b(X)$, le morphisme $\mathrm{R}\Gamma(X, K) \to \mathrm{R}\Gamma(Y, f^\star K)$ est un quasi-isomorphisme. Les homéomorphismes universels étant exactement les morphismes entiers surjectifs et radiciels, ce théorème fournit les résultats ci-dessous.

Corollaire 1.5.6.

1. Soit X un schéma de dimension cohomologique finie, et X_{red} son réduit. Le morphisme $X_{\text{red}} \to X$ est un homéomorphisme universel [Stacks, 054M] et induit donc pour tout $K \in \mathrm{D}^b(X)$ un quasi-isomorphisme
$$\mathrm{R}\Gamma(X, K) \xrightarrow{\sim} \mathrm{R}\Gamma(X_{\text{red}}, K|_{X_{\text{red}}}).$$
2. Soit X un schéma sur un corps k. Soit $k' \to k$ une extension purement inséparable. Notons $X' = X \times_k k'$. Le morphisme $X' \to X$ est un homéomorphisme universel et induit pour tout $K \in \mathrm{D}(X)$ un quasi-isomorphisme
$$\mathrm{R}\Gamma(X, K) \xrightarrow{\sim} \mathrm{R}\Gamma(X', K|_{X'}).$$
En particulier, cela s'applique au cas où k' est une clôture parfaite de k.

I.5.3 Cohomologie de Čech et triangle de Mayer-Vietoris

Soient X un schéma, et $\mathcal{U} = (U_i \xrightarrow{f_i} X)_{i \in I}$ un recouvrement étale fini de X. Considérons le schéma $U = \coprod_{i \in I} U_i \to X$. Étant donné $i_1, \ldots, i_r \in I$, notons encore $f_{i_1,\ldots,i_r}\colon U_{i_1} \times_X \cdots \times_X U_{i_r} \to X$. Définissons le préfaisceau
$$\mathbb{Z}_{\mathcal{U}} \coloneqq \operatorname{coker}\left[\bigoplus_{i,j \in I} (f_{ij})_!\mathbb{Z} \to \bigoplus_{i \in I} (f_i)_!\mathbb{Z}\right]$$
où les extensions par zéro sont à comprendre au sens des préfaisceaux abéliens. Une résolution projective de $\mathbb{Z}_{\mathcal{U}}$ dans la catégorie $\operatorname{PAb}(X)$ des préfaisceaux de groupes abéliens sur X est donnée par
$$K_{\mathcal{U}} \coloneqq \cdots \to \bigoplus_{i_1,\ldots,i_r \in I} (f_{i_1,\ldots,i_r})_!\mathbb{Z} \to \cdots \to \bigoplus_{i,j \in I} (f_{ij})_!\mathbb{Z} \to \bigoplus_{i \in I} (f_i)_!\mathbb{Z}.$$
Pour tout faisceau $\mathcal{F} \in \operatorname{Ab}(X)$, le complexe $\operatorname{Hom}(K_{\mathcal{U}}, \mathcal{F})$, où les termes non nuls de $K_{\mathcal{U}}$ sont placés en degrés $]-\infty, 0]$, est le complexe de Čech usuel. Notons
$$\check{\Gamma}_P(\mathcal{U}, -) \coloneqq \operatorname{Hom}_{\operatorname{PAb}(X)}(\mathbb{Z}_{\mathcal{U}}, -)\colon \operatorname{PAb}(X) \to \operatorname{Ab}.$$
Soit $O\colon \operatorname{Ab}(X) \to \operatorname{PAb}(X)$ le foncteur d'oubli. Alors
$$\Gamma(X, -) = \check{\Gamma}_P(\mathcal{U}, -) \circ O\colon \operatorname{Ab}(X) \to \operatorname{Ab}$$
et comme tout faisceau injectif est encore un préfaisceau injectif,
$$\mathrm{R}\Gamma(X, -) = \mathrm{R}\check{\Gamma}_P(\mathcal{U}, -) \circ \mathrm{R}O.$$

Étant donné un faisceau $\mathcal{F} \in \mathrm{Ab}(X)$, $\mathrm{R}^i O(\mathcal{F})$ associe à tout X-schéma étale Y le groupe $\mathrm{H}^i(Y, \mathcal{F})$. Dans le cas où $\mathcal{U} = \{U, V\}$ est un recouvrement de X par deux ouverts, la suite spectrale

$$E_2^{pq} = \check{\mathrm{H}}^p(\mathcal{U}, R^q O(\mathcal{F})) \Rightarrow \mathrm{H}^{p+q}(X, \mathcal{F})$$

dégénère à la seconde page, et donne une suite exacte

$$0 \to \mathrm{H}^0(X, \mathcal{F}) \to \mathrm{H}^0(U, \mathcal{F}) \oplus \mathrm{H}^0(V, \mathcal{F}) \to \mathrm{H}^0(U \cap V, \mathcal{F}) \to \mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F}) \oplus \mathrm{H}^1(V, \mathcal{F}) \to \dots.$$

Cette suite exacte, dite de Mayer-Vietoris, découle également de la proposition suivante.

Proposition 1.5.7 (Triangle de Mayer-Vietoris)**.** [Stacks, 0CRS] Soit X un schéma recouvert par deux ouverts U, V. Soit $\mathcal{F} \in \mathrm{Ab}(X)$. Alors il y a un morphisme $\mathrm{R}\Gamma(U \cap V, \mathcal{F}) \to \mathrm{R}\Gamma(X, \mathcal{F})[1]$ qui fait de

$$\mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(U, \mathcal{F}) \oplus \mathrm{R}\Gamma(V, \mathcal{F}) \to \mathrm{R}\Gamma(U \cap V, \mathcal{F}) \to \mathrm{R}\Gamma(X, \mathcal{F})[1]$$

un triangle distingué.

I.5.4 Théorèmes de changement de base

Les théorèmes de changement de base permettent d'exprimer autrement des images directes dérivées ; par exemple, le théorème de changement de base propre permet d'exprimer les fibres de l'image directe dérivée d'un faisceau comme la cohomologie de ce faisceau sur les fibres du morphisme propre en question. Ils servent dans de nombreuses démonstrations, notamment celles des théorèmes de finitude présentés dans la section suivante.

Considérons le diagramme cartésien de schémas suivant :

$$\begin{tikzcd} X' \arrow[r, "v"'] \arrow[d, "u"] & X \arrow[d, "f"] \\ S' \arrow[r, "g"] & S \end{tikzcd}$$

Soit $\mathcal{F}$ un faisceau de groupes abéliens sur X. Le morphisme

$$\mathrm{R}f_\star \mathcal{F} \to \mathrm{R}f_\star \mathrm{R}v_\star v^\star \mathcal{F}$$

obtenu par l'adjonction $v^\star \dashv \mathrm{R}v_\star$ donne via les identifications canoniques

$$\mathrm{R}f_\star \mathrm{R}v_\star = \mathrm{R}(f \circ v)_\star = \mathrm{R}(g \circ u)_\star = \mathrm{R}g_\star \mathrm{R}u_\star$$

un morphisme

$$\mathrm{R}f_\star \mathcal{F} \to \mathrm{R}g_\star \mathrm{R}u_\star v^\star \mathcal{F}$$

qui fournit lui-même, par l'adjonction $g^\star \dashv \mathrm{R}g_\star$, un morphisme dit de changement de base

$$g^\star \mathrm{R}f_\star \mathcal{F} \to \mathrm{R}u_\star v^\star \mathcal{F}.$$

Théorème 1.5.8 (Changement de base propre)**.** [SGA4$_3$, XII, Th. 5.1] Si f est propre et $\mathcal{F}$ est un faisceau de torsion alors le morphisme de changement de base est un isomorphisme.

Corollaire 1.5.9. Soit $\bar{s}$ un point géométrique de S. Si $f\colon X \to S$ est propre et $\mathcal{F}$ est un faisceau abélien de torsion sur X alors la fibre $(\mathrm{R}f_\star \mathcal{F})_{\bar{s}}$ est canoniquement isomorphe à $\mathrm{R}\Gamma(X_{\bar{s}}, \mathcal{F})$.

Théorème 1.5.10 (Changement de base lisse)**.** [SGA4$_3$, XVI, Th. 1.1] Si g est lisse, f est quasi-compact et quasi-séparé et $\mathcal{F}$ est un faisceau dont les fibres géométriques sont de torsion d'ordre inversible sur X alors le morphisme de changement de base est un isomorphisme.

I.5.5 Images directes dérivées et finitude de la cohomologie

Soit $f\colon Y \to X$ un morphisme de schémas. Le foncteur image directe $f_\star\colon \mathrm{Ab}(Y) \to \mathrm{Ab}(X)$ est exact à gauche, et son foncteur dérivé est noté $\mathrm{R}f_\star$. Cette section résume comment calculer les fibres de l'image directe dérivée d'un faisceau, et sous quelles hypothèses les propriétés de constructibilité et de lissité d'un faisceau sont préservées par l'image directe dérivée.

Proposition 1.5.11. [SGA4$_2$, VIII, Th. 5.2] Soit $f\colon Y \to X$ un morphisme quasi-compact et quasi-séparé de schémas. Soit $K \in D^b(Y)$ un complexe de faisceaux abéliens sur Y. Soit $\bar{x}$ un point géométrique de X. Notons $X_{\bar{x}}$ le spectre de l'anneau local strictement hensélien de X en $\bar{x}$. Il y a un isomorphisme canonique dans $D^+(\mathrm{Ab})$:

$$(Rf_\star K)_{\bar{x}} \xrightarrow{\sim} \mathrm{R}\Gamma(Y \times_X X_{\bar{x}}, K).$$

Théorème 1.5.12. [ILO, XIII, Th. 1.1.1] Soient X un schéma quasi-excellent, $f\colon Y \to X$ un morphisme de type fini, $n \geqslant 1$ un entier inversible sur X et $\mathcal{F}$ un faisceau constructible de $\mathbb{Z}/n\mathbb{Z}$-modules sur Y. Alors :

1. Pour tout entier $q \geqslant 0$, le faisceau $\mathrm{R}^q f_\star \mathcal{F}$ est constructible.
2. Il existe un entier N tel que $\mathrm{R}^q f_\star \mathcal{F} = 0$ pour tout $q \geqslant N$.

Un cas particulier de ce théorème, lorsque la cible du morphisme est un corps séparablement clos, est le suivant.

Corollaire 1.5.13. Soit X un schéma de type fini sur un corps séparablement clos k. Pour tout faisceau constructible $\mathcal{F}$ de groupes abéliens sur X et tout entier naturel i, le groupe $\mathrm{H}^i(X, \mathcal{F})$ est fini.

Théorème 1.5.14. [FKD13, I, Th. 8.9] Soit $f\colon Y \to X$ un morphisme propre et lisse de schémas. Soit n un entier inversible sur X. Pour tout faisceau lisse de $\mathbb{Z}/n\mathbb{Z}$-modules sur Y et tout entier naturel i, le faisceau $\mathrm{R}^i f_\star \mathcal{F}$ est lisse sur X.

I.6 Cohomologie à support dans un fermé

I.6.1 Généralités

Soit X un schéma. Soient $i\colon Z \to X$ une immersion fermée, et $j\colon U \to X$ l'inclusion de l'ouvert complémentaire.

Définition 1.6.1. Le foncteur $\Gamma_Z(X, -)\colon \mathrm{Ab}(X) \to \mathrm{Ab}$ des sections à support dans Z est défini par

$$\Gamma_Z(X, -) = \Gamma(Z, i^! -)\colon \mathcal{F} \mapsto \ker(\mathcal{F}(X) \to \mathcal{F}(U)).$$

Ce foncteur est exact à gauche, et ses foncteurs dérivés à droite sont notés $\mathrm{H}^j_Z(X, -)$.

Proposition 1.6.2. [Mil80, III, Prop. 1.25] Soit $K \in \mathrm{D}^b(X)$. La suite exacte

$$0 \to j_!\mathbb{Z} \to \mathbb{Z} \to i_\star\mathbb{Z} \to 0$$

produit par $\mathrm{RHom}(-, \mathcal{F})$ un triangle distingué "ouvert-fermé"

$$\mathrm{R}\Gamma_Z(X, \mathcal{F}) \to \mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(U, \mathcal{F}) \xrightarrow{+1}.$$

I.6.2 Théorème de pureté et suite de Gysin

Le théorème suivant permettra de calculer la cohomologie à support dans un fermé des faisceaux lisses.

Théorème 1.6.3 (Pureté)**.** [ILO, XVI, Th. 3.1.1] Soit X un schéma régulier. Soit $i\colon Z \to X$ une immersion fermée d'un sous-schéma régulier, de codimension c. Soit $\mathcal{F}$ un faisceau localement constant sur X de torsion inversible sur X. Alors il y a un isomorphisme $\Lambda \to \mathrm{R}i^!\Lambda(c)[2c]$ dans $D^+(Z,\Lambda)$.

Nous serons intéressés par le cas où Z et X sont des variétés sur un corps séparablement clos k, et $\mathcal{F}$ est un faisceau lisse de $\mathbb{Z}/n\mathbb{Z}$-modules sur X. Le théorème fournit alors un isomorphisme

$$\mathrm{H}^{r-2c}(Z,\mathcal{F}(-c)) \xrightarrow{\sim} \mathrm{H}^r_Z(X,\mathcal{F}).$$

En notant U l'ouvert complémentaire de Z dans X, la suite ouvert-fermé devient alors la *suite de Gysin* :

$$0 \to \mathrm{H}^{2c-1}(X,\mathcal{F}) \to \cdots \to \mathrm{H}^{r-2c}(Z,\mathcal{F}(-c)) \to \mathrm{H}^r(X,\mathcal{F}) \to \mathrm{H}^r(U,\mathcal{F}) \to \cdots$$

I.7 Cohomologie à support compact

I.7.1 Généralités

Soit k un corps. Soit X un schéma séparé de type fini sur k. D'après un théorème de Nagata [Nag62, Th. 4.3], il existe une immersion ouverte $j\colon X \to \bar{X}$, où $\bar{X}$ est propre sur k. Étant donné un complexe $K \in \mathrm{D}^b(X)$, l'élément $\mathrm{R}\Gamma(\bar{X}, j_!K) \in \mathrm{D}^b(\mathrm{Ab})$ est indépendant du choix de $\bar{X}$ [Mil13, Prop. 18.2].

Définition 1.7.1. Pour tout $K \in \mathrm{D}^b(X,\Lambda)$, on définit

$$\mathrm{R}\Gamma_c(X,K) = \mathrm{R}\Gamma(\bar{X}, j_!K).$$

Les groupes de cohomologie à support compact de K, notés $\mathrm{H}^i_c(X,K)$, sont les groupes de cohomologie de $\mathrm{R}\Gamma_c(X,K)$.

Remarque 1.7.2. Le foncteur $\mathrm{R}\Gamma_c(X,-)$ n'est pas le foncteur dérivé de $\mathrm{H}^0_c(X,-)$. Prenons $X = \mathbb{A}^1$. Nous verrons dans la section II.4.2 que $\mathrm{H}^1(\mathbb{P}^1, j_!\Lambda) = \Lambda$. Par contre,

$$\mathrm{H}^0(\mathbb{P}^1, j_!-) = \bigoplus_{x\in|\mathbb{A}^1|} \mathrm{H}^0_x(\mathbb{A}^1,-).$$

Comme $\mathrm{H}^1_x(\mathbb{A}^1,\Lambda) = \Lambda$ (voir section II.5),

$$\mathrm{R}^1\,\mathrm{H}^0_c(\mathbb{A}^1,\Lambda) \simeq \bigoplus_{x\in|\mathbb{A}^1|} \Lambda \neq \mathrm{H}^1_c(\mathbb{A}^1,\Lambda).$$

I.7.2 Dualité de Poincaré

Soient k un corps algébriquement clos et n un entier inversible dans k. Notons Λ l'anneau $\mathbb{Z}/n\mathbb{Z}$. Soit X un schéma connexe séparé de type fini sur k, lisse de dimension d. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X. Rappelons que pour tout entier naturel i, $\mathrm{Ext}^i(\mathcal{F},\Lambda(d)) = \mathrm{Hom}_{\mathrm{D}(X,\Lambda)}(\mathcal{F},\Lambda(d)[i])$. Un morphisme $\mathcal{F} \to \Lambda(d)[i]$ définit pour tous entiers naturels i,j un morphisme

$$\mathrm{H}^j_c(X,\mathcal{F}) \to \mathrm{H}^{i+j}_c(X,\Lambda(d)).$$

Ceci permet de définir un accouplement

$$\mathrm{H}_c^j(X,\mathcal{F}) \times \mathrm{Ext}^i(\mathcal{F},\Lambda(d)) \to \mathrm{H}_c^{i+j}(X,\Lambda(d)).$$

L'énoncé général de la dualité de Poincaré se trouve dans [SGA4$_3$, XVIII, Th. 3.2.5] ; le cas particulier qui nous concerne est le suivant.

Théorème 1.7.3. [Mil80, VI, Th. 11.1] Il y a un isomorphisme canonique $\mathrm{H}_c^{2d}(X,\Lambda(d)) \xrightarrow{\sim} \Lambda$. Pour tout entier $j \in \{0 \dots 2d\}$, l'accouplement

$$\mathrm{H}_c^j(X,\mathcal{F}) \times \mathrm{Ext}^{2d-j}(\mathcal{F},\Lambda(d)) \to \mathrm{H}_c^{2d}(X,\Lambda(d)) \xrightarrow{\sim} \Lambda$$

est non dégénéré.

Nous nous intéresserons particulièrement au cas où X est une courbe et $\mathcal{F}$ est lisse. Le groupe $\mathrm{Ext}^{2-j}(\mathcal{F},\Lambda(d))$ est alors canoniquement isomorphe à $\mathrm{H}^{2-j}(X,\mathcal{F}^\vee(1))$. Il y a donc en particulier un accouplement non dégénéré

$$\mathrm{H}_c^1(X,\mathcal{F}) \times \mathrm{H}^1(X,\mathcal{F}^\vee(1)) \to \Lambda.$$

I.8 Formule des traces et comptage de points

Soient k_0 un corps fini de cardinal q, et k une clôture algébrique de k_0. Pour tout entier $m \geqslant 1$, notons k_m l'extension de degré m de k_0 dans k. Soit ℓ un nombre premier inversible dans k.

Définition 1.8.1. Soit X un schéma sur k_0. L'endomorphisme de Frobenius géométrique de X, noté Frob_X, est l'endomorphisme défini par l'identité sur l'espace topologique sous-jacent, et par la mise à la puissance q sur le faisceau structural $\mathcal{O}_X$.

En particulier, si X_0 est une variété sur k_0, le morphisme de Frobenius géométrique sur $X(k)$ correspond à la mise à la puissance q des coordonnées des points. Notons $X = X_0 \times_{k_0} k$. Les k_m-points de X sont alors les points fixes de Frob_X^m sur $X_0(k)$. La formule des traces permet de calculer le nombre d'intersection dans $X \times X$ du graphe de Frob_X avec la diagonale ; cette intersection étant transverse, ce nombre d'intersection est exactement le nombre de k_0-points de X_0. Nous n'aurons pas besoin de l'énoncé général portant sur la cohomologie ℓ-adique, mais simplement de la formulation suivante.

Théorème 1.8.2. [SGA4$\frac{1}{2}$, Rapport, Th. 3.2] Soit X un schéma de type fini sur k_0 de dimension d. Notons $X = X_0 \times_{k_0} k$. Soit ℓ un nombre premier inversible dans k_0. Alors pour tous entiers $m, n \geqslant 1$,

$$\#X(k_m) \quad \equiv \quad \sum_{i=1}^{2d} \mathrm{tr}((\mathrm{Frob}_X^m)^\star \mid \mathrm{H}_c^i(X,\mathbb{Z}/\ell^n\mathbb{Z})) \mod \ell^n.$$

CHAPITRE II

Revêtements et cohomologie des courbes

Dans tout ce chapitre, le mot *courbe* désigne un schéma équidimensionnel de dimension 1 sur un corps. Nous préciserons à chaque fois que cela sera nécessaire s'il s'agit d'une courbe connexe, intègre, lisse, affine, projective... Ce chapitre décrit explicitement les groupes de cohomologie des faisceaux constants sur les courbes intègres lisses ou nodales, ainsi que leurs revêtements galoisiens. En particulier, il contient en II.7 la construction d'un revêtement caractéristique de ces courbes qui servira par la suite.

Notations Rappelons que la cohomologie d'un schéma sur un corps non parfait est canoniquement isomorphe à celle du changement de base de ce schéma à la clôture parfaite du corps (voir section I.5.2). Dans tout ce chapitre, k_0 désigne un corps parfait de caractéristique $p \geqslant 0$, et k une clôture algébrique de k_0. Le groupe $\mathrm{Gal}(k|k_0)$ est noté $\mathfrak{G}_0$. Nous fixons un nombre premier ℓ distinct de p ainsi qu'un entier naturel n premier à p et notons Λ l'anneau $\mathbb{Z}/n\mathbb{Z}$.

II.1 Groupe fondamental des courbes

II.1.1 Revêtements de courbes

Nous serons principalement intéressés par les morphismes entre courbes normales (i.e. régulières par [Ser89, IV, Th. 11]), qui sont déterminés par des extensions de corps.

Théorème 2.1.1. [Sza09, Th. 4.3.10, Prop. 4.4.5] Soit X une courbe intègre régulière sur un corps. Soient $\mathcal{C}$ la catégorie des courbes intègres régulières Y munies d'un morphisme fini $f\colon Y \to X$, et $\mathcal{D}$ la catégorie des extensions finies du corps des fonctions $k(X)$ de X. Le foncteur $\mathcal{C}^{\mathrm{op}} \to \mathcal{D}$ qui à (Y, f) associe l'extension $k(X) \xrightarrow{f^\star} k(Y)$ est une équivalence de catégories.

Ceci n'est *jamais* le cas pour les courbes singulières, puisque le morphisme de normalisation induit un isomorphisme entre les corps de fonctions. Pour les morphismes vers une courbe régulière, la platitude est garantie par le résultat ci-après.

Lemme 2.1.2. [Stacks, 0CCK] Soit $f\colon Y \to X$ un morphisme non constant de courbes intègres sur un corps. Si X est normale alors f est plat.

Par conséquent, il est aisé de vérifier si un morphisme $f\colon Y \to X$ entre courbes régulières sur un corps est étale en un point y de Y. L'anneau local $\mathcal{O}_{X,f(y)}$ est un anneau de valuation discrète ; choisissons une uniformisante π de cet anneau. Alors f est étale si et seulement si $f^\star\pi$ est une uniformisante de $\mathcal{O}_{Y,y}$. La proposition suivante affirme qu'une extension séparable de corps de fonctions correspond à un morphisme *génériquement étale*.

Proposition 2.1.3. [Sza09, Prop. 4.5.9] Soit $f\colon Y \to X$ un morphisme de courbes intègres sur un corps. Si l'extension de corps de fonctions correspondante est séparable alors il existe un ouvert U de Y tel que $f|_U$ soit étale.

Exemple 2.1.4.

1. Soit p un nombre premier. Soit $X = \mathbb{P}^1_{\mathbb{F}_p}$. Le morphisme $Y \to X$ défini par l'extension purement inséparable $\mathbb{F}_p(t) \to \mathbb{F}_p(\sqrt[p]{t})$ n'est étale en aucun point de Y [Stacks, 0CCY].
2. Considérons le morphisme de courbes lisses

$$f\colon Y = \operatorname{Spec} \mathbb{C}[x,y]/(y^3 - y + x) \to \mathbb{A}^1_{\mathbb{C}} = \operatorname{Spec} \mathbb{C}[x]$$

défini par $(x,y) \mapsto x$. L'extension de corps de fonctions $\mathbb{C}(x) \to \mathbb{C}(x)[y]/(y^3-y+x)$ est séparable, car son discriminant $-4+27x^2$ est non nul. Par conséquent, le morphisme f est génériquement étale. Elle n'est pas normale, car comme $-4+27x^2$ n'est pas un carré dans $\mathbb{C}(x)$, le polynôme minimal T^3-T+x de y n'a pas toutes ses racines dans $\mathbb{C}(Y)$. Le morphisme est ramifié au-dessus des racines de $-4+27x^2$. Considérons l'ouvert

$$U = \operatorname{Spec} k[x, (27x^2-4)^{-1}]$$

de $\mathbb{A}^1$, et sa préimage

$$V = \operatorname{Spec} k[x, (27x^2-4)^{-1}, y]/(y^3 - y + x)$$

dans X. Le morphisme $V \to U$ est alors fini étale, mais pas galoisien.

II.1.2 Groupe fondamental des courbes

Il est généralement très difficile de calculer le groupe fondamental d'un schéma ; toutefois, le cas des courbes sur un corps algébriquement clos est bien étudié. Soit X une courbe intègre lisse sur un corps algébriquement clos k de caractéristique p. Lorsque $k = \mathbb{C}$, la théorie des extensions de corps de $k(X)$ revient à l'étude des extensions du corps des fonctions méromorphes sur la surface de Riemann associée à X, et le groupe fondamental de X est le complété profini du groupe fondamental topologique de cette surface de Riemann. Ce résultat se transpose ensuite à tout corps de caractéristique nulle. La preuve du résultat correspondant en caractéristique positive, dû à Grothendieck, utilise des techniques bien plus profondes. Elle consiste à considérer X comme la fibre spéciale d'un schéma sur un anneau de valuation discrète de corps des fractions de caractéristique nulle et de corps résiduel k, puis à conclure par un théorème de spécialisation du groupe fondamental [SGA1, X, Th. 3.8].

Théorème 2.1.5. [Sza09, Th. 5.7.13] Soit $r \in \mathbb{N}$. Soit X une courbe intègre propre lisse sur k de genre g. Soient $x_1, \ldots, x_r$ des points fermés de X. Le plus grand quotient pro-p' (c'est-à-dire limite de groupes finis d'ordre premier à p) du groupe fondamental de $U := X - \{x_1, \ldots, x_r\}$ est le groupe pro-p' donné par la présentation suivante.

$$\pi_1^{(p')}(U) = \langle a_1, b_1, \ldots, a_g, b_g, c_1, \ldots, c_r \mid [a_1,b_1]\cdots[a_g,b_g]c_1\cdots c_r = 1\rangle_{p'}$$

Ce théorème donne en particulier une condition nécessaire pour qu'un groupe fini G apparaisse comme le groupe d'automorphismes d'un revêtement galoisien d'une courbe de genre g : il faut pour cela que le plus grand quotient de G d'ordre premier à p puisse être engendré par une famille d'au plus $2g+r$ éléments. La conjecture d'Abhyankar, démontrée par Harbater en 1994 [Har94, Th. 6.2], affirme la réciproque.

Remarque 2.1.6. En caractéristique positive, le groupe fondamental lui-même devient gigantesque. Par exemple, celui de $\mathbb{A}^1_{\overline{\mathbb{F}_p}}$ n'est pas topologiquement de type fini. En effet, il y a pour toute puissance p^j de p un revêtement de groupe $(\mathbb{Z}/p\mathbb{Z})^j$: le revêtement d'Artin-Schreier $x \mapsto x^{p^j} - x$. Ceci permet de construire, pour chaque entier j positif, p^j morphismes continus $\pi_1(\mathbb{A}^1_{\overline{\mathbb{F}_p}}) \to \mathbb{Z}/p\mathbb{Z}$. Il y a donc une infinité de tels morphismes continus, ce qui serait impossible si le groupe fondamental était topologiquement de type fini.

Le cas des courbes singulières a été étudié récemment ; par normalisation, le groupe fondamental d'une courbe singulière s'exprime comme produit libre du groupe fondamental d'une courbe lisse par un groupe profini libre.

Théorème 2.1.7. [Das22, Th. 1.1] Soit X une courbe projective connexe sur k à s composantes irréductibles. Soit $\nu\colon \tilde{X} = C_1 \sqcup \cdots \sqcup C_s \to X$ sa normalisation. Notons

$$\delta := 1 - s + \sum_{x \in X} \left(|\nu^{-1}(x)| - 1 \right).$$

Notons F_δ le groupe libre à δ générateurs, et $\widehat{F_\delta}$ son complété profini. Il y a un isomorphisme de groupes profinis

$$\pi_1(X) \xrightarrow{\sim} \pi_1(C_1) \star \cdots \star \pi_1(C_s) \star \widehat{F_\delta}.$$

II.1.3 Revêtements génériquement étales

Définition 2.1.8. Soit $f\colon Y \to X$ un morphisme fini de courbes intègres sur k_0. Nous dirons que f est génériquement galoisien si l'extension de corps de fonctions correspondante est galoisienne.

Proposition 2.1.9. Soit $f\colon Y \to X$ un morphisme fini étale de courbes intègres normales sur un corps. Notons L/K l'extension de corps de fonctions correspondante. Alors $\mathrm{Aut}(Y|X)^{\mathrm{op}} = \mathrm{Aut}(L|K)$, et le morphisme f est un revêtement galoisien si et seulement s'il est génériquement galoisien.

Démonstration. Le théorème 2.1.1 assure que $\mathrm{Aut}(Y|X)^{\mathrm{op}} = \mathrm{Aut}(L|K)$. Si f est étale alors l'extension L/K est séparable. Par conséquent, le groupe $\mathrm{Aut}(L|K)$ est d'ordre $\deg(f) = [L : K]$ si et seulement si l'extension L/K est galoisienne. □

Un morphisme génériquement galoisien de courbes est étale, et donc galoisien, sur un ouvert. En particulier, si $f\colon Y \to X$ est un revêtement galoisien de courbes affines connexes, le morphisme $\bar{f}\colon \bar{Y} \to \bar{X}$ entre les compactifications lisses de ces courbes est un revêtement génériquement galoisien. Lorsque les courbes en question sont régulières, l'étude locale du morphisme $Y \to X$ au-dessus d'un point x de X revient à l'étude d'une extension de l'anneau de valuation discrète $\mathcal{O}_{X,x}$. Nous nous placerons donc pour le reste de cette section dans la situation

$$\begin{tikzcd} B \arrow[r, hook] & L \\ A \arrow[u, hook] \arrow[r, hook] & K \arrow[u, hook] \end{tikzcd}$$

où A est un anneau de valuation discrète, L est une extension galoisienne de son corps des fractions K, et B est la normalisation de A dans L. Le groupe $G \coloneqq \mathrm{Aut}(L|K)$ agit transitivement sur les idéaux maximaux de B au-dessus de $\mathfrak{m}_A$. Soit $\mathfrak{m}_B$ un idéal maximal de B au-dessus de $\mathfrak{m}_A$. Notons $k_A \coloneqq A/\mathfrak{m}_A$.

Définition 2.1.10. Le groupe de décomposition de $\mathfrak{m}_B$ est le groupe

$$D_{\mathfrak{m}_B} = \{\sigma \in G \mid \sigma(\mathfrak{m}_B) = \mathfrak{m}_B\}.$$

Le groupe d'inertie associé est le groupe

$$I_{\mathfrak{m}_B} = \ker(D_{\mathfrak{m}_B} \to \mathrm{Aut}((B/\mathfrak{m}_B)|k_A)).$$

Supposons désormais L/K finie. Notons $\mathfrak{m}_1, \ldots, \mathfrak{m}_d$ les idéaux maximaux de B au-dessus de $\mathfrak{m}_A$, et $k_1, \ldots, k_d$ leurs corps résiduels. Il existe [Stacks, 09EB] des entiers e et f, appelés respectivement indice de ramification et degré résiduel de B/A, tels que pour tout $i \in \{1 \ldots d\}$, $\mathfrak{m}_A B_{\mathfrak{m}_i} = \mathfrak{m}_i^e B_{\mathfrak{m}_i}$ et $[k_i : k_A] = f$. L'extension est dite sauvagement ramifiée au-dessus de $\mathfrak{m}_A$ si la caractéristique de k_A divise e, et modérément ramifiée sinon. De plus, $[L : K] = def$.

Fixons un indice $i \in \{1 \ldots d\}$, posons $\mathfrak{m} = \mathfrak{m}_i$ et $k_\mathfrak{m} = k_i$. Notons π_A une uniformisante de A, et π_B une uniformisante du localisé $B_\mathfrak{m}$. Alors pour tout $\sigma \in I_\mathfrak{m}$, il existe un unique élément $u_\sigma \in B_\mathfrak{m}^\times$ tel que $\pi_B = \sigma(\pi_B) u_\sigma$.

Proposition 2.1.11. [Stacks, 09EE] La composée

$$I_\mathfrak{m} \xrightarrow{\sigma \mapsto u_\sigma} B_\mathfrak{m}^\times \to k_\mathfrak{m}^\times$$

est à image dans le groupe $\mu_e(k_\mathfrak{m})$ des racines e-ièmes de l'unité dans $k_\mathfrak{m}$ et définit un morphisme de groupes surjectif

$$I_\mathfrak{m} \to \mu_e(k_\mathfrak{m})$$

dont le noyau $P_\mathfrak{m}$ est nul si k_A est de caractéristique nulle, et un p-groupe si la caractéristique de k_A est $p > 0$. Le groupe quotient $I_\mathfrak{m}/P_\mathfrak{m}$ est cyclique d'ordre le plus grand diviseur de e premier à p.

Démonstration. Vérifions simplement la première assertion. Il existe un unique $u \in A^\times$ tel que $\pi_B^e = u\pi_A$. Comme $u_\sigma = \sigma(\pi_B)\pi_B^{-1}$, $u_\sigma^e = \sigma(u)u^{-1}$. Comme $\sigma \in I_\mathfrak{m}$, cet élément est congru à 1 modulo $\mathfrak{m}_B$. □

Nous serons amenés, étant donné un tel revêtement, à calculer la cohomologie de son groupe d'inertie.

Lemme 2.1.12. Soit m un entier. Soit C un groupe cyclique d'ordre divisible par m. Soit M un $(\mathbb{Z}/m\mathbb{Z})[C]$-module sur lequel le sous-groupe de C d'ordre m agit trivialement. Alors le choix d'un générateur de C détermine un isomorphisme $\mathrm{H}^1(C, M) \to M_C$. La notation M_C désigne le module des coinvariants, c'est-à-dire le quotient de M par le sous-module engendré par les éléments de la forme $\sigma \cdot m - m$ où $\sigma \in C$ et $m \in M$.

Démonstration. Soit t un générateur de C. Notons c l'ordre de C, et $N = \sum_{j=0}^{c-1} t^j \in \mathrm{End}(M)$. Les résultats classiques sur la cohomologie des groupes cycliques [Bro82, III.1, Ex. 2] montrent alors qu'il y a un isomorphisme $\mathrm{H}^1(C, M) \to \ker(N)/(t-1)M$, qui associe à un morphisme croisé $f\colon C \to M$ la classe de l'élément $f(t) \in \ker(N)$. Comme $\langle t^{c/m} \rangle$ agit trivialement sur A,

$$N = \sum_{i=0}^{m-1} \sum_{j=0}^{c/m-1} t^{ie/m+j} = m \sum_{j=0}^{c/m-1} t^j$$

est l'endomorphisme nul puisque M est de m-torsion. Par conséquent, $\mathrm{H}^1(C, M)$ est isomorphe à

$$M/(t-1)M = M_C.$$

□

La preuve du résultat suivant est une adaptation de celle de [Fu15, Prop. 8.1.4]. Rappelons que $\Lambda = \mathbb{Z}/n\mathbb{Z}$, où n est un entier inversible dans le corps algébriquement clos k.

Corollaire 2.1.13. Soit $f\colon Y \to X$ un revêtement galoisien de courbes lisses sur k de groupe G. Soient y un point fermé de Y et $x = f(y)$. Supposons que l'indice de ramification de f en y soit divisible par n. Il y a pour tout $\Lambda[G]$-module M un isomorphisme canonique

$$\mathrm{H}^1(I_y, M) \xrightarrow{\sim} M_I(-1)$$

où $M_I(-1)$ désigne $M_I \otimes_\Lambda \mu_n(k)^\vee = M_I \otimes_\Lambda \mathrm{Hom}(\mu_n, \Lambda)$.

Démonstration. D'après la proposition 2.1.11, le groupe I_y/P_y est canoniquement isomorphe à $\mu_e(k)$, où e est l'indice de ramification en y. Fixons un générateur ζ de $\mu_e(k)$. Comme P_y est un p-groupe et M est de n-torsion, le morphisme $M^{P_y} \to M_{P_y}$ est un isomorphisme et les groupes de cohomologie $\mathrm{H}^i(P_y, M)$ sont nuls dès que $i \geqslant 1$ [Wei94, Prop. 6.1.10]. Le lemme précédent appliqué au I_y/P_y-module M^{P_y} assure qu'il y a un isomorphisme

$$\mathrm{H}^1(I_y/P_y, M^{P_y}) \xrightarrow{\sim} (M^{P_y})_{I_y/P_y} \simeq (M_{P_y})_{I_y/P_y} \simeq M_{I_y}$$

qui à un morphisme croisé $f\colon I_y/P_y \simeq \mu_e(k) \to M$ associe l'élément $f(\zeta)$. Le morphisme

$$\mathrm{H}^1(I_y/P_y, M) \otimes \mu_e(k) \to M_{I_y}$$

qui à un morphisme croisé $f\colon I_y/P_y \simeq \mu_e(k) \to M_{I_y}$ et un élément $t \in \mu_n(k)$ associe $f(t)$ est encore un isomorphisme, canonique cette fois-ci. Par conséquent, il y a des isomorphismes canoniques

$$\mathrm{H}^1(I_y/P_y, M) = M_{I_y} \otimes \mu_e(k)^\vee = M_{I_y} \otimes \mu_n(k)^\vee.$$

La suite spectrale de Hochschild-Serre fournit alors la suite exacte

$$0 \to \mathrm{H}^1(I_y/P_y, M_{P_y}) \to \mathrm{H}^1(I_y, M) \to \mathrm{H}^0(I_y/P_y, \mathrm{H}^1(P_y, M)) = 0$$

qui permet de conclure. □

Définition 2.1.14 (Troncature)**.** Soit

$$K = \cdots \xrightarrow{d^{i-1}} K^i \xrightarrow{d^i} K^{i+1} \xrightarrow{d^{i+1}} \cdots$$

un complexe dans une catégorie abélienne $\mathcal{A}$. Soit r un entier. Nous noterons $\tau_{\leqslant r}K$ et appellerons tronqué de K en degré $\leqslant r$ le complexe :

$$\cdots \xrightarrow{d^{r-2}} K^{r-1} \xrightarrow{d^{r-1}} \ker(d^r) \to 0 \to 0 \to \cdots$$

Le morphisme évident $\tau_{\leqslant r}K \to K$ induit un isomorphisme $\mathrm{H}^i(\tau_{\leqslant r}K) \to \mathrm{H}^i K$ pour tout entier $i \leqslant r$. Ce foncteur de troncature définit un endofoncteur de la catégorie dérivée $D(\mathcal{A})$, que nous noterons encore $\tau_{\leqslant r}$.

Pour tout groupe H agissant sur M, notons $C^{12}(H, M)$ le groupe des morphismes croisés $H \to M$. Le complexe $M \xrightarrow{\partial} C^{12}(H, M)$ représente alors $\tau_{\leqslant 1} \operatorname{R}\Gamma(H, M)$.

Lemme 2.1.15. Reprenons les notations et hypothèses du corollaire précédent. Le morphisme canonique $C^{12}(I_y/P_y, M^{P_y}) \to C^{12}(I_y, M)$ admet une section.

Démonstration. Soit $u\colon I_y \to M$ un morphisme croisé. Considérons le diagramme commutatif

$$\begin{tikzcd} I_y \arrow[r, "u"] \arrow[d] & M \arrow[r, "q"] & M_{P_y} \\ I_y/P_y \arrow[r, dashed] & M^{P_y} \arrow[u] \arrow[ur, "\alpha"] & \end{tikzcd}$$

et notons $f = q \circ u$. Pour tout $x \in P_y$ et tout $g \in I_y$, la définition de M_{P_y} assure que $f(xg) = f(x) + q(x \cdot u(g)) = f(x) + f(g)$. Par conséquent, pour tout $x \in P_y$, $f(x^{|P_y|}) = |P_y| f(x)$ doit être nul ; comme la multiplication par $|P_y|$ est un automorphisme de M, cela signifie que $f(x) = 0$. Par conséquent, f passe au quotient en $\bar{f}\colon I_y/P_y \to M_{P_y}$. Notons $\bar{u} = \alpha^{-1} \circ \bar{f}\colon I_y/P_y \to M^{P_y}$. L'application $u \mapsto \bar{u}$ est évidemment linéaire. De plus, $\bar{u}$ est encore un morphisme croisé car $\bar{u}(\bar{g}\bar{h}) = \alpha^{-1} f(gh) = \alpha^{-1} f(g) + q(g \cdot \alpha^{-1} u(h))$. La I_y-linéarité de $\alpha^{-1} q$ conclut. $\square$

Remarque 2.1.16. Ce lemme assure que le quasi-isomorphisme des complexes de cochaînes usuels

$$\tau_{\leqslant 1} \operatorname{R}\Gamma(I_y/P_y, M^{P_y}) \to \tau_{\leqslant 1} \operatorname{R}\Gamma(I_y, M)$$

admet un inverse dans $\mathrm{D}^b_c(\Lambda)$ qui est donné par un vrai morphisme de complexes.

Les revêtements étales d'une courbe affine modérément ramifiés à l'infini sont eux aussi classifiés par un groupe profini : le groupe fondamental modéré.

Définition 2.1.17. Soient X une courbe projective intègre lisse sur un corps séparablement clos k, et K son corps des fonctions. Soit U un ouvert de X. Soient K^{sep} une clôture séparable de K, et $\bar{\eta}$ le point générique géométrique correspondant de U. Soit K^{t} la composée dans K^{sep} des extensions finies L/K telles que la normalisation de X dans L soit étale sur U et modérément ramifiée au-dessus de $X - U$. Le groupe fondamental modéré de U, noté $\pi_1^{\mathrm{t}}(U, \bar{\eta})$ ou simplement $\pi_1^{\mathrm{t}}(U)$, est le groupe $\mathrm{Gal}(K^{\mathrm{t}}|K)$.

De la même façon que $\pi_1^{(p')}(U)$, le groupe $\pi_1^{\mathrm{t}}(U)$ est topologiquement de type fini [SGA1, XIII, Cor. 2.12]. Un résultat plus fort a été récemment démontré par Esnault, Shusterman et Srinivas.

Théorème 2.1.18. [ESS22, Th. 1.2] Soit X une courbe intègre lisse sur un corps algébriquement clos de caractéristique positive. Le groupe $\pi_1^{\mathrm{t}}(X)$ est un groupe profini de présentation finie. Si X est affine alors $\pi_1^{\mathrm{t}}(X)$ est projectif, c'est-à-dire isomorphe à un sous-groupe d'un groupe profini libre.

II.1.4 Ramification : théorie locale

Soit X une courbe intègre lisse sur k. Notons K le corps des fonctions de X, et K^{sep} une clôture séparable de K. Notons $G = \mathrm{Gal}(K^{\mathrm{sep}}|K)$. Soit $\bar{x}$ un point fermé de X. Notons $K_{\bar{x}}$ le corps des fractions de l'anneau strictement hensélien $\mathcal{O}_{X,\bar{x}} \subset K$. Soit $K_{\bar{x}}^{\mathrm{sep}}$ une clôture séparable de $K_{\bar{x}}$. Le choix d'un plongement $K^{\mathrm{sep}} \to K_{\bar{x}}^{\mathrm{sep}}$ détermine une place $\mathfrak{m}$ de K^{sep}. Le groupe de décomposition $D_{\mathfrak{m}} \subset G$ de $\mathfrak{m}$ s'identifie à $\mathrm{Gal}(K_{\bar{x}}^{\mathrm{sep}}|K_{\bar{x}})$; c'est aussi, puisque k est algébriquement clos, le groupe d'inertie $I_{\mathfrak{m}}$, que nous noterons encore I. Rappelons que $G = \lim_\lambda G_\lambda$, où les G_λ sont les quotients finis de G, c'est-à-dire les groupes d'automorphismes des revêtements finis génériquement galoisiens de X. Le résultat suivant découle alors de la proposition 2.1.11.

Proposition 2.1.19. [Stacks, 0BUA] Il y a un morphisme canonique surjectif $I \to \lim_{p \nmid n} \mu_n(k)$. Son noyau P est trivial si $p = 0$, et un pro-p-groupe sinon.

Les groupes I, P, $I_{\mathrm{t}} := I/P$ sont encore appelés groupe d'inertie (resp. d'inertie sauvage, resp. d'inertie modérée) en x. La proposition suivante est analogue au corollaire 2.1.13.

Proposition 2.1.20. [Fu15, Prop. 8.1.4] Avec les notations ci-dessus, soit M un $\Lambda[I]$-module. Alors

$$\mathrm{H}^i(I, M) = \begin{cases} M^I & \text{si } i = 0 \\ M_I(-1) & \text{si } i = 1 \\ 0 & \text{si } i \geqslant 2. \end{cases}$$

Corollaire 2.1.21. Soit $f\colon Y \to X$ un revêtement galoisien de courbes lisses sur k. Soient y un point fermé de Y et $x = f(y)$. Supposons que l'indice de ramification de f en y soit divisible par n. Notons $I \subset \mathrm{Gal}(K^{\mathrm{sep}}|K)$ le groupe d'inertie en x, et $I_y \subset \mathrm{Aut}(Y|X)$ le quotient correspondant. Soit M un $\Lambda[I]$-module. Alors le morphisme composé

$$\tau_{\leqslant 1} \mathrm{R}\Gamma(I_y, M) \to \tau_{\leqslant 1} \mathrm{R}\Gamma(I, M) \to \mathrm{R}\Gamma(I, M)$$

est un isomorphisme dans $\mathrm{D}^b_c(X, \Lambda)$.

Démonstration. Les morphismes en degrés 0 et 1 sont des isomorphismes d'après les propositions précédentes ; en degré supérieur, les groupes de cohomologie de $\mathrm{R}\Gamma(I, M)$ sont nuls. □

II.2 Groupe de Picard et variété jacobienne

Nous verrons dans la suite que le premier groupe de cohomologie d'un faisceau constant sur une courbe lisse sur k est isomorphe à un groupe de points de torsion de la jacobienne de cette courbe.

II.2.1 Foncteur de Picard et variété jacobienne

Définition 2.2.1. Le groupe de Picard d'un schéma X est le groupe des classes d'isomorphisme de $\mathcal{O}_X$-modules (pour la topologie de Zariski) inversibles, avec pour loi de groupe le produit tensoriel. Soit $f\colon X \to S$ un morphisme propre de schémas. Le foncteur de Picard $\mathrm{Pic}_{X/S}$ (resp. $\mathrm{Pic}^0_{X/S}$) est le faisceau associé au préfaisceau $T \mapsto \mathrm{Pic}(X \times_S T)$ (resp. $T \mapsto \mathrm{Pic}^0(X \times_S T)$) sur le gros site étale de S.

Si f admet une section alors pour tout S-schéma T, les sections de ce faisceau sur T sont données par $\mathrm{Pic}_{X/S}(T) = \mathrm{Pic}(X \times_S T)/\mathrm{Pic}(T)$ [BLR90, 8.1, Th. 4].

Théorème 2.2.2. [BLR90, 8.2, Th. 1] Soit $f\colon X \to S$ un morphisme projectif de présentation finie. Supposons f plat à fibres géométriques intègres. Alors le foncteur $\mathrm{Pic}_{X/S}$ est représentable par un S-schéma séparé localement de présentation finie sur S.

Dans le cas des courbes projectives lisses sur un corps, le schéma qui représente le foncteur de Picard est encore une variété projective.

Théorème 2.2.3. [Mil08, III, Th. 1.6] Soit X_0 une courbe projective lisse de genre g sur k_0 munie d'un point rationnel. Alors le foncteur de Picard Pic^0_{X/k_0} est représenté par une variété abélienne J_{X_0} de dimension g appelée variété jacobienne de X_0.

Soit X_0 une courbe projective lisse connexe de genre g sur k_0. La première construction de la variété jacobienne J_{X_0} est due à Weil [Wei48]. Elle consiste à construire une loi de groupe birationnelle sur la puissance symétrique $X_0^{(g)}$ exprimant l'addition des diviseurs, puis à montrer qu'il existe une variété abélienne G et un morphisme birationnel $X_0^{(g)} \to G$ compatible aux lois de groupe. Une deuxième construction, plus directe en ce qu'elle évite l'intermédiaire de la loi de groupe birationnelle, a été donnée par Chow en 1954 [Cho54]. Enfin, Anderson propose dans [And02] une construction différente de la variété jacobienne, sans donner de bornes sur le nombre d'étapes de la construction.

Il existe donc plusieurs algorithmes calculant des équations de la jacobienne de n'importe quelle courbe lisse ; cependant, pour aucun d'entre eux, nous ne disposons de bornes sur sa complexité. Dans le cas des courbes hyperelliptiques, une description explicite de la jacobienne est connue [Mum07, §2]. La complexité du calcul représente un obstacle conséquent à cette construction : par exemple, la jacobienne d'une courbe de genre 2 est décrite par Cassels et Flynn comme intersection de 72 quadriques dans $\mathbb{P}^{15}$ [CF98, Ch. 2, §3]. Cependant, il est beaucoup plus simple de calculer avec des classes de diviseurs sans se soucier de la structure de variété de la jacobienne. Les algorithmes effectuant ces calculs sont présentés dans l'annexe C.3. Nous n'aurons besoin que de résultats précis concernant par exemple la n-torsion de la jacobienne. La proposition suivante est un cas particulier d'un résultat général sur les variétés abéliennes [Mil08, I, Th. 7.2].

Proposition 2.2.4. Soit X une courbe intègre projective lisse sur k de genre g. Soit n un entier inversible dans k. La multiplication par n sur J_X est une isogénie étale de degré n^{2g}, et les k-points de son noyau $J_X[n]$ forment un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang $2g$.

II.2.2 Jacobienne généralisée

Soient X_0 une courbe lisse géométriquement connexe sur k_0, et $X = X_0 \times_{k_0} k$. Notons K le corps des fonctions de X. Soit $\mathfrak{m} = \sum_P m_P P \in \mathrm{Div}(X)$ un diviseur invariant sous l'action du groupe $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$. Notons $|\mathfrak{m}|$ son support. Étant donné une fonction $f \in K^\times$, on dit que $f \equiv 1 \mod \mathfrak{m}$ si pour tout $P \in |\mathfrak{m}|$, $v_P(1-f) \geqslant m_P$. Deux diviseurs $D, D' \in \mathrm{Div}(X)$ sont dits $\mathfrak{m}$-équivalents s'il existe $f \in K^\times$ telle que $D' = D + \mathrm{div}(f)$ et $f \equiv 1 \mod \mathfrak{m}$. Notons $\mathrm{Div}_{\mathfrak{m}}(X) := \mathrm{Div}(X - |\mathfrak{m}|)$.

Définition 2.2.5. Le groupe de Picard $\mathrm{Pic}_{\mathfrak{m}}(X)$ de X relativement à $\mathfrak{m}$ est le quotient de $\mathrm{Div}_{\mathfrak{m}}(X)$ par le sous-groupe des diviseurs de fonctions congrues à 1 modulo $\mathfrak{m}$. Notons encore $\mathrm{Pic}^0_{\mathfrak{m}}(X)$ le sous-groupe de $\mathrm{Pic}_{\mathfrak{m}}(X)$ des classes de diviseurs de degré 0.

Comme le diviseur $\mathfrak{m}$ est défini sur k_0, les groupes $\mathrm{Pic}_{\mathfrak{m}}(X)$ et $\mathrm{Pic}^0_{\mathfrak{m}}(X)$ sont naturellement munis d'une action du groupe $\mathfrak{G}_0$. Remarquons que la classe d'équivalence modulo $\mathfrak{m}$ d'un diviseur D est incluse dans sa classe d'équivalence linéaire usuelle, ce qui permet de définir un morphisme surjectif $\mathrm{Pic}_{\mathfrak{m}}(X) \to \mathrm{Pic}(X)$. Nous supposons dans toute la suite que $\mathfrak{m}$ est réduit, c'est-à-dire que tous les coefficients non nuls de $\mathfrak{m}$ soient égaux à 1. Au vu de sa définition, le groupe $\mathrm{Pic}_{\mathfrak{m}}(X)$ décrit alors les faisceaux inversibles sur X triviaux sur $|\mathfrak{m}|$. Nous supposons dans toute la suite de cette section que X est projective.

Lemme 2.2.6. [Ser75, V.13, Prop. 7] Rappelons que $\mathfrak{m}$ est réduit. Notons $P_1, \ldots, P_s$ les points de son support. Il y a des suites exactes de groupes abéliens

$$0 \to \frac{(k^\times)^s}{k^\times} \to \mathrm{Pic}_{\mathfrak{m}}(X) \to \mathrm{Pic}(X) \to 0$$

et

$$0 \to \frac{(k^\times)^s}{k^\times} \to \mathrm{Pic}^0_{\mathfrak{m}}(X) \to \mathrm{Pic}^0(X) \to 0$$

où $k^\times$ agit par la diagonale sur $(k^\times)^s$, et la flèche de gauche associe à $(\lambda_1, \dots, \lambda_s)$ le diviseur d'une fonction f vérifiant $f(P_i) = \lambda_i$ pour tout i.

Démonstration. Un diviseur sur $X - \mathfrak{m}$ est un diviseur principal sur X si et seulement s'il est de la forme $\mathrm{div}(f), f \in K^\times$ où f n'a ni zéro ni pôle sur le support de $\mathfrak{m}$; il est alors de degré 0. Deux diviseurs $\mathrm{div}(f), \mathrm{div}(g)$ de cette forme sont $\mathfrak{m}$-équivalents si et seulement si $f(P_i) = g(P_i)$ pour tout $i \in \{1 \dots s\}$, d'où l'exactitude au milieu. De même, le diviseur d'une fonction f est $\mathfrak{m}$-équivalent à 0 si et seulement s'il prend la même valeur en tous les points de $\mathfrak{m}$, d'où l'injectivité à gauche. La surjectivité du morphisme de droite découle du fait que tout diviseur sur X est équivalent à un diviseur de support disjoint de $\mathfrak{m}$ (voir annexe C.3.4 ou [Sha94, §1.3]). Par construction, les morphismes de cette suite sont compatibles à l'action de $\mathrm{Gal}(k|k_0)$. □

La proposition suivante permettra de calculer le sous-groupe de n-torsion de $\mathrm{Pic}^0_{\mathfrak{m}}(X)$.

Proposition 2.2.7. Il y a une suite exacte courte de Λ-modules

$$0 \to \frac{\mu_n(k)^{|\mathfrak{m}|}}{\mu_n(k)} \to \mathrm{Pic}^0_{\mathfrak{m}}(X)[n] \to \mathrm{Pic}^0(X)[n] \to 0.$$

Démonstration. Le diagramme commutatif à lignes exactes

$$\begin{tikzcd}
0 \arrow[r] & \frac{(K^\times)^{|\mathfrak{m}|}}{K^\times} \arrow[r] \arrow[d, "n"] & \mathrm{Pic}^0_{\mathfrak{m}}(X) \arrow[r] \arrow[d, "n"] & \mathrm{Pic}^0(X) \arrow[r] \arrow[d, "n"] & 0 \\
0 \arrow[r] & \frac{(K^\times)^{|\mathfrak{m}|}}{K^\times} \arrow[r] & \mathrm{Pic}^0_{\mathfrak{m}}(X) \arrow[r] & \mathrm{Pic}^0(X) \arrow[r] & 0
\end{tikzcd}$$

fournit, par surjectivité de la mise à la puissance n sur $(K^\times)^{|\mathfrak{m}|}/K^\times$, la suite exacte des noyaux :

$$0 \to \frac{\mu_n(k)^{|\mathfrak{m}|}}{\mu_n(k)} \to \mathrm{Pic}^0_{\mathfrak{m}}(X)[n] \to \mathrm{Pic}^0(X)[n] \to 0.$$

□

Remarque 2.2.8. Il existe un groupe algébrique $J_{\mathfrak{m}}$ sur k_0 muni d'une application rationnelle $X_0 \to J_{\mathfrak{m}}$ régulière sur $X - |\mathfrak{m}|$ qui induit un isomorphisme $\mathrm{Pic}^0_{\mathfrak{m}}(X) \to J_{\mathfrak{m}}(k)$: c'est la jacobienne généralisée de X relativement à $\mathfrak{m}$ [Ser75, V.9, Th. 1]. Il paraît hors de portée pour l'instant de déterminer explicitement en temps raisonnable des équations définissant cette jacobienne généralisée ; la proposition précédente montre toutefois comment calculer dans son groupe de n-torsion.

II.2.3 Les μ_n-torseurs sur une courbe lisse

Proposition 2.2.9. Soit X une courbe intègre lisse sur k, de corps des fonctions K. Le groupe $\mathrm{H}^1(X, \mu_n)$ est canoniquement isomorphe au quotient du groupe

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

par le sous-groupe des (D, f) où $f \in (K^\times)^n$.

Démonstration. Soit G le groupe quotient en question. Remarquons que si un couple (D, f) est nul dans G alors D est un diviseur principal. Rappelons que d'après la proposition 1.3.10, le groupe $\mathrm{H}^1(X, \mu_n)$ est canoniquement isomorphe au groupe des classes d'isomorphisme de couples $(\mathcal{L}, \alpha)$ où $\mathcal{L}$ est un faisceau inversible sur X et $\alpha \colon \mathcal{L}^{\otimes n} \xrightarrow{\sim} \mathcal{O}_X$. Considérons le morphisme $F \colon G \to \mathrm{H}^1(X, \mu_n)$ défini par $F(D, f) = (\mathcal{O}_X(D), \mathcal{O}_X(nD) \xrightarrow{m_f} \mathcal{O}_X)$ où m_f désigne la multiplication par f.

- Injectivité : si $F(D,f)$ est égal dans $\mathrm{H}^1(X,\mu_n)$ à $(\mathcal{O}_X,\mathrm{id})$ alors il existe un isomorphisme $\phi\colon \mathcal{O}_X(D) \to \mathcal{O}_X$ tel que ϕ^n soit la multiplication par f. Un tel isomorphisme étant nécessairement la multiplication par un élément de $K^\times$, il en résulte que f est une puissance n-ième dans $K^\times$.
- Surjectivité : soit $(\mathcal{L},\alpha) \in S$. Il existe un diviseur $D \in \mathrm{Div}(X)$ et un isomorphisme de faisceaux $\phi\colon \mathcal{L} \to \mathcal{O}_X(D)$. En particulier, ceci livre un isomorphisme $\alpha \circ \phi^{-n}\colon \mathcal{O}_X(nD) \to \mathcal{O}_X$, qui est la multiplication par une section globale $f \in K^\times$ de $\mathcal{O}_X(nD)$. Alors $(\mathcal{L},\alpha)$ est égal dans S à $F(D,f)$.

□

Corollaire 2.2.10. Sous les mêmes hypothèses, $\mathrm{H}^1(X,\mu_n)$ est isomorphe au quotient du groupe

$$\{(A,f) \in \mathrm{Pic}(X) \times K^\times \mid \exists D \in \mathrm{Div}(X)\colon [D] = A \text{ et } nD = \mathrm{div}(f)\}$$

par le sous-groupe des (A,f) avec $f \in (K^\times)^n$. Si de plus X est projective alors $\mathrm{H}^1(X,\mu_n)$ est isomorphe au sous-groupe de n-torsion $\mathrm{Pic}(X)[n]$ de $\mathrm{Pic}(X)$.

Démonstration. Le morphisme $(D,f) \mapsto ([D],f)$ défini par passage au quotient est évidemment surjectif et a pour noyau les couples (D,f) tels que $f \in (K^\times)^n$. Si X est projective alors l'application surjective $\mathrm{H}^1(X,\mu_n) \to \mathrm{Pic}(X)[n]$ qui à un couple (A,f) associe A est également injective, puisque deux fonctions rationnelles sur X de même diviseur sont égales à un élément de $k^\times$ près. □

Lemme 2.2.11. Supposons X projective. Soient U un ouvert de X, et Z le fermé réduit complémentaire. Notons $\mathrm{Div}^0_Z(X)$ le sous-groupe de $\mathrm{Div}^0(X)$ formé des diviseurs à support dans Z. Considérons les triplets (A,D',f) où $A \in \mathrm{Pic}^0(X)$, $D' \in \mathrm{Div}^0_Z(X)$, $f \in K^\times$ et il existe un diviseur $\bar{D}$ de classe A tels que $n\bar{D} = \mathrm{div}(f) + D'$ dans $\mathrm{Div}^0(X)$. Ces triplets forment un sous-groupe de $\mathrm{Pic}^0(X) \times \mathrm{Div}^0_Z(X) \times K^\times$. Soit H le quotient de ce sous-groupe par celui des $([D'],nD',f)$. Alors $\mathrm{H}^1(U,\mu_n)$ est canoniquement isomorphe à H.

Démonstration. Considérons le morphisme

$$\begin{array}{rcl} H & \longrightarrow & \mathrm{H}^1(U,\mu_n) \\ (A,D',f) & \longmapsto & (A|_U,f) \end{array}$$

où $\mathrm{H}^1(U,\mu_n)$ est identifié au groupe décrit dans le corollaire précédent. Notons que comme $n\bar{D} = \mathrm{div}(f) + D'$, la restriction à U donne bien $n\bar{D}_{|U} = \mathrm{div}(f)|_U$. De plus, si f est une puissance n-ième alors il existe $h \in K^\times$ tel que $n\bar{D} = \mathrm{div}(h^n) + D'$, autrement dit $D' = n(\bar{D} - \mathrm{div}(h))$, et $([D'],D',f) = ([\bar{D} - \mathrm{div}(h)], n(\bar{D} - \mathrm{div}(h)), f)$. Reste à montrer la surjectivité de ce morphisme. Soit donc $([D],f) \in \mathrm{H}^1(U,\mu_n)$, avec $D \in \mathrm{Div}(U)$. Alors $nD = \mathrm{div}(f)|_U$. Soit $\bar{D} \in \mathrm{Div}^0(X)$ un diviseur de restriction D. Alors $E := n\bar{D} - \mathrm{div}(f)$ est un diviseur à support dans Z, de degré nul. Par conséquent, $([D],f)$ est l'image de $([\bar{D}],E,f) \in H$. □

II.3 Groupe de Picard des courbes nodales

II.3.1 Groupe de Picard des courbes singulières

Soit X_0 une courbe intègre sur k_0, et $X = X_0 \times_{k_0} k$. Soit $\pi\colon \tilde{X} \to X$ sa normalisation, qui est finie [Stacks, 035S]. Supposons que X a un unique point singulier P, qui est alors nécessairement défini sur k_0, et que les points de $\tilde{X}$ au-dessus de P sont également définis sur k_0. Considérons la suite exacte de faisceaux sur X :

$$0 \to \mathbb{G}_{m,X} \to \pi_\star \mathbb{G}_{m,\tilde{X}} \to (\pi_\star \mathbb{G}_{m,\tilde{X}})/\mathbb{G}_{m,X} \to 0.$$

Comme π est un isomorphisme en-dehors du lieu singulier de X, le support du faisceau quotient $\mathcal{Q} := (\pi_\star \mathbb{G}_{m,\tilde{X}})/\mathbb{G}_{m,X}$ est $\{P\}$. Par conséquent, la suite exacte longue en cohomologie de cette suite exacte courte est :

$$0 \to \mathrm{H}^0(X, \mathbb{G}_m) \to \mathrm{H}^0(\tilde{X}, \mathbb{G}_m) \to \mathrm{H}^0(X, \mathcal{Q}) \to \mathrm{Pic}(X) \to \mathrm{Pic}(\tilde{X}) \to 0.$$

Lorsque X est projective, $\mathrm{H}^0(X, \mathbb{G}_m) = \mathrm{H}^0(\tilde{X}, \mathbb{G}_m) = k^\times$, ce qui fournit une suite exacte :

$$0 \to \mathrm{H}^0(X, \mathcal{Q}) \to \mathrm{Pic}(X) \to \mathrm{Pic}(\tilde{X}) \to 0.$$

Remarque 2.3.1. La normalisée de la cubique nodale $\operatorname{Spec} k[x,y]/(y^2 - x^2(x+1))$ ou de la cubique cuspidale $\operatorname{Spec} k[x,y]/(y^2 - x^3)$ est la droite affine $\operatorname{Spec} k[t]$. Dans ces deux cas, $\mathrm{H}^0(X, \mathbb{G}_m) = \mathrm{H}^0(\tilde{X}, \mathbb{G}_m) = k^\times$, et la suite

$$0 \to \mathrm{H}^0(X, \mathcal{Q}) \to \mathrm{Pic}(X) \to \mathrm{Pic}(\tilde{X}) \to 0$$

est exacte.

Exemple 2.3.2. Voici un exemple de courbe affine X telle que $\mathrm{H}^0(\tilde{X}, \mathbb{G}_m)$ contienne strictement $\mathrm{H}^0(X, \mathbb{G}_m)$. Considérons l'ouvert $\{x \neq 0\}$ de la cubique nodale précédente, c'est-à-dire

$$X = \operatorname{Spec} k[x,y,z]/(y^2 - x^2(x+1), zx - 1).$$

Sa normalisée est l'ouvert de $k[t]$ situé au-dessus de $\{x \neq 0\}$, c'est-à-dire $\tilde{X} = \operatorname{Spec} k[t,s]/(st^2 - 1)$. Le morphisme de normalisation est donné par $x \mapsto t^2, y \mapsto t^3, z \mapsto s$. La fonction $t = \frac{y}{x}$ est inversible sur $\tilde{X}$ d'inverse st, alors que $\frac{y}{x} \notin \mathrm{H}^0(X, \mathcal{O}_X)^\times$.

II.3.2 Courbes nodales

Soit X_0 une courbe sur k_0. Notons $X = X_0 \times_{k_0} k$, où k désigne toujours la clôture algébrique de k.

Définition 2.3.3. [Stacks, 0C47] Un point fermé P_0 de X_0 est dit nodal s'il existe un point P de X d'image P_0 tel que le complété de l'anneau local $\mathcal{O}_{X,P}$ soit isomorphe à $k[[x,y]]/(xy)$. Une courbe sera dite nodale si elle est singulière et tous ses points singuliers sont nodaux.

Remarque 2.3.4. Le critère jacobien montre que si X possède un unique point singulier P alors X_0 possède un unique point singulier P_0, qui est un k_0-point. Si P est nodal alors P_0 l'est aussi.

Voyons comment reconstruire une courbe nodale à partir de sa normalisation.

Définition 2.3.5. Étant donné une courbe lisse Y sur k et des points deux à deux distincts

$$Q_1, R_1, \ldots, Q_s, R_s \in Y(k)$$

nous noterons $Y_{Q_1=R_1,\ldots,Q_s=R_s}$, ou $Y_{\underline{Q}=\underline{R}}$, la courbe obtenue en identifiant pour tout $i \in \{1 \ldots s\}$ les deux points Q_i et R_i. Sa construction est décrite dans [Ser75, IV,§4].

Proposition 2.3.6. [Ser75, IV.3, Prop. 2) et IV.4, Exemple b] Avec les notations de la définition, si Y est connexe, la courbe $Y_{Q_1=R_1,\ldots,Q_s=R_s}$ est irréductible, de normalisation Y. Elle possède s points singuliers nodaux.

Remarque 2.3.7. Pour $i \in \{1 \ldots s\}$, notons P_i l'image dans $Y_{\underline{Q}=\underline{R}}$ de Q_i et R_i. Les morphismes $C_{Q_i}Y \to C_{P_i}(Y_{\underline{Q}=\underline{R}})$ et $C_{R_i}Y \to C_{P_i}(Y_{\underline{Q}=\underline{R}})$ entre cônes tangents induisent un isomorphisme

$$(C_{Q_i}Y \sqcup C_{R_i}Y)_{Q_i=R_i} \xrightarrow{\sim} C_{P_i}(Y_{\underline{Q}=\underline{R}})$$

où $\sqcup$ désigne le coproduit de schémas.

II.3.3 Groupe de Picard d'une courbe nodale

Soit X_0 une courbe sur k_0, et $X = X_0 \times_{k_0} k$. Supposons que X soit intègre, nodale et possède un unique point singulier P. Notons K le corps des fonctions de X. Soient $\pi\colon \tilde{X} \to X$ sa normalisation, et $j\colon \tilde{X} \to \bar{X}$ la complétion projective lisse de $\tilde{X}$. Il y a exactement deux points Q, R de $\tilde{X}$ au-dessus de P [Stacks, 0CBW]. Remarquons que pour un ouvert U de X contenant P,

$$\mathcal{O}_X(U) = \{f \in \mathcal{O}_{\tilde{X}}(U \times_X \tilde{X}) \mid f(Q) = f(R)\}$$

(voir [Ser75, IV.4,Exemple b)]). Ainsi, un fibré en droites sur X est défini par la donnée d'un fibré en droites $\tilde{\mathcal{L}}$ sur $\tilde{X}$ muni d'un isomorphisme entre les fibres $\tilde{\mathcal{L}}(Q)$ et $\tilde{\mathcal{L}}(R)$.

Lemme 2.3.8. Le groupe $\mathrm{Pic}^0 X$ est isomorphe au groupe $\mathrm{Pic}^0_{\mathfrak{m}}(\tilde{X})$ de la définition 2.2.5, où $\mathfrak{m}$ est le diviseur effectif $Q + R$.

Démonstration. Soit $D \in \mathrm{Div}(X - P)$. Considérons le faisceau inversible $\tilde{\mathcal{L}}_D := \mathcal{O}_{\tilde{X}}(D)$, où l'on considère D comme un diviseur sur la normalisée $\tilde{X}$ de X via l'isomorphisme $X - P \xrightarrow{\sim} \tilde{X} - \{Q, R\}$. Comme la valuation de D en P est nulle, $\tilde{\mathcal{L}}_D(Q)$ est canoniquement isomorphe à la fibre en Q de $\mathcal{O}_{\tilde{X}}$, elle-même canoniquement isomorphe à k. Il en est de même pour $\tilde{\mathcal{L}}_D(R)$. Les fibres $\tilde{\mathcal{L}}_D(Q)$ et $\tilde{\mathcal{L}}_D(R)$ sont identifiées par ces isomorphismes canoniques, ce qui permet de définir canoniquement un fibré en droites $\mathcal{L}_D$ sur X. Le morphisme de groupes $\mathrm{Div}(X - P) \to \mathrm{Pic}(X)$ qui à un diviseur D associe $\mathcal{L}_D$ a pour noyau l'ensemble des diviseurs D tels que $\tilde{\mathcal{L}}_D$ soit isomorphe à $\mathcal{O}_{\tilde{X}}$, c'est-à-dire les diviseurs de la forme $\mathrm{div}(f) \in \mathrm{Div}(X - P)$, où $f \in K^\times$ est définie et n'a ni zéro ni pôle en P. Ceci définit par passage au quotient un morphisme injectif $\mathrm{Pic}^0_{\mathfrak{m}}(\tilde{X}) \to \mathrm{Pic}^0(X)$. Montrons qu'il est surjectif. Un faisceau inversible $\mathcal{L}$ sur X donne un faisceau inversible $\tilde{\mathcal{L}} = \pi^\star \mathcal{L}$ sur $\tilde{X}$ dont les fibres en Q et R sont canoniquement isomorphes. Le faisceau $\tilde{\mathcal{L}}$ est isomorphe à un faisceau $\tilde{\mathcal{L}}_D$, où $D \in \mathrm{Div}(\tilde{X})$; quitte à lui ajouter le diviseur d'une fonction définie en P, on peut supposer que $D \in \mathrm{Div}(\tilde{X} - \{Q, R\}) = \mathrm{Div}(X - P)$. □

Lemme 2.3.9. Nous retrouvons ainsi explicitement la suite exacte courte de groupes abéliens

$$0 \to \mathrm{H}^0(X, \mathbb{G}_m) \to \mathrm{H}^0(\tilde{X}, \mathbb{G}_m) \to (k^\times \times k^\times)/k^\times \to \mathrm{Pic}(X) \to \mathrm{Pic}(\tilde{X}) \to 0$$

déjà évoquée dans la section II.3.1.

Démonstration. On utilise la description de $\mathrm{Pic}(X)$ donnée dans le lemme 2.3.8. La flèche

$$\mathrm{H}^0(\tilde{X}, \mathbb{G}_m) \to (k^\times \times k^\times)/k^\times$$

associe à une fonction f inversible sur $\tilde{X}$ la classe du couple $(f(Q), f(R)) \in k^\times \times k^\times$; ce couple appartient à la diagonale si et seulement si f est définie en P, c'est-à-dire $f \in \mathrm{H}^0(X, \mathbb{G}_m)$. La flèche $k^\times \times k^\times \to \mathrm{Pic}(X)$ associe à (a, b) le diviseur d'une fonction f telle que $f(Q) = a$ et $f(R) = b$. Ce diviseur est celui d'une fonction définie et non nulle en P si et seulement si $a = b$. La flèche de droite est le tiré en arrière $\pi^\star$, qui à la classe de $D \in \mathrm{Div}(X - P)$ dans $\mathrm{Pic}(X)$ associe la classe de $D \in \mathrm{Div}(\tilde{X} - \{Q, R\})$ dans $\mathrm{Pic}(\tilde{X})$. □

Remarque 2.3.10. Décrivons l'action de $\mathfrak{G}_0$ sur $\mathrm{H}^0(X, \pi_\star \mathbb{G}_m/\mathbb{G}_m) = (k^\times \times k^\times)/k^\times$. Soit $\sigma \in \mathfrak{G}_0$. Si σ échange Q et R alors pour tout $(a, b) \in k^\times \times k^\times$, $\sigma \cdot [(a, b)] = [(\sigma(b), \sigma(a))]$, où les crochets désignent la classe dans le quotient par $k^\times$. Sinon, $\sigma \cdot (a, b) = (\sigma(a), \sigma(b))$. Dans toute la suite de ce chapitre, l'action de $\mathfrak{G}_0$ sur $(k^\times \times k^\times)/k^\times$ sera celle-ci.

Remarque 2.3.11. Tous les résultats précédents se généralisent immédiatement au cas où une courbe projective X a plusieurs singularités nodales toutes définies sur k_0. Notons $P_1, \ldots, P_r$ ces points. Au-dessus de chaque P_i se trouvent deux points Q_i, R_i de $\tilde{X}$. Alors $\pi_\star \mathbb{G}_m / \mathbb{G}_m$ est supporté en $P_1, \ldots, P_r$. Il y a de même une suite exacte

$$0 \to \left(\frac{k^\times \times k^\times}{k^\times} \right)^r \to \mathrm{Pic}(X) \to \mathrm{Pic}(\tilde{X}) \to 0.$$

Le groupe $\mathrm{Pic}(X)$ se décrit comme le quotient du groupe des diviseurs sur $X - \{P_1, \ldots, P_r\}$ par les diviseurs de fonctions $f \in \bigcap_i \mathcal{O}_{X,P_i}^\times$. Le premier morphisme de la suite exacte associe à $(a_i, b_i)_{1 \leqslant i \leqslant r}$ le diviseur d'une fonction telle que $f(Q_i) = a_i$ et $f(R_i) = b_i$. On obtient enfin la suite exacte

$$0 \to \left(\frac{\mu_n(k) \times \mu_n(k)}{\mu_n(k)} \right)^r \to \mathrm{H}^1(X, \mu_n) \to \mathrm{H}^1(\tilde{X}, \mu_n) \to 0.$$

II.3.4 Description des μ_n-torseurs sur une courbe nodale

Soient X_0 une courbe sur k_0, et $X = X_0 \times_{k_0} k$. Supposons que X soit intègre, nodale et possède un unique point singulier P. Soit $\bar{X}$ la compactification lisse de $\tilde{X}$. Rappelons (voir lemme 2.2.11) que $\mathrm{H}^1(X, \mu_n)$ s'identifie au groupe des classes d'isomorphisme de couples $(\mathcal{L}, \alpha)$ où $\mathcal{L}$ est un fibré en droites sur X et $\alpha \colon \mathcal{L}^{\otimes n} \to \mathcal{O}_X$ est un isomorphisme. Soit G le quotient du groupe

$$\{(D, f) \in \mathrm{Div}(\tilde{X}) \times (\mathcal{O}_{\tilde{X},Q}^\times \cap \mathcal{O}_{\tilde{X},R}^\times) \mid nD = \mathrm{div}(f)|_{\tilde{X}}, f(Q) = f(R)\}$$

par le sous-groupe des couples (D, f) tels que f soit la puissance n-ième dans $K^\times$ d'une fonction g vérifiant $g(Q) = g(R)$. Ici, les groupes d'inversibles des anneaux locaux $\mathcal{O}_{\tilde{X},Q}$ et $\mathcal{O}_{\tilde{X},R}$ sont vus comme sous-groupes de $K^\times$. Construisons une application $\Phi \colon G \to \mathrm{H}^1(X, \mu_n)$. Soit $(D, f) \in G$. Alors comme $nD = \mathrm{div}(f)$ et f est inversible en Q et R, les points Q et R n'appartiennent pas au support de D. Par conséquent, les fibres en Q et R du faisceau inversible $\tilde{\mathcal{L}}_D \coloneqq \mathcal{O}_{\tilde{X}}(D)$ sur $\tilde{X}$ sont canoniquement isomorphes à celles de $\mathcal{O}_{\tilde{X}}$, elles-mêmes canoniquement isomorphes à k. L'isomorphisme $\tilde{\mathcal{L}}_D(Q) \to \tilde{\mathcal{L}}_D(R)$ défini par le diagramme

$$\begin{tikzcd}
\tilde{\mathcal{L}}_D(Q) \arrow[r, "\sim"] \arrow[d] & \mathcal{O}_{\tilde{X}}(Q) \arrow[r, "\sim"] & k \arrow[d, "1_k"] \\
\tilde{\mathcal{L}}_D(R) \arrow[r, "\sim"] & \mathcal{O}_{\tilde{X}}(R) \arrow[r, "\sim"] & k
\end{tikzcd}$$

permet de définir un faisceau inversible $\mathcal{L}_D$ sur X. La multiplication par f définit un isomorphisme $\tilde{\mathcal{L}}_D^{\otimes n} \to \mathcal{O}_{\tilde{X}}$. La condition $f(Q) = f(R)$ assure que cet isomorphisme de $\mathcal{O}_{\tilde{X}}$-modules définit un isomorphisme de $\mathcal{O}_X$-modules $m_f \colon \mathcal{L}_D^{\otimes n} \to \mathcal{O}_X$. L'application $\Phi \colon G \to \mathrm{H}^1(X, \mu_n)$ associe au couple (D, f) le couple $(\mathcal{L}_D, m_f)$.

Proposition 2.3.12. L'application $\Phi \colon G \to \mathrm{H}^1(X, \mu_n)$ construite ci-dessus est un isomorphisme de $\mathbb{Z}/n\mathbb{Z}$-modules.

Démonstration. Elle est bien définie car elle associe à un couple (D, f) où $D = \mathrm{div}(f)$ et f est la puissance n-ième d'une fonction $g \in K^\times$ vérifiant $g(Q) = g(R)$, le couple $(\mathcal{L}_D, m_f)$, qui est isomorphe au couple $(\mathcal{O}_X, 1)$ via la multiplication par g (qui définit bien un isomorphisme $\mathcal{L}_D \to \mathcal{O}_X$ car $g(Q) = g(R)$). La linéarité de Φ découle directement de sa construction ; passons à l'injectivité. Soit $(D, f) \in G$ tel qu'il existe un isomorphisme de couples $(\mathcal{L}_D, m_f) \to (\mathcal{O}_X, 1)$. Il y a encore un isomorphisme $(\tilde{\mathcal{L}}_D, f) \to (\mathcal{O}_{\tilde{X}}, 1)$, qui est nécessairement la multiplication par une fonction g telle

que $D = \mathrm{div}(g)$. Comme l'isomorphisme$(\tilde{\mathcal{L}}_D, f) \to (\mathcal{O}_{\tilde{X}}, 1)$ défini par g provient d'un isomorphisme $(\mathcal{L}_D, m_f) \to (\mathcal{O}_X, 1)$, la fonction g vérifie encore $g(Q) = g(R)$; par conséquent, la classe du couple (D, f) dans G est 0. Enfin, soit $(\mathcal{L}, \alpha) \in \mathrm{H}^1(X, \mu_n)$. Le couple $(\tilde{\mathcal{L}}, \tilde{\alpha}) \in \mathrm{H}^1(\tilde{X}, \mu_n)$ qui s'en déduit est isomorphe à $(\mathcal{O}_{\tilde{X}}(D), g)$ pour un diviseur D sur $\tilde{X}$ et une fonction $g \in K^\times$ telle que $nD = \mathrm{div}(g)$. Supposons, quitte à ajouter à D un diviseur principal, que le support de D ne contient pas Q et R. Par conséquent, $(\mathcal{L}, \alpha)$ est égal dans $\mathrm{H}^1(X, \mu_n)$ à $(\mathcal{L}_D, m_g)$. □

Supposons maintenant X affine. Soit Z le fermé réduit complémentaire de $\tilde{X}$ dans $\bar{X}$. Notons H le quotient du groupe

$$\{(\bar{D}, D', f) \in \mathrm{Div}^0(\bar{X}) \times \mathrm{Div}^0_Z(X) \times (\mathcal{O}^\times_{\bar{X},Q} \cap \mathcal{O}^\times_{\bar{X},R}) \mid n\bar{D} + D' = \mathrm{div}(f), f(Q) = f(R)\}$$

par le sous-groupe des $(\bar{D}, D', f)$ où f est la puissance n-ième dans $K^\times$ d'une fonction g vérifiant $g(Q) = g(R)$. Considérons l'application $\Psi\colon H \to \mathrm{H}^1(X, \mu_n)$ qui à $(\bar{D}, D', f)$ associe $(\bar{D}|_{\tilde{X}}, f)$.

Proposition 2.3.13. L'application $\Psi\colon H \to \mathrm{H}^1(X, \mu_n)$ définie ci-dessus est un isomorphisme de $\Lambda[\mathfrak{G}_0]$-modules.

Démonstration. La linéarité et l'injectivité de Ψ découlent immédiatement de sa construction. Soit maintenant $(D, f) \in \mathrm{H}^1(X, \mu_n)$. Ce couple vérifie $nD = \mathrm{div}(f)|_{\tilde{X}}$. Soit $\bar{D}$ un diviseur de degré 0 sur $\bar{X}$ de restriction D. Posons $D' = n\bar{D} - \mathrm{div}(f)$. C'est un diviseur de degré 0 et de support inclus dans Z. Par conséquent, $(\bar{D}, D', f) \in H$ a pour image (D, f) par Ψ. □

II.4 Cohomologie des faisceaux constants sur les courbes

II.4.1 Courbes lisses sur un corps algébriquement clos

II.4.1.1 Courbes projectives

Soit X une courbe intègre lisse sur un corps algébriquement clos k. Rappelons que n désigne un entier premier à la caractéristique de k.

Proposition 2.4.1. [SGA4$\frac{1}{2}$, Arcata, Prop. 3.1] Il y a des isomorphismes canoniques

$$\mathrm{H}^i(X, \mathbb{G}_m) = \begin{cases} \Gamma(X, \mathcal{O}_X)^\times & \text{si} \quad i = 0 \\ \mathrm{Pic}(X) & \text{si} \quad i = 1 \\ 0 & \text{si} \quad i \geqslant 2. \end{cases}$$

Supposons désormais X projective ; ceci entraîne que le morphisme $\mathbb{G}_m \xrightarrow{f \mapsto f^n} \mathbb{G}_m$ est, sur les sections globales, la mise à la puissance n sur $k^\times$. La suite exacte de Kummer

$$0 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 0$$

donne alors la suite exacte longue

$$0 \to \mathrm{H}^1(X, \mu_n) \to \mathrm{Pic}(X) \xrightarrow{n} \mathrm{Pic}(X) \to \mathrm{H}^2(X, \mu_n) \to 0.$$

La théorie des variétés abéliennes nous enseigne que la multiplication par n sur la jacobienne J_X est surjective. La suite exacte

$$0 \to J_X(k) \to \mathrm{Pic}(X) \xrightarrow{\deg} \mathbb{Z} \to 0$$

permet d'en déduire que le conoyau de la multiplication par n sur $\mathrm{Pic}(X)$ est $\mathbb{Z}/n\mathbb{Z}$.

Théorème 2.4.2. [Stacks, 03RQ] Soit X une courbe intègre projective lisse sur k. Les groupes de cohomologie de X à valeurs dans μ_n sont canoniquement isomorphes aux groupes suivants.

$$\mathrm{H}^i(X,\mu_n) = \begin{cases} \mu_n(k) & \text{si} \quad i=0 \\ J_X[n] & \text{si} \quad i=1 \\ \mathbb{Z}/n\mathbb{Z} & \text{si} \quad i=2 \\ 0 & \text{si} \quad i \geqslant 3. \end{cases}$$

Si $f\colon Y \to X$ est un morphisme de courbes intègres projectives lisses sur k alors le morphisme induit $f^\star\colon \mathrm{H}^2(X,\mu_n) \to \mathrm{H}^2(Y,\mu_n)$ est la multiplication par $\deg(f)$.

Lemme 2.4.3. Supposons que X provient par changement de base d'une courbe définie sur le sous-corps parfait k_0 de k. L'action de $\mathrm{Gal}(k|k_0)$ sur $\mathrm{H}^1(X,\mu_n)$ se factorise par un quotient d'ordre $n^{O(g^2)}$, où g désigne le genre de X. Par conséquent, si k_0 est fini, il existe une extension k_1/k_0 de degré $n^{O(g^2)}$ et des diviseurs k_1-rationnels $D_1,\dots,D_{2g}$ formant une base de $\mathrm{H}^1(X,\Lambda)$.

Démonstration. La première assertion vient par passage au quotient du morphisme

$$\mathrm{Gal}(k|k_0) \to \mathrm{Aut}_\Lambda(\mathrm{H}^1(X,\mu_n))$$

sachant que $\mathrm{H}^1(X,\mu_n)$ est un Λ-module libre de rang $2g$. La deuxième phrase découle du fait qu'une classe de diviseurs k_1-rationnelle contient toujours un diviseur k_1-rationnel (voir lemme C.3.5 en annexe). □

II.4.1.2 Action du Frobenius et comptage de points

Supposons que k_0 soit un corps fini $\mathbb{F}_q$, et que X provienne par changement de base d'une courbe X_0 sur k_0. Alors X est munie de l'action du morphisme de Frobenius géométrique Frob_q. L'action de Frob_q sur $\mu_n(k)$ est la mise à la puissance q, et celle sur $\mathrm{H}^2(X,\mu_n)$ est l'identité puisqu'un automorphisme ne change pas le degré des diviseurs. Ainsi, en notant t la trace de l'endomorphisme de Frobenius sur $\mathrm{H}^1(X,\mu_n)$, la formule des traces (théorème 1.8.2) assure que le nombre de k_0-points de X est donné par :

$$\#X(k_0) = 1 + q - t \mod n.$$

La fonction zêta de X_0 est alors

$$Z_{X_0}(t) = \frac{L(t)}{(1-t)(1-qt)}$$

où $L(t) = \det(\mathrm{id} - t\,\mathrm{Frob}_q^\star \mid \mathrm{H}^1(X,\mathbb{Q}_\ell)) \in \mathbb{Z}[t]$ est un polynôme de degré $2g$ dont les racines complexes ont pour module $\sqrt{q}^{-1}$. Ceci permet également de compter le nombre de $\mathbb{F}_q$-points de la jacobienne J_X de X. En effet, comme montré dans [Lor96, VIII, Cor. 6.3] :

$$\#J_X(\mathbb{F}_q) = \#\ker(\mathrm{id} - t\,\mathrm{Frob}_q) = \det(1 - \mathrm{Frob}_q^\star \mid \mathrm{H}^1(C,\mathbb{Q}_\ell)) = L(1).$$

En particulier,

$$\#J_X(\mathbb{F}_{q^r}) \sim_{r\to\infty} q^{rg}.$$

II.4.1.3 Courbes affines lisses : suite de Gysin

Soit X une courbe projective connexe lisse sur k. Soient U un ouvert de X, et Z le fermé réduit complémentaire. Seuls les groupes $\mathrm{H}^0(U,\mu_n) = \mu_n(k)$ et $\mathrm{H}^1(U,\mu_n)$ sont non nuls. Rappelons (voir lemme 2.2.11) qu'un élément de $\mathrm{H}^1(U,\mu_n)$ est représenté par un triplet $(D,D',f) \in \mathrm{Div}^0(X) \times \mathrm{Div}^0_Z(X) \times K^\times$

vérifiant $nD = \mathrm{div}(f) + D'$. La suite exacte de Gysin est alors la suite exacte de Λ-modules libres [Stacks, 03RR]

$$0 \to \mathrm{H}^1(X, \mu_n) \xrightarrow{\phi} \mathrm{H}^1(U, \mu_n) \xrightarrow{\psi} \mathrm{H}^0(Z, \Lambda) \xrightarrow{\Sigma} \Lambda \to 0$$

où les flèches sont décrites, avec les notations précédentes, par :

- $\phi([D], f) = ([D], 0, f)$
- $\psi([D], D', f) = D' \mod n$
- $\Sigma((\alpha_P)_{P \in Z}) = \sum_{P \in Z} \alpha_P$.

On peut également décrire explicitement la fonctorialité en la paire (X, U) de cette suite. Soient $\phi\colon X' \to X$ un morphisme de courbes projectives lisses, $U' = X' \times_X U$ et $Z' = X' \times_X Z$. Alors le morphisme $\phi^\star\colon \mathrm{H}^1(U, \mu_n) \to \mathrm{H}^1(U', \mu_n)$ défini par $\phi^\star([D], D', f) = ([\phi^\star D], \phi^\star D', \phi^\star f)$, où $\phi^\star$ désigne encore les tirés en arrière usuels, s'insère dans le diagramme suivant.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(X, \mu_n) \arrow[r] \arrow[d, "\phi^\star"] & \mathrm{H}^1(U, \mu_n) \arrow[r] \arrow[d, "\phi^\star"] & \mathrm{H}^0(Z, \Lambda) \arrow[r] \arrow[d, "\phi^\star"] & \mathrm{H}^2(X, \mu_n) \arrow[r] \arrow[d, "\phi^\star"] & 0 \\
0 \arrow[r] & \mathrm{H}^1(X', \mu_n) \arrow[r] & \mathrm{H}^1(U', \mu_n) \arrow[r] & \mathrm{H}^0(Z', \Lambda) \arrow[r] & \mathrm{H}^2(X', \mu_n) \arrow[r] & 0
\end{tikzcd}$$

Ici, le morphisme $\mathrm{H}^2(X, \mu_n) \to \mathrm{H}^2(X', \mu_n)$ est la multiplication par le degré de ϕ [Stacks, 0AMB].

II.4.2 Dualité de Poincaré pour les courbes lisses

Soit X_0 une courbe projective lisse sur k_0. Soit $j_0\colon U_0 \to X_0$ l'inclusion d'un ouvert strict, et $i_0\colon Z_0 \to X_0$ l'inclusion du fermé réduit complémentaire. Notons U, X, Z, i, j leurs changements de base à k. La suite exacte de faisceaux sur X

$$0 \to j_! \mu_n \to \mu_n \to i_\star \mu_n \to 0$$

montre que $\mathrm{H}^0_c(U, \mu_n) = \ker(\mu_n(k) \to \mu_n(k)^{|Z|}) = 0$ et $\mathrm{H}^2_c(U, \mu_n) = \mathrm{H}^2(X, \mu_n) = \Lambda$. Dans le cas des faisceaux constants, le seul calcul à effectuer est donc celui de $\mathrm{H}^1_c(U, \mu_n)$.

