

Algebra & Number Theory

Volume 9

2015

No. 7

**Calculabilité de la
cohomologie étale modulo ℓ**

David A. Madore et Fabrice Orgogozo



Calculabilité de la cohomologie étale modulo ℓ

David A. Madore et Fabrice Orgogozo

À Jean-Louis Colliot-Thélène, qui nous a beaucoup appris

Soient X un schéma algébrique sur un corps algébriquement clos et ℓ un nombre premier inversible sur X . D'après le théorème 1.1 de (SGA 4 $\frac{1}{2}$, Th. finitude), les groupes de cohomologie étale $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ sont de dimension finie. Utilisant une variante ℓ -adique des bons voisinages d'Artin et des résultats élémentaires sur la cohomologie des pro- ℓ groupes, on exprime la cohomologie de X comme colimite bien contrôlée de celle de topos construits sur des BG , où les G sont des ℓ -groupes finis calculables. On en déduit que les nombres de Betti modulo ℓ de X sont algorithmiquement calculables (au sens de Church–Turing). La première partie du texte est consacrée à la démonstration de ce fait et de quelques compléments naturels. Elle s'appuie sur les outils de la seconde partie, dédiée à la géométrie algébrique effective.

Let X be an algebraic scheme over an algebraically closed field and ℓ a prime number invertible on X . According to Theorem 1.1 of (SGA 4 $\frac{1}{2}$, Th. finitude), the étale cohomology groups $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ are finite-dimensional. Using an ℓ -adic variant of Artin's good neighborhoods and elementary results on the cohomology of pro- ℓ groups, we express the cohomology of X as a well controlled colimit of that of toposes constructed on BG where the G are computable finite ℓ -groups. From this, we deduce that the Betti numbers modulo ℓ of X are algorithmically computable (in the sense of Church and Turing). The proof of this fact, along with certain related results, occupies the first part of this paper. This relies on the tools collected in the second part, which deals with computational algebraic geometry.

MSC2010: primary 14F20; secondary 03D99, 12G05, 12Y05, 13P10, 14A20, 14F35, 18G30, 20E18, 55P20, 55T05.

Mots-clefs: cohomologie étale, cohomologie galoisienne, descente cohomologique, suite spectrale, schéma simplicial, groupe profini, espace d'Eilenberg–MacLane, voisinage d'Artin, champ algébrique, gerbe, géométrie algébrique effective, calculabilité, étale cohomology, Galois cohomology, cohomological descent, spectral sequence, simplicial scheme, profinite group, Eilenberg–MacLane space, Artin's neighborhood, stack, effective algebraic geometry, computability.

Introduction	1648
I. Cohomologie étale	1653
1. $K(\pi, 1)$ pro- ℓ	1653
2. Calculabilité du H^1	1666
3. Série ℓ -centrale descendante et groupe fondamental	1668
4. Cohomologie ℓ -étale n -approchée d'un schéma simplicial	1673
5. Systèmes essentiellement constants	1677
6. Approximation d'un pro- ℓ -groupe par ses quotients finis	1680
7. Calcul de la cohomologie d'une polycourbe ℓ -élémentaire	1685
8. Descente	1687
9. Fonctorialité	1690
10. Structure de l'algorithme et exemple simple	1692
11. Compléments	1694
II. Algèbre commutative et géométrie algébrique effectives	1704
12. Corps et extensions de corps	1704
13. Modules de type fini sur une k -algèbre de type fini	1711
14. Algèbres de type fini sur un corps: description algorithmique	1716
15. Algèbre commutative effective	1720
16. Schémas de type fini sur un corps: description algorithmique	1726
17. Géométrie algébrique effective	1731
Remerciements	1733
Bibliographie	1733

Introduction

L'objet principal de ce texte est de démontrer le théorème suivant, ainsi que la variante relative 0.9.

Théorème 0.1. *Il existe un algorithme calculant la cohomologie étale $H^i(X, \mathbb{F}_\ell)$ à coefficients dans \mathbb{F}_ℓ d'un schéma algébrique X sur un corps algébriquement clos de caractéristique différente de ℓ , ainsi que l'application $H^i(X, \mathbb{F}_\ell) \rightarrow H^i(Y, \mathbb{F}_\ell)$ déduite par fonctorialité d'un morphisme $Y \rightarrow X$.*

Bien entendu, il faut préciser l'énoncé et notamment ce qu'on entend par « calculer » : nous rappelons dans la [partie II](#) les faits essentiels dont nous aurons besoin sur les corps calculables et la calculabilité des opérations algébriques. Calculer le groupe $H^i(X, \mathbb{F}_\ell)$ signifie notamment en calculer la dimension, en fonction de i, ℓ et des équations de X , et calculer l'application $H^i(X, \mathbb{F}_\ell) \rightarrow H^i(Y, \mathbb{F}_\ell)$ signifie en calculer la matrice dans une base déterminée par l'algorithme. (Voir [0.4](#) ci-dessous et [¶ 9.1.2–9.1.3](#) pour des précisions.)

L'énoncé précédent répond notamment à la question posée en [Poonen, Testa et van Luijk 2015, hypothèse 7.4] et également considérée dans [Edixhoven et Couveignes 2011, chapitre 1 et chapitre 15, p. 401], où l'accent est mis sur la dépendance du temps d'exécution en ℓ .

En caractéristique nulle ce résultat est déjà connu : voir par exemple [Simpson 2008, corollaire 2.5] ou [Poonen, Testa et van Luijk 2015, §7.2], qui calcule aussi l'action galoisienne lorsque le schéma X est obtenu par extension des scalaires d'un corps de caractéristique nulle à une clôture algébrique. Pour une discussion du problème de la calculabilité des groupes d'homotopie ou d'homologie en topologie algébrique, voir par exemple [Sergeraert 1994].

0.2. Rappelons [Deligne 1980, 5.2.2] brièvement une définition à la Čech de ces groupes de cohomologie étale. Soit X une variété algébrique sur un corps algébriquement clos dénombrable de caractéristique $p \neq \ell$ (par exemple $\overline{\mathbb{F}}_p$). Il existe un système projectif, indexé par les entiers naturels α , de recouvrements étales $X_\alpha \rightarrow X$, cofinal au sens suivant : pour tout $U \rightarrow X$ étale, il existe une factorisation d'un $X_\alpha \rightarrow X$ à travers U . Notons $X_{\alpha\bullet}$ le cosquelette du morphisme $X_\alpha \rightarrow X$ c'est-à-dire le schéma simplicial $X_{\alpha n} := X_\alpha \times_X \cdots \times_X X_\alpha$ ($n + 1$ facteurs). La cohomologie de Čech $\check{H}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ est, par définition, celle de l'ensemble simplicial $\pi_0(X_{\alpha\bullet})$. (Pour tout ensemble simplicial, on peut considérer le $\mathbb{Z}/\ell\mathbb{Z}$ -module cosimplicial naturellement associé puis le complexe dont les dérivations sont les sommes alternées des faces (cf. [SGA 4₂ 1972, V, §1.0 et §2.3; Milne 1980, III, §2]).) Si X est quasi-projective, il résulte de [Artin 1971, corollaire 4.2] que le groupe $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ est isomorphe à la colimite des $\check{H}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$. Le problème auquel on est immédiatement confronté est que, donnés k , les $X_\alpha \rightarrow X$ et ℓ , il n'est *a priori* pas évident de calculer deux entiers $\alpha \leq \beta$ tels que $H^i(X, \mathbb{Z}/\ell\mathbb{Z}) = \text{Im}(\check{H}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow \check{H}^i(X_{\beta\bullet}, \mathbb{Z}/\ell\mathbb{Z}))$ (ces entiers existent car le système inductif $\check{H}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ de groupes abéliens finis, ayant une colimite finie, est « essentiellement constant » au sens de la section 5; voir notamment 5.1).

0.3. Stratégie. Inspirés par des travaux de Michael Artin [SGA 4₃ 1973, XI] et Gerd Faltings [1988, §2], nous nous ramenons au cas où l'on peut se restreindre dans la description précédente à des revêtements étales $X_\alpha \rightarrow X$ galoisiens de groupe un ℓ -groupe. Nous montrons alors que le système inductif $\check{H}^i(X_{\alpha\bullet}, \mathbb{Z}/\ell\mathbb{Z})$ — il s'agit maintenant de cohomologie de ℓ -groupes — est « explicitement » essentiellement constant. La technique utilisée pour résoudre (ou plutôt ignorer) les divers problèmes d'extension que l'on rencontre est semblable à celle de [Schön 1991, chapitres I–II] (également connue, indépendamment de [Schön 1991], de Ofer Gabber). La réduction à des espaces « $K(\pi, 1)$ » n'est possible que localement pour la topologie de la descente cohomologique universelle : si X n'est pas lisse,

on utilise un théorème de résolution des singularités de A. Johan de Jong. (En particulier, la *topologie des altérations* est suffisamment fine pour notre propos.)

Les ingrédients essentiels de la démonstration, présentés en §1–8, sont résumés en §10 qui récapitule l’algorithme de calcul des nombres de Betti.

0.4. Cette approche permet également de résoudre le problème posé à la fin de 0.2. On montre en effet que l’on peut obtenir pour chaque i des cocycles (hyper-Čech) pour une base de $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ et, pour tout autre hyperrecouvrement $X_\bullet \rightarrow X$ pour la topologie des altérations, le moyen de développer l’image dans cette base d’un cocycle (hyper-Čech) par le morphisme $\check{H}^i(X_\bullet, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ (voir 8.3). Comme nous le fait remarquer Pierre Deligne, il n’est pas difficile d’en déduire un calcul de $R\Gamma(X, \mathbb{Z}/\ell\mathbb{Z})$ (voir 8.4).

Remarque 0.5. Dans l’énoncé du [théorème 0.1](#), le schéma X est supposé décrit explicitement, c’est-à-dire par des équations le définissant (ou définissant un atlas d’ouverts affines : cf. §16 pour les détails). Il est donc tentant de se demander quelles constructions naturelles, par exemple solutions de problèmes universels, peuvent être ainsi décrites explicitement par des équations. Cette question fait l’objet d’une vaste littérature ; signalons simplement ici les articles [[Anderson 2002](#)] (jacobienne ; voir aussi [[Mumford 1975](#)]) et [[Haiman et Sturmfels 2004](#)] (schéma de Hilbert). Bien entendu, nous utiliserons d’autres résultats de ce type au cours de la démonstration ; cf. par exemple ¶ 15.5, où l’on « calcule » la normalisation.