Soient $P_1, \ldots, P_r$ les points fermés de Z. Le diviseur $\mathfrak{m} = \sum_i P_i$ sur X est $\mathfrak{G}_0$-invariant puisque Z provient de Z_0. Considérons le faisceau $\mathbb{G}_{m,Z} \coloneqq \ker(\mathbb{G}_m \to i_\star \mathbb{G}_m)$ des fonctions congrues à 1 modulo $\mathfrak{m}$. Le groupe $\mathrm{H}^1(X, \mathbb{G}_{m,Z})$ classifie les faisceaux inversibles sur X trivialisés sur Z [SGA4$\frac{1}{2}$, Arcata, §2.3] et est donc isomorphe à $\mathrm{Pic}_{\mathfrak{m}}(X)$. La suite longue en cohomologie qui se déduit de cette suite exacte courte est la suite

$$0 \to \frac{\mathrm{H}^0(Z, \mathbb{G}_m)}{\mathrm{H}^0(X, \mathbb{G}_m)} \to \mathrm{Pic}_{\mathfrak{m}}(X) \to \mathrm{Pic}(X) \to 0$$

du lemme 2.2.6.

Lemme 2.4.4. [SGA4$\frac{1}{2}$, Arcata, 2.3.(a)] Il y a un isomorphisme de $\Lambda[\mathfrak{G}_0]$-modules

$$\mathrm{H}^1_c(U, \mu_n) \xrightarrow{\sim} \mathrm{Pic}^0_{\mathfrak{m}}(X)[n].$$

Démonstration. La suite exacte de faisceaux sur X

$$0 \to j_! \mu_n \to \mathbb{G}_{m,Z} \xrightarrow{n} \mathbb{G}_{m,Z} \to 0.$$

donne la suite exacte longue de $\Lambda[\mathfrak{G}_0]$-modules

$$\mathrm{H}^1_c(U,\mu_n) \to \mathrm{H}^1(X,\mathbb{G}_{m,Z}) \xrightarrow{n} \mathrm{H}^1(X,\mathbb{G}_{m,Z}) \to 0.$$

Comme le groupe $H^0(X,\mathbb{G}_{m,Z})$ est trivial, le groupe $\mathrm{H}^1_c(U,\mu_n)$ est donc isomorphe à $\mathrm{H}^1(X,\mathbb{G}_{m,Z})[n] = \mathrm{Pic}_{\mathfrak{m}}(X)[n] = \mathrm{Pic}^0_{\mathfrak{m}}(X)[n]$. □

Dans le cas où $U = X$, l'accouplement

$$\mathrm{H}^1(U,\mu_n) \times \mathrm{H}^1_c(U,\mu_n) \to \mathrm{H}^2_c(U,\mu_n^{\otimes 2}) \xrightarrow{\sim} \mu_n(k)$$

provient de l'autodualité de la jacobienne [SGA4$\frac{1}{2}$, Arcata, §2.3] et est appelé accouplement de Weil. Sa construction explicite se trouve dans [Mum08, §20, p184]. La construction suivante généralise cette dernière au cas où U est affine. Notons K son corps des fonctions.

Définition 2.4.5. Soit $f \in K$. Soit $D \in \mathrm{Div}(X)$ tel que f n'ait ni zéro, ni pôle sur le support de D. L'évaluation de f en D est définie par

$$f(D) = \prod_{P \in |D|} f(P)^{v_P(D)}.$$

La loi de réciprocité suivante, due à Weil, servira dans la construction de l'accouplement.

Proposition 2.4.6. [Ser75, III.4, Prop. 7] Soient $f, g \in K^\times$ deux fonctions de diviseurs disjoints. Alors

$$f(\mathrm{div} g) = g(\mathrm{div} f).$$

Souvenons-nous qu'un élément du groupe $\mathrm{H}^1(U,\mu_n)$ est la classe d'un triplet $([D], D', f)$ avec $[D] \in \mathrm{Pic}^0(X)[n]$, $D' \in \mathrm{Div}^0_Z(X)$ et $f \in K^\times$ vérifie $nD = D' + \mathrm{div}(f)$ (voir lemme 2.2.11). D'autre part, $\mathrm{H}^1_c(U,\mu_n)$ est la n-torsion du groupe $\mathrm{Div}(U)/\{\mathrm{div}(f), f \equiv 1 \mod Z\}$ (voir lemme 2.4.4). Fixons une uniformisante t de X en P_0. Soient $u_1 = ([D_1], D'_1, f_1) \in \mathrm{H}^1(U,\mu_n)$ et $u_2 = [D_2] \in \mathrm{H}^1_c(U,\mu_n)$. Soit $f_2 \in K$ telle que $nD_2 = \mathrm{div}(f_2)$ et $f_2 \equiv 1 \mod Z$. On peut supposer, quitte à ajouter à D_1 le diviseur d'une fonction g et multiplier f_1 par g^n, que les supports de $\mathrm{div}(f_1)$ et D_2 sont disjoints. On suppose également, quitte à multiplier f_1, f_2 par des éléments de $K^\times$, que $(t^{-v_{P_0}(f_i)} f_i)(P_0) = 1$ pour $i = 1, 2$.

Lemme 2.4.7. Avec ces notations,

$$\frac{f_1(D_2)}{f_2(D_1)} \in \mu_n(k).$$

Démonstration.

$$\begin{aligned}
\left(\frac{f_1(D_2)}{f_2(D_1)}\right)^n &= \frac{f_1(nD_2)}{f_2(nD_1)} \\
&= \frac{f_1(\mathrm{div} f_2)}{f_2(\mathrm{div} f_1 + D'_1)} \\
&= \frac{f_1(\mathrm{div} f_2)}{f_2(\mathrm{div}(f_1)) f_2(D'_1)} \\
&= \frac{1}{f_2(D'_1)} && \text{par réciprocité de Weil} \\
&= 1 && \text{car } f_2 \equiv 1 \mod Z.
\end{aligned}$$

□

Définition 2.4.8. Avec ces notations, nous appellerons accouplement de Weil généralisé l'application $e_n\colon \mathrm{H}^1(X,\mu_n)\times \mathrm{H}^1_c(U,\mu_n)\to\mu_n$ définie par

$$e_n(u_1,u_2)\coloneqq \frac{f_1(D_2)}{f_2(D_1)}.$$

Décrivons explicitement comment ces flèches permettent de réaliser la suite de Gysin comme la duale de la suite exacte de cohomologie à support propre. Considérons les isomorphismes

$$\Lambda^\vee \xrightarrow{\mathrm{tr}^\vee} \mathrm{H}^2(X,\mu_n)^\vee \xrightarrow{u} \mathrm{H}^0(X,\Lambda)=\Lambda$$

et $\mathrm{H}^0(Z,\Lambda)^\vee \xrightarrow{v} \mathrm{H}^0(Z,\Lambda)$ donnés respectivement par $u\colon \alpha\mapsto\alpha(1)$ et $v\colon \alpha\mapsto(\alpha(i_P))_{P\in Z}$, où $(i_P)_{P\in Z}$ désigne la base canonique de $\mathrm{H}^0(Z,\Lambda)$. Ici, tr est l'isomorphisme $\mathrm{H}^2(X,\mu_n)\to\Lambda$ du théorème 1.7.3. Le diagramme

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^2(X,\mu_n)^\vee(1) \arrow[r] \arrow[d, "u(1)"] & \mathrm{H}^0(Z,\Lambda)^\vee(1) \arrow[r] \arrow[d, "v(1)"] & \mathrm{H}^1(U,\mu_n)^\vee(1) \arrow[r] \arrow[d] & \mathrm{H}^1(X,\mu_n)^\vee(1) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{H}^0(X,\mu_n) \arrow[r] & \mathrm{H}^0(Z,\mu_n) \arrow[r] & \mathrm{H}^1_c(U,\mu_n) \arrow[r] & \mathrm{H}^1(X,\mu_n) \arrow[r] & 0
\end{tikzcd}$$

où la ligne supérieure est la duale de la suite de Gysin décrite dans la section I.6.2, la suite du bas est celle décrite dans la proposition 2.2.7, et les flèches verticales sont celles décrites précédemment, est commutatif. En particulier, l'orthogonal de $\mathrm{H}^0(Z,\mu_n)/\mathrm{H}^0(X,\mu_n)$ dans $\mathrm{H}^1(U,\mu_n)$ est l'image de $\mathrm{H}^1(X,\mu_n)$.

II.4.3 Courbes nodales sur un corps algébriquement clos

Proposition 2.4.9. Soit X une courbe sur un corps algébriquement clos k, de normalisée $\tilde{X}$. Le morphisme canonique $\mathrm{H}^2(X,\mu_n)\to\mathrm{H}^2(\tilde{X},\mu_n)$ déduit de $\tilde{X}\to X$ par fonctorialité est un isomorphisme.

Démonstration. Notons S le lieu singulier de X et $\nu\colon\tilde{X}\to X$ la normalisation de X. Comme ν est fini, le morphisme $\mu_n\to\nu_\star\nu^\star\mu_n$ est injectif ; comme ν est un isomorphisme en-dehors de S, le quotient $\mathcal{Q}$ est supporté sur S. La suite exacte

$$0\to\mu_n\to\nu_\star\mu_n\to\mathcal{Q}\to 0$$

donne la suite exacte longue

$$\mathrm{H}^1(X,\mathcal{Q})\to\mathrm{H}^2(X,\mu_n)\to\mathrm{H}^2(X,\nu_\star\mu_n)\to\mathrm{H}^2(X,\mathcal{Q})$$

dont les extrémités sont nulles car $\mathcal{Q}$ est un faisceau gratte-ciel. Par conséquent, $\mathrm{H}^2(X,\mu_n)$ est isomorphe à $\mathrm{H}^2(X,\nu_\star\mu_n)$, lui-même isomorphe à $\mathrm{H}^2(\tilde{X},\mu_n)$ par exactitude de $\nu_\star$. □

II.4.3.1 Courbes nodales projectives

Soit X_0 une courbe projective nodale sur k_0, ayant un unique point nodal P. Rappelons que n est premier à la caractéristique de k_0. Notons $X=X_0\times_{k_0}k$, et $\tilde{X}$ la normalisée de X ; c'est le changement de base à k de la normalisée de X_0. Soient Q,R les points de $\tilde{X}$ au-dessus de P. Soit $\mathfrak{m}$ le diviseur $Q+R$ sur $\tilde{X}$.

Proposition 2.4.10. Il y a une suite exacte courte de $\Lambda[\mathrm{Gal}(k|k_0)]$-modules

$$0\to\frac{\mu_n(k)\times\mu_n(k)}{\mu_n(k)}\to\mathrm{H}^1(X,\mu_n)\to\mathrm{H}^1(\tilde{X},\mu_n)\to 0.$$

Démonstration. Comme $P \in X(k_0)$, le diviseur $\mathfrak{m}$ sur X est $\mathfrak{G}_0$-invariant. La suite de Kummer fournit la suite exacte

$$0 \to \mathrm{H}^1(X, \mu_n) \to \mathrm{H}^1(X, \mathbb{G}_m) \xrightarrow{n} \mathrm{H}^1(X, \mathbb{G}_m).$$

Le lemme 2.3.8 fournit alors un isomorphisme canonique

$$\mathrm{H}^1(X, \mu_n) \xrightarrow{\sim} \mathrm{Pic}^0_{\mathfrak{m}}(\tilde{X})[n].$$

Le résultat est maintenant une conséquence directe de la proposition 2.2.7. □

Corollaire 2.4.11. Les groupes de cohomologie de X à valeurs dans μ_n sont les suivants.

$$\mathrm{H}^i(X, \mu_n) = \begin{cases} \mu_n(k) & \text{si} \quad i = 0 \\ \mathrm{Pic}^0_{\mathfrak{m}}(X)[n] & \text{si} \quad i = 1 \\ \mathbb{Z}/n\mathbb{Z} & \text{si} \quad i = 2 \\ 0 & \text{si} \quad i \geqslant 3. \end{cases}$$

II.4.3.2 Courbes nodales affines

Reprenons les notations précédentes, en supposant X affine ; soit $\bar{X}$ la compactification lisse de la normalisation $\tilde{X}$ de X, et Z le fermé réduit complémentaire de $\tilde{X}$ dans $\bar{X}$. Soit Y la courbe construite à partir de $\bar{X}$ en identifiant Q et R. C'est une courbe projective qui contient X, est lisse en-dehors de P et a pour normalisation $\bar{X}$. Elle se construit par exemple de la façon suivante. Soit $X \to \mathbb{A}^1 \to \mathbb{P}^1$ le morphisme donné par une coordonnée. Alors la normalisation de $\mathbb{P}^1$ dans X est une courbe projective contenant un ouvert isomorphe à X [Stacks, 03GT], et lisse en-dehors de cet ouvert. Rappelons que $\mathrm{H}^1(X, \mu_n)$ est le groupe des classes de triplets $([D], D', f) \in \mathrm{Pic}^0(\bar{X}) \times \mathrm{Div}^0_Z(\bar{X}) \times k(X)^\times$ tels que $\mathrm{div}(f) = nD + D'$ et $f(Q) = f(R) \neq 0$. Le groupe $\mathrm{H}^1(Y, \mu_n)$ est le sous-groupe de $\mathrm{H}^1(X, \mu_n)$ constitué des triplets $(\bar{D}, D', f)$ tels que $D' = 0$.

Corollaire 2.4.12. Il y a une suite exacte de $\Lambda[\mathfrak{G}_0]$-modules

$$0 \to \mathrm{H}^1(Y, \mu_n) \xrightarrow{\phi} \mathrm{H}^1(X, \mu_n) \xrightarrow{\psi} \mathrm{Div}^0_Z(\bar{X}) \otimes_{\mathbb{Z}} \Lambda \to 0$$

dont les flèches sont décrites, via les isomorphismes précédents, par :

- $\phi(D, f) = (D, 0, f)$
- $\psi(\bar{D}, D', f) = D' \mod n$

Démonstration. L'exactitude de la suite en $\mathrm{H}^1(Y, \mu_n)$ et $\mathrm{H}^1(X, \mu_n)$ est immédiate. Vérifions la surjectivité à droite. Soit D' un zéro-cycle sur Z vu comme diviseur sur X. Soit $\bar{D} \in \mathrm{Div}(\bar{X})$ un diviseur tel que dans $\mathrm{Pic}(\bar{X})$, $n[\bar{D}] = [D']$. Quitte à ajouter un diviseur principal à $\bar{D}$, on peut supposer que son support est disjoint de $\{Q, R\}$. Il existe donc une fonction $f \in \mathcal{O}^\times_{\bar{X},Q} \cap \mathcal{O}^\times_{\bar{X},R}$ telle que $n\bar{D} = D' + \mathrm{div}(f)$. Alors D' est l'image de $([\bar{D}], D', f)$. □

II.4.4 Courbes lisses sur un corps fini

Supposons ici que k_0 soit un corps fini à q éléments. Soit X_0 une courbe intègre projective lisse sur k_0. Notons $f \colon X_0 \to \operatorname{Spec} k_0$ le morphisme structural, et K_0 le corps des fonctions de X_0. Notons encore $X = X_0 \times_{k_0} k$. Soit $\mathfrak{G}_0$ le groupe $\mathrm{Gal}(k|k_0)$.

II.4.4.1 Cohomologie de $\mathbb{G}_m$ et μ_n

La suite spectrale de Leray associée à l'isomorphisme canonique

$$\mathrm{R}\Gamma(X_0, \mathbb{G}_m) = \mathrm{R}\Gamma(\operatorname{Spec} k_0, \mathrm{R}f_\star \mathbb{G}_m) = \mathrm{R}\Gamma(\mathfrak{G}_0, \mathrm{R}\Gamma(X, \mathbb{G}_m))$$

fournit, grâce à la proposition 2.4.1 et quelques calculs de cohomologie galoisienne, le résultat suivant. Une démonstration détaillée se trouve dans [Lim21].

Théorème 2.4.13. Les groupes de cohomologie de X_0 à valeurs dans $\mathbb{G}_m$ sont les suivants.

$$\mathrm{H}^i(X_0, \mathbb{G}_m) = \begin{cases} \Gamma(X_0, \mathcal{O}_{X_0})^\times & \text{si} \quad i = 0 \\ \operatorname{Pic}(X_0) & \text{si} \quad i = 1 \\ \mathbb{Q}/\mathbb{Z} & \text{si} \quad i = 3 \\ 0 & \text{sinon.} \end{cases}$$

Comme dans le cas des corps algébriquement clos, la suite exacte de Kummer permet alors de calculer la cohomologie de μ_n.

Théorème 2.4.14. Les groupes de cohomologie de X_0 à valeurs dans μ_n sont les suivants.

$$\mathrm{H}^i(X_0, \mu_n) = \begin{cases} \mu_n(k_0) & \text{si} \quad i = 0 \\ \operatorname{Tors}_{X_0}(\mu_n) & \text{si} \quad i = 1 \\ \operatorname{Pic}(X_0)/n \operatorname{Pic}(X_0) & \text{si} \quad i = 2 \\ \mathbb{Z}/n\mathbb{Z} & \text{si} \quad i = 3 \\ 0 & \text{si} \quad i \geqslant 4. \end{cases}$$

Nous avons vu que

$$\mathrm{H}^1(X_0, \mu_n) = \frac{\{([D], f) \in \operatorname{Pic}(X_0) \times K_0^\times \mid nD = \operatorname{div} f\}}{\{\{(D, f) \mid f \in (K_0^\times)^n\}}.$$

Rappelons que $\mathfrak{G}_0 \simeq \hat{\mathbb{Z}}$ est de dimension cohomologique 1, et que $\mathrm{H}^1(\mathfrak{G}_0, \mu_n(k)) = k_0^\times/(k_0^\times)^n$ par le théorème de Hilbert 90. La suite spectrale de Hochschild-Serre associée à l'isomorphisme canonique de foncteurs dérivés

$$\mathrm{R}\Gamma(X_0, \mu_n) = \mathrm{R}\Gamma(\mathfrak{G}_0, \mathrm{R}\Gamma(X, \mu_n))$$

fournit alors une suite exacte courte de groupes abéliens

$$0 \to k_0^\times/(k_0^\times)^n \to \mathrm{H}^1(X_0, \mu_n) \to \mathrm{H}^1(X, \mu_n)^{\mathfrak{G}_0} \to 0$$

dont la première flèche associe à α le couple $(0, \alpha)$. Le morphisme de droite est surjectif car k_0 est de dimension cohomologique 1.

Remarque 2.4.15. Le Λ-module $\mathrm{H}^1(X_0, \mu_n)$ est libre si et seulement si $k_0^\times/(k_0^\times)^n$ l'est, ce qui est le cas si $\operatorname{pgcd}(n, q-1) \in \{1, n\}$.

II.4.4.2 Cup-produit sur les corps finis

Soit ℓ un nombre premier divisant $q-1$. L'étude de l'accouplement

$$\mathrm{H}^1(X_0, \mu_\ell) \times \mathrm{H}^1(X_0, \mu_\ell) \to \mathrm{H}^2(X_0, \mu_\ell^{\otimes 2}) = \operatorname{Pic}(X_0) \otimes \mu_\ell(k)$$

est réalisée dans [BC21]. Les résultats qui y sont obtenus ne permettent le calcul de tous les cup-produits que dans le cas des courbes de genre 1. De même que sur les corps algébriquement clos, il

est nécessaire de fixer un point $P \in X_0(k)$; une fonction $f \in K_0^\times$ est dite normalisée si le coefficient dominant de sa série de Laurent en P est une puissance ℓ-ième dans le corps résiduel $k_0(P)$ [BC21, §1]. Ceci est indépendant du choix d'une uniformisante en P. Toute fonction s'écrit alors comme produit d'une fonction normalisée avec un élément de $k_0^\times/(k_0^\times)^n$. Étant donné une fonction $f \in K_0^\times$ dont la classe du diviseur appartient à $\ell \operatorname{Pic}(X)$, notons $[f]$ son image dans $\mathrm{H}^1(X_0, \mu_\ell)$. Le calcul du cup-produit $[a] \cup [b]$, où $a, b \in K_0^\times$, se ramène alors à deux situations : a et b sont toutes les deux normalisées, ou a est normalisée et $b \in k_0^\times$.

Théorème 2.4.16. [BC21, Th. 1.1, Th 1.2] Notons $\langle -, - \rangle$ l'accouplement de Weil sur $\mathrm{H}^1(X, \mu_\ell)$. Si X est de genre 1 alors pour toutes fonctions $a, b \in K_0$ normalisées et de diviseur dans $\ell \operatorname{Pic}(C)$,

$$[a] \cup [b] = \frac{1}{[k_0(P) : k]} \left([P] \otimes \left\langle \left[\frac{\operatorname{div}(a)}{\ell}\right], \left[\frac{\operatorname{div}(b)}{\ell}\right] \right\rangle \right) \in \operatorname{Pic}(X_0) \otimes \mu_\ell(k).$$

Si X est de genre $\geqslant 2$, cette formule est encore valable si et seulement si l'image dans $\mathrm{H}^2(X_0, \mu_\ell^{\otimes 2})$ par le cup-produit des classes de fonctions normalisées est un sous-espace vectoriel de dimension au plus 1.

Dans la section V.4, nous décrirons une façon de calculer explicitement les cup-produits dans la cohomologie des faisceaux lisses sur X.

II.5 Cohomologie à support dans un fermé

Soit X une courbe intègre sur un corps algébriquement clos k. Soient Z un sous-schéma fermé réduit strict de X, et U l'ouvert complémentaire. Comme Z est zéro-dimensionnel, $\mathrm{H}^0_Z(X, -) = \bigoplus_{z \in Z} \mathrm{H}^0_z(X, -)$, ce qui ramène le problème du calcul des $\mathrm{H}^i_Z(X, -)$ au cas où Z est un point fermé de X. Notons $i \colon z \to X$ l'inclusion de ce point, et $j \colon U \to X$ l'inclusion de l'ouvert $X - \{z\}$. Dans le cas où X est lisse et $\mathcal{F}$ est un faisceau lisse sur X, le théorème de pureté affirme que $\mathrm{H}^j_z(X, \mathcal{F}) = \mathrm{H}^{j-2}(z, \mathcal{F}(-1))$. Ces groupes sont donc tous nuls, sauf lorsque $j = 2$; le groupe $\mathrm{H}^2_z(X, \mathcal{F})$ est isomorphe par pureté à $\mathrm{H}^0(z, \mathcal{F}(-1))$. Le résultat suivant concerne le prolongement par zéro à X des faisceaux lisses sur U, sans hypothèse de régularité sur X.

Lemme 2.5.1. Soit $\mathcal{F}$ un faisceau lisse sur U.

- $\mathrm{H}^0_z(X, j_!\mathcal{F}) = \mathrm{H}^0_z(X, j_\star\mathcal{F}) = \mathrm{H}^1_z(X, j_\star\mathcal{F}) = 0$
- $\mathrm{H}^1_z(X, j_!\mathcal{F}) = \mathrm{H}^0(z, \mathcal{F})$
- $\mathrm{H}^2_z(X, j_!\mathcal{F}) = \mathrm{H}^2_z(X, j_\star\mathcal{F})$
- Pour tout $i \geqslant 3$, $\mathrm{H}^i_z(X, j_!\mathcal{F}) = \mathrm{H}^i_z(X, j_\star\mathcal{F}) = 0$.

Démonstration. Comme $\mathrm{H}^0(X, j_\star\mathcal{F}) \to \mathrm{H}^0(U, \mathcal{F})$ est un isomorphisme et $\mathrm{H}^1(X, j_\star\mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F})$ est un monomorphisme d'après le lemme 1.3.8, la suite exacte de cohomologie à support pour $j_\star\mathcal{F}$ assure que $\mathrm{H}^0_z(X, j_\star\mathcal{F}) = \mathrm{H}^1_z(X, j_\star\mathcal{F}) = 0$. De plus, pour tout $j \geqslant 3$, les groupes $\mathrm{H}^{j-1}(U, j_\star\mathcal{F})$ et $\mathrm{H}^j(X, \mathcal{F})$ sont nuls, donc $\mathrm{H}^j_z(X, j_\star\mathcal{F}) = 0$. Rappelons que $\mathrm{H}^i_z(X, i_\star -) = \mathrm{H}^i(Z, -)$. La suite exacte longue des $\mathrm{H}^i_z(X, -)$ associée à la suite exacte courte

$$0 \to j_!\mathcal{F} \to j_\star\mathcal{F} \to i_\star i^\star j_\star\mathcal{F} \to 0$$

assure que $\mathrm{H}^0_z(X, j_!\mathcal{F}) = 0$, $\mathrm{H}^1_z(X, j_!\mathcal{F}) = \mathrm{H}^0(Z, \mathcal{F})$ et $\mathrm{H}^2_z(X, j_!\mathcal{F}) = \mathrm{H}^2_z(X, j_\star\mathcal{F})$. De même, le groupe $\mathrm{H}^i_z(X, j_!\mathcal{F})$ est nul dès que $i \geqslant 3$.

□

Le seul groupe restant à calculer est donc $\mathrm{H}^2_z(X, j_!\mathcal{F}) = \mathrm{H}^2_z(X, j_\star\mathcal{F})$.

II.5.1 Calcul de $\mathrm{H}^2_z(X, j_!\mathcal{F})$ lorsque z est régulier

Voici la situation : X est une courbe intègre sur un corps algébriquement clos, z est un point fermé régulier de X de complémentaire l'ouvert U, et $\mathcal{F}$ est un faisceau lisse sur U. Notons $X_{\bar{z}}$ le spectre de l'hensélisé strict de l'anneau local de X en z. Notons $j' \colon \eta \to X_{\bar{z}}$ l'inclusion du point générique.

Lemme 2.5.2. Il y a un isomorphisme canonique $\mathrm{H}^2_z(X, j_!\mathcal{F}) \to \mathrm{H}^1(\eta, \mathcal{F}_\eta)$.

Démonstration. Par excision, pour tout voisinage étale affine de $Y \to X$ tel que la préimage de z soit réduite à un point y, le groupe $\mathrm{H}^2_z(X, j_!\mathcal{F})$ est canoniquement isomorphe à $\mathrm{H}^2_y(Y, (j_!\mathcal{F})|_Y)$ [Mil80, III, Cor. 1.28]. Comme la limite de ces voisinages est $X_{\bar{z}}$, on a $\mathrm{H}^2_z(X, j_!\mathcal{F}) = \mathrm{H}^2_z(X_{\bar{z}}, j'_!\mathcal{F}_\eta)$. La suite exacte de cohomologie sur $X_{\bar{z}}$ à support sur z montre alors que $\mathrm{H}^2_z(X_{\bar{z}}, j'_!\mathcal{F}_\eta) = \mathrm{H}^1(\eta, \mathcal{F}_\eta)$ [Mil06, II, Prop. 1.1]. □

Notons $K = \mathrm{Frac}(\mathcal{O}_{X,\bar{z}})$. Rappelons que le groupe d'inertie I_z est aussi le groupe $\mathrm{Gal}(K^{\mathrm{sep}}|K)$. La cohomologie de η est donc la cohomologie galoisienne de I_z, et $\mathrm{H}^1(\eta, \mathcal{F}_\eta) = \mathrm{H}^1(I_z, M)$, où M désigne le $\pi_1(U, u)$-module $\mathcal{F}_\eta$. Rappelons que $\mathrm{H}^1(I_z, M)$ est isomorphe à $M_{I_z}(-1)$ par la proposition 2.1.20.

Il est maintenant possible de comprendre plus explicitement la suite exacte ouvert-fermé de la proposition 1.6.2 pour le faisceau $j_!\mathcal{F}$. C'est la suite

$$0 \to \mathrm{H}^0(U, \mathcal{F}) \to \mathrm{H}^1_Z(X, j_!\mathcal{F}) \to \mathrm{H}^1(X, j_!\mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F}) \to \mathrm{H}^2_Z(X, j_!\mathcal{F}) \to \mathrm{H}^2(X, j_!\mathcal{F}) \to 0.$$

Soit G le groupe d'automorphismes d'un revêtement galoisien $V \to U$ qui trivialise $\mathcal{F}$. Le groupe $\mathrm{H}^2(X, j_!\mathcal{F})$ est isomorphe par dualité de Poincaré à $\mathrm{H}^0(U, \mathcal{F}^\vee(1))^\vee = ((M^\vee(1))^G)^\vee = M_G(-1)$. La suite se réécrit donc

$$0 \to M^G \to \bigoplus_z M^{I_z} \to \mathrm{H}^1(X, j_!\mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F}) \to \bigoplus_z M_{I_z}(-1) \to M_G(-1) \to 0.$$

Remarquons que l'inclusion $j_!\mathcal{F} \to j_\star\mathcal{F}$ fournit le diagramme commutatif

$$\begin{tikzcd}
\mathrm{H}^1(X, j_!\mathcal{F}) \arrow[r] \arrow[d] & \mathrm{H}^1(U, j^\star j_!\mathcal{F}) \arrow[r, "\sim"] \arrow[d] & \mathrm{H}^1(U, \mathcal{F}) \arrow[d, "\mathrm{id}"] \\
\mathrm{H}^1(X, j_\star\mathcal{F}) \arrow[r] & \mathrm{H}^1(U, j^\star j_\star\mathcal{F}) \arrow[r, "\sim"] & \mathrm{H}^1(U, \mathcal{F})
\end{tikzcd}$$

La flèche $\mathrm{H}^1(X, j_!\mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F})$ est donc la composée du morphisme $\mathrm{H}^1(X, j_!\mathcal{F}) \to \mathrm{H}^1(X, j_\star\mathcal{F})$ déduit de $j_!\mathcal{F} \to j_\star\mathcal{F}$ avec le morphisme injectif $\mathrm{H}^1(X, j_\star\mathcal{F}) \to \mathrm{H}^1(U, j^\star j_\star\mathcal{F}) = \mathrm{H}^1(U, \mathcal{F})$ obtenu par restriction. En termes de torseurs, cette flèche associe à un $j_!\mathcal{F}$-torseur $\mathcal{T}$ sur X la restriction à U du $j_\star\mathcal{F}$-torseur $\mathcal{T} \wedge^{j_!\mathcal{F}} j_\star\mathcal{F}$. La première moitié de la suite ci-dessus s'identifie à la suite exacte issue de la suite exacte longue associée à

$$0 \to j_!\mathcal{F} \to j_\star\mathcal{F} \to i_\star i^\star j_\star\mathcal{F} \to 0.$$

La deuxième moitié de la suite s'écrit

$$0 \to \mathrm{H}^1(X, j_\star\mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F}) \to \bigoplus_z M_{I_z}(-1) \to M_G(-1) \to 0.$$

Nous verrons dans la section II.7.1.1 comment construire un revêtement trivialisant $V \to U$ tel que $\mathrm{H}^1(U, \mathcal{F}) = \mathrm{H}^1(G, M)$, ce qui permet de comprendre le morphisme $\mathrm{H}^1(U, \mathcal{F}) \to \mathrm{H}^2_z(X, j_!\mathcal{F})$ comme le morphisme de restriction $\mathrm{H}^1(G, M) \to \mathrm{H}^1(I_z/(I_z \cap \pi_1 V), M)$.

II.5.2 Calcul de $\mathrm{H}^2_z(X, j_!\mathcal{F})$ lorsque z est nodal

Considérons désormais la situation suivante : X est une courbe intègre sur un corps algébriquement clos, z est un point fermé nodal de X de complémentaire l'ouvert U. Notons $\nu\colon \tilde{X} \to X$ la normalisation de X, et x, y les points de $\tilde{X}$ au-dessus de z. Notons $X_{\bar{z}}$ le spectre de l'hensélisé strict de l'anneau local de X en z. Il est constitué de trois points : un point fermé z', et deux idéaux premiers minimaux x', y' correspondant aux branches de X en z. Notons $U_{\bar{z}} := X_{\bar{z}} \times_X U = \{x'\} \sqcup \{y'\}$; ce schéma est canoniquement isomorphe au coproduit des points génériques des hensélisés de $\tilde{X}$ aux points x et y (voir section III.6 pour les détails). La situation est résumée par le diagramme cartésien suivant.

$$\begin{tikzcd}
U_{\bar{z}} \arrow[r, "j'"] \arrow[d, "g'"] & X_{\bar{z}} \arrow[d, "g"] & z' \arrow[l, "i'"'] \arrow[d] \\
U \arrow[r, "j"] & X & z \arrow[l, "i"']
\end{tikzcd}$$

Lemme 2.5.3. Soit $\mathcal{F}$ un faisceau sur $U_{\bar{z}}$. Pour tout entier naturel q, le groupe $\mathrm{H}^q(X_{\bar{z}}, j'_!\mathcal{F})$ est nul.

Démonstration. Cette preuve adapte celle de [Mil06, II, Prop. 1.1] au cas des courbes nodales. L'affirmation est vraie pour $q = 0$ car $\mathrm{H}^0(X_{\bar{z}}, j'_!\mathcal{F})$ est le noyau de $\mathrm{H}^0(X_{\bar{z}}, j'_\star\mathcal{F}) \to \mathrm{H}^0(X_{\bar{z}}, i'_\star i'^\star j'_\star\mathcal{F})$, qui n'est rien d'autre que le morphisme identité de $\mathrm{H}^0(U_{\bar{z}}, \mathcal{F})$. Montrons d'abord que pour tout faisceau injectif J sur $U_{\bar{z}}$, le faisceau $j'_!J$ sur X est acyclique. Pour ce faire, commençons par prouver que la suite exacte courte

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

est une résolution injective de $j'_!J$. Fixons des clôtures séparables de $k(x')$ et $k(y')$, et notons respectivement $I_{x'}$ et $I_{y'}$ les groupes de Galois associés. Le foncteur $i^\star j_\star$ s'identifie au foncteur

$$\begin{array}{rcl} \mathrm{Mod}_{I_{x'}} \times \mathrm{Mod}_{I_{y'}} & \to & \mathrm{Ab} \\ (M, N) & \mapsto & M^{I_{x'}} \times N^{I_{y'}} \end{array}$$

qui admet pour adjoint à gauche le foncteur associant à un groupe abélien M le couple (M, M) muni des actions triviales de $I_{x'}$ et $I_{y'}$. Cet adjoint à gauche étant exact, le foncteur $i'^\star j'_\star$ préserve les injectifs. Comme $i'_\star$ et $j'_\star$ préservent également les injectifs, la suite exacte ci-dessus est bien une résolution injective de $j'_!J$. La suite exacte longue en cohomologie associée à cette suite exacte courte montre alors que $\mathrm{H}^q(X_{\bar{z}}, j'_\star J) = 0$ pour tout entier $q \geqslant 1$. Soit $\mathcal{F}$ un faisceau sur $U_{\bar{z}}$, et $J^\bullet$ une résolution injective de $\mathcal{F}$. Alors $j'_!J^\bullet$ est une résolution acyclique de $j'_!\mathcal{F}$, et $\mathrm{H}^q(X_{\bar{z}}, j'_!\mathcal{F}) = \mathrm{H}^q(\Gamma(X_{\bar{z}}, j'_!J^\bullet))$. Ce dernier groupe est l'image de $\mathcal{F}$ par le q-ième foncteur dérivé de $\Gamma(X_{\bar{z}}, j'_!-)$, qui est nul. □

Lemme 2.5.4. Soit $\mathcal{L}$ un faisceau lisse sur $U_{\bar{z}}$. Il y a un isomorphisme canonique

$$\mathrm{H}^1(x', \mathcal{L}_{x'}) \times \mathrm{H}^1(y', \mathcal{L}_{y'}) \xrightarrow{\sim} \mathrm{H}^2_z(X, j_!\mathcal{L}).$$

Démonstration. Il y a toujours par excision un isomorphisme canonique

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

La suite exacte de cohomologie sur $X_{\bar{z}}$ à support sur z' pour le faisceau $j'_!g'^\star\mathcal{L}$ s'écrit :

$$\mathrm{H}^1(X_{\bar{z}}, j'_!g'^\star\mathcal{L}) \to \mathrm{H}^1(U_{\bar{z}}, g'^\star\mathcal{L}) \to \mathrm{H}^2_{z'}(X_{\bar{z}}, j'_!g'^\star\mathcal{L}) \to \mathrm{H}^2(X_{\bar{z}}, j'_!g'^\star\mathcal{L}).$$

Le lemme précédent assure alors que

$$\mathrm{H}^1(U_{\bar{z}}, g'^\star\mathcal{L}) \to \mathrm{H}^2_{z'}(X_{\bar{z}}, j'_!g'^\star\mathcal{L})$$

est un isomorphisme. Comme $U_{\bar{z}}$ est le coproduit des schémas $\{x'\}$ et $\{y'\}$, le groupe $\mathrm{H}^1(U_{\bar{z}}, g'^\star\mathcal{L})$ est simplement le produit de $\mathrm{H}^1(x', \mathcal{L}_{x'})$ et $\mathrm{H}^1(y', \mathcal{L}_{y'})$. □

Soit Z un fermé reduit zéro-dimensionnel de X, et U l'ouvert complémentaire. Notons $\nu\colon \tilde{X} \to X$ la normalisation de X, et $\tilde{Z}$ la préimage de Z dans $\tilde{X}$. Il y a un morphisme de foncteurs

$$\Gamma_Z(X, -) \to \Gamma_{\tilde{Z}}(\tilde{X}, \nu^\star -).$$

Corollaire 2.5.5. Soit $\mathcal{L}$ un faisceau lisse sur U. Le morphisme $\mathrm{R}\Gamma_Z(X, j_\star\mathcal{L}) \to \mathrm{R}\Gamma_{\tilde{Z}}(\tilde{X}, \nu^\star j_\star\mathcal{L})$ est un quasi-isomorphisme.

Démonstration. D'après le lemme 2.5.1, il suffit de montrer que $\mathrm{H}^2_Z(X, j_\star\mathcal{L}) \to \mathrm{R}\Gamma_{\tilde{Z}}(\tilde{X}, \nu^\star j_\star\mathcal{L})$ est un isomorphisme. Notons Z_{reg} (resp. Z_{sing}) l'ensemble des points de Z qui sont des points réguliers (resp. singuliers) de X. Soient $z_1, \dots, z_r$ les points de Z_{sing} ; pour chaque $i \in \{1 \dots r\}$, notons x_i, y_i les antécédents de z_i dans $\tilde{Z}$. En un point z de Z_{reg}, le morphisme $\mathrm{H}^2_z(X, j_\star\mathcal{L}) \to \mathrm{H}^2_z(\tilde{X}, \nu^\star j_\star\mathcal{L})$ est clairement un isomorphisme. Pour tout entier i, le morphisme

$$\mathrm{H}^2_{z_i}(X, j_\star\mathcal{L}) \to \mathrm{H}^2_{x_i}(\tilde{X}, j_\star\mathcal{L}) \oplus \mathrm{H}^2_{y_i}(\tilde{X}, j_\star\mathcal{L})$$

n'est autre que le morphisme identité de

$$\mathrm{H}^1(x'_i, \mathcal{L}_{x'_i}) \oplus \mathrm{H}^1(y'_i, \mathcal{L}_{y'_i}) \to \mathrm{H}^1(x'_i, \mathcal{L}_{x'_i}) \oplus \mathrm{H}^1(y'_i, \mathcal{L}_{y'_i})$$

où x'_i, y'_i désignent les points génériques respectifs des hensélisés stricts de $\tilde{X}$ en x_i, y_i. Le morphisme $\mathrm{H}^2_Z(X, j_\star\mathcal{L}) \to \mathrm{H}^2_{\tilde{Z}}(\tilde{X}, \nu^\star j_\star\mathcal{L})$ est simplement la somme directe de tous ces isomorphismes. □

II.6 Revêtements cycliques de courbes

II.6.1 Revêtements cycliques de courbes lisses

Fixons dans cette section un corps parfait k_0 et un entier n inversible dans k_0. Notons $\Lambda = \mathbb{Z}/n\mathbb{Z}$. Supposons également que k_0 contient une racine primitive n-ième de l'unité. Soit X_0 une courbe intègre lisse sur k_0. Notons K son corps des fonctions.

Lemme 2.6.1. [Sza09, Lem. 5.8.2] Soient $D \in \mathrm{Div}(X_0)$ et $f \in K$ tels que $\mathrm{div}(f) = nD \in \mathrm{Div}(X)$. Alors la normalisation Y_0 de X_0 dans $K(\sqrt[n]{f})$ est finie étale sur X_0. Si de plus D est d'ordre n dans $\mathrm{Pic}(X_0)$ alors $Y_0 \to X_0$ est galoisien de groupe Λ.

Démonstration. Soient P un point fermé de X_0, et $t \in K$ une uniformisante en P. Si $v_P(f) = 0$ alors la fibre $Y_{0,P}$ est isomorphe à $k[x]/(x^n - f(P))$, qui est une algèbre étale sur k puisque n est inversible dans k. Si $v_P(f) \neq 0$, comme $\mathrm{div}(f) = nD$, il existe $i \in \mathbb{N}$ et $u \in \mathcal{O}^\times_{X_0,P}$ tels que $f = ut^{ni}$. Alors $K(\sqrt[n]{f}) = K(\sqrt[n]{u})$, ce qui nous ramène au cas précédent puisque $v_P(u) = 0$. La finitude de $Y_0 \to X_0$ est une propriété de la normalisation [GW10, Prop. 12.44].
Supposons désormais que la classe de $\mathrm{div}(f)$ est d'ordre n dans $\mathrm{Pic}(X_0)$. Notons $g = \sqrt[n]{f} \in L := K(\sqrt[n]{f})$. Montrons que pour tout diviseur strict d de n, la fonction $g^d \in L$ n'est pas un élément de K, ce qui suffit d'après [Lan02, Th. 6.2.(ii)] à prouver que L/K est galoisienne de groupe Λ. Supposons qu'il existe un tel $d < n$ tel que $g^d \in K$. Alors le diviseur $D' := \mathrm{div}(g^d) - dD \in \mathrm{Div}\, X_0$ vérifie $\frac{n}{d}D' = 0 \in \mathrm{Div}(X_0)$, ce qui implique que $D' = 0$. Par conséquent, $dD = \mathrm{div}(g^d)$ est principal, ce qui est absurde puisque D est d'ordre n dans $\mathrm{Pic}(X_0)$. □

Corollaire 2.6.2. Rappelons que k_0 contient une racine primitive n-ième de l'unité. Un morphisme $Y_0 \to X_0$ est un revêtement étale galoisien de groupe Λ si et seulement s'il existe $f \in K^\times$ tel que Y_0 soit la normalisation de X_0 dans $K(\sqrt[n]{f})$.

Démonstration. Soit L le corps des fonctions de Y_0. Si $Y_0 \to X_0$ est galoisien de groupe Λ, c'est encore le cas de L/K. La théorie de Kummer assure alors qu'un tel f existe [Stacks, 09DX]. La réciproque est le lemme précédent. □

II.6.2 Revêtements de courbes nodales

II.6.2.1 Revêtements irréductibles

Soit X une courbe nodale sur k, de points nodaux $P^{(1)}, \dots, P^{(r)}$. Soit $\tilde{X}$ sa normalisée. Pour $i \in \{1 \dots r\}$, notons $Q^{(i)}, R^{(i)}$ les antécédents de $P^{(i)}$ dans $\tilde{X}$.

Soit $\tilde{Y}$ un revêtement galoisien de $\tilde{X}$ de groupe G d'ordre s. Au-dessus de $Q^{(i)} \in \tilde{X}$ se trouvent s points $Q_1^{(i)}, \dots, Q_s^{(i)} \in \tilde{Y}$. Pour $i \in \{1 \dots r\}$, soit $R_1^{(i)}$ un point de $\tilde{Y}$ au-dessus de $R^{(i)}$. Notons, pour $j \in \{1 \dots s\}$, $\sigma_j^{(i)}$ le $\tilde{X}$-automorphisme de $\tilde{Y}$ qui envoie $Q_1^{(i)}$ sur $Q_j^{(i)}$, et notons $R_j^{(i)}$ le point $\sigma_j^{(i)}(R_1^{(i)})$. Considérons la courbe $Y := (\tilde{Y})_{Q_j^{(i)} = R_j^{(i)}}$ où i parcourt $\{1 \dots r\}$ et j parcourt $\{1 \dots s\}$. Elle possède rs points singuliers $P_j^{(i)}$.

Lemme 2.6.3. La courbe Y est un revêtement galoisien de X de groupe G.

Démonstration. L'étalitude du morphisme $Y \to X$ au point $P^{(i)}$ est montrée par le diagramme commutatif suivant, déduit de la remarque 2.3.7.

$$\begin{tikzcd}
(C_{Q_i}\tilde{Y} \sqcup C_{R_i}\tilde{Y})_{Q_i = R_i} \arrow[r, "\sim"] \arrow[d, "\sim"] & C_{P_i}Y \arrow[d] \\
(C_Q\tilde{X} \sqcup C_R\tilde{X})_{Q=R} \arrow[r, "\sim"] & C_P X
\end{tikzcd}$$

Comme les points $Q_j^{(i)}, R_j^{(i)}$ ont été numérotés de façon compatible à l'action de G sur $\tilde{Y}$, tout $\tilde{X}$-automorphisme σ_j de $\tilde{Y}$ induit un X-automorphisme de Y, vérifiant $\sigma_j(P_1^{(i)}) = P_j^{(i)}$. Par conséquent, $Y \to X$ est un revêtement galoisien de groupe G. □

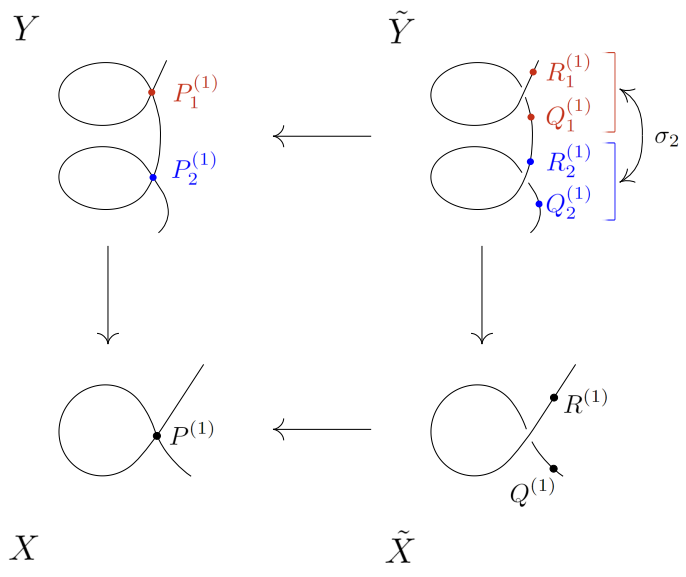


FIGURE II.1 – Le revêtement $Y \to X$ lorsque $r = 1$

Corollaire 2.6.4. Soit $\mathcal{C}$ la catégorie des revêtements galoisiens de X de groupe G. Soit $\tilde{C}$ la catégorie des revêtements galoisiens (connexes !) de $\tilde{X}$ de groupe G. Le foncteur $F\colon C \to \tilde{C}$ qui à un revêtement $W \to X$ associe $\tilde{W} \to \tilde{X}$, où $\tilde{W}$ est la normalisée de W, est une équivalence de catégories.

Démonstration. Montrons que le foncteur $F'\colon \tilde{C} \to C$ construit au début de cette section II.6.2.1 est un quasi-inverse de F. Soit $W \to X$ un revêtement galoisien. Le morphisme $\tilde{W} \to W$ passe au quotient en $F'(\tilde{W}) \to W$, qui est un isomorphisme. D'autre part, soit $Y \to \tilde{X}$ un revêtement galoisien. Le morphisme $Y \to F'(Y)$ est fini, et la propriété universelle de la normalisation assure qu'il se factorise par la normalisation de $F'(Y)$. Le morphisme $Y \to F(F'(Y))$ ainsi obtenu est un isomorphisme. □

II.6.2.2 Revêtements cycliques non irréductibles

Les courbes connexes lisses sur k_0 sont toutes irréductibles, ce qui n'est pas le cas des courbes connexes singulières. Voici comment construire des revêtements connexes cycliques non irréductibles de courbes nodales irréductibles.

Soit X une courbe intègre sur k_0. Supposons X nodale, de points singuliers $P^{(1)}, \dots, P^{(r)}$. Soit $\tilde{X}$ sa normalisée. Notons, pour $i \in \{1 \dots r\}$, $Q^{(i)}$ et $R^{(i)}$ les points de $\tilde{X}$ au-dessus de $P^{(i)}$. Nous supposerons dans la suite de la construction que les points $Q^{(i)}, R^{(i)}$ sont tous définis sur k_0. Dans $\tilde{X} \times \Lambda$, notons $Q_j^{(i)}, R_j^{(i)}$ les points de la j-ième composante $\tilde{X}$ au-dessus de $P^{(i)}$. Considérons la courbe W_i obtenue à partir de $\tilde{X} \times \Lambda$ en identifiant, pour tout $j \in \Lambda$ et tout $m \neq i$, $Q_j^{(i)}$ à $R_{j+1}^{(i)}$ et $Q_j^{(m)}$ à $R_j^{(m)}$. La courbe W_i est connexe, de normalisée $\tilde{X} \times \Lambda$, et possède n composantes irréductibles, images de celles de $\tilde{X} \times \Lambda$. Notons encore $P_1^{(i)}, \dots, P_n^{(i)}$ les antécédents de $P^{(i)}$ dans W_i. Dans l'illustration ci-dessous, les couleurs permettent de distinguer les deux composantes irréductibles de W_1.

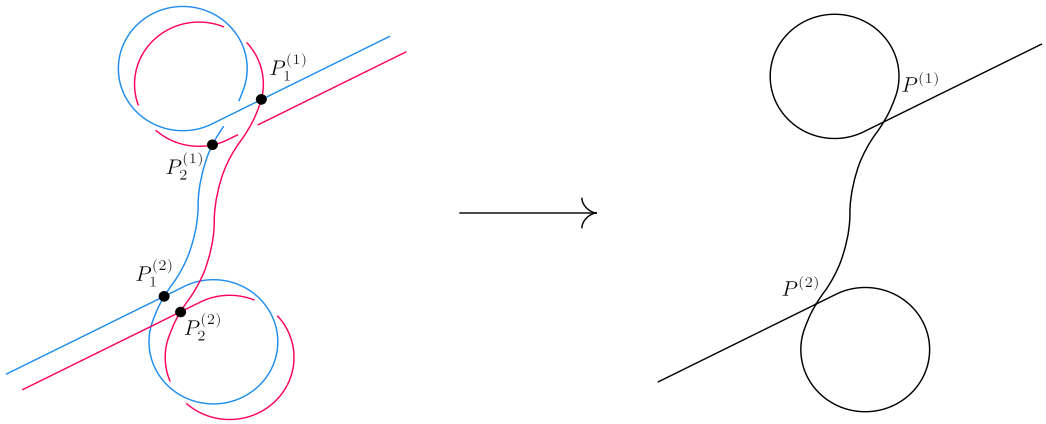


FIGURE II.2 – Le revêtement $W_1 \to X$ pour $n = 2$

Proposition 2.6.5. Le morphisme $f_i\colon W_i \to X$ est un revêtement galoisien de groupe Λ.

Démonstration. Le morphisme f_i est clairement étale en dehors de $f_i^{-1}(P^{(1)}, \dots, P^{(r)})$. Soit $m \neq i$. Au-dessus du point $P^{(m)}$ pour $m \neq i$, le revêtement $W_i \to X$ est localement coproduit de n revêtements obtenus à partir de $\tilde{X} \to X$ en identifiant les deux points $Q^{(m)}$ et $R^{(m)}$: il est donc étale en ce point.

Étudions les antécédents de $P^{(i)}$. Pour tout $j \in \Lambda$, la remarque 2.3.7 fournit un diagramme commutatif

$$\begin{tikzcd}
(C_{Q_j^{(i)}}\tilde{X} \sqcup C_{R_{j+1}^{(i)}}\tilde{X})_{Q_j^{(i)}=R_{j+1}^{(i)}} \arrow[r, "\sim"] \arrow[d, "\wr"] & C_{P_j^{(i)}}W \arrow[d, "f_i"] \\
(C_{Q^{(i)}}\tilde{X} \sqcup C_{R^{(i)}}\tilde{X})_{Q^{(i)}=R^{(i)}} \arrow[r, "\sim"] & C_{P^{(i)}}X
\end{tikzcd}$$

qui montre que f_i est étale en $P_j^{(i)}$. De plus, il est propre car $\tilde{X} \times \Lambda \to X$ l'est [Stacks, 0AH6]. Comme ses fibres sont finies, f_i est donc fini [Stacks, 02OG]. Le degré de f_i est clairement n. Exhibons un monomorphisme $\Lambda \to \mathrm{Aut}(W|X)$. Pour $i \in \Lambda$, le X-automorphisme $\sigma_i \colon \tilde{X} \times \Lambda \to \tilde{X} \times \Lambda$ qui envoie la j-ième copie de $\tilde{X}$ sur la $i+j$-ième induit un X-automorphisme de W_i. Par conséquent, f_i est un revêtement galoisien de groupe Λ. □

Remarque 2.6.6. Le revêtement $W_i \to X$ est en particulier un Λ-torseur (non trivial car connexe) sur X. Remarquons que $W_i \times_X \tilde{X}$ est la normalisation de W [Stacks, 07TD, 0CDV], c'est-à-dire $\tilde{X} \times \Lambda$. Le Λ-torseur non trivial $W_i \to X$ devient donc trivial après changement de base à $\tilde{X}$.

Considérons désormais le revêtement $W \coloneqq W_1 \times_X \cdots \times_X W_r$ de X.

Lemme 2.6.7. Le morphisme $f \colon W \to X$ est un revêtement galoisien de groupe Λ^r.

Démonstration. Le morphisme f est clairement fini étale de degré n^r. Montrons que W est connexe. Comme $W \to W_1$ est lisse, la normalisée de W est [Stacks, 07TD] :

$$\begin{aligned}
\tilde{W} &= \tilde{W}_1 \times_{W_1} (W_1 \times_X \cdots \times_X W_r) \\
&= (\tilde{X} \times \Lambda) \times_{W_1} W_1 \times_X W_2 \times \cdots \times_X W_r \\
&= (\tilde{X} \times \Lambda) \times_X W_2 \times_X \cdots \times_X W_r \\
&= (\tilde{W}_2 \times \Lambda) \times_X \cdots \times_X W_r \\
&= (\tilde{X} \times \Lambda^2) \times_X W_3 \times_X \cdots \times_X W_r \\
&\vdots \\
&= \tilde{X} \times \Lambda^r.
\end{aligned}$$

Le point $(Q^{(i)}, j_1, \ldots, j_r) \in \tilde{X} \times \Lambda^r$ a pour image

$$T^{(i)}_{j_1,\ldots,j_r} \coloneqq (f_1(Q^{(i)}_{j_1}), \ldots, f_r(Q^{(i)}_{j_r})) \in W_1 \times_X \times_X \cdots \times_X W_r.$$

Les images dans W des copies numéro $(j_1, \ldots, j_i, \ldots, j_r)$ et $(j_1, \ldots, j_i + 1, \ldots, j_r)$ de $\tilde{X}$ dans $\tilde{W}$ ont pour point commun $T^{(i)}_{j_1,\ldots,j_r}$, qui est l'image de $(Q^{(i)}, j_1, \ldots, j_r)$ et $(R^{(i)}, j_1, \ldots, j_i + 1, \ldots, j_r)$. Par conséquent, W est connexe. Le morphisme $\prod_{i=1}^{r-1} \mathrm{Aut}(W_i|X) \to \mathrm{Aut}(W|X)$ est injectif car chaque $W_i \to X$ est surjectif, et par conséquent $W \to X$ est galoisien de groupe Λ^r. □

II.6.3 Les courbes sont des $K(\pi, 1)$

Rappelons que le corps k est algébriquement clos.

Proposition 2.6.8. Soit X une courbe intègre sur k. Si X remplit l'une des conditions suivantes alors X est un $K(\pi, 1)$ et un $K(\pi, 1)$ pro-ℓ.

1. X est affine
2. X est projective lisse de genre non nul

3. X est projective nodale et de genre géométrique non nul

Démonstration. Soit $\mathcal{F}$ un faisceau lisse de $\Lambda = \mathbb{Z}/n\mathbb{Z}$-modules sur X. Notons ρ le morphisme de topos $X_{\text{ét}} \to X_{\text{fét}}$. Comme X est une courbe, $\mathrm{H}^i(X, \mathcal{F})$ est nul dès que $i > 2$. De plus, il est toujours vrai que $\mathrm{id} \to R\rho_\star\rho^\star$ est un isomorphisme en degrés $\leqslant 1$. La proposition est donc démontrée dans le cas où X est affine. Supposons désormais qu'elle est projective, de genre géométrique non nul. D'après la proposition 1.4.10, il suffit donc de montrer qu'il existe un revêtement $\pi\colon Z \to X$ tel que le morphisme $\mathrm{H}^2(X, \mathcal{F}|) \to \mathrm{H}^2(Z, \mathcal{F}|_Z)$ soit nul. Notons $\nu\colon \tilde{X} \to X$ la normalisation de X. Soit $Y \to \tilde{X}$ un revêtement connexe trivialisant le faisceau lisse $\nu^\star\mathcal{F}$. Considérons le revêtement Y_2 de Y de groupe $\mathrm{H}^1(Y, \Lambda)^\vee$. Soit Z le revêtement de X obtenu comme décrit dans la section II.6.2.1 ; sa normalisation est Y_2. Le morphisme $\mathrm{H}^2(Y, \mathcal{F}) \to \mathrm{H}^2(Y_2, \mathcal{F})$ est nul, car c'est la multiplication par $\deg(Z \to Y)$, qui est un multiple de n puisque le genre de Y est non nul. Le diagramme commutatif

$$\begin{tikzcd}
\mathrm{H}^2(Z, \mathcal{F}) \arrow[r, "\sim"] & \mathrm{H}^2(Y_2, \mathcal{F}) \\
\mathrm{H}^2(X, \mathcal{F}) \arrow[u] \arrow[r, "\sim"] & \mathrm{H}^2(\tilde{X}, \mathcal{F}) \arrow[u, "0"']
\end{tikzcd}$$

conclut. La courbe X est donc un $K(\pi, 1)$. La même preuve convient pour les $K(\pi, 1)$ pro-ℓ : un faisceau ℓ-monodromique sur $\tilde{X}$ est trivialisé par un revêtement $Y \to \tilde{X}$ de groupe un ℓ-groupe, et le revêtement $Z \to X$ obtenu à partir de $Y_2 \to Y$ est encore un ℓ-revêtement. □

Corollaire 2.6.9. Soit X_0 une courbe sur k_0. Notons $X = X_0 \times_{k_0} k$. Si X vérifie l'une des propriétés de la proposition précédente alors X_0 est un $K(\pi, 1)$ et un $K(\pi, 1)$ pro-ℓ.

Démonstration. Soit $\mathcal{F}$ un faisceau lisse sur X_0. L'isomorphisme canonique $\mathfrak{G}_0$-équivariant

$$\mathrm{R}\Gamma(\pi_1(X), \mathcal{F}_{\bar{\eta}}) \xrightarrow{\sim} \mathrm{R}\Gamma(X, \mathcal{F}|_X)$$

induit un isomorphisme canonique

$$\mathrm{R}\Gamma(\pi_1(X_0), \mathcal{F}_{\bar{\eta}}) = \mathrm{R}\Gamma(\mathfrak{G}_0, \mathrm{R}\Gamma(\pi_1(X), \mathcal{F}_{\bar{\eta}})) \xrightarrow{\sim} \mathrm{R}\Gamma(\mathfrak{G}_0, \mathrm{R}\Gamma(X, \mathcal{F}|_X)) = \mathrm{R}\Gamma(X_0, \mathcal{F}).$$

□

II.7 Un revêtement caractéristique

II.7.1 Sur un corps algébriquement clos

II.7.1.1 La construction

Proposition 2.7.1. Soit G un groupe topologiquement de type fini. Considérons le groupe abélien $\Lambda = \mathbb{Z}/n\mathbb{Z}$, muni de l'action triviale de G. Il existe un unique sous-groupe distingué H de G tel que G/H soit isomorphe au Λ-dual $\mathrm{H}^1(G, \Lambda)^\vee$ de $\mathrm{H}^1(G, \Lambda)$. Ce sous-groupe est l'adhérence de $G^n[G, G]$; il est caractéristique dans G.

Démonstration. Notons S l'adhérence de $G^n[G, G]$. C'est un sous-groupe caractéristique de G car tout automorphisme de G préserve G^n et $[G, G]$. Comme Λ est un groupe abélien de n-torsion, il y a un isomorphisme canonique

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

Notons que comme G est topologiquement de type fini et G/S est un Λ-module, G/S a un ouvert dense fini. Comme un ouvert d'un groupe topologique compact est d'indice fini, G/S est lui-même un Λ-module de type fini, et $\mathrm{Hom}_{\mathrm{cont}}(G/S,\Lambda) = \mathrm{Hom}(G/S,\Lambda)$. Un Λ-module de type fini n'étant rien d'autre qu'une somme directe de $\mathbb{Z}/n_i\mathbb{Z}$ avec $n_i|n$, tout Λ-module de type fini est canoniquement isomorphe à son bidual. Par conséquent, l'isomorphisme ci-dessus devient par passage au dual

$$\mathrm{H}^1(G,\Lambda)^\vee \xrightarrow{\sim} G/S.$$

De plus, comme $\mathrm{H}^1(G,\Lambda)^\vee$ est un groupe abélien de n-torsion, tout sous-groupe H de G tel qu'il y ait un isomorphisme $G/H \to \mathrm{H}^1(G,\Lambda)^\vee$ contient S ; il y est même égal puisque les quotients ont le même cardinal. □

Soit X une courbe intègre lisse ou nodale sur k. Notons K son corps des fonctions. Comme le groupe $\pi_1^{(p')}(X)$ est topologiquement de type fini, il existe un revêtement galoisien $X_2 \to X$, modérément ramifié à l'infini, de groupe $\mathrm{H}^1(\pi_1^{(p')}(X),\Lambda)^\vee = \mathrm{H}^1(\pi_1(X),\Lambda)^\vee$. Décrivons comment construire ce revêtement $X_2 \to X$. Nous avons vu dans la proposition 2.2.9 que le groupe

$$\mathrm{H}^1(\pi_1(X),\mu_n(k)) \simeq \mathrm{H}^1(X,\mu_n) \simeq \{(D,g) \in \mathrm{Div}(X) \times K^\times \mid nD = \mathrm{div} g\}/\{(D,g) \mid g \in (K^\times)^n\}$$

est un $\mathbb{Z}/n\mathbb{Z}$-module libre. Notons r son rang. Soit $(D_i,g_i)_{1\leqslant i\leqslant r}$ une base de $\mathrm{H}^1(X,\mu_n)$. Considérons, pour $i = 0,\dots,r$, les extensions $L_i = K(\sqrt[n]{g_1},\dots,\sqrt[n]{g_i})$ de K ; soit $\phi_i\colon Y_i \to X$ la normalisation de X dans L_i. Notons $L = L_r$, et $\phi\colon Y \to X$ le revêtement correspondant de X.

Lemme 2.7.2. Le morphisme $\phi\colon Y \to X$ ainsi construit est isomorphe à $X_2 \to X$.

Démonstration. Vérifions par récurrence sur $j \in \{1,\dots,r\}$ que $Y_j \to Y_{j-1}$ est galoisien de groupe Λ. C'est vrai pour $j = 1$. Pour tout $i \in \{1,\dots,j-1\}$ l'extension $k(Y_i) = k(Y_{i-1})(\sqrt[n]{g_i})/k(Y_{i-1})$ est galoisienne de groupe Λ par hypothèse de récurrence. La suite spectrale de Hochschild-Serre donne une suite exacte

$$0 \to \mathrm{H}^1(\Lambda,\Lambda) \to \mathrm{H}^1(Y_{i-1},\Lambda) \to \mathrm{H}^1(Y_i,\Lambda).$$

Par conséquent, le noyau de $\phi_i^\star\colon \mathrm{H}^1(X,\Lambda) \to \mathrm{H}^1(Y_i,\Lambda)$ est $\Lambda[D_1] \oplus \cdots \oplus \Lambda[D_i] \simeq \Lambda^i$, et $[D_j]$ n'y appartient pas ; l'élément $\phi_i^\star[D_j]$ est encore d'ordre n dans $\mathrm{H}^1(Y_i,\mu_n)$. Ainsi, $Y \to X$ est fini étale d'ordre n^r. Le corps k étant algébriquement clos, l'extension L/K est le corps de décomposition des polynômes $T^n - g_1,\dots,T^n - g_r$, elle est donc galoisienne. Par la proposition 2.1.9, le morphisme $Y \to X$ est donc un revêtement galoisien. Un élément du groupe $\mathrm{Aut}(Y|X)$ est un automorphisme défini par $(\sqrt[n]{g_1} \mapsto \zeta_1\sqrt[n]{g_1},\dots,\sqrt[n]{g_r} \mapsto \zeta_r\sqrt[n]{g_r})$, où les ζ_i sont des racines n-ièmes de l'unité dans k ; le groupe $\mathrm{Aut}(Y|X)$ est donc canoniquement isomorphe à $\mathrm{Hom}_\Lambda(\mathrm{H}^1(X,\mu_n),\mu_n) = \mathrm{H}^1(X,\Lambda)^\vee$. La proposition précédente assure que Y est isomorphe à X_2. □

Remarque 2.7.3. Si X est affine de compactification lisse $\bar{X}$, alors il est possible pour tout point $P \in Z \coloneqq \bar{X} - X$ de choisir les fonctions $g_1,\dots,g_r$ de façon à ce qu'elles soient toutes de valuation positive en P. En effet, les éléments d'une base (D_i,g_i) de $\mathrm{H}^1(\bar{X},\mu_n)$ peuvent être choisis de façon à ce que le support de D_i évite Z (voir annexe C.3.4). Cette base peut être complétée en une base de $\mathrm{H}^1(X,\mu_n)$ en ajoutant des antécédents de la base $(Q - Q_0)_{Q\in Z}$ de $\mathrm{Div}^0_Z(X) \otimes \Lambda$ pour un $Q_0 \in Z - \{P\}$ fixé.

Lemme 2.7.4. Pour tout Λ-module de type fini F, le revêtement $\phi\colon X_2 \to X$ trivialise tous les F-torseurs sur X.

Démonstration. Par construction, le revêtement $X_2 \to X$ trivialise les Λ-torseurs sur X. Le Λ-module de type fini F n'est qu'un produit de $\mathbb{Z}/n_i\mathbb{Z}$ où n_i divise n, et $\mathrm{H}^1(X,\mathbb{Z}/n_i\mathbb{Z}) \subset \mathrm{H}^1(X,\Lambda)$. Par conséquent, le morphisme $\mathrm{H}^1(X,\mathbb{Z}/n_i\mathbb{Z}) \to \mathrm{H}^1(X_2,\mathbb{Z}/n_i\mathbb{Z})$ est nul, et $\mathrm{H}^1(X,F) \to \mathrm{H}^1(X_2,F)$ est nul. □

Remarque 2.7.5. Dans le cas où X est une courbe projective lisse sur k de jacobienne J, le choix d'un point $P \in X(k)$ détermine un plongement $i_P \colon X \to J$. Considérons le revêtement $Y \to X$ défini par le diagramme cartésien :

$$\begin{tikzcd} Y \arrow[r] \arrow[d] & J \arrow[d, "{[n]}"] \\ X \arrow[r, "i_P"] & J \end{tikzcd}$$

Le groupe d'automorphismes de l'isogénie $[n]$ est isomorphe à $J[n] = \mathrm{H}^1(X, \mu_n)$. Le revêtement $Y \to X$, qui est de même degré que $[n]$, est encore galoisien de groupe d'automorphismes isomorphe à $\mathrm{H}^1(X, \mu_n)$.

Remarque 2.7.6. La même construction s'applique au cas de la cohomologie des courbes sur les corps finis. Supposons k_0 fini. Soit X_0 une courbe projective lisse géométriquement connexe sur k_0 de corps des fonctions K_0. Le morphisme $\mathrm{H}^1(X_0, \mu_n) \to \mathrm{H}^1(X, \mu_n)^{\mathfrak{G}_0}$ est surjectif ; en effet, comme $\mathfrak{G}_0$ est de dimension cohomologique 1, le terme suivant dans la suite spectrale de Hochschild-Serre est nul. Le lemme C.3.5 assure alors que tout classe $\mathfrak{G}_0$-invariante de $\mathrm{Pic}^0(X)[n]$ contient un diviseur $\mathfrak{G}_0$-invariant D, et il existe une fonction $f \in K_0$ telle que $\mathrm{div}(f) = nD$. Un algorithme permettant de déterminer ces éléments $\mathfrak{G}_0$-invariants, et donc de construire une base de $\mathrm{H}^1(X, \mu_n)^{\mathfrak{G}_0}$, est donné dans la proposition C.3.9. Il suffit ensuite de compléter cette base par la classe d'un générateur de $k_0^\times$, qui engendre le Λ-module $k_0^\times/(k_0^\times)^n$, pour obtenir une famille génératrice $(([D_0], f_0), \ldots, ([D_r], f_r))$ de $\mathrm{H}^1(X_0, \mu_n)$. Par la même preuve que ci-dessus, la normalisation de X_0 dans $K_0(\sqrt[n]{f_0}, \ldots, \sqrt[n]{f_r})$ est alors un revêtement galoisien de X_0 de groupe $\mathrm{H}^1(X_0, \Lambda)^\vee$.

II.7.1.2 Composition avec un autre revêtement

Considérons maintenant le cas d'un revêtement galoisien de courbes intègres lisses $f \colon Y \to X$. Soit $\bar{f} \colon \bar{Y} \to \bar{X}$ le morphisme fini entre les compactifications lisses induit par f. Alors $\bar{f}^{-1}(\bar{X} - X) = \bar{Y} - Y$, et en particulier, tout élément $\tau \in \mathrm{Aut}(Y|X)$ induit une permutation de $\bar{Y} - Y$. L'image de $(D_i, g_i) \in \mathrm{H}^1(X, \mu_n(k))$ par $\tau^\star$ est donc simplement $(\tau^\star D_i, \tau^\star g_i)$. Considérons le revêtement $Y_2 \to Y$ construit précédemment.

Lemme 2.7.7. Le morphisme composé $Y_2 \to Y \to X$ est encore un revêtement galoisien.

Démonstration. Ceci découle directement du fait que $\pi_1(Y_2)$ est caractéristique dans $\pi_1(Y)$. □

Lemme 2.7.8. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X trivialisé par Y. Alors le revêtement $Y_2 \to X$ trivialise tous les $\mathcal{F}$-torseurs.

Démonstration. Notons $F = \mathrm{H}^0(Y, \mathcal{F})$. Le morphisme $\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(Y_2, F)$ se factorise par la flèche $\mathrm{H}^1(Y, F) \to \mathrm{H}^1(Y_2, F)$, qui est nulle par le lemme 2.7.4. □

II.7.1.3 Ramification

Soit X une courbe affine lisse sur k, de compactification lisse $\bar{X}$ et de genre géométrique g_X. Notons $P_0, \ldots, P_r$ les points de $\bar{X} - X$, et $\overline{X_2}$ la compactification lisse du revêtement $X_2 \to X$ de groupe $\mathrm{H}^1(X, \Lambda)^\vee$. Le morphisme $\overline{X_2} \to \bar{X}$ est fini [Har08, II, Prop. 6.8], et

$$\overline{X_2} \times_{\bar{X}} (\bar{X} - X) = \overline{X_2} - X_2.$$

Étudions les antécédents des P_i dans $\overline{X_2} - X_2$ et leur ramification. Rappelons que $\mathrm{H}^1(\bar{X}, \Lambda)^\vee$ est un quotient de $\mathrm{H}^1(X, \Lambda)^\vee$; la compactification lisse $(\bar{X})_2$ du revêtement de X correspondant est étale

au-dessus de $\bar{X}$. Il suffit donc d'étudier le revêtement $\overline{X_2} \to (\bar{X})_2$. Une Λ-base de $\mathrm{Div}^0_{\bar{X}-X}(\bar{X}) \otimes \Lambda$ est donnée par $P_1 - P_0, \ldots, P_r - P_0$. Considérons des fonctions $g_1, \ldots, g_r$ telles que

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

où $D_i \in \mathrm{Div}^0(X - \{P_0, \ldots, P_r\})$. Le revêtement $\overline{X_2} \to (\bar{X})_2$ a pour corps de fonctions

$$k((\bar{X})_2)(\sqrt[n]{g_1}, \ldots, \sqrt[n]{g_r}).$$

Soit $i \in \{1 \ldots r\}$. L'extension $k((\bar{X})_2)(\sqrt[n]{g_j}, j \neq i)$ de $k((\bar{X})_2)$ fournit un revêtement $Y_i \to (\bar{X})_2$ non ramifié au-dessus de P_i puisque $v_{P_i}(g_j) = 0$. Le revêtement $\overline{X_2} \to Y_i$ y est, quant à lui, ramifié ; soit Q_i l'un des points de Y_i au-dessus de P_i. Comme $v_{Q_i}(g_i) = 1$, la fibre $(\overline{X_2})_{Q_i}$ est isomorphe à $k[x]/(x^n)$, et l'indice de ramification est n. En résumé, il y a au-dessus de P_i exactement $\frac{1}{n}|\mathrm{H}^1(X, \Lambda)|$ points de $\overline{X_2}$, tous d'indice de ramification n au-dessus de P_i. Soit R_i un antécédent de Q_i dans $\overline{X_2}$.

Le sous-groupe d'inertie $I_{R_i|P_i} \subset \mathrm{Aut}(X_2|X)$ du point R_i au-dessus de $\bar{X}$ s'insère dans la suite exacte

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

(voir [Stacks, 0BU7] pour la surjectivité). Comme $I_{Q_i|P_i} = 0$, il y a des isomorphismes

$$I_{R_i|P_i} = I_{R_i|Q_i} = \mathrm{Aut}(\overline{X_2}|Y_i) \simeq \Lambda.$$

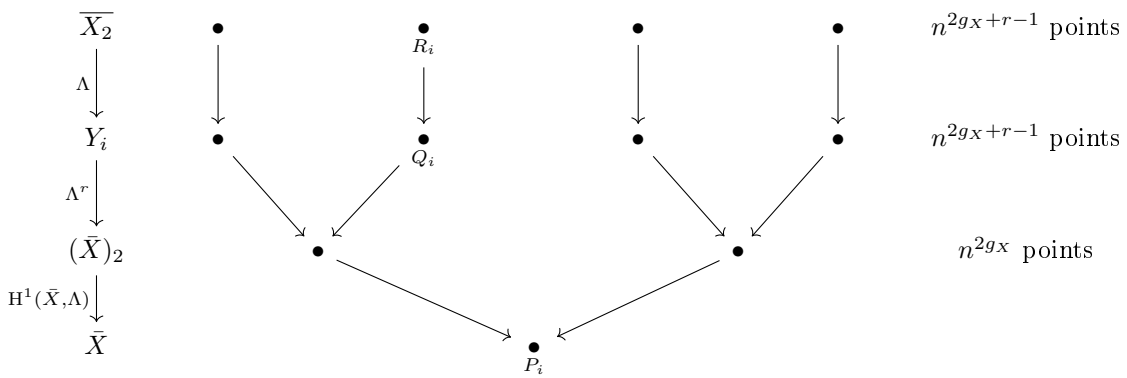


FIGURE II.3 – Ramification à l'infini de $X_2 \to X$

En tant que sous-groupe de $\mathrm{Aut}(X_2|X)$, le groupe $I_{R_i|P_i}$ est celui engendré par $\sqrt[n]{g_i} \mapsto \zeta \sqrt[n]{g_i}$, où ζ est une racine n-ième primitive de l'unité. Tout ceci s'applique encore au point P_0, qui avait été choisi arbitrairement au début. Avec les notations ci-dessus, le sous-groupe $I_{R_0|P_0}$ est engendré par $(\sqrt[n]{g_1}, \ldots, \sqrt[n]{g_r}) \mapsto (\zeta \sqrt[n]{g_1}, \ldots, \zeta \sqrt[n]{g_r})$.

Lemme 2.7.9. Le genre géométrique de X_2 est donné par

$$g_{X_2} = 1 + \frac{1}{2} n^{2g_X - 1 + r} \left(n(2g_X - 2) - 1\right).$$

Démonstration. L'application de la formule de Riemann-Hurwitz au revêtement ramifié de courbes projectives lisses $\overline{X_2} \to \bar{X}$ fournit l'égalité

$$2g_{X_2} - 2 = |\mathrm{H}^1(X, \Lambda)|(2g_{\bar{X}} - 2) + \sum_{P \in \overline{X_2} - X_2} (e_P - 1)$$

où e_P désigne l'indice de ramification de $X_2 \to X$ en P. Rappelons que $|\operatorname{H}^1(X,\Lambda)| = n^{2g_X+r}$. De plus, il y a au-dessus de chaque point $Q \in \bar{X} - X$ exactement n^{2g_X-1+r} points, tous d'indice de ramification n. Par conséquent,

$$2g_{X_2} = 2 + n^{2g_X+r}(2g_X - 2) + (n-1)n^{2g_X-1+r}$$

et le résultat s'en déduit immédiatement. □

II.7.2 Un revêtement semblable défini sur k_0

Soit Y_0 une courbe connexe (mais pas nécessairement géométriquement connexe) lisse sur k_0. Notons $Y = Y_0 \times_{k_0} k$. Le but de cette section est de déterminer un revêtement galoisien caractéristique $Y_{2,0} \to Y_0$ tel que $Y_{2,0} \times_{k_0} k \to Y$ trivialise tous les μ_n-torseurs sur Y. Soient X_0 une courbe lisse géométriquement connexe sur k_0, et $f\colon Y_0 \to X_0$ un revêtement galoisien. Notons encore $X = X_0 \times_{k_0} k$.

Remarque 2.7.10. Considérons le cas particulier où Y_0 possède un k_0-point y_0 ; dans ce cas, Y est connexe [Stacks, 04KV]. Soient $\bar{y}$ un point géométrique de Y d'image y_0, et $\bar{x}$ son image par f. Soit $\bar{y}_2$ un point géométrique de Y_2 d'image $\bar{y}$. Le groupe $\pi_1(Y,\bar{y}_2)$ est caractéristique dans $\pi_1(Y,\bar{y})$, qui est lui-même distingué dans $\pi_1(X,\bar{x})$. Ainsi, l'action de $\mathfrak{G}_0$ par automorphismes sur $\pi_1(X,\bar{x})$ induit encore une action sur $\pi_1(Y_2,\bar{y}_2)$, et par passage au quotient une action sur $\operatorname{Aut}(Y_2|X)$.

Cependant, la courbe Y n'est pas nécessairement connexe : soient $Y^{(1)},\dots,Y^{(t)}$ ses composantes connexes.

Résumé de l'idée Commençons par construire le revêtement $Y_2^{(1)} \to Y^{(1)}$ de groupe $\operatorname{H}^1(Y^{(1)},\Lambda)$, puis le schéma $W = \coprod_\sigma (Y_2^{(1)})^\sigma$, où σ parcourt les automorphismes d'une extension galoisienne suffisamment grande de k_0. Le revêtement $W \to Y$ provient d'un k_0-revêtement $Y_{2,0} \to Y_0$, qui vérifie la propriété recherchée.

Construction Soit k_1 la clôture algébrique de k_0 dans $k_0(Y_0)$. C'est une extension séparable car $Y_0 \to X_0$ est étale. Soit k_2 l'extension minimale de k_0 par laquelle se factorise l'action de $\mathfrak{G}_0$ sur $\operatorname{H}^1(Y_1,\mu_n)$. Soit L la clôture galoisienne de la sous-extension de k engendrée par $\mu_n(k), k_1, k_2$. Soit α un élément primitif de l'extension séparable L/k_1, et $m \in k_1[t]$ son polynôme minimal. Écrivons $k_0(Y_0) = k_0(x)[y]/(f)$. Soient $(D_1,g_1),\dots,(D_r,g_r)$ des couples diviseur-fonction qui forment une base de $\operatorname{H}^1(Y^{(1)},\mu_n)$. Écrivons $g_i = g_i'(\alpha,x,y)$ avec $g_i' \in k_0(x)[t,y]/(m(t),f(x,y))$. Le morphisme $Y_{2,0} \to Y_0$ est alors défini par l'extension

$$k_0(Y_{2,0}) = k_0(\alpha,x,y)(\sqrt[n]{g_1'},\dots,\sqrt[n]{g_r'})$$

de $k_0(Y_0)$. La courbe $Y_{2,0} \times_{k_0} k$ est alors isomorphe à l'orbite sous $\operatorname{Gal}(L|k_0)$ de $Y_2^{(1)}$, et possède $[L:k_0]$ composantes connexes.

Lemme 2.7.11. Le degré de $Y_{2,0} \to X_0$ est $n^r[L:k_1]\deg(Y_0 \to X_0)$.

Démonstration. Le degré de $Y_{2,0} \to (Y_0 \times_{k_1} L)$ est n^r et le degré de $Y_0 \times_{k_1} L \to Y_0$ est $[L:k_1]$. □

Calcul de $\operatorname{Aut}(Y_{2,0}|X_0)$ Le morphisme $Y_{2,0} \to Y_0$ est de degré $n^r[L:k_1]$. Posons $z_i = \sqrt[n]{g_i'}$ avec les notations ci-dessus. Le groupe $\operatorname{Aut}(k_0(Y_{2,0})|k_0(Y_0))$ est constitué des automorphismes définis par $t \mapsto \sigma(t), z_i \mapsto \zeta_i z_i$ où $\sigma \in \operatorname{Gal}(L|k_1)$ et $\zeta_i \in \mu_n(L)$. Il y en a $\deg(Y_{2,0} \to Y_0) = n^r[L:k_1]$ car $\mu_n(k) \subset L$: le revêtement $Y_{2,0} \to Y_0$ est donc galoisien. Calculons les automorphismes de $Y_{2,0} \to X_0$. Ce sont les

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

où $\sigma \in \mathrm{Gal}(L|k_0)$, où (x', y') est l'image de (x, y) par un X_0-automorphisme de Y_0 induisant le même élément de $\mathrm{Gal}(k_1|k_0)$ que σ, et $z_i' \in k_0(Y_{2,0})$ vérifie $z_i'^n = \phi(g_i')$. Il y a comme attendu $\deg(Y_{2,0}|X_0) = n^r[L : k_1]\deg(Y_0 \to X_0)$ automorphismes de $Y_{2,0} \to X_0$, qui est donc un revêtement galoisien.

II.7.3 Adaptation aux courbes nodales

Soit X_0 une courbe nodale sur k_0. Notons $X = X_0 \times_{k_0} k$, et $\nu\colon \tilde{X} \to X$ sa normalisation. Soient $P_1, \ldots, P_r$ les points nodaux de X. Notons $s = |H^1(\tilde{X}, \Lambda)|$. Soit $\tilde{X}_2 \to \tilde{X}$ le revêtement galoisien de $\tilde{X}$ de groupe $\mathrm{H}^1(\tilde{X}, \Lambda)^\vee$. Soit $X' \to X$ le revêtement de X de groupe $\mathrm{H}^1(\tilde{X}, \Lambda)^\vee$ obtenu par la construction de la section II.6.2.1. C'est une courbe qui a rs points nodaux. Considérons également le revêtement $W \to X$ non irréductible de groupe Λ^r construit dans la section II.6.2.2. Considérons la courbe $Z \coloneqq W \times_X X'$. Le diagramme à carrés cartésiens ci-dessous, dont les flèches sont étiquetées par le degré des morphismes, résume la situation.

$$\begin{tikzcd}
\tilde{X}_2 \arrow[r] \arrow[d, "s"] & X' \arrow[d, "s"] & Z \arrow[l, "n^r"'] \arrow[d, "s"] \\
\tilde{X} \arrow[r] & X & W \arrow[l, "n^r"']
\end{tikzcd}$$

Lemme 2.7.12. Le schéma Z est connexe.

Démonstration. Le morphisme $X' \to X$ étant lisse, le morphisme $Z \to W$ l'est encore ; d'après [Stacks, 07TD], la normalisation de Z est donc

$$\tilde{Z} = \tilde{W} \times_W Z = \tilde{W} \times_W W \times_X X' = \tilde{W} \times_X X' = (\tilde{X} \times \Lambda^r) \times_X X' = \tilde{X}_2 \times \Lambda^r.$$

Les points de $\tilde{X}_2$ au-dessus de $P^{(i)}$ sont $Q_1^{(i)}, \ldots, Q_s^{(i)}, R_1^{(i)}, \ldots, R_s^{(i)}$. Soient $P_1^{(i)}, \ldots, P_s^{(i)}$ leurs images respectives dans X'. Notons $T^{(i)}_{j_1,\ldots,j_r}$, où $(j_1, \ldots, j_r) \in \Lambda^r$, les points de W au-dessus de $P^{(i)}$. Les notations des antécédents de $P^{(i)}$ dans $\tilde{X}$, $\tilde{X}_2$, X' et W sont résumées dans le tableau ci-après, où $a \in \{1 \ldots s\}$ et $(j_1, \ldots, j_r) \in \Lambda^r$.

$\tilde{X}_2$	X'	$Z = X' \times_X W$	$\tilde{Z} = \tilde{X}_2 \times \Lambda^r$
$Q_a^{(i)}, R_a^{(i)}$	$P_a^{(i)}$	$(P_a^{(i)}, T^{(i)}_{j_1,\ldots,j_r})$	$(Q_a^{(i)}, j_1, \ldots, j_r), (R_a^{(i)}, j_1, \ldots, j_r)$
$Q^{(i)}, R^{(i)}$	$P^{(i)}$	$T^{(i)}_{j_1,\ldots,j_r}$	$(Q^{(i)}, j_1, \ldots, j_r), (R^{(i)}, j_1, \ldots, j_r)$
$\tilde{X}$	X	W	$\tilde{W} = \tilde{X} \times \Lambda^r$

Souvenons-nous que le morphisme $\tilde{W} = \tilde{X} \times \Lambda^r \to W$ associe au couple $(Q^{(i)}, j_1, \ldots, j_r)$ le point $T^{(i)}_{j_1,\ldots,j_r}$ et à $(R^{(i)}, j_1, \ldots, j_r)$ le point $T^{(i)}_{j_1,\ldots,j_i-1,\ldots,j_r}$. Le morphisme

$$\tilde{Z} = \tilde{X}_2 \times_X \Lambda^r \to Z = X' \times_X W$$

associe aux points $(Q_a^{(i)}, j_1, \ldots, j_r)$ et $(R_a^{(i)}, j_1, \ldots, j_i + 1, \ldots, j_r)$ le couple $(P_a^{(i)}, T^{(i)}_{j_1,\ldots,j_r})$. Les composantes irréductibles de Z sont les images des n composantes connexes de $\tilde{Z}$, toutes isomorphes à $\tilde{X}_2$; le

point $(P_1^{(1)}, T^{(1)}_{j_1,\dots,j_r})$ appartient à l'image dans Z de la $(j_1,\dots,j_r)$-ième et de la $(j_1,\dots,j_i+1,\dots,j_r)$-ième composante de $\tilde{Z}$. Ainsi, deux composantes irréductibles C, C' de $\tilde{Z}$ sont toujours jointes par une suite

$$(C = C_0, C_1, \dots, C_m = C')$$

telle que pour tout i, l'intersection $C_i \cap C_{i+1}$ soit non vide. □

Proposition 2.7.13. Le morphisme $Z \to X$ est un revêtement galoisien de groupe isomorphe à $\mathrm{H}^1(X,\Lambda)^\vee$.

Démonstration. Il est fini étale de degré $n^r s$ car composée de morphismes finis étales de degrés respectifs n^r et s, et connexe d'après le lemme précédent. Comme $Z = W \times_X X'$, il y a un morphisme $\mathrm{Aut}(W|X) \times \mathrm{Aut}(X'|X) = \Lambda^r \times \mathrm{H}^1(\tilde{X},\Lambda)^\vee \to \mathrm{Aut}(Z|X)$, qui est injectif car $W \to X$ et $X' \to X$ sont surjectifs. Le groupe de gauche étant d'ordre $\deg(Z \to X)$, ceci prouve que $Z \to X$ est galoisien. Rappelons que le groupe $\mathrm{H}^1(X,\Lambda)$ est isomorphe à $\Lambda^r \times \mathrm{H}^1(\tilde{X},\Lambda)^\vee$, ce qui conclut. □

Corollaire 2.7.14. Le revêtement $Z \to X$ est caractéristique et trivialise tous les Λ-torseurs sur X.

Démonstration. Le revêtement est caractéristique car son groupe est isomorphe à $\mathrm{H}^1(X,\Lambda)^\vee$ (voir proposition 2.7.1). Notons $G = \mathrm{Aut}(Z|X)$. La suite spectrale de Hochschild-Serre pour $Z \to X$ donne une suite exacte

$$0 \to \mathrm{H}^1(G,\Lambda) \to \mathrm{H}^1(X,\Lambda) \to \mathrm{H}^1(Z,\Lambda).$$

Sachant que le groupe $G \simeq \mathrm{H}^1(X,\Lambda)$ est un Λ-module libre et que l'action de G sur Λ est triviale, $\mathrm{H}^1(G,\Lambda) = \mathrm{Hom}_\Lambda(G,\Lambda) = \Lambda^{\mathrm{rg}_\Lambda G} = \mathrm{H}^1(X,\Lambda)$. Par conséquent, le morphisme $\mathrm{H}^1(X,\Lambda) \to \mathrm{H}^1(Z,\Lambda)$ est nul. □

Construction du revêtement défini sur k_0 Soit k'/k_0 l'extension minimale de k_0 sur laquelle sont définis les antécédents dans $\tilde{X}$ des points singuliers de X. Soit X_1 la normalisation de X_0 dans $k_1(X_0)$. Considérons le revêtement galoisien $\tilde{Z}_1 \to \tilde{X}_1$ de la section II.7.2. Construisons comme dans la section II.6.2.1 le revêtement galoisien Z_1 de X_1 correspondant. De même, construisons le revêtement non irréductible W de X_1 de groupe Λ^r défini dans la section II.6.2.2. Posons enfin $X_{2,0} = Z_1 \times_{X_1} W$. La connexité de $X_{2,0}$ se montre comme dans le lemme 2.7.12. Si $X_0 \to Y_0$ est un revêtement galoisien, le même argument que précédemment montre que $\mathrm{Aut}(X_{2,0}|Y_0)$ est isomorphe à $\Lambda^r \times \mathrm{Aut}(Z_1|Y_0)$; or $Z_1 \to Y_0$ est galoisien car $\tilde{Z}_1 \to \tilde{Y}_0$ l'est, donc $X_{2,0} \to Y_0$ l'est encore.

II.7.4 Un exemple détaillé

Prenons $n = 2$. Supposons que -1 n'est pas un carré dans k_0. Notons $V = \mathbb{P}^1 - \{0, \pm 1, \infty\}$ et $U = \mathbb{P}^1 - \{0, 1, \infty\}$. Considérons le revêtement étale de degré 2

$$\begin{array}{rccc} f\colon & V & \longrightarrow & U \\ & y & \longmapsto & y^2 \end{array}$$

de groupe d'automorphismes engendré par $\tau\colon y \mapsto -y$. Le faisceau $\mathcal{F} := f_\star\Lambda$ est un faisceau lisse sur U, trivialisé par le revêtement $f\colon V \to U$ puisque $f^\star f_\star \Lambda \simeq \Lambda^2$. Il correspond au $\mathrm{Aut}(V|U)$-module Λ^2, où l'élément non trivial de $\mathrm{Aut}(V|U)$ intervertit les deux copies de Λ.

Calcul de V_2 Le groupe $\mathrm{H}^1(V,\mu_2)\simeq\Lambda^3$ est engendré par les couples diviseur-fonction $(0-\infty,x),(1-\infty,x-1),(-1-\infty,x+1)$. Le revêtement $V_2\to V$ de groupe $\mathrm{H}^1(V,\Lambda)^\vee$ correspond à l'extension de corps $k(\sqrt{x},\sqrt{x-1},\sqrt{x+1})/k(x)$. Le revêtement de $\bar{V}=\mathbb{P}^1$ correspondant est le morphisme

$$\begin{array}{ccc}\operatorname{Proj} k[y,z,t,h]/(z^2-(y^2-h^2),t^2-(y^2+h^2)) & \longrightarrow & \operatorname{Proj} k[y,h]\\ (y:z:t:h) & \longmapsto & (y^2:h^2)\end{array}$$

ramifié au-dessus de $0,\pm1,\infty$.

Calcul de $\mathrm{Aut}(V_2|U)$ Le groupe d'automorphismes $G:=\mathrm{Aut}(V_2|U)$ est d'ordre 16 ; il suffit pour le déterminer entièrement d'y trouver un antécédent du générateur τ de $\mathrm{Aut}(V|U)$. Un tel antécédent est $\gamma\colon(y:z:t:h)\mapsto(\sqrt{-1}y:\sqrt{-1}t:\sqrt{-1}z:h)$. Notons $\sigma_1\colon y\mapsto -y$, $\sigma_2\colon z\mapsto -z$, $\sigma_3\colon t\mapsto -t$ les générateurs évidents de $\mathrm{Aut}(V_2|V)\lhd G$. Alors $\gamma\sigma_2=\sigma_3\gamma$ et $\gamma\sigma_3=\sigma_3\gamma$, ce qui implique que $\langle\sigma_2,\sigma_3\rangle$ est distingué dans G. On vérifie aisément que la composée

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

est un isomorphisme ; par conséquent,

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

Ramification Notons $Z=\bar{U}-U$, $W=\bar{V}-V$ et $W'=\overline{V}_2-V_2$. Le tableau ci-dessous résume la situation.

Points de Z	0	1		∞
Antécédents dans W Ramification	0 indice 2	-1 indice 1	1 indice 1	∞ indice 2
Antécédents dans W' Ramification	4 points indice 4	4 points indice 2	4 points indice 2	4 points indice 4
Un antécédent dans W' Son groupe d'inertie	$P_0=(0,\sqrt{-1},1)$ $\langle\gamma\sigma_2\rangle\simeq\mu_4(k)$	$P_{-1}=(\sqrt{-1},\sqrt{-2},0)$ $\langle\sigma_3\rangle\simeq\mu_2(k)$	$P_1=(1,0,\sqrt{2})$ $\langle\sigma_2\rangle\simeq\mu_2(k)$	$P_\infty=(1:1:1:0)$ $\langle\gamma\rangle\simeq\mu_4(k)$

L'isomorphisme canonique $I_{P_0}\to\mu_4(k)$ est obtenu explicitement de la façon suivante. Une uniformisante de $\bar{V}_2$ en $P_0=(0,\sqrt{-1},1)$ est y. L'orbite de y sous l'action de $I_{P_0}=\langle\gamma\sigma_2\rangle$ est $\{\pm y,\pm\sqrt{-1}y\}$. L'ensemble des $\frac{\sigma(y)}{y}(P_0)$ où σ parcourt I_{P_0} est donc exactement $\mu_4(k)$. À un élément $\sigma\in I_{P_0}$, l'isomorphisme $I_{P_0}\to\mu_4(k)$ associe $\frac{\sigma(y)}{y}(P_0)$.

Le générateur $\sqrt{-1}$ de $\mu_4(k)$ échange les deux copies de Λ dans $M=\Lambda^2$. Le Λ-module des morphismes croisés $\mu_4(k)\to M$ est isomorphe à Λ^2, et $\tau_{\leqslant1}\mathrm{R}\Gamma(I_{P_0},M)$ est représenté par le complexe suivant.

$$\begin{array}{ccc}\Lambda^2 & \to & \Lambda^2\\ (a,b) & \mapsto & \left[\sqrt{-1}\mapsto(a+b,a+b)\right]\end{array}$$

Le groupe $\mathcal{F}_0=\mathrm{H}^0(I_{P_0},M)$ est engendré par $(1,1)$, et $\mathrm{H}^2_0(X,j_\star\mathcal{F})=\mathrm{H}^1(I_{P_0},M)$ est engendré par la classe de $(0,1)$. Le calcul de $\tau_{\leqslant1}\mathrm{R}\Gamma(I_{P_\infty},M)$ est très semblable. Le groupe I_{P_1} est, quant à lui, canoniquement isomorphe à $\mu_2(k)$, et agit trivialement sur M. Par conséquent, $\tau_{\leqslant1}\mathrm{R}\Gamma(I_{P_1},M)$ est représenté par le complexe suivant.

$$\begin{array}{ccc}\Lambda^2 & \to & \Lambda^2\\ (a,b) & \mapsto & 0\end{array}$$

Nous calculerons $\mathrm{R}\Gamma(U,\mathcal{F})$ dans la section V.3.4.

CHAPITRE III

Algorithmique des faisceaux constructibles

Fixons un corps k_0, et une clôture algébrique k de k_0. Soit n un entier naturel non nul. Notons Λ l'anneau $\mathbb{Z}/n\mathbb{Z}$. Dans toute cette section, les faisceaux constructibles considérés seront des faisceaux de Λ-modules.

L'objectif de ce chapitre est de donner diverses représentations et opérations sur les faisceaux lisses sur les k_0-schémas de type fini, puis des faisceaux constructibles sur les courbes lisses sur k. Nous donnons dans le cas des courbes lisses des algorithmes permettant de passer d'une représentation à une autre, ainsi que des algorithmes permettant d'effectuer des opérations (images directes et réciproques, noyaux et conoyaux de morphismes, Hom interne et produit tensoriel...) sur ces faisceaux. Nous montrons également comment effectuer ces opérations dans le cas général des faisceaux constructibles après avoir décrit comment calculer les poussés en avant de faisceaux lisses par des morphismes entre variétés régulières de même dimension. Nous nous assurons que tous les algorithmes présentés sont de complexité élémentaire (voir annexe A.1) en les entrées. Les schémas sont décrits comme recollement de schémas affines (voir annexe B.1.1). Pour cette représentation, il existe des algorithmes de complexité élémentaire calculant la normalisation ou la décomposition primaire d'une variété. Les courbes projectives lisses sont décrites par des produits de corps de fonctions (voir annexe C.1.2), et les courbes affines lisses comme un ouvert d'un modèle plan de leur compactification lisse.

III.1 Faisceaux lisses

III.1.1 Représentations des faisceaux lisses

Soit X un schéma intègre de type fini sur k_0. Soit $\mathcal{F}$ un faisceau lisse sur X, correspondant à un $\pi_1(X)$-module M. Nous nous intéresserons à deux façons de définir explicitement $\mathcal{F}$:

1. par un X-schéma en groupes fini étale F qui le représente ;
2. par un revêtement galoisien $Y \to X$ qui le trivialise ainsi que le $\mathrm{Aut}(Y|X)$-module M.

Passage de la première à la deuxième représentation Supposons $\mathcal{F}$ défini par un morphisme fini étale $T \to X$ de degré d, ainsi qu'une application $T \times_X T \to T$ définissant sa loi de groupe. Le

calcul d'un revêtement trivialisant, décrit par exemple dans [Fu15, Prop. 5.8.1.(i)], se fait de la façon suivante : trouver une composante connexe T' de T telle que $T' \to X$ soit de degré >1, et changer de base à T'. Recommencer cette opération avec $T' \times_X T \to T'$ (toujours de degré d), jusqu'à obtenir un schéma Y avec d composantes connexes.

Remarquons qu'à chaque étape, le nombre de composantes connexes de T, et donc le nombre d'éléments de $\mathcal{F}(T)$, augmente. Il y a dans cet algorithme au plus $d-1$ appels récursifs ; comme $\mathcal{F}$ est un faisceau de groupes abéliens, c'est même $\log_2(d)$ puisqu'à chaque étape, $\mathcal{F}(T)$ est un sous-groupe strict de $\mathcal{F}(T')$. Chacune de ces étapes consiste en une décomposition primaire, puis le calcul d'un produit fibré.

Une fois cette opération effectuée, il reste à calculer la clôture galoisienne $Z \to X$ de $Y \to X$, qui est une composante connexe de $Y \times_X \cdots \times_X Y$. Celle-ci se calcule d'une façon semblable à la clôture galoisienne d'une extension de corps [HL17, §2]. L'action de $\sigma \in \mathrm{Aut}(Z|X)$ sur $\mathcal{F}(Z)$ est donnée par la permutation des composantes connexes de $T \times_X Z \simeq \sqcup^d Z$ induite par

$$T \times_X Z \xrightarrow{\mathrm{id} \times \sigma} T \times_X Z.$$

Rappelons que le degré de $Z \to X$ est majoré par $\deg(Y \to X)!$. Le cardinal de $\mathcal{F}(Z)$ est, quant à lui, égal au degré de $T \to X$.

Passage de la deuxième à la première représentation Supposons $\mathcal{F}$ défini par un revêtement galoisien $f\colon Y \to X$ de groupe G, et le G-module $M = \mathrm{H}^0(Y, f^\star\mathcal{F})$. Rappelons que $\mathcal{F} = (f_\star f^\star \mathcal{F})^G$. Le faisceau $f_\star f^\star \mathcal{F}$ est représenté par la restriction de Weil $R \coloneqq R_{Y \to X}(M \times Y)$, et est encore muni d'une action de G qui permute ses composantes connexes. Le faisceau $(f_\star f^\star \mathcal{F})^G$ est représenté par l'intersection schématique $\bigcap_{g \in G} \ker(g - \mathrm{id}_R)$.

Calcul du revêtement trivialisant minimal Une fois calculé un revêtement galoisien $Z \to X$ qui trivialise $\mathcal{F}$, un revêtement minimal est donné par Z/H, où H est le noyau de $\mathrm{Aut}(Z|X) \to \mathrm{Aut}(\mathrm{H}^0(Z, \mathcal{F}))$. Le degré de $Z/H \to X$ est le cardinal du groupe de monodromie, image de $\mathrm{Aut}(Z|X)$ dans $\mathrm{Aut}(\mathrm{H}^0(Z, \mathcal{F}))$.

Simplifications dans le cas des courbes intègres lisses Soit X une courbe intègre lisse sur k_0. Un revêtement Y de X est simplement défini par l'extension L/K de corps de fonctions correspondante. Le groupe $\mathrm{Aut}(Y|X)$ est $G = \mathrm{Aut}(L|K)$, et si le revêtement est galoisien, le faisceau lisse $\mathcal{F}$ n'est rien d'autre qu'un $\Lambda[G]$-module F. Le revêtement minimal est alors donné par L^H, où $H = \ker(G \to \mathrm{Aut}_\Lambda(M))$; c'est un simple calcul d'algèbre linéaire sur le K-espace vectoriel L.

Complexité du calcul d'un revêtement trivialisant Tous nos algorithmes utiliseront la représentation par fibre générique et revêtement trivialisant. Soit X une courbe intègre lisse sur k_0. Soit $\mathcal{F}$ un faisceau lisse sur X, représenté par un schéma en groupes $F = \bigsqcup_{i=1}^r F_i \to X$ où les F_i sont connexes et étales sur X. Supposons X et les F_i décrites par un modèle plan (voir annexe C.1.2). Pour chaque $i \in \{1 \dots r\}$, notons d_i le degré de F_i et f_i le degré de $F_i \to X$. Notons $f = f_1 + \cdots + f_r$ le degré de $F \to X$, c'est-à-dire le cardinal de la fibre générique de $\mathcal{F}$. Soit $d = \max(d_1, \dots, d_r, f)$. D'après l'annexe C.2, le calcul de $F_i \times_X F_j$ nécessite $d_i^{4d_i} f_j^{8f_j}$ opérations, et la courbe obtenue est de degré $O(d_i f_j^2)$. L'algorithme peut commencer par la composante de F correspondant à la section nulle : quitte à la remplacer par X, son degré est celui de X. Comme il y a au plus $\log_2 f$ étapes de récursion, le degré de la courbe trouvée à la fin est $O(d^{1+f})$. Le nombre de calculs à effectuer est $O(d^{13fd^{1+f}})$.

III.1.2 Morphismes, noyaux et conoyaux

Soient $\mathcal{F}, \mathcal{F}'$ deux faisceaux lisses de Λ-modules sur un schéma intègre X. Soit $Y \to X$ un revêtement galoisien de groupe G et de degré d qui trivialise $\mathcal{F}$. Définissons de même Y', G', d' pour $\mathcal{F}'$. Un revêtement galoisien W de X ayant pour corps de fonctions la composée de ceux de Y et Y' trivialise $\mathcal{F}$. Son degré est borné par dd'. Soit $H = \mathrm{Aut}(W|X)$. Notons M et M' les $\Lambda[H]$-modules $\mathrm{H}^0(W, f^\star\mathcal{F})$ et $\mathrm{H}^0(W, f^\star\mathcal{F}')$. Le revêtement W est l'une des composantes connexes de $Y \times_X Y'$ (qui est encore galoisienne sur X). Dans le cas général, le calcul de W est donc de complexité élémentaire en les entrées (voir annexe B.2). Dans le cas des courbes, le produit fibré $Y \times_X Y'$ se détermine comme décrit dans l'annexe C.2.

Un morphisme $\alpha\colon \mathcal{F} \to \mathcal{F}'$ peut être représenté par un morphisme de X-schémas en groupes $T \to T'$, ou par un morphisme de $\Lambda[H]$-modules $M \to M'$. Le faisceau $\operatorname{coker}\alpha$ est encore lisse puisque $\phi^\star \operatorname{coker}\alpha = \operatorname{coker}(\phi^\star\alpha)$ est le conoyau d'un morphisme de faisceaux constants et est donc constant [Stacks, 093J]. Le noyau et le conoyau de α se calculent alors dans la catégorie $\mathrm{Mod}_{\Lambda[H]}$. Soient m, m' les nombres de générateurs donnés de M et M'. Les calculs de $\ker\alpha$ et $\operatorname{coker}\alpha$ se font donc en $O(\max(m, m')^3)$ opérations une fois que W est construit.

III.1.3 Faisceaux lisses sur les courbes nodales

Voici comment seront représentés les faisceaux lisses sur les courbes nodales. Soient X une courbe intègre nodale, $\tilde{X}$ sa normalisée, $\mathcal{F}$ un faisceau lisse sur X, et $Y \to X$ un revêtement trivialisant de $\mathcal{F}$. La courbe X est représentée par la donnée d'un modèle plan $\tilde{X}_P$ de $\tilde{X}$ dont les singularités sont images de points de $\tilde{X}$ d'image régulière dans X, et des couples $(x, y) \in \tilde{X}_P(k)^2$ de points marqués qui sont les antécédents des points nodaux de X. L'utilité de distinguer les points de $\tilde{X}$ au-dessus des points nodaux de X deviendra claire dans la section III.6 ; un tel modèle s'obtient par transformations quadratiques à partir d'un modèle plan de X en éclatant chacun des points nodaux. La courbe Y est décrite par sa normalisée $\tilde{Y} = Y \times_X \tilde{X}$, qui n'est peut-être pas connexe : c'est une réunion disjointe $\tilde{Y}_P$ de courbes planes (dont les points singuliers ne sont pas au-dessus de points singuliers de Y) avec des couples de points marqués (n'appartenant pas nécessairement à une même composante connexe). Le faisceau $\mathcal{F}$ est donné par $\tilde{Y}_P \to \tilde{X}_P$ et le $\mathrm{Aut}(\tilde{Y}|\tilde{X})$-module $F = \mathrm{H}^0(Y, \mathcal{F})$.

III.2 Images directes de faisceaux lisses

Soit $f\colon Y \to X$ un morphisme quasi-fini de variétés régulières intègres de même dimension sur k. Nous allons décrire comment, étant donné un faisceau lisse sur Y, calculer les faisceaux constructibles $f_\star\mathcal{F}$ et $f_!\mathcal{F}$ sur X. Rappelons que par le théorème principal de Zariski [Stacks, 02LR], f peut être décomposé en

$$\begin{tikzcd} Y \arrow[r, "j"] \arrow[dr, "f"'] & X' \arrow[d, "\nu"] \\ & X \end{tikzcd}$$

où j est une immersion ouverte quasi-compacte et la normalisation $X' \to X$ de X dans Y est un morphisme fini. Comme X et Y sont régulières, le théorème de "platitude miraculeuse" [Stacks, 00R4] assure que $X' \to X$ est plat, c'est-à-dire localement libre [Stacks, 02KB]. Par conséquent, il suffit de considérer deux cas particuliers : celui où f est une immersion ouverte, et celui où f est fini localement libre.

Voici un argument ad hoc pour calculer une telle décomposition $Y \to X' \to X$. Comme f est quasi-fini, il est génériquement fini [Stacks, 03I1]. Le morphisme $Y \to X$ correspond (localement sur X) à

une extension $A \to B$ de k-algèbres, et une extension $K \to L$ de corps de fonctions. Soient $x_1, \dots, x_r$ des générateurs de B comme A-algèbre, et $f_1, \dots, f_r \in K[t]$ leurs polynômes minimaux respectifs. Pour tout $i \in \{1 \dots r\}$, soit g_i le produit des dénominateurs de f_i. Alors en posant $U = \operatorname{Spec} A[(g_1 \cdots g_r)^{-1}]$, le morphisme

$$X' = U \times_X Y \to U$$

est fini.

Remarque 3.2.1. Dans le cas où X et Y sont des courbes intègres régulières, la normalisation de X dans Y est simplement l'image inverse de X dans la compactification régulière de Y.

III.2.1 Image directe

Par une immersion ouverte Le résultat permettant de calculer le poussé en avant d'un faisceau lisse par une immersion ouverte est le suivant.

Proposition 3.2.2. [Jin20, Corollary 5.8] Soit k un corps. Soient X un schéma de type fini sur k, et $j\colon U \to X$ une immersion ouverte telle que la normalisation de X dans U soit X (ce qui est toujours le cas si X est normal). Soit $\mathcal{F}$ un faisceau fini localement constant d'ensembles sur U, représenté par un U-schéma fini étale F. Alors $j_\star\mathcal{F}$ est représenté par le lieu étale sur X de la normalisation de X dans F.

Si $j\colon U \to X$ est une immersion ouverte de variétés normales et $\mathcal{F}$ est un faisceau sur U représenté par un U-schéma F, le faisceau $j_\star\mathcal{F}$ se détermine donc en calculant la normalisation de X dans F, puis le lieu étale (c'est-à-dire non ramifié) de cette dernière au-dessus de X.

Remarque 3.2.3. Si $\mathcal{F}$ est un faisceau de groupes abéliens, voici comment se calcule la loi de groupe sur le schéma représentant $j_\star\mathcal{F}$. Notons que comme

$$j_\star(\mathcal{F} \times \mathcal{F}) = j_\star\mathcal{F} \times j_\star\mathcal{F}$$

il y a un isomorphisme canonique de schémas

$$j_\star(F \times_U F) \xrightarrow{\sim} j_\star F \times_X j_\star F.$$

La loi de groupe $F \times_U F \to F$ est donnée. Notons X' la normalisation de X dans F, et X'' la normalisation de X dans $F \times_U F$. Alors le morphisme $F \times_U F \to F \to X'$ donne lieu par propriété universelle de la normalisation relative [Stacks, 035I] à un morphisme de X-schémas $X'' \to X'$. La restriction de celui-ci au lieu étale de $X' \to X$ donne un morphisme $j_\star(F \times_U F) \to j_\star F$.

Par un morphisme fini localement libre Supposons que $f\colon Y \to X$ soit fini localement libre. Soit $\mathcal{F}$ un faisceau sur Y représenté par un Y-schéma F. Alors par [BLR90, 7.6, Th. 4], la restriction de Weil $R_{Y\to X}(F)$ existe et représente $f_\star\mathcal{F}$. L'algorithme qui calcule la restriction de Weil se trouve dans la section B.5.

III.2.2 Image directe à support propre

Par une immersion ouverte

Remarque 3.2.4. Soient U un schéma, et $f\colon G \to U$ un U-schéma en groupes fini étale. Considérons la section nulle $e\colon U \to G$. Alors $fe = \mathrm{id}_U$ est fini étale, et comme f est fini étale, e l'est aussi. En particulier, $e(U)$ est ouvert-fermé dans G, c'est donc une composante connexe de G. De plus, e a un inverse à gauche, c'est donc un isomorphisme sur son image. Le schéma G s'écrit donc $G = U \sqcup G'$, et $G(U) = \{\mathrm{id}\} \sqcup G'(U)$.

Lemme 3.2.5. Soit $j\colon U \to X$ une immersion ouverte de schémas connexes. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur U, représenté par un U-schéma en groupes $G \to U$. Notons $G = U \sqcup G'$, où U est la section nulle. Alors le schéma $Y \coloneqq X \sqcup G'$, muni de la loi de groupe induite par celle de $U \sqcup G'$, représente le faisceau $j_!\mathcal{F}$.

Démonstration. Soit $\alpha\colon T \to X$ étale. Supposons T connexe. Alors $Y(T) = X(T) \sqcup G'(T) = \{\alpha\} \sqcup G'(T)$. Remarquons que si l'image de $T \to X$ est incluse dans U, alors $\mathrm{Hom}_X(T, G') = \mathrm{Hom}_U(T, G')$, et sinon $\mathrm{Hom}_X(T, G') = \varnothing$. Ainsi, $Y(T) = \mathrm{Hom}_U(T, G) = \mathcal{F}(T)$ dans le premier cas, et $Y(T) = \{\alpha\}$ dans le second, ce qui implique que Y représente $j_!\mathcal{F}$. □

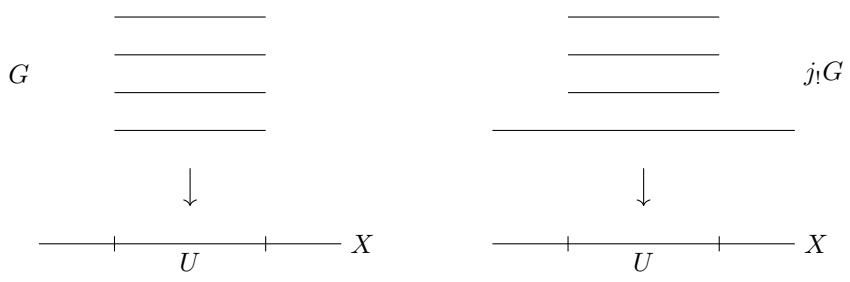


FIGURE III.1 – Prolongement par zéro d'un faisceau lisse

Par un morphisme fini localement libre Pour un morphisme fini f, les foncteurs $f_!$ et $f_\star$ sont égaux ; la représentabilité de $f_\star\mathcal{F}$ a été traitée ci-dessus.

En résumé, comme la détermination des composantes connexes d'un schéma et le calcul d'une restriction de Weil sont de complexité élémentaire (voir annexes B.2 et B.5), nous avons montré le résultat suivant.

Proposition 3.2.6. Il existe un algorithme de complexité élémentaire qui, étant donné un morphisme de k-variétés régulières $f\colon Y \to X$ et un faisceau lisse $\mathcal{F}$ sur Y représenté par un Y-schéma en groupes étale, calcule des X-schémas en groupes représentant les faisceaux $f_\star\mathcal{F}$ et $f_!\mathcal{F}$.

III.3 Faisceaux constructibles sur les courbes lisses

Nous allons maintenant décrire trois représentations différentes des faisceaux constructibles de Λ-modules sur une courbe intègre lisse sur k. Tout d'abord, un faisceau constructible peut toujours être exprimé comme conoyau d'un morphisme de la forme $f_!\Lambda \to g_!\Lambda$, où f et g sont étales. De même, il peut être exprimé comme noyau d'un morphisme $p_\star M \to q_\star N$, où p et q sont finis et M, N sont des Λ-modules de type fini. Enfin, il peut être défini par recollement relativement à un ouvert sur lequel il est lisse.

III.3.1 Représentation comme conoyau "(!)"

Proposition 3.3.1. [SGA4$_3$, IX, Prop. 2.7] Soit A un anneau noethérien. Soient X un schéma quasi-compact et quasi-séparé et $\mathcal{F}$ un faisceau de A-modules sur X. Pour que $\mathcal{F}$ soit constructible, il faut et il suffit qu'il soit isomorphe au conoyau d'un morphisme $f_!A \to g_!A$, où $f\colon X_1 \to X$ et $g\colon X_2 \to X$ sont deux morphismes étales de présentation finie.

La preuve classique de cette proposition consiste à considérer pour chaque point $x \in X$ un point géométrique $\bar{x}$ d'image x, et chaque $s \in \mathcal{F}_{\bar{x}}$ un schéma affine $\phi_{\bar{x},s} \colon T_{\bar{x},s} \to X$ tel que s appartienne à l'image de $\mathcal{F}(T_{\bar{x},s}) \to \mathcal{F}_{\bar{x}}$; cela signifie qu'il y a un morphisme $(\phi_{\bar{x},s})_!\Lambda \to \mathcal{F}$ dont l'image contient s. La constructibilité du faisceau permet alors d'appliquer un argument de noethérianité à $\bigoplus_{\bar{x},s} \phi_{\bar{x},s}$. En particulier, si X est une courbe intègre sur k, cet argument de finitude peut être rendu explicite : si U est un ouvert de lissité de $\mathcal{F}$, il suffit de considérer la fibre générique de U, ainsi que les fibres en les points du complémentaire zéro-dimensionnel de U. Pour la fibre générique, si $\phi \colon V \to U$ est un revêtement trivialisant, le morphisme $\mathcal{F}(V) \to \mathcal{F}_{\bar{\eta}}$ est un isomorphisme.

La représentation (!) Soit X une courbe intègre sur k. Un faisceau constructible $\mathcal{F}$ sur X sera représenté par deux morphismes étales $f \colon X_1 \to X$ et $g \colon X_2 \to X$ ainsi que d'un morphisme $u \colon f_!\Lambda \to g_!\Lambda$ tel que $\mathcal{F} = \operatorname{coker}(u)$; ce morphisme sera décrit explicitement de l'une des deux façons suivantes.

Représentation d'un morphisme $f_!\Lambda \to g_!\Lambda$ Soient $f \colon X_1 \to X$ et $g \colon X_2 \to X$ deux morphismes étales. Les faisceaux $f_!\Lambda$ et $g_!\Lambda$ sont représentables, et nous savons d'après III.2 déterminer explicitement des schémas en groupes Y_1, Y_2 qui les représentent. Un morphisme $f_!\Lambda \to g_!\Lambda$ est alors simplement un morphisme de schémas en groupes $Y_1 \to Y_2$. Un tel morphisme peut également être représenté de façon plus succincte : par adjonction, il est défini par la donnée d'un morphisme $\Lambda \to f^\star g_!\Lambda$, c'est-à-dire d'une section globale de $f^\star g_!\Lambda$ pour chaque composante connexe de X_1. Comme f est étale, cela revient à se donner un élément de $g_!\Lambda(X_1)$. Or [Fu15, p209] $g_!\Lambda(X_1)$ est l'ensemble des $s \in \Lambda(X_1 \times_X X_2) = \Lambda^{\pi_0(X_1 \times_X X_2)}$ de support propre sur X_1. Le support d'une telle section est une réunion de composantes connexes de $X_1 \times_X X_2$: il suffit de déterminer quelles composantes connexes sont propres (c'est-à-dire finies puisque f est étale, voir [Stacks, 02OG]) sur X_1.

Calcul du morphisme $f_!\Lambda \to \mathcal{F}$ associé à une section de $f^\star\mathcal{F}$ Soit $f \colon Y \to X$ un morphisme étale. Il se décompose en $f = gj$, où $j \colon Y \to X'$ est une immersion ouverte et $g \colon X' \to X$ est fini localement libre. Soit $\mathcal{F}$ un faisceau lisse sur X, représenté par un schéma en groupes fini étale $F \to X$. Soit $s \in \mathrm{H}^0(Y, f^\star\mathcal{F})$, qui correspond à un morphisme de Y-schémas en groupes $\coprod_\Lambda Y \to F \times_X Y$. Par adjonction, s définit un morphisme $j_!\Lambda \to g^\star\mathcal{F}$. Le faisceau $j_!\Lambda$ est représenté par $X' \sqcup \coprod_{\Lambda - \{0\}} Y$. Les $n-1$ morphismes $Y \to F \times_X X'$ sont simplement les composées $Y \to F \times_X Y \to F \times_X X'$. Le morphisme $X' \to F \times_X X'$ est la section nulle, déduite de la section nulle $X \to F$ par changement de base. Ce morphisme $j_!\Lambda \to g^\star\mathcal{F}$ donne à nouveau par adjonction un morphisme $f_!\Lambda = g_\star j_!\Lambda \to \mathcal{F}$, qui se calcule explicitement puisque $g_\star j_!\Lambda$ est la restriction de Weil $R_{X' \to X}(j_!\Lambda)$.

III.3.2 Représentation comme noyau "$(\star)$"

Proposition 3.3.2. [SGA4$_3$, IX, Prop. 2.14.(ii)] Soit X un schéma de type fini sur un corps ou sur $\mathbb{Z}$. Soit A un anneau noethérien. Soit $\mathcal{F}$ un faisceau constructible de A-modules sur X. Il existe des schémas noethériens intègres $X_i, i = 1, \ldots, m$, des morphismes finis $p_i \colon X_i \to X$ et des A-modules de type fini M_i tels qu'il y ait un monomorphisme

$$\mathcal{F} \hookrightarrow \bigoplus_{i=1}^{m} p_{i\star} M_i.$$

La preuve classique de cette proposition consiste (dans le cas irréductible) à considérer une décomposition $X = \bigcup_i U_i$ en parties localement fermées telles que chaque $\mathcal{F}|_{U_i}$ soit lisse. Il existe des morphismes finis étales $U_i' \to U_i$ tels que chaque $\mathcal{F}|_{U_i'}$ soit constant. La normalisation X_i de U_i' fournit le morphisme $p_i \colon X_i \to X$ recherché. Notons que si X est normal, les X_i le sont aussi.

Description d'un morphisme $p_\star M \to q_\star N$ Soit X une courbe intègre sur k. Soient $p\colon Y \to X$ et $q\colon Z \to X$ des morphismes finis, avec Y, Z intègres. Soient M, N deux groupes abéliens finis. Montrons, selon les dimensions de Y et Z, comment décrire un morphisme $p_\star M \to q_\star N$, c'est-à-dire par adjonction un morphisme $q^\star p_\star M \to N$.

1. Si Y et Z sont deux courbes, $p_\star M \to q_\star N$ est un morphisme de X-schémas entre les restrictions de Weil $R_p(Y \times M) \to R_q(Z \times N)$.
2. Si Z est un point fermé de X, $q^\star p_\star M$ est le faisceau de fibre $(p_\star M)_q = \bigoplus_{Y_q} M$ sur le point. Un morphisme $q^\star p_\star M \to N$ est donc simplement un morphisme de Λ-modules $\bigoplus_{Y_q} M \to N$.
3. Si Y est un point fermé et Z est une courbe, montrons que le seul morphisme $p_\star M \to q_\star N$ est le morphisme nul. Notons j l'inclusion d'un ouvert de X ne contenant pas Y. La transformation naturelle $\mathrm{id} \to j_\star j^\star$ fournit un diagramme commutatif :

$$\begin{tikzcd} p_\star M \arrow[r] \arrow[d] & j_\star j^\star p_\star M \arrow[d] \\ q_\star N \arrow[r] & j_\star j^\star q_\star N \end{tikzcd}$$

   D'une part, $j_\star j^\star p_\star M = 0$. D'autre part, notons $q'\colon Z \times_X U \to U$ et $j'\colon Z \times_X U \to Z$. Le morphisme $q_\star N \to j_\star j^\star q_\star N$ est un isomorphisme, car il s'identifie via les isomorphismes canoniques $j^\star q_\star N \xrightarrow{\sim} q'_\star j'^\star N$ et $N \xrightarrow{\sim} j'_\star j'^\star N$ au morphisme identité de $q_\star N$. Par conséquent, le morphisme $p_\star M \to q_\star N$ est nul.

La représentation $(\star)$ Reprenons les notations de la proposition 3.3.2, en supposant que X est une courbe intègre sur k. En appliquant la proposition au conoyau $\mathcal{G}$ de $\mathcal{F} \to \bigoplus_i p_{i\star} M_i$, le faisceau $\mathcal{F}$ s'exprime comme le noyau d'un morphisme $\bigoplus_i p_{i\star} M_i \to \bigoplus_j q_{j\star} N_j$. La représentation $(\star)$ de $\mathcal{F}$ est la donnée de ces morphismes $p_{i\star} M_i \to q_{j\star} N_j$, décrits explicitement comme dans le paragraphe précédent.

III.3.3 Représentation par recollement "$(\sqcup)$"

Soient X une courbe intègre sur k et $\mathcal{F}$ un faisceau constructible sur X. Soit U un ouvert de X sur lequel $\mathcal{F}$ est localement constant. Notons Z le fermé réduit complémentaire. Notons $j\colon U \to X, i\colon Z \to X$ les inclusions, et $z_1, \ldots, z_r$ les points fermés de Z. Par recollement (voir section I.2.6), $\mathcal{F}$ est uniquement déterminé par les données suivantes :

- le faisceau lisse $\mathscr{L} = j^\star \mathcal{F}$;
- le faisceau $\mathcal{F}_Z = i^\star \mathcal{F}$, défini par les groupes abéliens finis $\mathcal{F}_{z_1}, \ldots, \mathcal{F}_{z_r}$;
- le morphisme de recollement $\phi\colon \mathcal{F}_Z \to i^\star j_\star \mathscr{L}$.

Nous appellerons représentation par recollement ou représentation $(\sqcup)$ de $\mathcal{F}$ par rapport à (U, Z) la donnée du triplet $(\mathscr{L}, \mathcal{F}_Z, \phi)$. Toute donnée de cette forme définit un faisceau constructible sur X. Le carré suivant, où les flèches non étiquetées désignent les unités d'adjonction, est alors cartésien.

$$\begin{tikzcd} \mathcal{F} \arrow[r] \arrow[d] & i_\star \mathcal{F}_Z \arrow[d, "i_\star \phi"] \\ j_\star \mathscr{L} \arrow[r, "c"] & i_\star i^\star j_\star \mathscr{L} \end{tikzcd}$$

Soit $Y \to X$ étale. Le diagramme cartésien ci-dessus montre que

$$\mathcal{F}(Y) = \{(s, t) \in i_\star \mathcal{F}_Z(Y) \times j_\star \mathscr{L}(Y) \mid i_\star \phi(s) = c(t)\}.$$

D'une part,

$$i_\star \mathcal{F}_Z(Y) = \mathcal{F}_Z(Y|_Z) = \bigoplus_{i=1}^{r} \bigoplus_{y \in Y_{z_i}(k)} \mathcal{F}_{z_i}.$$

D'autre part, $j_\star \mathscr{L}(Y) = \mathscr{L}(Y|_U)$ et le morphisme

$$j_\star \mathscr{L}(Y) \to i_\star i^\star j_\star \mathscr{L}(Y) = \bigoplus_{i=1}^{r} \bigoplus_{y \in Y_{z_i}(k)} (j_\star \mathscr{L})_{z_i}$$

envoie une section $s \in \mathscr{L}(Y)$ sur $(s_{z_i})_{i \in \{1 \dots r\}, y \in Y_{z_i}(k)}$. En résumé :

$$\mathcal{F}(Y) = \{(s,t) \in (\bigoplus_{i=1}^{r} \bigoplus_{y \in Y_{z_i}(k)} \mathcal{F}_{z_i}) \times j_\star \mathscr{L}(Y) \mid \forall i \in \{1 \dots r\}, \forall y \in Y_{z_i}(k), \phi(s_{z_i,y}) = t_{z_i}\}.$$

Remarque 3.3.3. Nous disposons de deux moyens pour déterminer la fibre en chaque z_i de $j_\star \mathscr{L}$. D'une part, si $\mathscr{L}$ est donné comme un U-schéma en groupes fini étale, le schéma F représentant $j_\star \mathscr{L}$ se calcule comme décrit en 3.2.2, et la fibre de $j_\star \mathscr{L}$ en z_i est simplement $F \times_X z_i$. Afin de déterminer cette fibre explicitement comme groupe fini, il est nécessaire de déterminer ses points. D'autre part, si X est lisse et $\mathscr{L}$ est donné par un revêtement trivialisant $X' \to X$ et une action de $\mathrm{Aut}(X'|X)$ sur $F := \mathcal{F}(X')$, alors $(j_\star \mathscr{L})_{z_i} = F^{I_{z_i}}$, où $I_{z_i} \subset \mathrm{Aut}(X'|X)$ désigne le stabilisateur dans $\mathrm{Aut}(X'|X)$ d'un antécédent de z_i. Il suffit donc de déterminer ces groupes d'inertie.

Remarque 3.3.4. Le faisceau constructible défini par $(\mathscr{L}, \mathcal{F}_Z, \phi)$ est lisse si et seulement si la fibre M de $\mathscr{L}$ est invariante sous les groupes d'inertie $I_z, z \in Z$ et le morphisme ϕ est un isomorphisme.

III.3.4 Représentation ($\sqcup$) d'un faisceau constructible représentable

Soit X une courbe intègre sur k. Soit $\mathcal{F}$ un faisceau constructible sur X représenté par un schéma étale $F \to X$. Montrons comment représenter $\mathcal{F}$ par recollement. Comme f est étale, il est quasi-fini. Soit $j\colon U \to X$ un ouvert tel que $F' := F \times_X U$, qui représente alors $j^\star \mathcal{F}$, soit fini sur U. Notons X' le normalisé de X dans F, qui est encore le normalisé de X dans l'ouvert F' de F : la situation est résumée par le diagramme commutatif suivant.

$$\begin{tikzcd} F' \arrow[r] \arrow[d] & F \arrow[r] \arrow[d] & X' \arrow[dl] \\ U \arrow[r] & X & \end{tikzcd}$$

Comme $F \to X$ est étale, F est inclus dans le lieu étale de $X' \to X$, qui représente $j_\star j^\star \mathcal{F}$. Ceci fournit directement la flèche injective $\mathcal{F} \to j_\star j^\star \mathcal{F}$, qui sur les fibres en les points de $X - U$ donne le morphisme de recollement.
Un morphisme $f\colon F \to G$ de schémas finis étales sur X, peut également être représenté par recollement, en choisissant pour U un ouvert sur lequel les deux schémas sont finis. Le morphisme de faisceaux lisses $f|_U$ sur U est alors simplement un morphisme de schémas en groupes, et le morphisme sur la fibre en un point $z\colon \operatorname{Spec} k \to X - U$ est simplement $F_z \to G_z$.

III.3.5 Équivalence entre ($\star$) et ($\sqcup$)

Soit X une courbe intègre lisse sur k. Soit $\mathcal{F}$ un faisceau constructible sur X.

$(\star) \to (\sqcup)$ Voici comment donner une représentation par recollement d'un faisceau défini par une représentation $(\star)$. Dans cette représentation, le faisceau est somme directe de noyaux de morphismes de la forme $p_\star M \to q_\star N$ où p, q sont des morphismes finis de cible X. Il suffit donc de savoir représenter par recollement un faisceau de la forme $p_\star M$ avec $p\colon Y \to X$ fini, ainsi que les morphismes entre de tels faisceaux. Il y a deux cas à considérer :

1. Si Y est une courbe lisse, $p_\star M$ est la restriction de Weil $R_p(Y \times M)$, qui est étale sur X [Sch94, Prop. 4.9]. Nous avons décrit dans la section III.3.4 comment représenter par recollement les (morphismes de) X-schémas étales.
2. Si Y est l'inclusion d'un point fermé de X, le faisceau $p_\star M$ est constant sur $X - Y$ de valeur 0, a pour fibre M en Y, et son morphisme de recollement est nul.

$(\sqcup) \to (\star)$ Supposons $\mathcal{F}$ représenté par recollement relativement à un ouvert de lissité $j\colon U \to X$ et son fermé réduit complémentaire $i\colon Z \to X$. Soit V un revêtement galoisien de U trivialisant le faisceau lisse $j^\star\mathcal{F}$ de fibre M. Nous avons décrit dans la section III.1.1 comment calculer un U-schéma F représentant $j^\star\mathcal{F}$. La normalisation $p\colon V' \to X$ de X dans V fournit un premier morphisme fini ; les inclusions $z\colon \operatorname{Spec} k \to X$ des points de Z fournissent les autres. Décrivons par recollement l'injection

$$\phi\colon \mathcal{F} \longrightarrow p_\star M \oplus \bigoplus_{z \in Z} \mathcal{F}_z.$$

Sur U, c'est le morphisme

$$j^\star\mathcal{F} \longrightarrow j^\star p_\star M = j^\star p_\star p^\star \mathcal{F} = p|_U{}_\star p|_U{}^\star j^\star \mathcal{F}$$

obtenu en appliquant l'unité d'adjonction $\mathrm{id} \to p|_U{}_\star p|_U^\star$ au faisceau lisse $j_\star\mathcal{F}$. En termes de schémas, c'est le morphisme $F \to R_{Y\to X}(F \times_U V)$ qui est calculable explicitement (voir annexe B.5). Sur $z \in Z$, le morphisme ϕ est l'injection $0 \oplus \mathcal{F}_z \to M^{I_z} \oplus \mathcal{F}_z$. Cette description de ϕ par recollement permet de calculer $\operatorname{coker}\phi$, et d'obtenir par la même procédure une injection

$$\operatorname{coker}\phi \to q_\star N \oplus \bigoplus_{w \in W} w_\star N_w$$

où q est la normalisation de X dans un schéma étale sur X, et W est un fermé zéro-dimensionnel de X. Le morphisme

$$p_\star M \oplus \bigoplus_z z_\star \mathcal{F}_z \to q_\star N \oplus \bigoplus_w w_\star N_w$$

qui s'en déduit a pour noyau $\mathcal{F}$. Ce morphisme est représenté de la façon suivante. Le morphisme $p_\star M \to q_\star N$ est la composée

$$p_\star M \longrightarrow j^\star \operatorname{coker}\phi \longrightarrow q_\star N.$$

Il est décrit par le morphisme correspondant entre restrictions de Weil. Les morphismes

$$p_\star M \oplus \bigoplus_z z_\star \mathcal{F}_z \to \bigoplus_w w_\star N_w$$

sont décrits fibre à fibre.

III.3.6 Équivalence entre (!) et $(\sqcup)$

Soit X une courbe intègre lisse sur k. Soit $\mathcal{F}$ un faisceau constructible sur X.

(!) $\to$ ($\sqcup$) Étant donné une représentation de $\mathcal{F}$ comme $\operatorname{coker}(u\colon f_!\Lambda \to g_!\Lambda)$, où f est g sont étales de type fini, il est possible de calculer explicitement le morphisme de X-schémas étales représenté par u. Nous avons décrit dans la section III.3.4 comment donner une représentation par recollement d'un tel morphisme.

($\sqcup$) $\to$ (!) Supposons $\mathcal{F}$ défini par recollement relativement à un couple ouvert-fermé

$$U \xhookrightarrow{\ j\ } X \xhookleftarrow{\ i\ } Z$$

par la donnée d'un faisceau lisse $\mathscr{L}$ sur U trivialisé par un revêtement étale V, des fibres $\mathcal{F}_z$ en les points de Z et un morphisme $\phi\colon i^\star\mathcal{F} \to i^\star j_\star\mathscr{L}$. Remarquons que la preuve de la proposition 3.3.1 est constructive, mis à part pour la détermination, pour $z \in Z$ et $s \in \mathcal{F}_z$, d'un morphisme étale $f\colon T \to X$ tel que l'image de $\mathcal{F}(T) \to \mathcal{F}_z$ contienne s.

Soient donc $z \in Z$ et $s \in \mathcal{F}_z$. Rappelons que $\mathcal{F} = j_\star\mathscr{L} \times_{i_\star i^\star j_\star\mathscr{L}} i_\star i^\star\mathcal{F}$. Par conséquent, l'image de $\mathcal{F}(T) \to \mathcal{F}_z$ contient s si et seulement si l'image de s par le morphisme de recollement $\phi_T\colon i^\star\mathcal{F}(T) = \bigoplus_z \mathcal{F}_z \to i^\star j_\star\mathscr{L}(T) = \bigoplus_z (j_\star\mathscr{L})_z$ a un antécédent par $j_\star\mathscr{L}(T) \to \bigoplus_z (j_\star\mathscr{L})_z$. Notons G le schéma représentant $\mathscr{L}$. Le faisceau $\mathcal{F}' \coloneqq j_\star\mathscr{L}$ est représentable par un schéma étale F sur X et la fibre $\mathcal{F}'_z$ est simplement $F \times_X z$. Le diagramme commutatif suivant résume les notations.

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & F \arrow[d] & F_z \arrow[l] \arrow[d] \\
U \arrow[r] & X & z \arrow[l]
\end{tikzcd}$$

Dans le cas où $\mathcal{F}$ est lisse sur X, l'algorithme classique consiste à construire par changements de base successifs un revêtement étale $Y \to X$ qui trivialise $\mathcal{F}$; le morphisme $\mathcal{F}(Y) \to \mathcal{F}_z$ est alors un isomorphisme. L'algorithme suivant, qui s'inspire de celui-ci, permettra d'obtenir le schéma souhaité pour les faisceaux constructibles.

Posons $U_0 = U$, $X_0 = X$, $F_0 = F$, $G_0 = G$ et $z_0 = z$. L'algorithme construit une suite $(X_i, U_i, F_i, G_i, z_i)_{i\geqslant 0}$ de la façon suivante. Soit $i \in \mathbb{N}$. Soit C une composante connexe de G_i. Notons Y le lieu étale de la normalisation de X_i dans C.

- Si $\deg(C \to U_i) > 1$ et la fibre Y_{z_i} est non vide, soit $z_{i+1} \in Y_{z_i}$. Posons alors $U_{i+1} = C$, $X_{i+1} = Y$, $G_{i+1} = G_i \times_{U_i} C$ et $F_{i+1} = F_i \times_{X_i} Y$.
- Sinon, on revient au choix de C ; si pour toute composante connexe C de G_i, $\deg(C \to U_i) > 1$ ou Y_{z_i} est vide, l'algorithme s'arrête et renvoie $Y_f \coloneqq X_i$.

Cet algorithme s'arrête au bout d'un nombre fini d'opérations : en effet, pour chaque entier $i \in \{0 \dots i_f - 1\}$, G_{i+1} a strictement plus de composantes connexes que G_i alors que $\deg(G_{i+1} \to U_{i+1}) = \deg(G \to U)$. Notons i_f la valeur de l'indice i lorsque l'algorithme termine. Nous allons prouver que $\mathcal{F}(Y_f) \to \mathcal{F}_z$ est surjectif.

Lemme 3.3.5. Pour tout entier $i \in \{0 \dots i_f\}$, $j_{i,\star}(G_i) = F_i$.

Démonstration. Montrons-le par récurrence sur l'entier i. L'assertion concernant F_0 vient directement de sa définition. Soit désormais i tel que $j_{i,\star}(G_i) = F_i$. Soient C la composante connexe de G_i choisie

et Y la normalisation de X_i dans C. Il y a un diagramme commutatif :

$$\begin{tikzcd}
 & G_{i+1} \arrow[rr] \arrow[dl] \arrow[dd] & & F_{i+1} \arrow[dl] \arrow[dd] \\
G_i \arrow[rr] \arrow[dd] & & F_i \arrow[dd] & \\
 & C \arrow[rr] \arrow[dl] & & Y \arrow[dl] \\
U_i \arrow[rr, "j_i"] & & X_i &
\end{tikzcd}$$

Nous savons que $j_{i+1,\star}(G_{i+1})$ est le lieu étale de la normalisation $\tilde{Y}$ de Y dans G_i. De plus, par hypothèse de récurrence, $j_{i,\star}G_i = F_i$ est le lieu étale de la normalisation $\tilde{X}_i$ de X_i dans G_i. Comme le morphisme $Y \to X_i$ est lisse, le changement de base $- \times_{X_i} Y$ commute à la normalisation [Stacks, 03GV] et $\tilde{Y} = \tilde{X}_i \times_{X_i} Y$. Enfin, comme Y est plat sur X_i et $\tilde{X}_i \to X_i$ est de présentation finie, le lieu étale de $\tilde{X}_i \times_{X_i} Y \to Y$ est le changement de base à Y du lieu étale de $\tilde{X}_i \to X_i$ [Stacks, 0476]. Cela signifie que le lieu étale de $\tilde{Y} \to Y$, qui représente $j_{i+1,\star}(G_{i+1})$, est F_{i+1}. □

Lemme 3.3.6 (3.3.6.0.2)**.** Si, pour toute composante connexe C de G_i telle que $\deg(C_i \to U_i) > 1$, le lieu étale de la normalisation de X_i dans C ne contient aucun point au-dessus de z_i, alors le morphisme $F_i(X_i) \to F_{i,z_i}$ est un isomorphisme.

Démonstration. Écrivons $G_i = \bigsqcup_\alpha C_\alpha$. Alors $j_{i,\star}G_i$ est représenté par $F_i = \bigsqcup_\alpha X_{i,\alpha}$, où $X_{i,\alpha}$ est le lieu étale de la normalisation de X_i dans C_α. La normalisation de X_i dans U_i étant X_i,

$$j_{i,\star}G_i = \coprod_{\deg(C_\alpha \to U_i)=1} X \sqcup \coprod_{\deg(C_\alpha \to U_i)>1} X_{i,\alpha}.$$

Par conséquent, l'hypothèse assure que

$$|F_{i,z_i}| = |\{\alpha \mid \deg(C_\alpha \to U_i) = 1\}| =: d.$$

De plus, pour tout $T \to X_i$ voisinage étale de z_i, $F_i(T) = G_i(T \times_X U)$ contient au moins d éléments (les flèches $T \times_{X_i} U_i \to C_\alpha$ avec $\deg(C_\alpha \to U) = 1$), qui sont préservés par les flèches de restriction $F_i(T) \to F_i(T')$ et sont donc encore distincts dans $F_{i,z_i} = \operatorname{colim}_{(T,t)\to(Y,z)} F_i(T)$. Enfin, $F_i(X_i) = G_i(U_i)$ contient exactement d éléments, puisque comme $G_i \to U_i$ est fini étale, les sections $U_i \to G_i$ sont en bijection avec les composantes connexes de G_i de degré 1 sur U_i. □

Proposition 3.3.7. Le morphisme $\mathcal{F}(Y_f) \to \mathcal{F}_z$ est un isomorphisme.

Démonstration. À chaque étape de la boucle, $F_{i,z_i} = F_z$ et comme $F_i \to F$ est étale, $F_i(X_i) = F(X_i)$. Par conséquent, lorsque l'algorithme s'est arrêté, $F(X_i) \to F_z$ est un isomorphisme. Choisissons un ouvert Y' de Y_f ne contenant qu'un seul point au-dessus de Z, d'image z. Alors $F(Y') = F(Y_f)$ et le morphisme $F(Y') \to F_z$ est encore un isomorphisme. Rappelons que

$$\mathcal{F}_z = \operatorname{colim}_{T\to(X,z)}[\mathcal{F}|_Z(T \times_X Z) \times_{F(T\times_X Z)} F(T)]$$

et que la catégorie des voisinages étales connexes T de (X, z) n'ayant au-dessus de Z qu'un seul point d'image z est cofinale dans celle des voisinages étale de (X, z). Par conséquent, $\mathcal{F}_z = \operatorname{colim}_T \mathcal{F}_z \times_{F_z} F(T)$. Le morphisme $F(Y') \to F_z$ étant bijectif, le morphisme $\mathcal{F}(Y') \to \mathcal{F}_z$ l'est encore. Par conséquent, le morphisme $\mathcal{F}(Y_f) \to \mathcal{F}_z$ l'est aussi. □

III.4 Opérations sur les faisceaux dans la représentation ($\sqcup$)

Dans toute cette section, X désigne une courbe intègre lisse sur k. Nous décrivons comment effectuer des opérations sur les faisceaux constructibles sur X. La représentation par recollement est celle utilisée par les algorithmes de calcul de cohomologie du chapitre V, c'est pourquoi nous nous efforçons de décrire toutes les opérations dans cette représentation, même si elles admettent une expression plus simple dans l'une des autres représentations (ce que nous mentionnons le cas échéant).

III.4.1 Restriction à un ouvert plus petit

Il sera utile par la suite, étant donné une représentation par recollement d'un faisceau constructible $\mathcal{F}$ par rapport à un ouvert de lissité U, de déterminer la représentation par recollement de ce même faisceau $\mathcal{F}$ par rapport à un ouvert plus petit que U.

Soient U un ouvert de X, et Z le fermé complémentaire. Étant donné un faisceau constructible $\mathcal{F}$ lisse sur U, défini comme ci-dessus par le triplet $(\mathscr{L}, \mathcal{F}_Z, \phi)$, et un autre ouvert $U' \subset U$ de complémentaire réduit Z' dans X, comment calculer la représentation de $\mathcal{F}$ relativement au couple (U', Z') ?

$$U' \xrightarrow{\alpha} U \xrightarrow{j} X \xleftarrow{i'} Z' \xleftarrow{\beta} Z$$

Le morphisme donné est $\phi\colon \beta^\star i'^\star \mathcal{F} \to \beta^\star i'^\star j_\star j^\star \mathcal{F}$. Calculons $\psi\colon i'^\star \mathcal{F} \to i'^\star j_\star \alpha_\star \alpha^\star j^\star \mathcal{F}$, défini par ses fibres en les points $z \in Z'$.

Pour les points $z \in Z$, ce morphisme est le morphisme déja donné. En effet, d'après le lemme 1.4.14, le morphisme $j^\star \mathcal{F} \to \alpha_\star \alpha^\star j^\star \mathcal{F}$ est un isomorphisme. Par conséquent, le morphisme

$$i'^\star j_\star j^\star \mathcal{F} \to i'^\star j_\star \alpha_\star \alpha^\star j^\star \mathcal{F}$$

est encore un isomorphisme, et le morphisme cherché

$$i'^\star \mathcal{F} \to i'^\star j_\star \alpha_\star \alpha^\star j^\star \mathcal{F}$$

s'identifie au morphisme

$$i'^\star \mathcal{F} \to i'^\star j_\star j^\star \mathcal{F}.$$

Ses fibres en chaque point de Z sont celles du morphisme donné

$$\phi\colon \beta^\star i'^\star \mathcal{F} \to \beta^\star i'^\star j_\star j^\star \mathcal{F}.$$

Pour un point $w \in Z' - Z = U - U'$, la flèche cherchée

$$\mathcal{F}_w \to (j_\star \alpha_\star \alpha^\star j^\star \mathcal{F})_w$$

s'identifie à la flèche $\mathcal{F}_w \to (j_\star j^\star \mathcal{F})_w$, qui est elle-même un isomorphisme puisque w est un point de U.

III.4.2 Morphismes et somme directe

Soient $\mathcal{F}_1$ et $\mathcal{F}_2$ deux faisceaux constructibles sur X. Soient U_1, U_2 les ouverts de lissité de $\mathcal{F}_1$ et $\mathcal{F}_2$ donnés dans leur définition. Posons $U = U_1 \cap U_2$ et $Z = X - U$. Notons $j\colon U \to X$ et $i\colon Z \to X$ les inclusions. Alors U est un ouvert de lissité de $\mathcal{F}_1$ et $\mathcal{F}_2$, et nous savons déterminer les représentations $(\mathscr{L}_1, \mathcal{F}_{1,Z}, \phi_1)$ et $(\mathscr{L}_2, \mathcal{F}_{2,Z}, \phi_2)$ de $\mathcal{F}_1$ et $\mathcal{F}_2$ relativement à (X, U, Z). Un morphisme $f\colon \mathcal{F}_1 \to \mathcal{F}_2$ est alors déterminé par la donnée suivante :

- un morphisme de faisceaux lisses $\alpha\colon \mathscr{L}_1 \to \mathscr{L}_2$;
- un morphisme $\beta\colon \mathcal{F}_{1,Z} \to \mathcal{F}_{2,Z}$ défini sur les fibres en les $z \in Z$;
- un morphisme $\gamma\colon i^\star j_\star \mathscr{L}_1 \to i^\star j_\star \mathscr{L}_2$ vérifiant $\gamma \circ \phi_1 = \phi_2 \circ \beta$.

Pour qu'une telle donnée définisse correctement un morphisme, il faut et il suffit que $\gamma = i^\star j_\star \alpha$.

Noyau Par exactitude à gauche de $i^\star$, $j^\star$ et $j_\star$, le noyau d'un tel morphisme est défini par le triplet $(\ker\alpha, \ker\beta, \phi|_{\ker\beta})$.

Conoyau De même, l'exactitude à droite de $i^\star$ et $j^\star$ montre que

$$\operatorname{coker}\alpha = j^\star \operatorname{coker} f \quad \text{et} \quad \operatorname{coker}\beta = i^\star \operatorname{coker} f.$$

Enfin, la flèche $j_\star j^\star \mathcal{F}_2 \to j_\star j^\star \operatorname{coker}(f)$ se factorise par $\operatorname{coker}(j_\star j^\star f)$; la flèche composée

$$\mathcal{F}_2 \to j_\star j^\star \mathcal{F}_2 \to \operatorname{coker} j_\star j^\star f \xrightarrow{u} j_\star j^\star \operatorname{coker}(f)$$

passe au quotient en

$$\operatorname{coker} f \to \operatorname{coker}(j_\star j^\star \mathcal{F}_1) \xrightarrow{u} j_\star j^\star \operatorname{coker}(f).$$

On en déduit que la flèche de recollement $i^\star \operatorname{coker}(f) \to i^\star j_\star j^\star \operatorname{coker}(f)$ est la composée du morphisme $\operatorname{coker}(\beta) \to \operatorname{coker}(\gamma)$ (induit par la flèche de recollement ϕ_2) suivi de $i^\star u\colon \operatorname{coker}\gamma \to i^\star j_\star j^\star \operatorname{coker}(f)$. Remarquons que la dernière flèche se décrit explicitement. Soit $z \in Z(k)$. Soient F_1, F_2 les fibres des faisceaux lisses $\mathscr{L}_1, \mathscr{L}_2$, et notons $f_{\bar\eta}\colon F_1 \to F_2$ le morphisme induit par f. Notons I_z le groupe d'inertie en z. Alors la flèche u_z est simplement $F_2^{I_z}/f_{\bar\eta}(F_1^{I_z}) \to (F_2/f_{\bar\eta}(F_1))^{I_z}$.

Somme directe De même, la somme directe de $\mathcal{F}_1$ et $\mathcal{F}_2$ est simplement définie sur (X, U, Z) par $(\mathscr{L}_1 \oplus \mathscr{L}_2, \mathcal{F}_{1,Z} \oplus \mathcal{F}_{2,Z}, \phi_1 \oplus \phi_2)$.

III.4.3 Produit tensoriel et Hom interne

Lemme 3.4.1. Soit Y un schéma. Soit $j\colon U \to Y$ un morphisme étale. Alors pour tous faisceaux $\mathcal{F}, \mathcal{F}'$ de groupes abéliens sur Y, il y a des isomorphismes canoniques $j^\star\mathcal{F} \otimes j^\star\mathcal{F}' \xrightarrow{\sim} j^\star(\mathcal{F} \otimes \mathcal{F}')$ et $j^\star\underline{\mathrm{Hom}}(\mathcal{F}, \mathcal{F}') \xrightarrow{\sim} \underline{\mathrm{Hom}}(j^\star\mathcal{F}, j^\star\mathcal{F}')$.

Démonstration. Le foncteur $j^\star$ étant simplement la restriction du site étale de X à celui de U, l'assertion pour le Hom interne est claire, puisque les deux faisceaux en question ont pour sections sur $V \to U$ le groupe $\mathrm{Hom}(\mathcal{F}|_V, \mathcal{F}'|_V)$. Quant au produit tensoriel, les isomorphismes canoniques suivants, valables pour tout faisceau $\mathcal{G}$ de groupes abéliens sur X, permettent de conclure.

$$\begin{aligned}
\mathrm{Hom}(j^\star\mathcal{F} \otimes j^\star\mathcal{F}', \mathcal{G}) &= \mathrm{Hom}(j^\star\mathcal{F}, \underline{\mathrm{Hom}}(j^\star\mathcal{F}', \mathcal{G})) && [\text{Mil80, 3.19}]\\
&= \mathrm{Hom}(\mathcal{F}, j_\star\underline{\mathrm{Hom}}(j^\star\mathcal{F}', \mathcal{G}))\\
&= \mathrm{Hom}(\mathcal{F}, \underline{\mathrm{Hom}}(\mathcal{F}', j_\star\mathcal{G})) && [\text{Mil80, 3.22.a)}]\\
&= \mathrm{Hom}(\mathcal{F} \otimes \mathcal{F}', j_\star\mathcal{G})\\
&= \mathrm{Hom}(j^\star(\mathcal{F} \otimes \mathcal{F}'), \mathcal{G}).
\end{aligned}$$

□

Soit U un ouvert de X, de complémentaire réduit Z. Soient $\mathcal{F}$ et $\mathcal{F}'$ deux faisceaux constructibles de Λ-modules sur X lisses sur U, définis par recollement par les données $(\mathscr{L}, \mathcal{F}_Z, \phi)$ et $(\mathscr{L}', \mathcal{F}'_Z, \phi')$. Notons F, F' les fibres respectives des faisceaux lisses $\mathscr{L}, \mathscr{L}'$.

Produit tensoriel Comme le produit tensoriel commute au tiré en arrière, $j^\star(\mathcal{F}\otimes\mathcal{F}') = \mathscr{L}\otimes\mathscr{L}'$; le faisceau $\mathscr{L}\otimes\mathscr{L}'$ est encore un faisceau lisse sur U [Stacks, 093V]. Notons $M = \mathrm{H}^0(V,\mathscr{L})$ et $M' = \mathrm{H}^0(V,\mathscr{L}')$. Soit $V\to U$ un revêtement qui trivialise $\mathscr{L}$ et $\mathscr{L}'$. Pour $z\in Z$, notons I_z le sous-groupe des éléments de $\mathrm{Aut}(V|U)$ fixant un même antécédent de z dans la compactification lisse $\bar{V}$ de V. La fibre de $\mathcal{F}\otimes\mathcal{F}'$ en un point z de Z est encore $\mathcal{F}_z\otimes\mathcal{F}'_z$. Il reste à décrire les fibres en les points de Z du morphisme $\mathcal{F}\otimes\mathcal{F}'\to j_\star j^\star(\mathcal{F}\otimes\mathcal{F}')$, qui provient par adjonction des foncteurs $j^\star$ et $j_\star$ du morphisme identité de $\mathcal{F}\otimes\mathcal{F}'$. Notons $g\colon \mathcal{F}\otimes\mathcal{F}'\to j_\star j^\star\mathcal{F}\otimes j_\star j^\star\mathcal{F}'$ le morphisme déduit de $\mathrm{id}\to j_\star j^\star$. Le diagramme commutatif

$$\begin{tikzcd}
j^\star(\mathcal{F}\otimes\mathcal{F}') \arrow[r, "\mathrm{id}"] \arrow[d, "j^\star g"', "\wr"] & j^\star(\mathcal{F}\otimes\mathcal{F}') \\
j^\star(j_\star j^\star\mathcal{F}\otimes j_\star j^\star\mathcal{F}') \arrow[ur, "(j^\star g)^{-1}"'] &
\end{tikzcd}$$

produit par adjonction le diagramme commutatif

$$\begin{tikzcd}
\mathcal{F}\otimes\mathcal{F}' \arrow[r] \arrow[d, "g"'] & j_\star j^\star(\mathcal{F}\otimes\mathcal{F}') \\
j_\star j^\star\mathcal{F}\otimes j_\star j^\star\mathcal{F}' \arrow[ur] &
\end{tikzcd}$$

qui montre que le morphisme de recollement $i^\star(\mathcal{F}\otimes\mathcal{F}')\to i^\star j_\star j^\star(\mathcal{F}\otimes\mathcal{F}')$ est la composée

$$\mathcal{F}_Z\otimes\mathcal{F}'_Z\to i^\star j_\star\mathscr{L}\otimes i^\star j_\star\mathscr{L}' = i^\star(j_\star\mathscr{L}\otimes j_\star\mathscr{L}')\to i^\star j_\star(\mathscr{L}\otimes\mathscr{L}').$$

Sa fibre en z est la composée

$$\mathcal{F}_z\otimes\mathcal{F}'_z\xrightarrow{\phi_z\otimes\phi'_z} M^{I_z}\otimes M'^{I_z}\to(M\otimes M')^{I_z}.$$

Hom interne Comme vu dans le lemme 3.4.1, $j^\star\underline{\mathrm{Hom}}(\mathcal{F},\mathcal{F}')$ est le faisceau lisse $\underline{\mathrm{Hom}}(\mathscr{L},\mathscr{L}')$ dont la fibre est $\mathrm{Hom}_\Lambda(F,F')$.

Proposition 3.4.2. Soit z un point de Z. Soit $V\to U$ un revêtement galoisien trivialisant $\mathcal{F}$ et $\mathcal{F}'$. Notons $I\triangleleft\mathrm{Aut}(V|U)$ le sous-groupe distingué engendré par les groupes d'inertie en tous les points de $\bar{V}$ au-dessus de Z. Alors

$$\underline{\mathrm{Hom}}(\mathcal{F},\mathcal{F}')_z = \{(\alpha,\beta)\in\mathrm{Hom}_\Lambda(F,F')^I\times\mathrm{Hom}_\Lambda(\mathcal{F}_z,\mathcal{F}'_z)\mid \alpha\phi_{\mathcal{F}} = \phi_{\mathcal{F}'}\beta\}.$$

Démonstration. Soit $V\to U$ un revêtement galoisien trivialisant les faisceaux $\mathscr{L}$ et $\mathscr{L}'$. Soit V_1 le sous-revêtement de V de groupe $\mathrm{Aut}(V_1|U) = G/I$. Notons $X' = X-(Z-\{z\})$. Soient V' et V'_1 les normalisées respectives de X' dans V et V_1. Le morphisme $V'_1\to X'$ est étale, puisque G/I agit librement sur $(V'_1)_z$; c'est le sous-revêtement non ramifié maximal de $V'\to X'$. Par définition,

$$\underline{\mathrm{Hom}}(\mathcal{F},\mathcal{F}')_z = \mathrm{colim}_{(Y,y)}\,\mathrm{Hom}(\mathcal{F}|_Y,\mathcal{F}'|_Y)$$

où les couples (Y,y) sont des voisinages étales de (X,z). La sous-catégorie des voisinages étales (Y,y) vérifiant :

- Y est connexe
- Y_z est réduit à un point
- $Y\to X$ se factorise par V'_1

- $k(Y)/k(X)$ est galoisienne

est cofinale dans celle des voisinages étales de (X, z). Considérons un tel $f\colon (Y, y) \to (X, z)$ et le diagramme cartésien suivant.

$$\begin{tikzcd}
Y_U \arrow[r] \arrow[dd] & Y \arrow[d] & y \arrow[l] \arrow[dd] \\
 & V_1' \arrow[d] & \\
U \arrow[r, "j"] & X' & z \arrow[l]
\end{tikzcd}$$

Montrons que $\mathrm{Hom}(\mathcal{F}|_Y, \mathcal{F}'|_Y)$ est le groupe décrit dans l'énoncé. Par recollement,

$$\mathrm{Hom}(\mathcal{F}|_Y, \mathcal{F}'|_Y) = \{(\alpha, \beta) \in \mathrm{Hom}(\mathcal{F}|_{Y_U}, \mathcal{F}'|_{Y_U}) \times \mathrm{Hom}_\Lambda(\mathcal{F}_z, \mathcal{F}'_z) \mid \alpha\phi_{\mathcal{F}} = \phi_{\mathcal{F}'}\beta\}.$$

Il suffit désormais de montrer que $\mathrm{Hom}(\mathcal{F}|_{Y_U}, \mathcal{F}'|_{Y_U})$ est égal à $\mathrm{Hom}_\Lambda(F, F')^I$. C'est le groupe des sections sur Y_U du faisceau lisse $\underline{\mathrm{Hom}}(\mathscr{L}, \mathscr{L}')$ sur U de fibre $\mathrm{Hom}(F, F')$. Par conséquent, il est canoniquement isomorphe à $\mathrm{Hom}(F, F')^{\pi_1(Y_U)}$. Or l'action de $\pi_1(Y_U)$ sur $\mathrm{Hom}(F, F')$ se factorise de la façon suivante :

$$\begin{tikzcd}
\pi_1(Y_U) \arrow[r] \arrow[dr] & \pi_1(V_1) \arrow[r] \arrow[d] & \pi_1(U) \arrow[d] \arrow[dr] & \\
 & I \arrow[r] & G \arrow[r] & \mathrm{Aut}_\Lambda(\mathrm{Hom}(F, F'))
\end{tikzcd}$$

Notons J l'image de $\pi_1(Y_U)$ dans I. Le morphisme $Y_U \to V_1$ se factorise par le sous-revêtement W de $V \to V_1$ défini par $\mathrm{Aut}(V|W) = J$; par conséquent, $Y \to V_1'$ se factorise encore par la normalisation W' de V_1' dans W. Comme $k(Y)/k(X)$ est galoisienne, $Y \to X$ se factorise alors par la clôture galoisienne de $W' \to X$, qui ne saurait être étale en aucun point au-dessus de z, sauf si $W' = V_1'$, c'est-à-dire $J = I$. L'étalitude de $Y \to X$ entraîne donc la surjectivité de $\pi_1(Y_U) \to I$. Par conséquent,

$$\mathrm{Hom}_\Lambda(F, F')^{\pi_1(Y_U)} = \mathrm{Hom}_\Lambda(F, F')^I.$$

□

Enfin, le morphisme de recollement $\underline{\mathrm{Hom}}(\mathcal{F}, \mathcal{F}')_z \to (j_\star \underline{\mathrm{Hom}}(\mathscr{L}, \mathcal{F}'_U))_z$ se calcule en considérant les sections sur chaque $Y \to X$; c'est simplement la projection

$$\underline{\mathrm{Hom}}(\mathcal{F}, \mathcal{F}')_z \subseteq \mathrm{Hom}_\Lambda(F, F')^I \times \mathrm{Hom}_\Lambda(\mathcal{F}_z, \mathcal{F}'_z) \to \mathrm{Hom}_\Lambda(F, F')^{I_z}$$

où I_z est le groupe d'inertie d'un point de V' au-dessus de Z.

III.4.4 Tiré en arrière

Soit $f\colon Y \to X$ un morphisme de courbes intègres lisses sur k. Comme vu en III.2, f se factorise en $Y \xrightarrow{s} Y' \xrightarrow{\nu} X$, où s est une immersion ouverte et ν est un morphisme fini localement libre. Il suffit donc de traiter séparément le cas où f est une immersion ouverte, et le cas où f est fini.

Soit $\mathcal{F}$ un faisceau constructible sur X, défini par un ouvert de lissité $j\colon U \to X$, le fermé réduit complémentaire $i\colon Z \to X$, le faisceau lisse $\mathscr{L} = j^\star\mathcal{F}$ sur U, le faisceau $\mathcal{F}_Z = i^\star\mathcal{F}$ sur Z et le morphisme de recollement $\phi\colon i_\star\mathcal{F}_Z \to i_\star i^\star j_\star\mathscr{L}$.

Le cas d'une immersion ouverte Supposons que $f\colon Y \to X$ soit une immersion ouverte. Notons $V = U \cap Y, W = Z \cap Y$. Alors $f^\star\mathcal{F}$ est clairement lisse sur V, les fibres de $f^\star\mathcal{F}$ en les points de W sont égales à celles de $\mathcal{F}$ en leurs images dans Z, et le morphisme de recollement de $f^\star\mathcal{F}$ relativement à V, W est simplement la restriction à W de celui de $\mathcal{F}$.

Le cas d'un morphisme fini Supposons que $f\colon Y \to X$ soit fini. Considérons le diagramme suivant, dont les carrés sont cartésiens.

$$\begin{tikzcd} V \arrow[r, "j'"] \arrow[d, "p"'] & Y \arrow[d, "f"] & W \arrow[l, "i'"'] \arrow[d, "q"] \\ U \arrow[r, "j"] & X & Z \arrow[l, "i"'] \end{tikzcd}$$

Le faisceau $j'^\star f^\star\mathcal{F} = p^\star j^\star\mathcal{F}$ est lisse sur V. De plus, la commutativité du carré de droite permet de calculer simplement les fibres de $f^\star\mathcal{F}$ en les points de W. Déterminons le morphisme d'adjonction $i'^\star f^\star\mathcal{F} \to i'^\star j'_\star j'^\star f^\star\mathcal{F} = i'^\star j'_\star p^\star\mathscr{L}$. La flèche $i^\star\mathcal{F} \to i^\star j_\star j^\star\mathcal{F}$ est connue ; en lui appliquant $q^\star$, on obtient $i'^\star f^\star\mathcal{F} \to i'^\star f^\star j_\star j^\star\mathcal{F}$. Reste à calculer la flèche de comparaison $f^\star j_\star j^\star\mathcal{F} \to j'_\star j'^\star f^\star\mathcal{F} = j'_\star p^\star j^\star\mathcal{F}$. Notons que $f^\star j_\star j^\star\mathcal{F}$ est représenté par un schéma étale sur Y qui se calcule explicitement par une normalisation puis un produit fibré. Il en est de même du morphisme de schémas qui représente la flèche d'adjonction $j^\star\mathcal{F} \to p_\star p^\star j^\star\mathcal{F}$, ainsi que celui représentant $f^\star j_\star j^\star\mathcal{F} \to f^\star j_\star p_\star p^\star j^\star\mathcal{F}$. Remarquons que le faisceau de droite est canoniquement isomorphe à $f^\star f_\star j'_\star p^\star j^\star\mathcal{F}$; il suffit maintenant de lui appliquer l'unité d'adjonction $f^\star f_\star \to \mathrm{id}$ (pour sa description, voir l'annexe B.5) pour obtenir la composée $f^\star j_\star j^\star\mathcal{F} \to j'_\star p^\star j^\star\mathcal{F}$. En résumé, il s'agit de calculer les fibres en les points de W de la composée :

$$f^\star\mathcal{F} \to f^\star j_\star j^\star\mathcal{F} \to f^\star j_\star p_\star p^\star j^\star\mathcal{F} \xrightarrow{\sim} f^\star f_\star j'_\star p^\star j^\star\mathcal{F} \to j'_\star p^\star j^\star\mathcal{F} \xrightarrow{\sim} j'_\star j'^\star f^\star\mathcal{F}.$$

Remarque 3.4.3. Les représentations (!) et ($\star$) sont conceptuellement bien mieux adaptées à cette tâche, car le foncteur $f^\star$, qui se calcule sur les schémas par un simple produit fibré, commute aux noyaux et conoyaux. L'avantage de la méthode décrite ci-dessus est de ne pas avoir recours au calcul possiblement coûteux de l'une de ces deux représentations.

III.4.5 Poussé en avant

Soit $f\colon Y \to X$ un morphisme de courbes intègres lisses sur k. Nous allons montrer comment calculer les foncteurs $\mathrm{R}^i f_\star$, $i \geqslant 0$. La notation $f_\star$ seule désignera toujours le foncteur non dérivé. Lorsque f est fini, l'exactitude de $f_\star$ assure que $\mathrm{R}^i f_\star = 0$ dès que $i \geqslant 0$.

Le cas d'une immersion ouverte Soit $j\colon U \to X$ une immersion ouverte de courbes intègres lisses sur k. Soit Z le fermé réduit complémentaire de U dans X. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur U, lisse sur un ouvert V de U, de fibre générique géométrique M. Comme $j^\star j_\star\mathcal{F} \to \mathcal{F}$ est un isomorphisme, le faisceau $j_\star\mathcal{F}$ est encore lisse sur V. De plus, pour tout point géométrique z de Z, la proposition 1.5.11 assure que

$$\begin{aligned} (\mathrm{R}j_\star\mathcal{F})_z &= \mathrm{R}\Gamma(U \times_X X_{(\bar{z})}, \mathcal{F}) \\ &= \mathrm{R}\Gamma(V \times_X X_{(\bar{z})}, \mathcal{F}) \\ &= \mathrm{R}\Gamma(\eta_z, \mathcal{F}) \\ &= \mathrm{R}\Gamma(I_z, M) \end{aligned}$$

où η_z est le point générique de l'anneau local strictement hensélien $X_{\bar{z}} = \operatorname{Spec} \mathcal{O}^{sh}_{X,z}$, le point $\bar{\eta}_z$ est un point générique géométrique de $X_{(\bar{z})}$ et $I = \operatorname{Gal}(\bar{\eta}_z|\eta_z)$. Le morphisme de recollement $j_\star\mathcal{F} \to j_\star j^\star j_\star\mathcal{F}$ est un isomorphisme. D'autre part,

$$j^\star \mathrm{R}^1 j_\star = \mathrm{R}^1(j^\star j_\star) = 0$$

puisque $j^\star j_\star$ est un isomorphisme. Le faisceau $\mathrm{R}^1 j_\star\mathcal{F}$ est donc supporté sur Z, et $j_\star j^\star \mathrm{R}^1 j_\star\mathcal{F} = 0$. Comme la cohomologie de $\mathrm{R}\Gamma(I, M)$ est concentrée en degrés 0 et 1, le foncteur $\mathrm{R}^i j_\star$ est nul pour tout $i \geqslant 2$.

Le cas d'un morphisme fini Soit $f\colon Y \to X$ un morphisme fini de courbes intègres lisses. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur Y défini par recollement relativement à $V \xrightarrow{j} Y \xleftarrow{i} W$, où V est un ouvert de Y tel que $\mathcal{F}|_V$ soit lisse, trivialisé par un revêtement étale $T \to V$. Notons $\phi\colon i^\star\mathcal{F} \to i^\star j_\star j^\star\mathcal{F}$ le morphisme de recollement. Décrivons par recollement le faisceau $f_\star\mathcal{F}$, qui est encore constructible d'après [SGA4$_3$, IX, Prop. 2.14.(i)]. Quitte à remplacer f par sa complétion projective lisse et les faisceaux en question par leur prolongement par zéro, nous pouvons supposer X et Y projectives. Si la caractéristique de k est nulle, le morphisme f est génériquement étale. Si la caractéristique de k est $p > 0$, le morphisme f se factorise en composée d'une succession de Frobenius relatifs suivi d'un morphisme génériquement étale [Stacks, 0CD2]. Il suffit donc de traiter séparément les cas du Frobenius et d'un morphisme génériquement étale.

Le morphisme de Frobenius relatif $\phi\colon Y \to Y^{(p)}$ étant un homéomorphisme universel, le théorème 1.5.5 assure que le foncteur $\phi^\star$, dont $\phi_\star$ est l'adjoint à droite, est une équivalence de catégories. Voici comment la donnée de recollement de $\phi_\star\mathcal{F}$ se déduit de celle de $\mathcal{F}$. Le faisceau $\phi_\star\mathcal{F}$ est lisse sur l'ouvert $V^{(p)}$ de $Y^{(p)}$. Son fermé complémentaire réduit Z a autant de points fermés que W, et étant donné un point fermé w de W, la fibre du faisceau $\phi_\star\mathcal{F}$ en $\phi(w)$ est $\mathcal{F}_w$ car ϕ est radiciel. La description de $\phi_\star\mathcal{F}$ sur X est donc la suivante : il est lisse sur l'ouvert $V^{(p)}$, de même fibre générique géométrique que $\mathcal{F}$ et trivialisé par $T^{(p)}$. Ses fibres sur Z sont les mêmes que sur W. En notant j' l'inclusion de U dans X, la finitude de ϕ assure que $j'_\star j'^\star\phi_\star\mathcal{F} = \phi_\star j'_\star j'^\star\mathcal{F}$ a les mêmes fibres que $j_\star j^\star\mathcal{F}$, et le morphisme de recollement de $\phi_\star\mathcal{F}$ est le même que celui de $\mathcal{F}$.

Supposons désormais f génériquement étale. Soit Z un fermé réduit de X contenant $f(W)$ ainsi que tous les points de X au-dessus desquels f n'est pas étale. Soit U l'ouvert complémentaire. Considérons le diagramme suivant, dont les deux carrés sont cartésiens :

$$\begin{tikzcd} V' \arrow[r, "j'"] \arrow[d, "p"'] & Y \arrow[d, "f"] & W' \arrow[l, "i'"'] \arrow[d, "q"] \\ U \arrow[r, "j"] & X & Z \arrow[l, "i"'] \end{tikzcd}$$

Comme $V' \subset V$, le faisceau $j'^\star\mathcal{F}$ est lisse ; le morphisme p étant fini étale, $p_\star j'^\star\mathcal{F}$ est lisse sur U. Il est représenté par le U-schéma fini étale $R_{V'\to U}(j'^\star\mathcal{F})$. Par finitude de f, les morphismes de changement de base des deux carrés de ce diagramme sont des isomorphismes [Fu15, Corollary 5.3.9]. Par conséquent, le faisceau $i^\star f_\star\mathcal{F}$ est isomorphe à $q_\star i'^\star\mathcal{F}$, qui se calcule explicitement comme un ensemble de Λ-modules indexé par les points de Z. Le morphisme $\phi\colon i'^\star\mathcal{F} \to i'^\star j'_\star j'^\star\mathcal{F}$ est connu. Alors comme $j_\star j^\star f_\star\mathcal{F} = j_\star p_\star j'^\star\mathcal{F} = f_\star j'_\star j'^\star\mathcal{F}$, la flèche $q_\star\phi$ est un morphisme $i^\star f_\star\mathcal{F} \to i^\star j_\star j^\star f_\star\mathcal{F}$. Il s'agit du morphisme d'adjonction $f_\star\mathcal{F} \to j_\star f^\star f_\star\mathcal{F}$, défini pour tout X-schéma étale T par le morphisme $\mathcal{F}(T \times_X Y) \to \mathcal{F}(T \times_X V')$ obtenu par fonctorialité à partir de l'inclusion $T \times_X V' \to T \times_X Y$.

Remarque 3.4.4. Au moins pour le cas d'un morphisme fini, les représentations ($\star$) et (!) se prêtent conceptuellement mieux au calcul de $f_\star$, qui s'effectue alors par restriction de Weil.

III.5 Un exemple détaillé

Considérons sous une perspective différente l'exemple de la mise au carré sur la droite affine. Dans cet exemple, $\Lambda = \mathbb{Z}/2\mathbb{Z}$ et $k = \bar{\mathbb{Q}}$. Considérons $X = \mathbb{A}^1_k = \operatorname{Spec} k[x]$ et $Y = \operatorname{Spec} k[x,y]/(x-y^2)$. Notons $A = k[x], B = k[x,y]/(x-y^2)$. Soit $f\colon Y \to X$ le morphisme défini par $x \mapsto x$. Remarquons que $B = A \cdot 1 \oplus A \cdot y$: le morphisme f est fini et libre. Il est étale au-dessus de $U = \mathbb{G}_m = \operatorname{Spec} k[x^{\pm 1}]$, et ramifié au-dessus de 0 où la fibre est $k[y]/(y^2)$. Notons $U' = Y|_{\mathbb{G}_m}$.
Considérons le faisceau constant $\mathcal{F} = \Lambda \simeq \mu_2$ sur Y, représenté par le Y-schéma $F := \operatorname{Spec} B[t]/(t^2-1)$, et calculons le faisceau constructible $f_\star\mathcal{F}$.

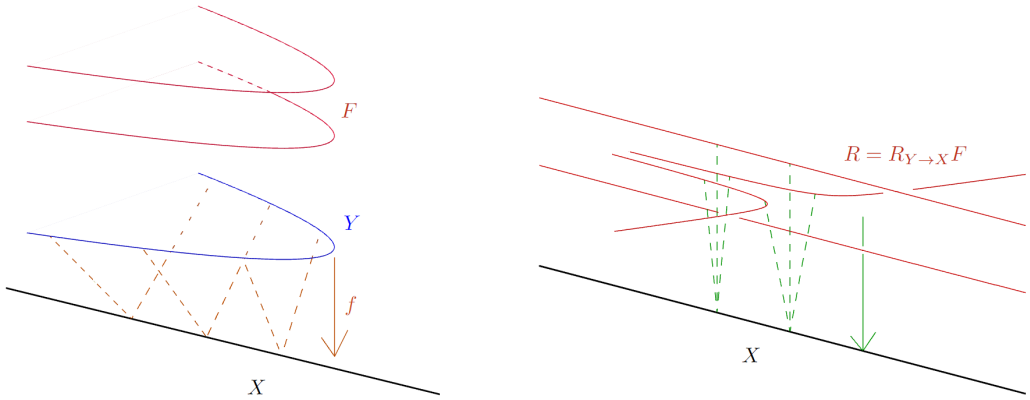


FIGURE III.2 – Le Y-schéma F et sa restriction de Weil

Calcul de $f_\star\mathcal{F}$ Le faisceau $f_\star\mathcal{F}$ est représenté par la restriction de Weil $R := R_{Y\to X}F$. En notant $\phi = t^2 - 1 \in A[t]$,

$$\phi(\alpha \cdot 1 + \beta \cdot y) = (\alpha^2 + \beta^2 x - 1) \cdot 1 + 2\alpha\beta \cdot y.$$

Par conséquent,

$$R = \operatorname{Spec} A[\alpha,\beta]/(\alpha^2 + \beta^2 x - 1, \alpha\beta).$$

Il est prévisible que $R \to X$ soit étale, mais pas fini car f est ramifié. L'étalitude se vérifie rapidement : le déterminant jacobien de la présentation ci-dessus est égal à $\alpha^2 - x\beta^2$, qui vaut encore $2\alpha^2 - 1 = (1 - 2x\beta^2)^{-1}$ dans $\mathrm{H}^0(R, \mathcal{O}_R)$. Il n'est effectivement pas fini puisque β n'est pas racine d'un polynôme unitaire à coefficients dans $k[x]$. Cependant, R doit être fini au-dessus de U (où f est étale), ce qui est le cas puisque $\alpha^3 = \alpha$ et $\beta^3 = x^{-1}\beta$. Calculons la loi de groupe sur R. La loi de groupe sur F est donnée par

$$\begin{array}{ccc} B[t]/(t^2-1) & \longrightarrow & B[a,b]/(a^2-1, b^2-1) \\ t & \longmapsto & ab. \end{array}$$

En écrivant $t = \alpha + y\beta$, $a = a_1 + ya_2$, $b = b_1 + yb_2$, la loi de groupe sur R est alors donnée par

$$\begin{array}{ccc} A[\alpha,\beta]/(\alpha^2 + x\beta^2 - 1, \alpha\beta) & \to & A[a_1,b_1,a_2,b_2]/(a_1^2 + xa_2^2 - 1, a_1a_2, b_1^2 + xb_2^2 - 1, b_1b_2) \\ \alpha & \mapsto & a_1a_2 + xb_1b_2 \\ \beta & \mapsto & a_1b_2 + b_1a_2. \end{array}$$

Calcul de $(f_\star\mathcal{F})_0$ La fibre de R en $x=0$ est $k[\alpha,\beta]/(\alpha^2-1,\beta)$ et contient deux points. La fibre générique géométrique de $R\to X$ est $\operatorname{Spec}\overline{k(x)}[\alpha,\beta]/(\alpha^2+x\beta^2-1,\alpha\beta)=\{(0,\pm\sqrt{x^{-1}}),(\pm1,0)\}$. La loi de groupe sur cette fibre se déduit des formules déterminées ci-dessus ; par exemple, $(0,\sqrt{x^{-1}})\cdot(-1,0)=(0\cdot(-1)+x\sqrt{x^{-1}}\cdot 0, 0\cdot 0+\sqrt{x^{-1}}\cdot(-1))=(0,-\sqrt{x^{-1}})$. C'est un groupe isomorphe à Λ^2, d'élément neutre $(1,0)$.

Calcul de $j_\star j^\star f_\star\mathcal{F}$ Notons $j\colon U\to X$. Le faisceau $j_\star j^\star R$ est représenté par le lieu étale sur $\mathbb{A}^1$ du normalisé de $\mathbb{A}^1$ dans $R'\coloneqq R|_U=\operatorname{Spec}k[x^{\pm1},\alpha,\beta]/(\alpha^2+\beta^2x-1,\alpha\beta)$. Il est temps de s'intéresser à la structure de R'. Le morphisme $R'\to U$ admet au moins deux sections (les sections globales de $f_\star\mathcal{F}$, correspondant à $\beta=0$ et $\alpha=\pm1$), dont les images sont des composantes connexes de R' isomorphes à U. Un calcul rapide donne $R'=U\sqcup U\sqcup\operatorname{Spec}k[x^{\pm1},\beta]/(x\beta^2-1)$. D'une part, la normalisation de $\mathbb{A}^1$ dans $\mathbb{G}_m$ est $\mathbb{A}^1$. Calculons d'autre part la clôture intégrale de $k[x]$ dans $S=k[x^{\pm1},\beta]/(x\beta^2-1)$. Le couple $(1,x\beta)$ est une $k(x)$-base de $\operatorname{Frac}S$. Le sous-anneau $k[x,x\beta]\simeq k[x,s]/(s^2-x)$ de S est entier sur $k[x]$, et son corps des fractions est $\operatorname{Frac}S$; comme il est normal, c'est la clôture intégrale de $k[x]$ dans S. Par conséquent, $j_\star R'$ est le lieu étale de $\mathbb{A}^1\sqcup\mathbb{A}^1\sqcup\operatorname{Spec}k[x,s]/(s^2-x)\to\mathbb{A}^1$, c'est-à-dire $\mathbb{A}^1\sqcup\mathbb{A}^1\sqcup\operatorname{Spec}k[x^{\pm1},s]/(s^2-x)$. La fibre en $x=0$ de $j_\star R'$ est donc $\operatorname{Spec}(k[x]\times k[x])$: elle contient deux k-points. La flèche de recollement $R_0\to(j_\star R')_0$ est, comme précisé plus haut, l'identité.

Remarques sur R' et $(j_\star R')_0$ Nous avons vu que le faisceau lisse $j^\star f_\star\Lambda$ sur U était représenté par $R'=U\sqcup U\sqcup V$ où $V=\operatorname{Spec}k[x^{\pm1},\beta]/(x\beta^2-1)$. Le morphisme $V\to U$ est fini étale, et galoisien car de degré 2. Par conséquent, $V\times_U V=V\sqcup V$, et $R'\times_U V=\sqcup^4 V$. Le revêtement $V\to U$ trivialise donc $j^\star f_\star\Lambda$, et le groupe $G=\operatorname{Aut}(V|U)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$. Le morphisme non trivial dans G est $\sigma\colon\beta\mapsto-\beta$. Considérons les complétions projectives lisses $\bar U=\mathbb{P}^1=\operatorname{Proj}k[X,Y]$ et $\bar V=\operatorname{Proj}k[X,B,Y]/(XB^2-Y)$ de U et V. Au-dessus du point $0=(0:1)$ de $\mathbb{P}^1$ se trouve uniquement $(0:1:0)\in\bar V$, qui est donc invariant sous σ. Par conséquent, l'action sur $(j^\star f_\star\Lambda)(V)=\operatorname{Hom}_U(V,U\sqcup U\sqcup V)=\{V\to U^{(1)},V\to U^{(2)},\mathrm{id}_V,\sigma\}$ du groupe d'inertie I_0 est l'action (par précomposition) de $G=\{\mathrm{id}_V,\sigma\}$. L'élément $\sigma\in G$ agit trivialement sur les deux morphismes $V\to U$, mais échange id_V et σ. Par conséquent, $R'(V)^{I_0}=\{V\to U^{(1)},V\to U^{(2)}\}\simeq\mathbb{Z}/2\mathbb{Z}$ est bien isomorphe au groupe $(j_\star R')_0$ trouvé précédemment.

III.6 Faisceaux constructibles sur les courbes nodales

Soit X une courbe intègre nodale sur k de corps des fonctions K. Soient $j\colon U\to X$ et $i\colon Z\to X$ les immersions d'un ouvert et d'un fermé réduit complémentaires. Afin de décrire par recollement un faisceau constructible sur X lisse sur U, il est nécessaire de savoir décrire le faisceau $j_\star j^\star\mathcal{F}$. Notons $\mathscr{L}$ le faisceau $j^\star\mathcal{F}$, et F sa fibre générique. Soit $\bar z$ un point géométrique de Z. Notons $K_{\bar z}$ le corps des fractions de $\mathcal{O}_{X,\bar z}$, et $I_{\bar z}$ le groupe d'inertie associé à un choix de plongement $K^{\mathrm{sep}}\to K_{\bar z}^{\mathrm{sep}}$. Notons V l'intersection de U avec le lieu non singulier de X. Calculons $(j_\star\mathscr{L})_{\bar z}$.