Signalons maintenant quelques améliorations du [théorème 0.1](#). D’autres améliorations et compléments, ainsi que quelques questions, figurent dans la [section 11](#).

0.6. Notons tout d’abord que le cas de la cohomologie à support compact, et plus généralement de la cohomologie relative (c’est-à-dire modulo un fermé), en résulte formellement ; cf. ¶ 11.2. Nous avons énoncé 0.1 avec des coefficients dans $\mathbb{Z}/\ell\mathbb{Z}$ pour plus de simplicité, mais nous traiterons plus généralement le cas de la cohomologie à valeurs dans $\mathbb{Z}/\ell^n\mathbb{Z}$ (ou même à valeurs dans un faisceau constructible sur un tel anneau ; voir 0.9 *infra*).

0.7. Stratifications. En analysant plus précisément le formalisme de calculabilité sur les éléments d’un corps arbitraire, comme nous le présentons dans un texte complémentaire au présent article ([[Madore et Orgogozo 2014](#)] ; ou cf. [[Bürgisser, Clausen et Shokrollahi 1997](#), proposition 4.27]), il n’est guère difficile de montrer que les résultats énoncés ci-dessus, interprétés dans un modèle de calcul différent où ils restent encore valables, entraînent automatiquement la calculabilité de stratifications associées aux objets calculés. Plus exactement, on peut montrer les affirmations suivantes, où ℓ est un nombre premier *fixé*, inversible sur les schémas considérés :

- si les équations de X comportent des indéterminées, on peut calculer les équations des parties constructibles de l’espace (affine) de ces indéterminées correspondant

à une stratification par la dimension : autrement dit, donnés ℓ et n et un morphisme de type fini $\mathcal{X} \rightarrow \mathbb{A}_k^r$ (où k est un corps algébriquement clos calculable, cf. 12.1), on peut calculer une partition de \mathbb{A}_k^r en un nombre fini de parties constructibles sur chacune desquelles $H^i(X, \mathbb{Z}/\ell^n \mathbb{Z})$ (où X désigne une fibre en un point géométrique de la partie) a un type d'isomorphisme¹ donné, qu'on peut calculer ; il en va de même, par exemple, du type de $H^i(X, \mathbb{Z}/\ell^n \mathbb{Z}) \rightarrow H^i(Y, \mathbb{Z}/\ell^n \mathbb{Z})$ (pour un morphisme $\mathcal{X} \rightarrow \mathcal{Y}$ sur \mathbb{A}_k^r) ;

- si X est un schéma de type fini sur un ouvert de $\text{Spec } \mathbb{Z}$, on peut calculer, en fonction de ℓ et n (et de la description de X), un p_0 tel que le type de $H^i(X_p, \mathbb{Z}/\ell^n \mathbb{Z})$ ne dépende pas de p lorsque $p \geq p_0$, où X_p désigne une fibre géométrique au-dessus de p ; il en va de même du type de $H^i(X_p, \mathbb{Z}/\ell^n \mathbb{Z}) \rightarrow H^i(Y_p, \mathbb{Z}/\ell^n \mathbb{Z})$;
- variante de l'affirmation précédente : donné un morphisme de type fini $\mathcal{X} \rightarrow \mathbb{A}_{\mathbb{Z}[1/\ell]}^r$, on peut calculer une partition de $\mathbb{A}_{\mathbb{Z}[1/\ell]}^r$ en un nombre fini de parties constructibles sur chacune desquelles $H^i(X, \mathbb{Z}/\ell^n \mathbb{Z})$ a un type d'isomorphisme fixé, où X désigne une fibre en un point géométrique de la partie.

Notons que l'existence d'une stratification (resp. d'un nombre premier p_0) comme ci-dessus est conséquence des résultats généraux de constructibilité et commutation aux changements de base. Les démonstrations de [Orgogozo 2013] (resp. [Katz et Laumon 1985, théorème 3.3.2]), de nature géométrique, devraient fournir une stratification (resp. un nombre premier p_0) explicite qui convienne pour *chaque* nombre premier ℓ inversible sur les schémas considérés.

Comme l'observe Olivier Wittenberg [Poonen, Testa et van Luijk 2015, proposition 8.3], le théorème 0.1 (étendu au cas des coefficients $\mathbb{Z}/\ell^n \mathbb{Z}$) a le corollaire suivant.

Corollaire 0.8. *Il existe un algorithme calculant la structure de la partie de torsion du groupe de cohomologie ℓ -adique $H^i(X, \mathbb{Z}_\ell)$ d'une variété propre et lisse X sur un corps algébriquement clos de caractéristique différente de ℓ .*

(Le rang des $H^i(X, \mathbb{Z}_\ell)$ se calcule, dans le cas d'une variété sur un corps fini, en comptant les points de celles-ci et en utilisant une borne a priori, et dans le cas général en se ramenant au cas des corps finis : cf. [Poonen, Testa et van Luijk 2015].) Par contre, hormis dans le cas propre et lisse, permettant d'utiliser des arguments de poids, on ne sait malheureusement rien dire de la cohomologie ℓ -adique (cf. 11.5).

On déduira du théorème 0.1 le résultat suivant (voir 11.4).

Théorème 0.9. *Soit $f: X \rightarrow S$ un morphisme de schémas algébriques sur un corps algébriquement clos k . Pour tout faisceau abélien \mathcal{F} constructible sur X , de torsion*

1. Par « type d'isomorphisme » d'un ℓ -groupe abélien fini V , nous entendons ici bien sûr des $d_1 \leq \dots \leq d_s$ tels que $V \simeq (\mathbb{Z}/\ell^{d_1} \mathbb{Z}) \times \dots \times (\mathbb{Z}/\ell^{d_s} \mathbb{Z})$; et par type d'isomorphisme d'un morphisme entre deux tels groupes, la donnée d'une matrice à équivalence près.

inversible sur k , et tout entier $i \geq 0$, on peut explicitement calculer le faisceau $R^i f_ \mathcal{F}$, fonctoriellement en \mathcal{F} .*

Il en résulte formellement que l'on peut calculer $R^i f_* \mathcal{F}$: appliquer le théorème à une compactification de f et au prolongement par zéro correspondant de \mathcal{F} .

(Idéalement, on aimerait plutôt déduire 0.1 du [théorème 0.9](#), démontré par dévissage.)

0.10. Remarques sur la notion d'algorithme. La « calculabilité » dans le titre de cet article, et le mot « algorithme calculant » dans l'énoncé du [théorème 0.1](#) doivent se comprendre au sens (standard) de Church–Turing, c'est-à-dire le fait que les fonctions annoncées soient (générales) récursives, autrement dit calculables par un ordinateur idéalisé, par exemple une machine de Turing ou une machine à registres : cf. [\[Odifreddi 1989, définition I.1.7 et théorèmes I.4.3 et I.7.9\]](#). Voir [12.1](#) sur la manière dont la machine doit manipuler les éléments du corps de base.

Soulignons que le fait de travailler avec des fonctions générales récursives nous permet d'effectuer des « recherches non bornées » (ce qu'on appelle aussi utiliser l'« opérateur μ de Kleene ») : si pour chaque m il existe n vérifiant une certaine propriété $P(m, n)$ elle-même calculable, alors la fonction $\mu_n P$ qui à m associe le plus petit n vérifiant $P(m, n)$ est calculable (l'idée étant qu'on parcourt les n jusqu'à en trouver un qui vérifie la propriété recherchée).

Nous utiliserons notamment librement ce résultat pour construire des objets géométriques : dès lors qu'un théorème garantit l'existence d'un objet géométrique (schéma, morphisme de schémas,...) possédant une propriété *algorithmiquement testable*, on peut calculer algorithmiquement un tel objet, simplement en énumérant toutes les équations possibles pour les objets géométriques en question et en testant la propriété souhaitée jusqu'à en trouver un qui vérifie la condition voulue (cf. [12.8](#) pour plus de détails).

Pour une discussion sur la question de savoir dans quelle mesure on pourrait se passer de ce procédé, et si les fonctions dont on affirme la calculabilité seraient en fait *primitivement* récursives, voir ¶ [11.6](#) plus bas.

0.11. Leitfaden. Des efforts ont été faits pour rendre la lecture des deux parties largement indépendante chacune de l'autre. L'ordre logique est de commencer par la [partie II](#), mais le lecteur prêt à admettre la calculabilité des opérations classiques de la géométrie algébrique (ainsi que la représentation algorithmique des objets) pourra se contenter de lire la [partie I](#). Inversement, la [partie II](#) peut servir de présentation autonome de certains résultats de géométrie algébrique effective.

Par ailleurs, le lecteur souhaitant démontrer les affirmations énoncées en [0.7](#) doit commencer par la lecture du texte complémentaire [\[Madore et Orgogozo 2014\]](#), et ensuite interpréter la notion de calculabilité utilisée tout au long du présent article comme faisant référence à la notion universelle introduite dans ce complément.

I. Cohomologie étale

1. $K(\pi, 1)$ pro- ℓ

Les résultats de cette section, essentiellement dus à Ofer Gabber,² permettent d'établir une variante (1.4.7) de [Friedlander 1982, théorème 11.7] (dont l'énoncé est rappelé en 1.3.3). Ceux qui préfèrent admettre les résultats de cette section pourront se contenter de lire les définitions 1.3.1 à 1.3.4 et 1.4.4, ainsi que les propositions 1.4.7 et 1.4.12.

Il est fort probable que les hypothèses noëthériennes faites dans cette section sur les schémas puissent être remplacées par des hypothèses de finitude plus faibles (cohérence, ouverture des composantes connexes).