Si $\bar z$ est non singulier Rappelons que $(j_\star\mathscr{L})_{\bar z}=\mathrm{H}^0(U\times_X X_{\bar z},\mathscr{L})$. Or $U\times_X X_{\bar z}=V\times_X X_{\bar z}$, qui est réduit au point générique de $X_{\bar z}$, dont le groupe fondamental est $\operatorname{Gal}(K_{\bar z}^{\mathrm{sep}}|K^{\mathrm{sep}})=I_{\bar z}$. Par conséquent,

$$(j_\star\mathscr{L})_{\bar z}=\mathrm{H}^0(I_{\bar z},F).$$

Si $\bar z$ est singulier Notons $\tilde X$ et $\widetilde{X_{\bar z}}$ les normalisations respectives de X et $X_{\bar z}=\operatorname{Spec}\mathcal{O}_{x,\bar z}$. Le schéma $X_{\bar z}$ est constitué de trois points : un point fermé, et deux idéaux premiers minimaux p,q correspondant

aux branches de X en $\bar{z}$ [Stacks, 06DT]. D'après [Stacks, 0CBM], $\widetilde{X_{\bar{z}}} = \tilde{X} \times_X X_{\bar{z}}$. Par conséquent, en notant P, Q les antécédents de $\bar{z}$ dans $\tilde{X}$,

$$\widetilde{X_{\bar{z}}} = \tilde{X}_P \sqcup \tilde{X}_Q.$$

Les schémas $\tilde{X}_P$ et $\tilde{X}_Q$ sont des traits dont les points fermés ont pour image celui de $X_{\bar{z}}$, et les points génériques ont pour images les points p, q de $X_{\bar{z}}$. Notons η_P, η_Q les points génériques respectifs de $\tilde{X}_P, \tilde{X}_Q$. En particulier, il y a des isomorphismes de schémas

$$U \times_X X_{\bar{z}} = \{p, q\}$$

et

$$U \times_X X_{\bar{z}} \times_{X_{\bar{z}}} \widetilde{X_{\bar{z}}} = \eta_P \sqcup \eta_Q \xrightarrow{\sim} \{p, q\}.$$

Par conséquent,

$$\begin{aligned} (j_\star \mathscr{L})_{\bar{z}} &= \mathrm{H}^0(\{p, q\}, \mathscr{L}) \\ &= \mathrm{H}^0(\eta_P, \mathscr{L}) \times \mathrm{H}^0(\eta_Q, \mathscr{L}) \\ &= \mathrm{H}^0(I_P, F) \times \mathrm{H}^0(I_Q, F). \end{aligned}$$

Représentation ($\sqcup$) **pour les courbes nodales** Voici comment représenter par recollement un faisceau constructible $\mathcal{F}$ sur une courbe nodale X sur k. La courbe X est représentée par sa normalisée $\tilde{X}$ avec des couples de points marqués. L'ouvert de lissité U – dont nous supposons, quitte à ce qu'il ne soit pas maximal, qu'il ne contient pas les points nodaux – est défini par sa normalisée $j\colon \tilde{U} \to \tilde{X}$. De même, le fermé Z est donné par $\tilde{Z} \coloneqq Z \times_X \tilde{X} \to \tilde{X}$. Le faisceau $\mathcal{F}$ est défini par :

1. un faisceau lisse $\mathscr{L}$ sur $\tilde{U}$ de fibre F, représenté comme dans la section III.1.3 à l'aide d'un revêtement trivialisant $\tilde{Y} \to \tilde{X}$;
2. des fibres M_z en les points de $\tilde{Z}$ – une seule fibre $M_{(x,y)}$ par couple (x, y) de points marqués ;
3. des morphismes $M_z \to F^{I_z}$ pour z non marqué, et $M_{(x,y)} \to F^{I_x} \times F^{I_y}$ pour tout couple de points marqués (x, y), où I_z, I_x, I_y sont des sous-groupes du groupe de X-automorphismes d'une composante connexe de $\tilde{Y}$, déterminés par le choix d'antécédents quelconques de z, x, y dans une même composante connexe de $\tilde{Y}$.

III.7 Constructions sur les surfaces

Voyons brièvement comment représenter les faisceaux constructibles en dimension supérieure. Afin de simplifier l'exposition, considérons le cas des surfaces, où apparaissent déjà quelques complications. Soit X une surface lisse sur k. Soit $\mathcal{F}$ un faisceau constructible sur X. Il existe un ouvert $j\colon U \to X$ sur lequel $\mathcal{F}$ est lisse ; soit $i\colon Z \to X$ le fermé réduit complémentaire.

La représentation ($\sqcup$) Les faisceaux $i^\star \mathcal{F}$ et $i^\star j_\star j^\star \mathcal{F}$ sont constructibles sur Z, qui est une courbe : nous savons représenter ces faisceaux ainsi que le morphisme de recollement entre eux. Cet argument s'adapte récursivement au cas où X est de dimension supérieure.

La représentation (!) La représentation comme conoyau s'adapte immédiatement en dimension quelconque : nous avons décrit la représentabilité de $f_! \Lambda$ pour tout morphisme étale f entre k-variétés.

La représentation ($\star$) Il s'agit ici de décrire des morphismes de faisceaux $\alpha\colon p_\star M \to p'_\star N$, où $p\colon Y \to X$ et $p'\colon Y' \to X$ sont des morphismes finis et M, N sont des Λ-modules de type fini. La difficulté est le cas (inexistant si X est une courbe) où $\dim Y = \dim Y' = 1$: le morphisme α peut être non nul, par exemple si $Y = Y'$, et les faisceaux $p_\star\Lambda$ et $q_\star\Lambda$ ne sont pas représentables par des schémas sur X.

CHAPITRE IV

Calculabilité de la cohomologie et algorithmes existants

Soit X un schéma de type fini sur un corps algébriquement clos k. Soit n un entier inversible dans k. Les groupes $\mathrm{H}^i(X, \mathbb{Z}/n\mathbb{Z})$ sont des $\mathbb{Z}/n\mathbb{Z}$-modules de type fini, dont la question du calcul effectif a été extensivement étudiée. D'abord prouvée en caractéristique nulle par Poonen, Testa et van Luijk [PTv15, Th. 7.9], la calculabilité de ces groupes a été démontrée en 2015 par Madore et Orgogozo [MO15, Th. 0.1]. L'algorithme décrit dans leur article est résumé dans la section IV.1 ; nous y montrerons que sa complexité est primitivement récursive. Les seuls algorithmes pour lesquels des bornes de complexité sont connues concernent le cas particulier des courbes projectives lisses. Dans ce cas, seul le groupe $\mathrm{H}^1(X, \mathbb{Z}/n\mathbb{Z})$, qui s'identifie d'après le théorème 2.4.2 au groupe de n-torsion de la jacobienne de X, présente un intérêt. La meilleure complexité pour le calcul de ce groupe est atteinte par l'algorithme probabiliste de Couveignes [Cou09], décrit dans la section IV.2. Cependant, cet algorithme se cantonne au cas des courbes définies sur un corps fini, et nécessite d'avoir calculé au préalable la fonction zêta de la courbe en question. L'algorithme de Huang et Ierardi [HI98], pensé pour le comptage de points des courbes sur les corps finis, s'adapte quant à lui à tous les corps calculables munis d'un algorithme de factorisation. Une légère modification, détaillée dans la section IV.3, permet même de l'adapter au calcul de la division par n dans $\mathrm{Pic}^0(X)$. Enfin, plus récemment, Jin a proposé une méthode de calcul de la cohomologie des faisceaux lisses sur les courbes lisses, ainsi que des bornes de complexité explicites [Jin20]. Son algorithme est expliqué dans la section IV.4.

IV.1 Calculabilité : l'algorithme de Madore et Orgogozo

IV.1.1 Représentation des objets et résumé de l'algorithme

Soient k un corps algébriquement clos et ℓ un nombre premier inversible dans k. Notons Λ l'anneau $\mathbb{Z}/\ell\mathbb{Z}$. Les schémas de type fini sur k sont représentés par recollement de schémas affines comme décrit dans l'annexe B.1.1.

Théorème 4.1.1. [MO15, Th. 0.1] Il existe un algorithme calculant les groupes de cohomologie $\mathrm{H}^i(X, \Lambda)$ d'un schéma X de type fini sur k, ainsi que l'application $\mathrm{H}^i(X, \Lambda) \to \mathrm{H}^i(Y, \Lambda)$ déduite par fonctorialité d'un morphisme $Y \to X$.

Soit X un schéma de type fini sur k. Notons d la dimension de X. L'algorithme procède de la façon suivante. Il commence par calculer les r premiers étages d'un hyperrecouvrement $X_\bullet \to X$ dont les composantes sont des $K(\pi, 1)$ pro-ℓ et tel que la cohomologie de X soit celle du topos total $\operatorname{Tot} X_\bullet$ associé à l'hyperrecouvrement (voir début de la section IV.1.4). Dès que $r > d$, le morphisme canonique

$$\mathrm{R}\Gamma(\operatorname{Tot} X_{\bullet\leqslant r}, \Lambda) \to \mathrm{R}\Gamma(\operatorname{Tot} X_\bullet, \Lambda)$$

est un quasi-isomorphisme. La cohomologie de $\operatorname{Tot} X_{\bullet\leqslant r}$ est calculée à l'aide d'approximations $X^{(\lambda)}_{\bullet\leqslant r}$ de $X_{\bullet\leqslant r}$, constituées de ℓ-revêtements galoisiens des composantes connexes de $X_{\bullet\leqslant r}$, vérifiant

$$\mathrm{H}^i(\operatorname{Tot} X_{\bullet\leqslant r}, \Lambda) = \operatorname{colim}_\lambda \mathrm{H}^i(\operatorname{Tot} X^{(\lambda)}_{\bullet\leqslant r}, \Lambda).$$

La cohomologie de $\operatorname{Tot} X^{(\lambda)}_{\bullet\leqslant r}$ est déterminée explicitement à partir d'une résolution de Godement tronquée du faisceau Λ. Il reste à déterminer des entiers α, β tels que

$$\mathrm{H}^i(X, \Lambda) = \operatorname{im}(\mathrm{H}^i(\operatorname{Tot} X^{(\alpha)}_{\bullet\leqslant r}, \Lambda) \to \mathrm{H}^i(\operatorname{Tot} X^{(\beta)}_{\bullet\leqslant r}, \Lambda)).$$

La cohomologie de $\operatorname{Tot} X^{(\lambda)}_{\bullet\leqslant r}$ est également l'aboutissement d'une suite spectrale dont les coefficients de la première page sont les $\mathrm{H}^j(X^{(\lambda)}_i, \Lambda)$. Chaque composante connexe de X_i est un $K(\pi, 1)$ pro-ℓ, et les $X^{(\lambda)}_i$ correspondent à des quotients $\pi^{(\lambda)}$ du pro-ℓ groupe fondamental π de cette composante ; il y a pour tout entier naturel j un isomorphisme canonique

$$\mathrm{H}^j(\pi, \Lambda) = \operatorname{colim}_\lambda \mathrm{H}^j(\pi^{(\lambda)}, \Lambda).$$

Un résultat sur les systèmes inductifs de suites spectrales permet de déterminer des entiers a, b tels que

$$\mathrm{H}^j(\pi, \Lambda) = \operatorname{im}(\mathrm{H}^j(\pi^{(a)}, \Lambda) \to \mathrm{H}^j(\pi^{(b)}, \Lambda))$$

et par conséquent les entiers α, β cherchés.

IV.1.2 Fibrations en courbes élémentaires

Définition 4.1.2. Soit $f\colon X \to S$ un morphisme de schémas. Il est appelé courbe élémentaire sur S s'il peut être plongé dans un diagramme commutatif

$$\begin{tikzcd} X \arrow[r, "j"] \arrow[dr, "f"'] & Y \arrow[d, "\bar{f}"] & D \arrow[l, "i"'] \arrow[dl, "g"] \\ & S & \end{tikzcd}$$

où $X = Y - D$, le morphisme $\bar{f}$ est une courbe relative projective lisse à fibres géométriquement connexes, et g est un revêtement étale à fibres non vides. Une courbe ℓ-élémentaire est une courbe élémentaire $f\colon X \to S$ telle que le faisceau $\mathrm{R}^1 f_\star \mathbb{Z}/\ell\mathbb{Z}$ soit ℓ-monodromique (voir définition 1.4.6). Un morphisme de schémas est appelé polycourbe (ℓ-)élémentaire s'il admet une factorisation en courbes (ℓ-)élémentaires.

Le résultat suivant, dû à M. Artin, affirme que tout schéma lisse sur un corps algébriquement clos est, localement pour la topologie de Zariski, une polycourbe élémentaire.

Proposition 4.1.3. [SGA4$_3$, XI, Prop. 3.3] Soit X un schéma lisse sur un corps algébriquement clos k. Soit $x \in X$ un k-point. Il existe un ouvert U de X contenant x tel que $U \to \operatorname{Spec} k$ soit une polycourbe élémentaire.

Afin d'appliquer au schéma X la théorie des pro-ℓ-groupes, il suffit de montrer que l'on peut supposer, après changement de base étale, que l'ouvert U de la proposition est une polycourbe ℓ-élémentaire. Ceci se montre de la façon suivante : si $U \to k$ se factorise par une courbe élémentaire $g\colon U \to V$, et si V' désigne un revêtement étale de V trivialisant le faisceau $\mathrm{R}^1 g_\star \Lambda$ (qui est lisse par [SGA1, XIII, Cor. 2.9]), le changement de base $U \times_V V' \to V'$ est une courbe ℓ-élémentaire. Une récurrence sur la dimension permet de conclure. Voici comment construire V' : soit η le point générique de V. Le $\mathrm{Gal}(\bar{\eta}|\eta)$-module $\mathrm{H}^1(U_{\bar{\eta}}, \Lambda)$ se calcule comme un groupe de cohomologie d'une courbe (par exemple avec l'un des algorithmes des sections IV.3 et IV.4) ; si $\eta' \to \eta$ est une extension finie séparable par laquelle se factorise l'action de $\mathrm{Gal}(\bar{\eta}|\eta)$, un ouvert étale sur V de la normalisation de V dans η' convient pour V'.

Enfin, les polycourbes ℓ-élémentaires sur k sont des $K(\pi, 1)$ pro-ℓ. En effet, si $f\colon Y \to X$ est une courbe ℓ-élémentaire et $\bar{\eta}$ est un point générique géométrique de X, il y a une suite exacte

$$1 \to \pi_1^{\mathrm{pro}-\ell}(Y_{\bar{\eta}}) \to \pi_1^{\mathrm{pro}-\ell}(Y) \to \pi_1^{\mathrm{pro}-\ell}(X) \to 1.$$

Par récurrence sur la dimension relative de f, partant du cas des courbes affines lisses sur k déjà vu dans la proposition 2.6.8, on peut supposer que $X \to \operatorname{Spec} k$ et $Y_{\bar{\eta}} \to \bar{\eta}$ sont des $K(\pi, 1)$ pro-ℓ. Ainsi, pour tout faisceau ℓ-monodromique $\mathcal{F}$ sur Y,

$$\mathrm{R}\Gamma(Y, \mathcal{F}) = \mathrm{R}\Gamma(X, \mathrm{R}f_\star \mathcal{F}) = \mathrm{R}\Gamma(\pi_1^{\mathrm{pro}-\ell}(X), \mathrm{R}\Gamma(\pi_1^{\mathrm{pro}-\ell}(X_{\bar{\eta}}, \mathcal{F}_{\bar{\eta}})) = \mathrm{R}\Gamma(\pi_1^{\mathrm{pro}-\ell}(Y), \mathcal{F}_{\bar{\eta}}).$$

Complexité de la construction lorsque X est lisse Soit $x \in X$. Montrons que la construction d'un voisinage étale de (X, x) qui est une polycourbe ℓ-élémentaire sur $\operatorname{Spec} k$ est primitivement récursive. D'après les explications ci-avant, il suffit de construire un voisinage de Zariski de (X, x) qui est une polycourbe élémentaire. Cette construction est décrite explicitement dans [SGA4$_3$, XI, Prop. 3.3] : supposons X plongé dans un espace affine $\mathbb{A}^r$. La construction commence par considérer un plongement projectif de la normalisation $\bar{X}$ de l'adhérence de X dans $\mathbb{P}^r$. Le point clé est la construction d'hyperplans en position générale $H_1, \ldots, H_{d-1}$, où $d = \dim X$, qui coupent $\bar{X}$ et Y transversalement et contiennent x. Ceci est décrit dans l'annexe B.3.2. Le reste de la construction se résume à un éclatement et à la détermination d'un ouvert de lissité par critère jacobien. Comme toutes ces opérations sont primitivement récursives, étant donné $x \in X(k)$, la construction d'un voisinage de X qui est une polycourbe ℓ-élémentaire est primitivement récursive. L'annexe B.1.2 assure alors qu'il existe un algorithme primitivement récursif qui recouvre X par des polycourbes ℓ-élémentaires.

IV.1.3 Calcul explicite de la filtration de Frattini itérée

Soit X une courbe intègre lisse sur k de genre non nul. Notons π le complété pro-ℓ du groupe fondamental de X. D'après [Dix+99, 1.20], le sous-groupe de Frattini $\Phi(\pi)$ de π est alors le groupe $\pi^\ell[\pi, \pi]$, et le quotient $\pi/\Phi(\pi)$ est canoniquement isomorphe à $\mathrm{H}^1(\pi, \mathbb{F}_\ell)^\vee$ comme vu à la proposition 2.7.1.

Définissons comme dans [MO15, 3.3], la filtration de Frattini descendante par $\pi_1 = \pi$, puis $\pi^{[\lambda+1]} = (\pi^{[\lambda]})^\ell[\pi^{[\lambda]}, \pi^{[\lambda]}]$, et considérons les quotients $\pi^{(\lambda)} = \pi/\pi^{[\lambda]}$. En particulier, $\pi^{(\lambda)}$ est un quotient de $\pi^{(\lambda+1)}$. D'après [Dix+99, 1.116.(iii)], les $\pi^{[\lambda]}$ forment une base de voisinages de 1 dans π, ce qui entraîne que le morphisme $\pi \to \lim_{\lambda \geqslant 2} \pi^{(\lambda)}$ est un isomorphisme. Soit $X^{[\lambda]}$ un revêtement de X correspondant à $\pi^{[\lambda]}$.

Nous avons vu dans la section II.7.1.1 comment calculer $X^{[2]}$, alors noté X_2. Évaluons la complexité de cette construction. Afin de simplifier la présentation, supposons d'abord X projective ; notons g son genre. Nous avons vu dans la section II.7.1.3 que

$$g(X^{[2]}) = 1 + \ell^{2g}(g-1) \sim_{\ell, g} g\ell^{2g}.$$

Le genre de $X^{[\lambda]}$ est alors

$$g(X^{[\lambda]}) = O_{g,\ell}\left(g\ell^{2g+2g\ell^{2g}+\cdots+2g\ell^{2g+2g\ell^{2g}+\cdots+2g\ell^{\cdot^{\cdot^{\cdot^{2g\ell^{2g}}}}}}}\right)$$

où le nombre de termes horizontaux et de termes verticaux est λ. D'autre part, si $X = \bar{X} - \{P_1, \ldots, P_r\}$, la courbe $\bar{X}_2$ a ℓ^{r-2} points au-dessus de chaque P_i, et

$$|\,\mathrm{H}^1(X^{(\lambda)}, \Lambda)| \geqslant \ell^{\ell^{\cdot^{\cdot^{\cdot^{\ell^{r-2}}}}}}.$$

Ainsi, dans tous les cas sauf $\ell = 2$ et $X = \mathbb{G}_m$, la complexité du calcul de $X^{(\lambda)}$ est une exponentielle à λ étages : ce n'est pas une fonction élémentaire en (g_X, r, λ).

Remarque 4.1.4. La filtration considérée dans [MO15] est plus fine que la filtration de Frattini ; elle consiste à itérer, pour un sous-groupe H de π, $H \mapsto \mathrm{H}^\ell[H, \pi]$, et non $\mathrm{H}^\ell[H, H]$ comme dans la filtration de Frattini. Cependant, une partie des bornes explicites obtenues sur les constructions s'exprime uniquement en termes de la filtration de Frattini.

IV.1.4 Topos ℓ-étale λ-approché d'un schéma simplicial

Soit X un schéma. Soit λ un entier naturel non nul. Le topos ℓ-étale λ-approché $X^{(\lambda)}$ de X est le topos des faisceaux sur X trivialisés par le revêtement $X^{[\lambda]} \to X$. C'est le topos associé au site X_λ dont les objets sont les quotients (finis étales) de $X^{[\lambda]} \to X$. Un faisceau constructible sur $X^{(\lambda)}$ n'est rien d'autre qu'un $\pi^{(\lambda)}$-module.

De même, il est possible d'associer à un schéma simplicial $X_\bullet$ un topos $X_\bullet^{(\lambda)}$. Le topos total associé est noté $\operatorname{Tot} X_\bullet^{(\lambda)}$; un objet de ce topos est la donnée, pour tout i et tout ouvert U du site $X_{i,\lambda}$, d'un ensemble $\mathcal{F}_i(U)$, fonctoriellement en i et en U. On définit de même les topos $\operatorname{Tot} X_\bullet$ (resp. $\operatorname{Tot} X_{\bullet\ell\text{ét}}$), en remplaçant le site $X_{i,\lambda}$ par le site étale (resp. ℓ-étale, voir section I.4.3) du schéma X_i.

Soit $\mathcal{F}_\bullet$ un faisceau abélien du topos $\operatorname{Tot} X_\bullet^{(\lambda)}$. La construction pour chaque i d'une résolution flasque $\mathcal{F}_i^\bullet$ de $\mathcal{F}_i$ permet de représenter $\mathrm{R}\Gamma(\operatorname{Tot} X_\bullet^{(\lambda)}, \mathcal{F}_\bullet)$ par le complexe total associé au complexe double $(\Gamma(X_i^{(\lambda)}, \mathcal{F}_i^j)_{i,j}$. Une telle résolution flasque se détermine en choisissant un point géométrique de chaque composante connexe de X_0, puis en calculant toutes ses images dans $X_0, \ldots, X_r$ par les applications de bord et de dégénérescence. Ceci fournit un ensemble fini de points, qui forment un topos simplicial discret $P_{\bullet\leqslant r}$. Le morphisme $u\colon P_{\bullet\leqslant r} \to X_{\bullet\leqslant r}^{(\lambda)}$ est à image inverse conservative, et pour tout faisceau $\mathcal{F}_\bullet$ sur $\operatorname{Tot} X_\bullet^{(\lambda)}$, le morphisme $\mathcal{F}_{\bullet\leqslant r} \to u_\star u^\star \mathcal{F}_{\bullet\leqslant r}$ est le début d'une résolution flasque de $\mathcal{F}_{\bullet\leqslant r}$. Étant donné un schéma simplicial en groupes abéliens représentant $\mathcal{F}_{\bullet\leqslant r}$, il est possible de calculer explicitement un schéma simplicial représentant $u_\star u^\star \mathcal{F}_{\bullet\leqslant r}$: c'est simplement un coproduit de composantes connexes de $X^{[\lambda]}$ [MO15, 4.2.1].

Par descente cohomologique, il y a un isomorphisme dans $\mathrm{D}_c^b(X, \Lambda)$:

$$\mathrm{R}\Gamma(X, \Lambda) \xrightarrow{\sim} \mathrm{R}\Gamma(\operatorname{Tot} X_\bullet, \Lambda).$$

Si de plus chaque X_i est un $K(\pi, 1)$ pro-ℓ, il y a un isomorphisme :

$$\mathrm{R}\Gamma(X, \Lambda) \xrightarrow{\sim} \mathrm{R}\Gamma(\operatorname{Tot} X_{\bullet\ell\text{ét}}, \Lambda).$$

Pour tout entier $j \geqslant 0$, il y a un isomorphisme :

$$\operatorname{colim}_\lambda \mathrm{H}^j(\operatorname{Tot} X_{\bullet\ell\text{ét}}^{(\lambda)}, \Lambda) \xrightarrow{\sim} \mathrm{H}^j(\operatorname{Tot} X_{\bullet\ell\text{ét}}, \Lambda).$$

La cohomologie de $\operatorname{Tot} X^{(\lambda)}_{\bullet\ell\text{ét}}$ est calculée par la suite spectrale

$$E_1^{i,j} = \mathrm{H}^j(X_i^{(\lambda)}, \Lambda) = \mathrm{H}^j(\pi_1^{\mathrm{pro}-\ell}(X_i)^{(\lambda)}, \Lambda) \Rightarrow \mathrm{H}^{i+j}(\operatorname{Tot} X^{(\lambda)}_{\bullet\ell\text{ét}}, \Lambda).$$

Les résultats de la section suivante permettent de déterminer $\mathrm{H}^j(X, \Lambda)$ comme l'image d'un morphisme

$$\mathrm{H}^j(\operatorname{Tot} X^{(\alpha)}_{\bullet\ell\text{ét}}, \Lambda) \to \mathrm{H}^j(\operatorname{Tot} X^{(\beta)}_{\bullet\ell\text{ét}}, \Lambda).$$

IV.1.5 Systèmes essentiellement constants et cohomologie des polycourbes ℓ-élémentaires

Soit $\mathcal{C}$ une catégorie abélienne dans laquelle les colimites filtrantes existent. Soit $(A_i)_{i\in\mathbb{N}}$ un système inductif d'objets noethériens dans $\mathcal{C}$. Si la colimite A_∞ est noethérienne, il existe des entiers j, k tels que la restriction du morphisme $A_k \to A_\infty$ à l'image de $A_j \to A_k$ soit un isomorphisme.

Définition 4.1.5. Soient N un entier naturel et $\phi\colon \mathbb{N} \to \mathbb{N}$ une application. Le système inductif A est dit (N, ϕ)-essentiellement constant (ou (N, ϕ)-ec) s'il vérifie les deux conditions suivantes :

1. pour tout entier j et tout $k \geqslant \phi(j)$, $\ker(A_j \to A_{\phi(j)}) \to \ker(A_j \to A_k)$ est un isomorphisme ;
2. pour tout $j \geqslant N$, $\operatorname{im}(A_N \to A_{\phi(j)}) \to \operatorname{im}(A_j \to A_{\phi(j)})$ est un isomorphisme.

Un tel système inductif A est dit explicitement essentiellement constant (ou eec) s'il existe (N, ϕ) calculables tels que A soit (N, ϕ)-ec. L'essentielle constance des systèmes inductifs se comporte bien vis-à-vis des suites exactes.

Proposition 4.1.6. [MO15, Prop. 5.6] Soit

$$0 \to A' \to A \to A'' \to 0$$

une suite exacte de systèmes inductifs dans $\mathcal{C}$ indexés par $\mathbb{N}$.

1. Si A est (N, ϕ)-ec et A'' est (N'', ϕ'')-ec alors A' est $(\phi''(N), \phi)$-ec.
2. Si A est (N, ϕ)-ec et A' est (N', ϕ')-ec alors A'' est $(N, \max(\phi, N'))$-ec.
3. Si A' est (N', ϕ')-ec et A'' est (N'', ϕ'')-ec alors A est $(\max(N', N''), \phi' \circ \phi'')$-ec.

Ceci implique qu'étant donné un système inductif de suites spectrales $(E_{2,\lambda}^{p,q} \Rightarrow \mathrm{H}_\lambda^{p+q})_\lambda$, si chaque $(E_{2,\lambda}^{p,q})_\lambda$ est eec et s'il existe un entier r tel que $E_{2,\lambda}^{p,q} = 0$ dès que $q > r$ alors $(\mathrm{H}_\lambda^{p+q})_\lambda$ est eec. Le résultat suivant précise cet énoncé dans un cas particulier.

Lemme 4.1.7. Soit $(E_{2,\lambda}^{pq} \Longrightarrow H_\lambda^{p+q})_\lambda$ un système inductif de suites spectrales. Supposons que pour tous entiers p, q, le système inductif $(E_{2,\lambda}^{pq})_\lambda$ soit (N, ϕ)-essentiellement constant. Alors le système $(E_{r,\lambda}^{pq})_\lambda$ est $(\phi^{r-2}(N), \max(\phi, \phi^{r-3}(N))$-essentiellement constant.

Démonstration. Ceci se démontre par récurrence sur r. Le groupe $E_{r+1,\lambda}^{pq}$ est un quotient de la forme $\ker(f_\lambda)/\operatorname{im}(g_\lambda)$, où f et g sont des flèches de la page E_r. Par la proposition précédente et l'hypothèse de récurrence, le système $(\ker f_\lambda)_\lambda$ est $(\phi^{r-1}(N), \max(\phi, \phi^{r-3}(N))$-essentiellement constant, et le système $(\operatorname{im} g_\lambda)_\lambda$ est $(\phi^{r-2}(N), \max(\phi, \phi^{r-3}(N))$-essentiellement constant. Une nouvelle application de la proposition précédente montre que le système $(E_{r+1,\lambda}^{pq})_\lambda$ est $(\phi^{r-1}(N), \max(\phi, \phi^{r-2}(N))$-essentiellement constant. $\square$

Soit

$$X = X_d \to X_{d-1} \to \cdots \to X_1 \to \operatorname{Spec} k$$

une polycourbe ℓ-élémentaire (affine) sur k. Notons π le groupe fondamental pro-ℓ de X et $\bar{\eta}$ un point générique géométrique de X_1. Il y a, comme vu précédemment, une suite exacte

$$1 \to \pi_1^{\mathrm{pro}-\ell}(X_{\bar{\eta}}) \to \pi \to \pi_1^{\mathrm{pro}-\ell}(X_1) \to 1$$

où le groupe de droite est un pro-ℓ-groupe libre, et le groupe de gauche est (par récurrence sur la dimension) une extension itérée de tels groupes. Pour tout niveau d'approximation λ, cette suite fournit une nouvelle suite

$$1 \to \pi''_\lambda \to \pi^{(\lambda)} \to \pi_1^{\mathrm{pro}-\ell}(X_1)^{(\lambda)} \to 1$$

où π''_λ est simplement défini comme étant le noyau de $\pi^{(\lambda)} \to \pi_1^{\mathrm{pro}-\ell}(X_1)^{(\lambda)}$. Les groupes de cette suite se calculent explicitement. Il est montré dans [MO15, Cor. 6.4] que si $(\pi_1^{\mathrm{pro}-\ell}(X_{\bar{\eta}})^{(\lambda)})_\lambda$ est eec, il en est de même pour π''_λ. Notons qu'un couple (N, ϕ) explicitant ce fait est exhibé dans [MO15, Prop. 6.3] : sa détermination est primitivement récursive. Par récurrence sur la dimension, il suffit pour montrer que le système $(\mathrm{H}^j(\pi^{(\lambda)}, \Lambda))_\lambda$ est eec, de montrer que c'est le cas lorsque X est une courbe. C'est évident lorsque $j = 0$. Pour $j = 1$, nous verrons dans la section V.3.1 que le système est $(2, \lambda \mapsto \lambda + 1)$-essentiellement constant. Pour $j \geqslant 2$, il est possible de trouver λ_0 tel que pour tout $\lambda > \lambda_0$, $\mathrm{H}^j(\pi^{(\lambda_0)}, \Lambda) \to \mathrm{H}^j(\pi^{(\lambda)}, \Lambda)$ soit nulle. Il suffit pour cela que $\mathrm{H}^1(\pi^{[\lambda_0]}, \Lambda) \to \mathrm{H}^j(\pi^{[\lambda]}, \Lambda)$ soit nulle [MO15, Rem. 6.6], ce qui est le cas dès que $\lambda_0 \geqslant 2$ (voir lemme 2.7.4). Le système $(\mathrm{H}^j(\pi^{(\lambda)}, \Lambda))_\lambda$ est donc également $(2, \lambda \mapsto \lambda + 1)$-ec.

IV.1.6 Adaptation de l'algorithme à des cas plus généraux

Variétés singulières Soit X un schéma de type fini sur k. Le théorème de résolution des singularités de de Jong assure qu'il est localement lisse pour la topologie des altérations. Ceci permet de se ramener par changement de base au cas des schémas lisses, mais pose problème en termes de complexité : à moins d'étudier en détail chaque construction de [Jon96], une recherche non bornée est nécessaire pour trouver une altération convenable.

Images directes de faisceaux constructibles Pour calculer les groupes de cohomologie d'un faisceau constructible $\mathcal{F}$, il suffit de plonger $\mathcal{F}$ dans un faisceau $\tilde{\mathcal{F}}$ tel que pour tout $i > 0$, le morphisme

$$\mathrm{R}^i f_\star \mathcal{F} \to \mathrm{R}^i f_\star \tilde{\mathcal{F}}$$

soit nul. En effet, $\mathrm{R}^j f_\star \mathcal{F}$ se calcule alors récursivement comme

$$\mathrm{R}^j f_\star \mathcal{F} = \operatorname{coker}(\mathrm{R}^{j-1} f_\star \tilde{\mathcal{F}} \to \mathrm{R}^{j-1} f_\star (\tilde{\mathcal{F}}/\mathcal{F})).$$

La calcul d'un tel $\tilde{\mathcal{F}}$ est décrit en détail dans [MO15, 11.4.4]. Nous donnerons une construction explicite dans le cas des courbes dans la section V.5.2.

Cohomologie d'un complexe de faisceaux constants sur une courbe Soit X une courbe affine lisse sur k. Soit $K = [K^0 \to \cdots \to K^N]$ un complexe de Λ-modules. Considérons toujours les quotients de Frattini $\pi^{(\lambda)}$ du groupe fondamental pro-ℓ de X. Rappelons qu'il y a une suite spectrale [Stacks, 0AVG] de deuxième page

$$E_2^{p,q} = \mathrm{H}^p(\pi, \mathrm{H}^q K) \Longrightarrow \mathrm{H}^{p+q}(\pi, K).$$

Rappelons que pour tout $p \geqslant 2$ et tout $q \in \{0 \dots N\}$, le système $(\mathrm{H}^p(\pi^{(\lambda)}, \mathrm{H}^q K))_\lambda$ est $(2, \lambda \mapsto \lambda + 1)$ essentiellement constant.

Lemme 4.1.8. Pour tout entier $i \geqslant 0$, le système inductif $(\mathrm{H}^i(\pi^{(\lambda)}, K))_{\lambda \geqslant 2}$ est $(N+2, \lambda \mapsto \lambda+N+2)$-essentiellement constant.

Démonstration. Considérons la suite spectrale $E_{2,\lambda}^{pq} = \mathrm{H}^p(\pi^{(\lambda)}, \mathrm{H}^q(K)) \Longrightarrow \mathrm{H}^{p+q}(\pi^{(\lambda)}, K)$. Le terme $E_{2,\lambda}^{pq}$ est nul dès que $q > N$. Par conséquent, toutes les flèches de la page E_{N+2} sont nulles, et la suite spectrale converge : $E_{\infty,\lambda} = E_{N+2,\lambda}$. Pour tous p, q, le système $(E_{2,\lambda}^{pq})_{\lambda \geqslant 2}$ est $(2, \lambda \mapsto \lambda+1)$-essentiellement constant. Le lemme 4.1.7 assure alors que le système $(E_{N+2,\lambda}^{pq})_\lambda$ est $(N+2, \lambda \mapsto \max(\lambda, N)+1))$-essentiellement constant.
Le groupe $\mathrm{H}^i(\pi^{(\lambda)}, K)$ est extension itérée des $E_{N+2,\lambda}^{p,q}$ avec $p+q=i$. Plus précisément, il y a une suite exacte courte de groupes abéliens

$$0 \to A_{i,\lambda} \to \mathrm{H}^i(\pi^{(\lambda)}, K) \to E_{N+2,\lambda}^{0,i} \to 0$$

puis, pour $1 \leqslant r \leqslant i-1$, une suite exacte courte

$$0 \to A_{i-r,\lambda} \to A_{i-r+1,\lambda} \to E_{N+2,\lambda}^{r,i-r} \to 0$$

et enfin une suite exacte courte

$$0 \to E_{N+2,\lambda}^{i,0} \to A_{1,\lambda} \to E_{N+2,\lambda}^{i-1,1} \to 0.$$

D'après les résultats précédents, le système inductif $(A_{1,\lambda})_\lambda$ est $(N+2, \max(\lambda \mapsto \lambda+2, N+1))$-essentiellement constant. Une récurrence immédiate donne alors que $\mathrm{H}^i(\pi^{(\lambda)}, K)$ est $(N+2, \lambda \mapsto \max(N+1, \lambda+N+2))$-essentiellement constant, c'est-à-dire $(N+2, \lambda \mapsto \lambda+N+2)$-essentiellement constant. □

IV.1.7 Remarques sur la complexité de l'algorithme

Proposition 4.1.9. Soit X un schéma lisse de type fini sur un corps algébriquement clos k. Soit ℓ un nombre premier inversible dans k. L'algorithme décrit dans [MO15] qui calcule les groupes de cohomologie $\mathrm{H}^j(X, \mathbb{Z}/\ell\mathbb{Z})$ pour $j \in \{0 \ldots 2\dim X\}$ est primitivement récursif.

Démonstration. Nous avons montré ci-dessus que le calcul d'un hyperrecouvrement de X par des $K(\pi, 1)$ pro-ℓ était primitivement récursif, de même que le calcul des r premiers étages d'une résolution flasque du faisceau $\mathbb{Z}/\ell\mathbb{Z}$ dans chaque topos $\operatorname{Tot} X_{\bullet \leqslant r}^{[\lambda]}$. Nous avons vu qu'il en est de même, pour tout entier $j \leqslant 2\dim X$, des fonctions explicitant le fait que le système inductif $(\mathrm{H}^j(\operatorname{Tot} X_{\bullet \leqslant r}^{(\lambda)}, \Lambda))_\lambda$ est essentiellement constant. □

De la difficulté de montrer qu'il est élémentaire Considérons la forme la plus simple de l'algorithme, qui calcule les $\mathrm{H}^i(X, \Lambda)$ pour un schéma X intègre lisse de type fini sur k. Notons d sa dimension. Soit $X_\bullet$ un hyperrecouvrement étale de X. Notons s_i (resp. D_i) le nombre (resp. le degré maximal sur X) des composantes connexes de X_i. Alors

$$s_{i+1} \leqslant s_i^2 D_i \quad \text{et} \quad D_{i+1} \leqslant D_i^2.$$

Remarquons que dès que l'une des composantes connexes de X_0 est galoisienne de degré b sur son image dans X, le nombre de composantes connexes de X_r est supérieur à b^r. Déjà lorsque X est une courbe, les systèmes $(\mathrm{H}^q(X_p^{(\lambda)}, \Lambda))_\lambda$ pour $2 \leqslant q \leqslant r$ sont $(2, \lambda \mapsto \lambda+1)$-essentiellement constants pour la filtration de Frattini, et nous n'avons pour l'instant pas de borne pour une autre filtration. Dans le cas d'un schéma de dimension supérieure, nous n'arriverons certainement pas à obtenir mieux. Il faut donc s'attendre à ce que la première page

$$E_1^{pq} = \mathrm{H}^q(X_p^{(\lambda)}, \Lambda)$$

de la suite spectrale calculant $\mathrm{H}^j(X,\Lambda)$ soit constituée d'au moins $r \times r$ systèmes inductifs, dont au moins $(r-2)\times r$ ne sont pas constants. Le raisonnement du lemme 4.1.7 montre alors que par exemple $(\mathrm{H}^r(\mathrm{Tot}\, X^{(\lambda)}_{\bullet\leqslant r},\Lambda))_\lambda$ est $(r-4, \lambda \mapsto \lambda + r - 5)$-essentiellement constant. Comme l'algorithme prend pour r un nombre strictement supérieur à la dimension d de X, il faut s'attendre à calculer au moins le $(d-4)$-ième revêtement de Frattini d'une courbe, dont la complexité est une exponentielle à $d-4$ étages, qui n'est pas une fonction élémentaire en d. Il faudrait donc, afin d'obtenir une complexité élémentaire, trouver des bornes sur l'essentielle constance des systèmes ci-dessus pour une filtration plus fine, comme celle proposée dans [MO15, §3].

IV.2 L'algorithme de Couveignes

IV.2.1 Données et principe de l'algorithme

Soient ℓ un nombre premier, et $\mathbb{F}_q$ un corps fini de caractéristique différente de ℓ. Soit j un entier naturel. Soit X une courbe projective intègre lisse sur $\mathbb{F}_q$ de genre g, décrite par un modèle plan et ses branches singulières comme dans l'annexe C.1.2. L'algorithme décrit dans [Cou09] a pour but de calculer des diviseurs représentant les éléments de $J(\mathbb{F}_q)[\ell^j]$. Nous nous contentons ici de résumer cet algorithme et de décrire en IV.2.6 le travail restant à faire pour généraliser l'algorithme à la division par n dans $J(\overline{\mathbb{F}_q})$.

Soit i un entier naturel. Soit Q une puissance de q assez grande pour que $|J(\mathbb{F}_Q)[\ell^{2g}]| = \ell^{2g}$. La procédure décrite dans la section IV.2.2 permet de tirer aléatoirement des diviseurs non principaux dans $J(\mathbb{F}_Q)$ qui engendrent un sous-groupe de $J(\mathbb{F}_Q)$ de petit indice. L'application de Kummer décrite dans la section IV.2.4.2 permet de leur associer des éléments d'un sous-groupe $H \subset J(\mathbb{F}_Q)[\ell^i]$, où i est un entier naturel. En choisissant i assez grand, il est possible de faire en sorte que le sous-groupe H contienne $J(\mathbb{F}_Q)[\ell^j]$. Le couplage de Weil permet alors de retrouver $J(\mathbb{F}_q)[\ell^j]$. La complexité de l'algorithme de Couveignes est donnée par le résultat suivant.

Théorème 4.2.1. [Cou09, Th. 1] Il existe un algorithme probabiliste (Monte-Carlo) qui prend en entrée une courbe projective lisse géométriquement intègre X de genre g sur $\mathbb{F}_q$ définie par un modèle plan de degré d, un diviseur $\mathbb{F}_q$-rationnel $O = D^+ - D^-$ de degré 1 sur $\mathbb{F}_q$ avec $\deg D^+ = O(g)$, un nombre premier ℓ ne divisant pas q, un entier naturel j et la fonction zêta de X, et renvoie une $\mathbb{Z}/\ell^j$-base de $\mathrm{Pic}(X)(\mathbb{F}_q)[\ell^j]$ dont les éléments sont des diviseurs de la forme $G - gO$ où G est effectif. Le nombre d'opérations arithmétiques effectué par l'algorithme est polynomial en $d, g, \log q$ et ℓ^j ; l'algorithme renvoie un sous-groupe de $\mathrm{Pic}(X)(\mathbb{F}_q)[\ell^j]$, qui est le groupe entier avec probabilité $\geqslant \frac{1}{2}$.

IV.2.2 Tirage aléatoire de diviseurs

L'algorithme de Couveignes construit un sous-groupe assez grand de $\mathrm{Pic}^0(X)(\mathbb{F}_q)$ en tirant aléatoirement des diviseurs $\mathbb{F}_q$-rationnels sur X. L'idée est la suivante : le modèle plan donné de X fournit un morphisme $x\colon X \to \mathbb{P}^1$. L'image par x de l'ensemble $\mathcal{P}(r,q)$ de $\mathbb{F}_q$-places de X de degré r est incluse dans l'ensemble $\mathcal{U}(r,q)$ des polynômes unitaires irréductibles de degré r sur $\mathbb{F}_q$. Le tirage des diviseurs est réalisé en tirant aléatoirement selon une distribution uniforme un polynôme unitaire de degré r à coefficients dans $\mathbb{F}_q$, puis en testant son irréductibilité, avant de calculer le cas échéant ses antécédents dans $\mathcal{P}(r,q)$. Le choix d'un diviseur effectif Ω de degré r sur X détermine une application $\mathcal{P}(r,q) \to \mathrm{Pic}^0(X)(\mathbb{F}_q), \alpha \mapsto [\alpha] - \Omega$. Il existe une unique mesure μ sur $\mathcal{P}(r,q)$ telle que les fibres non vides de $\mathcal{P}(r,q) \to \mathcal{U}(r,q)$ soient de même mesure, et tous les points d'une même fibre aient la même mesure. La mesure de l'ensemble des places dans $\mathcal{P}(r,q)$ d'image non nulle dans $\mathrm{Pic}^0(X)(\mathbb{F}_q)$ est alors supérieure à $\frac{1}{2d}$, et au bout de $2d$ tirages, la probabilité d'avoir obtenu un diviseur non trivial est supérieure à $\frac{1}{2}$.

Cette méthode permet de construire par tirages successifs des diviseurs engendrant avec probabilité $\geqslant \frac{1}{2}$ un sous-groupe G de $\mathrm{Pic}^0(X)(\mathbb{F}_q)$ d'indice inférieur à une borne ι fixée. Pour que la complexité de l'algorithme reste polynomiale en les entrées, il n'est pas possible d'obtenir ainsi $\mathrm{Pic}^0(X)(\mathbb{F}_q)$ tout entier ; il est toutefois loisible de choisir ι linéaire en d et g (dans l'article, $\iota = \max\{48g, 24d, 720\}$).

IV.2.3 Groupes ℓ-divisibles

Soit χ_ℓ la réduction mod ℓ du polynôme caractéristique de l'endomorphisme de Frobenius sur J_X. Il se factorise en

$$\chi_\ell(t) = (t-1)^b \bar{f}^\perp(t)$$

où $\bar{f}^\perp(t)$ est premier à $t-1$. Le lemme de Hensel permet de relever cette factorisation en une unique factorisation en produit de polynômes unitaires

$$\chi(t) = f(t)f^\perp(t) \in \mathbb{Z}_\ell[t].$$

Soient $e, e^\perp$ les idempotents de $\mathbb{Z}_\ell[t]/\chi$ correspondant respectivement aux éléments $(1,0)$ et $(0,1)$ de $\mathbb{Z}_\ell[t]/f \times \mathbb{Z}_\ell[t]/f^\perp$. Les éléments $e_1(\phi_q)$ et $e_1^\perp(\phi_q)$ définissent des endomorphismes du groupe $J_X[\ell^\infty]$, et leurs images respectives sont les sous-groupes ℓ-divisibles $\mathbb{G}_1$ et $\mathbb{G}_1^\perp$ de $J_X[\ell^\infty]$. Ceci définit une décomposition

$$J_X[\ell^\infty] = \mathbb{G}_1 \times \mathbb{G}_1^\perp$$

en produit de deux groupes ℓ-divisibles.

IV.2.4 Une surjection $J(\mathbb{F}_q) \to J[\ell^j](\mathbb{F}_q)$

IV.2.4.1 Détermination d'une extension de corps adéquate

Soit A une variété abélienne sur $\mathbb{F}_q$. Soit $\mathbb{G}$ un sous-groupe de $A[\ell^\infty]$. Pour une extension L de $\mathbb{F}_q$, notons $\mathbb{G}(L) = \mathbb{G} \cap A(L)$. Soit $\chi \in \mathbb{Z}_\ell[t]$ le polynôme caractéristique de l'automorphisme de Frobenius sur A. Voici comment déterminer une extension $L/\mathbb{F}_q$ telle que $\mathbb{G}[\ell^j](L) = \mathbb{G}[\ell^j](\overline{\mathbb{F}_q})$. Considérons l'application

$$(\mathbb{Z}/\ell^j\mathbb{Z})[t]/(\chi \bmod \ell^j) \to \mathrm{End}(\mathbb{G}[\ell^j])$$

qui envoie t sur l'automorphisme de Frobenius ϕ_q. L'ordre de ϕ_q dans $\mathrm{Aut}(\mathbb{G}[\ell^j])$ est le degré de la plus petite extension de $\mathbb{F}_q$ sur laquelle sont définis tous les points de $\mathbb{G}[\ell^j]$. Il divise l'ordre de t dans $\big((\mathbb{Z}/\ell^j\mathbb{Z})[t]/\chi\big)^\times$.

Dans le cas où $\mathbb{G}$ est le groupe $\mathbb{G}_1$ de la section précédente, voici comment déterminer cet ordre. Soit b la valuation $(t-1)$-adique de $\chi \in \mathbb{F}_\ell[t]$. L'entier $\gamma = \lceil \log_\ell b \rceil$ vérifie $(t-1)^{\ell^\gamma} = 0 \in \mathbb{F}_\ell[t]/\chi$, et l'ordre de t dans $(\mathbb{F}_\ell[t]/\chi)^\times$ divise ℓ^γ. Par conséquent, l'ordre de t dans $(\mathbb{Z}/\ell^j\mathbb{Z}[t]/\chi)^\times$ divise $\ell^{\gamma+j-1}$. Dans le cas où $\mathbb{G} = J_X$, l'ordre de t divise

$$A_k := \ell^{\lceil \log_\ell(2g) \rceil + j - 1} \prod_i (\ell^{f_i} - 1)$$

où les f_i sont les degrés des facteurs irréductibles de χ modulo ℓ.

IV.2.4.2 L'application de Kummer

Soit A une variété abélienne sur $\mathbb{F}_q$. Soit $\mathbb{G}$ un sous-groupe ℓ-divisible de $A[\ell^\infty]$. Supposons que $\mathbb{G}[\ell^j](\mathbb{F}_q) = \mathbb{G}[\ell^j](\overline{\mathbb{F}_q})$. Pour chaque $P \in \mathbb{G}(\mathbb{F}_q)$, choisissons un point $R_P \in \mathbb{G}(\overline{\mathbb{F}_q})$ tel que $\ell^j R_P = P$. Associons à P l'élément

$$K_{\ell^j,q}(P) := R_P^{\phi_q} - R_P \in \mathbb{G}[\ell^j](\overline{\mathbb{F}_q}) = \mathbb{G}[\ell^j](\mathbb{F}_q).$$

Ceci définit un isomorphisme de groupes abéliens

$$K_{\ell^j,q} \colon \mathbb{G}(\mathbb{F}_q)/\ell^j\mathbb{G}(\mathbb{F}_q) \to \mathbb{G}[\ell^j](\mathbb{F}_q).$$

Il n'est évidemment pas question de calculer explicitement l'élément R_P : cet isomorphisme se calcule de façon plus efficace. Comme vu dans la partie précédente, il est possible de calculer un entier a tel que $t^a = 1$ dans $(\mathbb{Z}/\ell^j\mathbb{Z})[t]/\chi$. En relevant cette identité à $\mathbb{Z}_\ell$, il existe un unique $M_{j,a} \in \mathbb{Z}_\ell[t]/\chi$ tel que $t^a - 1 = M_{j,a}(t)\ell^j$. L'isomorphisme de Kummer ci-dessus s'identifie alors à $P \mapsto M_{j,a}(\phi_q)(P)$.

IV.2.5 Calcul de la ℓ-torsion du groupe de Picard

Soit $Q = q^{(\ell-1)\ell^{\gamma+j-1}}$. Alors $\mathbb{G}_1[\ell](\mathbb{F}_Q) = \mathbb{G}_1[\ell](\overline{\mathbb{F}_q})$. On commence par tirer des éléments de $J(\mathbb{F}_Q)$ qui engendrent un sous-groupe d'indice inférieur à $\iota = \max(48g, 24d, 720)$. L'image de ce sous-groupe par la composition de morphismes surjectifs

$$J(\mathbb{F}_Q) \xrightarrow{e(\phi_q)} \mathbb{G}_1(\mathbb{F}_Q) \xrightarrow{K_{n,q}} \mathbb{G}_1[\ell^j](\mathbb{F}_Q)$$

est un sous-groupe H de $\mathbb{G}_1[\ell^j](\mathbb{F}_Q)$ d'indice au plus ι. Dès que j est supérieur à $\delta := \lceil \log_\ell \iota \rceil$, le sous-groupe H contient $\mathbb{G}_1[\ell^{j-\delta}](\mathbb{F}_Q) = \mathbb{G}_1[\ell^{j-\delta}](\overline{\mathbb{F}_q})$. Calculer l'ordre des éléments de H permet alors de déterminer $\mathbb{G}_1[\ell^{j-\delta}](\mathbb{F}_Q)$. Le groupe $J[\ell^{j-\delta}](\mathbb{F}_q)$ s'en déduit comme le noyau de l'endomorphisme $\phi_q - \mathrm{id}$ de $\mathbb{G}_1[\ell^{j-\delta}](\mathbb{F}_Q)$.

IV.2.6 Racines n-ièmes d'éléments non nuls de $J_X(\mathbb{F}_q)$

Soit n un entier naturel premier à q. L'algorithme de Couveignes produit les éléments de n-torsion de $J_X(\mathbb{F}_q)$. Une question plus générale, et qui sert dans le calcul de la cohomologie des courbes affines, est la suivante : étant donné un élément $D \in J_X(\mathbb{F}_q)$, déterminer $D' \in J_X(\overline{\mathbb{F}_q})$ tel que $nD' = D$. L'endomorphisme $\phi_q - \mathrm{id}$ de J_X étant surjectif, il existe $D_1 \in \mathrm{Pic}^0(X)$ tel que $D = D_1^{\phi_q} - D_1$. Notons τ_{D_1} la translation par D_1 sur J_X. Alors l'application

$$K_{\ell^j,q} \circ \tau_{D_1} \colon \mathbb{G}_1(\mathbb{F}_Q) \to \{E \in \mathbb{G}_1(\mathbb{F}_Q) \mid nE = D\}$$

est surjective. La même procédure que précédemment permet alors de tirer un élément non trivial de $J(\mathbb{F}_Q)$, de calculer son image dans $\mathbb{G}_1(\mathbb{F}_Q)$ puis par translation un antécédent de D par $[n]_{\mathbb{G}_1(\mathbb{F}_Q)}$. Ici, connaissant déjà $J[n]$, il suffit de trouver un seul antécédent. Étant donné D, le problème du calcul dans $J(\overline{\mathbb{F}_q})$ d'un antécédent par la multiplication par n se réduit donc au calcul d'un antécédent par $\phi_q - \mathrm{id}$.

En fonction des objectifs de complexité, cette réduction peut ou non apporter un bénéfice : l'isogénie de multiplication par n est de degré n^{2g}, alors que $\phi_q - \mathrm{id}$ est de degré $O(q^g)$. Cependant, il n'y a à la connaissance de l'auteur de ces lignes pas de méthode efficace pour calculer un antécédent par $\phi_q - \mathrm{id}$. Une possibilité serait d'employer un analogue de l'algorithme de Huang-Ierardi présenté dans la section suivante, qui consisterait étant donné un diviseur D à chercher explicitement des diviseurs F tels que $F^{\phi_q} - F$ soit équivalent à un diviseur très simple (voir définition 4.3.4) équivalent à D. Cependant, la complexité de cet algorithme serait au moins linéaire en q.

IV.3 L'algorithme de Huang et Ierardi

Dans toute cette section, $C_0 = \mathrm{Proj}\, k_0[x,y,z]/(f)$ désigne une courbe projective plane intègre sur $k_0 = \mathbb{F}_q$, et X_0 désigne sa normalisée. Notons d le degré de f et g le genre de X_0. Notons $X = X_0 \times_{k_0} k$. Soit J_X la jacobienne de X.

IV.3.1 Structure de l'algorithme

IV.3.1.1 Données et hypothèses

La courbe C_0 est décrite par le polynôme homogène $f \in k_0[x, y, z]$ de degré d. Pour le calcul de C_0 étant donné X_0, et vice-versa, voir les annexes C.1.2 et C.1.1.1. Notons $Q_1, \ldots, Q_r$ les points singuliers de C, et $m_1, \ldots, m_r$ leurs multiplicités respectives. Rappelons que $r \leqslant \binom{d-1}{2}$. Les singularités de C sont supposées ordinaires ; ceci s'obtient par des transformations quadratiques [Kol07, §1.7], et demande éventuellement de remplacer C par une courbe C' de degré $d' = O(2^{d^2})$. Supposons C remplacée par C', et d par d'.
Pour chaque $i \in \{1 \ldots r\}$ est donnée (voir [HI98, §3.3]) une courbe C'_{Q_i} birationnelle à C sur laquelle Q_i a m_i antécédents Q_{ij} ; elle est obtenue en éclatant C en Q_i. Il est possible que la courbe C contienne un point Q_T dit "terrible" (voir [FW89, Appendix A, p113], qui est alors unique. Il peut être régulier ou singulier. Notons m_T sa multiplicité. Il est toujours possible de construire, en au plus deux transformations birationnelles [HI98, §3.3], une courbe C'_T birationnelle à C sur laquelle Q_T a m_T antécédents réguliers et non terribles. Si T est régulier, il sera parfois traité de la même façon que les points singuliers, ce que nous préciserons le cas échéant.

Le corps fini k_0 est supposé assez grand ($d^6 < |k_0|$) pour pouvoir énumérer un nombre suffisant d'éléments distincts dans k_0 dans les diverses constructions, ainsi que pour contenir les coordonnées des Q_i et des Q_{ij} (ce qui nécessite de remplacer le corps de départ par une extension de degré au plus $d'^3!$), ainsi que d'un point régulier de C, qui sera noté ∞. Dans la description de l'algorithme, nous supposerons que k_0 a été remplacé par une telle extension.

IV.3.1.2 Le résultat

L'algorithme développé par Huang et Ierardi avait pour but principal le comptage de points sur les courbes, d'où le premier énoncé. Cependant, les calculs de complexité présentés dans [HI98, §5.4] démontrent également le second résultat.

Théorème 4.3.1. [HI98, Theorem 1.1] Soit $d \in \mathbb{N}$. Il existe un réel $\alpha > 0$ et un algorithme probabiliste Las Vegas qui prend en entrée une puissance q d'un nombre premier, un entier n et une courbe projective plane $C_0 \subset \mathbb{P}^2_{\mathbb{F}_q}$ de degré d n'ayant que des singularités ordinaires, de normalisée X_0, et qui renvoie le $\Lambda[\mathfrak{G}_0]$-module $\mathrm{H}^1(X_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mu_n)$ en $O((d \log(q))^{d^\alpha})$ opérations dans $\mathbb{F}_q$ dès lors que $n = O(d^2 \log q)$. La probabilité de succès de l'algorithme est supérieure à $\frac{1}{2}$.

Proposition 4.3.2. Soient n, d deux entiers naturels. Soit q une puissance d'un nombre premier p. Il existe des entiers $\alpha, \beta > 0$ et un algorithme déterministe qui prend en entrée une courbe projective plane $C_0 \subset \mathbb{P}^2_{\mathbb{F}_q}$ de degré d n'ayant que des singularités ordinaires, de normalisée X_0, et qui renvoie le $\Lambda[\mathfrak{G}_0]$-module $\mathrm{H}^1(X_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}, \mu_n)$ en $O_{n,d,q}(p^{\alpha d^3!}(dn)^{d^\beta})$ opérations dans $\mathbb{F}_q$.

L'énoncé correspondant pour une courbe plane quelconque s'obtient en remplaçant d par 2^d dans la complexité. Nous nous servirons par la suite du résultat suivant, qui se déduit des précédents en adaptant l'algorithme de Huang et Ierardi en suivant les remarques 4.3.5, 4.3.6 et 4.3.8, à l'aide des calculs de complexité effectués dans les sections IV.3.4.1 et IV.3.4.2.

Proposition 4.3.3. Soit $d \in \mathbb{N}$. Il existe un algorithme probabiliste (Las Vegas) qui prend en entrée une puissance q d'un nombre premier, un entier n, une courbe projective plane $C_0 \subset \mathbb{P}^2_{\mathbb{F}_q}$ de degré d et de genre g n'ayant que des singularités ordinaires, de normalisée X_0, et un diviseur $F = F^+ - F^- \in \mathrm{Div}^0(X_0)(\mathbb{F}_q)$ avec $\deg(F^+) \leqslant g$, et qui renvoie le $\Lambda[\mathfrak{G}_0]$-module

$$\{[D] \in \mathrm{Pic}^0(X_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}) \mid n[D] = F\}$$

en $\mathcal{P}(d, g, n, \log q)^{O(g^4)}$ opérations dans $\mathbb{F}_q$, où $\mathcal{P}$ est un polynôme. La probabilité de succès de l'algorithme est supérieure à $\frac{1}{2}$.

IV.3.1.3 Résumé de l'algorithme

L'algorithme de Huang et Ierardi est essentiellement l'algorithme de Brill-Noether (voir annexe C.3.2) appliqué à un diviseur générique. Il consiste à considérer un diviseur D dont les coordonnées des points du support sont des indéterminées, calculer un diviseur équivalent à nD, et construire comme dans l'algorithme de Brill-Noether une fonction dont nD est le diviseur. L'existence d'une telle fonction se traduit par des équations sur les indéterminées ; il suffit alors de trouver des points dans le schéma défini par ces équations.

Définition 4.3.4. Un diviseur $D = \sum a_i P_i \in \mathrm{Div}(X)$ est dit très simple si les P_i sont des points réguliers non-terribles deux à deux distincts de C et si $a_i = \pm 1$ pour tout i.

Soit $D \in \mathrm{Div}^0(X)$. Rappelons qu'un point $\infty \in X$ a été fixé. Le théorème de Riemann-Roch assure que l'espace $\mathcal{L}(D + g\infty)$ est non vide ; il existe donc un diviseur effectif E de degré g sur X tel que $E - g\infty$ soit équivalent à D. Par conséquent, les diviseurs de degré zéro seront représentés par un diviseur équivalent de la forme $E - g\infty$ avec $E \geqslant 0$.

Tout diviseur effectif D de degré g sur C s'écrit de façon unique $D = D_1 + D_2$, où le support de D_1 est constitué de points de X au-dessus de points singuliers ou terribles de C et $\deg(D_1) \leqslant g$. Pour chaque D_1 (décrit explicitement comme $\sum_i a_i Q_i$), l'algorithme cherche les D_2 (décrits par des indéterminées) de degré $g - \deg(D_1)$ tels que $D_1 + D_2 - g\infty$ soit un diviseur de n-torsion. Soit donc $D = D_1 + D_2$ un diviseur effectif de degré g sur X. L'algorithme construit un diviseur très simple D' (dont les coordonnées s'expriment en fonction de celles de D_2) équivalent à $n(D - g\infty)$, puis vérifie si D' est principal. Il construit un polynôme homogène G_∞ de façon à ce que D' soit principal si et seulement s'il existe un numérateur G_0 tel que $D' = \mathrm{div}(G_0/G_\infty)$. Une condition nécessaire et suffisante d'existence d'un tel numérateur est donnée par des équations portant sur les coordonnées de D_2.

Ceci fournit un schéma affine S_{D_1} dont chaque k-point paramètre un diviseur D_2 tel que $n(D_1+D_2)$ soit principal. Soit S le coproduit des S_{D_1}. Alors chaque classe de diviseurs de n-torsion contient au moins un diviseur décrit par un point de S. Le morphisme $S \to J[n]$ qui à un diviseur associe sa classe est constant sur chaque composante irréductible ; il suffit donc de trouver un point dans chaque composante pour obtenir un diviseur de chaque classe.

Remarque 4.3.5. Cet algorithme peut également s'adapter, comme nous le verrons, à la recherche des racines n-ièmes dans $\mathrm{Pic}^0(X)$ d'un diviseur de degré zéro F fixé : il convient de construire un diviseur très simple équivalent à $n(D - g\infty) - F$, où $D = D_1 + D_2$ avec D_2 décrit par des indéterminées.

IV.3.2 Construction d'un diviseur très simple

IV.3.2.1 Pour un diviseur connu

Voici comment déterminer un diviseur très simple équivalent à un diviseur donné $n(D - g\infty)$. Soit $P \in |D|$: c'est un point de X, dont l'image dans C est peut-être singulière. Soit $f\colon C'_P \to C$ un morphisme birationnel tel que P corresponde au point régulier $(0, 0)$ de C'_P ; il se construit par transformée quadratique. Choisissons des éléments $r_1, \ldots, r_n$ deux à deux distincts de k. Supposons donné un ensemble fini S_P de points "à éviter" de C'_P. Soit $a_P \in k$ tel que les droites L_i d'équation $y = (r_i + a_P)x$ vérifient :

- Chaque L_i intersecte C'_P seulement en des points réguliers et non terribles dont l'image par f a un unique antécédent
- Chaque droite L_i intersecte C'_P en $\deg(C'_P)$ points affines
- $L_i \cap S_P = \varnothing$

Les deux premiers points assurent que le diviseur $\mathrm{div}(L_i) - (0,0)$ est très simple sur C'_P, et que son image dans C est encore très simple. Le troisième point assure que le support de ce diviseur sur C'_P ne contient aucun point de S_P. Un tel a_P vérifie que le diviseur du produit $L_P := L_1 \cdots L_n$ sur la partie affine de C'_P est égal à $nP + A_P$, où A_P est un diviseur effectif très simple dont le support est disjoint de $S_P \cup \{P\}$.

Pour construire un diviseur très simple équivalent à $n(D - g\infty)$ où $D = D_1 + D_2$ comme précédemment, Huang et Ierardi commencent par appliquer cette procédure à D_1. Posons $T = |D_2|$ et pour un premier point $P \in |D_1|$, $S_P = (C'_P \to C)^{-1}T$. Ceci donne un produit L_P tel que $\mathrm{div}(L_P) = nP + A_P \in \mathrm{Div}(C'_P \cap \mathbb{A}^2)$ avec A_P effectif très simple. Pour chaque P, ils appliquent ensuite la procédure au point $\infty \in C'_P$, en remplaçant S par $(S \cup |A_P|) - \{\infty\}$. Ceci fournit un polynôme L'_P de diviseur $n\infty + B_P$. Le diviseur de la fonction rationnelle $\frac{L_P}{L'_P}$ est alors $nP - n\infty + A_P - B_P$. Le diviseur très simple $A_P - B_P$ est équivalent à $nP - n\infty$, et son support disjoint de celui de D. Pour passer au point P suivant, il suffit de remplacer T par $T \cup |A_P - B_P|$. Cette construction donne un diviseur $D'_1 = D'^{+}_1 - D'^{-}_1$ équivalent à $n(D_1 - \deg(D_1)\infty)$.

Pour D_2, la procédure est plus simple : nul besoin de courbes C'_P, puisque les points du support de D_2 sont déjà réguliers. L'ensemble S considéré pour chaque $P \in |D_2|$ est $|D'_1| \cup |D_2| - |P|$. Pour le point ∞, la même procédure est appliquée avec $S = |D'_1| \cup |D_2| - \{\infty\}$.

Remarque 4.3.6. Soit F un diviseur de degré 0 sur X. Supposons qu'il est de la forme $D_F - g\infty$. Afin de trouver un diviseur très simple équivalent à $n(D - g\infty) + F$, la procédure ci-dessus peut être appliquée à D_F (en cherchant une seule droite pour chaque $P \in |D_F|$ et non pas n) pour le rendre très simple, puis à D en ajoutant à chaque ensemble S_P les points du support de F.

IV.3.2.2 Pour un diviseur indéterminé

Fixons un diviseur D_1 de degré $d_1 \leqslant g$ dont le support ne contient que des points singuliers ou terribles de C. Notons $d_2 = g - d_1$. L'algorithme cherchant les D_2 tels que $D_1 + D_2 - g\infty$ soit de n-torsion procède de la façon suivante. Soit $|D_2|$ un ensemble de d_2 éléments, qui représente moralement le support du diviseur D_2 cherché. Fixons deux familles $(r_{P,i})_{P \in |D_2|, 1 \leqslant i \leqslant n} \in k^{nd_2}$ et $(r_{P,\infty,i})_{P \in |D_2|, 1 \leqslant i \leqslant n} \in k^{nd_2}$ d'éléments de k deux à deux distincts. Fixons également un ensemble $\mathcal{A} \subset k^{d_2+1}$ de familles $a = (a_P)_{P \in |D_2| \cup \{\infty\}}$. Ces deux ensembles serviront à paramétrer des droites passant par les points de $|D_2|$. Soit $a \in \mathcal{A}$. Soient d_2 triplets d'indéterminées $(x_P, y_P, z_P)_{P \in |D_2|}$, qui représentent les points de D_2. Nous noterons $k(D_2)$ le corps $k((x_P, y_P, z_P)_{P \in |D_2|})$.

Notons, pour tout $i \in \{1 \dots n\}$ et tout $P \in |D_2|$, $L_{P,i} = (y - y_P z) - (r_{P,i} + a_P)(x - x_P z) \in k(D_2)[x, y, z]$, et $L_{P,\infty,i} = (y - y_\infty z) - (r_{P,\infty,i} + a_\infty)(x - x_\infty z)$. Supposons, quitte à changer $\mathcal{A}$, que pour tout $Q \in |D'_1| \cup \mathrm{Sing}(C)$, $L_{P,\infty,i}(x_Q, y_Q, z_Q) \neq 0$. Considérons les conditions suivantes sur ces indéterminées :

- pour tout point singulier ou terrible $Q = (x_Q, y_Q, z_Q)$ de C, pour tout $i \in \{1 \dots n\}$, pour tout $P \in |D_2|$, $L_{P,i}(x_Q, y_Q, z_Q) \neq 0$;
- pour tout point $Q \in |D'_1|$ (déjà calculé explicitement), pour tout $i \in \{1 \dots n\}$, pour tout $P \in |D_2|$, $L_{P,i}(x_Q, y_Q, z_Q) \neq 0$;

- pour tout $P \in |D_2|$, pour tout $i \in \{1 \dots n\}$, $L_{P,\infty,i}(x_P, y_P, z_P) \neq 0$;
- pour tous $i, j \in \{1 \dots n\}$, pour tous $P \neq P' \in |D_2|$, le point d'intersection des droites d'équations $L_{P,i}$ et $L_{P',j}$ n'est pas un zéro du polynôme f qui définit C ;
- pour tout $i \in \{1, \dots, n\}$ et tout $P \in |D_2|$, la droite d'équation $L_{P,i}$ n'est pas tangente à C.

La dernière condition se vérifie de la façon suivante : les abscisses des points d'intersection de la droite $L_{P,i}$ avec C dans le plan affine $\mathbb{A}^2 = \operatorname{Spec} k(D_2)[x, y]$ sont les racines du polynôme $f(x, y_P + (r_{P,i} + a_P)(x - x_P)) \in k(D_2)[x]$. Les points P pour lesquels $L_{P,i}$ est tangente à C en un point sont ceux tels que le discriminant de ce polynôme s'annule. La condition est donc $\operatorname{discr}(f(x, y_P + (r_{P,i} + a_P)(x - x_P)) \neq 0$. Une condition semblable est imposée pour l'ouvert affine $\operatorname{Spec} k(D_2)[x, z]$.

Ces inéquations définissent, pour chaque $a \in \mathcal{A}$, un ouvert S_a de $\mathbb{A}_k^{3d_2}$ qui paramètre les diviseurs D_2 tels que pour ce a fixé, les droites $L_{P,i}$ d'équation $y - y_P z = (r_{P,i} + a_P)(x - x_P z)$ vérifient les trois conditions mentionnées précédemment, et permettent donc de remplacer $n(D - g\infty)$ par un diviseur très simple qui lui est équivalent. En effet, soient $L_0 = \prod_{P,i} L_{P,i}$ et $L_\infty = \prod_{P,i} L_{P,\infty,i}$: alors le diviseur $\operatorname{div}(\frac{L_0}{L_\infty}) - n(D_2 - d_2\infty)$ est un diviseur très simple $B = B^+ - B^-$. Par conséquent, $A = B + D_1'$ est linéairement équivalent à $n(D - g\infty)$. Notons $A = A^+ - A^-$. Alors $A^+ = B^+ + D_1'^+$, et $A^- = B^- + D_1'^-$.

Remarque 4.3.7. Si l'ensemble $\mathcal{A}$ est assez grand (de taille $O(n^2 g^2 d)$, voir [HI98, 4.2, p12]), alors chaque diviseur de $\operatorname{Div}^0 X$ est paramétré par un point de l'un des $S_a, a \in \mathcal{A}$.

Remarque 4.3.8. La méthode décrite dans cette section fonctionne tout aussi bien, étant donné un diviseur F de degré nul, pour remplacer $n(D_1 + D_2 - g\infty) + F$ par un diviseur très simple. Construisons d'abord F' très simple équivalent à F, comme décrit précédemment. Ajoutons $|F'|$ à l'ensemble S utilisé pour construire les équations. Finalement, ajoutons F' au diviseur A. Ceci donne un diviseur très simple équivalent à $n(D - g\infty) + F$. Cette construction ajoute $O(n)$ équations et inéquations et n'altère donc pas la complexité globale de l'algorithme.

IV.3.3 Construction d'une fonction de diviseur très simple

La partie précédente a permis de déterminer une fonction $\frac{L_0}{L_\infty}$ telle que $A = \operatorname{div}(\frac{L_0}{L_\infty}) - n(D - g\infty)$ soit très simple. Il reste à tester s'il existe une fonction $\frac{G_0}{G_\infty}$ dont A est le diviseur. Pour ce faire, la procédure classique de l'algorithme de Brill-Noether commence par construire un dénominateur G_∞ (explicitement, en fonction des indéterminées x_P, y_P, z_P pour $P \in |D_2|$) qui vérifie que A est principal si et seulement s'il existe un numérateur G_0 tel que $\operatorname{div}(\frac{G_0}{G_\infty}) = A$. Des conditions nécessaires et suffisantes pour l'existence de ce numérateur sont ensuite déterminées. Rappelons que $Q_1, \dots, Q_r$ sont les points singuliers de C. Notons $m_1, \dots, m_r$ leurs multiplicités respectives. Pour chaque Q_i, notons $Q_{i,1}, \dots, Q_{i,m_i}$ les points de X au-dessus de Q_i. Définissons pour la suite le diviseur

$$E = \sum_{i=1}^{r} \sum_{j=1}^{m_i} (m_i - 1) Q_{ij}.$$

IV.3.3.1 Construction du dénominateur

Soit $H \in k[x, y, z]$ un polynôme homogène tel que $\operatorname{div}(H) - E$ soit effectif et très simple. Un tel polynôme se construit explicitement en choisissant, pour chaque point singulier Q_i, $m_i - 1$ droites passant par Q_i avec multiplicité m_i qui intersectent C en $d - m_i$ autres points, et en considérant le produit de toutes les formes linéaires définissant ces droites. Pour les détails, voir [HI98, §4.3,p13]. Notons $A_e = \operatorname{div}(H) - E$. Supposons avoir calculé H avant la section précédente, et avoir ajouté $|\operatorname{div}(H)|$ à chaque ensemble S de points à éviter dans la section précédente. Par construction, le degré de H est inférieur à $\deg(E)d \leqslant d^4$: ceci n'altère pas la complexité globale de l'algorithme, et permet d'assurer

que $|\mathrm{div}(H)|$ soit disjoint de $|A|$. Supposons fixés les $a_P, r_{P,i} \in k$, les droites $L_{P,i} \in k(D_2)[x,y,z]$ et enfin les polynômes $L_0, L_\infty \in k(D_2)[x,y,z]$ comme ci-dessus. Rappelons que $\mathrm{div}(L_\infty) = B^- + nd_2\infty$, où B^- est la partie négative du diviseur $\mathrm{div}(\frac{L_0}{L_\infty}) - n(D_2 - d_2\infty)$.

Soit $U \in k(D_2)[u_x, u_y, u_z]$ le u-résultant de f et L_∞ (voir annexe C.3.1). Il vérifie

$$U = \prod_{P \in |B^-| \cup \{\infty\}} (x_P u_x + y_P u_y + z_P u_z) = (x_\infty u_x + y_\infty u_y + z_\infty u_z)^{nd_2} R_B(u_x, u_y, u_z).$$

Comme les coordonnées du point ∞ sont connues, il est possible de calculer explicitement R_B, et en particulier $R_B(-z,0,x) = \prod_{P \in |B^-|}(x - x_P z)$. La même procédure appliquée à $D_1'^-$ fournit $R_D(-z,0,x) = \prod_{P \in |D_1'^-|}(x - x_P z)$. Posons $R(x,y,z) = R_B(-z,0,x)R_D(-z,0,x)$. Supposons que $\mathrm{div}(R)$ soit très simple et que son support soit disjoint de $A^+ + A_e$, et définissons $G_\infty := HR$. Alors le diviseur de G_∞ est supérieur à $A^- + E + A_e$, et s'écrit

$$\mathrm{div}(G_\infty) = A^- + E + A_e + M$$

avec $M + A_e$ très simple.

Proposition 4.3.9. [HI98, Th. 4.1] Soient $D, D' \in \mathrm{Div}(C)$ deux diviseurs. Soit $G_\infty \in k[x,y,z]$ un polynôme homogène tel que $\mathrm{div}(G_\infty) \geqslant E$. Notons $F = \mathrm{div}(G_\infty) - D - E$. Alors D est équivalent à D' si et seulement s'il existe un polynôme homogène $G_0 \in k[x,y,z]$ tel que $\mathrm{div}(G_0) \geqslant E$ et $\mathrm{div}(G_0) = D' + E + F$.

Rappelons que dans notre situation, $A = A^+ - A^-$ est un diviseur équivalent à $n(D - g\infty)$, et le polynôme G_∞ vérifie $\mathrm{div}(G_\infty) = A^- + E + A_e + M$. Le diviseur $n(D - g\infty)$ est principal si et seulement si A^+ est équivalent à A^-. La proposition affirme, en prenant $F = A_e + M$, $D = A^+$ et $D' = A^-$, que $n(D - g\infty)$ est principal si et seulement s'il existe un polynôme homogène $G_0 \in k[x,y,z]$ tel que $\mathrm{div}(G_0) \geqslant E$ et $\mathrm{div}(G_0) = A^+ + E + A_e + M$.

Remarque 4.3.10. Ci-dessus, le diviseur de R était supposé très simple. Il peut toujours être rendu très simple par un automorphisme de $\mathbb{P}^2$ dont la restriction à $\mathbb{A}^2 = \mathrm{Spec}\, k[x,y]$ est de la forme $(x,y) \mapsto (ax+by, y)$. Un tel automorphisme se trouve toujours en considérant un ensemble Φ d'automorphismes assez grand (de taille $O(dgn)$, cf [HI98, 4.3, p14]).

IV.3.3.2 Existence d'un numérateur

Il reste à donner une condition nécessaire et suffisante sur $(x_P, y_P, z_P)_{P \in |D_2|}$ pour qu'il existe un polynôme homogène $G_0 \in k[x,y,z]$ de même degré que G_∞ tel que $\mathrm{div}(G_0) \geqslant E$ et

$$\mathrm{div}(G_0) = A^+ + E + A_e + M.$$

Le polynôme G_0 est défini par ses coordonnées dans la base canonique du k-espace vectoriel des polynômes homogènes de degré $\deg G_\infty$. Il suffit, au vu de la contrainte sur son degré, de montrer que G_0 est supérieur à la fois à E, à A^+ et à $A_e + M$.

Condition 1 : $\mathrm{div}(G_0) \geqslant E$ Cette condition est équivalente à ce que la multiplicité de G_0 en chaque point singulier Q_i soit supérieure à $m_i - 1$ [HI98, Lem. 4.2], ce qui se décrit par l'annulation de certaines formes linéaires en les coefficients de G_0 [HI98, Lem. 4.3].

Condition 2 : $\operatorname{div}(G_0) \geqslant A^+$ Souvenons-nous que $A^+ = B^+ + D_1'^+$, où D_1' est un diviseur explicitement connu, et $B^+ = \operatorname{div}(L_0) - nD_2$ est un diviseur indéterminé, où L_0 est un produit de polynômes homogènes de degré 1 dans $k(D_2)[x, y, z]$. L'annulation de G_0 en les points du support de $D_1'^+$ se traduit par des équations linéaires en ses coefficients. Soit maintenant $L_{P,i}$ une des formes linéaires qui divisent L_0 ; pour simplifier l'exposition, supposons qu'il s'agit de la droite $y = mx$. Le diviseur de $L_{P,i}$ a $\deg(f)$ points sur la partie affine de C. Alors le diviseur de G_0 est supérieur à $\operatorname{div}(L_{P,i}) - P$ si et seulement si les polynômes $G_0(t, mt, 1)$ et $f(t, mt, 1)$ ont $\deg(f) - 1$ zéros en commun, c'est-à-dire s'ils ont un facteur commun de degré $d - 1$. Ceci revient à demander qu'il existe un polynôme $h(t) \in k(D_2)[t]$ de degré $\deg(G_0) - \deg(f) + 1$ tel que $tG_0(t, mt, 1) - h(t)f(t, mt, 1) = 0$, ce qui se traduit par un système linéaire en les coefficients de G_0.

Condition 3 : $\operatorname{div}(G_0) \geqslant A_e + M$ Un paramétrage rationnel du support de M (resp. A_e) permet de s'assurer que G_0 s'annule en chaque point de M (resp. A_e). Il s'obtient en construisant un polynôme $Q \in k(D_2)[t]$ et des fonctions rationnelles $r, s \in k(D_2)(t)$ tels que les $\overline{k(D_2)}$-points de M (resp. A_e) soient les $(r(\theta), s(\theta))$ où $\theta \in \overline{k(D_2)}$ parcourt les racines de Q. Pour les détails, voir [HI98, Lem. 4.4] et [Can88, Lem. 2.2]. Alors G_0 s'annule sur le support de M si et seulement si $G_0(r(t), s(t))$ s'annule sur les zéros de Q. Réduisons les fractions r et s au même dénominateur, et considérons leurs numérateurs respectifs r', s'. Notons $G_0'(t) = G_0 \circ (r', s') \in k(D_2)[t]$. La fonction G_0 s'annule sur $|M|$ si et seulement s'il existe $I' \in k(D_2)[t]$ de degré $\deg(G_0) - \deg(Q)$ tel que $G_0' = I'Q$. Ceci se traduit encore par un système linéaire en les coefficients de I' et G_0. De même, la condition $\operatorname{div}(G_0) \geqslant A_e$ se traduit par l'existence d'un I'' solution d'un certain système linéaire.

Résumé La mise bout à bout de ces systèmes linéaires fournit une matrice T à coefficients dans $k(D_2)$ telle que G_0 soit un numérateur convenable si et seulement si (G_0, I', I'') est un élément non trivial du noyau de T. Par conséquent, le diviseur D_2 vérifie que $n(D_1 + D_2 - g\infty)$ est principal si et seulement si le rang de T n'est pas maximal, ce qui se traduit par des équations en les $(x_P, y_P, z_P)_{P \in |D_2|}$.

En résumé, l'algorithme détermine pour chaque diviseur D_1 de degré inférieur à g de support inclus dans $\operatorname{Sing}(C)$, chaque transformation projective $\phi \in \Phi$ (voir remarque 4.3.10) et chaque $a \in \mathcal{A}$ (voir début de la section IV.3.2.2), une partie constructible $S_{D_1,\phi,a}$ de l'espace affine $\mathbb{A}^{3(g-\deg D_1)} = \operatorname{Spec} k[x_P, y_P, z_P; P \in |D_2|]$ et un morphisme

$$\begin{aligned} S_{D_1,\phi,a} &\to J_X[n] \\ D_2 &\mapsto D_1 + D_2 - g\infty. \end{aligned}$$

Chaque diviseur de n-torsion est équivalent à un diviseur de la forme $D_1 + D_2 - g\infty$, où D_2 appartient à l'un des S_{D_1}. Par conséquent, en notant $S = \bigsqcup_{D_1,\phi,a} S_{D_1,\phi,a}$, il y a un morphisme surjectif $f \colon S \to J_X[n]$ qui s'insère dans le diagramme commutatif

$$\begin{tikzcd} S \arrow[r] \arrow[d, "f"'] & C^g \arrow[r] & C^{(g)} \arrow[d, "D \mapsto D - g\infty"] \\ J_X[n] \arrow[rr] & & J_X \end{tikzcd}$$

IV.3.4 Détermination de $J_X[n]$

IV.3.4.1 Détermination de représentants des classes de diviseurs

Pour chaque diviseur D_1 de degré g, chaque transformation projective $\phi \in \Phi$ (voir remarque 4.3.10) et chaque $a \in \mathcal{A}$ (voir début de la section IV.3.2.2), il y a une application $S_{D_1,\phi,a} \to J_X[n]$,

$D_2 \mapsto D_1 + D_2 - g\infty$. Chaque diviseur de n-torsion est équivalent à un diviseur de la forme $D_1 + D_2$, avec $D_2 \in S_{D_1}$. Ceci définit une application surjective $f\colon \bigsqcup_{D_1} S_{D_1} \to J_X[n]$.

Lemme 4.3.11. Soit $f\colon X \to Y$ une application continue entre espaces topologiques. Si Y est discret alors f est constante sur chaque composante connexe.

Démonstration. L'image d'une partie connexe par une application continue est connexe. Comme Y est discret, ses composantes connexes sont des points. □

L'application $f\colon S = \bigcup_{D_1,\phi,a} S_{D_1,\phi,a} \to J_X[n]$ est donc surjective et constante sur chaque composante irréductible. Par conséquent, pour trouver tous les éléments de $J_X[n]$, il suffit de trouver au moins un point de chaque composante irréductible de S.

Dans la suite, la notation $\mathcal{P}(d, g, n)$ sera employée génériquement pour remplacer des polynômes en d, g, n à coefficients réels : le polynôme exact caché derrière la notation $\mathcal{P}$ pourra varier. Chaque $S_{D_1,\phi,a} \subset \mathbb{A}^{3g}$ est défini par un nombre d'équations et d'inéquations polynomial en d, g, n ; le degré de chacune de ces (in)équations est également polynomial en d, g, n. Par conséquent, la complexité totale du calcul d'un élément de chaque composante irréductible à l'aide de l'algorithme décrit dans l'annexe B.4.2.2 est $\mathcal{P}(d, g, n)^{O(g^3)} + 3g\,\mathrm{Fact}(\mathcal{P}(d, g, n))$, où Fact désigne la complexité de la factorisation absolue d'un polynôme de $k_0[t]$ de degré donné. De plus, le nombre de points trouvés est $\mathcal{P}(d, g, n)^{O(g^2)}$, et chaque point est défini sur une extension de k_0 de degré $n^{O(g^3)}$. Enfin, le nombre de valeurs de Φ et de a à considérer est polynomial en d, g, n, et le nombre de diviseurs D_1 à considérer est $O(n^{2g})$. Au total, la complexité de cet algorithme est donc $\mathcal{P}(d, g, n)^{O(g^3)} + \mathcal{P}(d, g, n)\,\mathrm{Fact}(k_0, \mathcal{P}(d, g, n))$.

IV.3.4.2 Calcul de $J_X[n]$ et de sa loi de groupe

L'algorithme précédent a permis de trouver un ensemble T de $\mathcal{P}(d, g, n)^{O(g^2)}$ diviseurs, tel que chaque élément de $\mathrm{Pic}^0(X)[n]$ soit la classe d'un diviseur de T. L'algorithme choisit $D^1 \in T$ et pose $J = \{D^1\}$. Puis, pour chaque diviseur $D \in T$, il vérifie s'il est équivalent à un diviseur $D' \in J$; si non, il remplace J par $J \cup \{D'\}$. Au total, il vérifie pour $|T|$ diviseurs s'ils sont équivalents à $O(n^{2g})$ diviseurs. Il y a donc $\mathcal{P}(d, g, n)^{O(g^2)}$ vérifications à faire. Chacune de ces vérifications nécessite seulement de construire une extension de corps sur laquelle sont définis les deux diviseurs.

Afin de vérifier si deux diviseurs de degré zéro D, D' sont équivalents, il suffit de calculer l'espace de Riemann-Roch $\mathcal{L}(D - D') = \mathrm{H}^0(X, \mathcal{O}_X(D - D'))$ et de tester s'il est nul. Comme les diviseurs en question sont de la forme $D - g\infty$, ce calcul se fait en temps $O(g^7 d^{14})$ (voir annexe C.3.2). Ce processus fournit exactement un représentant de chaque classe de $J_X[n]$ en temps $\mathcal{P}(d, g, n)^{O(g^2)}$.

Notons $D^1, \ldots, D^{n^{2g}}$ les diviseurs obtenus. L'addition dans J de deux classes de diviseurs D^i et D^j se fait en calculant le diviseur $D^i + D^j$ puis en vérifiant pour chaque indice ℓ si $D^i + D^j$ est équivalent à D^ℓ, c'est-à-dire si $\mathcal{L}(D^i + D^j - D^\ell)$ contient un élément non nul. La complexité totale de cette opération est $O(n^{4g} g^7 d^{14})$.

IV.3.5 Complexité sur $\mathbb{F}_q(t)$

La construction du schéma S paramétrant les diviseurs de n-torsion est parfaitement indépendante du corps de base k_0, et peut être réalisée sur n'importe quel corps calculable. Le calcul des points dans les composantes connexes demande simplement de disposer d'un algorithme de factorisation absolue des polynômes à coefficients dans k_0.

Intéressons-nous à la complexité de cet algorithme dans le cas où $k_0 = \mathbb{F}_q(t)$ et les points Q_{ij} au-dessus des points singuliers ou terribles du modèle plan de X sont tous définis sur $\mathbb{F}_q(t)$. C'est

une restriction très forte, mais elle permet d'obtenir rapidement une évaluation de la complexité de l'algorithme. Étant donné $f = \frac{a}{b} \in k_0$ avec $a, b \in \mathbb{F}_q[t]$ premiers entre eux, définissons sa hauteur par $h(x) = \max(\deg_t a, \deg_t b)$. Notons D la hauteur maximale des coefficients de l'équation F de la courbe C, et des points Q_{ij}. Une transformation quadratique ne change pas la hauteur des coefficients. En supposant toujours q assez grand ($d^6 < q$ et $n = O(g \log q)$), il est possible de choisir pour l'ensemble $\mathcal{A}$ une partie de $\mathbb{F}_q$. Les coefficients des équations de S sont obtenus par produit d'un nombre polynomial en d, g, n d'éléments de $\mathcal{A}$, de coordonnées des points Q_{ij} et de coefficients de F ; la hauteur de ces coefficients est alors polynomiale en D, d, g, n. Par conséquent, le calcul d'éléments de chaque composante irréductible de S à l'aide de l'algorithme probabiliste de factorisation dans $\mathbb{F}_q(t)[s]$ présenté dans l'annexe A.2.3.2 nécessite $\mathcal{P}(D, d, g, n)^{O(g^3)} + \mathcal{P}(D, d, g, n) \log(q)$ opérations.

IV.4 L'algorithme de Jin

IV.4.1 Données et structure de l'algorithme

Cet algorithme calcule les groupes de cohomologie d'un faisceau lisse sur une courbe lisse sur un corps algébriquement clos. C'est le seul algorithme existant qui effectue cette tâche pour les faisceaux lisses en un nombre d'opérations borné explicitement. Cependant, il n'est pas utilisable dans la pratique en raison du grand nombre de variables en jeu.

IV.4.1.1 Données

Soient k_0 un corps parfait et k une clôture algébrique de k_0. Soit X une courbe projective lisse sur k_0. Elle est représentée comme décrit dans l'annexe C.1.3.1, c'est-à-dire par une $\mathcal{O}_{\mathbb{P}^1}$-algèbre $\mathcal{E}$ telle qu'il existe un morphisme $\phi\colon X \to \mathbb{P}^1$ avec $\phi_\star \mathcal{O}_X = \mathcal{E}$. Cette algèbre est définie par des entiers $a_1, \ldots, a_r$ tels que $\mathcal{E} \simeq \mathcal{O}_{\mathbb{P}^1}(a_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(a_r)$, la matrice $M \in \mathrm{Mat}_{r \times r^2}(k_0[x, y])$ qui décrit la multiplication sur $\mathcal{E}$, et la matrice $I \in \mathrm{Mat}_{1 \times r}(k_0[x, y])$ qui décrit le morphisme structural $\mathcal{O}_{\mathbb{P}^1} \to \mathcal{E}$.

Le faisceau lisse $\mathcal{F}$ est décrit par la donnée d'un revêtement galoisien $f\colon Y \to X$ (lui-même représenté comme $\mathcal{O}_{\mathbb{P}^1}$-algèbre) qui le trivialise, du groupe G du revêtement, et du G-module $F := \mathrm{H}^0(Y, f^\star \mathcal{F})$. D'après le corollaire 1.4.5, la catégorie des $\mathcal{F}$-torseurs sur X est équivalente à celle des F-torseurs sur Y munis d'une action de G telle que l'action de F soit G-équivariante.