1.1. Champs ℓ -monodromiques : définitions.

1.1.1. Soit \mathcal{C} un champ en groupoïdes sur un schéma localement noëthérien S , muni de la topologie étale [Giraud 1971, II.1.2.1.3]. Rappelons que l'on note $\pi_0(\mathcal{C})$ le faisceau associé au préfaisceau

$$U/S \mapsto \{\text{classes d'isomorphie d'objets de } \mathcal{C}(U)\}$$

— c'est aussi le faisceau des *sous-gerbes maximales* (= strictement pleines ; [Giraud 1971, III.2.1.3]) de \mathcal{C} — et, pour chaque section locale $c_U \in \text{Ob } \mathcal{C}(U)$, où U/S est un ouvert étale, $\pi_1(\mathcal{C}, c_U)$ le faisceau en groupes $\underline{\text{Aut}}(c_U)$ sur U . Le champ \mathcal{C} est dit *constructible* si le faisceau $\pi_0(\mathcal{C})$ et les divers $\pi_1(\mathcal{C}, c)$ sont constructibles. Dans [SGA 1 2003, XIII, §0], un tel champ est dit 1-constructible. (Comparer avec [Giraud 1971, VII.2.2.1] et [Orgogozo 2003, §2].)

1.1.2. Un *lien* sur S est une section cartésienne (sur S) du champ associé au préchamp des faisceaux de groupes à *automorphisme intérieur près* [Giraud 1971, IV.1.1] ; un tel objet peut être représenté par un triplet constitué d'un recouvrement étale S' de S , d'un faisceau en groupes G' sur S' et d'un isomorphisme extérieur $\phi \in \text{Isomex}(p_1^*G', p_2^*G')$, où $p_1, p_2 : S' \times_S S' \rightrightarrows S'$ sont les deux projections, satisfaisant la condition de cocycle usuelle [Deligne et al. 1982, II, appendice].

1.1.3. À tout champ localement connexe-non vide (*gerbe*) \mathcal{G} sur S , est associé un lien \mathcal{L} ; si $c_{S'} \in \text{Ob } \mathcal{G}(S')$ pour S' couvrant S , on peut prendre $G' = \pi_1(\mathcal{G}, c_{S'})$ dans la description précédente : le lien « est » le faisceau des groupes d'automorphismes de sections locales, à conjugaison près. On dit que \mathcal{G} est *lié* par le lien \mathcal{L} ou encore que \mathcal{G} est une \mathcal{L} -gerbe.

Si \mathcal{G} est le champ BG des toseurs sous un S -faisceau en groupes G , son lien est celui naturellement associé à G , représenté par le triplet ($S' = S$, $G' = G$, $\phi = \text{Id}$).

2. Les auteurs sont bien entendu seuls responsables des éventuelles imprécisions ou erreurs dans l'exposition.

Le faisceau des automorphismes de ce lien est le faisceau des automorphismes *extérieurs* de G et l'ensemble des classes d'isomorphie de liens *localement* représentés par le S -schéma en groupes G est naturellement isomorphe à $H^1(S, \text{Autex}(G))$.

1.1.4. Soit \mathcal{L} un lien sur S . L'ensemble $H^2(S, \mathcal{L})$ des classes d'équivalences de gerbes liées par \mathcal{L} est naturellement muni d'une action libre et transitive du groupe de cohomologie $H^2(S, Z(\mathcal{L}))$, où $Z(\mathcal{L})$ désigne le *centre* du lien \mathcal{L} . (Voir [Deligne et al. 1982, loc. cit.] et [Giraud 1971, IV, 1.5.3, 3.1.1 et 3.3.3].)

Définition 1.1.5. Soit ℓ un nombre premier. Un objet sur S du type suivant est dit *ℓ -monodromique* s'il satisfait l'une des conditions suivantes :

- un faisceau d'ensembles F : s'il est localement constant, constructible, et si pour tout point géométrique s de S , le groupe de monodromie, image de $\pi_1(S, s)$ dans $\text{Aut}(F_s)$, est un ℓ -groupe ;
- un faisceau de groupes G : s'il est ℓ -monodromique en tant que faisceau d'ensembles et si ses fibres sont des ℓ -groupes (finis) ;
- un lien \mathcal{L} : s'il est *localement* représenté par un ℓ -groupe fini (constant) G et si, sur chaque composante connexe, le $\text{Autex}(G)$ -torseur $\text{Isom}_{\text{liens}}(\mathcal{L}, \text{lien}(G))$ est ℓ -monodromique, où $\text{lien}(G)$ désigne (abusivement) le lien du champ des G -torseurs ;
- un champ \mathcal{C} : si le faisceau d'ensembles $\pi_0(\mathcal{C})$ est ℓ -monodromique et si, sur le revêtement correspondant de S , les sous-gerbes maximales sont à liens ℓ -monodromiques.

Nous dirons également qu'un morphisme Y/X est un *ℓ -revêtement* s'il est fini étale galoisien d'ordre une puissance de ℓ .

1.1.6. Mise en garde. Un faisceau ℓ -monodromique provient par image inverse du topos $S_{\ell\text{ét}}$ considéré en 1.4.3 mais il n'en est pas de nécessairement de même d'un champ ℓ -monodromique quelconque ; cela reflète le fait qu'une classe dans $H^2(S, \mathbb{Z}/\ell\mathbb{Z})$ n'est pas nécessairement tuée par un revêtement galoisien d'ordre une puissance de ℓ (cf. 1.1.4).

Remarque 1.1.7. Les faisceaux ℓ -monodromiques sont également utilisés en [Orgogozo 2003, 4.6], où l'on démontre la locale constance générique du type d'homotopie étale pro- ℓ des fibres d'un morphisme de type fini.

1.2. Champs ℓ -monodromiques : sorites.

1.2.1. Un faisceau abélien extension (resp. un sous-quotient) de faisceaux abéliens ℓ -monodromiques est également ℓ -monodromique. La lissité (locale constance et constructibilité) résulte de [SGA 4₃ 1973, IX, 2.1(ii) et 2.6(ii)]. Que la monodromie d'une extension soit un ℓ -groupe est conséquence immédiate du fait qu'un élément

unipotent de $GL_n(\mathbb{Z}/\ell^r\mathbb{Z})$ est de ℓ -torsion, c'est-à-dire annulé par une *puissance* de ℓ .

Réciproquement, tout faisceau abélien ℓ -monodromique est extension successive du faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$.

1.2.2. Un faisceau en groupes G est ℓ -monodromique si et seulement si son lien est ℓ -monodromique. (Cette dernière propriété est tautologiquement équivalente au fait que la gerbe BG des G -torseurs soit ℓ -monodromique.) Pour vérifier ce fait, on peut supposer S connexe, et en choisir un point géométrique s . Les deux derniers termes de la suite exacte

$$1 \rightarrow G_s/Z(G_s) \rightarrow \text{Aut}(G_s) \rightarrow \text{Autex}(G_s) \rightarrow 1$$

reçoivent le groupe $\pi_1(S, s)$. Le noyau $G_s/Z(G_s)$ étant un ℓ -groupe, l'image de $\pi_1(S, s)$ dans $\text{Aut}(G_s)$ est un ℓ -groupe si et seulement si l'image de $\pi_1(S, s)$ dans $\text{Autex}(G_s)$ l'est.

1.2.3. *Gerbe quotient.* Par sous-groupe normal d'une gerbe \mathcal{G} sur S nous entendons la donnée pour chaque section locale $\sigma \in \text{Ob } \mathcal{G}(U)$ d'un sous-faisceau en groupes distingués $N_\sigma \trianglelefteq \underline{\text{Aut}}(\sigma) = \pi_1(\mathcal{G}, \sigma)$ et ceci de façon compatible aux restrictions et aux isomorphismes entre sections locales. La *gerbe quotient* de \mathcal{G} par $N = (N_\sigma)_\sigma$ est, par définition, le champ associé à la catégorie fibrée \mathcal{G}' ayant mêmes objets que \mathcal{G} mais dont les homomorphismes sont les faisceaux quotients $\underline{\text{Hom}}_{\mathcal{G}}(\sigma, \tau) := \underline{\text{Hom}}_{\mathcal{G}}(\sigma, \tau)/N_\sigma$. On la note \mathcal{G}/N . Le morphisme $\mathcal{G} \rightarrow \mathcal{G}/N$ est conservatif et couvrant, c'est-à-dire localement surjectif sur les objets et les flèches.

Cette construction s'applique en particulier aux centres $Z_\sigma = Z(\underline{\text{Aut}}(\sigma))$ des faisceaux d'automorphismes locaux. Ici, Z_σ ne « dépend pas » du choix de la section locale et se descend donc à S : il existe un faisceau en groupes abéliens Z et, pour chaque section locale $\sigma \in \text{Ob } \mathcal{G}(U)$, un isomorphisme $Z(U) \xrightarrow{\sim} Z_\sigma$ commutant aux restrictions et aux isomorphismes entre sections locales. Lorsque \mathcal{G} est une gerbe des G -torseurs, où G est un faisceau en groupes, la gerbe quotient ainsi obtenue est équivalente à celle des G' -torseurs, où G' est le quotient de G par son centre.

Si σ est une section globale de la gerbe quotient \mathcal{G}/Z , la gerbe $\mathcal{K}(\sigma)$ des relèvements de σ à \mathcal{G} [Giraud 1971, IV.2.5.1, 2.5.4] est naturellement une Z -gerbe (cf. [Giraud 1971, 2.5.6.(ii)]). Rappelons que $\mathcal{K}(\sigma)$ est triviale si et seulement si la section σ se relève à \mathcal{G} .

Lemme 1.2.4. *Soit $\iota : \mathcal{K} \hookrightarrow \mathcal{G}$ un morphisme fidèle entre gerbes constructibles localement constantes sur un schéma localement noëthérien S . Si \mathcal{G} est ℓ -monodromique, il en est de même de \mathcal{K} .*

Démonstration. Supposons S connexe, comme il est loisible de le faire, et choisissons en un point géométrique s . Pour chaque section locale h de \mathcal{K} , le morphisme ι induit une injection $\underline{\text{Aut}}_{\mathcal{K}}(h) \hookrightarrow \underline{\text{Aut}}_{\mathcal{G}}(\iota h)$. Il en résulte que, localement, le morphisme

lien(ι) : lien(\mathcal{H}) \rightarrow lien(\mathcal{G}) est représenté par une injection de groupes finis $H \subseteq G$ et que l'action du groupe fondamental $\pi_1(S, s)$ sur les liens de \mathcal{H} et \mathcal{G} se factorise à travers le morphisme horizontal ci-dessous :

$$\begin{array}{ccc}
 & & \text{Autex}(H) \\
 & \nearrow & \uparrow \\
 \pi_1(S, s) & \longrightarrow & \text{Aut}(H \subseteq G) / (H/Z(G) \cap H) \\
 & \searrow & \downarrow (\dagger) \\
 & & \text{Autex}(G)
 \end{array}$$

où $\text{Aut}(H \subseteq G)$ désigne le groupe des automorphismes de G préservant globalement H . Bien entendu, G étant un ℓ -groupe, il en est de même de H . Notons d'autre part que le noyau de la flèche (\dagger) est un ℓ -groupe : c'est un quotient du normalisateur de H dans G . Il en résulte que l'image du morphisme horizontal est un ℓ -groupe, car \mathcal{G} est supposé ℓ -monodromique. Partant, il en est de même de l'image du morphisme $\pi_1(S, s) \rightarrow \text{Autex}(H)$. CQFD. \square

Lemme 1.2.5. Soient ℓ un nombre premier, G un ℓ -groupe fini et \mathcal{G} une gerbe ℓ -monodromique sur un topos S , localement isomorphe à BG . Si $H^2(S, \mathbb{Z}/\ell\mathbb{Z}) = 0$, alors la gerbe \mathcal{G} est triviale : elle a une section globale.

En d'autres termes, \mathcal{G} est une gerbe de toiseurs sous un faisceau en groupes, localement isomorphe à G .

Démonstration. Soit \mathcal{G}' la gerbe quotient de \mathcal{G} par son centre Z (cf. 1.2.3). Cette gerbe est localement isomorphe à BG' , où G' est le quotient de G par son centre (non trivial, à moins que G ne le soit). Par récurrence sur l'ordre du groupe, elle a une section globale. La Z -gerbe \mathcal{H} de ses relèvements à \mathcal{G} (cf. loc. cit.) a une classe dans $H^2(S, Z)$ (1.1.4), nécessairement nulle par hypothèse (utiliser 1.2.1). Il en résulte que la gerbe \mathcal{H} est triviale et, par conséquent, que la section globale de \mathcal{G}' considérée se relève à la gerbe \mathcal{G} , qui est donc également triviale. \square

1.3. Courbes et polycourbes ℓ -élémentaires. Rappelons les définitions [SGA 4₃ 1973, XI.3.1 et XI.3.2].

1.3.1. On appelle *courbe élémentaire* sur S un morphisme de schémas $f : X \rightarrow S$ qui peut être plongé dans un diagramme commutatif

$$\begin{array}{ccccc}
 X & \xrightarrow{j} & \bar{X} & \xleftarrow{i} & D \\
 & \searrow f & \downarrow \bar{f} & \swarrow g & \\
 & & S & &
 \end{array}$$

satisfaisant aux conditions suivantes :

- (i) j est une immersion ouverte et $X = \bar{X} - D$;
- (ii) \bar{f} est une courbe (relative) projective lisse, à fibres géométriquement connexes ;
- (iii) g est un revêtement étale à fibres non vides.

Donnés un morphisme projectif \bar{f} et une immersion fermée i , les conditions (i)-(iii) sont algorithmiquement testables : pour la lissité de \bar{f} et g , utiliser 17.2 ; pour la connexité géométrique (resp. non vacuité) des fibres de \bar{f} (resp. de g), on peut supposer que S est un corps en localisant en ses points maximaux (calculables par 15.2), car le faisceau $\bar{f}_*\underline{2}$ (resp. $g_*\underline{2}$) est lisse, et utiliser 16.6.

(Notons que si S est *normal* intègre — comme il serait loisible de le supposer pour notre propos — on pourrait également utiliser la connexité géométrique des fibres d'un morphisme propre $Y \rightarrow S$ dont la fibre générique est géométriquement connexe.)

1.3.2. On appelle *polycourbe élémentaire* sur S un morphisme de schémas $X \rightarrow S$ admettant une factorisation en courbes élémentaires. (Lorsque cela ne semble pas prêter à confusion, on s'autorise à confondre X avec le morphisme $X \rightarrow S$.) Notre terminologie, inspirée des courbes et polycourbes *hyperboliques* de [Mochizuki 1999], nous semble plus explicite que les « fibrations élémentaires » et « bons voisinages » de [SGA 4₃ 1973, XI]. (Voir aussi [ÉGA V, IV.20 ou V.5 (« Sections hyperplanes et projections coniques ») §13 (« Morphismes élémentaires et théorème de M. Artin »)], où un tel morphisme est dit « polyélémentaire ».)

1.3.3. Soient X un schéma algébrique sur un corps parfait infini k et x un point fermé en lequel $X \rightarrow \text{Spec}(k)$ est *lisse*. D'après [SGA 4₃ 1973, XI.3.3], il existe un voisinage ouvert de Zariski U de x qui est une polycourbe élémentaire sur k . (Si $k = \mathbb{C}$, l'espace topologique $U(\mathbb{C})$ est un $K(\pi, 1)$ et toute classe de cohomologie en degré > 0 est tuée par un revêtement fini étale $U' \rightarrow U$ [SGA 4₃ 1973, XI.4.6].) On a le raffinement suivant [Friedlander 1982, théorème 11.7] : il existe un voisinage *étale* de x qui est un « $K(\pi, 1)$ pro- ℓ » (au sens expliqué en ¶ 1.4), où π est un pro- ℓ -groupe extension itérée de pro- ℓ -groupes libres de type fini. Dans cette section et la suivante, on donne une démonstration alternative de ce résultat, amélioré par la possibilité d'utiliser le théorème de résolution des singularités de A. J. de Jong.

1.3.4. Soit ℓ un nombre premier. Une courbe élémentaire $f : X \rightarrow S$ est dite *ℓ -élémentaire* si le faisceau $R^1 f_* \mathbb{Z}/\ell\mathbb{Z}$ est ℓ -monodromique (1.1.5). Lorsque ℓ est inversible sur les schémas considérés, ce qui est systématiquement le cas dans cet article, les faisceaux $R^i f_* \mathbb{Z}/\ell\mathbb{Z}$ sont automatiquement localement constants constructibles, de formation commutant aux changements de base (cf. [SGA 1 2003, XIII.2.9] pour $i \leq 1$, et [SGA 4_{1/2} 1977, Th. finitude, appendice, 1.3.3] pour $i \geq 0$ arbitraire) ; l'hypothèse précédente porte donc sur la *monodromie* de $R^1 f_* \mathbb{Z}/\ell\mathbb{Z}$: si S est connexe et \bar{s} en est un point géométrique, on demande que l'image de $\pi_1(S, \bar{s})$

dans $GL(H^1(X_{\bar{s}}, \mathbb{Z}/\ell\mathbb{Z}))$ soit un ℓ -groupe. Une *polycourbe* f est dite ℓ -élémentaire si elle admet une factorisation en courbes qui sont ℓ -élémentaires ; nous déduisons de la [proposition 1.3.7](#) ci-dessous que $R^1 f_* \mathbb{Z}/\ell\mathbb{Z}$ est alors ℓ -monodromique.

Avant d'énoncer la proposition principale de cette section, commençons par deux lemmes.

Lemme 1.3.5. *Soient X/S une courbe élémentaire (resp. ℓ -élémentaire), ℓ un nombre premier inversible sur S et Y/X un ℓ -revêtement connexe. Alors, le morphisme $Y \rightarrow S$ se factorise à travers un ℓ -revêtement $S' \rightarrow S$ en une courbe élémentaire (resp. ℓ -élémentaire) $Y \rightarrow S'$.*

Démonstration. Commençons par l'énoncé non respé. Soit \bar{X}/S une compactification comme en 1.3.1. Par modération et le lemme d'Abhyankar relatif [SGA 1 2003, XIII.5.5], il existe — localement sur \bar{X} pour la topologie étale — un prolongement de Y/X en un morphisme de Kummer généralisé relativement à $D \subseteq \bar{X}$ [Grothendieck et Murre 1971, 1.3.9.c]. Celui-ci est unique à isomorphisme unique près et sa source est lisse sur S . Si, en coordonnées locales, $D = V(t)$ et $Y \rightarrow X$ est $t = f(y)$, le diviseur E d'équation f/f' est étale sur S . (Si $f(y) = y^n$, avec n inversible sur S , le diviseur E est d'équation y , comme attendu.)³ Par unicité (forte), on peut recoller ces morphismes construits étale-localement en un morphisme fini et plat $\bar{Y} \rightarrow \bar{X}$, prolongeant $Y \rightarrow X$, tel que $\bar{Y} \rightarrow S$ soit une courbe propre et lisse et $E = \bar{Y} - Y$ soit un diviseur fini étale sur S , à fibres non vides. (Cf. par exemple [Illusie, Laszlo et Orgogozo 2014, IX.2.1] pour une approche log-géométrique, lorsque S est un schéma régulier, cas suffisant dans cet article.) Les fibres de $\bar{Y} \rightarrow S$ ne sont pas nécessairement géométriquement connexes mais sa factorisation de Stein répond à la question. (Rappelons que d'après [ÉGA III₂ 1963, 7.8.10], la factorisation de Stein d'un morphisme propre et réduit est un revêtement étale.)

$$\begin{array}{ccc}
 Y & & \\
 \omega \downarrow & \searrow g & \\
 X & & S' \\
 f \downarrow & \swarrow \pi & \\
 S & &
 \end{array}$$

Montrons maintenant que si $f : X \rightarrow S$ est ℓ -élémentaire, il en est de même de $g : Y \rightarrow S'$. L'égalité $\pi_* R^1 g_* \mathbb{Z}/\ell\mathbb{Z} = R^1 (f\omega)_* \mathbb{Z}/\ell\mathbb{Z}$, où π (resp. ω) est le ℓ -revêtement $S' \rightarrow S$ (resp. $Y \rightarrow X$) nous ramène à montrer que le faisceau $R^1 (f\omega)_* \mathbb{Z}/\ell\mathbb{Z}$ est ℓ -monodromique car un faisceau \mathcal{L} sur S' est ℓ -monodromique si $\pi_* \mathcal{L}$ l'est. (Utiliser

3. Notons que si S est réduit, ce qui est suffisant pour nos applications, cela revient à prendre l'image inverse réduite de D .

la surjectivité de la coïunité $\pi^* \pi_* \mathcal{L} \rightarrow \mathcal{L}$.) Enfin, le faisceau $\omega_* \mathbb{Z}/\ell\mathbb{Z}$ étant abélien ℓ -monodromique, il est extension successive du faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$ et, par conséquent, son image directe par $R^1 f_*$ est extension successive de sous-quotients du faisceau $R^1 f_* \mathbb{Z}/\ell\mathbb{Z}$, qui est ℓ -monodromique par hypothèse. \square

Lemme 1.3.6. *Soient $X \rightarrow S$ une courbe élémentaire, ℓ un nombre premier inversible sur S et \mathcal{C} un champ en groupoïdes sur X . Si S est strictement local et si \mathcal{C} est ℓ -monodromique, il existe un ℓ -revêtement étale $X' \rightarrow X$ tel que $\mathcal{C}' = (X' \rightarrow X)^* \mathcal{C}$ soit isomorphe à un coproduit (fini) de champs de toseurs sous des ℓ -groupes finis.*

Ceci nous permettra de ramener — étale-localement sur S — l'étude des champs ℓ -monodromiques à celle des champs de toseurs sous un ℓ -groupe fini.