Les F-torseurs $T \to Y$ cherchés sont décrits de la même manière, par des entiers $b_1, \ldots, b_s$, une matrice de multiplication $N \in \mathrm{Mat}_{s \times s^2}(k_0[x, y])$ et une matrice $J \in \mathrm{Mat}_{1 \times s}(k_0[x, y])$ avec quelques données supplémentaires. Le morphisme $T \to Y$ est donné par une matrice $S \in \mathrm{Mat}_{s \times r}(k_0[x, y])$. L'action du groupe G est décrite par des matrices $\Phi_g \in \mathrm{Mat}_{s \times s}(k_0[x, y])$, où g parcourt G. De même, l'action du groupe F est décrite par des matrices $\Psi_f \in \mathrm{Mat}_{s \times s}(k_0[x, y])$, où f parcourt F. Ces matrices vérifient des égalités traduisant le fait qu'elles définissent une action, ainsi que la G-équivariance de l'action de F (voir section IV.4.3).

IV.4.1.2 Résumé de l'algorithme

L'algorithme construit un schéma paramétrant tous les $\mathcal{F}$-torseurs sur X, de façon à ce que les composantes connexes de ce schéma soient en bijection avec les classes d'isomorphisme de $\mathcal{F}$-torseurs sur X.

Il commence par sélectionner un nombre fini de $b = (b_i)$ possibles pour les torseurs T envisagés, déterminés par les conditions $b_i \leqslant 0$ [Jin20, Lem. 6.17] et $\sum_i b_i = |G| \cdot \sum_j a_j$ (voir le corollaire 4.4.9).

Pour chacun de ces b, l'algorithme écrit les équations que la $\mathcal{O}_{\mathbb{P}^1}$-algèbre $\mathcal{O}_T$, munie des actions de F et G, vérifie si et seulement si $T \to Y$ est un F-torseur G-équivariant. Ceci donne un fermé $\mathcal{U}_b$ d'un espace affine sur k_0. Il se trouve que les composantes connexes de $\mathcal{U}_b$ sont irréductibles, et en bijection $\mathrm{Gal}(k|k_0)$-équivariante avec les classes d'isomorphisme de F-torseurs sur Y (voir la proposition 4.4.19).

Il suffit alors de trouver un point dans chaque composante irréductible de chaque $\mathcal{U}_b$ afin d'obtenir $\mathrm{H}^1(X, \mathcal{F})$ comme $\mathrm{Gal}(k|k_0)$-ensemble.

IV.4.2 Conditions pour être un torseur

Rappelons qu'un F-torseur sur un schéma Y est un Y-schéma étale T tel que le morphisme $F \times T \to T \times T$ soit un isomorphisme. Les morphismes $T \to Y$ considérés sont toujours plats, c'est-à-dire localement libres. L'étalitude de $T \to Y$ se vérifie en deux étapes : tout d'abord, une condition nécessaire pour qu'un morphisme localement libre soit étale est que son rang soit constant. Ensuite, une condition nécessaire et suffisante portant sur les morphismes de rang constant garantit l'étalitude.

IV.4.2.1 Rang constant

Lemme 4.4.1. [Jin17, Lem. 3.49] Soit S un schéma. Soit X un $\mathbb{P}^1_S$-schéma fini localement libre, et lisse sur S. Soit T un X-schéma fini localement libre sur $\mathbb{P}^1_S$. Alors T est un X-schéma fini localement libre.

Lemme 4.4.2. Soient S un schéma, et $f\colon X \to \mathbb{P}^1_S$ un morphisme fini localement libre de S-schémas. Alors la restriction de f à toute composante connexe de X est surjective.

Démonstration. Ceci se vérifie fibre à fibre sur S : il suffit de traiter le cas où S est le spectre d'un corps K. Soit Y une composante connexe de X. Le morphisme $f|_Y\colon Y \to \mathbb{P}^1_K$ est fini localement libre, donc $\dim_K Y = \dim_K X = 1$. De même, par finitude de f, $\dim f(Y) = \dim Y = 1$. Enfin, comme f est fini, il est fermé, donc $f(Y)$ est un fermé de $\mathbb{P}^1_K$ de dimension 1 : $f(Y) = \mathbb{P}^1_K$. Par conséquent, $f|_Y$ est surjectif. □

Lemme 4.4.3. Soient S un schéma et $f\colon T \to X$, $g\colon X \to \mathbb{P}^1_S$ deux morphismes de S-schémas finis localement libres. Supposons que le morphisme $f_0\colon T_0 \to X_0$ entre les fibres au-dessus de $0 \in \mathbb{P}^1_S(S)$ est fini localement libre de rang constant r. Alors f est fini localement libre de rang constant r.

Démonstration. Soit Y une composante connexe de X. Alors $f|_Y\colon T|_Y Y \to Y$ est localement libre de rang constant un entier d. Montrons que $d = r$. Notons $Y_0 = Y \times_{\mathbb{P}^1_S} 0$: c'est un schéma non vide par le lemme précédent. Alors $T_0 \times_X Y_0$ peut s'écrire comme le tiré en arrière de $T_0 \to X_0$ par $Y \to X$, mais aussi comme le tiré en arrière de $f|_Y\colon T|_Y \to X$ par $0 \to \mathbb{P}^1_S$, ce qui implique que $r = d$. □

Les morphismes $T \to Y$ qui sont de rang constant $m = |G|$ sont donc définis par la donnée supplémentaire d'un isomorphisme de $\mathcal{O}_{Y_0}$-modules $\mathcal{O}_{T_0} \xrightarrow{\sim} \mathcal{O}_{Y_0}^m$. L'évaluation de la matrice de multiplication de $\mathcal{O}_T$, à coefficients dans $k_0[x, y]$, en $x = 0$ et $y = 1$ permet de déduire $\mathcal{O}_{T_0}$ de $\mathcal{O}_T$. En particulier, ceci fournit la matrice N_0 de la multiplication sur le k_0-espace vectoriel $\mathcal{O}_{T_0}$. La matrice M_0 de multiplication sur $\mathcal{O}_{Y_0}$ se détermine de la même façon. La structure de $\mathcal{O}_{Y_0}$-module sur $\mathcal{O}_{T_0}$ est obtenue en évaluant de même la matrice du morphisme $\mathcal{O}_Y \to \mathcal{O}_T$. Un isomorphisme de $\mathcal{O}_{X_0}$-modules $\mathcal{O}_{T_0} \xrightarrow{\sim} \mathcal{O}_{Y_0}^m$ est un isomorphisme de k_0-espaces vectoriels compatible à l'action de $\mathcal{O}_{Y_0}$. Il est donc défini par une matrice $B \in \mathrm{Mat}_{sm \times sm}(k_0)$ à coefficients dans k_0, où $s = \deg(Y \to \mathbb{P}^1)$. Notons F_0 la matrice du morphisme $\mathcal{O}_{Y_0} \to \mathcal{O}_{T_0}$, obtenue en évaluant la matrice de $\mathcal{O}_X \to \mathcal{O}_T$ en $x = 0$ et $y = 1$. La condition de $\mathcal{O}_{Y_0}$-linéarité est la commutativité du diagramme suivant.

$$\begin{tikzcd}
\mathcal{O}_{Y_0} \otimes_{k_0} \mathcal{O}_{Y_0}^m \arrow[r, "I_s \otimes B"] \arrow[d, "I_n \otimes M_0"'] & \mathcal{O}_{Y_0} \otimes_{k_0} \mathcal{O}_{T_0} \arrow[d, "N_0(F_0 \otimes B)"] \\
\mathcal{O}_{Y_0}^m \arrow[r, "B"'] & \mathcal{O}_{T_0}
\end{tikzcd}$$

IV.4.2.2 Discriminant

Rappelons que le déterminant d'un module localement libre $\mathcal{E}$ de rang r sur un schéma X est le faisceau inversible $\wedge^r\mathcal{E}$. Un morphisme de modules localement libres de même rang $E \to E'$ induit un morphisme $\det\mathcal{E} \to \det\mathcal{E}'$, qui est localement la multiplication par une section de $\mathcal{O}_X$.

Définition 4.4.4. Soit $f\colon Y \to X$ un morphisme fini localement libre. Le morphisme composé $f_\star\mathcal{O}_Y \otimes_{\mathcal{O}_X} f_\star\mathcal{O}_Y \to f_\star\mathcal{O}_Y \xrightarrow{Tr} \mathcal{O}_X$ définit un morphisme $\phi\colon f_\star\mathcal{O}_Y \to \mathrm{Hom}_{\mathcal{O}_X}(f_\star\mathcal{O}_Y, \mathcal{O}_X)$. Le déterminant de ϕ est un faisceau d'idéaux principaux sur X appelé discriminant de f et noté Δ_f.

Proposition 4.4.5. [Stacks, 0BVH, 49.3.1] Un morphisme fini localement libre $f\colon Y \to X$ de schémas est étale si et seulement si $\Delta_f \simeq \mathcal{O}_X$.

Proposition 4.4.6. [Jin20, Cor. 6.8] Soient $g\colon T \to Y$, $f\colon Y \to W$ des morphismes finis localement libres de rang constant. Notons r le rang de g. Alors g est étale si et seulement si $\det_{\mathcal{O}_W}\mathcal{O}_T \simeq (\det_{\mathcal{O}_W}\mathcal{O}_Y)^{\otimes r}$ et $\Delta_{f\circ g}$ et $\Delta_f^{\otimes r}$ diffèrent d'un élément de $\mathcal{O}_W^\times$.

Dans la situation qui nous concerne, $W = \mathbb{P}^1_S$, le schéma Y est une courbe projective lisse, et T est un Y-schéma dont l'étalitude est à vérifier. Voici comment calculer le discriminant Δ_f d'un morphisme $f\colon Y \to \mathbb{P}^1_{k_0}$, représenté par la $\mathcal{O}_{\mathbb{P}^1}$-algèbre $\mathcal{E} = f_\star\mathcal{O}_Y$. C'est le déterminant de la trace de la multiplication $\mathcal{E}\otimes_{\mathcal{O}_{\mathbb{P}^1}}\mathcal{E} \to \mathcal{E}$. Pour le calculer, plaçons-nous sur un ouvert de $\mathbb{P}^1$, disons $U_0 = \operatorname{Spec} k_0[x]$. Alors $\mathcal{E}(U_0)$ est un $k_0[x]$-module libre, et la matrice de la multiplication sur U_0 dans une base $(e_1, \dots, e_s)$ est fournie. Pour chaque couple $(i,j) \in \{1\dots s\}^2$, soit t_{ij} la trace de la matrice à coefficients dans $k_0[x]$ dans la base $(e_1, \dots, e_s)$ de la multiplication par e_ie_j dans $\mathcal{E}(U_0)$. Le déterminant $\det(\mathcal{E})(U_0)$ est le déterminant de la matrice $(t_{ij})_{ij}$ est un élément de $k_0[x]$. La même procédure s'applique à l'ouvert U_1. Algorithmiquement, il suffit de calculer une seule matrice à coefficients dans $k_0[x,y]$, puis d'évaluer son déterminant successivement en $x = 1$ et $y = 1$. Un calcul direct donne le résultat suivant.

Lemme 4.4.7. Soit $N \in \mathrm{Mat}_{s\times s}(k_0[x,y])$ la matrice de la multiplication sur $\mathcal{E}$ avec les notations ci-dessus. Alors

$$\mathrm{Tr}(e_ie_j\cdot) = \sum_{\alpha,\beta=1}^{s} N_{\alpha,(i-1)s+j}N_{\beta,(\alpha-1)s+j}.$$

Exemple 4.4.8. Considérons la courbe elliptique $E = \operatorname{Proj} k[X,Y,Z]/(X^2Z - Y^3 + YZ^2)$ munie du morphisme $f\colon (X:Y:Z) \mapsto (X:Z)$ vers $\mathbb{P}^1 = \operatorname{Proj} k[X,Z]$. Soit U_0 l'ouvert $\operatorname{Spec} k[x]$ de $\mathbb{P}^1$. Alors $f_\star\mathcal{O}_E(U_0) = k[x][y]/(x^2 - y^3 + y)$, de $k[x]$-base $1, y, y^2$. Calculons par exemple la matrice de la multiplication par $y\cdot y = y^2$. On a $y^2\cdot 1 = y^2, y^2\cdot y = x^2 + y, y^2\cdot y^2 = x^2y + y^2$. La matrice est donc

$$\begin{pmatrix} 0 & x^2 & 0 \\ 0 & 1 & x^2 \\ 1 & 0 & 1 \end{pmatrix}$$

et sa trace vaut 2. De même, la matrice la multiplication par y^3 est

$$\begin{pmatrix} x^2 & 0 & x^2 \\ 1 & x^2 & 1 \\ 0 & 1 & x^2 \end{pmatrix}$$

car $y^5 = y^2(x^2+y) = x^2 + y + x^2y^2$, et sa trace vaut $3x^2$. Après avoir fait tous les calculs, on obtient la matrice $(\mathrm{tr}(y^iy^j\cdot))_{0\leqslant i,j\leqslant 2}$:

$$\begin{pmatrix} 3 & 0 & 2 \\ 0 & 2 & 3x^2 \\ 2 & 3x^2 & 2 \end{pmatrix}.$$

Le déterminant de cette matrice est $4 - 9x^4$. Par conséquent, $\Delta_{E \to \mathbb{P}^1}(U_0) = 4 - 9x^4$, et le morphisme $E \to \mathbb{P}^1$ n'est pas étale.

Le corollaire suivant sert à borner le nombre de $\mathcal{O}_{\mathbb{P}^1}$-algèbres à considérer au début de l'algorithme décrit en IV.4.1.2.

Corollaire 4.4.9. Soit S un schéma. Soit $T \to Y$ est un morphisme fini localement libre de rang m de $\mathcal{O}_{\mathbb{P}^1_S}$-modules localement libres. Notons $(T \to \mathbb{P}^1)_\star \mathcal{O}_T \simeq \bigoplus_{j=1}^s \mathcal{O}_{\mathbb{P}^1}(b_j)$ et $(Y \to \mathbb{P}^1_S)_\star \mathcal{O}_Y \simeq \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(a_i)$. Si f est étale alors $\sum_j b_j = m \sum_i a_i$.

Démonstration. Cela découle immédiatement du fait que $\det_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_T \simeq (\det_{\mathcal{O}_{\mathbb{P}^1}} \mathcal{O}_X)^{\otimes m}$. □

IV.4.2.3 Vérification que T est un F-torseur

Lemme 4.4.10. [Jin20, Lem. 6.14] Soit T un schéma muni d'une action d'un groupe G d'ordre r. Soit $f\colon T \to X$ un morphisme étale G-équivariant de rang constant r. Alors le lieu de X au-dessus duquel T est un torseur est ouvert et fermé dans X.

Corollaire 4.4.11. Soit X un $\mathbb{P}^1_S$-schéma fini localement libre. Soient T un schéma muni d'une action d'un groupe G d'ordre r, et $f\colon T \to X$ un morphisme étale G-équivariant de rang constant r. Notons X_0, T_0 les fibres de X et T au-dessus de $0 \in \mathbb{P}^1_S$. Si T_0 est un G-torseur sur X_0 alors T est un G-torseur sur X.

Démonstration. Le lemme 4.4.2 montre que X_0 rencontre toutes les composantes connexes de X. Par le lemme précédent, le lieu de X où T est un G-torseur est ouvert et fermé, et il contient X_0, c'est donc tout X. □

Un morphisme étale $T \to X$ est donc un F-torseur si et seulement si $F \times_{Y_0} T_0 \to T_0 \times_{Y_0} T_0, (f, x) \mapsto (x, f \cdot x)$ est un isomorphisme de schémas. Cela revient à demander que $\mathcal{O}_{T_0} \otimes_{\mathcal{O}_{Y_0}} \mathcal{O}_{T_0} \to \mathcal{O}_{T_0}^{|F|}, x \otimes y \mapsto (f \cdot xy)_{f \in F}$ soit un isomorphisme de $\mathcal{O}_{Y_0}$-modules. Concrètement, la matrice du morphisme $\mathcal{O}_{T_0} \otimes_{\mathcal{O}_{Y_0}} \mathcal{O}_{T_0} \to \mathcal{O}_{T_0}^{|F|}, x \otimes y \mapsto (f \cdot xy)_{f \in F}$ se calcule comme le produit $\Psi_{F,0} N_0$ où $\Psi_{F,0}$ est la concaténation (verticale) des matrices $\Psi_{f,0}, f \in F$ qui représentent l'action des éléments $f \in F$ sur $\mathcal{O}_{T_0}$. La matrice obtenue est à coefficients dans k, et demander à ce qu'elle soit inversible revient à ajouter une variable W et exiger que $\det(\Psi_{F,0} N_0) W - 1 = 0$.

IV.4.3 Résumé des données et équations

Soit Y une courbe projective lisse munie d'un morphisme $\phi\colon Y \to \mathbb{P}^1$ tel que $\phi_\star \mathcal{O}_Y \simeq \mathcal{O}_{\mathbb{P}^1}(a_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(a_r)$. Elle est représentée par des matrices $I \in \mathrm{Mat}_{r \times 1}(k_0)$ et $M \in \mathrm{Mat}_{r \times r^2}(k_0)$ qui définissent la structure de $\mathcal{O}_{\mathbb{P}^1}$-algèbre sur $\phi_\star \mathcal{O}_Y$. Soient G un groupe fini d'ordre n donné par une famille génératrice $(g_1, \ldots, g_\alpha)$, et $F = \{f_1, \ldots, f_\beta\}$ un Λ-module. Un Y-schéma T de type $b = (b_1, \ldots, b_s)$, avec $s = rn$, est défini par les indéterminées suivantes :

- Une matrice $J \in \mathrm{Mat}_{1 \times s}(k_0[x, y])$ et une matrice $N \in \mathrm{Mat}_{s \times s^2}(k_0[x, y])$ qui définissent la structure de $\mathcal{O}_{\mathbb{P}^1}$-algèbre de $\mathcal{O}_T$
- Des matrices $\Phi_{g_1}, \ldots, \Phi_{g_\alpha} \in \mathrm{Mat}_{s \times s}(k_0[x, y])$ qui définissent l'action de G sur $\mathcal{O}_T$
- Des matrices $\Psi_{f_1}, \ldots, \Psi_{f_\beta} \in \mathrm{Mat}_{s \times s}(k_0[x, y])$ qui définissent l'action de F sur $\mathcal{O}_T$
- Une matrice $S \in \mathrm{Mat}_{r \times s}(k_0[x, y])$ qui définit le morphisme de $\mathcal{O}_{\mathbb{P}^1}$-algèbres $T \to Y$
- Une matrice $B \in \mathrm{Mat}_{s \times s}(k_0)$ qui définit un isomorphisme de $\mathcal{O}_{Y_0}$-modules $\mathcal{O}_{Y_0}^n \to \mathcal{O}_{T_0}$
- Des indéterminées supplémentaires $V_1, \ldots, V_6$

Pour une matrice A à coefficients dans $k_0[x,y]$, notons A_0 la matrice A évaluée en $x=0$ et $y=1$. Notons également

$$\Psi_F = \begin{pmatrix} \Psi_{f_1} \\ \vdots \\ \Psi_{f_\alpha} \end{pmatrix}.$$

Soient $\Delta_{T,1}, \Delta_{T,2}, \Delta_{X,1}, \Delta_{X,2}$ les discriminants respectifs des morphismes $T \to \mathbb{P}^1$ et $Y \to \mathbb{P}^1$ sur les deux ouverts standard de $\mathbb{P}^1$, calculés à partir des matrices N et M grâce aux formules du lemme 4.4.7. Pour que le schéma $T \to Y$ défini par les données ci-dessus soit un torseur, il faut et il suffit que ces données vérifient les équations suivantes :

- $N(N \otimes I_s) = N(I_s \otimes N)$ (associativité de la multiplication)
- $N = N\left(\begin{smallmatrix} 0 & I_s \\ I_s & 0 \end{smallmatrix}\right)$ (commutativité de la multiplication)
- $N(J \otimes I_s) = I_s$ (unité)
- $\Phi_{1_G} = I_s$ et pour tous $i,j \in \{1 \dots \alpha\}$: $\Phi_{g_i}\Phi_{g_j} = \Phi_{g_i g_j}$ (action de G)
- $\Psi_{0_F} = I_s$ et pour tous $i,j \in \{1 \dots \beta\}$: $\Psi_{f_i}\Psi_{f_j} = \Psi_{f_i f_j}$ (action de F)
- Pour tous $i \in \{1 \dots \alpha\}, j \in \{1 \dots \beta\}$: $\Phi_{g_i}\Phi_{f_j}\Phi_{g_i}^{-1} = \Phi_{g_i \cdot f_j}$ (G-équivariance de l'action de F)
- $N(S \otimes S) = SM$ (compatibilité à la multiplication du morphisme $\mathcal{O}_X \to \mathcal{O}_T$)
- $B(I_n \otimes M_0) = N_0(S_0 \otimes B)$ ($\mathcal{O}_{X_0}$-linéarité de $\mathcal{O}_{X_0}^n \xrightarrow{\sim} \mathcal{O}_{T_0}$)
- $V_2\Delta_{T,1} - V_1\Delta_{X,1} = 0$, $V_1V_2 - 1 = 0$ (non-ramification de $T \to X$)
- $V_4\Delta_{T,2} - V_3\Delta_{X,2} = 0$, $V_3V_4 - 1 = 0$ (non-ramification de $T \to X$)
- $\det(B)V_5 - 1 = 0$ (bijectivité du morphisme $\mathcal{O}_{Y_0}^n \to \mathcal{O}_{T_0}$)
- $\det(\Psi_{F,0}M_0)V_6 - 1 = 0$ (bijectivité du morphisme $G \times_{X_0} T_0 \to T_0 \times_{X_0} T_0$)

Le schéma $\mathcal{U}_b$ défini par ces équations est un sous-schéma fermé d'un espace affine $\mathbb{A}^N_{k_0}$; chacun de ses k-points définit un F-torseur T sur Y. Un schéma $\mathcal{R}_b$ qui paramètre les morphismes entre deux torseurs se construit de la même façon. En particulier, il y a deux morphismes "source" et "but" $s_b, t_b \colon \mathcal{R}_b \to \mathcal{U}_b$. La classe d'isomorphisme d'un torseur défini par un point $x \in \mathcal{U}_b(k)$ est $s_b(t_b^{-1}x)$. Une étude détaillée de la construction de $\mathcal{U}_b$ et $\mathcal{R}_b$ donne le résultat suivant.

Proposition 4.4.12. [Jin20, Prop. 7.2] Les morphismes $s_b, t_b \colon \mathcal{R}_b \rightrightarrows \mathcal{U}_b$ sont lisses à fibres géométriques irréductibles. De plus, les schémas $t_b(s_b^{-1}x)$, pour $x \in \mathcal{U}_b(k)$, ont tous la même dimension.

Définissons enfin $\mathcal{U} := \bigsqcup_b \mathcal{U}_b$, $\mathcal{R} := \bigsqcup_b \mathcal{R}_b$; les morphismes s_b, t_b définissent encore des morphismes $s, t \colon \mathcal{U} \rightrightarrows \mathcal{R}$.

IV.4.4 Le schéma en groupoïdes qui paramètre les torseurs

IV.4.4.1 Catégories fibrées et schémas en groupoïdes

Définition 4.4.13. Soit $p \colon \mathcal{D} \to \mathcal{C}$ un foncteur.

1. Soit $f \colon y \to x$ un morphisme dans $\mathcal{D}$. Le morphisme f est dit fortement cartésien si pour tout objet z de $\mathcal{D}$, l'application $\mathrm{Hom}_{\mathcal{D}}(z,y) \to \mathrm{Hom}_{\mathcal{D}}(z,x) \times_{\mathrm{Hom}_{\mathcal{C}}(p(z),p(x))} \mathrm{Hom}_{\mathcal{C}}(p(z),p(y)), \phi \mapsto (f \circ \phi, p(\phi))$ est bijective.
2. La catégorie $\mathcal{D}$ est dite fibrée au-dessus de $\mathcal{C}$ si pour tout objet x de $\mathcal{D}$, et tout morphisme $g \colon c \to p(x)$ dans $\mathcal{C}$, il existe un morphisme fortement cartésien $f \colon y \to x$ dans $\mathcal{D}$ tel que $p(f) = g$.
3. Un morphisme entre deux catégories fibrées $p \colon \mathcal{D} \to \mathcal{C}$, $p' \colon \mathcal{D}' \to \mathcal{C}$ est un foncteur $F \colon \mathcal{D} \to \mathcal{D}'$ tel que $p' \circ F = p$, et qui préserve la forte cartésianité des morphismes.

Définition 4.4.14. Soit $p\colon \mathcal{D} \to \mathcal{C}$ une catégorie fibrée. Étant donné un objet c de $\mathcal{C}$, notons $\mathcal{D}(c)$ la catégorie des objets d de $\mathcal{D}$ tels que $p(d) = c$, avec pour morphismes les $f\colon d' \to d$ tels que $p(f) = \mathrm{id}_c$. La catégorie $\mathcal{D}$ est dite fibrée en groupoïdes au-dessus de $\mathcal{C}$ si pour tout objet c de $\mathcal{C}$, la catégorie $\mathcal{D}(c)$ est un groupoïde.

Remarque 4.4.15. Soit $p\colon \mathcal{D} \to \mathcal{C}$ une catégorie fibrée.

1. Étant donné un objet x de $\mathcal{D}$ et un morphisme $g\colon c \to p(x)$ dans $\mathcal{C}$, un relèvement fortement cartésien $f\colon y \to x$ de g est unique à isomorphisme près. La notation $y = g^\star x$ est donc sans ambiguïté. Fixons désormais un tel élément $g^\star x'$ pour chaque morphisme $x' \to x$ dans $\mathcal{D}(p(x))$. Alors, pour un tel morphisme $\alpha\colon x' \to x$, il existe un unique morphisme $g^\star\alpha\colon g^\star x' \to g^\star x$ dans $\mathcal{D}(c)$ tel que le diagramme suivant soit commutatif.

$$\begin{tikzcd} g^\star x' \arrow[r, "g^\star\alpha"] \arrow[d] & g^\star x \arrow[d] \\ x' \arrow[r, "\alpha"] & x \end{tikzcd}$$

   Ceci définit un foncteur $g^\star\colon \mathcal{D}(p(x)) \to \mathcal{D}(c)$ [Stacks, 02XJ, Def. 4.33.6]. De plus, si f et g sont des morphismes composables dans $\mathcal{C}$ alors il y a un unique isomorphisme $(f \circ g)^\star \xrightarrow{\sim} g^\star \circ f^\star$ [Stacks, 02XJ, Lem. 4.33.7]. De plus, un morphisme de catégories fibrées préserve (à isomorphisme près) les tirés en arrière.
2. En particulier, étant donné un schéma S, il y a dans toute catégorie fibrée au-dessus de Sch/S des foncteurs de changement de base : si $f\colon Y \to X$ est un morphisme de S-schémas, il y a un foncteur $f^\star = \times_X Y\colon \mathcal{D}(X) \to \mathcal{D}(Y)$.
3. Lorsque $S = \operatorname{Spec} K$ est le spectre d'un corps et L est une extension galoisienne de K, l'ensemble $\pi_0(\mathcal{D}(L))$ des classes d'isomorphisme dans $\mathcal{D}(L)$ est muni d'une action à droite de $\mathrm{Gal}(L|K)$, c'est-à-dire un morphisme de groupes $\mathrm{Gal}(L|K)^{\mathrm{op}} \to \mathfrak{S}(\pi_0(\mathcal{D}(L))$ défini par $\sigma \mapsto \sigma^\star$.

Définition 4.4.16. Soient S un schéma, X un S-schéma et G un X-schéma en groupes. La catégorie fibrée sur Sch/S des G-torseurs sur X est la catégorie $\mathcal{T}$ dont les objets sont les (S', T) où $S' \in \mathrm{Sch}/S$ et T est un $G_{S'}$-torseur sur $X_{S'}$. Les morphismes entre (S'', T'') et (S', T') sont les morphismes de torseurs si $S'' = S'$, et il n'y en a pas si $S'' \neq S'$. Étant donné $S'' \to S'$, le foncteur de changement de base $\mathcal{T}(S') \to \mathcal{T}(S'')$ est le foncteur $\times_{S'} S''$. Le foncteur vers Sch/S est le foncteur d'oubli, qui à un torseur associe le schéma sous-jacent, et à un morphisme $(S', T) \to (S', T')$ associe $\mathrm{id}_{S'}$.

Définition 4.4.17. Un schéma en groupoïdes sur un schéma S est la donnée d'un couple (R, U) de S-schémas muni de morphismes "source" et "but" $s, t\colon R \rightrightarrows U$ et "composition" $\circ\colon R \times_{U,s,t} R \to R$ tels que pour tout S-schéma T, la catégorie d'objets $U(T)$, de morphismes $R(T)$ dont la source et le but sont donnés par s_T et t_T, avec la composition définie par $\circ_T$, soit un groupoïde.

Définition 4.4.18. Soient $s, t\colon R \rightrightarrows U$ un schéma en groupoïdes sur un k_0-schéma S. La catégorie fibrée au-dessus de Sch/S associée est définie comme suit. Ses objets sont les couples (S', x) avec $S' \to S$ et $x \in U(S')$. Ses morphismes sont définis par $\mathrm{Hom}((S', x'), (S', x)) = \{f \in R(S') \mid s(f) = x', t(f) = x\}$, et le foncteur vers Sch/S est le foncteur d'oubli $(S', x) \mapsto S'$ qui envoie tout morphisme sur $\mathrm{id}_{S'}$. Ceci définit une catégorie fibrée en groupoïdes sur Sch/S, dont la fibre au-dessus de $T \in \mathrm{Sch}/k_0$ est le groupoïde $U(T)$. Étant donné un morphisme $\alpha\colon S'' \to S'$ dans Sch/S, le foncteur de changement de base $\alpha^\star\colon U(S') \to U(S'')$ est la composition à gauche par α.

IV.4.4.2 Le résultat principal

La proposition suivante est une variante de [Jin20, Prop. 7.5] avec des hypothèses moins contraignantes ; la preuve est essentiellement inchangée.

Proposition 4.4.19. Soit U un k_0-schéma de type fini. Soit $\mathcal{T} \to \mathrm{Sch}/k_0$ une catégorie fibrée en groupoïdes. Soit, pour chaque k_0-schéma S, une application $F_S \colon U(S) \to \mathcal{T}(S)$. Supposons que ces données vérifient les propriétés suivantes :

1. pour tout morphisme $\phi \colon S'' \to S'$ de k_0-schémas et tout $x \in U(S')$, $F_{S''}(x \circ \phi) = \phi^\star(F_{S'}(x))$;
2. l'application $F_k \colon U(k) \to \mathcal{T}(k)$ est essentiellement surjective ;
3. pour tout k_0-schéma S et tous objets $x, y \in \mathcal{T}(S)$, le foncteur $\mathrm{Sch}/S \to \mathrm{Set}$, $(S' \xrightarrow{\alpha} S) \mapsto \mathrm{Isom}_{\mathcal{T}(S')}(\alpha^\star x, \alpha^\star y)$ est représenté par un schéma $Y \to S$ ouvert et fermé.

Alors l'application surjective et $\mathrm{Gal}(k|k_0)$-équivariante $U(k) \to \pi_0(\mathcal{T}(k))$ induite par F_k se factorise en une application encore surjective et $\mathrm{Gal}(k|k_0)$-équivariante $\pi_0^{sch}(U_k) \to \pi_0(\mathcal{T}(k))$.

Démonstration. La Galois-équivariance de l'application vient de la compatibilité de F au changement de base. Soient $x \in \mathcal{U}(k)$, et C la composante connexe de U_k contenant l'image de x. Notons $f \colon C \to \operatorname{Spec} k$ le morphisme structural, et $\bar{x} \colon \operatorname{Spec} k \to C$ la factorisation de x par C. La situation est résumée par le diagramme suivant (qui devient commutatif en retirant la flèche f) :

$$\begin{tikzcd} \operatorname{Spec} k \arrow[r, "x"] \arrow[d, shift left, "\bar{x}"] & U \\ C \arrow[r, "j"'] \arrow[u, shift left, "f"] & U_k \arrow[u, "i"'] \end{tikzcd}$$

Soient $\phi_x = x \circ f = f^\star x^\star \mathrm{id}_U$ et $\phi_C = i \circ j = j^\star i^\star \mathrm{id}_U \in U(C)$. Notons ψ_x, ψ_C les images par F_C de ϕ_x, ϕ_C dans $\mathcal{T}(C)$. Le foncteur $\mathrm{Sch}/C \to \mathrm{Set}$, $(S \xrightarrow{\alpha} C) \mapsto \mathrm{Isom}_{\mathcal{T}(C)}(\alpha^\star \psi_C, \alpha^\star \psi_x)$ est par hypothèse représentable par un schéma $Y \to C$ ouvert et fermé. Par construction, $Y(\bar{x})$ est non vide. En effet,

$$\bar{x}^\star \psi_x = \bar{x}^\star F_C(\phi_x) = F_k(\phi_x \circ \bar{x}) = F_k(x \circ f \circ \bar{x}) = F_k(x)$$

par compatibilité au changement de base, et car $\bar{x}$ est une section de f. De même, $\bar{x}^\star \psi_C = F_k(x)$ car $x = i \circ j \circ \bar{x}$. Ainsi, $\mathrm{id}_{F_k(x)} \in Y(\bar{x})$. Le morphisme $Y \to C$ est donc un morphisme ouvert et fermé d'un schéma non vide vers un schéma connexe : il est surjectif. Par conséquent, pour tout autre point $\bar{x}' \in C(k)$, $Y(\bar{x}') \neq 0$. Il y a donc pour tous $\bar{x}, \bar{x}' \in C(k)$ un isomorphisme $\bar{x}'^\star \psi_x \simeq \bar{x}'^\star \psi_C$ dans $\mathcal{T}(k)$. Or $\bar{x}'^\star \psi_x = \bar{x}'^\star F_C(x \circ f) = F_k(x \circ f \circ \bar{x}') = F_k(x)$; de même, $\bar{x}'^\star \psi_{x'} = F_k(x')$.

Par conséquent, $F_k(x)$ et $F_k(x')$ sont isomorphes dans $\mathcal{T}(k)$. La surjection $\mathcal{U}(k) \to \mathcal{T}(k)$ se factorise donc en une application $\pi_0^{sch}(\mathcal{U}_k) \to \pi_0(\mathcal{T}(k))$, qui est encore surjective. □

Rappelons [Stacks, 0478] que tout schéma de type fini X sur k est un schéma de Jacobson : les points fermés sont denses dans tout fermé de X. En particulier, les composantes irréductibles (resp. connexes) de X sont en bijection canonique avec celles de $X(k)$ muni de sa topologie de Zariski naïve.

Proposition 4.4.20. Mêmes notations et hypothèses que la proposition précédente. Si, de plus, les préimages par F_k des classes d'isomorphisme de $\mathcal{T}(k)$ sont connexes dans $U(k)$ alors l'application $\pi_0^{sch}(U_k) \to \pi_0(\mathcal{T}(k))$ induite par F_k est bijective. Enfin, si ces préimages sont irréductibles dans $U(k)$ alors les composantes connexes de U_k sont irréductibles.

Démonstration. Considérons $x, x' \in U(k)$ tels que $F_k(x)$ soit isomorphe à $F_k(x')$ dans $\mathcal{T}(k)$. Par hypothèse, ils appartiennent à une même partie connexe de $|U_k|$. L'image dans U_k de cette partie connexe est encore connexe puisque l'injection $|U_k| \to U_k$ est continue, et les images de x, x' dans U_k appartiennent donc à une même composante connexe de U_k. Pour le second point, servons-nous de la bijection croissante entre les composantes connexes (resp. irréductibles) de U_k et celles de son ensemble de points fermés $|U_k| = U(k)$. Considérons deux points $x, x' \in U(k)$ dans une même composante connexe de $U(k)$. Alors d'après la proposition 4.4.19, leurs images par F_k sont isomorphes. Par conséquent, ils appartiennent à une même composante irréductible de $U(k)$, ce qui conclut. □

IV.4.4.3 Application

Le théorème est appliqué à la catégorie $\mathcal{T}$ des G-torseurs sur une courbe Y (voir la définition 4.4.16), et au schéma $\mathcal{U}$ construit à la fin de la section IV.4.3.

Étant donné un k-schéma S, un point de $\mathcal{U}(S)$ définit encore un torseur sur X_S. En effet, un morphisme de fibrés vectoriels $\bigoplus_{i=1}^{s} \mathcal{O}_{\mathbb{P}^1_S}(a_i) \to \bigoplus_{j=1}^{t} \mathcal{O}_{\mathbb{P}^1_S}(b_j)$ est défini par une matrice $t \times s$ à coefficients dans $\mathrm{H}^0(S, \mathcal{O}_S)[x, y]$, dont l'élément en position (i, j) est un polynôme homogène de degré $b_j - a_i$. La donnée de matrices (multiplication, action du groupe F) à coefficients dans $\mathrm{H}^0(S, OO_S)$ définit donc encore un schéma fini localement libre sur $\mathbb{P}^1_S$. Les conditions suffisantes pour être un torseur ont été démontrées dans un cadre relatif (voir la section IV.4.2), et s'appliquent donc encore ici. Remarquons également que toute cette construction commute au changement de base : étant donnés un morphisme $f\colon S' \to S$ et un point $x \in U(S)$ définissant un torseur $T \to X$, le torseur défini par $f^\star x = x \circ f \in U(S')$ est le torseur $T \times_S S'$. Enfin, chaque F-torseur sur Y est isomorphe à un torseur défini par l'un des k-points de $\mathcal{U}$. La proposition 4.4.19 s'applique donc à $\mathcal{U}$: pour trouver un représentant de chaque classe d'isomorphisme de F-torseurs sur Y, il suffit de trouver un k-point dans chaque composante connexe de $\mathcal{U}_k$.

Corollaire 4.4.21. Le schéma $\mathcal{U}_b$ est équidimensionnel.

Démonstration. Les composantes irréductibles de $\mathcal{U}_b$ sont d'après le théorème principal les classes d'isomorphisme $t(s^{-1}x)$ pour $x \in \mathcal{U}_b(k)$. D'après le lemme 4.4.12, elles sont toutes de même dimension. □

Nous avons expliqué la construction du schéma $\mathcal{U}$ paramétrant les $\mathcal{F}$-torseurs sur X. D'après la discussion précédente, il suffit désormais pour calculer $\mathrm{H}^1(X, \mathcal{F})$ de déterminer un point dans chaque composante connexe de X, c'est-à-dire dans chaque composante irréductible de X d'après la proposition 4.4.20.

IV.4.5 Calcul de représentants des classes de torseurs

Voici comment déterminer au moins un point de chaque composante irréductible du schéma affine $\mathcal{U}$ calculé précédemment. Comme ce dernier est équidimensionnel, la procédure décrite dans la section B.4.3, qui consiste à calculer la fibre en 0 d'une normalisation de Noether $\nu\colon \mathcal{U} \to \mathbb{A}^D$, convient. Elle fournit une liste de points, dont plusieurs appartiennent peut-être à une même composante. Deux points x, y de cette liste appartiennent à la même composante si et seulement si $s^{-1}x \times_{\mathcal{R}} t^{-1}y$ est non vide : il suffit d'en déterminer des équations, puis de tester si elles engendrent l'idéal unité. Une fois déterminé l'ensemble $\mathrm{H}^1(X, \mathcal{F})$, il reste à calculer sa loi de groupe ; celle-ci est donnée par le produit contracté, et s'exprime en termes de corps de fonctions par des méthodes d'algèbre linéaire.

Ceci conclut la description de l'algorithme de Jin pour les faisceaux lisses sur les courbes projectives. Nous expliquons dans la section suivante comment une petite modification de cet algorithme permet de calculer également la cohomologie d'un faisceau lisse sur une courbe affine.

IV.4.6 Courbes affines

L'algorithme de Jin est exposé dans [Jin20] dans un cadre plus général, qui englobe le calcul de $\mathrm{H}^1(U, \mathcal{F})$ et $\mathrm{H}^1_c(U, \mathcal{F})$ où U est une courbe affine lisse sur k. Considérons la situation suivante : U est une courbe lisse, X sa complétion projective lisse munie d'un morphisme $X \to \mathbb{P}^1_k$ tel que $U = X \times_{\mathbb{P}^1} \mathbb{A}^1$. La construction d'un tel morphisme est décrite dans [Jin20, Prop. 9.8]. Le faisceau lisse $\mathcal{F}$ sur U de fibre F est trivialisé par un revêtement galoisien $V \to U$ de groupe G ; le schéma Y est la normalisation de X dans V, et W est la fibre de Y au-dessus de $0 \in \mathbb{P}^1$.

$$\begin{tikzcd}
V \arrow[r, "j'"] \arrow[d, "g"] & Y \arrow[d, "f"] & W \arrow[l, "i'"'] \arrow[d, "h"] \\
U \arrow[r, "j"] \arrow[d] & X \arrow[d] & Z \arrow[l, "i"'] \arrow[d] \\
\mathbb{A}^1_k \arrow[r] & \mathbb{P}^1_k & 0 \arrow[l]
\end{tikzcd}$$

Lemme 4.4.22. Soient C la catégorie des $\mathcal{F}$-torseurs sur U, et D la catégorie des schémas $T \to Y$ lisses sur k, munis d'une action G-équivariante de F tels que $T|_V \to V$ soit un $\mathcal{F}$-torseur. La composition de $g^\star$ avec la complétion projective lisse définit une équivalence de catégories $C \to D$, de quasi-inverse $g_\star^G \circ (- \times_{\mathbb{P}^1} \mathbb{A}^1)$.

Démonstration. D'après le corollaire 1.4.5, $g^\star$ induit une équivalence de la catégorie C avec la catégorie des $\mathcal{F}|_V$-torseurs G-équivariants sur V. Ensuite, un schéma T est un $\mathcal{F}|_V$-torseur G-équivariant sur V si et seulement si sa complétion projective lisse est un schéma lisse sur k muni d'un morphisme G-équivariant vers Y qui en fait un $\mathcal{F}|_V$-torseur sur V. □

Afin de calculer $\mathrm{H}^1(U, \mathcal{F})$, il suffit de modifier deux choses dans la construction du schéma paramétrant les F-torseurs G-équivariants sur Y. D'une part, l'étalitude de $T \to Y$ doit être remplacée par celle de $T \times_{\mathbb{P}^1} \mathbb{A}^1 \to V$. Cela revient [Jin20, Prop. 6.12] à demander que le discriminant de $\Delta_{T \to \mathbb{P}^1}$ diffère de $\Delta_{Y \to \mathbb{P}^1}$ non pas d'un élément de $k^\times$, mais d'un élément de $k^\times$ fois une puissance de y qui se calcule à partir des données de $\mathcal{O}_T$ et $\mathcal{O}_X$. D'autre part, il faut s'assurer que le schéma T est lisse au-dessus de $0 \in \mathbb{P}^1$: une condition nécessaire et suffisante se traduisant par des équations est donnée dans [Jin20, Prop. 6.16].

IV.4.7 Complexité

Soit X une courbe lisse sur k_0 de genre géométrique g. Supposons donné un morphisme $\phi\colon X \to \mathbb{P}^1$, ainsi que la $\mathcal{O}_{\mathbb{P}^1}$-algèbre $\phi_\star \mathcal{O}_X \simeq \mathcal{O}_{\mathbb{P}^1}(a_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(a_r)$. Soit $\mathcal{F}$ un faisceau lisse de groupes abéliens sur X, de fibre F, décrit explicitement par un revêtement galoisien trivialisant $Y \to X$ de groupe G et le groupe abélien $F = \mathrm{H}^0(Y, \mathcal{F})$ d'ordre m. Les torseurs $T \to X$ considérés par l'algorithme vérifient $(T \to \mathbb{P}^1)_\star \mathcal{O}_T \simeq \mathcal{O}_{\mathbb{P}^1}(b_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(b_s)$ avec $s = mr$.

Proposition 4.4.23. [Jin20, Prop. 6.21,6.24] Le nombre de types $b = (b_1, \ldots, b_s)$ vérifiant $b_j \leqslant 0$, $s = mr$ et $\sum_j b_j = m \sum_j a_j$ est $O((rgm)^{rm})$, où g est le genre de X. Pour chaque type b, le schéma $\mathcal{U}_b$ calculé par l'algorithme est donné par $O(s^5 m^4)$ polynômes de degré au plus sn en $O(s^5 n^4)$ variables.

Proposition 4.4.24. [Jin20, Cor. 8.12] L'algorithme de Jin calcule un k-schéma en groupes zéro-dimensionnel représentant $\mathrm{H}^1(X, \mathcal{F})$ en $\exp(O(r^{15} m^{12} g^3 \log(rm)^3))$ opérations dans k_0.

La complexité exponentielle en $m \log(m)$ de l'algorithme global vient donc directement de la construction du schéma $\mathcal{U}$, et non d'un problème de nature algorithmique lié au calcul des composantes connexes de ce schéma : cette complexité ne peut pas être améliorée par des astuces algorithmiques.

Remarque 4.4.25. Afin d'obtenir cette complexité, Jin fait usage d'un algorithme de Khuri-Makdisi [KM06, §7], qui suppose qu'il existe un algorithme de factorisation des polynômes de $k_0[t]$ en temps polynomial. Ceci est vrai lorsque k_0 est fini, et encore vrai si k_0 est un corps de nombres ; cependant, dans ce cas, il faut prendre en compte dans le calcul de la complexité la hauteur des coefficients des polynômes concernés (et non pas seulement leur degré), ce qui n'est pas étudié dans [Jin20]. Ce travail paraît fastidieux, mais pas difficile, à réaliser.

IV.5 Aspects pratiques

Voici quelques remarques sur les aspects pratiques des algorithmes mentionnés ci-dessus, dont aucun n'a été implémenté jusqu'ici. Le seul algorithme qui paraît implémentable avec une quantité d'efforts raisonnable est celui de Couveignes. De plus, au vu de sa complexité, il serait certainement utilisable dans la pratique pour de petits paramètres. Les algorithmes de Huang et Ierardi et de Jin sont très semblables : ils construisent tous les deux un grand schéma S paramétrant les objets dont on cherche des classes d'isomorphisme, puis cherchent des points dans les composantes irréductibles de ce schéma. Les deux paraissent en l'état cauchemardesques à implémenter. Cependant, une fois implémenté, l'algorithme de Huang et Ierardi aurait un avantage de rapidité d'exécution, car la dimension de l'espace dans lequel est plongé le schéma S, linéaire en le genre de la courbe, augmente bien moins vite en fonction des paramètres que dans le cas de l'algorithme de Jin, où elle dépend non seulement de la représentation de la courbe mais aussi du cardinal de la fibre du faisceau (voir lemme 4.4.23). La complexité de la recherche de points étant exponentielle en cette dimension (voir annexe B.4.2.2), cet avantage serait conséquent. Enfin, l'algorithme de Madore et Orgogozo nécessite en premier lieu l'utilisation d'un algorithme de calcul du H^1 des faisceaux constants sur les courbes, dont aucun n'a encore été implémenté ; de plus, il ne serait pas utilisable dans la pratique en raison de sa complexité conséquente.

Dans le chapitre suivant, nous décrivons des algorithmes de calcul de la cohomologie des faisceaux constructibles sur les courbes lisses ou nodales. Nous nous baserons sur les algorithmes de Couveignes et de Huang et Ierardi pour nos résultats ; en l'absence d'une implémentation de ces algorithmes, nous nous contenterons dans nos exemples de courbes où le calcul de points de torsion de la jacobienne peut se faire par des moyens plus élémentaires.

CHAPITRE V

Calcul effectif de la cohomologie

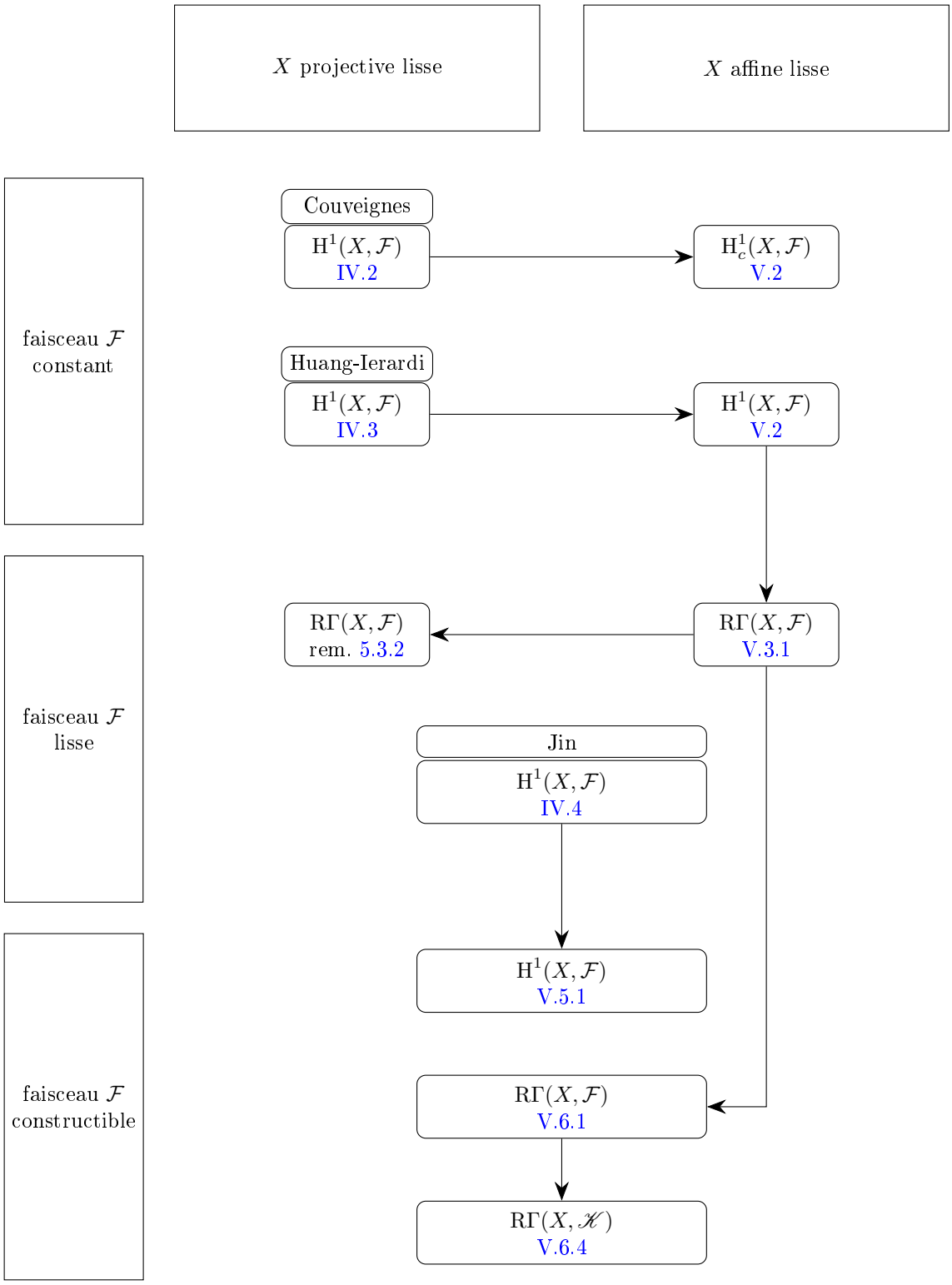
Dans l'ensemble de ce chapitre, k_0 désigne un corps parfait, k une clôture algébrique de k_0, et n un entier inversible dans k. Nous noterons Λ l'anneau $\mathbb{Z}/n\mathbb{Z}$, et $\mathfrak{G}_0$ le groupe $\mathrm{Gal}(k|k_0)$.

L'objectif de ce chapitre est de donner une description explicite, étant donné un complexe $\mathscr{K}$ de faisceaux constructibles de Λ-modules sur une k-courbe lisse X, d'un complexe de Λ-modules représentant $\mathrm{R}\Gamma(X, \mathscr{K}) \in \mathrm{D}_c^b(\Lambda)$. Lorsque X provient par changement de base de k_0, nous décrivons l'action de $\mathfrak{G}_0$ sur un tel complexe. Nous estimerons également la complexité du calcul de $\mathrm{R}\Gamma(X, \mathscr{K})$. Ce calcul repose sur celui de la cohomologie des faisceaux lisses sur une courbe affine lisse, qui se déduit lui-même du cas des faisceaux constants. Nous prouverons en particulier le résultat suivant.

Théorème 5.0.1. Soit X une courbe intègre lisse sur k. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X. Soient U un ouvert de X sur lequel $\mathcal{F}$ est lisse de fibre générique géométrique M, et Z le fermé réduit complémentaire. Soient $V \to U$ un revêtement galoisien qui trivialise $\mathcal{F}|_U$, et $V_2 \to V$ le revêtement de V de groupe $H^1(V, \Lambda)^\vee$. Notons $G = \mathrm{Aut}(V_2|U)$. Pour chaque point $z \in Z$, notons I_z le groupe d'inertie d'un point de la compactification lisse de V_2 au-dessus de z, et P_z le groupe d'inertie sauvage correspondant. Notons $\phi_z \colon \mathcal{F}_z \to M^{I_z} \subseteq M^{P_z} \xrightarrow{\sim} M_{P_z}$ le morphisme de recollement en z composé avec l'isomorphisme canonique $M^{P_z} \xrightarrow{\sim} M_{P_z}$, qui à un élément P_z-invariant de M associe sa classe dans le module des coinvariants M_{P_z}. Alors $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ est le cône du morphisme de complexes suivant, où $C^{12}(G, M)$ désigne le groupe des morphismes croisés $G \to M$.

$$\begin{tikzcd}
M \oplus \bigoplus_{z\in Z} \mathcal{F}_z \arrow[r, "(\partial_G, 0)"] \arrow[d, "\bigoplus_{z\in Z}(\mathrm{id} - \phi_z)"] & C^{12}(G, M) \arrow[r] \arrow[d, "\bigoplus_z \mathrm{res}_{I_z}^G"] & \bigoplus_{z\in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
\bigoplus_{z\in Z} M_{P_z} \arrow[r, "\bigoplus_z \partial_{I_z}"] & \bigoplus_{z\in Z} C^{12}(I_z/P_z, M_{P_z}) \arrow[r] & \bigoplus_{z\in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] & 0
\end{tikzcd}$$

Nous étudierons en détail la complexité des algorithmes présentés, et montrerons qu'elle est doublement exponentielle en le genre de la courbe dans le cas général. Les différentes méthodes de calcul de la cohomologie et leurs interdépendances sont résumées dans le diagramme ci-après. Ici, X est une courbe intègre lisse sur k, $\mathcal{F}$ est un faisceau constructible sur X et $\mathscr{K}$ est un complexe de faisceaux constructibles sur X. La colonne de gauche indique la nature de $\mathcal{F}$ (resp. des termes de $\mathscr{K}$).


X projective lisse
X affine lisse
faisceau $\mathcal{F}$ constant
faisceau $\mathcal{F}$ lisse
faisceau $\mathcal{F}$ constructible
Couveignes
$\mathrm{H}^1(X,\mathcal{F})$ IV.2
$\mathrm{H}^1_c(X,\mathcal{F})$ V.2
Huang-Ierardi
$\mathrm{H}^1(X,\mathcal{F})$ IV.3
$\mathrm{H}^1(X,\mathcal{F})$ V.2
$\mathrm{R}\Gamma(X,\mathcal{F})$ rem. 5.3.2
$\mathrm{R}\Gamma(X,\mathcal{F})$ V.3.1
Jin
$\mathrm{H}^1(X,\mathcal{F})$ IV.4
$\mathrm{H}^1(X,\mathcal{F})$ V.5.1
$\mathrm{R}\Gamma(X,\mathcal{F})$ V.6.1
$\mathrm{R}\Gamma(X,\mathscr{K})$ V.6.4

V.1 Scindage explicite des suites exactes courtes

Le principe ci-dessous sera souvent utilisé dans la suite. Soit G un groupe fini. Considérons une suite exacte courte de $\Lambda[G]$-modules de type fini

$$0 \to A \xrightarrow{\phi} B \xrightarrow{\psi} C \to 0$$

où C est libre. Le but est de calculer B en connaissant A et C. Supposons que l'on dispose d'une description explicite de A et C comme $\Lambda[G]$-modules, c'est-à-dire de présentations de A et C comme Λ-modules et pour tout $\sigma \in G$, des endomorphismes de A et C définis par σ. Soient $(a_1, \ldots, a_r)$ et $(c_1, \ldots, c_m)$ des familles génératrices respectives de A et C. Supposons également qu'il existe des éléments $\lambda_{ij,g} \in \Lambda, a_{i,g} \in A$ (que l'on sait calculer) tels qu'il existe une section Λ-linéaire s de ψ vérifiant pour tous $g \in G, i \in \{1, \ldots, m\}$:

$$g \cdot s(c_i) = \sum_{j=1}^{m} \lambda_{ij,g} s(c_j) + a_{i,g}. \qquad (\star)$$

Décrivons comment calculer le $\Lambda[G]$-module B explicitement. Il est représenté en tant que Λ-module par $A \oplus C$; l'action de $g \in G$ sur $a + c \in B$ se calcule à l'aide de $(\star)$.

Voyons comment cette description se comporte vis-à-vis des morphismes de suites exactes. Étant donné un morphisme de suites exactes de $\Lambda[G]$-modules :

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\phi"] \arrow[d, "\alpha"] & B \arrow[r, "\psi"] \arrow[d, "f"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\phi'"] & B' \arrow[r, "\psi'"] & C' \arrow[r] & 0
\end{tikzcd}$$

où l'on dispose explicitement des données ci-dessus pour les deux suites exactes, ainsi que des morphismes α et γ, il est possible de calculer le morphisme f dès que les sections Λ-linéaires s de ψ et s' de ψ' sont compatibles au sens où $s'\gamma = fs$. Soit $b \in B$. Écrivons $b = \phi(a) + s(c)$, où s est la section donnée de ψ. Alors la commutativité du carré de gauche donne $f(b) = \phi'\alpha(a) + f(b - \phi(a)) = \phi'\alpha(a) + fs(c) = \phi'\alpha(a) + s'\gamma(c)$.

V.2 Faisceaux constants sur les courbes affines

Soit X_0 une courbe projective lisse sur k_0. Soient Z_0 un fermé réduit de X_0, et U_0 l'ouvert complémentaire. Notons X, Z, U leurs changements de base à k. Cette section porte sur le calcul de $\mathrm{H}^1(U, \Lambda)$, où Λ est le faisceau constant de valeur $\mathbb{Z}/n\mathbb{Z}$. Le choix d'une racine primitive n-ième de l'unité dans k détermine un isomorphisme $\Lambda \to \mu_n$. Il y a un isomorphisme canonique

$$\mathrm{H}^1(U, \Lambda) \otimes \mu_n \xrightarrow{\sim} \mathrm{H}^1(U, \mu_n)$$

qui permet de déduire $\mathrm{H}^1(U, \Lambda)$ avec son action de $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$ de $\mathrm{H}^1(U, \mu_n)$; cet isomorphisme se construit par exemple aisément sur les groupes de cohomologie de Čech. Nous expliquons d'abord comment représenter et manipuler les éléments de $\mathrm{H}^1(U, \mu_n)$, puis comment calculer les groupes $\mathrm{H}^1(U, \mu_n)$ et $\mathrm{H}^1_c(U, \mu_n)$, puis comment, étant donné un morphisme de courbes affines $V \to U$, décrire le morphisme canonique $\mathrm{H}^1(U, \mu_n) \to \mathrm{H}^1(V, \mu_n)$.

V.2.1 Calcul dans $\mathrm{H}^1(U, \mu_n)$

Rappelons (cf lemme 2.2.11) que $\mathrm{H}^1(U, \mu_n)$ est en bijection avec le groupe des classes d'équivalence de triplets $([D], D', f)$ où $D \in \mathrm{Div}^0 X$, $D' \in \mathrm{Div}^0 X$ est à support dans Z et $nD = \mathrm{div}(f) + D'$.

Remarque 5.2.1. Décrivons précisément comment calculer dans ce groupe quotient isomorphe à $\mathrm{H}^1(U, \mu_n)$. Deux triplets $([D_1], D'_1, f_1)$ et $([D_2], D'_2, f_2)$ sont égaux dans le quotient si et seulement si $D'_1 - D'_2 \in n\,\mathrm{Div}^0_Z(X)$ et $(D_1 - D_2) - \frac{1}{n}(D'_1 - D'_2)$ est principal. Ceci se teste algorithmiquement, en vérifiant si les coefficients de $D'_1 - D'_2$ sont multiples de n, puis en calculant le cas échéant l'espace de Riemann-Roch associé à $(D_1 - D_2) - \frac{1}{n}(D'_1 - D'_2)$ à l'aide de l'un des algorithmes présentés dans l'annexe C.3.2.

La proposition suivante montre comment la décomposition d'un élément de $\mathrm{H}^1(U, \mu_n)$ dans une base de ce Λ-module libre se traduit en termes de corps de fonctions. Elle servira dans la section V.3.2.

Lemme 5.2.2. Notons $A_i = ([D_i], D'_i, f_i), i = 1, \ldots, r$ les éléments d'une base de $\mathrm{H}^1(U, \mu_n)$ avec les notations ci-dessus. Soit $A = ([D], D', f) \in \mathrm{H}^1(U, \mu_n)$. Soient $\alpha_1, \ldots, \alpha_r \in \Lambda$ tels que

$$A = \sum_{j=1}^{r} \alpha_i A_i \in \mathrm{H}^1(U, \mu_n).$$

Alors il existe une fonction $h \in k(X)^\times$ et des entiers a_i relevant les α_i tels que

$$f = h^n \prod_{i=1}^{r} f_i^{a_i}.$$

Démonstration. D'après la remarque 5.2.1, il existe $h \in k(X)^\times$, des entiers a_i relevant les α_i et $D'' \in \mathrm{Div}^0_Z(X)$ tels que

$$D = \sum_{i=1}^{r} a_i D_i + D'' + \mathrm{div}(h), \qquad D' = \sum_{i=1}^{r} a_i D'_i + nD'' \quad \text{et} \quad \mathrm{div}(f) = nD - D''.$$

Sur la courbe projective lisse X, il y a donc une égalité de diviseurs :

$$\begin{aligned}
\mathrm{div}(f) &= \sum_{i=1}^{r} a_i(nD_i - D'_i) + \mathrm{div}(h^n) \\
&= \sum_{i=1}^{r} a_i \mathrm{div}(f_i) + \mathrm{div}(h^n) \\
&= \mathrm{div}\left(h^n \prod_{i=1}^{r} f_j^{a_i}\right).
\end{aligned}$$

Par conséquent, il existe $C \in k^\times$ tel que $Ch^n \prod_i f_i^{a_i} = f$. Comme k est algébriquement clos, il existe $c \in k^\times$ tel que $c^n = C$; il suffit de remplacer h par ch pour conclure. □

Remarque 5.2.3. Étant donné les éléments $A, A_1, \ldots, A_r, \alpha_1, \ldots, \alpha_r$ du lemme, le diviseur D'' de la démonstration se calcule comme $\frac{1}{n}(D' - \sum a_i D'_i)$. Le calcul de la fonction h nécessite le calcul de l'espace de Riemann-Roch du diviseur $nD - D''$ (différence de deux diviseurs effectifs de même degré inférieur à $g + n$), ainsi que le calcul dans k d'une racine n-ième de C (voir annexe A.2.2 dans le cas des corps finis).

V.2.2 Calcul de la cohomologie

Voyons comment calculer explicitement les groupes $\mathrm{H}^1(U,\mu_n)$ et $\mathrm{H}^1_c(U,\mu_n)$. Le lemme 2.4.4 assure que $\mathrm{H}^1_c(U,\mu_n)$ est isomorphe au groupe des classes d'équivalence (modulo $X-U$) de diviseurs sur U. Rappelons également qu'il y a des suites exactes courtes fonctorielles en (X,U) :

$$0 \to \mathrm{H}^1(X,\mu_n) \to \mathrm{H}^1(U,\mu_n) \to \mathrm{Div}^0_Z(X)\otimes\Lambda \to 0$$

dont les flèches sont données respectivement par $([D],f)\mapsto([D],0,f)$ et $([D],D',f)\mapsto D'$, et

$$0 \to \frac{\bigoplus_{z\in Z}\mu_n(k)}{\mu_n(k)} \to \mathrm{H}^1_c(U,\mu_n) \to \mathrm{H}^1(X,\mu_n) \to 0$$

dont la flèche de gauche associe à $(\zeta_P)_{P\in Z}$ la classe du diviseur d'une fonction f vérifiant $f(P)=\zeta_P$ pour tout $P\in Z$, et celle de droite associe à un diviseur D le couple $([D],f)$ où f est n'importe quelle fonction de diviseur nD. Comme les termes de gauche et de droite de ces suites exactes sont des Λ-modules libres, $\mathrm{H}^1(U,\mu_n)$ et $\mathrm{H}^1_c(U,\mu_n)$ sont des Λ-modules libres. Ces deux suites sont duales l'une de l'autre par l'accouplement de Weil, comme vu à la fin de la section II.4.2. Soit Γ un quotient de $\mathfrak{G}_0=\mathrm{Gal}(k|k_0)$ tel que l'action de $\mathfrak{G}_0$ sur $\mathrm{H}^1(X,\mu_n)$ et $\mathrm{Div}^0_Z(X)\otimes\Lambda$ se factorise par Γ. Il suffit, afin de disposer d'une description complète de $\mathrm{H}^1(U,\mu_n)$ comme $\Lambda[\Gamma]$-module, de calculer explicitement une section Λ-linéaire de $\mathrm{H}^1(U,\mu_n)\to\mathrm{Div}^0_Z(X)\otimes\Lambda$, ainsi que l'action de Γ sous la forme décrite dans la section V.1. Une telle section existe toujours car les Λ-modules en question sont libres. Cela revient, étant donné $P,Q\in Z$, à calculer un diviseur $D\in\mathrm{Div}^0(X)$ tel que nD soit linéairement équivalent à $E:=(P)-(Q)$, ce qui s'effectue à l'aide de l'adaptation de l'algorithme de Huang-Ierardi décrite dans la remarque 4.3.5.

Remarque 5.2.4. Voici comment calculer l'action de Γ sur $\mathrm{H}^1(U,\mu_n)$ en suivant la méthode décrite dans la section V.1. Soit $(([D_1],f_1),\dots,([D_{2g}],f_{2g}))$ une Λ-base de $\mathrm{H}^1(X,\mu_n)$. Soit également $(D'_{2g+1},\dots,D'_{2g+r})$ une Λ-base de $\mathrm{Div}^0_Z(X)\otimes\Lambda$. Pour chaque $i\in\{2g+1\dots 2g+r\}$, soit $([D_i],D'_i,f_i)$ un représentant d'un antécédent de D'_i dans $\mathrm{H}^1(U,\mu_n)$. La famille des classes de triplets

$$([D_1],0,f_1),\dots,([D_{2g}],0,f_{2g}),([D_{2g+1}],D'_{2g+1},f_{2g+1}),\dots,([D_{2g+r}],D'_{2g+r},f_{2g+r})$$

forme alors une base de $\mathrm{H}^1(U,\mu_n)$. Soit $([D],D',f)\in\mathrm{H}^1(U,\mu_n)$. L'action d'un $\sigma\in\Gamma$ sur le triplet $([D],D',f)$ se calcule de la façon suivante : l'élément $\sigma\cdot D'\in\mathrm{Div}^0_Z(X)\otimes\Lambda$ se décompose comme combinaison linéaire

$$\sigma\cdot D'=\sum_{i=2g+1}^{2g+r}\alpha_i D'_i.$$

L'élément $\sigma\cdot([D],D',f)-\sum_i\alpha_i([D_i],D'_i,f_i)$ appartient à l'image de $\mathrm{H}^1(X,\mu_n)$: il suffit maintenant de décomposer $(\sigma\cdot[D]-\sum_i\alpha_i[D_i],(\sigma\cdot f)/\prod_i f_i^{\alpha_i})$ dans la base $([D_i],f_i)_{1\leqslant i\leqslant 2g}$ de $\mathrm{H}^1(X,\mu_n)$ pour obtenir la décomposition complète de $\sigma\cdot([D],D',f)$ dans la base $([D_i],D'_i,f_i)_{1\leqslant i\leqslant 2g+r}$.

Exemple 5.2.5. Soit E une courbe elliptique sur k. Soit $C=E-Z$ où $Z=\{P_1,\dots,P_r\}$. Le Λ-module $\mathrm{Div}^0_Z(E)\otimes\Lambda$ est engendré par les diviseurs de la forme $(P_i)-(P_r)$ pour $i=1,\dots,r-1$. Pour chaque $i\in\{1,\dots,r\}$, soit Q_i un point tel que $nQ_i=P_i$. Ces points s'obtiennent concrètement de la façon suivante. La multiplication par n sur E est donnée sur les abscisses des points par le polynôme de n-division $\phi_n\in k[x]$. Il suffit alors de résoudre $\phi_n(x)=x_{P_i}$; choisissons une solution x. L'un des deux points de E ayant x pour abscisse convient. Ayant ainsi obtenu des points $Q_1,\dots,Q_r$, posons $D_i=(Q_r)-(Q_i)$. Le diviseur $(P_i)-(P_r)+nD_i$ est alors principal, car de degré et de somme nuls. C'est un antécédent dans $\mathrm{H}^1(C,\mu_n)$ de $(P_i)-(P_r)$.

Voyons comment déterminer explicitement le $\Lambda[\mathfrak{G}_0]$-module $\mathrm{H}^1_c(U,\mu_n)$. Supposons X_0 décrite par un modèle plan birationnel C_0, tel que la restriction de $X \to C_0 \times_{k_0} k$ à Z soit un isomorphisme. Décrivons d'abord l'inclusion de $(\bigoplus_{z\in Z}\mu_n(k))/\mu_n(k)$ dans $\mathrm{H}^1_c(U,\mu_n)$. Notons $P_i = (x_i, y_i)$, $i = 1,\dots,r$ les points de $Z \subset C$, que nous pouvons tous supposer dans la carte affine $z \neq 0$. Soit $(\zeta_{P_1},\dots,\zeta_{P_r}) \in \mu_n(k)^Z$. La fonction

$$f(x,y) = \sum_{i=1}^{r} \zeta_{P_i} \prod_{j|x_j\neq x_i} \frac{x-x_j}{x_i-x_j} \prod_{j|y_j\neq y_i} \frac{y-y_j}{y_i-y_j} \tag{$\diamond$}$$

vérifie $f(P_i) = \zeta_{P_i}$ pour tout $i \in \{1\dots r\}$. L'image de $(\zeta_{P_1},\dots,\zeta_{P_r})$ dans $\mathrm{H}^1_c(U,\mu_n)$ est alors $\mathrm{div}(f)$. D'autre part, un antécédent dans $\mathrm{H}^1_c(U,\mu_n)$ d'un élément de $\mathrm{H}^1(X,\mu_n)$ représenté par un diviseur D se détermine de la façon suivante. Commençons par calculer un diviseur D' équivalent à D de support disjoint de Z, comme décrit dans l'annexe C.3.4. Le diviseur nD' est le diviseur d'une fonction f. Calculons, pour $i = 1,\dots,r$, une racine n-ième λ_i de $f(P_i)$ dans k, puis une fonction g telle que $g(P_i) = \lambda_i$ pour tout i. Le diviseur $D' - \mathrm{div}(g)$ est un antécédent de D dans $\mathrm{H}^1_c(U,\mu_n)$. En utilisant l'algorithme de Couveignes décrit dans la section IV.2, nous obtenons le résultat suivant.

Proposition 5.2.6. Il existe un algorithme probabiliste (Monte-Carlo) qui, étant donné une courbe projective lisse X_0 de genre g sur $\mathbb{F}_q$ représentée par un modèle plan de degré d, un entier n premier à q, un diviseur $\mathbb{F}_q$-rationnel de degré 1 sur X, le polynôme caractéristique de la fonction zêta de X_0 et un ensemble non vide $Z = \{P_1,\dots,P_r\} \subset X_0(\mathbb{F}_q)$ calcule un ensemble de diviseurs $D_1,\dots,D_{2g+r-1}$ de degré 0 sur $(X_0 - Z)_{\overline{\mathbb{F}_q}}$ dont les classes forment une base de $\mathrm{H}^1_c((X_0-Z)_{\overline{\mathbb{F}_q}},\mu_n)$. Le nombre d'opérations effectué est polynomial en d, $\log q$, n^{2g} et r.

Démonstration. Quitte à passer à une extension de degré d de $\mathbb{F}_q$ pour trouver un point $P_0 \in X(\mathbb{F}_q)$, l'algorithme de Couveignes renvoie des classes $D_1,\dots,D_{2g}$ de diviseurs de degré 0 sur X de la forme $G_i - gP_0$, où les G_i sont définis sur une extension de $\mathbb{F}_q$ de degré $O(gn^{2g})$, en temps polynomial en d, n^{2g} et $\log q$. Le calcul d'un diviseur équivalent à $G_i - gP_0$ de support disjoint de Z se fait donc en temps polynomial en d, n^{2g}, $\log q$ et r d'après l'annexe C.3.4. Les diviseurs $D_{2g+1},\dots,D_{2g+r-1}$ sont obtenus en calculant le diviseur de fonctions données par la formule ($\diamond$), qui sont de degré $O(r)$. □

Remarque 5.2.7. Le groupe $\mathrm{H}^1_c(U,\mu_n)$ se détermine très facilement une fois que l'on connaît une description de $\mathrm{H}^1(X,\mu_n)$ en termes de diviseurs. Ce n'est pas le cas de $\mathrm{H}^1(U,\mu_n)$, dont le calcul nécessite de déterminer des racines n-ièmes dans $\mathrm{Pic}(X)$. Si la dualité de Poincaré permet de décrire l'un des groupes à partir de l'autre, elle ne permet pas de déterminer une fonction f telle que $\mathrm{div}(f)$ soit un antécédent dans $\mathrm{H}^1(U,\mu_n)$ d'un diviseur de degré 0 supporté sur Z.

V.2.3 Fonctorialité en U

Soit U' une courbe affine lisse sur k munie d'un k-morphisme $f\colon U' \to U$. Soient X' la compactification lisse de U', et Z' le fermé réduit complémentaire de U' dans X'. Considérons également $V' = U \times_X X'$, et son fermé réduit complémentaire W' dans X'. Le diagramme commutatif suivant, dont les deux rectangles sont cartésiens, résume la situation.

$$\begin{tikzcd}
U' \arrow[r] \arrow[dr, "f"'] & V' \arrow[r] \arrow[d] & X' \arrow[d] & Z' \arrow[l] & W' \arrow[l] \arrow[d] \\
& U \arrow[r] & X & & Z \arrow[ll]
\end{tikzcd}$$

Décrivons comment calculer le morphisme $\mathrm{H}^1(U,\Lambda) \to \mathrm{H}^1(U',\Lambda)$ induit par f. La fonctorialité de la suite exacte précédente permet de calculer le morphisme $\mathrm{H}^1(U,\Lambda) \to \mathrm{H}^1(V',\Lambda)$, c'est-à-dire la

composée des morphismes de Λ-modules

$$\mathrm{H}^1(U,\Lambda) \xrightarrow{\sim} \mathrm{H}^1(X,\Lambda) \oplus \big(\mathrm{Div}^0_Z(X)\otimes\Lambda\big) \to \mathrm{H}^1(X',\Lambda) \oplus (\mathrm{Div}^0_{W'}(X')\otimes\Lambda) \xrightarrow{\sim} \mathrm{H}^1(V',\Lambda)$$

où le calcul de l'isomorphisme de droite repose sur celui d'une section Λ-linéaire s' de

$$\mathrm{H}^1(V',\Lambda) \to \mathrm{Div}^0_{W'}(X')\otimes\Lambda$$

compatible à f. Pour faire cela, notons s une section déjà calculée de $\mathrm{H}^1(X,\mu_n) \to \mathrm{Div}^0_Z(X)\otimes\Lambda$ et $\gamma\colon \mathrm{Div}^0_Z(X) \to \mathrm{Div}^0_{W'}(X')$. Pour chaque diviseur $w = \gamma(v) \in \mathrm{im}(\gamma)$, définissons $s'(w) := f^\star s(v)$. Pour les w qui ne sont pas dans l'image de γ, définissons $s'(w)$ comme étant une racine n-ième de w dans $\mathrm{Pic}^0(X')$.

Remarquons que la flèche $\mathrm{Div}^0_Z(X)\otimes\Lambda \to \mathrm{Div}^0_{W'}(X')\otimes\Lambda$ dépend des indices de ramification du morphisme : notons $|Z| = \{z_1,\dots,z_n\}$, $|W| = \{w_1,\dots,w_d\}$ avec $f(w_i) =: z_{\delta_i}$. L'image de $(f_0,\dots,f_s) \in \mathrm{H}^0(Z,\Lambda)$ est alors $(e_{w_i}(f)z_{\delta_i})_{1\leqslant i\leqslant d}$.

Le morphisme $\mathrm{H}^1(U,\Lambda) \to \mathrm{H}^1(U',\Lambda)$ se factorise par $\mathrm{H}^1(U,\Lambda) \to \mathrm{H}^1(V',\Lambda)$. Il reste à déterminer la flèche $\mathrm{H}^1(V',\Lambda) \to \mathrm{H}^1(U',\Lambda)$. Remarquons qu'avec la description explicite de $\mathrm{H}^1(V',\Lambda)$ et $\mathrm{H}^1(U',\Lambda)$ dont nous disposons, le morphisme $\mathrm{H}^1(V',\Lambda) \to \mathrm{H}^1(U',\Lambda)$ se calcule explicitement et est simplement une inclusion. À un triplet $([D],D',f)$ où $[D] \in \mathrm{Pic}(X')[n], D' \in \mathrm{Div}^0_{Z'}(X')\otimes\Lambda$ et $nD = D' + \mathrm{div}(f)$, il associe encore $([D],D',f)$. Il est donc possible de calculer explicitement un complémentaire de $\mathrm{H}^1(V',\Lambda)$ dans $\mathrm{H}^1(U',\Lambda)$, et ainsi représenter le morphisme composé

$$\mathrm{H}^1(U,\Lambda) \to \mathrm{H}^1(V',\Lambda) \hookrightarrow \mathrm{H}^1(U',\Lambda).$$

V.3 Cohomologie des faisceaux lisses

Cette section est dédiée au calcul du complexe de cohomologie d'un faisceau lisse sur une courbe lisse ou nodale sur un corps algébriquement clos. Dès que son genre géométrique est non nul, une telle courbe est un $K(\pi,1)$, et notre méthode consiste à calculer la cohomologie des faisceaux lisses comme cohomologie du groupe d'automorphismes d'un revêtement galoisien de la courbe. Nous commençons par décrire cette méthode, puis nous détaillons les algorithmes employés pour la mettre en œuvre et calculons leur complexité. Nous montrons également comment calculer explicitement les morphismes de la suite de Gysin. Nous donnons ensuite deux exemples de calcul de groupes de cohomologie. Nous terminons par la description de la généralisation de cette méthode à la détermination de la cohomologie d'un complexe de faisceaux lisses sur une telle courbe.

V.3.1 Calcul de la cohomologie

Rappelons que k est un corps algébriquement clos, et $\Lambda = \mathbb{Z}/n\mathbb{Z}$ avec n premier à la caractéristique de k. Soit U une courbe intègre lisse ou nodale de genre géométrique non nul sur k. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur U, de fibre générique géométrique M. D'après la proposition 2.6.8, U est un $K(\pi,1)$: le morphisme canonique

$$\mathrm{R}\Gamma(\pi_1(U),M) \to \mathrm{R}\Gamma(U,\mathcal{F})$$

est un isomorphisme dans $\mathrm{D}^b_c(\Lambda)$. Soit $f\colon V \to U$ un revêtement qui trivialise $\mathcal{F}$. Considérons un revêtement caractéristique $W \to V$ trivialisant tous les $f^\star\mathcal{F}$-torseurs sur V, par exemple celui construit dans la section II.7.1.1. Le revêtement $W \to U$ est encore galoisien. Notons $G = \mathrm{Aut}(W|U)$.

Proposition 5.3.1. Le morphisme canonique

$$\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G,M) \to \tau_{\leqslant 1}\,\mathrm{R}\Gamma(\pi_1(U),M) \xrightarrow{\sim} \tau_{\leqslant 1}\,\mathrm{R}\Gamma(U,\mathcal{F})$$

dans $\mathrm{D}_c^b(\Lambda)$ induit par le quotient $\pi_1(U) \to G$ est un isomorphisme dans $\mathrm{D}_c^b(\Lambda)$.

Démonstration. La suite spectrale de Hochschild-Serre fournit la suite exacte courte

$$0 \to \mathrm{H}^1(G,M) \to \mathrm{H}^1(U,\mathcal{F}) \to \mathrm{H}^0(G,\mathrm{H}^1(W,\mathcal{F}|_W)).$$

Comme $W \to V$ trivialise tous les M-torseurs, le morphisme $\mathrm{H}^1(U,\mathcal{F}) \to \mathrm{H}^1(W,\mathcal{F}|_W)$ est nul. Par conséquent, le morphisme

$$\mathrm{H}^1(G,M) \to \mathrm{H}^1(U,\mathcal{F})$$

induit par le quotient $\pi_1(U) \to G$ est un isomorphisme. De même, le morphisme $\mathrm{H}^0(G,M) \to \mathrm{H}^0(U,\mathcal{F})$ est un isomorphisme. Ceci implique que le morphisme composé

$$\mathrm{R}\Gamma(G,M) \to \mathrm{R}\Gamma(\pi_1(U),M) \xrightarrow{\sim} \mathrm{R}\Gamma(U,\mathcal{F})$$

dans $\mathrm{D}_c^b(\Lambda)$ est un quasi-isomorphisme en degrés 0 et 1. □

Remarque 5.3.2. Dans le cas où U est affine, $\mathrm{H}^i(U,\mathcal{F}) = 0$ dès que $i \geqslant 2$. Par conséquent, le morphisme

$$\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G,M) \to \tau_{\leqslant 1}\,\mathrm{R}\Gamma(\pi_1(U),M) \to \tau_{\leqslant 1}\,\mathrm{R}\Gamma(U,\mathcal{F}) \to \mathrm{R}\Gamma(U,\mathcal{F})$$

est un isomorphisme dans $\mathrm{D}_c^b(\Lambda)$.

Dans le cas où U est projective, choisissons deux ouverts U_1, U_2 de U. Le triangle de Mayer-Vietoris (voir section I.5.3) assure alors que

$$\mathrm{R}\Gamma(U,\mathcal{F}) = \text{cône}\left((\mathrm{R}\Gamma(\mathrm{U}_1,\mathcal{F}) \oplus \mathrm{R}\Gamma(\mathrm{U}_2,\mathcal{F}) \to \mathrm{R}\Gamma(\mathrm{U}_1 \cap \mathrm{U}_2,\mathcal{F})\right)[-1].$$

Fonctorialité sur $\operatorname{Spec} k$ Soit $\phi\colon U' \to U$ un morphisme de courbes affines intègres lisses sur k. Soit $\mathcal{F}$ un faisceau lisse sur U. Expliquons comment calculer le morphisme $\mathrm{R}\Gamma(U,\mathcal{F}) \to \mathrm{R}\Gamma(U',\phi^\star\mathcal{F})$ déduit de ϕ par fonctorialité. Soit $f\colon V \to U$ un revêtement galoisien de U qui trivialise $\mathcal{F}$. Ici, nous supposons que W est le revêtement V_2 de V de groupe $H^1(V,\Lambda)^\vee$ construit dans la section II.7.1.1. Calculons une décomposition primaire de $V \times_U U'$ (voir annexe C.2). Considérons une composante connexe V' de $V \times_U U'$. Notons K, K' les corps de fonctions respectifs de V, V'. Quitte à le remplacer par sa clôture galoisienne sur U, supposons $V' \to U$ galoisien. Le schéma W est la normalisation de V dans $K(\sqrt[n]{g_1},\ldots,\sqrt[n]{g_r})$, où les g_i ont un diviseur multiple de n dans $\operatorname{Pic}(X)$; considérons de même le revêtement W' de V' de groupe $\mathrm{H}^1(V',\Lambda)^\vee$. Notons L, L' les corps de fonctions respectifs de W, W'. Soit $T' \to V'$ la normalisation de V' dans $K'(\sqrt[n]{g_1},\ldots,\sqrt[n]{g_r}) \subseteq L'$. Le diagramme commutatif suivant, dont les deux flèches verticales composées sont des revêtements galoisiens, résume la situation.

$$\begin{tikzcd}
W' \arrow[d] & \\
T' \arrow[r] \arrow[d] & W \arrow[d] \\
V' \arrow[r] \arrow[d] & V \arrow[d, "f"] \\
U' \arrow[r, "\phi"] & U
\end{tikzcd}$$

Le morphisme $W' \to W$ ainsi obtenu induit un morphisme $u\colon \mathrm{Aut}(W'|U') \to \mathrm{Aut}(W|U)$. En effet, comme $L/k(U)$ est normale, tout élément de $\mathrm{Aut}(L'|k(U')) \subseteq \mathrm{Aut}(L'|k(U))$ donne par restriction un élément de $\mathrm{Aut}(L|k(U)) = \mathrm{Aut}(W|U)$. Ce morphisme $\mathrm{Aut}(W'|U') \to \mathrm{Aut}(W|U)$ donne par fonctorialité le morphisme cherché entre les complexes de Λ-modules représentant

$$\mathrm{R}\Gamma(\mathrm{Aut}(W|U), M) \to \mathrm{R}\Gamma(\mathrm{Aut}(W'|U'), M).$$

Remarque 5.3.3. Le morphisme $\mathrm{H}^1(U, \mathcal{F}) \to \mathrm{H}^1(V, \mathcal{F}|_V)$ est en particulier très simple à calculer : c'est simplement le morphisme $\mathrm{H}^1(G, M) \to \mathrm{H}^1(\mathrm{H}^1(V, \Lambda)^\vee, M)$ déduit de l'inclusion $\mathrm{H}^1(V, \Lambda)^\vee \subset G$.

Action de $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$ Supposons désormais que $U, \mathcal{F}$ proviennent par changement de base d'une courbe géométriquement connexe U_0 sur k_0 et d'un faisceau lisse $\mathcal{F}_0$ sur U_0 trivialisé par $f_0\colon V_0 \to U_0$. Notons $V = V_0 \times_{k_0} k$.

1. Traitons d'abord le cas où V est connexe et possède un k_0-point y_0. Soit $\bar{y}_0$ un point géométrique de V au-dessus de y_0, d'image un point géométrique $\bar{x}_0$ de U. Soit toujours $W = V_2$ le revêtement de V de groupe $\mathrm{H}^1(V, \Lambda)^\vee$. Notons $\bar{z}_0$ un point géométrique de W d'image un point géométrique $\bar{y}_0$ au-dessus de y_0. Pour tout $\sigma \in \mathfrak{G}_0$, l'automorphisme

$$\sigma_\star\colon \pi_1(U, \bar{x}_0) \to \pi_1(U, \bar{x}_0)$$

se restreint en un automorphisme de $\pi_1(V, \bar{y}_0)$, et donc encore en un automorphisme de $\pi_1(W, \bar{z}_0)$ puisque ce dernier est caractéristique dans $\pi_1(V)$. Par conséquent, il induit par passage au quotient un automorphisme de $\mathrm{Aut}(W|U)$. L'action de $\mathfrak{G}_0$ sur $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(\mathrm{Aut}(W|U), M)$ découle alors de son action sur $\mathrm{Aut}(W|U)$ par fonctorialité. Cette méthode sera illustrée dans la section V.3.4.

2. Supposons désormais que V n'est pas connexe, c'est-à-dire que $k_0(V_0)$ contient une extension finie non triviale de k_0. Construisons le revêtement $V_{2,0} \to V_0$ défini sur k_0 décrit dans la section II.7.2. Notons $W = V_{2,0} \times_{k_0} k$. Alors $W \to U$ est encore un $G = \mathrm{Aut}(V_{2,0}|U_0)$-torseur, et le même raisonnement permet de calculer $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(\mathrm{Aut}(V_{2,0}|U_0), \mathrm{H}^0(W, \mathcal{F}))$. Remarquons que les composantes connexes de W sont permutées par un groupe $\mathrm{Gal}(L'|k_0)$, où L' est une extension galoisienne de k_0. Ceci permet de calculer l'action de $\mathfrak{G}_0$ sur $\mathrm{H}^0(W, \mathcal{F})$. Le groupe $\mathfrak{G}_0$ agit ici trivialement sur $\mathrm{Aut}(V_{2,0}|U_0)$, puisque $V_{2,0}$ est défini sur k_0. Soient V' une composante connexe de V et W' une composante connexe de W d'image V'. Il y a une suite exacte

$$1 \to \mathrm{Aut}(W'|V') \to G \to \mathrm{Gal}(L'|k_0) \to 1$$

et

$$\mathrm{H}^0(W, \mathcal{F}) = \mathrm{ind}_{\mathrm{Aut}(W'|V')}^G \mathrm{H}^0(W', \mathcal{F}).$$

Le complexe $\mathrm{R}\Gamma(G, \mathrm{H}^0(W, \mathcal{F}))$ ainsi calculé, muni d'une action naturelle de $\mathfrak{G}_0$, représente bien $\mathrm{R}\Gamma(U, \mathcal{F})$, car le lemme de Shapiro [Neu13, Th. 4.19] assure qu'il y a un isomorphisme

$$\mathrm{R}\Gamma(G, \mathrm{H}^0(W, \mathcal{F})) = \mathrm{R}\Gamma(\mathrm{Aut}(W'|V'), \mathrm{H}^0(W', \mathcal{F})).$$

Mise en garde Il serait tentant, lorsque U est affine, de faire le raisonnement suivant. Le morphisme $V \to U$ étant galoisien, $\mathrm{R}\Gamma(U, \mathcal{F}) = \mathrm{R}\Gamma(\mathrm{Aut}(V|U), \mathrm{R}\Gamma(V, \mathcal{F}|_V))$. Comme V est un $K(\pi, 1)$, un complexe représentant $\mathrm{R}\Gamma(V, \mathcal{F}|_V)$ est le complexe de cochaînes usuel calculant $\mathrm{R}\Gamma(\pi_1(V, y), M)$. Il peut même être tronqué en degré $\leqslant 1$ puisque V est affine. Le morphisme

$$\tau_{\leqslant 1}\,\mathrm{R}\Gamma(\mathrm{Aut}(V_2|V), M) \to \tau_{\leqslant 1}\,\mathrm{R}\Gamma(\pi_1(V, y), M)$$

est encore un quasi-isomorphisme par les arguments ci-dessus. Comme $\mathcal{F}$ est constant sur V, l'action de $\pi_1(V,y)$ sur M est triviale ; par conséquent, la première flèche du complexe calculant $\mathrm{R}\Gamma(\mathrm{Aut}(V_2|V),M)$ est nulle. Il en découle que $\mathrm{R}\Gamma(V,\mathcal{F}|_V)$ est représenté par le complexe

$$\mathrm{H}^0(V,\mathcal{F}|_V) \xrightarrow{0} \mathrm{H}^1(V,\mathcal{F}|_V).$$

L'action de $\mathrm{Aut}(V|U)$ sur $\mathrm{Aut}(V_2|V) = \mathrm{H}^1(V,\Lambda)^\vee$, et donc sur ce complexe, se calcule aisément. Ceci permettrait de déterminer $\mathrm{R}\Gamma(\mathrm{Aut}(V|U),\mathrm{R}\Gamma(V,\mathcal{F}|_V))$ sans avoir à calculer de revêtement de V. L'erreur est la suivante : le complexe $\mathrm{H}^0(V,\mathcal{F}|_V) \xrightarrow{0} \mathrm{H}^1(V,\mathcal{F}|_V)$ représente $\mathrm{R}\Gamma(V,\mathcal{F}|_V)$ dans $\mathrm{D}^b_c(\Lambda)$, et ses groupes de cohomologie sont munis d'une action naturelle de $\mathrm{Aut}(V|U)$. Mais ce complexe *ne représente en général pas* $\mathrm{R}\Gamma(V,\mathcal{F}|_V)$ dans $\mathrm{D}^b_c(\Lambda[\mathrm{Aut}(V|U)])$. Lorsque $[V:U]$ est divisible par n, ce n'est pas le cas. Prenons l'exemple de $V = U = \mathbb{G}_m$ et $f\colon V \to U, x \mapsto x^n$. Considérons le faisceau constant Λ sur U. Alors

$$\mathrm{R}\Gamma(V,\Lambda) = [\Lambda \xrightarrow{0} \Lambda]$$

et l'action de $\mathrm{Aut}(V|U) \simeq \mu_n(k)$ sur $\mathrm{H}^0(V,\Lambda)$ et $\mathrm{H}^1(V,\Lambda)$ est triviale puisque $\mu_n(k)$ fixe les points 0 et ∞. Par conséquent, $\mathrm{R}\Gamma(V,\Lambda)$ est le complexe de $\mu_n(k)$-modules triviaux $\Lambda[0] \oplus \Lambda[-1]$, et pour tout entier $i \geqslant 0$, $\mathrm{H}^i(U,\Lambda) = \mathrm{H}^i(\mu_n(k),\Lambda) \oplus \mathrm{H}^{i-1}(\mu_n(k),\Lambda)$. Ce résultat est absurde puisque ces groupes doivent être nuls en degré $i \geqslant 2$, et que $\mathrm{H}^1(U,\Lambda)$ est de rang 1 et non 2.

V.3.2 Algorithmes et complexité

Nous allons décrire ici les algorithmes permettant de calculer explicitement la cohomologie d'un faisceau lisse par la méthode décrite dans la section précédente. Rappelons les notations : U_0 est une courbe lisse géométriquement connexe sur le corps parfait k_0, et $V_0 \to U_0$ est un revêtement galoisien. Supposons d'abord par simplicité que V_0 est géométriquement connexe. Les courbes U, V sont les changements de base de U_0, V_0 à la clôture algébrique k de k_0. Le revêtement caractéristique $V_2 \to V$ défini dans la section II.7.1.1 a pour groupe $H^1(V,\Lambda)^\vee$.

Pour les résultats de complexité, nous noterons $C(g,q,n,r)$ la complexité du calcul de $\mathrm{H}^1(U,\mu_n)$, où U est une courbe intègre lisse sur $\overline{\mathbb{F}_q}$ provenant de $\mathbb{F}_q$, de compactification lisse X de genre g, avec $r = |X - U|$. Notons également $D(g,n,r)$ le degré de la plus petite extension de $\mathbb{F}_q$ sur laquelle sont définis les éléments de $\mathrm{H}^1(U,\mu_n)$ obtenus. Une majoration de ces deux entiers est donnée à la fin de la section IV.3.4.1.

Remarque 5.3.4. Il est possible de majorer $D(g,n,r)$ par $|\operatorname{Aut}_\Lambda \mathrm{H}^1(U,\mu_n)| = \mathcal{O}(n^{(2g+r)^2})$. En effet, l'action de $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$ sur $\mathrm{H}^1(U,\mu_n)$ se factorise par un quotient $\mathfrak{G}_1$ d'ordre $|\operatorname{Aut}_\Lambda \mathrm{H}^1(U,\mu_n)|$, c'est-à-dire le groupe de Galois d'une extension de $\mathbb{F}_q$ d'ordre $\mathcal{O}(n^{(2g+r)}{}^2)$ que l'on peut fixer. Les classes dans $\mathrm{Pic}(X)$ des diviseurs obtenus représentant des éléments de $\mathrm{H}^1(U,\mu_n)$ sont toutes $\mathfrak{G}_1$-invariantes, et l'algorithme de la proposition C.3.9 permet alors de trouver des diviseurs $\mathfrak{G}_1$-invariants qui leur sont équivalents ; la complexité de cette opération est négligeable devant celle des algorithmes de calcul du H^1.

Calcul de $\mathrm{Aut}(V_2|U)$ Soit $\tau \in \mathrm{Aut}(k(V)/k(U))$. Notons $t = 2g + r$. Il y a n^t automorphismes de $k(V_2)$ de restriction τ ; voici comment en construire un. Soit

$$\mathcal{B} = (([D_1], D_1', g_1), \ldots, ([D_t], D_t', g_t))$$

une Λ-base de $\mathrm{H}^1(V,\mu_n)$. Fixons $f_i = \sqrt[n]{g_i}$. Un automorphisme σ de $k(V_2)$ de restriction τ vérifie nécessairement $\sigma(f_i)^n = \tau(g_i)$. Calculons une racine n-ième de $\tau(g_i)$. Décomposons l'élément $\tau^\star([D_i], D_i', g_i)$ de $\mathrm{H}^1(V,\mu_n)$ dans la base $\mathcal{B}$: cela revient à calculer des éléments $\alpha_{ij} \in \Lambda$ tels que

$$(\tau^\star[D_i], \tau^\star D_i', \tau(g_i)) = \sum_{j=1}^{t} \alpha_{ij}([D_j], D_j', g_j)$$

dans $\mathrm{H}^1(V, \mu_n)$. Il existe d'après le lemme 5.2.2 une fonction $h_i \in k(V)^\times$ et des entiers a_{ij} relevant les α_{ij} tels que

$$\left(h_i \prod_{j=1}^{t} f_j^{a_{ij}}\right)^n = \tau(g_i)$$

dans $k(V)$. Une racine n-ième de $\tau(g_i)$ dans $k(V_2)$ s'obtient alors sous la forme

$$f_{\tau,i} := h_i \prod_{j=1}^{t} f_j^{a_{ij}}.$$

Soit $(b_1, \ldots, b_s)$ une $k(U)$-base de $k(V)$. Alors

$$(b_i f_1^{a_1} \ldots f_t^{a_t})_{1 \leqslant i \leqslant s, 0 \leqslant a_j \leqslant n-1}$$

est une $k(U)$-base de $k(V_2)$. L'endomorphisme σ de $k(V_2)$ défini par

$$\sigma(b_i f_1^{a_1} \ldots f_t^{a_t}) = \tau(b_i) f_{\tau,1}^{a_1} \ldots f_{\tau,t}^{a_t}$$

est un élément de $\mathrm{Aut}(k(V_2)|k(U))$ dont la restriction à $k(V)$ vaut τ. Les autres antécédents de τ dans $\mathrm{Aut}(k(V_2)|k(U))$ sont obtenus en composant celui-ci avec un élément de $\mathrm{Aut}(k(V_2)|k(V)) \simeq \mathrm{Hom}_\Lambda(\mathrm{H}^1(V, \mu_n), \mu_n)$.

L'algorithme pour calculer σ est donc le suivant : pour chaque $i \in \{1 \ldots t\}$, calculer $\tau^\star([D_i], D_i', g_i)$, puis déterminer h_i grâce à la preuve du lemme 5.2.2, et en déduire $f_{\tau,i}$. Rappelons (voir remarque 5.2.3) que le calcul de h_i nécessite des calculs d'espaces de Riemann-Roch de diviseurs sur V qui sont chacun différence de deux diviseurs effectifs de même degré $g+n$, ainsi que le calcul d'une racine n-ième dans k. La complexité du calcul de $\mathrm{Aut}(V_2|U)$, qui est d'ordre $\deg(V \to U)n^t$, est donc dominée par celle du calcul des $f_{\tau,i}$, c'est-à-dire de $\mathrm{H}^1(V, \mu_n)$.

Considérons désormais le cas général du calcul de $\mathrm{R}\Gamma(U, \mathcal{F})$: nous ne supposons plus V_0 géométriquement connexe. Le revêtement galoisien calculé, que nous noterons $V_{2,0} \to U_0$, est celui décrit dans la section II.7.2. Le diagramme suivant, dont le carré est cartésien, résume les notations.

$$\begin{tikzcd}
 & V_{2,0} \arrow[d] \\
V \arrow[r] \arrow[d] & V_0 \arrow[d] \\
U \arrow[r] & U_0
\end{tikzcd}$$

Ordre de $\mathrm{Aut}(V_{2,0}|U_0)$ Nous avons vu dans la section II.7.2 comment le déduire du calcul de $\mathrm{Aut}(V_2|U)$. Calculons son ordre lorsque $k_0 = \mathbb{F}_q$. Notons $r = |X - U|$, où X est la compactification lisse de U. Rappelons que le corps de fonctions de $V_{2,0}$ contient une extension L de k_0, qui est la composée de la clôture algébrique k_1 de k_0 dans $k_0(V_0)$, de $k_0(\mu_n)$ et de l'extension de k_0 par laquelle se factorise l'action de $\mathrm{Gal}(k|k_0)$ sur $\mathrm{H}^1(V_0 \times_{k_0} k, \Lambda)$. Soit $V^{(1)}$ une composante connexe de $V_{2,0} \times_{k_0} k$; d'après la formule de Riemann-Hurwitz, son genre est $O((g+r)[V^{(1)} : U]) = O((g+r)\frac{[V_0:U_0]}{[k_1:k_0]})$, où g est le genre de X. Notons $d = \frac{[V_0:U_0]}{[k_1:k_0]}$. D'après les lemmes 2.7.11 et 2.4.3, l'ordre de $G = \mathrm{Aut}(W_0|U_0)$ est donné par

$$\begin{aligned}
|G| &= n^{2g(V^{(1)})} \times [L : k_1] \times [V_0 : U_0] \\
&= O\left(g(V^{(1)}) n D(g(V^{(1)}), q, n, dr)\right) [V_0 : U_0] \\
&= O\left((g+r) dn [V_0 : U_0] D(d(2g+r), n, dr)\right).
\end{aligned}$$

Rappelons que $[V_0 : U_0]$ est l'ordre du groupe de monodromie $\mathfrak{S} \subseteq \mathrm{Aut}_\Lambda(M)$. De plus, la remarque 5.3.4 assure que $D(g,n,r)$ est majoré par n^{2g+r}. En particulier, si $M = \Lambda^j$, $|\mathrm{Aut}_\Lambda(M)| = O(n^{j^2})$ et

$$|G| \leqslant (2g+r)n^{2j^2+3(2g+r)n^{j^2}}.$$

Cette majoration donne une bonne idée de la complexité de l'algorithme dans le pire cas, mais cache le fait qu'à taille constante de groupe de monodromie, cette complexité est polynomiale en $j^3n^{2^g}$. Si la courbe V admet un modèle plan à singularités ordinaires de degré $O(g)$ (ce qui est le cas pour une courbe générale), cette complexité est $O(j^3n^{g^4})$.

Calcul de $\mathrm{R}\Gamma(U,\mathcal{F})$ En supposant que l'on ait déjà construit le revêtement $V_{2,0} \to U_0$ et calculé son groupe de Galois, il ne reste plus qu'à calculer le complexe $\mathrm{R}\Gamma(G,M)$ où $G = \mathrm{Aut}(V_{2,0}|U_0)$ grâce à la résolution libre usuelle (résolution bar) de Λ comme $\Lambda[G]$-module. Le module $M = \mathrm{H}^0(V,\mathcal{F})$ est représenté comme quotient d'un module libre : $M = \Lambda^m/N$. Rappelons que nous souhaitons calculer la cohomologie de G à valeurs dans un module M' induit à partir de M, isomorphe comme Λ-module à $M^{[k_1:k_0]}$. Notons $s = [k_1 : k_0] \leqslant [V_0 : U_0]$. Rappelons que l'ordre de G est $d = [L : k_1]n^r[V_0 : U_0]$, où $r = \mathrm{rg}_\Lambda(\mathrm{H}^1(V^{(1)},\Lambda))$. Le complexe représentant $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(U,\mathcal{F})$ est donc une troncature de la dernière ligne du diagramme commutatif à colonnes exactes suivant.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
N \arrow[r] \arrow[d] & N^d \arrow[r] \arrow[d] & N^{d^2} \arrow[d] \\
\Lambda^{sm} \arrow[r] \arrow[d] & \Lambda^{dsm} \arrow[r] \arrow[d] & \Lambda^{d^2sm} \arrow[d] \\
M^s \arrow[r] \arrow[d] & M^{sd} \arrow[r] \arrow[d] & M^{sd^2} \arrow[d] \\
0 & 0 & 0
\end{tikzcd}$$

Les calculs effectués pour déterminer $\mathrm{R}\Gamma(U,\mathcal{F})$ étant simplement des calculs de noyaux et conoyaux de morphismes de Λ-modules engendrés par au plus sd^2m éléments, la complexité du calcul de $\mathrm{R}\Gamma(U,\mathcal{F})$ est $O((sd^2m)^3)$ opérations dans Λ.

Théorème 5.3.5. Soit U_0 une courbe lisse géométriquement connexe sur $\mathbb{F}_q$. Notons $U = (U_0)_{\overline{\mathbb{F}_q}}$. Notons X sa compactification lisse, g son genre, et $r = |X - U|$. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur U_0 de fibre générique géométrique un Λ-module M à m générateurs ; notons $\mathfrak{S}$ l'image de $\pi_1(U)$ dans M, et d son ordre. Supposons donné un revêtement galoisien $V_0 \to U_0$ de groupe $\mathfrak{S}$ qui trivialise $\mathcal{F}$. Il existe un algorithme calculant un complexe de $\Lambda[\mathfrak{G}_0]$-modules représentant $\mathrm{R}\Gamma(U,\mathcal{F})$ en

$$O\left(C(d(g+r),q,n,dr) + (md^3n^{4d(g+2r)}D(d(2g+r),n,dr))^3\right)$$

opérations dans $\mathbb{F}_q$.

Démonstration. L'algorithme consiste à calculer le revêtement caractéristique $V_{2,0}$ de V_0 défini à partir de $\mathrm{H}^1(V,\Lambda)$, son groupe d'automorphismes G ainsi que $\mathrm{R}\Gamma(G,M')$ où $M' = \mathrm{H}^0(V_{2,0} \times_{k_0} k, \mathcal{F})$. Le rang de $\mathrm{H}^1(V^{(1)},\Lambda)$ est inférieur à $2d(g+r) + dr - 1 = 2d(g+2r) - 1$. L'ordre du groupe $G = \mathrm{Aut}(V_{2,0}|U_0)$

est donc inférieur à $dn^{2d(g+2r)}D(g,n,r)$. L'estimation précédente du coût du calcul de $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G,M')$ à partir de G permet de conclure. $\square$

Corollaire 5.3.6. Avec les notations et hypothèses du théorème, il existe un algorithme probabiliste (Las Vegas) qui calcule $\mathrm{R}\Gamma(U,\mathcal{F})$ en

$$\mathcal{P}(d,g,n,r,m,\log q)^{2^{O\left((d(g+r))^2\right)}}$$

opérations dans $\mathbb{F}_q$, où $\mathcal{P}$ est un polynôme. Si V admet un modèle plan ordinaire de degré $O(g)$, cette complexité devient

$$\mathcal{P}(d,g,n,r,m,\log q)^{O\left((d(g+r))^4\right)}.$$

Démonstration. Nous avons utilisé les majorations de $C(g,q,n,r)$ et $D(g,n,r)$ obtenues dans la section IV.3.4.1 : ils sont tous les deux bornés par $\mathcal{P}(d,g,n)^{O(g^4)}$ pour une courbe à singularités ordinaires, et donc $\mathcal{P}(d,g,n)^{2^{O(4g^2)}}$ pour une courbe quelconque. $\square$

V.3.3 Suite de Gysin

Soit $f\colon Y \to X$ un revêtement galoisien de courbes intègres projectives lisses sur k. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X, trivialisé par f. Notons $F = \mathrm{H}^0(Y, f^\star\mathcal{F})$. Soit Z un fermé réduit non vide de X. Notons U son ouvert complémentaire, $W = Z \times_X Y$ et $V = U \times_X Y$. Les notations sont résumées par le diagramme commutatif suivant, dont les deux carrés sont cartésiens.

$$\begin{tikzcd}
V \arrow[r] \arrow[d] & Y \arrow[d] & W \arrow[l] \arrow[d] \\
U \arrow[r] & X & Z \arrow[l]
\end{tikzcd}$$

Les suites exactes de Gysin pour $\mathcal{F}$ sur X et pour le faisceau constant F sur Y fournissent le diagramme commutatif

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(X,\mathcal{F}) \arrow[r] \arrow[d] & \mathrm{H}^1(U,\mathcal{F}) \arrow[r] \arrow[d] & \mathrm{H}^0(Z,\mathcal{F}(-1)) \arrow[r] \arrow[d] & \mathrm{H}^0(X,\mathcal{F}(-1)^\vee)^\vee \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{H}^1(Y,F) \arrow[r] & \mathrm{H}^1(V,F) \arrow[r] & \mathrm{H}^0(W,F(-1)) \arrow[r] & F(-1) \arrow[r] & 0
\end{tikzcd}$$

dont la ligne inférieure est celle de la section II.4.1.3.

Le morphisme $\mathrm{H}^0(Z,\mathcal{F}(-1)) = \mathrm{H}^0(Z,F(-1)) \to \mathrm{H}^0(W,F(-1))$ s'écrit

$$F(-1)^Z \to F(-1)^W, (a_z)_{z\in Z} \mapsto ((a_z)_{w\in W_z})_{z\in Z}$$

et admet une rétraction r donnée par des projections. Ceci permet de calculer le morphisme

$$\mathrm{H}^1(U,\mathcal{F}) \to \mathrm{H}^0(Z,\mathcal{F}(-1))$$

comme la composée

$$\mathrm{H}^1(U,\mathcal{F}) \to \mathrm{H}^1(V,F) \to \mathrm{H}^0(W,F(-1)) \xrightarrow{r} \mathrm{H}^0(Z,\mathcal{F}(-1)).$$

La flèche $\mathrm{H}^0(Z,\mathcal{F}(-1)) \to \mathrm{H}^0(X,\mathcal{F}(-1)^\vee)^\vee$ associe à $(a_z)_{z\in Z}$ le morphisme $\mathrm{H}^0(X,\mathcal{F}(-1)^\vee) \to \Lambda$ qui à $u\colon \mathcal{F}(-1) \to \Lambda$ associe $\sum_{z\in Z} u_z(a_z)$. La flèche verticale de droite associe à $u\colon \mathrm{H}^0(X,\mathcal{F}(-1)^\vee) \to \Lambda$ l'élément $\deg(f)u|_Y\colon F(-1)^\vee \to \Lambda$ de $F(-1)^{\vee\vee} = F(-1)$.

V.3.4 Trois exemples détaillés

V.3.4.1 Un ouvert de $\mathbb{P}^1$

Posons $n = 2$. Supposons que -1 n'est pas un carré dans le corps parfait k_0. Notons $V = \mathbb{P}^1 - \{0, \pm 1, \infty\}$ et $U = \mathbb{P}^1 - \{0, 1, \infty\}$. Considérons le revêtement étale de degré 2

$$\begin{array}{rccc} f\colon & V & \longrightarrow & U \\ & y & \longmapsto & y^2 \end{array}$$

de groupe d'automorphismes engendré par $\tau\colon y \mapsto -y$. Le faisceau $\mathcal{F} := f_\star\Lambda$ est un faisceau lisse sur U, trivialisé par le revêtement $f\colon V \to U$ puisque $f^\star f_\star\Lambda \simeq \Lambda^2$. Il correspond au $\mathrm{Aut}(V|U)$-module Λ^2, où l'élément non trivial de $\mathrm{Aut}(V|U)$ intervertit les deux copies de Λ. Comme f est fini, $\mathrm{R}f_\star\Lambda = (f_\star\Lambda)[0]$ et il y a un isomorphisme canonique

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

Nous devrions donc trouver

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

Nous avons déjà calculé dans l'exemple de la section II.7.4 le revêtement $V_2 \to V$ de groupe $\mathrm{H}^1(V, \Lambda)^\vee$. C'est la normalisation de V dans

$$\begin{array}{rcl} \mathrm{Proj}\, k[y, z, t, h]/(z^2 - (y^2 - h^2), t^2 - (y^2 + h^2)) & \longrightarrow & \mathrm{Proj}\, k[y, h] = \bar{V} \\ (y : z : t : h) & \longmapsto & (y^2 : h^2). \end{array}$$

Le groupe $G = \mathrm{Aut}(V_2|U)$ est d'ordre 16, engendré par $\gamma(y, z, t, h) = (\sqrt{-1}y, \sqrt{-1}t, \sqrt{-1}z, h)$ et trois éléments $\sigma_1, \sigma_2, \sigma_3$ d'ordre 2.

Calcul de $\mathrm{R}\Gamma(U, \mathcal{F})$ Un complexe à deux termes représentant $\mathrm{R}\Gamma(U, \mathcal{F})$ est

$$\Lambda^2 \to \{f\colon G \to \Lambda^2 \mid \forall g, h \in G, f(gh) = f(g) + gf(h)\}.$$

Un morphisme croisé $f\colon G \to \Lambda^2$ est déterminé par les images de $\sigma_1, \sigma_2, \sigma_3, \gamma$. En exploitant les relations $\gamma\sigma_1 = \sigma_1\gamma, \gamma\sigma_2 = \sigma_3\gamma$ et $\gamma^2 = \sigma_1\sigma_2\sigma_3$, il vient qu'un tel morphisme croisé est uniquement déterminé par un quadruplet $(a, a_1, a_2, a_3) \in \Lambda^4$; le morphisme croisé correspondant à ce quadruplet vérifie $f(\sigma_1) = (a_1, a_1)$, $f(\sigma_2) = (a_2, a_3)$, $f(\sigma_3) = (a_3, a_2)$ et $f(\gamma) = (a, a + a_1 + a_2 + a_3)$. Parmi ceux-ci, les morphismes croisés principaux sont les images de $(0, 0, 0, 0)$ et $(1, 0, 0, 0)$. Le complexe calculé est donc isomorphe à

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

et ses groupes de cohomologie sont Λ et Λ^3, ce qui est le résultat attendu.

Action de Galois L'action de $\mathfrak{G}_0 = \mathrm{Gal}(k|k_0)$ sur $\mathrm{Aut}(Y|X)$ se factorise manifestement par le quotient $\mathrm{Gal}(k_0(\sqrt{-1})|k_0)$. Ce groupe est engendré par la conjugaison $\sqrt{-1} \mapsto -\sqrt{-1}$. L'automorphisme ϕ agit trivialement sur $\sigma_1, \sigma_2, \sigma_3$, et $\phi \cdot \gamma = \sigma_1\sigma_2\sigma_3\gamma\colon (y, z, t) \mapsto (-\sqrt{-1}y, -\sqrt{-1}z, -\sqrt{-1}t)$. L'action de ϕ sur Λ^2 est triviale, et son action sur le groupe Λ^4 des morphismes croisés est $(\phi \cdot f)(x) = \phi f(\phi^{-1}x) = f(\phi^{-1}x)$. Explicitement, comme $\phi \cdot \gamma = \sigma_1\sigma_2\sigma_3\gamma$, cette action est

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

V.3.4.2 Une courbe elliptique

Cet exemple illustre la possibilité que les groupes de cohomologie d'un faisceau lisse dont la fibre générique géométrique est un Λ-module libre ne soient pas des Λ-modules libres. Soit E une courbe elliptique sur un corps algébriquement clos de caractéristique impaire. Posons $n = 4$. L'isogénie de multiplication par 2 sur E est un revêtement galoisien de groupe $(\mathbb{Z}/2\mathbb{Z})^2$; notons $E' \to E$ ce revêtement. Considérons le faisceau lisse $\mathcal{F}$ de $\Lambda = \mathbb{Z}/4\mathbb{Z}$-modules de fibre $M = \Lambda^2$ sur E trivialisé par $E' \to E$, correspondant à la représentation :

$$\begin{array}{rcl} (\mathbb{Z}/2\mathbb{Z})^2 & \longrightarrow & \mathrm{GL}_2(\Lambda) \\ (1,0),(0,1) & \longmapsto & \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \end{array}$$

Le groupe $\mathrm{H}^0(E,\mathcal{F}) = \mathrm{H}^0((\mathbb{Z}/2\mathbb{Z})^2, M)$ est $2\Lambda \times \Lambda \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$. Le revêtement $E'_2 \to E'$ de groupe $\mathrm{H}^1(E',\Lambda)^\vee$ est la multiplication par 4 sur E' ; le revêtement composé $E'_2 \to E$ est la multiplication par 8 sur E, de groupe d'automorphismes $(\mathbb{Z}/8\mathbb{Z})^2$. Le groupe $\mathrm{H}^1(E,\mathcal{F})$ est donc isomorphe à $\mathrm{H}^1((\mathbb{Z}/8\mathbb{Z})^2, M)$, où l'action de $(\mathbb{Z}/8\mathbb{Z})^2$ sur M est définie par le morphisme composé $(\mathbb{Z}/8\mathbb{Z})^2 \to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathrm{GL}_2(\Lambda)$. Ce groupe est isomorphe au quotient du Λ-module libre Λ^4 par le sous-module engendré par $(2,0,0,0)$. Plus précisément, il est engendré par les classes des cocycles c_1, c_2, c_3, c_4, où $2c_1$ est de classe nulle, définis comme suit.

Cocycle c	$c(1,0)$	$c(0,1)$
c_1	$(1\ 0)$	$(1\ 0)$
c_2	$(0\ 0)$	$(1\ 0)$
c_3	$(0\ 0)$	$(0\ 1)$
c_4	$(0\ 1)$	$(0\ 0)$

Le cocycle $2c_1$ associe à $(0,1)$ et $(1,0)$ le vecteur $(2,0)$; c'est $\partial c'$, où c' est le 0-cocycle de valeur $(0,1)$.

V.3.4.3 Un ouvert d'une courbe elliptique

Ce troisième exemple a nécessité l'utilisation d'un logiciel de calcul formel, à la fois pour les opérations dans la jacobienne d'une courbe de genre 2 et pour la cohomologie des groupes. Les algorithmes du chapitre IV n'ayant pas été implémentés, nous nous servons des spécificités des courbes hyperelliptiques pour la détermination de la 2-torsion de la jacobienne, et suivons pas à pas notre algorithme précédemment décrit pour tout le reste. Les fonctions pour calculer dans la jacobienne d'une courbe hyperelliptique sont disponibles dans SageMath et Magma.

Le revêtement considéré Dans ce deuxième exemple, nous prenons toujours $n = 2$. Le corps k_0 considéré est $\mathbb{F}_{11}$, et tous les calculs sont effectués sur $\mathbb{F}_{121} = \mathbb{F}_{11}(a)$, où a est un générateur de $\mathbb{F}_{121}^\times$ vérifiant $a^2 + 7a + 2 = 0$. Soit $\bar{E}$ la courbe elliptique sur $k = \overline{\mathbb{F}_{121}}$ définie par l'équation de Weierstrass affine $y^2 = (x-1)(x-2)(x-2)$. Soit $\bar{C}$ la courbe projective lisse de genre 2 sur k d'équation affine $y^2 = (x^2-1)(x^2-2)(x^2-3)$. La courbe $\bar{C}$ possède deux points ∞_+, ∞_- qui ne sont pas situés sur l'ouvert affine donné par cette équation. Considérons le revêtement $\bar{f}\colon \bar{C} \to \bar{E}$ de degré 2 donné par $(x,y) \mapsto (x^2, y)$. Il est ramifié en les points affines $P = (0,4)$ et $Q = (0,7)$ de $\bar{C}$ d'images respectives $(0,4)$ et $(0,7)$. Notons $C = \bar{C} - \{P,Q\}$ et $E = \bar{E} - \{\bar{f}(P), \bar{f}(Q)\}$. Notons $f\colon C \to E$ le revêtement étale galoisien obtenu. Remarquons que les courbes C et E proviennent de courbes C_0 et E_0 sur $k_0 = \mathbb{F}_{11}$.

Calcul de $\mathrm{H}^1(C,\mu_2)$ Notons

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

les points de C d'ordonnée nulle. Une base de la 2-torsion de la jacobienne $J_{\bar{C}}$ est donnée par les classes des diviseurs

$$D_1 := P_1^+ - P_1^-, \qquad D_2 := P_2^+ - P_2^-, \qquad D_3 := P_2^+ - P_3^+, \qquad D_4 := P_1^+ - P_3^-.$$

Les fonctions

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

vérifient $2D_i = \mathrm{div}(f_i)$. Notons D_5 le diviseur $P - Q$. Le double du diviseur

$$\bar{D}_5 := (a^{41}, a^{29}) + (-a^{41}, a^{29}) - (\infty_+ + \infty_-)$$

est équivalent à D_5. En l'absence d'algorithme implémenté à cet effet, nous l'avons obtenu en parcourant les points de $J_C(\mathbb{F}_{121})$. La fonction

$$f_5 = \frac{1}{xy} + \frac{a^8x^2+7}{x}$$

vérifie $\mathrm{div}(f_5) = 2\bar{D}_5 - D_5$. Une $\mathbb{F}_2$-base de $\mathrm{H}^1(C, \mu_2)$ est donc donnée par les triplets

$$([D_1], 0, f_1), \ldots, ([D_4], 0, f_4), ([\bar{D}_5], D_5, f_5).$$

Le revêtement $C_2 \to E$ Le revêtement $C_2 \to C$ de groupe $\mathrm{H}^1(C, \Lambda)^\vee$ a pour corps de fonctions $k(C)(z_1, \ldots, z_5)$ où $z_i^2 = f_i$. Le groupe $G = \mathrm{Aut}(C_2|E)$ est d'ordre 64 ; il contient le sous-groupe distingué $H = \mathrm{Aut}(C_2|C) \simeq (\mathbb{Z}/2\mathbb{Z})^5$ engendré par les $\gamma_i \colon z_i \mapsto -z_i$. Voici comment déterminer un élément de G d'image le générateur $\sigma \colon (x, y) \mapsto (-x, y)$ de $\mathrm{Aut}(C|E)$. Le calcul des diviseurs $\sigma^\star D_i$ fournit le résultat suivant.

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

Remarquons que $\sigma^\star f_3 = h_3^2 f_1 f_3$, $\sigma^\star f_4 = h_4^2 f_2 f_4$ et $\sigma^\star f_5 = -f_5$. Comme a^{30} est une racine carrée de -1 dans $\mathbb{F}_{121}$, un antécédent de σ est l'automorphisme δ défini par

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

En particulier, comme $h_3(x,y)h_3(-x,y) = h_4(x,y)h_4(-x,y) = -1$, l'automorphisme δ^2 est donné par

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

Par conséquent, $\delta^2 = \gamma_3\gamma_4\gamma_5$ et δ est d'ordre 4 dans G. De plus, $\delta\gamma_1 = \gamma_1\gamma_3\delta$ et $\delta\gamma_2 = \gamma_2\gamma_4\delta$. Les éléments $\gamma_3, \gamma_4, \gamma_5$ engendrent le centre de G. Son groupe dérivé est $\langle \gamma_3 = [\gamma_1, \delta], \gamma_4 = [\gamma_2, \delta] \rangle$. Une fois ce groupe calculé, il est possible par de simples méthodes d'algèbre linéaire implémentées dans tous les logiciels de calcul formel courants de calculer la cohomologie de n'importe quel faisceau lisse de Λ-modules sur E trivialisé par C. Il est également possible de calculer l'action de $\mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11}) =: \langle \phi \rangle$ sur G. L'action de ϕ sur les éléments de G se calcule simplement sur les équations qui les définissent : il fixe les γ_i et envoie δ sur $\gamma_5\delta$.

Un premier calcul de cohomologie Soit $\mathcal{F}_0$ le faisceau lisse de $\Lambda = \mathbb{Z}/2\mathbb{Z}$-modules sur E_0 trivialisé par C_0 de fibre générique géométrique un Λ-module libre M de dimension 2, défini par la représentation :

$$\begin{array}{rcl} \mathrm{Aut}(C_0|E_0) & \longrightarrow & \mathrm{GL}_2(\Lambda) \\ \sigma & \longmapsto & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{array}$$

Déterminons la cohomologie du faisceau $\mathcal{F} = (\mathcal{F}_0)|_E = f_\star\Lambda$. Le complexe

$$M \to C^{12}(G, M)$$

représentant $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G, M)$ est de la forme

$$\Lambda^2 \to \Lambda^6.$$

Le groupe $C^{12}(G, M)$ est engendré par des 1-cocycles $c_1, \ldots, c_5, c' \colon G \to M$. Ils sont donnés dans le tableau suivant.

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)	(1 1)	(0 0)	(0 0)	(0 1)
c_2	(0 1)	(0 0)	(1 1)	(0 0)	(0 0)	(0 1)
c_3	(0 0)	(1 0)	(0 0)	(1 1)	(0 0)	(0 1)
c_4	(0 0)	(0 1)	(0 0)	(1 1)	(0 0)	(0 1)
c_5	(0 0)	(0 0)	(0 1)	(0 0)	(1 1)	(0 1)
c'	(0 0)	(0 0)	(0 0)	(0 0)	(0 0)	(1 1)

Ici, c' est l'image des 0-cocycles $\alpha = (1\ 0)$ et $\beta = (0\ 1)$ par l'application $\partial \colon M \to C^1(G, M)$. En particulier, nous retrouvons le résultat attendu $\mathrm{H}^1(E, f_\star\Lambda) = \mathrm{H}^1(C, \Lambda) \simeq \Lambda^5$. L'action du groupe $\mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11}) = \langle\phi\rangle$ sur ce complexe fixe $c_1, \ldots, c_4, c'$ et envoie c_5 sur $\phi^\star c_5 = c_5 + c'$. Par conséquent, comme attendu, son action sur $\mathrm{H}^1(E, f_\star\Lambda)$ est triviale.

Un second calcul de cohomologie Considérons désormais le faisceau lisse $\mathcal{F}_0$ sur E_0 trivialisé par C_0 de fibre $M = \Lambda^3$ défini par la représentation :

$$\begin{array}{rcl} \mathrm{Aut}(C_0|E_0) & \longrightarrow & \mathrm{GL}_3(\Lambda) \\ \sigma & \longmapsto & \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \end{array}$$

Nous trouvons $\mathrm{H}^0(E, \mathcal{F}) \simeq \Lambda^2$ et $\mathrm{H}^1(E, \mathcal{F}) \simeq \Lambda^8$. Un calcul fournit des 1-cocycles $c_1, \ldots, c_8$ formant une base de $\mathrm{H}^1(G, M)$ et le 1-cocycle principal c' défini par $(1\ 0\ 0) \in M$.

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)

L'action de $\phi \in \mathrm{Gal}(\mathbb{F}_{121}|\mathbb{F}_{11})$ sur $C^{12}(G, M)$ fixe tous ces cocycles sauf c_7, qui vérifie $\phi^\star c_7 = c_7 + c'$. L'action sur $\mathrm{H}^1(G, M)$ est donc triviale.

V.3.5 Cohomologie des complexes de faisceaux lisses

Soit X une courbe intègre lisse sur k. Supposons d'abord X affine. Soit

$$\mathscr{K} = [\mathscr{K}^0 \to \cdots \to \mathscr{K}^m]$$

un complexe borné de faisceaux lisses sur X de fibre générique géométrique un complexe K de $\pi_1(X)$-modules. Nous allons montrer comment utiliser la méthode décrite en V.3.1 pour déterminer un complexe de Λ-modules représentant $\mathrm{R}\Gamma(X, \mathscr{K})$. Soit $f\colon Y \to X$ un revêtement galoisien de X qui trivialise tous les $\mathscr{K}^i$. Notons $\pi = \pi_1(X)$. Pour tout groupe profini H, notons $P_H(\Lambda)$ la résolution projective usuelle (résolution bar) de Λ comme $\Lambda[[H]]$-module. Nous souhaitons calculer $\mathrm{R}\Gamma(\pi, K) = \mathrm{RHom}_{\Lambda[[\pi]]}(\Lambda, K)$, qui est représenté par le complexe

$$\mathrm{Hom}^\bullet_{\Lambda[[\pi]]}(P_\pi(\Lambda), K) = \mathrm{Tot}(A^{\bullet,\bullet})$$

où $A^{p,q} = \mathrm{Hom}_{\Lambda[[\pi]]}(P_\pi^{-q}(\Lambda), K^p)$. Soit $Y_2 \to Y$ le revêtement de Y de groupe $\mathrm{H}^1(Y, \Lambda)^\vee$. Notons de plus $G = \mathrm{Aut}(Y_2|X)$. Considérons le complexe double $B^{p,q} = \mathrm{Hom}_{\Lambda[G]}(\tau_{\geqslant -1} P_G^{-q}(\Lambda), K^p)$.

Proposition 5.3.7. Le complexe $\mathrm{Tot}\, B^{\bullet,\bullet}$ représente $\mathrm{R}\Gamma(X, \mathscr{K})$.

Démonstration. Le morphisme $B^{\bullet,\bullet} \to A^{\bullet,\bullet}$ induit par le quotient $\pi \to G$ définit encore un morphisme entre les suites spectrales associées à ces quotients. Rappelons que pour tout faisceau lisse $\mathcal{F}$ sur X trivialisé par Y de fibre F, le morphisme $\tau_{\leqslant 1} \mathrm{Hom}_{\Lambda[G]}(P_G(\Lambda), F) \to \mathrm{Hom}_{\Lambda[[\pi]]}(P_\pi(\Lambda), F)$ est un quasi-isomorphisme. Remarquons que $\mathrm{Hom}_{\Lambda[G]}(\tau_{\geqslant -1} P_G(\Lambda), F) = \tau_{\leqslant 1} \mathrm{Hom}_{\Lambda[H]}(P_G(\Lambda), F)$ par exactitude à gauche de $\mathrm{Hom}(-, M)$. Le morphisme $B^{\bullet,\bullet} \to A^{\bullet,\bullet}$ est donc, sur chaque colonne, un quasi-isomorphisme de complexes. Par conséquent, il induit un isomorphisme entre les premières pages des suites spectrales (pour l'orientation verticale) associées à $B^{\bullet,\bullet}$ et $A^{\bullet,\bullet}$: il s'agit en position (p, q) de l'isomorphisme $\mathrm{H}^q(H, K^p) \to \mathrm{H}^q(\pi, K^p)$ si $q \leqslant 1$, et $0 \to \mathrm{H}^q(\pi, K^p) = 0$ sinon. Par conséquent, le morphisme entre les aboutissements de ces deux suites spectrales est un isomorphisme, c'est-à-dire que le morphisme $\mathrm{Tot}(B^{\bullet,\bullet}) \to \mathrm{Tot}(A^{\bullet,\bullet})$ est un quasi-isomorphisme. □

V.4 Cup-produits dans la cohomologie des faisceaux lisses

Nous décrivons dans cette section comment calculer des cup-produits dans la cohomologie de faisceaux lisses sur des courbes lisses sur un corps fini ou algébriquement clos. Dans un premier temps, nous décrivons un calcul du H^2 d'un faisceau lisse sur une courbe projective lisse comme groupe de cohomologie d'un quotient du groupe fondamental de la courbe. Nous indiquons ensuite comment calculer le cup-produit de la dualité de Poincaré dans un cas simple. Nous nous servons enfin du calcul du H^2 exposé au début de la section pour décrire les cup-produits $\mathrm{H}^1 \times \mathrm{H}^1 \to \mathrm{H}^2$ entre groupes de cohomologie de faisceaux lisses.

V.4.1 Un autre calcul du H^2

Soit X une courbe intègre propre lisse de genre non nul sur k. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur k de fibre M, trivialisé par un revêtement galoisien $Y \to X$. Nous allons montrer comment calculer $\mathrm{H}^2(X, \mathcal{F})$ comme le H^2 d'un quotient de $\pi_1(X)$ à valeurs dans M. Supposons (quitte à passer à un revêtement caractéristique de Y) que le degré de $Y \to X$ est un multiple de n. Soient $Y_2 \to Y$ le revêtement caractéristique de groupe $\mathrm{H}^1(Y, \Lambda)^\vee$ et $Y_3 \to Y_2$ le revêtement caractéristique de groupe $\mathrm{H}^1(Y_2, \Lambda)^\vee$. Notons $\pi, \pi_Y, \pi_Y^{[2]}, \pi_Y^{[3]}$ les groupes fondamentaux respectifs de X, Y, Y_2, Y_3. Notons $G = \pi/\pi_Y = \mathrm{Aut}(Y|X)$, $G_2 = \pi/\pi_Y^{[2]} = \mathrm{Aut}(Y_2|X)$ et $G_3 = \pi/\pi_Y^{[3]} = \mathrm{Aut}(Y_3|X)$.

Proposition 5.4.1. La restriction de $\mathrm{H}^2(G_3, M) \to \mathrm{H}^2(\pi, M)$ à l'image de $\mathrm{H}^2(G_2, M)$ est un isomorphisme.

Démonstration. Rappelons que comme les morphismes

$$\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(Y_2, \mathcal{F}) \to \mathrm{H}^1(Y_3, \mathcal{F})$$

sont nuls, les morphismes

$$\mathrm{H}^1(G_2, M) \to \mathrm{H}^1(G_3, M) \to \mathrm{H}^1(\pi, M) = \mathrm{H}^1(X, \mathcal{F})$$

sont des isomorphismes. Considérons les morphismes entre les suites spectrales de Hochschild-Serre associés aux morphismes d'extensions de groupes :

$$\begin{tikzcd}
1 \arrow[r] & \pi_Y^{[3]} \arrow[r] \arrow[d] & \pi \arrow[r] \arrow[d] & G_3 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \pi_Y^{[2]} \arrow[r] \arrow[d] & \pi \arrow[r] \arrow[d] & G_2 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \pi_Y \arrow[r] & \pi \arrow[r] & G \arrow[r] & 1
\end{tikzcd}$$

Ils donnent les morphismes de suites exactes de bas degré :

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^1(G, M) \arrow[r] \arrow[d] & \mathrm{H}^1(\pi, M) \arrow[r] \arrow[d] & \mathrm{H}^0(G, \mathrm{H}^1(\pi_Y, M)) \arrow[r] \arrow[d] & \mathrm{H}^2(G, M) \arrow[r] \arrow[d] & \ker(\mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y, M)) \arrow[r] \arrow[d] & \mathrm{H}^1(G, \mathrm{H}^1(\pi_Y, M)) \arrow[d] \\
0 \arrow[r] & \mathrm{H}^1(G_2, M) \arrow[r, "\sim"] \arrow[d] & \mathrm{H}^1(\pi, M) \arrow[r] \arrow[d] & \mathrm{H}^0(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M)) \arrow[r] \arrow[d] & \mathrm{H}^2(G_2, M) \arrow[r] \arrow[d] & \ker(\mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y^{[2]}, M)) \arrow[r] \arrow[d] & \mathrm{H}^1(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M)) \arrow[d] \\
0 \arrow[r] & \mathrm{H}^1(G_2, M) \arrow[r, "\sim"] & \mathrm{H}^1(\pi, M) \arrow[r] & \mathrm{H}^0(G_3, \mathrm{H}^1(\pi_Y^{[3]}, M)) \arrow[r] & \mathrm{H}^2(G_3, M) \arrow[r] & \ker(\mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y^{[3]}, M)) \arrow[r] & \mathrm{H}^1(G_3, \mathrm{H}^1(\pi_Y^{[3]}, M))
\end{tikzcd}$$

Comme les degrés des revêtements $Y \to X$ et $Y_2 \to X$ sont des multiples de n, les morphismes

$$\mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y, M) \quad \text{et} \quad \mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y^{[2]}, M)$$

sont nuls. De plus, comme $\mathcal{F}$ est trivial sur Y, le morphisme $\mathrm{H}^1(\pi_Y, M) \to \mathrm{H}^1(\pi_Y^{[2]}, M)$ est nul. Le carré supérieur droit du diagramme ci-dessus est donc

$$\begin{tikzcd}
\ker(\mathrm{H}^2(\pi, M) \to \mathrm{H}^2(\pi_Y, M)) \arrow[r] \arrow[d, "\wr"] & \mathrm{H}^1(G, \mathrm{H}^1(\pi_Y, M)) \arrow[d, "0"] \\
\mathrm{H}^2(\pi, M) \arrow[r] & \mathrm{H}^1(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M))
\end{tikzcd}$$

ce qui démontre la nullité du morphisme $\mathrm{H}^2(\pi, M) \to \mathrm{H}^1(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M))$. Le même raisonnement peut être appliqué au morphisme $Y_3 \to Y_2$ pour obtenir le diagramme commutatif suivant.

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^0(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M)) \arrow[r] \arrow[d, "0"] & \mathrm{H}^2(G_2, M) \arrow[r] \arrow[d] & \mathrm{H}^2(\pi, M) \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \mathrm{H}^0(G_3, \mathrm{H}^1(\pi_Y^{[3]}, M)) \arrow[r] & \mathrm{H}^2(G_3, M) \arrow[r] & \mathrm{H}^2(\pi, M) \arrow[r] & 0
\end{tikzcd}$$

Le morphisme $\mathrm{H}^2(G_2, M) \to \mathrm{H}^2(G_3, M)$ passe au quotient en un morphisme

$$\mathrm{H}^2(G_2, M)/\,\mathrm{H}^0(G_2, \mathrm{H}^1(\pi_Y^{[2]}, M)) \to \mathrm{H}^2(G_3, M)$$

et le cardinal de son image est au plus $|\,\mathrm{H}^2(\pi, M)|$. Par conséquent, la restriction du morphisme $\mathrm{H}^2(G_3, M) \to \mathrm{H}^2(\pi, M)$ à l'image de $\mathrm{H}^2(G_2, M) \to \mathrm{H}^2(G_3, M)$, que l'on savait déjà surjective, est un isomorphisme. □

Remarque 5.4.2. Le même raisonnement s'applique mot pour mot au cas des courbes projectives lisses géométriquement connexes sur les corps finis. La description du revêtement Y_2 se trouve dans la remarque 2.7.6.

Remarque 5.4.3. L'hypothèse de divisibilité par n du degré de $Y \to X$ est nécessaire pour notre méthode de démonstration, mais ne semble pas nécessaire en général pour obtenir ce résultat. Par exemple, soit E une courbe elliptique sur k. Alors $G_2 = \mathrm{Aut}(E_2|E) \simeq \Lambda^2$ et $G_3 = (\mathbb{Z}/n^2\mathbb{Z})^2$. Le groupe $\mathrm{H}^2(G_2, \Lambda)$ est un Λ-module libre de rang 3 par la formule de Künneth. Or il contient $\mathrm{Ext}^1(G_2, \Lambda)$ qui est de rang 2. Il y a donc une extension centrale de G_2 par Λ qui n'est pas abélienne, et qui fournit par produit fibré une extension centrale non abélienne de G_3 par Λ, c'est-à-dire un élément non nul de $\mathrm{H}^2(G_3, \Lambda)$. De plus, le morphisme $\mathrm{Ext}^1(G_2, \Lambda) \to \mathrm{Ext}^1(G_3, \Lambda)$ est nul : l'image du morphisme $\mathrm{H}^2(G_2, \Lambda) \to \mathrm{H}^2(G_3, \Lambda)$ est de rang 1, c'est donc $\mathrm{H}^2(E, \Lambda)$.

V.4.2 La dualité de Poincaré dans un cas particulier

Soit X une courbe projective lisse sur k. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X, trivialisé par un revêtement galoisien $f\colon Y \to X$ de groupe G. Nous souhaitons calculer le cup-produit

$$\mathrm{H}^1(X, \mathcal{F}) \times \mathrm{H}^1(X, \mathcal{F}^\vee) \to \mathrm{H}^2(X, \Lambda).$$

Dans le cas particulier où n est premier à l'ordre de G, le morphisme $\mathrm{H}^2(X, \Lambda) \to \mathrm{H}^2(Y, \Lambda)$ est un isomorphisme. Le diagramme commutatif suivant

$$\begin{array}{ccc}
\mathrm{H}^1(Y, f^\star\mathcal{F}) \times \mathrm{H}^1(Y, f^\star\mathcal{F}^\vee) & \longrightarrow & \mathrm{H}^2(Y, \Lambda) \\
\uparrow & & \uparrow \\
\mathrm{H}^1(X, \mathcal{F}) \times \mathrm{H}^1(X, \mathcal{F}^\vee) & \longrightarrow & \mathrm{H}^2(X, \Lambda)
\end{array}$$

permet alors de se ramener au cas particulier du cup-produit dans la cohomologie des faisceaux constants, qui est l'accouplement de Weil décrit dans la section II.4.2.

V.4.3 Calcul des cup-produits en général

Soit X une courbe projective lisse sur le corps algébriquement clos k. Soient $\mathcal{F}, \mathcal{G}$ deux faisceaux lisses de Λ-modules sur X de fibres respectives M et N. Nous souhaitons calculer le cup-produit

$$\mathrm{H}^1(X, \mathcal{F}) \times \mathrm{H}^1(X, \mathcal{G}) \to \mathrm{H}^2(X, \mathcal{F} \otimes \mathcal{G}).$$

Soit $f\colon Y \to X$ un revêtement galoisien qui trivialise à la fois $\mathcal{F}$ et $\mathcal{G}$. Supposons que le degré de $Y \to X$ soit divisible par n. Soient $Y_2 \to Y$ le revêtement caractéristique de groupe $\mathrm{H}^1(Y, \Lambda)^\vee$ et $Y_3 \to Y_2$ le revêtement caractéristique de groupe $\mathrm{H}^1(Y_2, \Lambda)^\vee$. Notons $G_2 = \mathrm{Aut}(Y_2|X)$ et $G_3 = \mathrm{Aut}(Y_3|X)$.

Théorème 5.4.4. Le cup-produit

$$\mathrm{H}^1(X,\mathcal{F}) \times \mathrm{H}^1(X,\mathcal{G}) \to \mathrm{H}^2(X,\mathcal{F}\otimes\mathcal{G})$$

est réalisée par la composée

$$\mathrm{H}^1(G_2,M) \times \mathrm{H}^1(G_2,N) \xrightarrow{\cup} \mathrm{H}^2(G_2,M\otimes N) \to \mathrm{im}(\mathrm{H}^2(G_2,M\otimes N) \to \mathrm{H}^2(G_3,M\otimes N)).$$

Démonstration. Rappelons que les morphismes

$$\mathrm{im}(\mathrm{H}^2(G_2,M\otimes N) \to \mathrm{H}^2(G_3,M\otimes N)) \to \mathrm{H}^2(\pi,M\otimes N) \to \mathrm{H}^2(X,\mathcal{F}\otimes\mathcal{G})$$

sont des isomorphismes d'après la proposition 5.4.1. Le diagramme commutatif

$$\begin{tikzcd}
\mathrm{H}^1(G_2,M)\times\mathrm{H}^1(G_2,N) \arrow[r] \arrow[d, "\wr"'] & \mathrm{H}^2(G_2,M\otimes N) \arrow[d] \\
\mathrm{H}^1(G_3,M)\times\mathrm{H}^1(G_3,N) \arrow[r] \arrow[d, "\wr"'] & \mathrm{H}^2(G_3,M\otimes N) \arrow[d] \\
\mathrm{H}^1(\pi,M)\times\mathrm{H}^1(\pi,N) \arrow[r] \arrow[d, "\wr"'] & \mathrm{H}^2(\pi,M\otimes N) \arrow[d, "\wr"'] \\
\mathrm{H}^1(X,\mathcal{F})\times\mathrm{H}^1(X,\mathcal{G}) \arrow[r] & \mathrm{H}^2(X,\mathcal{F}\otimes\mathcal{G})
\end{tikzcd}$$

où les trois premières lignes sont les cup-produits de cohomologie des groupes, montre comment calculer le cup-produit de la dernière ligne : c'est la composée

$$\mathrm{H}^1(G_2,M) \times \mathrm{H}^1(G_2,N) \xrightarrow{\cup} \mathrm{H}^2(G_2,M\otimes N) \to \mathrm{im}(\mathrm{H}^2(G_2,M\otimes N) \to \mathrm{H}^2(G_3,M\otimes N)).$$

□

Remarque 5.4.5. Ceci s'applique de la même façon au cas des courbes projectives lisses géométriquement connexes sur un corps fini.

V.5 Cohomologie des faisceaux constructibles : calcul du H^1

Cette section est dédiée aux méthodes de calcul direct du premier groupe de cohomologie d'un faisceau constructible sur une courbe lisse, en employant des méthodes déjà proposées dans la littérature.

V.5.1 Avec l'algorithme de Jin

Soit X une courbe intègre lisse sur k. Soit $\mathcal{F}$ un faisceau constructible sur X. Supposons $\mathcal{F}$ défini par recollement par rapport à un couple ouvert-fermé $(j\colon U \to X, i\colon Z \to X)$ par le triplet $(\mathscr{L}, \mathcal{F}_Z, \phi)$. La stratégie suivante, proposée par Jin dans [Jin20, §9.4], permet de calculer $\mathrm{H}^1(X,\mathcal{F})$. La suite exacte de faisceaux sur X

$$0 \to j_!\mathscr{L} \to \mathcal{F} \to i_\star i^\star\mathcal{F} \to 0$$

donne d'une part un isomorphisme

$$\mathrm{H}^2_c(U, j^\star\mathcal{F}) \to \mathrm{H}^2(X,\mathcal{F})$$

et d'autre part la suite exacte

$$0 \to \mathrm{H}^0(X, j_!\mathscr{L}) \to \mathrm{H}^0(X, \mathcal{F}) \to \mathrm{H}^0(Z, \mathcal{F}_Z) \xrightarrow{\delta} \mathrm{H}^1(X, j_!\mathscr{L}) \to \mathrm{H}^1(X, \mathcal{F}) \to 0.$$

Il suffit donc de savoir calculer explicitement la flèche δ afin de déterminer $\mathrm{H}^1(X, \mathcal{F})$. D'après [Jin20, Lem. 5.3], $\mathrm{H}^1(X, j_!\mathscr{L})$ est le groupe des classes d'isomorphismes de couples (T, s) où T est un $\mathscr{L}$-torseur sur U et $s \in i^\star j_\star \mathscr{L}(Z)$. La flèche δ associe à $s \in \mathrm{H}^0(Z, \mathcal{F}_Z)$ le $\mathscr{L}$-torseur trivial sur U, et la section $\phi(s) \in \mathrm{H}^0(Z, i^\star j_\star \mathscr{L})$.

Soit maintenant $g\colon V \to U$ un revêtement galoisien de groupe G qui trivialise $\mathscr{L}$. Notons $F \coloneqq g^\star \mathscr{L}$. Soit Y la normalisation de X dans V, et $i'\colon W \to Y$ le changement de base de $i\colon Z \to X$ par rapport à $Y \to X$. Notons également $j'_\star\colon U' \to Y$ le changement de base de $j\colon U \to X$. L'algorithme de Jin calcule des représentants des éléments de $\mathrm{H}^1(X, j_!\mathscr{L})$ sous forme de couples (T', s') où T' est un F-torseur G-équivariant sur Y, et $s' \in \mathrm{H}^0(G, i'^* T(W))$ [Jin20, Lem. 5.10]. Le couple (T', s') correspondant à (T, s) est $(j'_\star g^\star T, s)$. Comme $g^\star T$ est un G-torseur sur V, le morphisme $g^\star T \to V$ est fini étale. La proposition 3.2.2 indique alors comment calculer le torseur $j'_\star g^\star T$: c'est le lieu étale de la normalisation de Y dans $g^\star T$.

V.5.2 Par effacement

Soit X une courbe lisse sur k. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X. La méthode suivante, proposée en dimension quelconque dans [MO15, §11.4], permet de calculer $\mathrm{H}^1(X, \mathcal{F})$. Supposons $\mathcal{F}$ lisse sur un ouvert U, de complémentaire réduit Z. Soit $V \to U$ un revêtement galoisien trivialisant $\mathcal{F}|_U$. Construisons un monomorphisme $\mathcal{F} \to \mathcal{G}$ de faisceaux constructibles tel que $\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(X, \mathcal{G})$ soit nul. Dans ce cas, le groupe $\mathrm{H}^1(X, \mathcal{F})$ est isomorphe au conoyau du morphisme $\mathrm{H}^0(X, \mathcal{F}) \to \mathrm{H}^0(X, \mathrm{coker}(\mathcal{F} \to \mathcal{G}))$.

Plongeons $\mathcal{F}$ dans $p_\star M$, où M est un Λ-module de type fini et p est un morphisme fini. Explicitement, prenons $p\colon Y' = X' \sqcup Z \to X$ où X' est la normalisation de X dans V. Considérons $(X')_2$, le revêtement de X' de groupe $\mathrm{H}^1(X', \Lambda)^\vee$ qui trivialise les Λ-torseurs sur X', et $Y'' = (X')_2 \sqcup Z$. D'une part, la composée $\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(U, \mathcal{F}|_U) \to \mathrm{H}^1(X'', \mathcal{F}|_{X'})$ est nulle ; d'autre part, $\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(Z, \mathcal{F}|_Z)$ est nulle car $\mathrm{H}^1(Z, \mathcal{F}|_Z) = 0$. Par conséquent, le morphisme $\mathrm{H}^1(X, \mathcal{F}) \to \mathrm{H}^1(Y'', \mathcal{F})$ est nul. Notons $q\colon Y'' \to X$. Alors comme $Y'' \to Y'$ est surjectif, $\mathcal{F} \hookrightarrow p_\star M \hookrightarrow q_\star M$.

Les schémas X' et X'' se calculent explicitement, de même que le poussé en avant d'un faisceau constant par un morphisme fini. Ainsi, il est possible d'obtenir une description par recollement du faisceau $q_\star M$, du morphisme $p_\star M \to q_\star M$ et finalement du conoyau de la composée $\mathcal{F} \to q_\star M$. Les sections globales d'un faisceau constructible décrit par recollement étant simplement un produit fibré de groupes abéliens, le morphisme $\mathrm{H}^0(X, \mathcal{F}) \to \mathrm{H}^0(X, \mathrm{coker}(\mathcal{F} \to q_\star M))$ se déduit immédiatement de $\mathcal{F} \to q_\star M$.

V.6 Calcul de $\mathrm{R}\Gamma(X, -)\colon \mathrm{D}^b_c(X, \Lambda) \to \mathrm{D}^b_c(\Lambda)$

Le but de cette section est de donner un algorithme qui calcule explicitement le foncteur dérivé des sections globales sur une courbe lisse ou nodale sur un corps algébriquement clos. Dans un premier temps, nous décrivons une méthode pour calculer le $\mathrm{R}\Gamma$ d'un faisceau constructible sur une courbe lisse. Nous donnons ensuite des bornes précises sur la complexité de cet algorithme. Nous exposons ensuite la généralisation de cette méthode au calcul du $\mathrm{R}\Gamma$ d'un complexe de faisceaux constructibles, et terminons par un exemple détaillé.

V.6.1 Calcul de $\mathrm{R}\Gamma(X, \mathcal{F})$ pour $\mathcal{F}$ constructible sur X lisse

Soit X une courbe intègre lisse sur le corps algébriquement clos k. Nous notons toujours $\Lambda = \mathbb{Z}/n\mathbb{Z}$, avec n inversible dans k. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X, lisse sur un ouvert affine $j\colon U \hookrightarrow X$. Nous allons montrer comment calculer $\mathrm{R}\Gamma(X, \mathcal{F})$. Notons $\mathscr{L}$ le faisceau lisse $j^\star\mathcal{F}$. Soit $i\colon Z \to X$ l'inclusion du fermé réduit complémentaire. Notons $\phi\colon i^\star\mathcal{F} \to i^\star j_\star\mathscr{L}$ le morphisme de recollement.

V.6.1.1 Réduction à un cas particulier

Considérons le morphisme

$$f\colon \mathcal{F} \to j_\star\mathscr{L} \oplus i_\star i^\star\mathcal{F}$$

défini par adjonction. Sa fibre en $z \in Z$ est le morphisme injectif

$$f_z = (\phi_z, \mathrm{id})\colon \mathcal{F}_z \to (j_\star\mathscr{L})_z \oplus \mathcal{F}_z.$$

De plus, $f|_U$ est simplement l'isomorphisme canonique $\mathscr{L} \to j^\star j_\star\mathscr{L}$. Notons Q_Z le conoyau du morphisme $f_Z = \bigoplus_{z\in Z} f_z$. Les morphismes

$$(\mathrm{id}, -\phi_z)\colon (j_\star\mathscr{L})_z \oplus \mathcal{F}_z \to (j_\star\mathscr{L})_z$$

induisent un isomorphisme

$$Q_Z \xrightarrow{\sim} \bigoplus_{z\in Z} (j_\star\mathscr{L})_z.$$

Comme f est un isomorphisme sur U, le conoyau de f est $i_\star Q_Z$. La suite exacte

$$0 \to \mathcal{F} \to j_\star\mathscr{L} \oplus i_\star i^\star\mathcal{F} \to i_\star Q_Z \to 0$$

donne le triangle distingué

$$\mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathcal{F}) \to \mathrm{R}\Gamma(X, i_\star Q_Z) \xrightarrow{+1}$$

qui fait apparaître $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ comme le cône du morphisme de droite. Pour calculer $\mathrm{R}\Gamma(X, \mathcal{F})$, il suffit donc désormais, de calculer $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$ et le morphisme $\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \to \mathrm{R}\Gamma(Z, Q_Z)$.

V.6.1.2 Calcul de $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$ pour $\mathscr{L}$ lisse sur U

Soit $\mathscr{L}$ un faisceau lisse sur la courbe affine lisse U, trivialisé par le revêtement galoisien $V \to U$. Notons $V_2 \to V$ le revêtement caractéristique de V de groupe $\mathrm{H}^1(V, \Lambda)^\vee$, et $\overline{V_2}$ sa complétion projective lisse. Notons $G = \mathrm{Aut}(V_2|U)$, et $M = \mathrm{H}^0(V, \mathscr{L}|_V)$. Rappelons que $\mathrm{R}\Gamma_Z$ et H^i_z désignent les foncteurs de cohomologie à support sur Z définis dans la section I.6.1. Le triangle distingué

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

fait apparaître $\mathrm{R}\Gamma(X, j_\star\mathscr{L})[1]$ comme le cône de $\mathrm{R}\Gamma(U, \mathscr{L}) \to \mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})[1]$. Nous avons vu dans la section V.3.1 comment calculer un complexe représentant $\mathrm{R}\Gamma(U, \mathscr{L}) = \tau_{\leqslant 1}\,\mathrm{R}\Gamma(G, M)$. Soit $z \in Z$. Comme $\mathrm{H}^i_z(X, j_\star\mathscr{L}) = 0$ pour tout $i \neq 2$ d'après le lemme 2.5.1, il y a dans $\mathrm{D}^b_c(X, \Lambda)$ un isomorphisme

$$\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L}) \xrightarrow{\sim} \mathrm{H}^2_z(X, j_\star\mathscr{L})[-2].$$

Rappelons (cf lemme 2.5.2) qu'il y a un isomorphisme $\mathrm{H}^2_z(X, j_\star\mathscr{L}) = \mathrm{H}^1(I_z/P_z, M_{P_z})$ où $I_z \subseteq G$ est le groupe d'inertie en un point de $\overline{V_2}$ d'image z, et P_z son sous-groupe d'inertie sauvage. Rappelons

également que I_z/P_z est canoniquement isomorphe à $\mu_e(k)$, où e est l'indice de ramification de $\overline{V_2} \to X$ en z. Le morphisme $\mathrm{R}\Gamma(U, \mathscr{L}) \to \mathrm{R}\Gamma_Z(X, \mathscr{L})[1]$ n'est donc autre que

$$\tau_{\leqslant 1} \mathrm{R}\Gamma(G, M) \to \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z})[-1].$$

Ce morphisme est nul en tout degré sauf 1, et en degré 1 c'est le morphisme qui à un 1-cocycle $c\colon G \to M$ associe l'image dans $\mathrm{H}^1(I_z, M)$, puis dans $\mathrm{H}^1(I_z/P_z, M_{P_z})$, de la classe de c dans $\mathrm{H}^1(G, M)$. La description du morphisme $\mathrm{H}^1(I_z, M) \to \mathrm{H}^1(I_z/P_z, M_{P_z})$ se trouve dans le lemme 2.1.15.

V.6.1.3 Conclusion de l'argument

Reprenons le fil : X est une courbe intègre lisse sur k, le faisceau $\mathcal{F}$ est constructible sur X, lisse sur l'ouvert $j\colon U \to X$ de fibre M. Notons $\mathscr{L}$ le faisceau lisse $j^\star\mathcal{F}$. Le paragraphe précédent permet de calculer un complexe représentant $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$. Notons $C^\bullet(G, M)$ le complexe de cochaînes usuel représentant $\mathrm{R}\Gamma(G, M)$. Notons encore $C^{12}(G, M) = \ker(C^1(G, M) \to C^2(G, M))$ le groupe des morphismes croisés de G dans M. Le complexe calculé représentant $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$ est le suivant :

$$C^0(G, M) \to C^{12}(G, M) \to \bigoplus_z \mathrm{H}^1(I_z/P_z, M_{P_z}).$$

Calculons explicitement le morphisme

$$\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathcal{F}) \xrightarrow{(\mathrm{id}, -\phi_Z)} \mathrm{R}\Gamma(X, i_\star i^\star j_\star\mathscr{L}).$$

Le complexe

$$\mathrm{R}\Gamma(X, i_\star i^\star j_\star\mathscr{L}) \simeq \mathrm{H}^0(Z, i^\star j_\star\mathscr{L})[0] \simeq \bigoplus_{z \in Z} M^{I_z}[0]$$

est naturellement quasi-isomorphe au complexe

$$\bigoplus_{z \in Z} M_{P_z} \to \bigoplus_{z \in Z} C^{12}(I_z/P_z, M_{P_z}) \to \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}).$$

Le morphisme $\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathcal{F}) \to \mathrm{R}\Gamma(X, i_\star i^\star j_\star\mathscr{L})$ est donc le suivant.

$$\begin{tikzcd}
0 \arrow[r] & M \oplus \bigoplus_{z \in Z} \mathcal{F}_z \arrow[r, "(\partial_G, 0)"] \arrow[d, "\bigoplus_{z \in Z}(\mathrm{id} - \phi_z)"] & C^{12}(G, M) \arrow[r] \arrow[d, "\bigoplus_{z \in Z} \mathrm{res}^G_{I_z}"] & \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & \bigoplus_{z \in Z} M_{P_z} \arrow[r, "\bigoplus_z \partial_{I_z}"] & \bigoplus_{z \in Z} C^{12}(I_z/P_z, M_{P_z}) \arrow[r] & \bigoplus_{z \in Z} \mathrm{H}^1(I_z/P_z, M_{P_z}) \arrow[r] & 0
\end{tikzcd}$$

Les morphismes induits en cohomologie sont bien $\mathrm{H}^0(U, \mathscr{L}) \oplus \mathrm{H}^0(Z, i^\star\mathcal{F}) \to \mathrm{H}^0(X, j_\star\mathscr{L})$ en degré 0, et $\mathrm{H}^i(X, j_\star\mathscr{L}) \to 0$ en degré $i \geqslant 1$. Le complexe $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ est le cône de ce morphisme. Ceci démontre le théorème 5.0.1.

V.6.1.4 Fonctorialité sur $\operatorname{Spec} k$

Soit $\phi\colon X' \to X$ un morphisme de courbes intègres lisses sur k. Soit $\mathcal{F}$ un faisceau constructible sur X, lisse sur un ouvert affine U. Nous allons décrire comment calculer le morphisme $\mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(X', \phi^\star\mathcal{F})$. Soit $f\colon V \to U$ un revêtement galoisien de U trivialisant $\mathcal{F}|_U$. Soit $V_2 \to V$ le revêtement de groupe $\mathrm{H}^1(V, \Lambda)^\vee$, et $\overline{V_2}$ sa complétion projective lisse. Soit V' la clôture galoisienne d'une composante connexe de $V \times_X X'$. Notons $U' = U \times_X X'$. Pour chaque point $z \in X - U$, choisissons

un point $z_2 \in \overline{V_2}$ d'image z. Notons V_2' le revêtement de V' de groupe $\mathrm{H}^1(V', \Lambda)^\vee$, et $\overline{V_2'}$ sa complétion projective lisse. Pour chaque antécédent z' de z dans $X' - U'$, choisissons un antécédent $z_2' \in \overline{V_2'}$ de z' d'image z_2. Alors il y a un morphisme $\mathrm{Aut}(V_2'|U') \subseteq \mathrm{Aut}(V_2'|U) \to \mathrm{Aut}(V_2|U)$ qui induit pour tout z un morphisme $I_{z_2'} \to I_{z'}$, et par conséquent un morphisme $I_{z_2'}/P_{z_2'} \to I_{z_2}/P_{z_2}$. Le fonctorialité de la résolution bar permet d'en déduire le morphisme $\mathrm{R}\Gamma(X, \mathcal{F}) \to \mathrm{R}\Gamma(X', \phi^\star \mathcal{F})$ cherché.

V.6.1.5 Action de $\mathrm{Gal}(k|k_0)$

Supposons désormais que $X, U, Z, \mathcal{F}$ proviennent de $X_0, U_0, Z_0, \mathcal{F}_0$ sur le corps de base k_0. Soit V_0 un revêtement galoisien de U_0 qui trivialise $\mathcal{F}|_{U_0}$. Enfin, $\mathfrak{G}_0$ désigne toujours le groupe $\mathrm{Gal}(k|k_0)$. Lorsque V_0 est géométriquement connexe, nous allons décrire l'action de $\mathfrak{G}_0$ sur le complexe $\mathrm{R}\Gamma(X, \mathcal{F})$ déterminé précédemment. Nous donnerons ensuite un complexe de $\mathfrak{G}_0$-modules représentant $\mathrm{R}\Gamma(X, \mathcal{F})$ lorsque V_0 n'est pas géométriquement connexe.

Si V_0 est géométriquement connexe Supposons d'abord $V := V_0 \times_{k_0} k$ connexe. Soit $V_2 \to V$ le revêtement de groupe $\mathrm{H}^1(V, \Lambda)^\vee$, et soit $\overline{V_2}$ sa compactification lisse. Notons $G = \mathrm{Aut}(V_2|U)$, et M le G-module $\mathrm{H}^0(V, \mathcal{F})$. Le lemme suivant montre la compatibilité de l'action de $\mathfrak{G}_0$ sur G à celle de G sur M.

Lemme 5.6.1. Soient $g \in G$ et $\sigma \in \mathfrak{G}_0$. Pour tout $m \in M$,

$$g \cdot m = (\sigma \cdot g) \cdot m.$$

Démonstration. Il suffit de montrer que $g^{-1} \circ (\sigma \cdot g)$ agit trivialement sur M. Soit $\phi \in \mathrm{Aut}(V|U)$ l'image de g. Alors $\sigma \cdot g = \sigma g \sigma^{-1}$ a encore pour image ϕ, car $\mathfrak{G}_0$ agit trivialement sur $\mathrm{Aut}(V|U)$. Rappelons que $k(V_2) = k(V)(z_1, \ldots, z_r)$ où les z_i sont des racines n-ièmes d'éléments de $k(V)$. Alors il existe $\zeta_1, \ldots, \zeta_r \in \mu_n(k)$ tels que $(\sigma g)(z_i) = \zeta_i g(z_i)$, et $g^{-1} \circ (\sigma g)(z_i) = \zeta_i z_i$. Par conséquent, $g^{-1} \circ \sigma \cdot g \in \mathrm{Aut}(V_2|V)$ agit trivialement sur M. □

Soient $z \in Z(k_0)$, et $z' \in \overline{V_2}$ un antécédent de z. Soient $I_{z'}, P_{z'}$ les groupes d'inertie associés. Soient $\sigma \in \mathfrak{G}_0$ et $z'' = \sigma(z')$. La conjugaison par σ définit un isomorphisme $I_{z'}/P_{z'} \to I_{z''}/P_{z''}$. Le lemme précédent assure que $M^{P_{z'}} = M^{P_{z''}}$; de plus, l'action de $\mathfrak{G}_0$ sur $M^{P_{z'}}$ est triviale. Comme $I_{z'}/P_{z'}$ est canoniquement isomorphe à $\mu_e(k)$, où e est l'indice de ramification de $V_2 \to U$ en z', il est possible de calculer l'action de $\mathfrak{G}_0$ sur $\mathrm{R}\Gamma(\mu_e(k), M^{P_{z'}})$ grâce au diagramme commutatif suivant :

$$\begin{tikzcd} I_{z'}/P_{z'} \arrow[r, "\sigma"] \arrow[d, "\wr"'] & I_{z''}/P_{z''} \arrow[d, "\wr"] \\ \mu_e(k) \arrow[r] & \mu_e(k) \end{tikzcd}$$

L'action sur les groupes de cohomologie de ce complexe, qui sont $(j_\star \mathcal{F}|_{U_0})_{\bar{z}}$ et $\mathrm{H}^2_z(X, j_\star \mathcal{F}|_{U_0})$, s'en déduit immédiatement.

Soit désormais $z \in Z(k_1)$, où k_1 est une extension finie de k_0. Appelons W l'ensemble des conjugués de z sous $\mathfrak{G}_0$ et calculons le complexe $\bigoplus_{w \in W} \mathrm{R}\Gamma(I_{w'}/P_{w'}, M^{P'_w})$, où un antécédent w' de chaque point w de W a été choisi dans une même $\mathfrak{G}_0$-orbite. L'action de $\mathfrak{G}_0$ sur ce complexe permute les différents facteurs. L'action de $\mathfrak{G}_0$ sur les groupes $\mathrm{H}^0(W, j_\star \mathcal{F}|_{U_0})$ et $\mathrm{H}^2_W(X, j_\star \mathcal{F}|_{U_0})$ s'en déduit.

Si V_0 n'est pas géométriquement connexe Considérons maintenant le cas où V n'est pas connexe : le corps de fonctions de V_0 contient une extension galoisienne L de k_0. La construction de la section II.7.2 permet d'obtenir un revêtement galoisien $V_{2,0} \to U_0$ dont le corps de fonctions contient une extension galoisienne L' de k_0 suffisamment grande sur laquelle sont définis les éléments de $\mathrm{H}^1(V, \Lambda)$ ainsi que les points de la compactification lisse Y_2 de $V_2 \coloneqq V_{2,0} \times_{k_0} k$ au-dessus des points de Z. Ceci a l'avantage d'assurer que le corps résiduel de tout point fermé de $Y_{2,0}$ au-dessus d'un point de Z_0 soit exactement L'. Considérons une composante connexe V' de $V_2 = V_{2,0} \times_{k_0} k$; le choix de V' n'a aucune incidence sur ce qui suit. Le groupe $G' \coloneqq \mathrm{Aut}(V'|U) = \ker(\mathrm{Aut}(V_{2,0}|U_0) \to \mathrm{Gal}(L|k_0))$ est le stabilisateur de V' dans $G \coloneqq \mathrm{Aut}(V_{2,0}|U_0)$. Soient $M_0 = \mathrm{H}^0(V_{2,0}, \mathcal{F})$ et $M = \mathrm{H}^0(V_2, \mathcal{F})$; alors $M = \mathrm{ind}_{G'}^G(M_0)$, et le lemme de Shapiro [Neu13, Th. 4.19] assure que

$$\tau_{\leqslant 1} \mathrm{R}\Gamma(G, M) = \tau_{\leqslant 1} \mathrm{R}\Gamma(G', M_0) = \mathrm{R}\Gamma(U, \mathcal{F})$$

dans $\mathrm{D}_c^b(\Lambda)$. En tant que groupe abélien, $M = M_0^d$ où d est le nombre de composantes connexes de V_2. Le groupe $\mathfrak{G}_0$ agit naturellement sur M (en permutant ses facteurs), de façon compatible à son action sur G. Ceci permet de calculer l'action de $\mathfrak{G}_0$ sur $\tau_{\leqslant 1} \mathrm{R}\Gamma(G, M)$. Soit $z \in Z_0$ un point fermé de corps résiduel k_1. Soit v_2 un antécédent de z dans $Y_{2,0}$. Notons $W \coloneqq \{\tau(z), \tau \in \mathrm{Gal}(k_1|k_0)\}$ la $\mathfrak{G}_0$-orbite de z. Choisissons pour tout $\tau \in \mathrm{Gal}(k_1|k_0)$ un antécédent $v_{2,\tau}$ de $\tau(z_0)$ dans $V_{2,0}$; prenons les $v_{2,\tau}$ dans une même orbite sous $\mathfrak{G}_0$. Soit $D_\tau \triangleleft G$ le groupe de décomposition de $v_{2,\tau}$. Le morphisme $D_\tau \to \mathrm{Gal}(L'|k_0)$ est surjectif, de noyau le groupe d'inertie I_τ de $v_{2,\tau}$, de sorte que $M = \mathrm{ind}_{I_\tau}^{D_\tau} M_0$. Par le lemme de Shapiro,

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

dans $\mathrm{D}_c^b(\Lambda)$. Le groupe $\mathfrak{G}_0$ agit naturellement sur le complexe $\bigoplus_\tau \mathrm{R}\Gamma(D_\tau, M)$, dont les groupes de cohomologie respectifs sont $\mathrm{H}^0(W, j_\star\mathcal{F}|_U)$ et $\mathrm{H}^2_W(X, j_\star\mathcal{F}|_U)$. Avec ces notations, le complexe $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ est isomorphe dans $\mathrm{D}_c^b(\Lambda[\mathfrak{G}_0])$ au cône du morphisme de complexes :

$$\begin{tikzcd}
0 \arrow[r] & M \oplus \bigoplus_W \mathrm{H}^0(W, \mathcal{F}) \arrow[r, "(\partial_G, 0)"] \arrow[d, "\bigoplus_{W,\tau}(\mathrm{res}_{I_\tau}^G - \phi_z)"] & C^{12}(G, M) \arrow[r] \arrow[d, "\bigoplus_{W,\tau} \mathrm{res}_{I_\tau}^G"] & \bigoplus_W \bigoplus_\tau \mathrm{H}^1(I_\tau/P_\tau, M_{P_\tau}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & \bigoplus_W \bigoplus_\tau M_{P_\tau} \arrow[r, "\bigoplus_z \partial_{I_\tau}"] & \bigoplus_W \bigoplus_\tau C^{12}(I_\tau/P_\tau, M_{P_\tau}) \arrow[r] & \bigoplus_W \bigoplus_\tau \mathrm{H}^1(I_\tau/P_\tau, M_{P_\tau}) \arrow[r] & 0
\end{tikzcd}$$

où W parcourt les $\mathfrak{G}_0$-orbites de Z, et τ parcourt les k_0-automorphismes du corps résiduel des points fermés de W.

V.6.2 Complexité

Cet algorithme de calcul de $\mathrm{R}\Gamma(X, \mathcal{F})$ se compose essentiellement de deux étapes : le calcul de G et de ses sous-groupes I_z, puis des calculs d'algèbre linéaire. Soit $C = \mathrm{Spec}\, A$ le modèle plan de V utilisé par l'algorithme. Soit $z \in X$, et $z' \in \bar{V} - V$ un antécédent de z. Soit $(f_1, \ldots, f_t)$ la base de $\mathrm{H}^1(V, \mu_n)$ calculée par l'algorithme ; comme indiqué dans la remarque 2.7.3, nous pouvons supposer que l'ordre des f_i en z est positif. Pour tout $i \in \{1 \ldots t\}$, il existe donc des fonctions polynomiales g_i, h_i, où h_i ne s'annule pas en z', telles que

$$f_i = \frac{g_i}{h_i}.$$

Le construction explicite de ces fonctions est donnée dans [Sha94, §1.5, p15]. Alors V_2 est la normalisée de la courbe $C_2 \coloneqq \mathrm{Spec}\, A[z_1, \ldots, z_t]/(h_i z_i^n - g_i)$, où les f_i forment une base de $\mathrm{H}^1(V, \mu_n)$. Le point z' a n^{t-1} antécédents dans l'homogénéisée de C_2, et ceux-ci sont encore non singuliers, ce qui se lit sur les équations. Soit z'' l'un d'entre eux. Le groupe d'inertie $I_{z''}$ peut être calculé simplement en évaluant

les éléments de $\mathrm{Aut}(V_2|U)$ en z''.

Pour le résultat suivant, notons encore $C(g,q,n,r)$ la complexité du calcul de $\mathrm{H}^1(U,\mu_n)$, où U est une courbe intègre lisse sur $\overline{\mathbb{F}_q}$ provenant de $\mathbb{F}_q$, de compactification lisse X de genre g, avec $r = |X-U|$. Notons également $D(g,n,r)$ le degré de la plus petite extension de $\mathbb{F}_q$ sur laquelle sont définis les éléments de $\mathrm{H}^1(U,\mu_n)$ obtenus. Rappelons que des majorations de ces entiers ont été obtenues dans la section IV.3.4.1

Théorème 5.6.2. Soit X_0 une courbe lisse géométriquement connexe sur $\mathbb{F}_q$. Notons $X = (X_0)_{\overline{\mathbb{F}_q}}$. Soit $\bar{X}$ sa compactification lisse. Notons g le genre de $\bar{X}$. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X, lisse sur un ouvert U de X, de fibre générique géométrique un Λ-module M. Soit d l'ordre de l'image du morphisme $\pi_1(X) \to \mathrm{Aut}_\Lambda(M)$. Notons m un majorant du nombre de générateurs de M et de chacun des $\mathcal{F}_z$, $z \in X-U$. Enfin, notons $r = |X-U|$. Supposons donné un modèle plan d'un revêtement galoisien V de U trivialisant $\mathcal{F}$, et qui n'a pas de points singuliers au-dessus de $X-U$. Il existe un algorithme probabiliste (Las Vegas) qui calcule un complexe de $\Lambda[\mathfrak{G}_0]$-modules représentant $\mathrm{R}\Gamma(X,\mathcal{F})$ en

$$O\left(C(d(g+r),q,n,dr) + r(md^3n^{4d(g+2r)}D(d(2g+r),n,dr))^3\right)$$

opérations dans $\mathbb{F}_q$.

Démonstration. Le calcul est à peine plus compliqué dans le cas lisse (voir théorème 5.3.5) : une fois déterminé le groupe $\mathrm{Aut}(V_2|U)$, le calcul des groupes d'inertie en découle comme décrit ci-dessus. Le nombre de calculs d'algèbre linéaire à effectuer est proportionnel au nombre de points de $\bar{X}-U$. □

La borne obtenue sur $C(g,q,n,r)$ dans la proposition 4.3.3 permet d'en déduire le résultat suivant.

Corollaire 5.6.3. Avec les notations et hypothèses du théorème, il existe un algorithme probabiliste (Las Vegas) qui calcule $\mathrm{R}\Gamma(X,\mathcal{F})$ en

$$\mathcal{P}(d,g,n,r,m,\log q)^{2^{O\left((d(g+r))^2\right)}}$$

opérations dans $\mathbb{F}_q$, où $\mathcal{P}$ est un polynôme. Si V admet un modèle plan à singularités ordinaires de degré $O(g)$, cette complexité devient

$$\mathcal{P}(d,g,n,r,m,\log q)^{O\left((d(g+r))^4\right)}.$$

V.6.3 Adaptation au cas des courbes nodales

Soit X une courbe intègre à singularités au pire nodales sur le corps algébriquement clos k. Notons $\nu\colon \tilde{X} \to X$ sa normalisation. Soit $\mathcal{F}$ un faisceau constructible de Λ-modules sur X. Soit $j\colon U \to X$ l'inclusion d'un ouvert affine lisse de X tel que le faisceau $\mathscr{L} \coloneqq j^\star\mathcal{F}$ soit lisse, et $i\colon Z \to X$ l'inclusion du fermé réduit complémentaire. Notons M la fibre générique géométrique de $\mathscr{L}$. Comme dans le cas des courbes lisses, nous calculons $\mathrm{R}\Gamma(X,\mathcal{F})$ à l'aide des deux triangles distingués

$$\mathrm{R}\Gamma(X,\mathcal{F}) \to \mathrm{R}\Gamma(X,j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X,i_\star i^\star\mathcal{F}) \to \mathrm{R}\Gamma(X,i_\star i^\star j_\star\mathcal{F}) \xrightarrow{+1}$$

et

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

Soit $V \to U$ un revêtement galoisien trivialisant $\mathscr{L}$. Comme U est lisse, V l'est également. Notons $\tilde{V}$ sa normalisée, et $V_2 \to V$ le revêtement de groupe $\mathrm{H}^1(V,\Lambda)^\vee$. Notons G le groupe $\mathrm{Aut}(V_2|U)$. Le morphisme $\tau_{\leqslant 1}\,\mathrm{R}\Gamma(G,M) \to \mathrm{R}\Gamma(U,\mathscr{L})$ est toujours un quasi-isomorphisme. Notons $\tilde{Z}$ la préimage de

Z dans $\tilde{X}$. Le complexe $\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})$ est canoniquement quasi-isomorphe à $\mathrm{R}\Gamma_{\tilde{Z}}(\tilde{X}, \nu^\star j_\star\mathscr{L})$ d'après le corollaire 2.5.5. Pour chaque point régulier z de X appartenant à Z, notons I_z son stabilisateur dans G. Pour chaque point nodal z de X appartenant à Z, notons Q, R ses antécédents dans $\tilde{X}$, et I_Q, I_R leurs stabilisateurs respectifs dans G. Le complexe suivant représente donc $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$:

$$M \to C^{12}(G, M) \to \bigoplus_{z\in\tilde{Z}} \mathrm{H}^1(I_z, M)$$

Comme précédemment, il est possible de remplacer ici $\mathrm{H}^1(I_z, M)$ par $\mathrm{H}^1(I_z/P_z, M_{P_z})$ où P_z est le sous-groupe d'inertie sauvage de I_z (et de même pour les points Q, R). Rappelons que pour tout $z \in Z$, $(j_\star\mathscr{L})_z = \mathrm{H}^0(I_Q, M) \times \mathrm{H}^0(I_R, M)$. Nous noterons $\phi_z \colon \mathcal{F}_z \to \mathrm{H}^0(I_Q, M) \times \mathrm{H}^0(I_R, M)$ le morphisme de recollement. Par conséquent, $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ est représenté par le cône du morphisme de complexes :

$$\begin{tikzcd}
0 \arrow[r] & M \oplus \bigoplus_{z\in Z} \mathcal{F}_z \arrow[r, "(\partial_G, 0)"] \arrow[d, "\bigoplus_{z\in Z}(\mathrm{id} - \phi_z)"] & C^{12}(G, M) \arrow[r] \arrow[d, "\bigoplus_{\tilde{z}\in Z} \mathrm{res}^G_{I_{\tilde{z}}}"] & \bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) \arrow[r] \arrow[d, "\mathrm{id}"] & 0 \\
0 \arrow[r] & \bigoplus_{\tilde{z}\in\tilde{Z}} M_{P_{\tilde{z}}} \arrow[r, "\bigoplus_{\tilde{z}} \partial_{I_{\tilde{z}}}"] & \bigoplus_{\tilde{z}\in\tilde{Z}} C^{12}(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) \arrow[r] & \bigoplus_{\tilde{z}\in\tilde{Z}} \mathrm{H}^1(I_{\tilde{z}}/P_{\tilde{z}}, M_{P_{\tilde{z}}}) \arrow[r] & 0
\end{tikzcd}$$

V.6.4 Adaptation au cas des complexes

Soit X une courbe intègre lisse sur k. Soit $j \colon U \to X$ l'inclusion d'un ouvert. Soit $i \colon Z \to X$ le fermé réduit complémentaire. Soit $\mathscr{K}^\bullet = [\mathscr{K}^0 \to \cdots \to \mathscr{K}^b]$ un complexe de faisceaux constructibles sur X tel que tous les $\mathscr{K}^i$ soient lisses sur U, et que les $j^\star\mathscr{K}^i$ soient trivialisés par $V \to U$. Notons $\mathscr{L} = j^\star\mathscr{K}$. Notons $K^\bullet$ le complexe de $G = \mathrm{Aut}(V_2|U)$-modules associé. Les foncteurs $j_\star, j^\star, i_\star, i^\star$ s'étendent terme à terme aux catégories (non dérivées) de complexes de faisceaux constructibles sur X. L'utilisation surprenante de ces foncteurs non dérivés s'explique par notre stratégie pour calculer $\mathrm{R}\Gamma(X, \mathscr{K})$: elle consiste à insérer $\mathscr{K}$ dans une suite exacte dans la catégorie des complexes de faisceaux constructibles sur X, puis d'en déduire un triangle distingué dans $\mathrm{D}^b_c(\Lambda)$. En particulier, si $\mathscr{K}'$ est un autre complexe quasi-isomorphe à $\mathscr{K}$, les complexes obtenus représentant $\mathrm{R}\Gamma(X, \mathscr{K})$ et $\mathrm{R}\Gamma(X, \mathscr{K}')$ seront distincts ; étant donné un quasi-isomorphisme explicite entre $\mathscr{K}$ et $\mathscr{K}'$, il sera toutefois possible de calculer le quasi-isomorphisme $\mathrm{R}\Gamma(X, \mathscr{K}) \to \mathrm{R}\Gamma(X, \mathscr{K}')$ qu'il induit.

Afin de simplifier l'exposition, supposons que Z soit réduit à un seul point fermé z. Fixons un point $v \in V_2$ au-dessus de z, et notons $I_z = \{\sigma \in G \mid \sigma(v) = v\}$. Pour le cas général, il suffira de remplacer $C^j(I_z, -)$ (resp. $\mathrm{H}^j(I_z, -)$) par $\bigoplus_{z\in Z} C^j(I_z, -)$ (resp. $\bigoplus_{z\in Z} \mathrm{H}^j(I_z, -)$). Il y a une suite exacte de complexes de faisceaux constructibles :

$$0 \to \mathscr{K} \to j_\star\mathscr{L} \oplus i_\star i^\star\mathscr{K} \to i_\star Q \to 0$$

où $Q \simeq i^\star j_\star\mathscr{L}$, ce qui se déduit terme à terme de l'énoncé correspondant pour les faisceaux. L'élément $\mathrm{R}\Gamma(X, \mathscr{K})[1]$ de $\mathrm{D}^b_c(\Lambda)$ est donc le cône de

$$\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathscr{K}) \to \mathrm{R}\Gamma(X, i_\star Q).$$

V.6.4.1 Calcul de $\mathrm{R}\Gamma(X, j_\star\mathscr{L})$

Comme précédemment, il y a un triangle distingué dans $\mathrm{D}^b_c(X, \Lambda)$ [Stacks, 09XP] :

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

qui montre que $\mathrm{R}\Gamma(X, j_\star\mathscr{L})[1]$ est le cône de $\mathrm{R}\Gamma(U, \mathscr{L}) \to \mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})[1]$.

Lemme 5.6.4. Le complexe

$$0 \to 0 \to \mathrm{H}^1(I_z, K^0) \to \mathrm{H}^1(I_z, K^1) \to \mathrm{H}^1(I_z, K^2) \to \cdots$$

(où les termes ci-dessus sont placés en degrés $\geqslant 0$) représente $\mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})$.