Démonstration. D'après le lemme précédent (1.3.5) et l'hypothèse sur le champ \mathcal{C} , on peut supposer $\pi_0(\mathcal{C})$ constant. Quitte à remplacer \mathcal{C} par une sous-gerbe maximale, on peut supposer que c'est une gerbe. Il suffit de montrer qu'elle a une section : elle sera alors isomorphe à une gerbe ℓ -monodromique de toseurs et l'on pourra conclure par 1.2.2. L'existence d'une section résulte de 1.2.5 et du fait que, par modération et commutation aux changements de base, les groupes $H^2(X', \mathbb{Z}/\ell\mathbb{Z})$ sont nuls pour tout ℓ -revêtement X' de X . (Rappelons que S est strictement local.) \square

Proposition 1.3.7. *Soient S un schéma localement noëthérien sur lequel un nombre premier ℓ est inversible et $f : X \rightarrow S$ une courbe ℓ -élémentaire. Alors, pour tout champ ℓ -monodromique \mathcal{C} sur X , le champ image directe $f_* \mathcal{C}$ est également ℓ -monodromique. De plus, la formation de cette image directe commute aux changements de base $S' \rightarrow S$.*

Démonstration. La commutation aux changements de base et la lissité reviennent à montrer que si S est strictement local de point fermé s et $\bar{\eta}$ est un point générique géométrique, les morphismes $\mathcal{C}(X) \rightarrow \mathcal{C}(X_s)$ et $\mathcal{C}(X) \rightarrow \mathcal{C}(X_{\bar{\eta}})$ sont des équivalences. Par descente (finie étale) et les deux lemmes précédents (1.3.5, 1.3.6), on se ramène au cas particulier où \mathcal{C} est une gerbe de toseurs sous un ℓ -groupe fini : cela résulte alors des théorèmes bien connus de spécialisation du groupe fondamental (modéré). La constructibilité de l'image directe est également déjà connue [SGA 1 2003, XIII, §2] et résulte d'ailleurs de la démonstration ci-dessous.

Commençons par montrer que pour tout champ \mathcal{C} comme dans l'énoncé, le faisceau $\pi_0(f_* \mathcal{C})$ est ℓ -monodromique en traitant tout d'abord le cas d'un faisceau (c'est-à-dire d'un champ en catégories discrètes). Par passage à la limite, il suffit de montrer que si S est un schéma (non nécessairement noëthérien) n'admettant pas de revêtement connexe d'ordre ℓ (c'est-à-dire : le topos $S_{\ell\text{ét}}$ défini en 1.4.3 est local) et s est un point géométrique de S , alors le morphisme $\pi_1^{\text{pro-}\ell}(X \times_S S_{(s)}) \rightarrow \pi_1^{\text{pro-}\ell}(X)$ est surjectif. (Voir par exemple [Szamuely 2009, chapitre 5] pour une théorie du

groupe fondamental pour les schémas non nécessairement localement noëthériens.) Comme il s'agit de pro- ℓ groupes, cela est équivalent à montrer que la flèche induite par application du foncteur $H^1(-, \mathbb{Z}/\ell\mathbb{Z})$ à $X \times_S S_{(s)} \rightarrow X$ est injective (cf. [Serre 1994, I, §4.2, proposition 23]). Or, on a la suite exacte (Leray)

$$0 \rightarrow H^1(S, f_*\mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^1(X, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^0(S, R^1 f_*\mathbb{Z}/\ell\mathbb{Z}),$$

où : $f_*\mathbb{Z}/\ell\mathbb{Z} = \mathbb{Z}/\ell\mathbb{Z}$ (par connexité des fibres géométriques), $H^1(S, \mathbb{Z}/\ell\mathbb{Z}) = 0$ (par hypothèse sur S), et $R^1 f_*\mathbb{Z}/\ell\mathbb{Z}$ est constant sur S (par hypothèse sur f) de sorte que $H^0(S, R^1 f_*\mathbb{Z}/\ell\mathbb{Z}) = H^1(X \times_S S_{(s)}, \mathbb{Z}/\ell\mathbb{Z})$. Supposons maintenant que \mathcal{C} est un champ ℓ -monodromique quelconque et montrons que $\pi_0(f_*\mathcal{C})$ est ℓ -monodromique. D'après ce qui précède, on peut supposer — quitte à remplacer S par un ℓ -revêtement — le faisceau $f_*\pi_0(\mathcal{C})$ constant puis que le champ \mathcal{C} est une gerbe (ℓ -monodromique), notée \mathcal{G} dorénavant. Soit \mathcal{G}' son quotient par le centre Z de \mathcal{G} (1.2.3) et posons $\mathcal{L} := \pi_0(f_*\mathcal{G})$ et $\mathcal{L}' := \pi_0(f_*\mathcal{G}')$. Le faisceau en groupes abéliens $R^1 f_*Z$ agit sur le morphisme (localement constant) canonique $\mathcal{L} \rightarrow \mathcal{L}'$ et l'action est transitive sur les fibres : $(R^1 f_*Z) \backslash \mathcal{L} \rightarrow \mathcal{L}'$ est injective. (Ceci est l'analogie du fait bien connu (voir [Giraud 1971, III, 3.4.5] ou [Serre 1994, I, §5.7]) que si $1 \rightarrow Z \rightarrow G \rightarrow G' \rightarrow 1$ est une extension centrale de groupes sur un topos E , le groupe abélien $H^1(E, Z)$ agit sur $H^1(E, G)$ par produit contracté, c'est-à-dire par

$$[T] \cdot [P] = [T \overset{Z}{\wedge} P],$$

et l'application $H^1(E, Z) \backslash H^1(E, G) \rightarrow H^1(E, G')$, de source le quotient à gauche de $H^1(E, G)$ par $H^1(E, Z)$, est *injective*.) Le morphisme f étant ℓ -monodromique, on peut supposer $R^1 f_*Z$ constant ; par récurrence, on peut supposer qu'il en est de même de \mathcal{L}' . La conclusion résulte alors formellement de l'observation suivante : si un ℓ -groupe abélien fini C agit fidèlement et transitivement sur les fibres d'un morphisme $\mathcal{L} \rightarrow \mathcal{L}'$ de faisceaux lisses à but constant, le faisceau \mathcal{L} est ℓ -monodromique. En effet, l'action de la monodromie sur \mathcal{L} se factorise à travers C . Ceci achève la démonstration du fait que $\pi_0(f_*\mathcal{C})$ est ℓ -monodromique lorsque f est une courbe ℓ -élémentaire et \mathcal{C} est ℓ -monodromique.

Supposons dorénavant le faisceau $\mathcal{L} = \pi_0(f_*\mathcal{C})$ trivial et considérons une sous-gerbe maximale \mathcal{G} de $f_*\mathcal{C}$. Il nous faut montrer que son lien est ℓ -monodromique (1.1.5) ; on va utiliser le lemme 1.2.4. On vérifie en effet que le morphisme $f^*\mathcal{G} \rightarrow \mathcal{C}$ déduit par adjonction de l'inclusion $\mathcal{G} \hookrightarrow f_*\mathcal{C}$ est fidèle : par commutation des images directes au passage aux fibres, on se ramène à observer que si G est un faisceau localement constant sur X et x un point géométrique d'une fibre géométrique X_s , le morphisme $G(X_s) \rightarrow G_x$ est injectif. (On utilise la connexité des fibres géométriques du morphisme $f : X \rightarrow S$.) D'après *loc. cit.*, il en résulte que la gerbe $f^*\mathcal{G}$ est ℓ -monodromique. Pour démontrer que le lien de \mathcal{G} est ℓ -monodromique, on est donc ramené à vérifier qu'un faisceau \mathcal{F} sur S est ℓ -monodromique si $f^*\mathcal{F}$ l'est.

La constructibilité résulte de la surjectivité de f , cf. p. ex. [SGA 4₃ 1973, IX.2.8], et la lissité n'est guère plus difficile. Que \mathcal{F} soit ℓ -monodromique résulte, dans le cas où les schémas sont connexes, de la surjectivité du morphisme $\pi_1(X) \rightarrow \pi_1(S)$ rappelée en 1.4.7 (premier paragraphe). \square

1.4. Schémas $K(\pi, 1)$.

1.4.1. Commençons par rappeler quelques résultats de [Abbes et Gros 2011, §9]. Pour chaque schéma X , on note $X_{\text{ét}}$ le topos étale, $X_{f\text{ét}}$ le topos *fini étale* (autrement dit, le topos associé à la sous-catégorie pleine des X -schémas étales finis munie de la topologie étale) et $\rho : X_{\text{ét}} \rightarrow X_{f\text{ét}}$ le morphisme évident [ibid., §9.2]. Lorsque X est *cohérent*, le morphisme ρ est un morphisme cohérent entre topos cohérents [ibid., 9.11, 9.13]. Si l'on suppose de plus l'espace topologique quotient $\pi_0(X) = \text{Spec Idem}(X)$ discret (autrement dit : les composantes connexes de X ouvertes), le morphisme d'adjonction $\text{Id} \rightarrow \mathbf{R}\rho_*\rho^*$ induit un isomorphisme en degrés 0 et 1, comme on peut le vérifier par passage aux fibres, c'est-à-dire en supposant X simplement connexe (ou encore : $X_{f\text{ét}}$ local). On dit [ibid., 9.20] que le schéma X est un $K(\pi, 1)$ s'il satisfait la condition d'acyclicité suivante : pour tout entier $n \geq 1$ inversible sur X et tout faisceau \mathcal{L}_f de $\mathbb{Z}/n\mathbb{Z}$ -modules sur $X_{f\text{ét}}$, le morphisme d'adjonction $\mathcal{L}_f \rightarrow \mathbf{R}\rho_*\rho^*\mathcal{L}_f$ est un isomorphisme.

1.4.2. *Traduction dans le cas connexe.* Si X est connexe, le choix d'un point géométrique x de X identifie le topos $X_{f\text{ét}}$ au topos $\mathbf{B}\pi_1(X, x)$ des $\pi_1(X, x)$ -ensembles continus (cf. [ibid., §9.7]). En particulier, la cohomologie de $X_{f\text{ét}}$ n'est autre que la cohomologie (« galoisienne ») du groupe profini $\pi_1(X, x)$ [ibid., 9.7.6]. Si X est un $K(\pi, 1)$, alors pour tout chaque entier n inversible sur X et chaque faisceau étale \mathcal{L} de $\mathbb{Z}/n\mathbb{Z}$ -modules localement constant constructible sur X , la flèche canonique $\mathbf{R}\Gamma(\pi_1(X, x), \mathcal{L}_x) \rightarrow \mathbf{R}\Gamma(X, \mathcal{L})$ est un isomorphisme. La réciproque est vraie lorsque \tilde{X} est cohérent et ceci est encore équivalent au fait qu'un revêtement universel \tilde{X} de X n'a pas de cohomologie à valeur dans $\mathbb{Z}/n\mathbb{Z}$ en degré ≥ 1 (ou, de façon équivalente, > 1).

1.4.3. *Variante pro- ℓ .* Soit ℓ un nombre premier inversible sur un schéma cohérent X à composantes connexes ouvertes et considérons la sous-catégorie pleine des X -schémas finis étales dont la monodromie (en tant que faisceau d'ensembles représenté) est, sur chaque composante connexe, un ℓ -groupe, autrement dit, dont le groupe de Galois sur X d'une clôture galoisienne est un ℓ -groupe. Munie de la topologie étale, cette catégorie donne lieu à un site, dont on note $X_{\ell\text{ét}}$ le topos associé, naturellement équipé d'un morphisme $\rho_\ell : X_{\text{ét}} \rightarrow X_{\ell\text{ét}}$. Par construction, la cohomologie de $X_{\ell\text{ét}}$ est, dans le cas où X est connexe, la cohomologie du groupe fondamental pro- ℓ de X (pointé en un point géométrique).

1.4.4. Un schéma X comme ci-dessus est un $K(\pi, 1)$ *pro- ℓ* si pour tout faisceau

abélien de ℓ -torsion [SGA 4₃ 1973, IX.1.1] \mathcal{L}_ℓ sur $X_{\text{ét}}$, l'unité d'adjonction $\mathcal{L}_\ell \rightarrow R\rho_{\ell_*}\rho_\ell^*\mathcal{L}_\ell$ est un isomorphisme. En conséquence, si x est un point géométrique de X , supposé connexe, et \mathcal{L} est un faisceau abélien ℓ -monodromique (donc constructible) sur X , on a $R\Gamma(\pi_1^{\text{pro-}\ell}(X, x), \mathcal{L}_x) \xrightarrow{\sim} R\Gamma(X, \mathcal{L})$ et, réciproquement, ceci caractérise les $K(\pi, 1)$ pro- ℓ .

1.4.5. Mise en garde. Notons qu'avec nos définitions, un schéma $K(\pi, 1)$ n'est pas nécessairement un $K(\pi, 1)$ pro- ℓ : le noyau du morphisme de pro- ℓ -complétion (« sous-groupe ℓ -résiduel ») d'un groupe profini n'est en général pas pro- ℓ' et, *a fortiori*, pas nécessairement acyclique pour les coefficients de ℓ -torsion.

1.4.6. Exemple. Toute courbe affine lisse C sur un corps algébriquement clos est un $K(\pi, 1)$ pro- ℓ pour chaque nombre premier ℓ . En effet, ni la courbe (affine), ni le pro- ℓ groupe fondamental (libre, cf. p. ex. [Wingberg 1984, théorème 1.1] lorsque ℓ est inversible sur C) n'ont de cohomologie en degré > 1 . (On utilise également le fait général que l'unité d'adjonction $\text{Id} \rightarrow R\rho_{\ell_*}\rho_\ell^*$ est un isomorphisme en degré ≤ 1 pour les faisceaux de ℓ -torsion.)

Proposition 1.4.7. Soient ℓ un nombre premier inversible sur un corps algébriquement clos k et X une polycourbe ℓ -élémentaire sur $\text{Spec}(k)$. Alors, le schéma X est un $K(\pi, 1)$ pro- ℓ (cf. 1.4.4), et le pro- ℓ complété du groupe fondamental de chaque composante connexe de X est extension itérée de pro- ℓ groupes libres de type fini.

Démonstration. Soit $f : X \rightarrow Y$ une polycourbe ℓ -élémentaire, où Y est une courbe affine connexe lisse sur corps algébriquement clos de caractéristique $\neq \ell$. On note $\bar{\eta}$ un point générique géométrique de Y et on souhaite tout d'abord montrer que la suite de pro- ℓ groupes

$$1 \rightarrow \pi_1^{\text{pro-}\ell}(X_{\bar{\eta}}) \rightarrow \pi_1^{\text{pro-}\ell}(X) \rightarrow \pi_1^{\text{pro-}\ell}(Y) \rightarrow 1 \quad (\dagger)$$

est exacte. (On omet ici la notation de points bases.) L'exactitude à droite résulte de la surjection $\pi_1(X) \twoheadrightarrow \pi_1(Y)$ [SGA 1 2003, XIII.4.1]. Soit G un ℓ -groupe fini. Rappelons (cf. par exemple [SGA 4₃ 1973, XII, §1]) que l'on a une suite exacte d'ensembles pointés :

$$1 \rightarrow H^1(Y, f_*G) \rightarrow H^1(X, G) \rightarrow H^0(Y, R^1f_*G),$$

analogue non abélien de la suite exacte de bas degré usuelle (Leray). Ici, on a l'égalité $f_*G = G$ et le faisceau R^1f_*G est localement constant de fibre en $\bar{\eta}$ isomorphe à $H^1(X_{\bar{\eta}}, G)$ de sorte que le noyau de la flèche (d'ensembles pointés) $H^1(X, G) \rightarrow H^1(X_{\bar{\eta}}, G)$ est l'image de $H^1(Y, G)$: (\dagger) est exacte au centre (voir p. ex. [SGA 1 2003, V, §6] pour la traduction en terme de groupes fondamentaux).

Notons \mathcal{C} le champ sur Y image directe par f du champ des G -torseurs sur X . Rappelons [Giraud 1971, V.3.1.6] l'interprétation champêtre de la suite exacte

d'ensembles pointés précédente. Le terme de droite s'identifie à l'ensemble des sous-gerbes maximales de $\mathcal{C} : \text{à une classe } c \in H^0(Y, R^1 f_* G)$ est associée la gerbe $D(c)$ sur Y dont la fibre en $V \rightarrow Y$ est la catégorie des G -torseurs sur $U = X \times_Y V$ dont la classe dans $H^1(U, G)$ s'envoie sur la restriction $c|_V \in H^0(V, R^1 f_* G)$. La gerbe $D(c)$ est triviale si et seulement si c est l'image d'une classe $[T] \in H^1(X, G)$ et, dans ce cas, $D(c)$ est équivalente au champ des $f_* \text{Aut}(T)$ -torseurs sur Y . D'après 1.3.7, il existe un ℓ -revêtement étale de $Y' \rightarrow Y$ tel que le faisceau $\pi_0(\mathcal{C}')$ des sous-gerbes maximales de $\mathcal{C}' = (Y' \rightarrow Y)^* \mathcal{C}$ soit fini constant et que chacune des sous-gerbes maximales soient *localement* liées par le lien d'un ℓ -groupe constant. (On utilise la commutation au changement de base de la formation de l'image directe $f_* \text{BG}$.) D'après 1.2.5, ces sous-gerbes maximales, sur la *courbe affine* Y' , sont triviales. Il en résulte que le foncteur de restriction $\mathcal{C}'(Y') = \mathcal{C}(Y') \rightarrow \mathcal{C}(\bar{\eta})$ est essentiellement surjectif : tout G -torseur sur $X_{\bar{\eta}}$ s'obtient par restriction à partir d'un G -torseur sur $X' = X \times_Y Y'$. Ceci suffit pour achever la démonstration de l'exactitude de (\dagger) (cf. [SGA 1 2003, V.6.8 et XIII.4.3]). On utilise le fait qu'une clôture galoisienne *sur* X d'un G -torseur sur X' est un revêtement d'ordre une puissance de ℓ : si $H'' \trianglelefteq H' \trianglelefteq H$ sont des groupes finis avec $[H : H']$ et $[H' : H'']$ des puissances d'un nombre premier ℓ , le sous-groupe $\bigcap_{h \in H/H''} hH''h^{-1}$ est d'indice une puissance de ℓ dans H .