Démonstration. Soit $I^{\bullet,\bullet}$ une résolution de Cartan-Eilenberg de $j_\star\mathscr{L}$. La colonne $I^{p,\bullet}$ est alors une résolution injective de $j_\star\mathscr{L}^p$. Rappelons que pour chaque entier p et chaque point z de Z, les $\mathrm{H}^i_z(X, j_\star\mathscr{L}^p)$ sont nuls dès que $i \neq 2$, et $\mathrm{H}^2_z(X, j_\star\mathscr{L}^p) = \mathrm{H}^1(I_z, K^p)$. Les morphismes

$$\tau_{q\geqslant 2}\tau_{q\leqslant 2}\Gamma_Z(X, I^{\bullet,\bullet}) \leftarrow \tau_{q\leqslant 2}\Gamma_Z(X, I^{\bullet,\bullet}) \to \Gamma_Z(X, I^{\bullet,\bullet})$$

induisent donc des isomorphismes entre les premières pages des suites spectrales associées à ces complexes doubles pour l'orientation verticale, et donc des quasi-isomorphismes entre les complexes totaux associés. Comme le complexe double de gauche a exactement un terme non nul dans chaque colonne, à hauteur 2, son complexe total associé est celui de l'énoncé du lemme. □

Le morphisme $\mathrm{R}\Gamma(U, \mathscr{L}) \to \mathrm{R}\Gamma_Z(X, j_\star\mathscr{L})[1]$ est donc représenté par le morphisme de complexes

$$\begin{tikzcd}
C^0(G, K^0) \arrow[r] \arrow[d] & C^{12}(G, K^0) \oplus C^0(G, K^1) \arrow[r] \arrow[d] & C^{12}(G, K^1) \oplus C^0(G, K^2) \arrow[r] \arrow[d] & \cdots \\
0 \arrow[r] & \mathrm{H}^1(I_z/P_z, K^0_{P_z}) \arrow[r] & \mathrm{H}^1(I_z/P_z, K^1_{P_z}) \arrow[r] & \ldots
\end{tikzcd}$$

où les flèches verticales sont déduites du morphisme $I_z \to G$. Le complexe $\mathrm{R}\Gamma(X, j_\star j^\star K)$ est donc

$$C^0(G, K^0) \to C^{12}(G, K^0) \oplus C^0(G, K^1) \to C^{12}(G, K^1) \oplus C^0(G, K^2) \oplus \mathrm{H}^1(I_z/P_z, K^0_{P_z}) \to \cdots$$

et son i-ième terme est

$$\mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(G, K^{i-1}) \oplus C^0(G, K^i).$$

V.6.4.2 Calcul de $\mathrm{R}\Gamma(X, \mathscr{K})$

Il reste à déterminer le complexe $\mathrm{R}\Gamma(X, i_\star Q)$ ainsi que le morphisme

$$\mathrm{R}\Gamma(X, j_\star\mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star\mathscr{K}) \to \mathrm{R}\Gamma(X, i_\star Q).$$

Lemme 5.6.5. Le complexe total associé au complexe double

$$\begin{tikzcd}
\mathrm{H}^1(I_z/P_z, K^0_{P_z}) \arrow[r] & \mathrm{H}^1(I_z/P_z, K^1_{P_z}) \arrow[r] & \mathrm{H}^1(I_z/P_z, K^2_{P_z}) \arrow[r] & \cdots \\
C^{12}(I_z/P_z, K^0_{P_z}) \arrow[r] \arrow[u] & C^{12}(I_z/P_z, K^1_{P_z}) \arrow[r] \arrow[u] & C^{12}(I_z/P_z, K^2_{P_z}) \arrow[r] \arrow[u] & \cdots \\
C^0(I_z/P_z, K^0_{P_z}) \arrow[r] \arrow[u] & C^0(I_z/P_z, K^1_{P_z}) \arrow[r] \arrow[u] & C^0(I_z/P_z, K^2_{P_z}) \arrow[r] \arrow[u] & \cdots
\end{tikzcd}$$

représente $\mathrm{R}\Gamma(X, i_\star Q) = \mathrm{R}\Gamma(X, i_\star i^\star j_\star\mathscr{L})$. Son i-ième terme est

$$L^i := \mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(I_z/P_z, K^{i-1}_{P_z}) \oplus C^0(I_z, K^i_{P_z}).$$

Démonstration. Pour tout complexe A de groupes abéliens, $\mathrm{R}\Gamma(Z, A) = A$. En particulier,

$$\mathrm{R}\Gamma(X, i_\star Q) = \mathrm{R}\Gamma(Z, Q) = Q = i^\star j_\star \mathscr{L} = (\mathrm{H}^0(I_z/P_z, K^p_{P_z}))_{p \geqslant 0}.$$

Il y a pour tout p un quasi-isomorphisme de complexes

$$\mathrm{H}^0(I_z/P_z, K^p_{P_z})[0] \to [C^0(I_z/P_z, K^p_{P_z}) \to C^{12}(I_z/P_z, K^p_{P_z}) \to \mathrm{H}^1(I_z/P_z, K^p_{P_z})].$$

Ce dernier étant compatible aux morphismes de transition de K, il induit un morphisme de complexes doubles entre le complexe ayant pour seule ligne $\mathrm{H}^0(I_z/P_z, K^\bullet_{P_z})$ et le complexe de l'énoncé, qui induit un isomorphisme entre les premières pages des suites spectrales associées (pour l'orientation verticale). Par conséquent, il induit un quasi-isomorphisme entre les complexes totaux associés. □

Le morphisme $\mathrm{R}\Gamma(X, j_\star \mathscr{L}) \to \mathrm{R}\Gamma(X, i_\star Q)$ est donc le suivant.

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(G, K^{i-1}_{P_z}) \oplus C^0(G, K^i_{P_z}) \arrow[r] \arrow[d, "(\mathrm{id}, \mathrm{res}^G_{I_z}, \mathrm{res}^G_{I_z})"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(I_z/P_z, K^{i-1}_{P_z}) \oplus C^0(I_z/P_z, K^i_{P_z}) \arrow[r] & \cdots
\end{tikzcd}$$

D'autre part, le morphisme $\mathrm{R}\Gamma(X, i_\star i^\star \mathscr{K}) \to \mathrm{R}\Gamma(X, i_\star Q)$ est le suivant.

$$\begin{tikzcd}
\cdots \arrow[r] & \mathscr{K}^i_z \arrow[r] \arrow[d, "(0,0,-\phi_z)"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}^1(I_z, K^{i-2}_{P_z}) \oplus C^{12}(I_z/P_z, K^{i-1}_{P_z}) \oplus C^0(I_z/P_z, K^i_{P_z}) \arrow[r] & \cdots
\end{tikzcd}$$

Le complexe $\mathrm{R}\Gamma(X, \mathscr{K})[1]$ est le cône de $\mathrm{R}\Gamma(X, j_\star \mathscr{L}) \oplus \mathrm{R}\Gamma(X, i_\star i^\star \mathscr{K}) \to \mathrm{R}\Gamma(X, i_\star Q)$. Nous avons démontré le théorème suivant.

Théorème 5.6.6. Soit X une courbe intègre lisse sur k. Soit $\mathscr{K} = [\mathscr{K}^0 \to \cdots \to \mathscr{K}^b]$ un complexe de faisceaux constructibles de Λ-modules sur X. Soient U un ouvert de X sur lequel chaque $\mathscr{K}^i$ est lisse de fibre K^i, et Z le fermé réduit complémentaire. Soient $V \to U$ un revêtement galoisien qui trivialise $\mathcal{F}|_U$, et $V_2 \to V$ le revêtement de V de groupe $\mathrm{H}^1(V, \Lambda)^\vee$. Notons $G = \mathrm{Aut}(V_2|U)$. Pour chaque point $z \in Z$, notons I_z le groupe d'inertie d'un point de la compactification lisse de V_2 au-dessus de z, et P_z le groupe d'inertie sauvage correspondant. Notons $\phi^i_z \colon \mathscr{K}^i_z \to \mathrm{H}^0(I_z, K^i) \subseteq \mathrm{H}^0(P_z, K^i) \xrightarrow{\sim} K^i_{P_z}$ le morphisme de recollement en z. Alors $\mathrm{R}\Gamma(X, \mathcal{F})[1]$ est le cône du morphisme de complexes suivant, où $C^{12}(G, M)$ désigne le groupe des morphismes croisés $G \to M$.

$$\begin{tikzcd}
\cdots \arrow[r] & \mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(G, K^{i-1}_{P_z}) \oplus C^0(G, K^i_{P_z}) \oplus \mathscr{K}^i_z \arrow[r] \arrow[d, "(\mathrm{id}, \mathrm{res}^G_{I_z}, \mathrm{res}^G_{I_z}\ -\phi_z)"] & \cdots \\
\cdots \arrow[r] & \mathrm{H}^1(I_z/P_z, K^{i-2}_{P_z}) \oplus C^{12}(I_z/P_z, K^{i-1}_{P_z}) \oplus C^0(I_z/P_z, K^i_{P_z}) \arrow[r] & \cdots
\end{tikzcd}$$

V.6.5 Un exemple détaillé

Le cas étudié Supposons que -1 n'est pas un carré dans k_0. Posons $n = 2$. Considérons les courbes $Y_0 = X_0 = \mathbb{P}^1_{k_0}$, et le morphisme $f_0 \colon Y_0 \to X_0, y \mapsto y^2$. Soit $\mathcal{F}_0$ le faisceau $(f_0)_\star \Lambda$, lisse sur l'ouvert $U_0 := \mathbb{G}_{m,k_0} = \operatorname{Spec} k[x^{\pm 1}]$ de X_0. Soit $V_0 = \operatorname{Spec} k[y^{\pm 1}]$ sa préimage dans Y_0. Soient Z_0, W_0 les complémentaires réduits respectifs de U_0, V_0 dans X_0, Y_0. Le faisceau $\mathcal{F}_0$ est lisse sur U_0, trivialisé par V_0, de fibre $M = \Lambda^2$. L'automorphisme de M induit par l'élément non trivial de $\mathrm{Aut}(V_0|U_0) \simeq \mathbb{Z}/2\mathbb{Z}$ échange les deux copies de Λ. Notons encore $X, Y, U, V, Z, W, \mathcal{F}$ les changements de base à k respectifs de $X_0, Y_0, U_0, V_0, Z_0, W_0, \mathcal{F}_0$. Notons $j \colon U \to X$ l'inclusion, et $\mathscr{L}$ le faisceau lisse $j^\star \mathcal{F}$. Calculons $\mathrm{R}\Gamma(X, \mathcal{F})$.

Le revêtement trivialisant les $\mathscr{L}$-torseurs Le revêtement $V_2 \to V$ de groupe $\mathrm{H}^1(V, \Lambda)$ est simplement $\mathbb{G}_m \to \mathbb{G}_m, z \mapsto z^2$. Par conséquent, $V_2 \to U$ est le revêtement $\mathbb{G}_m \to \mathbb{G}_m, z \mapsto z^4$ de groupe $G = \mathbb{Z}/4\mathbb{Z}$ engendré par $\gamma\colon z \mapsto iz$, où i est une racine carrée de -1 dans k. Les groupes d'inertie en 0 et ∞ sont encore égaux à G. Par conséquent, $(j_\star j^\star)\mathcal{F}_0 = \Lambda$ et $(j_\star \mathscr{L})_\infty = \Lambda$. Les morphismes de recollement $\mathcal{F}_0 \to (j_\star \mathscr{L})_0$ et $\mathcal{F}_\infty \to (j_\star \mathscr{L})_\infty$ sont l'identité $\Lambda \to \Lambda$.

Calcul de $\mathrm{R}\Gamma(U, \mathcal{F}|_U)$ Les morphismes croisés $G \to M$ sont uniquement déterminés par l'image $(a, b) \in \Lambda^2$ de γ. Le complexe de cochaînes usuel représentant $\mathrm{R}\Gamma(G, M) = \mathrm{R}\Gamma(U, \mathcal{F}|_U)$ est le suivant.

$$\begin{array}{ccc} \Lambda^2 & \longrightarrow & C^{12}(G, \Lambda^2) \\ (a, b) & \longmapsto & [\gamma \mapsto (a + b, a + b)] \end{array}$$

Le groupe $\mathrm{H}^1(G, M)$ est donc isomorphe à Λ, et le morphisme $\Lambda^2 \to \mathrm{H}^1(G, M)$ qui associe à morphisme croisé sa classe de cohomologie a pour noyau $\langle (1, 1) \rangle$; il s'identifie au morphisme

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

Calcul de $\mathrm{R}\Gamma(X, j_\star \mathscr{L})$ L'élément $\mathrm{R}\Gamma(X, j_\star \mathscr{L})[1] \in \mathrm{D}^b_c(X, \Lambda)$ est le cône du morphisme

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

Par conséquent, $\mathrm{R}\Gamma(X, j_\star \mathscr{L})$ est représenté par le complexe

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

où les deux morphismes sont définis par $(a, b) \mapsto (a + b, a + b)$.

Calcul de $\mathrm{R}\Gamma(X, \mathcal{F})$ Calculons désormais le morphisme

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

D'une part, $\mathrm{R}\Gamma(Z, i^\star \mathcal{F}) = \mathrm{H}^0(Z, i^\star \mathcal{F})[0] = \mathcal{F}_0[0] \oplus \mathcal{F}_\infty[0]$. D'autre part, $\mathrm{R}\Gamma(Z, i^\star j_\star \mathscr{L})$ est représenté par le complexe

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

où les flèches sont $\alpha'\colon (a, b, c, d) \mapsto (a + b, a + b, c + d, c + d)$ et $\beta'\colon (a, b, c, d) \mapsto (a + b, c + d)$. Le morphisme de complexes cherché est donc

$$\begin{tikzcd} \Lambda^4 \arrow[r, "\alpha"] \arrow[d, "u"] & \Lambda^2 \arrow[r, "\beta"] \arrow[d, "v"] & \Lambda^2 \arrow[d, "\mathrm{id}"] \\ \Lambda^4 \arrow[r, "\alpha'"] & \Lambda^4 \arrow[r, "\beta'"] & \Lambda^2 \end{tikzcd}$$

où, en écrivant le terme en haut à gauche comme $\mathcal{F}_0 \oplus \mathcal{F}_\infty \oplus M$,

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

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

En calculant le cône de ce morphisme puis en décalant de 1, on obtient le complexe suivant, qui représente $\mathrm{R}\Gamma(X,\mathcal{F})$.

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

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

Ce complexe a pour groupes de cohomologie $\mathrm{H}^0 = \langle (1,1,1,1) \rangle$, $\mathrm{H}^1 = 0$ et $\mathrm{H}^2 = \langle \overline{(1,0,1,0,0,0)} \rangle \simeq \Lambda$. C'est le résultat attendu : nous avons calculé la cohomologie du faisceau $(\mathbb{P}^1 \xrightarrow{x \mapsto x^2} \mathbb{P}^1)_\star \Lambda$, qui est la cohomologie de Λ sur $\mathbb{P}^1$.

Action de Galois L'action de $\mathrm{Gal}(k|k_0)$ sur $\mathrm{R}\Gamma(X,\mathcal{F})$ se factorise par celle de $\mathrm{Gal}(k_0(i)|k_0)$. Notons $\sigma \colon i \mapsto -i$ le k_0-automorphisme non trivial de $k_0(i)$. Le groupe $\mathfrak{G}_0$ agit sur $G = \mathrm{Aut}(V_2|V)$ par $\sigma \cdot \gamma = \gamma^3$, et trivialement sur M. Son action sur $\tau_{\leqslant 1} \mathrm{R}\Gamma(G,M) = \Lambda^2 \to \Lambda^2$ est donc triviale sur le premier terme, et $(a,b) \mapsto (b,a)$ sur le second. En particulier, son action sur $\mathrm{H}^1(G,M) = \Lambda$ est triviale. L'action de σ est également triviale sur $\mathcal{F}_0, \mathcal{F}_\infty$. En résumé, l'action sur le complexe

$$\Lambda^4 \to \Lambda^6 \to \Lambda^6 \to \Lambda^2$$

représentant $\mathrm{R}\Gamma(X,\mathcal{F})$ est triviale sur le premier et le dernier terme,

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

sur le deuxième, et

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

sur le troisième. Il en découle en particulier que $\mathfrak{G}_0$ agit trivialement sur les deux groupes non nuls $\mathrm{H}^0(X,\Lambda)$ et $\mathrm{H}^2(X,\Lambda)$, comme attendu.

CHAPITRE VI

Cohomologie des surfaces

Dans ce chapitre encore, k désigne un corps algébriquement clos, et n un entier inversible dans k. L'anneau $\mathbb{Z}/n\mathbb{Z}$ est toujours noté Λ. Nous indiquons comment utiliser les techniques présentées dans le chapitre V pour calculer la cohomologie d'un faisceau constant sur une k-surface lisse ; il reste à calculer précisément la complexité de l'algorithme obtenu. La technique utilisée est celle de la fibration en courbes projectives par le moyen d'un pinceau de Lefschetz, telle que suggérée dans [EC11, Epilogue].

VI.1 Pinceaux de Lefschetz

Soit X une variété projective connexe non singulière sur k, plongée dans $\mathbb{P}^n_k$. Un pinceau d'hyperplans dans $\mathbb{P}^n$ est une droite D de l'espace projectif dual $\check{\mathbb{P}}^n$. Elle paramètre les hyperplans contenant un sous-espace linéaire A de $\mathbb{P}^n$ de codimension 2 appelé l'axe de D. Pour tout $t \in D$, notons H_t l'hyperplan correspondant. Soit $\tilde{X}$ le fermé réduit de $X \times D$ dont les points (x, t) vérifient $x \in H_t$. Soit $\pi\colon \tilde{X} \to D$ la projection sur la deuxième coordonnée. La fibre de π en t est alors l'intersection schématique $X_t \coloneqq H_t \cap X$.

$$\begin{tikzcd} X & \tilde{X} \arrow[l] \arrow[d, "\pi"] \\ & D \end{tikzcd}$$

Définition 6.1.1. [SGA7$_2$, XVII, 2.2] Avec ces notations, un pinceau d'hyperplans D est dit de Lefschetz pour X s'il vérifie les conditions suivantes.

1. L'axe A est transverse à X [EGA 4$_4$, XVII, 17.13.7]. (Alors $\tilde{X}$ est l'éclaté de X en $X \cap A$.)
2. Il existe une partie finie $S \subset D$ et pour chaque point fermé $s \in S$ un unique point $x_s \in \tilde{X}_s$ tels que π soit lisse en-dehors des x_s.
3. Pour tout point fermé s du fermé S du point précédent, la courbe X_s est nodale avec pour unique point singulier x_s.

Si D est un pinceau de Lefschetz pour X, le morphisme $\pi\colon \tilde{X} \to D \xrightarrow{\sim} \mathbb{P}^1$ est propre, plat et admet une section. Sa fibre générique est lisse. De plus, le morphisme canonique $\mathcal{O}_{\mathbb{P}^1} \to \pi_\star \mathcal{O}_{\tilde{X}}$ est un

isomorphisme [Mil80, V, Th. 3.1]. Étant donné un point fermé x de l'intersection de X avec l'axe du pinceau, le morphisme $D \to \tilde{X}$, $t \mapsto (x,t)$ est une section de $\tilde{X} \to D$. Ceci revient à identifier D avec l'une des composantes du diviseur exceptionnel de l'éclatement $\tilde{X} \to X$. Si X est une surface alors, quitte à la plonger dans $\mathbb{P}^{\binom{n+3}{3}}$ via le plongement de Veronese de degré 3, un pinceau d'hyperplans général pour X est un pinceau de Lefschetz et les fibres du morphisme $X \to \mathbb{P}^1$ correspondant sont irréductibles [Igu56, p178, Conclusion].

Au vu de ces résultats, la façon la plus rapide d'obtenir un pinceau de Lefschetz est probabiliste : tirer au hasard une droite de $\mathbb{P}^3$, puis vérifier si elle est l'axe d'un pinceau en vérifiant les trois points de la définition, qui sont tous les trois algorithmiquement testables.

VI.2 Trivialisation des images directes dérivées

Proposition 6.2.1. Soit $\pi\colon X \to S$ un morphisme propre lisse de schémas intègres normaux de type fini sur k. Soit $\mathcal{F}$ un faisceau lisse de Λ-modules sur X. Soient η le point générique et $\bar{\eta}$ un point générique géométrique de S. Soit $i \in \mathbb{N}$. Soit $\eta' \to \eta$ un revêtement galoisien minimal par lequel se factorise l'action de $\mathrm{Gal}(\bar{\eta}|\eta)$ sur $\mathrm{H}^i(X_{\bar{\eta}}, \mathcal{F})$. Soit S' la normalisation de S dans η'. Alors le faisceau $\mathrm{R}^i\pi_\star\mathcal{F}$ est lisse, et $S' \to S$ est un revêtement étale galoisien minimal qui le trivialise.

Démonstration. Notons $\mathcal{G}$ le faisceau $\mathrm{R}^i\pi_\star\mathcal{F}$. Le théorème 1.5.14 de changement de base propre-lisse assure que $\mathcal{G}$ est lisse. Le théorème 1.5.8 de changement de base propre affirme que, pour tout point géométrique $\bar{s}$ de S, le morphisme canonique

$$\mathcal{G}_{\bar{s}} \to \mathrm{H}^i(X_{\bar{s}}, \mathcal{F})$$

est un isomorphisme. Alors

$$\mathrm{H}^0(\eta', \mathcal{G}_{\bar{\eta}}) = \mathrm{H}^0(\mathrm{Gal}(\bar{\eta}|\eta'), \mathcal{G}_{\bar{\eta}}) = \mathrm{H}^0(\mathrm{Gal}(\bar{\eta}|\eta'), \mathrm{H}^i(X_{\bar{\eta}}, \mathcal{F})) = \mathrm{H}^i(X_{\bar{\eta}}, \mathcal{F}) = \mathcal{G}_{\bar{\eta}}$$

et $\eta' \to \eta$ trivialise le faisceau $\eta^\star\mathcal{G}$. Notons $\mathfrak{S}$ l'image de $\pi_1 S$ dans $\mathrm{Aut}_\Lambda(\mathcal{G}_{\bar{\eta}})$: c'est le groupe de monodromie. Montrons que $\mathcal{G}|_{S'}$ est constant, c'est-à-dire que le morphisme $\pi_1 S' \to \mathfrak{S}$ est trivial. Le diagramme commutatif

$$\begin{tikzcd} S' \arrow[d, "f"] & \eta' \arrow[l, "g'"'] \arrow[d] \\ S & \eta \arrow[l, "g"'] \end{tikzcd}$$

fournit le diagramme commutatif suivant :

$$\begin{tikzcd} \mathrm{Gal}(\bar{\eta}|\eta') \arrow[r, two heads] \arrow[d] & \pi_1 S' \arrow[d] \arrow[dr] & \\ \mathrm{Gal}(\bar{\eta}|\eta) \arrow[r, two heads] & \pi_1 S \arrow[r, two heads] & \mathfrak{S} \end{tikzcd}$$

Comme $g'^\star f^\star\mathcal{G}$ est constant, le morphisme $\mathrm{Gal}(\bar{\eta}|\eta') \to \mathfrak{S}$ est trivial, et il en est de même du morphisme $\pi_1 S' \to \mathfrak{S}$. Il reste à montrer que le morphisme génériquement étale $S' \to S$ est étale. Soit $T \to S$ un revêtement étale galoisien minimal de S trivialisant $\mathcal{F}$. Soit η_T son point générique. Alors

$$\mathrm{Gal}(\eta_T|\eta) = \frac{\mathrm{Gal}(\bar{\eta}|\eta)}{\ker(\mathrm{Gal}(\bar{\eta}|\eta) \to \mathfrak{S})} = \mathrm{Gal}(\eta'|\eta)$$

et le théorème 2.1.1 assure que $S' \simeq T$. $\square$

VI.3 Calcul de la cohomologie de μ_n sur une surface

Soit X une surface intègre projective lisse sur k. Soit D un pinceau de Lefschetz pour X. Notons $\pi\colon \tilde{X} \to \mathbb{P}^1$ le morphisme correspondant défini dans la section VI.1. Soit $\mathcal{F}$ un faisceau constructible sur X, de tiré en arrière $\tilde{\mathcal{F}}$ sur $\tilde{X}$. Alors $\mathrm{R}\pi_\star\tilde{\mathcal{F}} \in \mathrm{D}^b_c(\mathbb{P}^1, \Lambda)$ et

$$\mathrm{R}\Gamma(\tilde{X}, \tilde{\mathcal{F}}) = \mathrm{R}\Gamma(\mathbb{P}^1, \mathrm{R}\pi_\star\tilde{\mathcal{F}}).$$

Soit U un ouvert de $\mathbb{P}^1$ au-dessus duquel π est lisse et $\tilde{\mathcal{F}}$ est lisse. La proposition précédente montre comment construire, pour tout entier naturel i, un revêtement galoisien de U trivialisant $(\mathrm{R}^1\pi_\star\tilde{\mathcal{F}})|_U$. Soit $\bar{\eta}$ un point générique géométrique de $\mathbb{P}^1$, d'image le point générique $\eta = \operatorname{Spec} k(t)$. Il suffit de calculer $\mathrm{H}^1(\tilde{X}_{\bar{\eta}}, \mathcal{F})$ avec son action de $\mathrm{Gal}(\bar{\eta}|\eta)$: cette dernière se factorise par l'action d'un quotient $\mathrm{Gal}(\eta'|\eta)$, et la normalisation de U dans η' convient. Le degré de $\eta' \to \eta$ est l'ordre du groupe de monodromie $\mathfrak{S} \subseteq \mathrm{Aut}_\Lambda(\mathrm{H}^i(\tilde{X}_{\bar{\eta}}, \tilde{\mathcal{F}}))$. Lorsque $\tilde{\mathcal{F}} = \mu_n$, il est borné par $n^{O(g^2)}$ où g est le genre de $\tilde{X}_{\bar{\eta}}$.

Le calcul des $\mathrm{H}^i(\tilde{X}, \mu_n)$ est traité dans [Mil80, V, §3]. Nous allons le résumer en insistant sur la description explicite des objets et des morphismes concernés. Tout d'abord, la connexité des fibres de π assure que $\pi_\star\mu_n = \mu_n$. De plus, le morphisme $\mathbb{Z} \to \mathrm{R}^2\pi_\star\mu_n$ par lequel se factorise $\mathrm{R}^1\pi_\star\mathbb{G}_m \to \mathrm{R}^2\pi_\star\mu_n$ induit un isomorphisme $\Lambda \to \mathrm{R}^2\pi_\star\mu_n$. Pour tout point fermé $\bar{s} \in \mathbb{P}^1$, le morphisme de spécialisation $\mathrm{H}^1(\tilde{X}_{\bar{\eta}}, \mu_n) \to \mathrm{H}^1(\tilde{X}_{\bar{s}}, \mu_n)$ associe à la classe d'un diviseur $D \in \mathrm{Div}^0(X_{\bar{\eta}})$ la classe de l'intersection de son adhérence dans $\tilde{X}$ avec la fibre $\tilde{X}_{\bar{s}}$. C'est un isomorphisme lorsque $\tilde{X}_{\bar{s}}$ est lisse.

VI.3.1 Morphismes de bord de la suite spectrale de Leray

Le faisceau $\mathrm{R}^1\pi_\star\mathbb{G}_m$ est le foncteur de Picard relatif

$$\mathrm{Pic}_{\tilde{X}/\mathbb{P}^1}\colon \mathrm{Pic}(T \times_{\mathbb{P}^1} \tilde{X})/\pi_T^\star \mathrm{Pic}(T).$$

C'est le faisceautisé du foncteur de Picard absolu $(T \to \mathbb{P}^1) \mapsto \mathrm{Pic}(T \times_{\mathbb{P}^1} \tilde{X})$. En particulier, le morphisme $\mathrm{H}^1(\tilde{X}, \mathbb{G}_m) \to \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^1\pi_\star\mathbb{G}_m)$ obtenu par faisceautisation n'est autre que le quotient $\mathrm{Pic}(\tilde{X}) \to \mathrm{Pic}(\tilde{X})/\pi^\star \mathrm{Pic}(\mathbb{P}^1) =: \mathrm{Pic}(\tilde{X}/\mathbb{P}^1)$. Comme $\pi\colon \tilde{X} \to \mathbb{P}^1$ admet une section α, la suite exacte

$$0 \longrightarrow \mathrm{Pic}(\mathbb{P}^1) \xrightarrow{\pi^\star} \mathrm{Pic}(\tilde{X}) \longrightarrow \mathrm{Pic}(\tilde{X}/\mathbb{P}^1) \longrightarrow 0$$

est scindée, et il y a un isomorphisme

$$\begin{array}{rcl} \mathrm{Pic}(\mathbb{P}^1) \oplus \mathrm{Pic}(\tilde{X}/\mathbb{P}^1) & \xrightarrow{\sim} & \mathrm{Pic}(\tilde{X}) \\ (D, [D']) & \longmapsto & D' + \pi^\star(D - \alpha^\star D'). \end{array}$$

Enfin, la platitude de π assure [Mil08, I, Th. 4.2] que pour tout $T \to \mathbb{P}^1$ et tout fibré en droites $\mathcal{L}$ sur T, le degré des fibres $\mathcal{L}_{T_s}$, $s \in \mathbb{P}^1$ est indépendant de s ; il est encore le même après un changement de base $T' \to T$. De plus, si $\mathcal{L}$ est obtenu comme tiré en arrière d'un fibré en droites sur $\mathbb{P}^1$ alors $\deg \mathcal{L}_s = 0$ pour tout $s \in \mathbb{P}^1$. Ceci permet de définir un morphisme

$$\deg\colon \mathrm{Pic}_{\tilde{X}/\mathbb{P}^1} \to \mathbb{Z}$$

de faisceaux sur $\mathbb{P}^1$. Le faisceau $\mathrm{R}^i\pi_\star\mu_n$ est le faisceau sur $\mathbb{P}^1$ associé au préfaisceau

$$(T \to \mathbb{P}^1) \mapsto \mathrm{H}^i(T \times_{\mathbb{P}^1} \tilde{X}, \mu_n).$$

Il y a donc un morphisme canonique entre les espaces de sections globales

$$\mathrm{H}^i(\tilde{X}, \mu_n) \to \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^i\pi_\star\mu_n)$$

qui est le morphisme de bord correspondant de la suite spectrale de Leray

$$E_2^{ij} = \mathrm{H}^i(\mathbb{P}^1, \mathrm{R}^j\pi_\star\mu_n) \Longrightarrow \mathrm{H}^{i+j}(\tilde{X}, \mu_n).$$

Ces morphismes de bord sont décrits en général dans [EGAIII$_1$, 0, §12.2.5]. Les cas particuliers $i = 1, 2$ nous intéressent ici. Pour $i = 1$, $\mathrm{R}^1\pi_\star\mu_n$ est le noyau de la multiplication par n sur $\mathrm{R}^1\pi_\star\mathbb{G}_m$. Le morphisme $\mathrm{H}^1(\tilde{X}, \mu_n) \to \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^1\pi_\star\mu_n)$ est simplement le quotient $\mathrm{Pic}(\tilde{X})[n] \to \mathrm{Pic}(\tilde{X}/\mathbb{P}^1)[n]$, qui s'insère dans le diagramme commutatif à lignes exactes :

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Pic}(\tilde{X})[n] \arrow[r] \arrow[d] & \mathrm{Pic}(\tilde{X}) \arrow[r, "n"] \arrow[d] & \mathrm{Pic}(\tilde{X}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & \mathrm{Pic}(\tilde{X}/\mathbb{P}^1)[n] \arrow[r] & \mathrm{Pic}(\tilde{X}/\mathbb{P}^1) \arrow[r, "n"] & \mathrm{Pic}(\tilde{X}/\mathbb{P}^1) \arrow[r] & 0
\end{tikzcd}$$

Pour $i = 2$, le morphisme $\mathrm{H}^2(\tilde{X}, \mu_n) \to \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n)$ s'insère dans le diagramme commutatif :

$$\begin{tikzcd}
\mathrm{Pic}(\tilde{X}) \arrow[r] \arrow[d] & \mathrm{Pic}(\tilde{X}/\mathbb{P}^1) \arrow[r, "\deg"] \arrow[d] & \mathbb{Z} \arrow[d] \\
\mathrm{H}^2(\tilde{X}, \mu_n) \arrow[r] & \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n) \arrow[r, "\sim"] & \Lambda
\end{tikzcd}$$

En particulier, il est possible d'en construire une section : il suffit pour cela d'envoyer $1 \in \Lambda$ sur l'image par $\mathrm{H}^1(\tilde{X}, \mathbb{G}_m) \to \mathrm{H}^2(\tilde{X}, \mu_n)$ d'un diviseur de degré 1. Par exemple, le diviseur E, image de $\mathbb{P}^1$ par la section α choisie au morphisme π, est de degré 1. En effet, par définition du degré, pour n'importe quel point fermé $\bar{s} \in \mathbb{P}^1$,

$$\deg(E) = \deg(E \cap \tilde{X}_{\bar{s}}) = 1.$$

D'autre part, le morphisme

$$\mathrm{H}^i(\mathbb{P}^1, \pi_\star\mu_n) \to \mathrm{H}^i(\tilde{X}, \mu_n)$$

s'obtient de la façon suivante. C'est la composée du morphisme $\mathrm{H}^i(\mathbb{P}^1, \pi_\star\mu_n) \to \mathrm{H}^i(\tilde{X}, \pi^\star\pi_\star\mu_n)$, déduit du morphisme canonique $\mathrm{H}^0(\mathbb{P}^1, -) \to \mathrm{H}^0(\tilde{X}, \pi^\star -)$, avec le morphisme $\mathrm{H}^i(\tilde{X}, \pi^\star\pi_\star\mu_n) \to \mathrm{H}^i(\tilde{X}, \mu_n)$ produit par l'adjonction $\pi^\star \dashv \pi_\star$. Dans notre cas, comme $\pi_\star\mu_n = \mu_n$, tout ceci est bien plus simple : la flèche

$$\mathrm{H}^i(\mathbb{P}^1, \mu_n) \to \mathrm{H}^i(\tilde{X}, \mu_n)$$

est le morphisme $\pi^\star$ obtenu par fonctorialité de H^i. En particulier, pour $i = 1$, c'est le tiré en arrière des diviseurs.

VI.3.2 Calcul des $\mathrm{H}^i(\tilde{X}, \mu_n)$

Rappelons qu'il y a des isomorphismes canoniques $\mathrm{R}^0\pi_\star\mu_n = \mu_n$ et $\mathrm{R}^2\pi_\star\mu_n = \Lambda$.

Théorème 6.3.1. [Mil80, V, Th. 3.22] Notons $\mathcal{F} := \mathrm{R}^1\pi_\star\mu_n$. Les groupes de cohomologie de $\tilde{X}$ à valeur dans μ_n sont les suivants.

$$\begin{array}{lcl}
\mathrm{H}^0(\tilde{X}, \mu_n) & = & \mu_n(k) \\
\mathrm{H}^1(\tilde{X}, \mu_n) & = & \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}) \\
\mathrm{H}^2(\tilde{X}, \mu_n) & = & \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \oplus \mathrm{H}^2(\mathbb{P}^1, \mu_n) \oplus \mathrm{H}^0(\mathbb{P}^1, \Lambda) \\
\mathrm{H}^3(\tilde{X}, \mu_n) & = & \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}) \\
\mathrm{H}^4(\tilde{X}, \mu_n) & = & \mathrm{H}^2(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n) = \mu_n(k)^\vee
\end{array}$$

et $\mathrm{H}^i(\tilde{X}, \mu_n) = 0$ pour $i \geqslant 5$.

Démonstration. La deuxième page de la suite spectrale de Leray

$$E_2^{ij} = \mathrm{H}^i(\mathbb{P}^1, \mathrm{R}^j\pi_\star\mu_n) \Longrightarrow \mathrm{H}^{p+q}(\tilde{X}, \mu_n)$$

s'écrit :

$$\begin{array}{c|ccc}
2 & \Lambda & 0 & \mu_n(k)^\vee \\
1 & \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}) & \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) & \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}) \\
0 & \mu_n(k) & 0 & \Lambda \\
\hline
 & 0 & 1 & 2
\end{array}$$

Notons $M = \ker(\phi\colon \mathrm{H}^2(\tilde{X}, \mu_n) \to \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n))$. La suite exacte de bas degré de cette suite spectrale de Leray s'écrit :

$$0 \longrightarrow \mathrm{H}^1(\tilde{X}, \mu_n) \longrightarrow \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}) \longrightarrow \mathrm{H}^2(\mathbb{P}^1, \mu_n) \xrightarrow{\pi^\star} M \longrightarrow \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \longrightarrow 0.$$

Comme π a une section, $\pi^\star$ a une rétraction, et la flèche $\mathrm{H}^0(\mathbb{P}^1, \mathcal{F}) \to \mathrm{H}^2(\mathbb{P}^1, \mu_n)$ est nulle. Ceci signifie d'une part que $\mathrm{H}^1(\tilde{X}, \mu_n) \to \mathrm{H}^0(\mathbb{P}^1, \mathcal{F})$ est un isomorphisme, et d'autre part qu'il y a une suite exacte scindée

$$0 \longrightarrow \mathrm{H}^2(\mathbb{P}^1, \mu_n) \xrightarrow{\pi^\star} M \longrightarrow \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \longrightarrow 0$$

qui fournit un isomorphisme

$$M \xrightarrow{\sim} \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \oplus \mathrm{H}^2(\mathbb{P}^1, \mu_n).$$

De plus, l'image de $\mathrm{H}^2(\tilde{X}, \mu_n) \xrightarrow{\phi} \mathrm{H}^0(\mathbb{P}^1, \Lambda) = \Lambda$ est $E_3^{02} = \ker(\psi\colon \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n) \to \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}))$. Le conoyau de ψ est $E_3^{21} = \mathrm{H}^3(\tilde{X}, \mu_n)$. Il y a donc une suite exacte :

$$0 \longrightarrow M \longrightarrow \mathrm{H}^2(\tilde{X}, \mu_n) \xrightarrow{\phi} \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n) \xrightarrow{\psi} \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}) \to \mathrm{H}^3(\tilde{X}, \mu_n) \longrightarrow 0.$$

La flèche ϕ a elle aussi une section, décrite dans la remarque VI.3.1. Par conséquent, ψ est nulle. Il en découle d'une part que $\mathrm{H}^2(\mathbb{P}^1, \mathcal{F}) \to \mathrm{H}^3(\tilde{X}, \mu_n)$ est un isomorphisme, et d'autre part qu'il y a un isomorphisme

$$\mathrm{H}^2(\tilde{X}, \mu_n) \xrightarrow{\sim} M \oplus \mathrm{H}^0(\mathbb{P}^1, \mathrm{R}^2\pi_\star\mu_n).$$

Enfin, en degré 4, la suite spectrale a convergé à la deuxième page et $\mathrm{H}^4(\tilde{X}, \mu_n) = \mu_n(k)^\vee$. □

VI.3.3 Cohomologie de l'éclatement

Nous décrivons dans cette section le lien entre la cohomologie de X et celle de $\tilde{X}$. Ces résultats sont bien connus et détaillés dans [SGA7$_2$, XVIII, §4]. Soit Δ l'intersection de X avec l'axe du pinceau, c'est-à-dire le centre de l'éclatement $\tilde{X} \to X$. Considérons le diagramme cartésien :

$$\begin{tikzcd}
\tilde{\Delta} \arrow[r, "\tilde{i}"] \arrow[d, "g"] & \tilde{X} \arrow[d, "f"] \\
\Delta \arrow[r, "i"] & X
\end{tikzcd}$$

Alors $\tilde{\Delta} \to \Delta$ est un fibré projectif, et le cup-produit par la classe de $\mathcal{O}_{\tilde{\Delta}}(1)$ dans $\mathrm{H}^2(\tilde{\Delta}, \mu_n)$ définit pour tout entier naturel i un morphisme surjectif

$$\mathrm{H}^i(\Delta, \Lambda) \to \mathrm{H}^{i+2}(\tilde{\Delta}, \mu_n)$$

de noyau l'image de

$$g^\star \colon \mathrm{H}^i(\Delta, \mu_n) \to \mathrm{H}^i(\tilde{\Delta}, \mu_n).$$

Le morphisme $\mathrm{H}^i(X, \mu_n) \to \mathrm{H}^i(\tilde{X}, \mu_n)$ est injectif, car il admet un inverse à gauche : le morphisme de Gysin

$$f_\star \colon \mathrm{H}^i(\tilde{X}, \mu_n) \to \mathrm{H}^i(X, \mu_n).$$

De plus, pour tout entier naturel i, le morphisme $\tilde{i}^\star \colon \mathrm{H}^i(\tilde{X}, \mu_n) \to \mathrm{H}^i(\tilde{\Delta}, \mu_n)$ induit un isomorphisme

$$\frac{\mathrm{H}^i(\tilde{X}, \mu_n)}{f^\star \mathrm{H}^i(X, \mu_n)} \xrightarrow{\sim} \frac{\mathrm{H}^i(\tilde{\Delta}, \mu_n)}{g^\star \mathrm{H}^i(\Delta, \mu_n)}.$$

Le diagramme commutatif à lignes exactes

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{H}^i(X, \mu_n) \arrow[r, "f^\star"] \arrow[d] & \mathrm{H}^i(\tilde{X}, \mu_n) \arrow[r] \arrow[d, "\tilde{i}^\star"] & \mathrm{H}^i_\Delta(X, \mu_n) \arrow[r] \arrow[d, "\wr"] & 0 \\
0 \arrow[r] & \mathrm{H}^i(\Delta, \mu_n) \arrow[r, "g^\star"] & \mathrm{H}^i(\tilde{\Delta}, \mu_n) \arrow[r, "g_\star"] & \mathrm{H}^{i-2}(\Delta, \Lambda) \arrow[r] & 0
\end{tikzcd}$$

montre alors qu'il y a un isomorphisme :

$$f_\star \oplus \tilde{i}^\star \colon \mathrm{H}^2(\tilde{X}, \mu_n) \xrightarrow{\sim} \mathrm{H}^2(X, \mu_n) \oplus \mathrm{H}^2(\tilde{\Delta}, \mu_n)$$

d'inverse $f^\star \oplus \tilde{i}_\star$. En particulier,

$$\mathrm{H}^2(X, \mu_n) = \ker(\mathrm{H}^2(\tilde{X}, \mu_n) \xrightarrow{\tilde{i}^\star} \mathrm{H}^2(\tilde{\Delta}, \mu_n))$$

et pour tout $i \neq 2$,

$$\mathrm{H}^i(X, \mu_n) = \mathrm{H}^i(\tilde{X}, \mu_n).$$

VI.4 Algorithme et indications sur le calcul de sa complexité

Reprenons les notations des sections précédentes ; en particulier, $\mathcal{F} = \mathrm{R}^1\pi_\star\mu_n$, et $S \subset \mathbb{P}^1$ est le lieu de singularité du pinceau. Les sections précédentes suggèrent l'algorithme suivant pour calculer $\mathrm{H}^1(\tilde{X}, \mu_n)$.

1. Calculer $\mathrm{H}^1(\tilde{X}_{\bar{\eta}}, \mu_n)$ à l'aide de l'algorithme de Huang-Ierardi présenté dans la section IV.3, et en particulier une extension K de $k(t)$ par laquelle se factorise l'action de $\mathrm{Gal}(\bar{\eta}|\eta)$ sur $\mathrm{H}^1(\tilde{X}_{\bar{\eta}}, \mu_n)$. Soit Y la normalisation de $U = \mathbb{P}^1 - S$ dans K. Le faisceau $\mathcal{F}$ est constructible sur $\mathbb{P}^1$, lisse sur U, et $\mathcal{F}|_U$ est trivialisé par $Y \to U$.
2. Calculer les $\mathrm{H}^1(\tilde{X}_{\bar{s}}, \mu_n)$ pour $\bar{s} \in S$ à l'aide de la cohomologie de la normalisée de $\tilde{X}_{\bar{s}}$ et de la suite exacte 2.4.10. Le calcul s'effectue comme dans le cas de la cohomologie à support décrit dans la section V.2.2.
3. Calculer les morphismes de spécialisation $\mathrm{H}^1(\tilde{X}_{\bar{\eta}}, \mu_n) \to \mathrm{H}^1(\tilde{X}_{\bar{s}}, \mu_n)$ décrits au début de la section VI.3. La description par recollement du faisceau $\mathcal{F}$ est maintenant complète.
4. Calculer $\mathrm{R}\Gamma(\mathbb{P}^1, \mathcal{F})$ à l'aide de l'algorithme de la section V.6.1.

5. En déduire les $\mathrm{H}^i(\tilde{X}, \mu_n)$ à l'aide du théorème 6.3.1.

Le calcul précis de la complexité de cet algorithme est encore à effectuer. Voici quelques indications en ce sens. Notons U l'ouvert maximal de lissité de $\mathcal{F}$. Le revêtement minimal $V \to U$ qui le trivialise est de degré $|\mathrm{H}^1(X_{\bar{\eta}}, \mu_n)| = n^{O(2g)}$ où g est le genre de $X_{\bar{\eta}}$. Il est modérément ramifié au-dessus de $S = \mathbb{P}^1 - U$. Les fibres singulières $X_{\bar{s}}$ sont des courbes nodales de genre géométrique $g - 1$. Afin d'étudier précisément la complexité de l'algorithme, il conviendrait de déterminer d'une part le genre géométrique de Y (qui dépend en particulier du cardinal de S et de la ramification à l'infini de $Y \to U$), et d'autre part la complexité des algorithmes calculant la n-torsion de la jacobienne d'une courbe définie sur $\mathbb{F}_q(t)$ sans hypothèse supplémentaire.

CHAPITRE VII

Problèmes ouverts

Pour finir, nous évoquons ici quelques questions restant sans réponse à l'issue de ce travail. Si certaines n'ont simplement pas pu être abordées par manque de temps, d'autres contiennent des difficultés réelles.

Faisceaux constructibles en dimension supérieure

Comme esquissé à la fin du chapitre III, les représentations que nous avons données des faisceaux constructibles sur les courbes s'adaptent immédiatement à des variétés de dimension supérieure. Par contre, notre description des opérations effectuées sur ces faisceaux ne se généralise pas aussi facilement ; en particulier, il faudrait se passer du fait que le complémentaire de l'ouvert de lissité soit zéro-dimensionnel, qui a énormément facilité notre travail.

Cohomologie des faisceaux constructibles sur les surfaces

La question principale laissée en suspens par ce travail est le calcul de la cohomologie d'un faisceau constructible sur une surface lisse. Soit X une surface intègre lisse, munie d'un morphisme propre $\pi\colon X \to \mathbb{P}^1$ admettant une section. Les méthodes du chapitre VI, qui utilisent une section de la fibration pour induire des scindages dans les suites exactes déduites de la suite spectrale de Leray, ne donnent des suites exactes courtes scindées que dans le cas des faisceaux constants. Afin de calculer la cohomologie d'un faisceau constructible $\mathcal{F}$ quelconque sur X, il conviendrait de calculer un complexe de faisceaux constructibles sur $\mathbb{P}^1$ représentant $\mathrm{R}\pi_\star\mathcal{F}$. Une piste serait d'exploiter la forme des complexes de cohomologie $\mathrm{R}\Gamma(X_{\bar{s}}, \mathcal{F})$ des fibres de π calculés dans la section V.3.1.

Cohomologie des faisceaux sur les courbes singulières

Nous avons montré comment calculer la cohomologie d'un faisceau constructible sur une courbe lisse ou nodale. Le calcul de la cohomologie d'une courbe X avec des singularités quelconques serait un prolongement naturel de ce travail. Il y aurait essentiellement deux difficultés à surmonter : la

première est la représentation des faisceaux constructibles sur une telle courbe, et la seconde est le calcul du revêtement $X_2 \to X$ qui trivialise les Λ-torseurs sur X. Nos méthodes devraient s'adapter sans obstacle aux courbes à singularités ordinaires ; pour les autres, la construction de ce revêtement paraît en outre difficile.

Calcul de cup-produits

La description explicite de l'accouplement de Weil pour les courbes lisses sur les corps finis a été réalisée par Bleher et Chinburg (voir section II.4.4.2). D'autre part, nous avons montré comment calculer les cup-produits

$$\mathrm{H}^1 \times \mathrm{H}^1 \xrightarrow{\cup} \mathrm{H}^2$$

dans la cohomologie des faisceaux lisses sur les courbes projectives lisses ou nodales sur les corps finis ou algébriquement clos. Il reste à étudier ce calcul dans le cadre plus large des faisceaux constructibles. En particulier, étant donné un faisceau lisse $\mathcal{F}$ sur ouvert U d'une courbe projective lisse X, il serait intéressant d'obtenir un calcul explicite de la dualité de Poincaré

$$\mathrm{H}^1_c(U, \mathcal{F}) \times \mathrm{H}^1(U, \mathcal{F}^\vee(1)) \xrightarrow{\cup} \mathrm{H}^2(X, \mu_n)$$

à partir des complexes représentant $\mathrm{R}\Gamma(X, j_!\mathcal{F})$ et $\mathrm{R}\Gamma(U, \mathcal{F}^\vee(1))$ déterminés dans le chapitre V. Notre méthode utilisant la cohomologie des groupes ne peut pas s'y appliquer immédiatement, puisque $j_!\mathcal{F}$ n'est pas localement constant. La difficulté de ce problème est encore difficile à évaluer.

Calcul de la n-torsion de la jacobienne sur les corps infinis

Le seul algorithme dont nous disposons actuellement pour déterminer la n-torsion de la jacobienne d'une courbe projective lisse sur un corps infini est celui de Huang et Ierardi. Un premier travail serait d'étudier sa complexité dans le cas des corps de fonctions, ce qui paraît fastidieux mais tout à fait faisable. S'il paraît difficile de mettre au point un algorithme plus efficace pour un corps quelconque, il serait tout de même intéressant de traiter le cas d'un corps de base fixé, par exemple $\mathbb{Q}$ ou $\mathbb{F}_q(t)$. Le cas de $\mathbb{F}_q(t)$ revêt une importance particulière, puisqu'il est le cas de base indispensable pour le calcul de la cohomologie des surfaces sur $\mathbb{F}_q$, et donc pour le comptage de points sur ces surfaces.

Six opérations

L'objectif de calculer les 6 opérations dans $D^b_c(X, \Lambda)$, où X est une courbe intègre lisse sur k, paraît pour l'instant hors de portée. Toutefois, certaines opérations semblent plus simples à calculer. Par exemple, pour un morphisme f entre courbes lisses, les foncteurs $\mathrm{R}^i f_\star$ se déterminent aisément comme décrit dans la section III.4.5, et le calcul explicite du foncteur $\mathrm{R}f_\star$ paraît accessible. Le calcul de $\mathrm{R}f_!$ devrait s'en déduire. Nous n'avons pas eu le temps de nous intéresser au calcul des foncteurs $f^!$, $\mathrm{R}\underline{\mathrm{Hom}}$ et $\otimes^L$, qui paraît difficile.

ANNEXE A

Corps calculables

A.1 Corps calculables et complexité

Calculabilité et classes de complexité Par fonction calculable, nous entendons toujours une fonction récursive au sens de [Odi89a, Def. I.1.7], c'est-à-dire une fonction calculable par une machine de Turing [Odi89a, Th. I.4.3]. Le mot algorithme désignera une machine de Turing qui s'arrête pour toute entrée.
La classe des fonctions primitivement récursives [Odi89a, Def. I.1.6] est la plus petite classe contenant la fonction nulle, la fonction $n \mapsto n+1$, les projections $\mathbb{N}^r \to \mathbb{N}$, et stable par composition et récursion. De façon informelle, les algorithmes primitivement récursifs sont ceux qui s'écrivent avec une successions de boucles "for" : ils ne font pas usage de recherches non bornées. La classe des fonctions élémentaires [Odi89b, Def. VIII.7.1] est la plus petite classe contenant la fonction nulle, la fonction $n \mapsto n+1$, la soustraction $(x, y) \mapsto \max(0, x-y)$ et stable par composition, somme bornée et produit borné. Toute fonction élémentaire est primitivement récursive. Une fonction est élémentaire (resp. primitivement récursive) si et seulement si elle est calculable en un nombre d'opérations donné par une fonction élémentaire (resp. primitivement récursive) [Odi89b, Th. VIII.7.6, VIII.8.8]. Intuitivement, la différence principale entre ces deux classes est la suivante : les fonctions exponentielles à nombre d'étages borné indépendamment des entrées sont élémentaires, mais la tétration $(n, x) \mapsto x \uparrow\uparrow n$ ne l'est pas.

Corps calculables Nous supposons que tous les corps rencontrés sont calculables et munis d'un algorithme de factorisation. Cela signifie que l'on dispose d'une représentation des éléments de k, d'algorithmes calculant la somme, l'opposé, le produit et l'inverse d'éléments dans k, ainsi que d'un algorithme calculant, étant donné $f \in k[t]$, la décomposition de f en produit de facteurs irréductibles. Si k est calculable et muni d'un algorithme de factorisation, il en est de même de tout corps de fonctions rationnelles à coefficients dans k et de toute extension finie séparable de k [FJ08, Lem. 19.2.2]. Si k est calculable de caractéristique $p > 0$ et est muni d'une p-base explicite (c'est-à-dire d'une k^p-base de k) et d'un algorithme de factorisation, il en est de même pour toute extension finie de k [MO15, Prop. 12.5]. Comme les corps $\mathbb{Q}$ et $\mathbb{F}_p$ vérifient ces hypothèses (voir section A.2.1 pour la factorisation), tous les corps globaux sont calculables et disposent d'un algorithme de factorisation.

Complexité et opérations élémentaires Nous indiquerons les complexités en termes soit d'opérations binaires, soit d'opérations dans $\mathbb{Z}$ en mentionnant la taille des entiers utilisés, soit d'opérations dans un anneau fixé. L'addition de deux entiers de longueur binaire n nécessite $O(n)$ opérations binaires. L'algorithme de multiplication de Harvey et van Der Hoeven, basé sur la transformée de Fourier discrète, multiplie deux entiers de longueur binaire n en $O(n \log n)$ opérations binaires [Hv21, Th. 1.1]. Une addition, multiplication ou inversion d'un élément de $\mathbb{Z}/d\mathbb{Z}$ requièrent $O(\log^2 d)$ opérations dans $\mathbb{Z}$. Une telle opération dans un quotient $k[t]/(f)$ nécessite $O(\log^2 \deg f)$ opérations dans le corps k. Étant donné un entier m et un élément x d'un anneau A, le calcul de x^m nécessite $O(\log m)$ multiplications dans A.

Algorithmes probabilistes Nous avons parfois recours à des algorithmes probabilistes. Il en existe deux grandes familles :

1. Les algorithmes de type Las Vegas renvoient toujours une réponse correcte, quitte à effectuer si nécessaire un grand nombre de tirages aléatoires ; nous indiquerons toujours leur complexité moyenne.
2. Les algorithmes de type Monte-Carlo font un nombre fixe de tirages aléatoires, et renvoient une réponse qui est correcte avec une certaine probabilité ; nous indiquerons toujours leur complexité dans le pire cas ainsi que la probabilité que la valeur renvoyée soit correcte.

A.1.1 Algèbre linéaire

A.1.1.1 Sur un corps

Définition A.1.1. La constante de l'algèbre linéaire, notée ω, est la borne inférieure de l'ensemble des réels τ tels que pour tout anneau A, il existe un algorithme de multiplication de deux matrices de $\mathrm{Mat}_{n\times n}(A)$ nécessitant $O(n^\tau)$ opérations dans A.

Soit k un corps. Soit $M \in \mathrm{Mat}_{n\times n}(k)$. Les opérations suivantes s'effectuent encore avec la même complexité que la multiplication dans $M_{n\times n}(k)$:

- calculer le déterminant de M [BCS97, Th. 16.7] ;
- calculer l'inverse de M si elle est inversible [BCS97, Prop. 16.6] ;
- échelonner M [BCS97, Prop. 16.10].

Il est clair que $\omega \geqslant 2$, puisque la matrice à calculer a n^2 coefficients. D'autre part, l'algorithme de multiplication naïf nécessite $O(n^3)$ opérations dans k ; nous utilisons cette majoration dans le manuscrit. Les algorithmes les plus efficaces sont des raffinements de l'algorithme de Coppersmith-Winograd présenté dans [CW90], et il est connu que $\omega \in [2, 2.3729[$ [VW12]. Les mêmes bornes (pour la multiplication et l'échelonnement) s'appliquent à des matrices rectangulaires $M \in \mathrm{Mat}_{a\times b}(k)$ en prenant $n = \max(a, b)$: il suffit d'ajouter des lignes/colonnes nulles pour se ramener au cas d'une matrice carrée.

Lemme A.1.2. [Zis21, §4.3.1, 4.3.2] Soient k un corps et $k(t)$ le corps des fonctions rationnelles sur k. Soit $M \in \mathrm{Mat}_{n\times n}(k(x))$ une matrice dont les entrées sont des quotients de deux polynômes de degrés au plus d. Alors le calcul de toutes les opérations citées ci-dessus se fait en $\tilde{O}(n^4 d)$ opérations dans k, où la notation $\tilde{O}(f(n))$ signifie $O(f(n) \log^\beta f(n))$ pour un $\beta > 0$.

A.1.1.2 Sur $\mathbb{Z}/d\mathbb{Z}$

Soit Λ un anneau. La complexité $O(n^\omega)$ de la multiplication des matrices est la même que dans le cas des corps. Il n'est cependant pas évident que cette complexité soit encore celle du calcul de noyaux

de morphismes de A-modules libres ou de la résolution de systèmes linéaires sur A. Dans le cas où tous les idéaux de Λ sont principaux, la forme normale de Smith permet de réaliser cette opération ; il existe des algorithmes pour la calculer dans le cas où $\Lambda = \mathbb{Z}$ [Sto96, §4] ou $\mathbb{Z}/d\mathbb{Z}$ [Sto96, §3]. Cependant, ces algorithmes calculent seulement la forme normale N d'une matrice M, et le calcul des matrices de transformation P, Q telles que $M = PNQ$ est plus coûteux. Lorsque $\Lambda = \mathbb{Z}/d\mathbb{Z}$, la forme normale de Howell se prête particulièrement bien à la tâche. À chaque matrice $M \in \mathrm{Mat}_{n\times m}(\Lambda)$, on peut associer une unique matrice $H(M) \in \mathrm{Mat}_{n\times m}(\Lambda)$ échelonnée vérifiant certaines conditions décrites dans [SM98, §3] et une unique matrice $P \in \mathrm{GL}_n(\Lambda)$ telle que $PM = H(M)$. En particulier, $H(M) = H(N)$ si et seulement si $\ker(M) = \ker(N)$.

Proposition A.1.3. [SM98, Th. 4] Soient n, m, d des entiers naturels non nuls. Notons $\Lambda = \mathbb{Z}/d\mathbb{Z}$. Il existe un algorithme qui, étant donné $M \in \mathrm{Mat}_{n\times m}(\Lambda)$, calcule sa forme normale de Howell $H(M)$ et une matrice $P \in \mathrm{GL}_n(\Lambda)$ telle que $PM = H(M)$ en $O(\max(n, m)^\omega)$ opérations dans Λ.

Cet algorithme permet en particulier de calculer le noyau d'une matrice, une famille génératrice de la réunion ou de l'intersection de sous-modules [SM98, §5, Tasks 1-3] avec cette complexité. Un Λ-module engendré par des éléments $v_1, \ldots, v_n$ vérifiant les relations linéaires $a_1, \ldots, a_m$ sera décrit par la matrice $M \in \mathrm{Mat}_{n\times m}(\Lambda)$ dont il est le conoyau. La description des morphismes et le calcul des noyaux et conoyaux se fait exactement comme dans [MO15, 13.2]. Remarquons également que comme tout idéal de Λ est principal, un sous-module de Λ^n est toujours engendré par une famille d'au plus n éléments qui se détermine simplement, ce qui fait que le nombre de relations entre les générateurs d'un Λ-module n'entre pas en compte dans le calcul de la complexité.

A.2 Polynômes

A.2.1 Factorisation des polynômes univariés

A.2.1.1 Sur un corps fini

Proposition A.2.1. [Sho90, Th. 1] Il existe un algorithme déterministe qui, étant donné un nombre premier p et un polynôme $f \in \mathbb{F}_p[t]$ de degré d, calcule les facteurs irréductibles de f dans $\mathbb{F}_p[t]$ en $O(d^{2+\epsilon}\sqrt{p}\log^2 p)$ opérations dans $\mathbb{F}_p$.

Ceci implique encore que la factorisation d'un polynôme dans $\mathbb{F}_{p^\alpha}[t]$ se calcule en un nombre d'opérations polynomial en p, α et d [vG13, 14.40]. Le recours aux algorithmes probabilistes permet d'obtenir une meilleure complexité.

Proposition A.2.2. [vG13, Th. 14.32] Il existe un algorithme probabiliste (Las Vegas) qui, étant donné une puissance $q = p^\alpha$ d'un nombre premier et un polynôme $f \in \mathbb{F}_q[t]$ de degré d, calcule les facteurs irréductibles de f dans $\mathbb{F}_q[t]$ en $\tilde{O}(d^\omega \alpha^2 \log^2 p)$ opérations dans $\mathbb{F}_q$, avec probabilité d'échec inférieure à $\frac{1}{2}$.

Remarque A.2.3. Afin de calculer la factorisation dans $\overline{\mathbb{F}_p}[t]$ d'un polynôme $f \in \mathbb{F}_{p^\alpha}[t]$ de degré d, il suffit de le factoriser dans une extension dont le degré est le ppcm des degrés des facteurs irréductibles de f, qui est majoré par la fonction de Landau $\lambda(d) \leqslant \exp(d/e)$, où $e = \exp(1)$; pour des majorations plus précises de la fonction de Landau, voir [Nic13]. La complexité de la factorisation est alors encore polynomiale en $p, \alpha, \exp(d/e)$ pour l'algorithme déterministe, et $O(d^{\omega+2} exp(2\alpha/e)\log^2 p)$ pour l'algorithme probabiliste.

A.2.1.2 Sur un corps de nombres

Par le lemme de Gauss, la factorisation d'un polynôme de $\mathbb{Q}[t]$ se ramène à celle d'un polynôme dans $\mathbb{Z}[t]$, que l'on peut supposer primitif après avoir factorisé ses coefficients dans $\mathbb{Z}$, opération dont

la complexité est sous-exponentielle en la valeur absolue des coefficients. Soit donc $f \in \mathbb{Z}[t]$ de degré d. Notons $\|f\|_\infty$ la plus grande des valeurs absolues des coefficients de f. L'algorithme "LLL" de Lenstra, Lenstra et Lovász calcule les facteurs premiers de f dans $\mathbb{Z}[t]$ en $O(d^6 + d^5 \log \|f\|_\infty)$ opérations sur des entiers de longueur binaire $O(d^3 + d^2 \log \|f\|_\infty)$ [LLL82, Th. 3.6].
Cet algorithme a été adapté par A. Lenstra au cas des corps de nombres. Soit $K = \mathbb{Q}[\alpha]$ un corps de nombres ; notons $n = [K : Q]$. Soit $f \in K[t]$ un polynôme de degré d. Soit D un entier tel que $f \in \frac{1}{D}\mathbb{Z}[\alpha][t]$. On peut écrire $f = \sum_{i=0}^{n-1} \sum_{j=0}^{d} a_{ij}\alpha^i x^j$. Notons alors $\|f\|_2$ la norme euclidienne du vecteur $(|a_{ij}|)_{i,j}$ et $\|f\|_\infty = \max_{i,j} |a_{ij}|$.

Théorème A.2.4. [Len83, Th. 4.5] Avec ces notations, il existe un algorithme déterministe qui calcule la factorisation de f dans $\mathbb{Q}(\alpha)[t]$ en $O(n^6 d^6 + n^5 d^6 \log(d\|f\|_2) + n^5 d^5 \log(d\|f\|_\infty))$ opérations arithmétiques sur des entiers de longueur binaire $O(n^3 d^2 + n^2 d^3 \log(d\|g\|_2) + n^2 d^2 \log(d\|f\|_\infty))$.

A.2.2 Calcul de racines n-ièmes

Dans les corps finis, le calcul d'une racine n-ième d'un élément par la méthode d'Adleman-Manders-Miller est bien plus rapide que la factorisation des polynômes en général.

Proposition A.2.5. [CSF12, §6] Soit q une puissance d'un nombre premier. Soit n un entier naturel non nul. Il existe un algorithme déterministe qui, étant donné $x \in \mathbb{F}_q$, détermine si x est une puissance n-ième dans $\mathbb{F}_q$ et, le cas échéant, calcule une racine n-ième de x en $O(\log^4 q + n \log^3 q)$ opérations dans $\mathbb{F}_q$.

A.2.3 Factorisation des polynômes multivariés

A.2.3.1 En général

Soit k un corps calculable disposant d'un algorithme de factorisation des polynômes. Alors il existe un algorithme de factorisation des éléments de $k[x_1, \ldots, x_m]$, basé sur l'observation suivante [FJ08, §11.3]. L'application

$$\begin{array}{ccc} k[x_1, \ldots, x_m] & \longrightarrow & k[t] \\ \sum a_i x_1^{i_1} \cdots x_m^{i_m} & \longmapsto & \sum a_i t^{i_1 + i_2 d + i_3 d^2 + \cdots + i_m d^{m-1}} \end{array}$$

définit, pour chaque entier d, une bijection κ_d de l'ensemble des polynômes de $k[x_1, \ldots, x_m]$ de degré $< d$ vers l'ensemble des polynômes de $k[t]$ de degré $< d^m$, qui vérifie $\kappa_d(fg) = \kappa_d(f)\kappa_d(g)$ dès que $\deg(fg) < d$. Son inverse se calcule explicitement par un algorithme d'écriture des entiers en base d. Un polynôme $f \in k[x_1, \ldots, x_m]$ de degré $< d$ est irréductible si et seulement si $\kappa_d(f)$ l'est. Afin de déterminer un facteur d'un polynôme f de degré $< d$, il suffit donc de calculer les facteurs irréductibles $g_1, \ldots, g_s$ de $\kappa_d(f)$. Les facteurs irréductibles stricts de f (s'il y en a) se trouvent parmi les images réciproques par κ_d des facteurs de $\kappa_d(f)$, c'est-à-dire parmi les polynômes de la forme $\kappa_d^{-1}(g_{i_1} \cdots g_{i_s})$. Il ne reste plus qu'à vérifier par division euclidienne si ces éléments divisent f. En particulier, si l'algorithme de factorisation dans $k[t]$ a une complexité élémentaire en le degré du polynôme et la taille de la représentation de ses coefficients, il en est de même de l'algorithme de factorisation dans $k[x_1, \ldots, x_n]$.

A.2.3.2 Sur les corps finis

En se basant sur l'algorithme LLL, A.K. Lenstra a également donné un algorithme de factorisation des polynômes en plusieurs variables sur les corps finis. La version qui nous est utile concerne deux variables.

Théorème A.2.6. [Len85, Th. 2.18] Il existe un algorithme déterministe qui, étant donné une puissance $q = p^m$ d'un nombre premier p et un polynôme $f \in \mathbb{F}_q[x, y]$, renvoie les facteurs irréductibles de f dans $\mathbb{F}_q[x, y]$ en $O(\deg_x(f)^6 \deg_y(f)^2 + (\deg_x(f)^3 + \deg_y(f)^3)pm)$ opérations dans $\mathbb{F}_q$.

De même que dans le cas univarié, il existe un algorithme probabiliste de complexité polynomiale pour factoriser des polynômes en deux variables sur un corps fini.

Théorème A.2.7. [Wan90, Cor. 4.2] Il existe un algorithme probabiliste Las Vegas qui, étant donné une puissance q d'un nombre premier et un polynôme $f \in \mathbb{F}_q[x, y]$ de degré total $d \leqslant \sqrt{q}$, calcule les facteurs irréductibles de f dans $\mathbb{F}_q[x, y]$ en $O(d^{4.89} \log^2 d \log q)$ opérations, avec une probabilité d'échec inférieure à $\frac{1}{\sqrt{\pi \log d}}$.

Remarquons que cet algorithme nécessite un corps fini assez grand par rapport au degré du polynôme. Lorsque $d^2 \geqslant q$ avec les notations du théorème, il faut construire une extension $\mathbb{F}_Q$ de $\mathbb{F}_q$ de degré supérieur à $2 \log_q d$, factoriser f dans $\mathbb{F}_Q$ puis multiplier entre eux les facteurs conjugués sous $\mathrm{Aut}(\mathbb{F}_Q|\mathbb{F}_q)$. Comme nous le verrons dans la section A.3.1, la construction de cette extension $\mathbb{F}_Q/\mathbb{F}_q$ n'est pas plus coûteuse que la factorisation du polynôme sur $\mathbb{F}_q$.

Remarque A.2.8. Les algorithmes précédents permettent également de factoriser des polynômes en une variable sur $\mathbb{F}_q(t)$. Soit $f \in \mathbb{F}_q(t)[x]$. Écrivons $f = \sum_i R_i(t)x^i$, où $R_i = \frac{P_i}{Q_i} \in \mathbb{F}_q(t)$. Notons $d_x = \deg_x f$, et $d_t = \max_i\{\deg_t P_i, \deg_t Q_i\}$. Notons encore $Q = \mathrm{ppcm}_i\, Q_i$; il est de degré inférieur à $d_x d_t$. Factoriser f dans $\mathbb{F}_q(t)[x]$ revient à factoriser $Q(t)f \in \mathbb{F}_q[t, x]$. C'est un polynôme de degré total inférieur à $d_t d_x^2$. Le polynôme f peut donc être factorisé par un algorithme probabiliste en $O((d_t d_x^2)^{4.89} \log^2(d_t d_x^2) \log q)$ opérations.

A.2.3.3 Sur les corps de nombres

Soit $\mathbb{Q}(\alpha) = \mathbb{Q}[t]/(F)$ une extension de $\mathbb{Q}$ de degré d. Soit $f \in \mathbb{Q}(\alpha)[x_1, \ldots, x_r]$. Soit D un entier tel que $f \in \frac{1}{D}\mathbb{Z}[\alpha][x_1, \ldots, x_r]$. Notons $n = \max(2, \min \deg_{x_i} f)$ et $N = \prod_{i=1}^{r}(1 + \deg_{x_i} f)$. Les polynômes f et F sont identifiés aux vecteurs complexes de leurs coefficients.

Théorème A.2.9. [Len84, Th. 3.26] Avec ces notations, il existe un algorithme déterministe qui calcule la décomposition de f en produit de facteurs irréductibles dans $\mathbb{Q}(\alpha)[x_1, \ldots, x_r]$ en

$$O(n^{r-1}(dn)^5(dn + \log(d\|f\|_\infty + d\log(d\|F\|_2))$$

opérations arithmétiques sur des entiers de longueur binaire

$$O(n^{r-1}(dn)^2(dn + \log(d\|f\|_\infty + d\log(d\|F\|_2)).$$

A.3 Extensions de corps

Une extension finie L d'un corps calculable K est représentée concrètement par une K-base $B = (b_1, \ldots, b_n)$ de L et la donnée, pour tous i, j, de la décomposition de $b_i b_j$ dans la base B. Le calcul d'un produit dans L nécessite donc n^ω opérations dans K, celui d'une somme n opérations dans k. Le polynôme minimal d'un élément $x \in L$ se détermine alors en calculant les puissances $1, x, x^2$... de x, et en vérifiant à chaque étape si x^i appartient au sous-espace vectoriel de L engendré par $1, x, \ldots, x^{i-1}$. Ce calcul nécessite $O(n^{3+\omega})$ opérations dans K.

A.3.1 Calcul de polynômes irréductibles sur les corps finis

Soit p un nombre premier. Soit d un entier naturel non nul. La construction d'une extension de degré d de $\mathbb{F}_p$ nécessite le calcul d'un polynôme irréductible de $\mathbb{F}_p[t]$ de degré d. De même que pour la factorisation, une complexité polynomiale en $\log p$ n'est pour l'instant garantie que par des algorithmes probabilistes.

Proposition A.3.1. [Sho88, Th. 3.2] Il existe un algorithme déterministe qui, étant donné un nombre premier p et un entier $d > 0$, construit un polynôme irréductible dans $\mathbb{F}_p[t]$ de degré d en

$$O(\sqrt{p}\log^3(p)d^{3+\epsilon} + \log^2(p)d^{4+\epsilon})$$

opérations dans $\mathbb{F}_p$ pour tout $\epsilon > 0$.

Proposition A.3.2. [Sho94, Th. 5.1] Il existe un algorithme probabiliste (Las Vegas) qui, étant donné une puissance q d'un nombre premier et un entier $d > 0$, construit un polynôme irréductible dans $\mathbb{F}_q[t]$ de degré d en $O((d^2 \log d + d \log q) \log d \log\log d)$ opérations dans $\mathbb{F}_q$ en moyenne.

A.3.2 Extensions normales, extensions séparables

A.3.2.1 Tester si une extension est normale ou séparable

Soit L/K une extension de corps de degré n. Soient $x_1, \ldots, x_d$ des générateurs de L comme K-algèbre, et $f_1, \ldots, f_d \in K[t]$ leurs polynômes minimaux. La séparabilité de L/K équivaut alors à celle des f_i, qui se teste en calculant $\mathrm{pgcd}(f_i, f_i')$. La normalité de L/K se teste en factorisant les polynômes f_i dans $L[t]$, et en vérifiant qu'ils y ont $\deg(f_i)$ racines avec multiplicité. La complexité de tester la séparabilité de L/K est donc celle de la factorisation dans L de $d < n$ polynômes de $K[t]$ de degré au plus n.

A.3.2.2 Calcul d'un élément primitif

Soit K un corps infini. Considérons une extension finie séparable $L = K(a, b)$ de degré d de K. Alors les éléments $\lambda \in K$ tels que $a + \lambda b$ ne soit pas un générateur de L sont les racines d'un polynôme de degré $d(d-1)$ [Lan02, V, Th. 4.6]. Afin de déterminer un élément primitif de L, il suffit donc d'énumérer au plus $d(d-1)+1$ éléments $\lambda \in K$. Pour chacun de ces éléments, le polynôme minimal de $a + \lambda b$ sur k se détermine en calculant ses puissances successives $(a + \lambda b)^i$ et en vérifiant par des méthodes d'algèbre linéaire si $(1, a+\lambda b, \ldots, (a+\lambda b)^{d-1})$ est une base de L/K. Le nombre d'opérations à effectuer dans K est donc polynomial en d.

Le cas général d'une extension $L = K(a_1, \ldots, a_s)$ s'en déduit par récurrence sur le nombre de variables : $K(a_1, \ldots, a_s) = K(a_1, \ldots, a_{s-2})(a_{s-1}, a_s)$. Le nombre d'opérations à effectuer dans K est alors polynomial en d^s, puisqu'une opération dans $k(a_1, \ldots, a_{s-2})$ correspond à $O(d^{s-2})$ opérations dans K.

Le raisonnement suivant, adapté de [YNT89, §5], permet de trouver un s-uplet $(\lambda_1, \ldots, \lambda_s)$ tel que $\lambda_1 a_1 + \cdots + \lambda_s a_s$ soit un élément primitif de L/K dans un ensemble défini à l'avance de taille $(s-1)[L : K]$. Soit A un anneau principal infini de corps des fractions K. Soit $L = K(a_1, \ldots, a_s)$ une extension finie séparable de degré N. Soit S un sous-ensemble de A^s dont toutes les familles de s éléments sont linéairement indépendantes. Si $|S| > (s-1)(N-1)$ alors il contient un s-uplet λ convenable [YNT89, Th. 4.5]. En particulier, un tel ensemble peut être construit sous la forme $S = \{(1, \lambda, \ldots, \lambda^{s-1}) \mid \lambda \in B\}$, où B est une partie de A de cardinal au moins $(s-1)(N-1)$. Pour $A = k[t]$, il suffit de prendre suffisamment d'éléments $\alpha \in k$ et de considérer les $(1, (t-\alpha), \ldots, (t-\alpha)^{s-1})$.

A.3.2.3 Groupe de Galois

Soit L/K une extension galoisienne de corps de degré n. Supposons avoir déjà calculé un élément primitif x_1 de L/K, ainsi que son polynôme minimal $f \in K[t]$, et les racines $x_1, x_2, \ldots, x_n$ de f dans L. Les éléments de $\mathrm{Gal}(L|K)$ sont alors déterminés par l'image de x_1, qui est l'un des autres x_i. La complexité du calcul de $\mathrm{Gal}(L|K)$ est donc dominée par celle de la factorisation dans L d'un polynôme de degré n à coefficients dans K.

A.3.3 Extensions radicielles et clôture parfaite

Soit k un corps de caractéristique p. Il sera souvent utile d'effectuer des calculs dans la clôture parfaite k^{pf} de k. Le principe systématiquement adopté est le suivant, proposé dans [Ste05, §2.3]. Il consiste à simuler une extension $k^{p^{-r}}$ assez grande pour effectuer les calculs désirés, en élevant à la puissance p^r tous les éléments de k rencontrés. L'isomorphisme $k \to k^{p^r}$ permet ainsi de remplacer k par k^{p^r}, et $k^{p^{-r}}$ par k. L'élévation d'un élément de k à la puissance p^r par exponentiation rapide nécessite $O(r \log p)$ opérations dans k.

ANNEXE B

Schémas de type fini sur un corps

B.1 Schémas et morphismes

B.1.1 Représentation des schémas et des morphismes

Soit k un corps. La description explicite des schémas de type fini sur k telle que présentée ci-dessous est celle de [MO15, §16]. Dans le cas particulier des courbes projectives, d'autres descriptions plus adaptées seront données dans la section C.1.

Schémas affines La donnée de polynômes $f_1, \ldots, f_r \in k[x_1, \ldots, x_m]$ définit le schéma $X = \operatorname{Spec} A$ où $A = k[x_1, \ldots, x_m]/(f_1, \ldots, f_r)$. Un ouvert U de X est défini par des polynômes $g_1, \ldots, g_s$ tels que $U = \bigcup_i D(g_i)$. Soit $X' = \operatorname{Spec} k[x'_1, \ldots, x'_p]/(f'_1, \ldots, f'_t)$ un autre schéma affine. Un morphisme $X \to X'$ est défini par ses fonctions coordonnées $\phi_1, \ldots, \phi_p \in k[x_1, \ldots, x_m]$. Étant donné un schéma affine X'' et des morphismes $\psi\colon X \to X''$ et $\psi'\colon X' \to X''$, le produit fibré $X \times_{X''} X'$ est défini par la k-algèbre $k[x_1, \ldots, x_m, x'_1, \ldots, x'_p]/(f_i, f'_j, \psi_\alpha - \psi'_\alpha)$.

Il est possible de détecter si le schéma affine X est vide : c'est le cas si et seulement s'il existe des polynômes $a_1, \ldots, a_r$ de degré inférieur à une constante (que l'on sait calculer) dépendant de m, s et des degrés des f_i tels que

$$a_1 f_1 + \cdots + a_r f_r = 1.$$

La résolution de cette équation se ramène à elle d'un système linéaire en les coefficients des a_i.

Schémas de type fini sur k Par défaut, un schéma de type fini sur k est représenté comme recollement de schémas affines. Reprenons les schémas X, U, X' ci-dessus. Soit $U' = \bigsqcup_i D(g'_i)$ un ouvert de X'. Un morphisme $U \to U'$ est défini par des morphismes

$$D(g_i) = \operatorname{Spec} k[x_1, \ldots, x_m, x]/(f_1, \ldots, f_r, xg_i - 1) \to X'$$

qui se factorisent par U' et coïncident sur $D(g_i) \cap D(g_j) = D(g_i g_j)$. Le fait qu'ils se factorisent par U' se teste en calculant, pour chaque indice i, le schéma $Z(g'_i) \times_{X'} X$, et en vérifiant qu'il est vide.

B.1.2 Recouvrement par des voisinages de points

Proposition B.1.1. Soit $X \subset \mathbb{A}_k^n$ un schéma de type fini sur k de dimension d. Supposons que l'on dispose d'un algorithme primitivement récursif calculant, pour un point $x \in X$, un voisinage de Zariski de x dans X vérifiant une certaine propriété (P). Alors il existe un algorithme primitivement récursif recouvrant X par un nombre fini d'ouverts $U_1, \ldots, U_r$ vérifiant (P).

Démonstration. Quitte à appliquer la procédure ci-après à chacune de ses composantes irréductibles (voir section B.2 pour leur calcul), nous pouvons supposer X irréductible. Commençons par choisir un point $x \in X$ et de lui appliquer l'algorithme pour obtenir un premier ouvert $U^{(1)}$, dont le complémentaire F_1 est de dimension $\leqslant d-1$. Le nombre r de composantes connexes de F_1 est borné en fonction du degré des équations qui le définissent. L'exécution de l'algorithme pour un point de chacune de ces composantes connexes construit des ouverts $U_1^{(2)}, \ldots, U_r^{(2)}$ de X, et ainsi de suite. Le complémentaire de la réunion des $U_i^{(j)}$, pour $1 \leqslant j \leqslant r$, est de dimension au plus $d-r$, et son nombre de composantes connexes est borné par le degré de ses équations, qui ont été explicitement calculées. Le nombre de points à considérer à l'étape $j = r+1$ est donc connu. Il y a au plus d étapes à effectuer. □

B.2 Bases de Gröbner et applications

Soit k un corps. Fixons un ordre monomial sur $R := k[x_1, \ldots, x_n]$, c'est-à-dire un bon ordre sur les monômes de R compatible à la multiplication [DK02, Def. 1.1.1]. Soit I un idéal de R. Une famille $(f_1, \ldots, f_r)$ d'éléments de I est appelée base de Gröbner si les monômes dominants des f_i engendrent l'idéal de R engendré par les monômes dominants de tous les éléments de I. Dans ce cas, l'algorithme de division multivariée permet de décider de l'appartenance à I : un élément $f \in R$ appartient à I si et seulement si le reste de la division de f par $(f_1, \ldots, f_r)$ est nul. Une base de Gröbner $(f_1, \ldots, f_r)$ de I est dite réduite si les f_i sont unitaires et si aucun monôme d'un f_i n'appartient à l'idéal engendré par les monômes dominants des $f_j \neq i$. Tout idéal admet une unique base de Gröbner réduite. Si l'idéal I est défini par des générateurs $g_1, \ldots, g_s$ de degré maximal d, le degré des éléments de la base de Gröbner réduite de I est $O(d^{2^n})$ [Dub90, Th. 8.2].

Proposition B.2.1. [BFS15, Prop. 1] Avec ces notations, il existe un algorithme calculant une base de Gröbner réduite de I en

$$O\left(\frac{s}{n!} 2^{n\omega} d^{(1+n\omega)2^n}\right)$$

opérations dans k.

En particulier, les bases de Gröbner permettent de résoudre des systèmes par élimination. Plus précisément, pour un ordre adapté à l'élimination des variables $x_1, \ldots, x_{j-1}$, si G est une base de Gröbner de l'idéal I alors $G \cap k[x_j, \ldots, x_n]$ est une base de Gröbner de $I \cap k[x_j, \ldots, x_n]$. Un excellent résumé des applications principales des bases de Gröbner se trouve dans [DK02, Ch. 1] ; une référence très détaillée est [BW93]. Supposons que le corps k est calculable, muni d'une p-base explicite et dispose d'un algorithme de factorisation des polynômes de complexité élémentaire en le degré du polynôme et la taille de la représentation informatique de ses coefficients. Il existe alors des algorithmes de complexité élémentaire en n, d, s qui utilisent les bases de Gröbner pour calculer :

1. le noyau d'un morphisme de k-algèbres de type fini ;
2. la fonction de Hilbert de I [BS92, Alg. 2.6] ;
3. une normalisation de Noether de I [Dic+91, Alg. 1.13] ;
4. le radical de I [BW93, Th. 8.99] ;
5. la décomposition primaire de I [BW93, Th. 8.101], [Ste05, Th. 5.1] ;

6. la normalisation de R/I [MO15, §15.5].

Le calcul de la décomposition primaire se ramène au cas zéro-dimensionnel par récurrence, et nécessite la factorisation de polynômes sur des corps de fractions rationnelles sur k. La normalisation d'une k-algèbre A de type fini est calculée de la façon suivante. Un anneau est normal si et seulement s'il est régulier en codimension 1 et vérifie la propriété (S_2) de Serre [Ser89, IV, Th. 11]. L'algorithme de normalisation de de Jong [Jon98] permet de régulariser l'anneau A en codimension 1 (le nombre d'étapes est alors borné par une multiplicité calculable elle-même avec complexité élémentaire [MO15, §15.4, 15.5.3]). Notons A_1 l'anneau obtenu. La plus petite extension de A_1 dans $\mathrm{Frac}(A_1)$ qui vérifie la propriété (S_2) se calcule à l'aide d'un bidual [Vas06, Prop. 6.21], et est la normalisation de A.

B.3 Construction de familles d'hyperplans

B.3.1 Hyperplans en position générale

Étant donné un corps k ayant suffisamment de points et un entier t donné, comment construire un ensemble de t hyperplans de $\mathbb{P}^n_k$ en position générale ?

Définition B.3.1. Soit k un corps. Soient n, t deux entiers strictement positifs. Un ensemble S de t hyperplans de $\mathbb{P}^n_k$ est en position générale si :

- pour tout $i \in \{1, \ldots, n\}$ et tous $H_1, \ldots, H_i \in S$ deux à deux distincts, $\dim(H_1 \cap \cdots \cap H_i) = n - i$;
- tout point fermé de $\mathbb{P}^n_k$ appartient à au plus n hyperplans de S.

Le théorème suivant permet de contrôler l'intersection de deux variétés projectives.

Proposition B.3.2. [Har08, Th. 1.7.2] Soient Y, Z deux sous-variétés de $\mathbb{P}^n$ de dimensions respectives r, s. Alors toute composante irréductible de $Y \cap Z$ est de dimension $\geqslant r + s - n$. Lorsque $r + s - n \geqslant 0$, l'intersection est non vide.

Lemme B.3.3. Soit S un ensemble de t hyperplans de $\mathbb{P}^n_k$ en position générale, avec $t \geqslant n$. Soit H un hyperplan de $\mathbb{P}^n_k$. Soient $P_1, \ldots, P_s$ les points d'intersection de toutes les familles de n hyperplans de S. Si H ne contient aucun des P_i alors $S \cup \{H\}$ est en position générale.

Démonstration. Soit $i \leqslant n - 1$. Considérons une intersection $I = H_1 \cap \cdots \cap H_i$ d'éléments de S. Alors il existe $j \in \{1, \ldots, s\}$ tel que $P_j \in I$. Par conséquent, H ne contient pas I, qui est irréductible, donc $\dim(H \cap I) = \dim(I) - 1 = n - i$ d'après la proposition B.3.2.
Soit P un point fermé de $\mathbb{P}^n_k$. Si P appartient à strictement moins de n hyperplans de S, il n'y a rien à vérifier. Si P appartient à n hyperplans de S alors c'est l'un des P_i et il n'appartient pas à H. □

Étant donné deux entiers $t, n \geqslant 1$, voici l'algorithme qui calcule un ensemble de t hyperplans de $\mathbb{P}^n_k$ en position générale.
Si $t \leqslant n + 1$, l'algorithme renvoie les hyperplans définis par les coordonnées $x_0, \ldots, x_{t-1}$.
Supposons construit un ensemble $S = \{H_1, \ldots, H_t\}$ d'hyperplans en position générale, avec $t \geqslant n + 1$. Voici comment construire H_{t+1} tel que $\{H_1, \ldots, H_{t+1}\}$ soit en position générale. Dans un premier temps, des algorithmes d'algèbre linéaire permettent de déterminer les points d'intersection $P_1, \ldots, P_s$ (avec $s \leqslant \binom{t}{n} \leqslant \frac{t^n}{n!}$) des familles de n hyperplans de S. Un hyperplan H défini par une forme linéaire $F = \sum_i a_i x_i \in k[x_0, \ldots, x_n]$ ne contient pas un point $P_i = (p^i_0 : \ldots : p^i_n)$ si et seulement si le point $a = (a_0, \ldots, a_n) \in k^{n+1}$ n'appartient pas au noyau de la forme linéaire $F_j = \sum_j p^i_j x_j$. Par conséquent, les points a convenables se trouvent en-dehors d'une réunion de s hyperplans de $\mathbb{A}^{n+1}_k$ qui se calculent explicitement.

L'astuce suivante pour trouver un point $a \in \mathbb{A}^{n+1}(k)$ convenable provient de [KPR16, Lem. 2.4]. Énumérons t^{n+1} éléments $b_1, \ldots, b_s \in k$. Considérons la grille $R = \{b_1, \ldots, b_{t^{n+1}}\}^{n+1} \subseteq \mathbb{A}^{n+1}(k)$. Alors tout hyperplan de $\mathbb{A}_k^{n+1}$ contient au plus t^{n^2+n} éléments de R ; en particulier, la réunion des hyperplans définis par $F_1, \ldots, F_s$ contient donc moins de $\frac{1}{n!}t^{n^2+2n}$ points de R. Or R contient t^{n^2+2n+1} éléments. Il suffit donc de prendre un point $a \in R$ qui n'est pas sur l'un des hyperplans, et de définir H_{t+1} comme l'hyperplan défini par la forme linéaire $\sum_i a_i x_i$.

Pour chaque hyperplan H'_j défini par F_j, le calcul de $H'_j \cap R$ se fait par recherche exhaustive sur les points de R : il y en a t^{n^2+2n+1}. Il existe donc $\alpha > 0$ tel que la complexité totale de l'algorithme soit $O(t^{\alpha n^2})$. Le résultat que nous avons montré est le suivant.

Proposition B.3.4. Soient n, t deux entiers. Soit k un corps ayant au moins t^{n+1} éléments. Il existe $\alpha > 0$ et un algorithme déterministe qui renvoie t hyperplans de $\mathbb{P}_k^n$ en position générale en $O(t^{\alpha n^2})$ opérations dans k.

Si $k = \mathbb{F}_q$ avec $q \leqslant t^{n+1}$, il convient de travailler sur une extension k' de $\mathbb{F}_q$ de degré $\lceil \log_q(t^{n+1}) \rceil$, qui se calcule en temps polynomial en q et $(n+1)\log_q t$. Il est alors possible de calculer avec l'algorithme ci-dessus t hyperplans en position générale dans $\mathbb{P}_{k'}^n$.

Remarque B.3.5. Remarquons qu'avec un algorithme probabiliste, la construction étant donné $H_1, \ldots, H_t$ en position générale, d'un hyperplan H_{t+1} tel que $H_1, \ldots, H_{t+1}$ soient en position générale se fait plus rapidement. En effet, en choisissant (avec les notations de la preuve de la proposition précédente) un élément aléatoire de la grille R, la probabilité qu'il appartienne à l'un des hyperplans $H_1, \ldots, H_t$ est

$$\frac{t^{n^2+2n}}{n! t^{n^2+2n+1}} = \frac{1}{n! t}.$$

L'algorithme de type Las Vegas consistant à choisir un élément aléatoire de R puis vérifier s'il vérifie l'une des équations des H_i nécessite $O(tn)$ opérations dans k, et a une probabilité d'échec égale à $\frac{1}{n!t}$.

B.3.2 Hyperplans qui coupent une variété transversalement

Soit k un corps algébriquement clos. Soit $X \subset \mathbb{P}^n$ un sous-schéma intègre lisse de dimension d. Soient $x \in X(k)$ et $r \leqslant n$. Le but de cette section est d'expliquer comment construire des hyperplans $H_1, \ldots, H_r$ en position générale tels que l'intersection $C := \cap_i H_i$ coupe X transversalement et contienne x. Comme X est lisse, il est localement intersection complète. Nous pouvons donc écrire $X = X_1 \cup \cdots \cup X_s$, où les X_i sont des schémas affines d'intersection complète. Le calcul des X_i est primitivement récursif : par la preuve explicite de [Stacks, 00SC], il est possible pour chaque point $x \in X$ d'en calculer un voisinage ouvert qui est intersection complète ; le principe de la section B.1.2 conclut. Remplaçons X par l'un des X_i. Écrivons $X = \operatorname{Spec} k[x_1, \ldots, x_n]/(f_1, \ldots, f_{n-d}) \subset \mathbb{P}^n = \operatorname{Proj} k[x_0, \ldots, x_n]$. Alors la preuve de [SGA4$_3$, XI, Th. 2.1.(i)] montre comment déterminer explicitement des équations d'une partie constructible Y de $\mathbb{A}^{n+1}$ paramétrant les hyperplans H_a d'équation $a_0x_0 + \cdots + a_nx_n$ tels que $x \in H_a$ et que l'intersection $H \cap X$ ne soit pas transversale. Il suffit de trouver un k-point de $\mathbb{P}^n$ qui ne se trouve pas dans Y pour construire un premier hyperplan H_1. Ayant déjà construit $H_1, \ldots, H_j$ en position générale, l'hyperplan H_{j+1} se construit en choisissant un point de $(\mathbb{P}^n)^\vee - Y$ qui vérifie également les contraintes décrites dans la section précédente (il suffit qu'il évite une réunion d'hyperplans de $\mathbb{A}^{n+1}$, tous distincts de celui qui paramètre les H contenant x).