Pour montrer que X est un $K(\pi, 1)$ pro- ℓ , commençons par constater que si \mathcal{F} est un faisceau abélien ℓ -monodromique, et f une polycourbe ℓ -élémentaire, les faisceaux $R^j f_* \mathcal{F}$ sont ℓ -monodromiques. La stabilité par extension des faisceaux abéliens ℓ -monodromiques (1.2.1) nous permet en effet de nous ramener, par récurrence, au cas où f est une courbe ℓ -élémentaire, auquel cas cela résulte de la proposition 1.3.7. La conclusion résulte alors de la suite exacte d'homotopie précédente, de l'égalité

$$R\Gamma(X, \mathcal{F}) = R\Gamma(Y, Rf_* \mathcal{F}),$$

de l'isomorphisme

$$R\Gamma(\pi_1^{\text{pro-}\ell}(Y, \bar{\eta}), (Rf_* \mathcal{F})_{\bar{\eta}}) \xrightarrow{\sim} R\Gamma(Y, Rf_* \mathcal{F})$$

(cf. 1.4.6) et enfin de l'isomorphisme

$$(Rf_* \mathcal{F})_{\bar{\eta}} = R\Gamma(X_{\bar{\eta}}, \mathcal{F}) \xleftarrow{\sim} R\Gamma(\pi_1^{\text{pro-}\ell}(X_{\bar{\eta}}), \mathcal{F}),$$

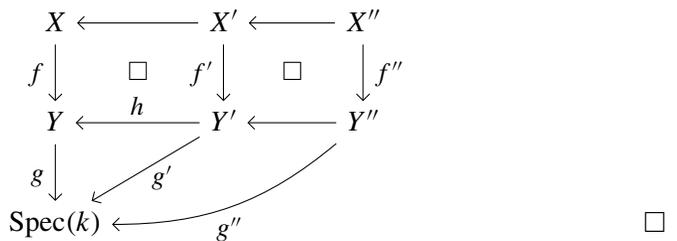
obtenu par récurrence sur la dimension relative. □

1.4.8. Avant d'énoncer le résultat d'abondance des $K(\pi, 1)$ pro- ℓ ci-dessous, rappelons que P. Deligne a défini dans [Deligne 1974, §5.3.5] la topologie de la descente cohomologique universelle [SGA 4₂ 1972, V^{bis}, §3.3] ; pour une introduction pédagogique à cette notion, le lecteur pourra se référer à [Conrad 2003]. Nous appellerons *topologie des altérations* la topologie définie par la prétopologie engendrée par les

recouvrements étales et les altérations (= morphisme propre et surjectif induisant un morphisme fini au-dessus d'un ouvert partout dense et envoyant tout point maximal sur un point maximal). La topologie de la descente cohomologique universelle est plus fine que la topologie des altérations.

Proposition 1.4.9. *Soit ℓ un nombre premier inversible sur un corps algébriquement clos k . Localement pour la topologie des altérations, tout k -schéma algébrique est une polycourbe ℓ -élémentaire (et en particulier, d'après 1.4.7, localement un $K(\pi, 1)$ pro- ℓ). De plus, si le schéma est supposé lisse, c'est même vrai localement pour la topologie étale.*

Démonstration. Soit X un schéma comme dans l'énoncé, que l'on peut supposer intègre. D'après [de Jong 1996, 4.1], il est localement (par une altération) lisse sur k . D'après [SGA 4₃ 1973, XI.3.3] (rappelé en 1.3.3), on peut donc supposer que le k -schéma lisse connexe X est une polycourbe élémentaire. Factorisons $X \rightarrow \text{Spec}(k)$ à travers une courbe élémentaire $f : X \rightarrow Y$. Il existe un revêtement étale $h : Y' \rightarrow Y$ trivialisant $R^1 f_* \mathbb{Z}/\ell\mathbb{Z}$, c'est-à-dire tel que le faisceau $h^* R^1 f_* \mathbb{Z}/\ell\mathbb{Z} = R^1 f'^* \mathbb{Z}/\ell\mathbb{Z}$ soit trivial (i.e., constant) donc, en particulier, ℓ -monodromique. Un tel revêtement est calculable : quitte à se placer au-dessus du point générique du schéma normal Y , ceci est expliqué en §2. (Le cas considéré ici est celui, plus facile, d'une courbe ; cf. 2.4 et 2.7.) Étant obtenu par changement de base de f , le morphisme f' est une courbe élémentaire, et même ℓ -élémentaire par construction. Par récurrence sur la dimension du schéma considéré, on peut supposer qu'il existe, localement pour la topologie étale au voisinage de chaque point, un morphisme $Y'' \rightarrow Y'$ tel que le morphisme g'' du diagramme commutatif ci-dessous soit une polycourbe ℓ -élémentaire. Le schéma X'' obtenu par changement de base convient. □



1.4.10. Notons que l'utilisation du théorème de A. J. de Jong fait perdre l'éventuelle primitive récursivité de notre algorithme (puisqu'on utilise ce théorème en énumérant tous les morphismes sur X jusqu'à trouver une altération qui en résolve les singularités, sans aucune borne sur le temps d'exécution autre que le fait que cette énumération terminera, cf. 11.6 et 12.8). Il est probable que, dans le cas lisse, on puisse préserver l'éventuelle primitive récursivité de notre algorithme par une analyse précise de [SGA 4₃ 1973, XI, §2–3].

1.4.11. Si k est algébrique séparable sur un corps ${}_0k$ et X/k obtenu par extension des scalaires d'un ${}_0k$ -schéma algébrique ${}_0X$, tout recouvrement $\{Y_\alpha \rightarrow X\}$ par des polycourbes ℓ -élémentaires est dominé par un recouvrement du même type défini sur ${}_0k$.⁴ En effet, si $Y_\alpha \rightarrow X$ se descend en un morphisme de ${}_1k$ -schémas algébriques ${}_1Y_\alpha \rightarrow {}_1X$, où ${}_1k/{}_0k$ est étale, il suffit de considérer le ${}_0k$ -morphisme composé ${}_1Y_\alpha \rightarrow {}_0X$. Le schéma ${}_1Y_\alpha \otimes_{{}_0k} k$ est isomorphe à $Y_\alpha \otimes_k ({}_1k \otimes_{{}_0k} k)$; c'est un coproduit de polycourbes ℓ -élémentaires, fini surjectif au-dessus de Y_α .

Nous utiliserons la proposition précédente sous la forme suivante (cf. [SGA 4₂ 1972, V^{bis}.5.1] ou bien [Deligne 1974, 5.3.3.1 et §6.2]).

Corollaire 1.4.12. Soient ℓ un nombre premier inversible sur un corps algébriquement clos k et X un k -schéma algébrique. Alors, il existe un X -schéma simplicial X_\bullet , tel que chaque X_i soit un coproduit fini de polycourbes ℓ -élémentaires et tel que la flèche d'adjonction $\mathrm{R}\Gamma(X_{\text{ét}}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet, \text{ét}}, \mathbb{Z}/\ell\mathbb{Z})$ soit un isomorphisme. De plus :

- un morphisme $Y \rightarrow X$ de k -schémas algébriques peut être coiffé par un morphisme simplicial $Y_\bullet \rightarrow X_\bullet$ du type précédent ;
- si k est algébrique séparable sur ${}_0k$ et X/k obtenu par extension des scalaires d'un ${}_0k$ -schéma algébrique ${}_0X$, on peut supposer pour tout entier r que la flèche $X_{\bullet, \leq r} \rightarrow X$ provient par extension des scalaires d'une flèche ${}_0X_{\bullet, \leq r} \rightarrow {}_0X$.

Le dernier point résulte de l'observation 1.4.11 et de la construction des hyperrecouvrements rappelée ci-dessous, effectuée sur ${}_0k$. Pour la définition du *topos total* $\mathrm{Tot} X_{\bullet, \text{ét}}$, voir les références citées en §4. (Voir également 4.1.1 pour une variante « n -approchée ».) Pour la définition d'un *hyperrecouvrement*, voir par exemple [SGA 4₂ 1972, V.7.3.1.1] ou bien [Deligne 1974, 5.3.5] (ou, de nouveau, [Conrad 2003] pour une approche pédagogique).

1.4.13. Par la suite, nous utiliserons implicitement le fait que les objets et les flèches ci-dessus sont calculables en tout étage : la construction décrite en [SGA 4₂ 1972, V^{bis}.5.1.3] (voir aussi [Deligne 1974, proposition 6.2.4]) ne fait intervenir que des limites et coproduits finis et explicites de schémas, que l'on « améliore » en utilisant 1.4.9. Traitons le problème de la construction d'une flèche $Y_\bullet \rightarrow X_\bullet$ plus en détail ; le cas de X_\bullet en est un cas particulier. Par produit fibré, il suffit de montrer le lemme suivant.

Lemme. *Tout hyperrecouvrement X_\bullet de X peut être dominé par un hyperrecouvrement X'_\bullet à composantes des coproduits de polycourbes ℓ -élémentaires, calculables en tout étage.*

4. Les indices sont mis à gauche pour éviter la confusion avec les indices simpliciaux utilisés ci-dessous.

Ici, « hyperrecouvrement » = « hyperrecouvrement pour la topologie des altérations ».

Démonstration. Fixons un entier $r \geq 0$ et supposons donné un morphisme simplicial (r -tronqué) $X'_{\bullet \leq r} \rightarrow \text{sq}_r X_\bullet$, où $X'_{\bullet \leq r}$ est scindé à composantes des coproduits de polycourbes ℓ -élémentaires. D'après 1.4.9, on peut « couvrir » le produit fibré de X_{r+1} et $\text{cosq}_r(X'_{\bullet \leq r})_{r+1}$ au-dessus de $\text{cosq}_r(\text{sq}_r X_\bullet)_{r+1}$ par un coproduit de polycourbes ℓ -élémentaires, noté N . Pour le calcul du cosquelette, on utilise la formule :

$$\text{cosq}_r(Z)_s = \lim_{\substack{k \leq r \\ [k] \rightarrow [s]}} Z_k$$

(la limite étant comprise dans la catégorie des X -schémas, et calculable d'après 16.3). D'après [SGA 4₂ 1972, V^{bis}.5.1.3], il existe un schéma simplicial $r + 1$ -tronqué scindé (calculable) $X'_{\bullet \leq r+1}$ prolongeant $X'_{\bullet \leq r}$, s'envoyant sur $\text{sq}_{r+1}(X_\bullet)$, tel que X'_{r+1} soit un coproduit de N et de composantes scindées de $X'_{\bullet \leq r}$; c'est donc un coproduit de polycourbes ℓ -élémentaires. □

2. Calculabilité du H^1

L'objectif de cette section est de démontrer le théorème suivant.