Le résultat ci-dessus s'étend à n'importe quel sous-schéma X de $\mathbb{P}^n$ dès que le point x est régulier : il suffit d'appliquer la procédure à $X - X_{\mathrm{sing}}$. Lorsque $r \geqslant d$, il est également possible d'adapter cet argument à un schéma X non nécessairement lisse, pour construire des hyperplans $H_1, \ldots, H_r$ qui

évitent de plus X_{sing}. À chaque étape $i \leqslant d$ de l'application de la procédure ci-dessus à $X - X_{\text{sing}}$, calculons les composantes connexes de $X_{\text{sing}} \cap H_1 \cap \cdots \cap H_i$, et déterminons un point de chacune : ceci fournit des points $P_1, \ldots, P_s$. Au moment de choisir H_{i+1}, ajoutons à la partie $Y \subset (\mathbb{P}^n)^\vee$ ci-dessus les hyperplans définis par les conditions linéaires $P_j \in H_{i+1}$. La condition $r \geqslant d$ assure que tous les points de X_{sing} sont évités.

Dans la section IV.1.2, nous avons besoin d'appliquer ces résultats à la situation suivante. Le schéma X est normal et contient un fermé V de dimension $d-1$ qui contient X_{sing}. Comme X est normal, X_{sing} est de dimension au plus $d-2$. Le but est de construire des hyperplans $H_1, \ldots, H_{d-1}$ dont l'intersection coupe X et V transversalement, et évite X_{sing}. À chaque étape $i \in \{0, \ldots, d-1\}$ sont construites des parties $Y_X^{(i)}$ et $Y_V^{(i)}$ de $(\mathbb{P}^n)^\vee$ qui paramètrent les hyperplans qui ne conviennent pas. Il suffit de choisir un point de $(\mathbb{P}^n)^\vee - (Y_X^{(i)} \cup Y_V^{(i)})$.

B.4 Recherche de points

Soit k un corps algébriquement clos. Le but de cette section est le suivant : étant donné une variété X plongée dans $\mathbb{P}^n_k$, trouver au moins un point fermé de $X_{\bar{k}}$ dans chaque composante irréductible de X. Le fait de ne pas se préoccuper des multiplicités rend cette tâche plus facile que la décomposition primaire. Dans un premier temps, voyons comment trouver les points fermés des composantes zéro-dimensionnelles de X, appelés points isolés.

B.4.1 Trouver des points isolés

Lemme B.4.1. [Ier89, Lem. 3.1] Soit k un corps algébriquement clos. Soient $f_1, \ldots, f_m$ des polynômes homogènes de $k[x_0, \ldots, x_n]$ de degré inférieur à d. Alors pour tout $s \leqslant n$, le fermé $V(f_1, \ldots, f_s)$ de $\mathbb{P}^n$ a au plus d^s composantes irréductibles de codimension inférieure à s. En particulier, il a au plus d^n composantes irréductibles.

Supposons X défini par m polynômes homogènes $f_1, \ldots, f_m \in k[x_0, \ldots, x_n]$ de degrés respectifs $d_1, \ldots, d_m \leqslant d$. Quitte à ajouter des équations redondantes si $m < n$, ou à agrandir X en oubliant certaines équations si $m > n$, nous pouvons supposer $n = m$. Notons $L_x(u) = \sum_{i=0}^n x_i^d u_i \in k[x_0, \ldots, x_n, u_0, \ldots, u_n]$ et $\hat{f}_i(x,t) = t x_i^{d_i} + (1-t) f_i(x) \in k[x_0, \ldots, x_n, t]$. Soit $\hat{X} \hookrightarrow \mathbb{P}^n \times \mathbb{A}^1$ le fermé défini par les $\hat{f}_i$.

Proposition B.4.2. [Ier89, Lem. 2.3] Notons $\bar{X} = \overline{\hat{X} \cap D(t)}$ l'adhérence dans $\mathbb{P}^n \times \mathbb{A}^1$ de l'intersection de $\hat{X}$ avec l'ouvert principal $D(t)$ (où $\mathbb{A}^1 = \operatorname{Spec} k[t]$), et $\bar{X}_0$ l'intersection de $\bar{X}$ avec le fermé $V(t)$. (En bref : $\bar{X}_0 = \lim_{t \to 0} \hat{X}_t$) Alors $\bar{X}_0$ est de dimension zéro et contient tous les points fermés isolés de X.

La procédure est décrite dans [Ier89, §2.2]. Elle consiste à construire un polynôme $R(u_0, \ldots, u_n)$ dont les zéros sont les mêmes que ceux de $\prod_{x \in \bar{X}_0} L_x(u_0, \ldots, u_n)$. Ce $R \in k[u_0, \ldots, u_n]$ est un résultant multivarié qui se calcule en temps $O(d^n)$ [Ier89, Prop. 2.5].

Il suffit ensuite de poser $R_i(t) = R(t, 0, \ldots, 0, -1, 0, \ldots, 0)$ et de factoriser $R_i(t)$ pour connaître la (puissance d-ième de la) projection sur le i-ième axe de coordonnées des points de $\bar{X}_0$. Ceci fournit d^2 coordonnées possibles sur chaque axe, et il suffit de tester les d^{2n} combinaisons possibles pour savoir si elles définissent un point fermé de X.

B.4.2 Trouver des points dans toutes les composantes

B.4.2.1 Pour un fermé de l'espace projectif

Soit $X \subsetneq \mathbb{P}^n$ donné par des équations homogènes. La stratégie pour trouver au moins un point dans chaque composante irréductible de X consiste à se ramener au cas précédent en intersectant X avec une succession d'hyperplans.
Considérons n hyperplans $H_1, \ldots, H_n$ en position générale (voir définition B.3.1) ; par exemple ceux définis par $x_1, \ldots, x_n$. Notons, pour $i > 0$, $L_i = H_1 \cap \cdots \cap H_i$. Notons encore $L_0 = \mathbb{P}^n$.

Lemme B.4.3. Soit C une composante irréductible de X. Alors il existe $i \in \{0, \ldots, n\}$ tel que $C \cap L_i$ soit non vide et de dimension nulle.

Démonstration. La suite $\dim(C \cap L_i)$ est décroissante. De plus, $\dim(C \cap L_i) \leqslant \dim(L_i) = n - i$ et $\dim(C \cap L_i) \geqslant \dim(C \cap L_{i-1}) - 1$. C'est donc une suite décroissante, qui décroît par pas de 0 ou 1, et qui stationne à 0. Soit i le plus petit indice tel que $C \cap L_i$ soit de dimension nulle. Si $i = 0$, alors $C \cap L_i = C$ est non vide et de dimension nulle. Si $i > 0$, cela signifie que $\dim(C \cap L_{i-1}) = 1$. D'après le théorème B.3.2, l'intersection $C \cap L_i$ est non vide. □

Ceci suggère l'algorithme suivant pour trouver au moins un point de chaque composante irréductible de X : déterminer, pour chaque $i \in \{0, \ldots, n\}$, les points isolés de $X \cap H_1 \cap \cdots \cap H_i$. La complexité est donc n fois celle de la recherche de points isolés.

B.4.2.2 Pour une partie constructible d'un espace projectif

Lemme B.4.4. Soient $H_1, \ldots, H_s$ des hyperplans en position générale dans $\mathbb{P}^n$. Soit C un fermé de $\mathbb{P}^n$. Alors C est contenu dans au plus $\operatorname{codim}(C)$ des hyperplans H_i.

Démonstration. La dimension de l'intersection de $\operatorname{codim}(C)+1$ de ces hyperplans, qui sont en position générale, est strictement inférieure à $\dim(C)$. □

Lemme B.4.5. Soit C un fermé irréductible de $\mathbb{P}^n$. Soit H un hyperplan de $\mathbb{P}^n$. Alors soit $C \subseteq H$, soit $\dim(C \cap H) = \dim(C) - 1$.

Démonstration. Si C n'est pas inclus dans H alors $C \cap H$ est un fermé strict de C. Prenons-en une composante irréductible de dimension maximale C'. D'une part, $\dim(C') \geqslant \dim(C) - 1$ par la proposition B.3.2 appliquée à l'intersection de C et H. D'autre part, $\dim(C') < \dim(C)$ puisque C' est un fermé irréductible strict de C. □

Corollaire B.4.6. Si C est un fermé de $\mathbb{P}^n$ de dimension d, et si $H_1, \ldots, H_s$ sont des hyperplans en position générale avec $s > \dim C$, alors il existe $i_1, \ldots, i_d$ tels que l'intersection de C avec $H_{i_1} \cap \cdots \cap H_{i_d}$ soit de dimension nulle.

Démonstration. Il y a au plus $\operatorname{codim} C$ hyperplans H_i contenant C. Il reste donc au moins un hyperplan ne le contenant pas : prenons-en un et notons-le H_{i_1}. Alors $C \cap H_{i_1}$ est inclus dans au plus n des hyperplans H_i, dont ceux qui contiennent C. Il y a donc au moins un hyperplan H_{i_2} qui ne le contient pas, et $\dim(C \cap H_{i_1} \cap H_{i_2}) = \dim(C) - 2$. Une récurrence immédiate conclut. □

Lemme B.4.7. Si C est un fermé de $\mathbb{P}^n$ de dimension d, et si $H_1, \ldots, H_{n-d}$ sont des hyperplans en position générale contenant C, alors $C = H_1 \cap \cdots \cap H_{n-d}$.

Démonstration. L'intersection est irréductible, de même dimension que C et contient C qui en est un fermé. □

Adaptons l'algorithme précédent au cas d'une partie constructible d'un espace projectif. Considérons donc un fermé réduit Y de $\mathbb{P}^n$ défini par les équations homogènes $f_1 = 0, \ldots, f_m = 0$, et un ouvert X de Y défini par des inéquations homogènes $g_1 \neq 0, \ldots, g_s \neq 0$. Notons, pour chaque $i \in \{1 \ldots s\}$, V_i le fermé de $\mathbb{P}^n$ défini par g_i. Soit d_X un majorant des degrés des f_i et des g_j. Construisons d'abord un ensemble $S = \{H_1, \ldots, H_D\}$ d'hyperplans de $\mathbb{P}^n$ en position générale, avec $D = snd_X^n + 1$.

Commençons par calculer les points isolés de Y (dont font partie les points isolés de X). Ensuite, intersectons Y avec chacun des hyperplans H_i. Les lemmes suivants montrent qu'alors toute composante de dimension 1 de X intersecte au moins l'un des H_i en un nombre fini non nul de points isolés, et que toute composante de dimension supérieure a une intersection non nulle avec au moins l'un des H_i.

Pour chaque i, la même procédure s'applique ensuite récursivement à $Y \cap H_i$. Elle s'arrête après une profondeur de récursion de n. Au total, elle nécessite le calcul de $O((sd_X^n)^n) = O(s^n d_X^{n^2})$ intersections, et pour chacune de ces intersections, la détermination des points isolés du fermé de $\mathbb{P}^n$ défini par $O(m+n)$ équations de degré $O(d_X)$. Chaque calcul d'intersection nécessite alors $O((m+n)d_X^{O(n)})$ opérations dans k. La complexité totale du calcul est donc de $ms^n d_X^{O(n^2)}$ opérations dans k.

Lemme B.4.8. Soit C une composante irréductible de X de dimension 1. Si S est un ensemble de $snd_X^n + 1$ hyperplans en position générale alors il existe $H \in S$ tel que $C \cap H$ soit de dimension nulle et non vide.

Démonstration. Notons $\bar{C}$ l'adhérence de C dans Y : c'est un fermé de $\mathbb{P}^n$. Pour tout i, comme C n'est pas inclus dans V_i, l'intersection de $\bar{C}$ avec V_i est de dimension nulle. En particulier, $C \cap V_i$ a $m_i \leqslant d_X^n$ points, et le nombre de points de $C \cap (\bigcup_i V_i)$ est $m \leqslant sd_X^n$. Comme les hyperplans H_i sont en position générale, chacun des m_i points de $C \cap V_i$ est contenu dans au plus n d'entre eux. Par conséquent, en prenant $nm + 1 \leqslant nsd_X^n + 1$ hyperplans de S, au moins l'un d'entre eux intersecte $\bar{C}$ en un point qui n'est pas à l'infini. □

Lemme B.4.9. Soit C une composante irréductible de X. Notons $d_X = \dim(X)$. Soit S un ensemble de $snd_X^n + 1$ hyperplans en position générale. Il existe $H_1, \ldots, H_d \in S$ tels que $C \cap H_1 \cap \cdots \cap H_d$ soit de dimension nulle et non vide.

Démonstration. Notons $\bar{C}$ l'adhérence de C dans Y. Pour chaque indice $i \in \{1, \ldots, s\}$, le lemme B.4.1 assure que $\bar{C} \cap V_i$ a au plus d_X^n composantes irréductibles. Il existe donc au plus snd_X^n hyperplans de S contenant l'une des composantes irréductibles de l'un des $\bar{C} \cap V_i$. Prenons-en un qui ne contient aucun $\bar{C} \cap V_i$, et notons-le H_1 ; en particulier, pour tout i, la dimension de $H_1 \cap \bar{C}$ est $\dim(\bar{C}) - 1$, et celle de $H_1 \cap \bar{C} \cap V_i$ est égale à $\dim(\bar{C}) - 2$. Par conséquent, $H_1 \cap \bar{C}$ contient un point de C. Il existe alors au plus nsd_X^n hyperplans de S contenant l'un des $\bar{C} \cap H_1 \cap V_i$; leur ensemble contient celui des hyperplans précédemment écartés contenant l'un des $\bar{C} \cap V_i$. Ceci fournit H_2 qui ne contient aucune de ces intersections. Continuons ainsi jusqu'à obtenir $H_1, \ldots, H_{d-1}$. Le lemme B.4.8 permet alors de construire H_d tel que tels que $C' := \bar{C} \cap H_1 \cap \cdots \cap H_d$ soit de dimension nulle, et contienne un point qui n'est dans aucun des V_i, c'est-à-dire un point de C. Le nombre d'hyperplans en position générale à éviter est majoré par nsd_X^n ; tout ensemble de $nsd_X^n + 1$ hyperplans en position générale contient donc un élément convenable. □

Par conséquent, il suffit de construire $O(nsd_X^n)$ hyperplans en position générale dans $\mathbb{P}^n$. Ceci se fait en temps $(nsd_X^n)^{O(n^2)}$ avec l'algorithme décrit dans la section B.3.1.

B.4.3 Le cas équidimensionnel

Cette méthode, bien plus élégante que celle présentée ci-avant, est décrite dans [Jin20, Alg. 8.5]. Soit $X = \operatorname{Spec} k[x_1, \ldots, x_n]/(f_1, \ldots, f_m)$ un schéma affine de type fini sur k dont toutes les composantes irréductibles sont de même dimension r. Soit $\nu \colon X \to \mathbb{A}^r_k$ une normalisation de Noether de X.

Lemme B.4.10. La restriction de ν à toute composante irréductible de X est encore surjective.

Démonstration. Si C est une composante irréductible de X alors $\nu|_C$ est encore un morphisme fini, et donc $\dim(\nu(C)) = \dim(C) = \dim(X) = r$ par équidimensionnalité de X. De plus, encore par finitude, $\nu(C)$ est un fermé de $\mathbb{A}^r_k$ de dimension r, il est donc égal à $\mathbb{A}^r_k$. □

La fibre $\nu^{-1}(0) =: \operatorname{Spec} R$ intersecte donc chaque composante irréductible de X. Une décomposition primaire de R (présenté par générateurs et relations), qui est une k-algèbre finie, fournit pour chaque composante primaire C une base de Gröbner de son réduit. Ceci permet d'obtenir par factorisation une liste de $\bar{k}$-points, qui contient au moins un élément de chaque composante irréductible. L'algorithme est donc composé de 4 étapes : un calcul de normalisation de Noether, une décomposition primaire, des calculs de bases de Gröbner d'idéaux zéro-dimensionnels puis des factorisations.

Nous n'avons pas précisé, dans la section sur les bases de Gröbner, la complexité des différents algorithmes ; cependant, la complexité de la normalisation de Noether décrite dans [Dic+91, Alg. 1.13] est déjà, pour un idéal de $k[x_1, \ldots, x_n]$ engendré par m équations de degré maximal d, de l'ordre de $m^3 d^{O(n^2)}$. Il n'y a donc pas de gain de complexité notable par rapport à la méthode par recherche de points isolés d'intersections avec des hyperplans présentée dans la section B.4.2.2.

B.5 Restriction de Weil

Définition B.5.1. Soit $f \colon Y \to X$ un morphisme de schémas. Soient V un Y-schéma, et h_V le faisceau représenté par V. Si le préfaisceau $f_\star h_V \colon U \mapsto \operatorname{Hom}_Y(U \times_X Y, V)$ sur Sch/X est représentable par un X-schéma R, ce dernier est appelé restriction de Weil de V relativement à f et noté $R_f(V)$, ou $R_{Y \to X}(V)$ si le contexte le permet.

Proposition B.5.2. [BLR90, 7.6, Th. 4] Soit $f \colon Y \to X$ un morphisme fini localement libre de schémas. Soit V un Y-schéma tel que pour tout $x \in X$, tout sous-ensemble fini de la fibre V_x soit contenu dans un ouvert affine de V (c'est le cas par exemple si V est affine). Alors $R_{Y \to X}(V)$ existe.

En particulier, si X et Y sont affines, le foncteur $R_{Y \to X}$ est l'adjoint à droite de $- \times_X Y$ sur les catégories de schémas affines sur X et Y. Soient

$$\begin{array}{rcl} A & = & k[x_1, \ldots, x_n]/(f_1, \ldots, f_r) \\ B & = & k[y_1, \ldots, y_m]/(g_1, \ldots, g_s) \\ C & = & B[v_1, \ldots, v_p]/(h_1, \ldots, h_t). \end{array}$$

Notons $X = \operatorname{Spec} A$, $Y = \operatorname{Spec} B$, $V = \operatorname{Spec} C$. Supposons donné un morphisme $F \colon A \to B$ défini par $F_1, \ldots, F_r \in k[y_1, \ldots, y_m]$ qui fait de B un A-module libre, et une base $(b_1, \ldots, b_N)$ de B comme A-module. Dans ce cadre, la proposition précédente assure que la restriction de Weil $R_{Y \to X}(V)$ existe et se calcule de la façon suivante (voir [Sch94, 4.4.1]).

Introduisons des indéterminées w_{ij} où $i \in \{1, \ldots, p\}$ et $j \in \{1, \ldots N\}$, et définissons, pour $\alpha \in \{1, \ldots, t\}$ et $\beta \in \{1, \ldots, N\}$, des éléments $f_{\alpha\beta} \in A[w_{ij}]$ par :

$$h_\alpha \left(\sum_{j=1}^N w_{1j} b_j, \ldots, \sum_{j=1}^N w_{pj} b_j \right) = \sum_{\beta=1}^N f_{\alpha\beta} b_\beta \in B[w_{ij}].$$

La restriction de Weil $R_{Y\to X}(V)$ est alors $\operatorname{Spec} k[w_{ij}]/(f_{\alpha\beta})$. Le morphisme d'adjonction

$$V \to R_{Y\to X}(V) \times_X Y$$

est donné par $k[v_i]/(h_\gamma) \to k[w_{ij}]/(f_{\alpha\beta}), v_i \mapsto \sum_j w_{ij} b_j$. De même, si $V = U \times_X Y$, le morphisme d'adjonction $U \to R_{Y\to X}(V)$ est donné en écrivant $1 = \sum_j a_j b_j$ avec $a_j \in A$, et en envoyant w_{ij} sur $a_j v_i \in A[v_i]$.

La restriction $R_{Y\to X}(\phi)$ d'un morphisme $\phi\colon V \to V'$ de Y-schémas se calcule par la même méthode. De plus, si V est un schéma en groupes sur Y, la même méthode permet de calculer la loi de groupe sur $R_{Y\to X}(V)$. En effet, comme la restriction de Weil est un adjoint à droite, elle commute aux limites, et $R_{Y\to X}(V \times_Y V) = R_{Y\to X}(V) \times_X R_{Y\to X}(V)$. Il suffit donc de déterminer le morphisme $R_{Y\to X}(V \times_Y V \to V)$.

ANNEXE C

Algorithmique des courbes

C.1 Représentations des courbes lisses

Par défaut, une courbe sur un corps k_0 est représentée par un recollement de courbes affines comme décrit dans l'annexe B.1.1. Une courbe intègre sur k_0 étant toujours isomorphe à un ouvert d'un fermé d'un espace projectif [Stacks, 0A27], d'autres représentations des courbes seront données ici.

C.1.1 Courbes singulières, compactification lisse

C.1.1.1 Résolution des singularités d'une courbe plane

Soit k_0 un corps. Soit $C = \operatorname{Proj} k_0[x, y, z]/(f)$ une courbe projective plane intègre de normalisée X. Notons $d = \deg(f)$. La courbe C a au plus $\frac{(d-1)(d-2)}{2}$ points singuliers [Fis01, Th. 3.8].

Définition C.1.1. Un point P d'une courbe plane C est dit ordinaire si le nombre de tangentes à C en P est égal à la multiplicité de C en P.

Par moins de d^2 transformations quadratiques, il est possible [FW89, 7.4, Th. 2] de construire une courbe X' birationnelle à X ayant uniquement des singularités ordinaires. Le degré de la courbe X' est $O(2^{d^2})$.
La méthode classique de résolution des singularités sur une variété quelconque procède par éclatements successifs ; elle a l'avantage de construire directement un plongement projectif de X, mais l'inconvénient que l'espace projectif dans lequel X est plongée est de grande dimension. En partant de X' à singularités ordinaires, il suffit d'un seul éclatement par singularité. Les algorithmes n'ont souvent pas besoin de connaître un plongement projectif de X, mais simplement une description des points de X au-dessus de chaque singularité de C.

Proposition C.1.2. [Koz94, §5] Il existe un algorithme déterministe qui prend en entrée une courbe $C \subset \mathbb{A}^2_{\mathbb{F}_q}$ (resp. $\mathbb{A}^2_{\mathbb{Q}}$) définie par un polynôme $f = \sum_{i,j} a_{ij} x^i y^j \in \mathbb{F}_q[x, y]$ (resp. $\mathbb{Z}[x, y]$) de degré d tel que $(0, 0) \in C$, et retourne l'arbre de désingularisation de C en $(0, 0)$, en un nombre d'opérations polynomial en d et en $\log q$ (resp. en $\log \max |a_{ij}|$).

C.1.1.2 Compactification lisse

Soit k_0 un corps parfait. Soit $X = \operatorname{Spec} k_0[x_1, \ldots, x_m]/(f_1, \ldots, f_r)$ une courbe affine lisse sur k_0. En homogénéisant les f_i, on obtient l'adhérence Y de X dans $\mathbb{P}^m_{k_0}$. La courbe Y est possiblement singulière en-dehors de son ouvert isomorphe à X. La normalisation $\bar{X}$ de Y est une courbe projective lisse dont un ouvert est isomorphe à X. Cette courbe $\bar{X}$ est appelée compactification lisse de X ; elle est unique à isomorphisme près. Étant donné un morphisme de courbes affines lisses $X_1 \to X_2$ sur k_0, le morphisme composé $X_1 \to X_2 \to \bar{X}_2$ s'étend à $\bar{X}_1$ par régularité [Har08, I, Prop. 6.8].

C.1.2 Corps de fonctions, modèle plan birationnel

Soit k_0 un corps. Rappelons que le foncteur qui à une courbe associe son corps de fonctions définit une équivalence entre la catégorie des courbes projectives régulières sur k_0 munie des morphismes non constants, et la catégorie des extensions de k_0 de degré de transcendance 1 [Stacks, 0BY1]. Une courbe projective régulière peut donc être définie par son corps de fonctions.

Proposition C.1.3. [Sti09, Prop. 3.10.2.(a)] Soit X une courbe connexe lisse sur un corps parfait k_0. Soient $P \in X(k_0)$ et t une uniformisante en P. Alors le corps des fonctions $k_0(X)$ est une extension finie séparable de $k_0(t)$.

Étant donné une telle courbe X plongée dans $\mathbb{P}^n_{k_0}$, un morphisme $X \to \mathbb{P}^1_{k_0}$ fini génériquement étale se calcule donc en cherchant une uniformisante t en un point $P \in X(k_0)$. Si $X(k_0)$ est vide, il suffit de remplacer k_0 par une extension k_0' (de degré $O(\deg X)$) sur laquelle X a un point pour obtenir un morphisme $X_{k_0'} \to \mathbb{P}^1_{k_0'}$. Sans perte de généralité, supposons que P se situe dans l'ouvert affine $U_0 = \{x_0 \neq 0\}$ de $\mathbb{P}^n$. La courbe X est donnée par des polynômes $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$ avec $m \geqslant n-1$. Comme X est lisse sur k_0, la matrice $(\frac{\partial f_i}{\partial x_j})_{i,j}$ est de rang $n-1$. Il existe donc $j \in \{1, \ldots, n\}$ tel que le morphisme $x_j - x_j(P) \colon X \cap U_0 \to \mathbb{A}^1$ soit étale en P, et donc que $t \coloneqq x_j - x_j(P)$ soit une uniformisante en P. Le degré du morphisme $X \to \mathbb{P}^1$ induit par t est donc de degré au plus $\deg X$, qui est le nombre maximal de points d'intersection de H avec un hyperplan de $\mathbb{P}^n$.

Afin de travailler avec un modèle birationnel plan de X, il suffit de chercher un élément primitif u de l'extension finie séparable $k_0(X)/k_0(t)$ à l'aide de l'algorithme décrit dans la section A.3.2.2. Rappelons que si $k(X)$ est engendré par $(x_1, x_2, \ldots, x_n)$, un tel élément primitif s'obtient sous la forme $u = t + \sum_{i \neq j} \lambda_i x_i$ avec $\lambda_i \in k$. Alors $k_0(X) = k_0(t, u) = k_0(t)[u]/(f)$, où f est le polynôme minimal de u sur $k_0(t)$. Ceci définit un morphisme birationnel $X \to C$, où C est une courbe projective plane d'équation dans une carte affine $f(t, u) = 0$. Supposons, quitte à le multiplier par un élément de $k_0[t]$, que f est un polynôme primitif dans $k_0[t][u]$. Le lemme de Gauss assure alors que f est irréductible dans $k_0[t, u]$ et dans $k_0(u)[t]$; par conséquent, $\deg(f) = [k_0(X) : k_0(u)]$. De même que ci-dessus, comme $u = t + \sum_i \lambda_i x_i$ est de degré 1, le degré du morphisme $X \to \mathbb{P}^1$ engendré par cette fonction est majoré par $\deg X$. Or $\deg_t(f) = [k_0(X) : k_0(u)] \leqslant \deg X$, et $\deg_u(f) = [k_0(X) : k_0(t)] \leqslant \deg X$. Par conséquent, $\deg(C) \leqslant \deg(X)^2$.

De plus, le degré d'un modèle plan peut être borné en fonction du genre de la courbe X. Si X est hyperelliptique, il est connu qu'elle admet un modèle plan de la forme

$$y^2 + h(x)y = f(x)$$

avec $\deg h, \deg f \leqslant 2g + 2$. Ce modèle s'obtient grâce au revêtement double $X \to \mathbb{P}^1$. Si X n'est pas hyperelliptique, son diviseur canonique K est très ample, et le choix de $g - 3$ points généraux $P_1, \ldots, P_{g-3}$ de X permet d'obtenir un diviseur $D = K - \sum_i P_i$ birationnellement très ample dont l'espace de Riemann-Roch $\mathscr{L}(D)$ est de dimension 3 [KM08, §1]. Dans tous les cas, il est possible de construire explicitement un modèle birationnel plan de X de degré $O(g)$.

Par conséquent, toute courbe projective lisse admet un modèle plan à singularités ordinaires de degré $O(2^g)$.

C.1.3 Représentation comme $\mathcal{O}_{\mathbb{P}^1}$-algèbre

C.1.3.1 Description

Cette description est celle employée par Jin dans [Jin20]. Soit X une courbe intègre projective lisse sur un corps parfait k_0. Supposons-la décrite comme fermé d'un espace projectif sur k_0. D'après la proposition C.1.3, le calcul d'une uniformisante permet d'obtenir un morphisme $X \to \mathbb{P}^1$ dont l'extension de corps de fonctions correspondante est séparable. Le morphisme $X \to \mathbb{P}^1$ est donc génériquement étale par [Mum15, 5.4.3].

Lemme C.1.4. Le faisceau $\phi_\star \mathcal{O}_X$ est un fibré vectoriel sur $\mathbb{P}^1$.

Démonstration. Le morphisme ϕ est un morphisme non constant d'une courbe vers une courbe régulière, il est donc plat par [Stacks, 0CCK]. Un module de présentation finie est localement libre si et seulement si il est plat [Stacks, 00NX] ; par conséquent, $\phi_\star \mathcal{O}_X$ est un $\mathcal{O}_{\mathbb{P}^1}$-module localement libre. □

Notons $U_0 = \operatorname{Spec} k_0[x]$ et $U_1 = \operatorname{Spec} k_0[x^{-1}]$ les ouverts standard de $\mathbb{P}^1$.

Lemme C.1.5. Si $\mathcal{F}$ est un $\mathcal{O}_{\mathbb{P}^1}$-module localement libre de type fini alors $\mathcal{F}(U_0)$ est un $k_0[x]$-module libre de rang fini, et $\mathcal{F}(U_1)$ est un $k_0[x^{-1}]$-module libre de rang fini.

Démonstration. Comme $\mathcal{F}$ est un module localement libre de type fini, il est projectif [Stacks, 00NX]. En particulier, $\mathcal{F}_{|U_0}$ est encore projectif, il est donc libre puisque $k_0[x]$ est principal. □

Un fibré vectoriel $\mathcal{F}$ de rang r sur $\mathbb{P}^1$ est défini par la donnée du $k_0[x]$-module $\mathcal{F}(U_0)$, du $k_0[x^{-1}]$-module $\mathcal{F}(U_1)$ et d'un isomorphisme de $k_0[x^{\pm 1}]$-modules

$$\mathcal{F}(U_0) \otimes_{k_0[x]} k_0[x^{\pm 1}] \to \mathcal{F}(U_1) \otimes_{k_0[x^{-1}]} k_0[x^{\pm 1}].$$

Ces deux modules étant libres de rang r, cet isomorphisme se représente par une matrice $M_{\mathcal{F}}$ à coefficients dans $k_0[x^{\pm 1}]$ qui dépend des bases choisies pour ces modules libres.

Calcul de $\phi_\star \mathcal{O}_X(U_0)$ La préimage $\phi^{-1} \operatorname{Spec} k_0[x]$ est la normalisation de $k_0[x]$ dans l'extension de corps de fonctions $\phi^\star \colon k_0(x) \to k_0(C)$. Comme k_0 est parfait, on sait calculer un modèle plan de C par le théorème de l'élément primitif, et ainsi présenter $k_0(C)$ comme $k_0(x)[y]/(f)$. Ensuite, on calcule la normalisation dans une extension de corps de la façon usuelle ; elle a dans ce cas précis une complexité plus abordable, comme décrit dans [Die08, Prop. 2.127]. D'après le théorème de Dedekind-Weber-Grothendieck [GW10, Th. 11.50], un fibré vectoriel sur $\mathbb{P}^1$ est isomorphe à une somme directe de fibrés en droites :

$$\mathcal{F} \simeq \mathcal{O}_{\mathbb{P}^1}(n_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(n_r)$$

où les n_i sont uniques à l'ordre près. De façon concrète, cela signifie qu'il existe des bases des modules libres $\mathcal{F}(U_0)$ et $\mathcal{F}(U_1)$ explicitement calculables telles que la matrice $M_{\mathcal{F}}$ soit égale à

$$\begin{pmatrix} x^{n_1} & & \\ & \ddots & \\ & & x^{n_r} \end{pmatrix}.$$

Cette somme de fibrés en droites est munie d'une structure de $\mathcal{O}_{\mathbb{P}^1}$-algèbre de la façon suivante. D'une part, le morphisme canonique $\mathcal{O}_{\mathbb{P}^1} \to \phi_\star \mathcal{O}_X$ définit un morphisme $\mathcal{O}_{\mathbb{P}^1} \to \mathcal{O}_{\mathbb{P}^1}(n_1) \oplus \cdots \oplus \mathcal{O}_{\mathbb{P}^1}(n_r)$. D'autre part, le morphisme de multiplication

$$(\bigoplus_i \mathcal{O}(n_i)) \otimes_{\mathcal{O}_{\mathbb{P}^1}} (\bigoplus_i \mathcal{O}(n_i)) \to \bigoplus_i \mathcal{O}(n_i)$$

est défini sur U_0 par la multiplication dans la $k_0[x]$-algèbre $\mathcal{F}(U_0)$ écrite dans la base choisie pour $\mathcal{F}(U_0)$, et sur U_1 par la multiplication dans la $k_0[x^{-1}]$-algèbre $\mathcal{F}(U_1)$ écrite dans la base choisie pour $\mathcal{F}(U_1)$. Par l'isomorphisme

$$(\bigoplus_i \mathcal{O}(n_i)) \otimes_{\mathcal{O}_{\mathbb{P}^1}} (\bigoplus_i \mathcal{O}(n_i)) \xrightarrow{\sim} \bigoplus_{i,j} \mathcal{O}(n_i + n_j)$$

cette multiplication équivaut à la donnée d'un morphisme

$$\bigoplus_{i,j} \mathcal{O}(n_i + n_j) \to \bigoplus_i \mathcal{O}(n_i).$$

Comme $\underline{\mathrm{Hom}}_{\mathcal{O}_{\mathbb{P}^1}}(\mathcal{O}_{\mathbb{P}^1}(a), \mathcal{O}_{\mathbb{P}^1}(b)) \simeq \mathcal{O}_{\mathbb{P}^1}(b-a)$, il y a des morphismes non triviaux $\mathcal{O}_{\mathbb{P}^1}(a) \to \mathcal{O}_{\mathbb{P}^1}(b)$ si et seulement si $b \geqslant a$. Dans ce cas, un tel morphisme est défini par un polynôme homogène de $k_0[X,Y]$ de degré $b-a$. La multiplication est donc définie par une matrice de taille $r \times r^2$ dont les coefficients sont des polynômes homogènes de $k_0[X,Y]$. Pour que la multiplication soit commutative, il faut et il suffit que les colonnes correspondant à (n_i, n_j) et (n_j, n_i) soient égales. Si X est géométriquement réduite alors $n_i \leqslant 0$ pour tout i [Jin20, Lem. 6.17].

Notons qu'un morphisme de $\mathcal{O}_{\mathbb{P}^1}$-modules $\bigoplus_{j=1}^s \mathcal{O}_{\mathbb{P}^1}(b_j) \to \bigoplus_{i=1}^r \mathcal{O}_{\mathbb{P}^1}(a_i)$ est donné par une matrice de taille $r \times s$ à coefficients dans $k_0[X,Y]$, dont le coefficient en position (i,j) est nul si $b_j > a_i$, et homogène de degré $a_i - b_j$ ou nul sinon. La composition de deux tels morphismes est définie par la multiplication matricielle. Un endomorphisme d'un $\mathcal{O}_{\mathbb{P}^1}$-module est inversible si et seulement si la matrice qui le décrit l'est.

Reconstruction de la courbe La courbe X peut être reconstruite à partir de la structure de $\mathcal{O}_{\mathbb{P}^1}$-algèbre sur $\bigoplus_i \mathcal{O}(n_i)$ induite par celle de $\phi_\star \mathcal{O}_X$. En effet, le morphisme $\phi\colon X \to \mathbb{P}^1$ est un morphisme fini localement libre, il est donc affine, et par conséquent $\underline{\mathrm{Spec}}_{\mathbb{P}^1}(\phi_\star \mathcal{O}_X) \simeq X$, où $\underline{\mathrm{Spec}}$ désigne le spectre relatif. Il suffit donc de déterminer les courbes affines $\mathrm{Spec}(\oplus \mathcal{O}_{\mathbb{P}^1}(n_i)(U_0))$ et $\mathrm{Spec}(\oplus \mathcal{O}_{\mathbb{P}^1}(n_i)(U_1))$ et de les recoller.

Remarque C.1.6. Certains couples (fibré, matrice de multiplication) ne définissent pas une courbe. Par exemple, le fibré $\mathcal{O} \oplus \mathcal{O}(-1) \oplus \mathcal{O}(-2)$ avec la matrice

$$\begin{pmatrix} 1 & & & Z^3 & Z^4 \\ & 1 & 2Z & & \\ & & 1 & & \end{pmatrix}$$

définirait au-dessus de l'ouvert $Z \neq 0$ de $\mathbb{P}^1$ le schéma $\mathrm{Spec}\, k_0[x,u,v]/(u^2-2, uv-1, v^2-1)$, qui est vide. De plus, rien ne garantit a priori la lissité du schéma obtenu.

Afin de s'assurer qu'un couple (fibré, matrice de multiplication) définit une courbe lisse, il convient de tester séparément si le schéma obtenu est de dimension 1 sur k_0 (voir B.2) et s'il est lisse (à l'aide du critère jacobien).

Remarque C.1.7. La même description est encore valable pour des courbes propres lisses qui ne sont pas nécessairement connexes : il suffit de faire la somme directe des fibrés obtenus pour chaque composante connexe. Cette remarque sert dans la section IV.4.

C.2 Produit fibré de courbes intègres lisses

Considérons un diagramme cartésien

$$\begin{tikzcd} T \arrow[r] \arrow[d] & Y \arrow[d] \\ Z \arrow[r] & X \end{tikzcd}$$

un diagramme cartésien de courbes sur un corps k_0 ; supposons X, Y, Z intègres, et $Y \to X$ lisse. Notons $\tilde{X}, \tilde{Y}, \tilde{Z}, \tilde{T}$ les normalisées respectives de X, Y, Z, T. L'objectif de cette section est de calculer le produit fibré $\tilde{Y} \times_{\tilde{X}} \tilde{Z}$, qui est encore lisse sur k_0 puisque $Y \to X$ l'est. Notons $S = \tilde{Y} \times_{\tilde{X}} \tilde{Z}$.

Lemme C.2.1. Il y a un isomorphisme canonique $S \to \tilde{T}$.

Démonstration. Le diagramme commutatif

$$\begin{tikzcd} \tilde{T} \arrow[r] \arrow[d] & \tilde{Y} \arrow[d] \\ \tilde{Z} \arrow[r] & \tilde{X} \end{tikzcd}$$

obtenu par fonctorialité de la normalisation produit un morphisme $\tilde{T} \to S$. Le diagramme suivant

$$\begin{tikzcd} S \arrow[r] \arrow[d] & Y \arrow[d] \\ Z \arrow[r] & X \end{tikzcd}$$

produit un morphisme $S \to T$, qui se factorise par $\tilde{T}$. La composée $S \to \tilde{T} \to S$ est l'unique morphisme $S \to S$ faisant commuter

$$\begin{tikzcd} S \arrow[dr] \arrow[drr] \arrow[ddr] & & \\ & S \arrow[r] \arrow[d] & Y \arrow[d] \\ & Z \arrow[r] & X \end{tikzcd}$$

□

Pour calculer $\tilde{Y} \times_{\tilde{X}} \tilde{Z}$, qui a pour anneau total des fractions un produit de corps, il suffit donc de calculer $Y \times_X Z$, qui a ce même anneau total des fractions. Les lemmes suivants montrent comment en calculer un élément primitif sur $k(x)$.

Lemme C.2.2. Soient K un corps et $L = K(z, t)$ une K-algèbre réduite de dimension finie d sur L. Dans tout ensemble S de d^{4d} éléments de k, il y a au moins un élément λ tel que $\lambda z + t$ engendre L en tant que K-algèbre.

Démonstration. Notons $L = L_1 \times \cdots \times L_r$, où les L_i sont des corps, et $d_i = [L_i : K]$. Soit $x = (x_1, \ldots, x_r) \in L$. Pour tout $i \in \{1 \ldots r\}$, l'élément $(x_1, \ldots, x_i)$ est primitif dans $L_1 \times \cdots \times L_i$ si et seulement si $(x_1, \ldots, x_{i-1})$ est primitif dans $L_1 \times \cdots \times L_{i-1}$, l'élément x_i est primitif dans L_i et le polynôme minimal de x_i sur K est premier au polynôme minimal de $(x_1, \ldots, x_{i-1})$ sur k. Cherchons un élément primitif sous la forme $z + \lambda t$ avec $\lambda \in k$. Rappelons qu'il y a moins de d_i^2 valeurs de λ

pour lesquelles $z + \lambda t$ n'est pas un élément primitif de L_i. Ainsi, le nombre de valeurs de λ à éviter est inférieur à

$$d_1^2 \cdot d_1 d_2^2 \cdot (d_1 + d_2) d_3^2 \cdots (d_1 + \cdots + d_{r-1}) d_r^2.$$

Comme $d_1 + \cdots + d_r = d$, ce nombre est inférieur à d^{4d}. □

Dans notre situation, écrivons $Z = \operatorname{Spec} k_0[a,b]/u$ et $Y = \operatorname{Spec} k_0[s,t]/v$. Appliquons le lemme d'abord à l'extension $L = k(a,b)[s,t]$ de $k(a,b)$, en remarquant que $k(a,b)$ est bien un corps. Commençons par trouver $\lambda \in k$ tel que $L = k(a,b)[\lambda s + t]$. Appliquons ensuite le lemme à l'extension $k(a)[b, \lambda s + t]$ de $k(a)$. Le degré de la première extension est le degré $[Y : X]$ du morphisme $Y \to X$. Le degré de la deuxième extension est $\deg(Z)[Y : X]$. Il suffit donc de tester $(\deg Z)^{4 \deg Z}[Y : X]^{8[Y:X]}$ éléments de la forme $\mu b + \lambda s + t$: pour chacun d'entre eux, on calcule le polynôme minimal par des moyens d'algèbre linéaire sur $k_0(a)$ faisant intervenir des polynômes de degré majoré par $d = \max(\deg(Z), \deg(Y), \deg(Z \to X), \deg(Y \to X))$. La complexité de ces opérations d'algèbre linéaire est polynomiale en d. La complexité totale est donc $O(d^{12d}\mathcal{P}(d))$, où $\mathcal{P}$ est un polynôme, et c'est encore $O(d^{13d})$.

Proposition C.2.3. Soient Y, Z deux courbes intègres planes sur k_0. Considérons une courbe plane X et des morphismes $Z \to X$, $Y \to X$ dont l'un au moins est lisse. Notons $\tilde{X}, \tilde{Y}, \tilde{Z}$ les normalisées respectives de X, Y, Z. Soit

$$d = \max\{\deg(Z), \deg(Y), \deg(Y \to X), \deg(Z \to X)\}.$$

Il existe un algorithme déterministe calculant une courbe plane birationnelle à $\tilde{Z} \times_{\tilde{X}} \tilde{Y}$ en $O(d^{13d})$ opérations dans k. La courbe obtenue est de degré $\deg(Z)[Y : X]^2 \leqslant d^3$.

Notons W la courbe plane obtenue. Rappelons que les composantes connexes de $\tilde{Y} \times_{\tilde{X}} \tilde{Z}$ sont les normalisées des composantes irréductibles de W [Stacks, 0CDV]. Afin de déterminer les composantes connexes de $\tilde{Y} \times_{\tilde{X}} \tilde{Z}$, il suffit donc de factoriser le polynôme définissant $Y \times_X Z$.

Proposition C.2.4. Soient Y, Z deux courbes planes sur k_0. Considérons une courbe plane X et des morphismes $Z \to X$, $Y \to X$ dont l'un au moins est lisse. Soit

$$d = \{\max \deg(Z), \deg(Y), \deg(Y \to X), \deg(Z \to X)\}.$$

Il existe un algorithme déterministe calculant les composantes connexes de $\tilde{Y} \times_{\tilde{X}} \tilde{Z}$ en $O(d^{13d})\mathrm{Fact}_{k_0}(d^2)$ opérations dans k_0, où $\mathrm{Fact}_{k_0}(\cdot)$ désigne la complexité de la factorisation d'un polynôme en deux variables de degré total donné dans k_0.

C.3 Diviseurs et espaces de Riemann-Roch

C.3.1 Représentations des classes de diviseurs

Soient k_0 un corps et k une clôture algébrique de k_0. Soient X_0 une courbe projective lisse sur k_0 et $X = X_0 \times_{k_0} k$. Supposons d'abord X_0 décrite par un plongement projectif. Un diviseur D sur X peut être représenté de deux manières : par une combinaison linéaire de points fermés de X_0 (chaque point étant défini par une extension k_1 de k_0 et des k_1-points de X_0) ou par sa forme de Chow.

Définition C.3.1. Soit $Z = a_i P_1 + \cdots + a_r P_r$ un zéro-cycle de $\mathbb{P}^n_k$. Pour tout i, notons p_{ij} les coordonnées de P_i. La forme de Chow de Z est le polynôme

$$\prod_{i=1}^{r} \left(\sum_{j=0}^{n} p_{ij} u_j \right)^{a_i} \in k[u_0, \ldots, u_n].$$

En particulier, si $X = \operatorname{Proj} k[x,y,z]/(F)$ est une courbe dans $\mathbb{P}^2$, le diviseur d'un polynôme homogène $G \in k[x,y,z]$ a pour forme de Chow le u-résultant [IK93, Lem. 15.7]

$$u - \operatorname{res}(F,G) \coloneqq \operatorname{res}(F, G, xu_x + yu_y + zu_z).$$

Le calcul de la forme de Chow d'un diviseur représenté par une somme de points est évident : il suffit de calculer une extension de k_0 sur laquelle sont définis tous les points du diviseur.

Il existe encore une autre représentation des diviseurs, qui ne travaille pas explicitement avec des équations de X dans un espace projectif. D'abord proposée par Khuri-Makdisi [KM06], elle a été utilisée dans de nombreux algorithmes probabilistes de Bruin [Bru12]. Supposons donné un faisceau inversible $\mathcal{L}$ sur X_0 de degré strictement supérieur à $2g$. Il est nécessairement très ample et fournit un plongement projectif de X ; soit S l'anneau de coordonnées homogènes de X pour ce plongement. Le morphisme

$$S \to \bigoplus_{i \geqslant 0} \Gamma(X, \mathcal{L}^{\otimes i})$$

est un isomorphisme. Pour les calculs, il suffit de connaître le quotient $S^{(h)}$ de S par l'idéal engendré par les éléments homogènes de degré strictement supérieur à un entier h suffisamment grand. Un diviseur D est alors représenté par l'espace des sections globales du faisceau $\mathcal{L}(-D)$. Les algorithmes qui font usage de cette représentation n'ont donc pas besoin d'une réelle description de X, mais simplement de l'algèbre $S^{(h)}$ et du sous-espace vectoriel $\Gamma(\mathcal{L}(-D))$ de $S^{(1)} = \Gamma(X, \mathcal{L})$. Étant donné un plongement projectif de X, un diviseur E tel que $\mathcal{L} = \mathcal{O}_X(E)$ et un diviseur D sur X représenté de l'une des façons ci-dessus, l'espace $\Gamma(\mathcal{L}(-D)) = \Gamma(\mathcal{O}_X(E - D))$ est calculé par les algorithmes de la section suivante. Réciproquement, étant donné l'espace $\Gamma(\mathcal{L}(-D))$, une décomposition de D en somme de diviseurs premiers est obtenue en calculant $\Gamma(D, \mathcal{O}_D)$ et en en réalisant la décomposition primaire (voir [Bru12, Alg. 2.4] pour les détails).

C.3.2 Espaces de Riemann-Roch

Soient k_0 un corps parfait et k une clôture algébrique de k_0. Soient X_0 une courbe projective lisse sur k_0 et $X = X_0 \times_{k_0} k$. Soit $D \in \operatorname{Div}(X)$ un diviseur stable sous l'action de $\operatorname{Gal}(k|k_0)$. Il existe dans la littérature deux approches pour calculer l'espace de Riemann-Roch $\mathscr{L}(D) \coloneqq \mathrm{H}^0(X, \mathcal{O}_X(D))$ associé à D. Un état de l'art détaillé se trouve dans [LGS20, §1, State of the art]. Citons deux approches différentes à ce problème.

Algorithmes géométriques D'une part, les algorithmes dits géométriques s'inspirent de la méthode présentée en 1874 par Brill et Noether dans [BN74]. Supposons donné un modèle plan C_0 de X_0 à singularités ordinaires. Soient $P_1, \ldots, P_r$ les points singuliers de C et $m_1, \ldots, m_r$ leurs multiplicités respectives. Soient $P_{i,1}, \ldots, P_{i,m_i}$ les points de X au-dessus de P_i. Considérons le diviseur adjoint

$$E = \sum_{i=1}^{r} \sum_{j=1}^{m_i} m_i(m_i - 1) P_{i,j}.$$

L'algorithme de Brill-Noether calcule les éléments d'une base de $\mathscr{L}(D)$ sous la forme $\frac{f_1}{h}, \ldots, \frac{f_s}{h}$. Dans un premier temps, il calcule le dénominateur commun $h \in k[x,y]$. Il suffit que le diviseur de h satisfasse

$$\operatorname{div}(h) \geqslant D + E.$$

Dans un second temps, il calcule les polynômes f_i de degré $\deg(h)$; ils satisfont

$$\operatorname{div}(f_i) \geqslant \operatorname{div}(h) - D.$$

Cette condition se traduit par un système d'équations linéaires en les coefficients des f_i.

Un algorithme inspiré de celui de Brill-Noether, qui représente les diviseurs par leur forme de Chow et utilise des résultants multivariés pour éviter le recours à la factorisation de polynômes dans des grandes extensions du corps de base, a été mis au point par Huang et Ierardi en 1994 ; c'est celui utilisé dans l'algorithme de la section IV.3. Les algorithmes les plus récents de cette famille sont [LGS20] et [Abe+22].

Théorème C.3.2. [HI98, Th. 5.1] Soit C une courbe projective plane de degré d sur un corps k_0. On suppose que tous les points singuliers de C sont ordinaires et définis sur k_0. Soit $D \in \mathrm{Div}_{k_0}(C)$. Écrivons $D = D^+ - D^-$, avec D^+ et D^- effectifs de degré $\leqslant m$. Il existe un algorithme déterministe qui calcule une base du k-espace vectoriel $\mathscr{L}(D)$ constituée d'éléments de $k_0(C)$ en $O(m^7 d^{14})$ opérations dans k_0.

Algorithmes arithmétiques D'autre part, les algorithmes dits arithmétiques représentent les diviseurs comme des ordres dans le corps de fonctions de la courbe. L'algorithme le plus récent de cette famille, dû à Hess [Hes02, Algorithm 8.5], nécessite d'avoir calculé au préalable la clôture intégrale de deux de ces ordres, ce qui peut s'avérer coûteux.

Remarque C.3.3. Notons g le genre de X, et $P_0 \in X(k)$. Le théorème de Riemann-Roch assure que tout diviseur de degré zéro sur X est équivalent à un diviseur de la forme $D - gP_0$, où $D \in \mathrm{Div}(X)$ est effectif. Étant donné un diviseur $E \in \mathrm{Div}^0(X)$, il est possible de calculer un diviseur effectif D et une fonction $f \in k(X)$ tels que $E = D - gP_0 + \mathrm{div}(f)$: il suffit pour cela de calculer l'espace de Riemann-Roch (nécessairement non vide) associé au diviseur $E + gP_0$.

C.3.3 Diviseurs $\mathbb{F}_q$-rationnels

Dans cette section, nous fixons une clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$ et notons $\mathfrak{G}_0$ le groupe $\mathrm{Gal}(\overline{\mathbb{F}_q}|\mathbb{F}_q)$.

Lemme C.3.4. Soient C_0 une courbe projective lisse sur $\mathbb{F}_q$ et $C = C_0 \times_{\mathbb{F}_q} \overline{\mathbb{F}_q}$. Alors il existe dans $\mathrm{Pic}(C)$ un élément $\mathfrak{G}_0$-invariant de degré 1.

Démonstration. Soit $\sigma \in \mathfrak{G}_0$ l'automorphisme de Frobenius. L'endomorphisme $\sigma - \mathrm{id}$ de la jacobienne J_C est une isogénie de noyau $J(\mathbb{F}_q)$, il est donc surjectif. Pour un point $P \in C(\overline{\mathbb{F}_q})$, il existe donc une classe d'un diviseur D de degré 0 tel que $(\sigma - \mathrm{id})D = (\sigma - \mathrm{id})P$. L'élément $P - D \in \mathrm{Pic}^1(C)$ est alors Galois-invariant. □

Lemme C.3.5. Soient k_0 un corps et k une clôture séparable de k_0. Soient C_0 une courbe projective lisse sur k_0 et $C = C_0 \times_{k_0} k$. Si $\mathrm{H}^2(\mathrm{Gal}(k|k_0), k^\times) = 0$ alors toute classe $\mathrm{Gal}(k|k_0)$-invariante dans $\mathrm{Pic}(C)$ contient un diviseur $\mathrm{Gal}(k|k_0)$-invariant.

Démonstration. Soient K_0 et K les corps des fonctions respectifs de C_0 et C. La suite exacte courte

$$0 \to K^\times/k^\times \to \mathrm{Div}\, C \to \mathrm{Pic}\, C \to 0$$

donne la suite exacte longue en cohomologie

$$\mathrm{H}^0(\mathfrak{G}_0, \mathrm{Div}\, C) \to \mathrm{H}^0(\mathfrak{G}_0, \mathrm{Pic}\, C) \to \mathrm{H}^1(\mathfrak{G}_0, K^\times/k^\times).$$

La flèche de droite se décrit de la façon suivante : à la classe d'un diviseur D, elle associe le cocycle $\sigma \mapsto f_{D,\sigma}$ où $D^\sigma - D = \operatorname{div}(f_{D,\sigma})$. Remarquons que $\mathrm{H}^1(\mathfrak{G}_0, K^\times) = \mathrm{H}^1(\mathrm{Gal}(K|K_0), K^\times)$ est nul d'après le théorème 90 de Hilbert [Ser94, III.1, Lem. 1]. La suite exacte longue associée à

$$0 \to k^\times \to K^\times \to K^\times/k^\times \to 0$$

assure alors que $\mathrm{H}^1(\mathrm{Gal}(k|k_0), K^\times/k^\times)$ s'injecte dans $\mathrm{H}^2(\mathrm{Gal}(k|k_0), k^\times)$, qui est nul par hypothèse. □

Corollaire C.3.6. Toute courbe projective lisse sur $\mathbb{F}_q$ possède un diviseur $\mathbb{F}_q$-rationnel de degré 1.

Démonstration. Le théorème de Wedderburn [Bou12, 11.1, Th. 1] assure que

$$\mathrm{H}^2(\mathfrak{G}_0, \overline{\mathbb{F}_q}^\times) = 0.$$

Le résultat découle alors des deux lemmes précédents. □

Le lemme C.3.5 est entièrement effectif, et se réduit à l'association du lemme du serpent avec le théorème 90 de Hilbert. Cependant, lorsque k_0 est fini, l'algorithme fourni par cette preuve est de complexité polynomiale en q, puisqu'il fait notamment intervenir le groupe des 1-cochaînes d'un certain groupe à valeurs dans $\mathbb{F}_q^\times$. Les lemmes suivants fournissent une méthode plus adaptée à la pratique, suggérée par Alain Couvreur.

Lemme C.3.7. Soient k_0 un corps et k une clôture séparable de k_0. Soit C_0 une courbe intègre projective lisse sur k_0. Notons $C = C_0 \times_{k_0} k$. Soit D_1 un diviseur sur C défini sur une extension séparable k_1 de k_0 telle que $C_0 \times_{k_0} k_1$ soit connexe. Soit $D = D_1 + \operatorname{div}(f)$, avec $f \in k_1(C)$, un diviseur k_0-rationnel équivalent à D_1. Soit enfin $b \in k_1$ tel que $\mathrm{tr}_{k_1/k_0}(bf) \neq 0$. Ici, la trace relative d'une fonction rationnelle est définie coefficient par coefficient. Alors

$$\mathrm{tr}_{k_1/k_0} \mathscr{L}_{k_1}(D_1) = \mathrm{tr}_{k_1/k_0}(bf)\mathscr{L}_{k_0}(D).$$

Démonstration. Notons $V = \mathscr{L}_{k_1}(D_1)$. D'une part, pour tout $u \in \mathscr{L}_{k_0}(D)$, $\mathrm{tr}_{k_1/k_0}(bf)u = \mathrm{tr}_{k_1/k_0}(bfu)$ appartient à $\mathrm{tr}_{k_1/k_0}(V)$, et $\dim_{k_0} \mathrm{tr}_{k_1/k_0}(V) \geqslant \dim_{k_0} \mathscr{L}_{k_0}(D)$. D'autre part, comme $V = bf\mathscr{L}_{k_1}(D)$, l'espace $\mathrm{tr}_{k_1/k_0}(V)$ est inclus dans $\mathrm{tr}_{k_1/k_0} \mathscr{L}_{k_1}(D) = \mathrm{tr}_{k_1/k_0}(bf)\mathscr{L}_{k_0}(D)$. □

Lemme C.3.8. Soit C une courbe intègre projective lisse de genre g sur un corps algébriquement clos k. Soit $D \in \mathrm{Div}(C)$ un diviseur de degré $\geqslant 2g$. Notons $V = \mathscr{L}(D)$. Alors

$$D = -\sum_{P \in |C|} \min_{f \in V} v_p(f)P.$$

Démonstration. Notons $D' = -\sum_{P \in C} \min_{f \in V} v_p(f)P$. D'une part, $D \geqslant D'$ car pour tout point P, $v_P(D - D') = v_P(D) + \min_{f \in V} v_P(f) \geqslant 0$. D'autre part, $V \subseteq \mathscr{L}(D')$ car pour tout $f \in V$ et tout point fermé $P \in C$, $v_P(\operatorname{div}(f) + D') = v_P(f) - \min_g v_P(g) \geqslant 0$. Par conséquent, $V = \mathscr{L}(D')$. Supposons que $D \neq D'$; il existe alors des points $P_1, \ldots, P_r$ tels que $D = D' + \sum_i P_i$. Or pour tout i, le théorème de Riemann-Roch assure que

$$\mathscr{L}(D - P_i) \neq \mathscr{L}(D)$$

car $\deg(D - P_i) > 2g - 2$. Comme $\mathscr{L}(D') \subseteq \mathscr{L}(D - P_i)$, c'est absurde. □

Proposition C.3.9. Soit X_0 une courbe intègre lisse sur $k_0 = \mathbb{F}_q$. Notons $X = X_0 \times_{k_0} k$. Supposons donné un modèle plan de X de degré d, ainsi qu'un diviseur k_0-rationnel E de degré 1 sur X. Soient k_1 une extension de $\mathbb{F}_q$ telle que $X_0 \times_{k_0} k_1$ soit connexe et $D_1 \in \mathrm{Div}(X)$ un diviseur défini sur k_1 dont la classe dans $\operatorname{Pic} X$ est $\mathrm{Gal}(k|k_0)$-invariante. Notons $D_1 = D_1^+ - D_1^-$ et $E = E^+ - E^-$ avec D_1^+, D_1^-, E^+, E^- effectifs de degré inférieur à un entier c. Il existe un algorithme de complexité polynomiale en $\log q$, g, c, d et $[k_1 : k_0]$ qui détermine un diviseur k_0-rationnel D équivalent à D_1.

Démonstration. Nous savons qu'il existe un tel diviseur D. Soit h une fonction telle que $D_1 = D + \operatorname{div}(g)$. Par séparabilité de l'extension k_1/k_0, il existe $b \in k_1$ tel que $\operatorname{tr}_{k_1/k_0}(bh) \neq 0$. Soit N un entier tel que $\deg(D_1 + NE) \geqslant 2g$. Appliquons la trace $\operatorname{tr}_{k_1/k_0}$ à l'espace de Riemann-Roch $\mathscr{L}_{k_1}(D_1 + NE)$. L'espace obtenu est $V \coloneqq \operatorname{tr}(bh)\mathscr{L}_{k_0}(D + NE)$ par le lemme C.3.7. Le diviseur $D + NE$ est égal à $-\sum_{P \in X} \min_{f \in V} v_P(f)P$ par le lemme C.3.8. Il suffit donc de calculer une base de V, puis le diviseur de chacun des éléments de cette base, pour obtenir le diviseur k_0-rationnel $D + NE + \operatorname{div}(\operatorname{tr} bh)$ équivalent à $D_1 + NE$. Pour le résultat de complexité, remarquons que $N \leqslant g + c$. □

C.3.4 Diviseur équivalent de support évitant un fermé

Soit X une courbe projective lisse sur un corps k. Soit C un modèle birationnel plan de X de degré d. Soient D un diviseur sur X, et Z un fermé de X. Il est toujours possible de calculer un diviseur D' sur X équivalent à D et de support disjoint de Z ; cette méthode est décrite par exemple dans [Cou09, §3.4]. Soit O un diviseur sur X de degré inférieur à d et de support disjoint de Z. Il suffit de calculer l'espace de Riemann-Roch $\mathscr{L}$ du diviseur $D + 2gO$, qui est de dimension strictement supérieure à 1. Dans $\mathscr{L}$, les fonctions f telles que $\operatorname{div}(f) + D$ ne soit pas disjoint de Z sont contenues dans une réunion d'hyperplans, qu'il suffit d'éviter.

Proposition C.3.10. [Cou09, Lem. 5] Il existe un algorithme déterministe qui, étant donné une courbe plane C sur $\mathbb{F}_q$ et sa normalisée X, un diviseur $\mathbb{F}_q$-rationnel $D = D^+ - D^-$ de degré 0 et un diviseur effectif Z, calcule un diviseur $E = E^+ - E^-$ linéairement équivalent à D et de support disjoint de Z en un nombre d'opérations dans $\mathbb{F}_q$ polynomial en d, $\log q$, $\deg(D^+)$ et $\deg(Z)$. Le degré des diviseurs E^+ et E^- est inférieur à $6gd(\log_q(\deg Z) + 1)$.

C.4 Fonction zêta et comptage de points

Soit $q = p^a$ une puissance d'un nombre premier. Soit X une courbe intègre projective lisse de genre g sur $\mathbb{F}_q$. Il existe différentes méthodes pour compter le nombre de $\mathbb{F}_q$-points ou la fonction zêta de X. L'une d'entre elles est le calcul de la cohomologie étale modulo ℓ, présenté dans ce manuscrit, pour $O(g \log q)$ valeurs de ℓ. L'avantage des méthodes ℓ-adiques est de proposer une complexité polynomiale en $\log q$; elles sont cependant exponentielles en g. Pour une courbe quelconque, la meilleure de ces méthodes est celle de Huang et Ierardi présentée dans la section IV.3. Pour les courbes hyperelliptiques, il existe des algorithmes plus efficaces, comme celui d'Adleman et Huang. À l'aide de la représentation de Mumford des diviseurs, il calcule directement les points de ℓ-torsion de la jacobienne de la courbe en question.

Proposition C.4.1. [AH01, Th. 4.1] Soit q une puissance d'un nombre premier impair. Il existe un algorithme déterministe qui, étant donné un polynôme $f \in \mathbb{F}_q[t]$ de degré $2g + 1$ sans racine multiple, renvoie le polynôme caractéristique de l'endomorphisme de Frobenius sur la jacobienne de la courbe hyperelliptique d'équation affine $y^2 = f(x)$ en $(\log q)^{O(g^2 \log g)}$ opérations.

Il existe également des méthodes p-adiques, comme celles décrites dans [Wan08] ou [Tui15]. La complexité de la plupart de ces algorithmes est polynomiale en p et en g. Cependant, Harvey a présenté en 2014 une méthode dont la complexité moyenne (sur p) est polynomiale en $\log p$.

Théorème C.4.2. [Har14, Th. 1] Il existe un algorithme déterministe explicite vérifiant les propriétés suivantes. Étant donné des entiers $N \geqslant 3$, $g \geqslant 1$, et un polynôme $Q \in \mathbb{Z}[x]$ définissant une courbe hyperelliptique X sur $\mathbb{Q}$ d'équation $y^2 = Q(x)$ de genre g, il calcule pour tous les premiers impairs $p < N$ ne divisant pas le discriminant de Q la fonction zêta de la réduction de X modulo p. L'algorithme nécessite $g^{8+\varepsilon} N \log^2(N) \log^{1+\varepsilon}(\|Q\|_\infty N)$ opérations binaires, où $\|Q\|_\infty$ désigne le maximum des valeurs absolues des coefficients de Q.

Comme le nombre de nombres premiers $p < N$ est équivalent à $N/\log(N)$, le temps moyen pour chaque premier p est $g^{8+\varepsilon}\log^3(N)\log^{1+\varepsilon}(\|Q\|_\infty N)$. Plus récemment, Harvey et Sutherland ont proposé et implémenté une méthode pour calculer la matrice de Hasse-Witt modulo p d'une telle courbe hyperelliptique X, et en déduire la réduction modulo p du polynôme caractéristique du Frobenius sur X [HS14] ; leur algorithme est particulièrement efficace dans la pratique pour les courbes de genre 2 ou 3.

Bibliographie

[Abe+22] Simon Abelard et al. "Computing Riemann–Roch Spaces via Puiseux Expansions". In : *Journal of Complexity* (avr. 2022), p. 101666. DOI : 10.1016/j.jco.2022.101666.

[Ach15] Piotr Achinger. "$K(\pi, 1)$ Spaces in Algebraic Geometry". Thèse de doct. University of California, Berkeley, 2015.

[Ach17] Piotr Achinger. "Wild Ramification and K(π,1) Spaces". In : *Inventiones mathematicae* 210.2 (nov. 2017), p. 453-499. DOI : 10.1007/s00222-017-0733-5.

[AG15] Ahmed Abbes et Michel Gros. *Topos co-évanescents et généralisations*. 2015. arXiv : 1107.2380 [math].

[AH01] Leonard M. Adleman et Ming-Deh Huang. "Counting Points on Curves and Abelian Varieties Over Finite Fields". In : *Journal of Symbolic Computation* 32.3 (sept. 2001), p. 171-189. DOI : 10.1006/jsco.2001.0470.

[And02] Greg W. Anderson. "Abeliants and Their Application to an Elementary Construction of Jacobians". In : *Advances in Mathematics* 172.2 (déc. 2002), p. 169-205. DOI : 10.1016/S0001-8708(02)00024-5.

[BC21] Frauke M. Bleher et Ted Chinburg. "Cup Products on Curves over Finite Fields". In : *arXiv :2101.00329 [math]* (jan. 2021). arXiv : 2101.00329 [math].

[BCS97] Peter Bürgisser, Michael Clausen et Mohammad Amin Shokrollahi. *Algebraic Complexity Theory*. Sous la dir. de S. S. Chern et al. T. 315. Grundlehren Der Mathematischen Wissenschaften. Berlin, Heidelberg : Springer Berlin Heidelberg, 1997. DOI : 10.1007/978-3-662-03338-8.

[BFS15] Magali Bardet, Jean-Charles Faugère et Bruno Salvy. "On the Complexity of the F 5 Gröbner Basis Algorithm". In : *Journal of Symbolic Computation* 70 (sept. 2015), p. 49-70. DOI : 10.1016/j.jsc.2014.09.025.

[BLR90] Siegfried Bosch, Werner Lütkebohmert et Michel Raynaud. *Néron Models*. Berlin, Heidelberg : Springer Berlin Heidelberg, 1990. DOI : 10.1007/978-3-642-51438-8.

[BN74] A. Brill et M. Nöther. "Ueber die algebraischen Functionen und ihre Anwendung in der Geometrie". In : *Mathematische Annalen* 7.2-3 (juin 1874), p. 269-310. DOI : 10.1007/BF02104804.

[Bou12] N. Bourbaki. *Algèbre*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012. DOI : 10.1007/978-3-540-35316-4.

[Bro82] Kenneth S. Brown. *Cohomology of Groups*. 3. [Nachdr.] Graduate Texts in Mathematics 87. New York Heidelberg : Springer, 1982.

[Bru12] Peter Bruin. "Computing in Picard Groups of Projective Curves over Finite Fields". In : *Mathematics of Computation* 82.283 (sept. 2012), p. 1711-1756. doi : 10.1090/S0025-5718-2012-02650-0.

[BS92] Dave Bayer et Mike Stillman. "Computation of Hilbert Functions". In : *Journal of Symbolic Computation* 14.1 (juil. 1992), p. 31-50. doi : 10.1016/0747-7171(92)90024-X.

[BW93] Thomas Becker et Volker Weispfenning. *Gröbner Bases*. T. 141. Graduate Texts in Mathematics. New York, NY : Springer New York, 1993. doi : 10.1007/978-1-4612-0913-3.

[Can88] John Canny. "Some Algebraic and Geometric Computations in PSPACE". In : *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing - STOC '88*. Chicago, Illinois, United States : ACM Press, 1988, p. 460-469. doi : 10.1145/62212.62257.

[CF98] J.W.S. Cassels et E.V. Flynn. "Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2". In : *Proceedings of the Edinburgh Mathematical Society* 41.1 (fév. 1998), p. 207-207. doi : 10.1017/S0013091500019519.

[Cho54] Wei-Liang Chow. "The Jacobian Variety of an Algebraic Curve". In : *American Journal of Mathematics* 76.2 (1954), p. 453-476.

[Cou09] Jean-Marc Couveignes. "Linearizing Torsion Classes in the Picard Group of Algebraic Curves over Finite Fields". In : *Journal of Algebra* 321.8 (avr. 2009), p. 2085-2118. doi : 10.1016/j.jalgebra.2008.09.032. arXiv : 0706.0272.

[CSF12] Zhengjun Cao, Qian Sha et Xiao Fan. "Adleman-Manders-Miller Root Extraction Method Revisited". In : *Information Security and Cryptology*. Sous la dir. de Chuan-Kun Wu, Moti Yung et Dongdai Lin. T. 7537. Berlin, Heidelberg : Springer Berlin Heidelberg, 2012, p. 77-85. doi : 10.1007/978-3-642-34704-7_6.

[CW90] Don Coppersmith et Shmuel Winograd. "Matrix Multiplication via Arithmetic Progressions". In : *Journal of Symbolic Computation* 9.3 (mar. 1990), p. 251-280. doi : 10.1016/S0747-7171(08)80013-2.

[Das22] Soumyadip Das. *Galois Covers of Singular Curves in Positive Characteristics*. Mar. 2022. arXiv : 2203.11870 [math].

[Dic+91] Alicia Dickenstein et al. "The Membership Problem for Unmixed Polynomial Ideals Is Solvable in Single Exponential Time". In : *Discrete Applied Mathematics* 33.1-3 (nov. 1991), p. 73-94. doi : 10.1016/0166-218X(91)90109-A.

[Die08] Claus Diem. "On Arithmetic and the Discrete Logarithm Problem in Class Groups of Curves". Habilitation. Universität Leipzig, 2008.

[Dix+99] J. D. Dixon et al. *Analytic Pro-P Groups*. Second. Cambridge University Press, août 1999. doi : 10.1017/CBO9780511470882.

[DK02] Harm Derksen et Gregor Kemper. *Computational Invariant Theory*. T. 130. Encyclopaedia of Mathematical Sciences. Berlin, Heidelberg : Springer Berlin Heidelberg, 2002. doi : 10.1007/978-3-662-04958-7.

[Dub90] Thomas W. Dubé. "The Structure of Polynomial Ideals and Gröbner Bases". In : *SIAM Journal on Computing* 19.4 (août 1990), p. 750-773. doi : 10.1137/0219053.

[EC11] Bas EDIXHOVEN et Jean-Marc COUVEIGNES, éd. *Computational Aspects of Modular Forms and Galois Representations : How One Can Compute in Polynomial Time the Value of Ramanujan's Tau at a Prime (AM-176)*. Princeton : Princeton University Press, déc. 2011. DOI : 10.1515/9781400839001.

[EGA 4_2] Alexander GROTHENDIECK. "Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Seconde partie". In : *Publications Mathématiques de l'IHÉS* 24 (1965), p. 5-231.

[EGA 4_4] Alexander GROTHENDIECK. "Éléments de géométrie algébrique : IV. Étude locale des schémas et des morphismes de schémas, Quatrième partie". In : *Publications Mathématiques de l'IHÉS* 24 (1965), p. 5-231.

[EGAIII_1] Alexander GROTHENDIECK. "Eléments de géométrie algébrique : III. Etude cohomologique des faisceaux cohérents, Première partie". In : *Institut des Hautes Études Scientifiques*. Publications Mathématiques de l'IHÉS 11 (1961), p. 5-167.

[ESS22] Hélène ESNAULT, Mark SHUSTERMAN et Vasudevan SRINIVAS. "Finite Presentation of the Tame Fundamental Group". In : *Selecta Mathematica* 28.2 (avr. 2022), p. 37. DOI : 10.1007/s00029-021-00732-4.

[Fis01] Gerd FISCHER. *Plane algebraic curves*. Providence : American Mathematical Society, 2001.

[FJ08] Michael D. FRIED et Moshe JARDEN. *Field Arithmetic*. 3rd ed., rev. Ergebnisse Der Mathematik Und Ihrer Grenzgebiete, A Series of Modern Surveys in Mathematics v. 11. OCLC : ocn232361356. Berlin : Springer, 2008.

[FKD13] Eberhard FREITAG, Reinhardt KIEHL et Jean Alexandre DIEUDONNÉ. *Etale Cohomology and the Weil Conjecture*. Softcover reprint of the hardcover 1st edition 1988. Ergebnisse Der Mathematik Und Ihrer Grenzgebiete 3. Folge, Band 13. Berlin Heidelberg : Springer-Verlag Berlin Heidelberg GmbH, 2013.

[Fu15] Lei FU. *Etale Cohomology Theory*. Revised edition. Nankai Tracts in Mathematics 14. New Jersey London Singapore Beijing Shanghai Hong Kong Taipei Chennai : World Scientific, 2015.

[FW89] William FULTON et Richard WEISS. *Algebraic Curves : An Introduction to Algebraic Geometry*. Advanced Book Classics. "This book was originally published as part of the Mathematics lecture note series.". Redwood City, Calif : Addison-Wesley Pub. Co., Advanced Book Program, 1989.

[Gro57] Alexander GROTHENDIECK. "Sur Quelques Points d'algèbre Homologique, I". In : *Tohoku Mathematical Journal* 9.2 (jan. 1957). DOI : 10.2748/tmj/1178244839.

[GW10] Ulrich GÖRTZ et Torsten WEDHORN. *Algebraic Geometry I : Schemes With Examples and Exercises*. Wiesbaden : Vieweg+Teubner, 2010. DOI : 10.1007/978-3-8348-9722-0.

[Har08] Robin HARTSHORNE. *Algebraic Geometry*. Fourteenth. Graduate Texts in Mathematics 52. New York, NY : Springer, 2008.

[Har14] David HARVEY. "Counting Points on Hyperelliptic Curves in Average Polynomial Time". In : *Annals of Mathematics* 179.2 (mar. 2014), p. 783-803. DOI : 10.4007/annals.2014.179.2.7.

[Har94] David HARBATER. "Abhyankar's Conjecture on Galois Groups over Curves". In : *Inventiones Mathematicae* 117.1 (déc. 1994), p. 1-25. DOI : 10.1007/BF01232232.

[Hes02] F. HESS. "Computing Riemann–Roch Spaces in Algebraic Function Fields and Related Topics". In : *Journal of Symbolic Computation* 33.4 (avr. 2002), p. 425-445. DOI : 10.1006/jsco.2001.0513.

[HI98] Ming-Deh HUANG et Doug IERARDI. "Counting Points on Curves over Finite Fields". In : *Journal of Symbolic Computation* 25.1 (jan. 1998), p. 1-21. DOI : 10.1006/jsco.1997.0164.

[HL17] Hau-Wen HUANG et Wen-Ching Winnie LI. "A Unified Approach to the Galois Closure Problem". In : *Journal of Number Theory* 180 (nov. 2017), p. 251-279. DOI : 10.1016/j.jnt.2017.04.011.

[HS14] David HARVEY et Andrew V. SUTHERLAND. "Computing Hasse–Witt Matrices of Hyperelliptic Curves in Average Polynomial Time". In : *LMS Journal of Computation and Mathematics* 17.A (2014), p. 257-273. DOI : 10.1112/S1461157014000187.

[Hv21] David HARVEY et Joris VAN DER HOEVEN. "Integer Multiplication in Time $O(N \log N)$". In : *Annals of Mathematics* 193.2 (mar. 2021). DOI : 10.4007/annals.2021.193.2.4.

[Ier89] D. IERARDI. "Quantifier Elimination in the Theory of an Algebraically-Closed Field". In : *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing - STOC '89*. Seattle, Washington, United States : ACM Press, 1989, p. 138-147. DOI : 10.1145/73007.73020.

[Igu56] Jun-Ichi IGUSA. "Fibre Systems of Jacobian Varieties". In : *American Journal of Mathematics* 78.1 (jan. 1956), p. 171. DOI : 10.2307/2372489.

[IK93] D. IERARDI et D. KOZEN. "Synthesis of Parallel Algorithms". In : sous la dir. de John H. REIF. Morgan Kaufmann, 1993. Chap. Parallel resultant computation.

[ILO] Luc ILLUSIE et al., éd. *Travaux de Gabber sur l'uniformisation locale et la cohomologie étale des schémas quasi-excellents : séminaire à l'École polytechnique 2006-2008*. Astérisque 363-364. "Publié avec le concours du Centre National de la Recherche Scientifique"–Title page. Paris, France : Société mathématique de France, 2014.

[Jin17] Jinbi JIN. "Computability of the Euler-Poincaré Characteristic". PhD Thesis. Universiteit Leiden, 2017.

[Jin20] Jinbi JIN. "Computation of Étale Cohomology on Curves in Single Exponential Time". In : *Journal de Théorie des Nombres de Bordeaux* 32.2 (oct. 2020), p. 311-354. DOI : 10.5802/jtnb.1124.

[Jon96] Aise Johan de JONG. "Smoothness, semi-stability and alterations". en. In : *Publications Mathématiques de l'IHÉS* 83 (1996), p. 51-93.

[Jon98] Theo de JONG. "An Algorithm for Computing the Integral Closure". In : *Journal of Symbolic Computation* 26.3 (sept. 1998), p. 273-277. DOI : 10.1006/jsco.1998.0211.

[KM06] Kamal KHURI-MAKDISI. "Asymptotically Fast Group Operations on Jacobians of General Curves". In : *arXiv :math/0409209* (juil. 2006). arXiv : math/0409209.

[KM08] Changho KEEM et Gerriet MARTENS. "Curves without Plane Model of Small Degree". In : *Mathematische Nachrichten* 281.12 (déc. 2008), p. 1791-1798. DOI : 10.1002/mana.200610714.

[Kol07] János KOLLÁR. *Lectures on Resolution of Singularities*. Annals of Mathematics Studies 166. Princeton : Princeton University Press, 2007.

[Koz94] Dexter KOZEN. "Efficient Resolution of Singularities of Plane Curves". In : *Foundation of Software Technology and Theoretical Computer Science*. Sous la dir. de Gerhard GOOS et al. T. 880. Berlin, Heidelberg : Springer Berlin Heidelberg, 1994, p. 1-11. DOI : 10.1007/3-540-58715-2_109.

[KPR16] Stefan Kratsch, Geevarghese Philip et Saurabh Ray. "Point Line Cover : The Easy Kernel Is Essentially Tight". In : *ACM Transactions on Algorithms* 12.3 (juin 2016), p. 1-16. doi : 10.1145/2832912.

[Lan02] Serge Lang. *Algebra*. Sous la dir. de S. Axler, F. W. Gehring et K. A. Ribet. T. 211. Graduate Texts in Mathematics. New York, NY : Springer New York, 2002. doi : 10.1007/978-1-4613-0041-0.

[Len83] A. K. Lenstra. "Factoring Polynomials over Algebraic Number Fields". In : *Computer Algebra*. Sous la dir. de J. A. van Hulzen. Berlin, Heidelberg : Springer Berlin Heidelberg, 1983, p. 245-254.

[Len84] Arjen K. Lenstra. "Factoring Multivariate Polynomials over Algebraic Number Fields". In : *Mathematical Foundations of Computer Science 1984*. Sous la dir. de M. P. Chytil et V. Koubek. T. 176. Berlin/Heidelberg : Springer-Verlag, 1984, p. 389-396. doi : 10.1007/BFb0030321.

[Len85] A.K. Lenstra. "Factoring Multivariate Polynomials over Finite Fields". In : *Journal of Computer and System Sciences* 30.2 (avr. 1985), p. 235-248. doi : 10.1016/0022-0000(85)90016-9.

[LGS20] Aude Le Gluher et Pierre-Jean Spaenlehauer. "A Fast Randomized Geometric Algorithm for Computing Riemann-Roch Spaces". In : *Mathematics of Computation* 89.325 (fév. 2020), p. 2399-2433. doi : 10.1090/mcom/3517.

[Lim21] David Benjamin Lim. *The étale cohomology of curves over finite fields*. 2021.

[LLL82] A. K. Lenstra, H. W. Lenstra et L. Lovász. "Factoring Polynomials with Rational Coefficients". In : *Mathematische Annalen* 261.4 (déc. 1982), p. 515-534. doi : 10.1007/BF01457454.

[Lor96] Dino Lorenzini. *An Invitation to Arithmetic Geometry*. Online-ausg. Providence, RI : American Mathematical Society, 1996.

[Mil06] J. S. Milne. *Arithmetic Duality Theorems*. 2. ed. First publ. by Academic Press, 1986. Charleston, SC : Booksurge, 2006.

[Mil08] James S. Milne. *Abelian Varieties (v2.00)*. Disponible à l'adresse www.jmilne.org/math/. 2008.

[Mil13] James S. Milne. *Lectures on Etale Cohomology (v2.21)*. Disponible à l'adresse www.jmilne.org/math/. 2013.

[Mil80] J. S. Milne. *Étale Cohomology*. Princeton Mathematical Series 33. Princeton, N.J : Princeton University Press, 1980.

[MO15] David A. Madore et Fabrice Orgogozo. "Calculabilité de La Cohomologie Étale modulo ℓ". In : *Algebra & Number Theory* 9.7 (sept. 2015), p. 1647-1739. doi : 10.2140/ant.2015.9.1647. arXiv : 1304.5376.

[Mum07] David Mumford. *Tata Lectures on Theta II*. Boston, MA : Birkhäuser Boston, 2007. doi : 10.1007/978-0-8176-4578-6.

[Mum08] David Mumford. *Abelian Varieties*. 2. ed., corr. repr. Tata Institute of Fundamental Research : Studies in Mathematics 5. New Delhi : Hindustan Book Agency, 2008.

[Mum15] David Mumford. *Algebraic Geometry. 2*. Texts and Readings in Mathematics 73. New Delhi, India : Hindustan Book Agency (India), 2015.

[Nag62] Masayoshi Nagata. "Imbedding of an Abstract Variety in a Complete Variety". In : *Kyoto Journal of Mathematics* 2.1 (jan. 1962). doi : 10.1215/kjm/1250524969.

[Neu13] Jürgen NEUKIRCH. *Class Field Theory*. Berlin, Heidelberg : Springer Berlin Heidelberg, 2013. DOI : 10.1007/978-3-642-35437-3.

[Nic13] Jean-Louis NICOLAS. "On Landau's Function g(n)". In : *The Mathematics of Paul Erdős I*. Sous la dir. de Ronald L. GRAHAM, Jaroslav NEŠETŘIL et Steve BUTLER. New York, NY : Springer New York, 2013, p. 207-220. DOI : 10.1007/978-1-4614-7258-2_14.

[Odi89a] Piergiorgio ODIFREDDI. *Classical Recursion Theory : The Theory of Functions and Sets of Natural Numbers*. Studies in Logic and the Foundations of Mathematics v. 125, 143. North-Holland, 1989.

[Odi89b] Piergiorgio ODIFREDDI. *Classical Recursion Theory, Volume II*. Studies in Logic and the Foundations of Mathematics 143. North-Holland, 1989.

[PTv15] Bjorn POONEN, Damiano TESTA et Ronald VAN LUIJK. "Computing Néron–Severi Groups and Cycle Class Groups". In : *Compositio Mathematica* 151.4 (avr. 2015), p. 713-734. DOI : 10.1112/S0010437X14007878.

[Sch94] Claus SCHEIDERER. *Real and Étale Cohomology*. Lecture Notes in Mathematics 1588. Berlin : Springer, 1994.

[Ser75] Jean-Pierre SERRE. *Groupes Algébriques et Corps de Classes*. 2e éd. revue et corrigée. Actualités Scientifiques et Industrielles 1264. Paris : Hermann, 1975.

[Ser89] Jean-Pierre SERRE. *Algèbre Locale, Multiplicités : Cours Au Collège de France, 1957 - 1958*. 3. éd., 2. corr. print. Lecture Notes in Mathematics 11. OCLC : 21060924. Berlin u.a : Springer, 1989.

[Ser94] Jean-Pierre SERRE. *Cohomologie Galoisienne*. T. 5. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. DOI : 10.1007/BFb0108758.

[SGA1] Alexander GROTHENDIECK et Michèle RAYNAUD. *Revêtements Etales et Groupe Fondamental. Séminaire de Géométrie Algébrique du Bois-Marie 1960-1961. (SGA 1)*. T. 224. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1971. DOI : 10.1007/BFb0058656.

[SGA4$_1$] Alexander GROTHENDIECK et Jean-Louis VERDIER. *Théorie Des Topos et Cohomologie Etale Des Schémas. Séminaire de Géométrie Algébrique Du Bois-Marie 1963-1964 (SGA 4). Tome 1 : Exposés I-IV*. T. 269. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1972. DOI : 10.1007/BFb0081551.

[SGA4$_2$] Jean-Louis VERDIER, Bernard SAINT-DONAT et Alexander GROTHENDIECK. *Théorie Des Topos et Cohomologie Etale Des Schémas. Séminaire de Géométrie Algébrique Du Bois-Marie 1963-1964 (SGA 4). Tome 2 : Exposés V-VIII*. T. 270. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1972. DOI : 10.1007/BFb0061319.

[SGA4$_3$] Pierre DELIGNE et Michael ARTIN. *Théorie Des Topos et Cohomologie Etale Des Schémas. Séminaire de Géométrie Algébrique Du Bois-Marie 1963-1964 (SGA 4). Tome 3 : Exposés IX-XIX*. T. 305. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1973. DOI : 10.1007/BFb0070714.

[SGA4$\frac{1}{2}$] Pierre DELIGNE. *Cohomologie Etale. Séminaire de Géométrie Algébrique du Bois-Marie (SGA 4 1/2)*. Sous la dir. d'A. DOLD et B. ECKMANN. T. 569. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1977. DOI : 10.1007/BFb0091516.

[SGA7$_2$] Pierre DELIGNE et Nicholas KATZ. *Groupes de Monodromie En Géométrie Algébrique. Séminaire de Géométrie Algébrique Du Bois-Marie 1967-1969. (SGA 7 II)*. T. 340. Lecture Notes in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 1973. DOI : 10.1007/BFb0060505.

[Sha94] Igor R. Shafarevich. *Basic Algebraic Geometry 1*. Berlin, Heidelberg : Springer Berlin Heidelberg, 1994. doi : 10.1007/978-3-642-57908-0.

[Sho88] Victor Shoup. "New Algorithms for Finding Irreducible Polynomials over Finite Fields". In : *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*. White Plains, NY, USA : IEEE, 1988, p. 283-290. doi : 10.1109/SFCS.1988.21944.

[Sho90] Victor Shoup. "On the Deterministic Complexity of Factoring Polynomials over Finite Fields". In : *Information Processing Letters* 33.5 (jan. 1990), p. 261-267. doi : 10.1016/0020-0190(90)90195-4.

[Sho94] Victor Shoup. "Fast Construction of Irreducible Polynomials over Finite Fields". In : *Journal of Symbolic Computation* 17.5 (mai 1994), p. 371-391. doi : 10.1006/jsco.1994.1025.

[SM98] Arne Storjohann et Thom Mulders. "Fast Algorithms for Linear Algebra Modulo N". In : *Algorithms — ESA' 98*. Sous la dir. de Gianfranco Bilardi et al. Berlin, Heidelberg : Springer Berlin Heidelberg, 1998, p. 139-150.

[Stacks] The Stacks Project authors. *Stacks Project*. https://stacks.math.columbia.edu. 2018.

[Ste05] Allan Steel. "Conquering Inseparability : Primary Decomposition and Multivariate Factorization over Algebraic Function Fields of Positive Characteristic". In : *Journal of Symbolic Computation* 40.3 (sept. 2005), p. 1053-1075. doi : 10.1016/j.jsc.2005.03.002.

[Sti02] Jakob Stix. "Projective Anabelian Curves in Positive Characteristic and Descent Theory for Log-Étale Covers". In : *Bonner Mathematische Schriften* 354 (2002).

[Sti09] Henning Stichtenoth. *Algebraic Function Fields and Codes*. T. 254. Graduate Texts in Mathematics. Berlin, Heidelberg : Springer Berlin Heidelberg, 2009. doi : 10.1007/978-3-540-76878-4.

[Sto96] Arne Storjohann. "Near Optimal Algorithms for Computing Smith Normal Forms of Integer Matrices". In : *Proceedings of the 1996 International Symposium on Symbolic and Algebraic Computation - ISSAC '96*. Zurich, Switzerland : ACM Press, 1996, p. 267-274. doi : 10.1145/236869.237084.

[Sza09] Tamas Szamuely. *Galois Groups and Fundamental Groups*. Cambridge : Cambridge University Press, 2009. doi : 10.1017/CBO9780511627064.

[Tho01] R. P. Thomas. *Derived Categories for the Working Mathematician*. Oct. 2001. arXiv : math/0001045.

[Tui15] Jan Tuitman. "Counting Points on Curves Using a Map to $\mathbb{P}^1$". In : *Mathematics of Computation* 85.298 (juil. 2015), p. 961-981. doi : 10.1090/mcom/2996.

[Vas06] Wolmer Vasconcelos. *Integral Closure : Rees Algebras, Multiplicities, Algorithms*. Springer Monographs in Mathematics. OCLC : 990606371. Berlin : Springer, 2006.

[vG13] Joachim von zur Gathen et Jürgen Gerhard. *Modern Computer Algebra*. Third. Cambridge : Cambridge University Press, 2013. doi : 10.1017/CBO9781139856065.

[VW12] Virginia Vassilevska Williams. "Multiplying Matrices Faster than Coppersmith-Winograd". In : *Proceedings of the 44th Symposium on Theory of Computing - STOC '12*. Version corrigée disponible à l'adresse https://people.csail.mit.edu/virgi/matrixmult-f.pdf. New York, New York, USA : ACM Press, 2012, p. 887. doi : 10.1145/2213977.2214056.

[Wan08] Daqing WAN. "Algorithmic Theory of Zeta Functions over Finite Fields". In : *Algorithmic Number Theory : Lattices, Number Fields, Curves and Cryptography*. Sous la dir. de Joe P. BUHLER et P. STEVENHAGEN. Mathematical Sciences Research Institute Publications 44. Cambridge : Cambridge Univ. Press, 2008, p. 551-578.

[Wan90] Daqing WAN. "Factoring Multivariate Polynomials over Large Finite Fields". In : *Mathematics of Computation* 54.190 (1990), p. 755-770. DOI : 10.1090/S0025-5718-1990-1011448-0.

[Wei48] André WEIL. *Variétés Abéliennes et Courbes Algébriques*. Publications de l'Institut de Mathématiques de l'Université de Strasbourg. Actualités Industrielles et Scientifiques 1064. Hermann, 1948.

[Wei94] Charles A. WEIBEL. *An Introduction to Homological Algebra*. Cambridge Studies in Advanced Mathematics 38. Cambridge : Cambridge university press, 1994.

[Yek19] Amnon YEKUTIELI. *Derived Categories*. First. Cambridge University Press, déc. 2019. DOI : 10.1017/9781108292825.

[YNT89] Kazuhiro YOKOYAMA, Masayuki NORO et Taku TAKESHIMA. "Computing Primitive Elements of Extension Fields". In : *Journal of Symbolic Computation* 8.6 (déc. 1989), p. 553-580. DOI : 10.1016/S0747-7171(89)80061-6.

[Zis21] Charilaos ZISOPOULOS. "Complexity of Linear Algebra of Rational Function Matrices". Mém. de mast. Universität des Saarlandes, 2021.