Théorème 2.1. *Soient X un schéma normal, de type fini sur un corps algébriquement clos k , et G un groupe fini constant d'ordre une puissance d'un nombre premier ℓ inversible sur X . Alors, on peut calculer $H^1(X, G)$, c'est-à-dire produire une liste de représentants des classes d'isomorphie de G -torseurs sur X .*

2.2. Il suffit de trouver une extension finie galoisienne du corps des fractions K de X qui domine tous ces G -torseurs, ou encore une extension les trivialisant tous. En effet, si L/K est une telle extension, de groupe de Galois π , l'ensemble $H^1(X, G)$ est naturellement un sous-ensemble de l'ensemble fini $H^1(L/K, G) = \text{Hom}(\pi, G)/G$ des classes d'isomorphie de G -torseurs sur K trivialisés par L/K . Si $\phi \in \text{Hom}(\pi, G)$, on peut construire explicitement le G -torseur $A_\phi = \text{Hom}_{\pi\text{-Ens}}(G, L)$ sur K correspondant par la théorie de Galois–Grothendieck, et tout G -torseur sur X est obtenu par normalisation de X dans un tel A_ϕ (voir 15.5 pour la calculabilité de la normalisation). Parmi ces X -schémas, en nombre fini, il faut vérifier quels sont ceux qui sont étales et galoisiens de groupe G sur X (cf. 17.2 et 17.3).

2.3. Réduction au cas abélien. Notons Z le centre (non trivial) du ℓ -groupe fini G . La suite exacte

$$1 \rightarrow Z \rightarrow G \rightarrow G/Z \rightarrow 1$$

induit [Giraud 1971, V.2.3] une suite exacte d'ensembles pointés

$$H^1(X, Z) \rightarrow H^1(X, G) \rightarrow H^1(X, G/Z).$$

Supposons, par récurrence, que l'on sache trouver une extension L du corps des fonctions de X trivialisant les G/\mathbb{Z} -torseurs. Soit X_L le normalisé de X dans L . L'image inverse sur X_L de chaque G -torseur sur X provient d'un \mathbb{Z} -torseur sur X_L . (On utilise le fait que la restriction au point générique induit une injection sur les H^1 car les schémas considérés sont normaux.) Ceci nous ramène au cas particulier où G est un ℓ -groupe abélien et, finalement, au cas où $G = \mathbb{Z}/\ell\mathbb{Z}$, ce qu'on supposera maintenant.

2.4. Cas d'une courbe.

2.4.1. Si X est une courbe lisse sur le corps algébriquement clos k , le cardinal de $H^1(X, \mathbb{Z}/\ell\mathbb{Z})$ est connu. On peut donc effectivement produire tous les $\mathbb{Z}/\ell\mathbb{Z}$ -torseurs sur X en un temps fini.

Remarque 2.4.2. Signalons comment l'on pourrait se ramener au cas d'une courbe projective (lisse). Si \bar{X} est la complétion projective de X et $\bar{X} - X = \{c_1, \dots, c_r\}$ sont les points à l'infini, il existe (Riemann–Roch) une fonction $f \in K^\times$ s'annulant exactement en ces points. Notons $L = K(\sqrt[r]{f})$. D'après le lemme d'Abhyankar, le tiré en arrière d'un $\mathbb{Z}/\ell\mathbb{Z}$ -torseur sur X au normalisé X_L de X dans L s'étend à la complétion projective \bar{X}_L . Pour trouver f , on note qu'il existe un entier n explicite tel que, pour chaque $i \in \{1, \dots, r\}$, il existe une fonction $f_i \in \mathcal{L}((n+1)c_i) - \mathcal{L}(nc_i)$, que l'on peut calculer algorithmiquement, cf. [Hess 2002]; la fonction $f = \sum_i f_i$ convient. (Une variante de cet argument est également possible lorsque X est un k -schéma algébrique normal, quitte à l'altérer pour en faire le complémentaire d'un diviseur à croisements normaux dans un k -schéma projectif lisse (de Jong).)

Signalons pour terminer que si X est une courbe projective lisse, on sait [Serre 1975, chapitre VI, n° 12] que tout revêtement connexe de groupe $\mathbb{Z}/\ell\mathbb{Z}$ est induit par une isogénie de la jacobienne de X (que l'on peut construire explicitement; cf. p. ex. [Anderson 2002]). Ceci fournit une approche différente de 2.4.1 pour la détermination effective de $H^1(X, \mathbb{Z}/\ell\mathbb{Z})$, qui peut probablement être rendue primitivement récursive.

2.5. Fibration en courbes.⁵ Supposons dorénavant le schéma X de dimension $d \geq 2$ et démontrons 2.1 par récurrence sur l'entier d . On peut supposer le schéma X intègre et, quitte à le modifier — c'est-à-dire le remplacer par un X -schéma propre et birationnel —, on peut également supposer qu'il existe un k -schéma de type fini intègre S de dimension $d - 1$ et un morphisme $X \rightarrow S$ faisant de X une courbe relative sur S à fibre générique lisse et géométriquement connexe. (cf. p. ex. [de Jong 1996, 4.11–12].) Il résulte de ce qui précède — appliqué à la courbe $X_{\bar{\eta}}$ où $\bar{\eta}$ est un point générique géométrique de S — qu'il existe un S -schéma étale S' intègre

5. Cette méthode nous a été suggérée par Ofer Gabber.

de point générique η' et un revêtement $Y' \rightarrow X_{S'}$ tel que si T est un G -torseur sur X et T' le toseur obtenu par le changement de base $Y' \rightarrow X$, la fibre générique géométrique $T'_{\eta'}$ est le G -torseur trivial. Quitte à changer les notations, on peut supposer $S = S'$ et $X = Y'$.

(Du point de vue algorithmique, signalons que l'on peut déterminer η par 15.2 et que les corps $\kappa(\eta)$ et $\kappa(\bar{\eta})$ conservent les bonnes propriétés de calculabilité que l'on peut imposer à k par 12.5.)

2.6. Quitte à remplacer S par un ouvert étale, on peut supposer que le morphisme $X \rightarrow S$ est une *courbe élémentaire*. Vérifions que, sous cette hypothèse, tout G -torseur T sur X à fibre générique géométrique triviale provient de S : ceci nous permettra de conclure, par récurrence, car $\dim(S) = d - 1 < d$. Supposons, comme il a été fait ci-dessus, que G est le groupe abélien $\mathbb{Z}/\ell\mathbb{Z}$, et notons f le morphisme $X \rightarrow S$. Considérons la suite exacte

$$0 \rightarrow H^1(S, f_*\mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^1(X, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^0(S, R^1 f_*\mathbb{Z}/\ell\mathbb{Z}).$$

Comme rappelé en 1.3.4, le morphisme d'adjonction $\mathbb{Z}/\ell\mathbb{Z} \rightarrow f_*\mathbb{Z}/\ell\mathbb{Z}$ est un isomorphisme, le faisceau $R^1 f_*\mathbb{Z}/\ell\mathbb{Z}$ est lisse sur S et la fibre générique géométrique de $R^1 f_*\mathbb{Z}/\ell\mathbb{Z}$ est isomorphe à $H^1(X_{\bar{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$. Il en résulte que la flèche $H^0(S, R^1 f_*\mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^1(X_{\bar{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$ est une injection et, par conséquent, que tout $\mathbb{Z}/\ell\mathbb{Z}$ -torseur sur X trivialisé par $X_{\bar{\eta}}$ provient de S . (Voir aussi 1.3.7 et 1.4.7.) Ceci achève la démonstration du [théorème 2.1](#).

Remarque 2.7. Supposons X obtenu par extension algébrique des scalaires à partir d'un schéma X_0 sur k_0 et $T^{(1)}, \dots, T^{(N)}$ des représentants des classes d'isomorphie de G -torseurs sur X . Il existe une sous-extension étale k_1/k_0 de k , calculable (16.11), telle que les G -torseurs précédents soient définis sur k_1 , c'est-à-dire que chaque $T^{(i)}$ soit X -isomorphe à $T_1^{(i)} \times_{X_1} X$, où $X_1 = X_0 \times_{k_0} k_1$ et $T_1^{(i)}$ est un G -torseur sur X_1 . Dans ce cas, l'action naturelle de $\text{Aut}(k/k_0)$ sur $H^1(X, G)$ se factorise à travers une action explicite du quotient fini $\text{Gal}(k_1/k_0)$: si (plus généralement) $g \in \text{Aut}_{k_0}(X_1)$, l'action (à droite) de g sur $[T_1] \in H^1(X_1, G)$ est donnée par $[T_1] \cdot g = [T_1 \times_{X_1, g} X_1]$.

3. Série ℓ -centrale descendante et groupe fondamental

3.1. Une filtration.

3.1.1. Soient ℓ un nombre premier et G un pro- ℓ groupe. Pour tout sous-groupe H de G , notons $F(H)$ l'adhérence du sous-groupe $H^\ell \cdot (H, G)$ de G , où (X, Y) désigne le sous-groupe engendré par les commutateurs $x^{-1}y^{-1}xy$ pour x dans X et y dans Y : autrement dit, il s'agit du sous-groupe fermé de G engendré par les puissances ℓ -ièmes des éléments de H et des commutateurs de ces éléments avec ceux de G . Rappelons ([Dixon et al. 1999, 1.15] ou [Neukirch, Schmidt et Wingberg

2000, définition 3.8.1]) que la *série ℓ -centrale descendante* de G est la filtration définie de la façon suivante : $G^{[1]} = G$, et $G^{[n+1]} = F(G^{[n]})$. Ces sous-groupes sont caractéristiques dans G et on note $G^{(n)}$ le quotient $G/G^{[n]}$. En particulier, $G^{[2]}$ est le sous-groupe de Frattini $\Phi(G)$ de G ([Serre 1978–79, §3.6] ou [Rotman 1995, théorème 5.48(ii)]) et le \mathbb{F}_ℓ -espace vectoriel $G^{(2)}$ est naturellement le dual de $\text{Hom}_{\text{cont}}(G, \mathbb{Z}/\ell\mathbb{Z})$.

Pour des raisons typographiques, nous noterons parfois $F^n G$ pour $G^{[n]}$, notamment en §6.

Remarques 3.1.2. On vérifie sans peine que $G^{[n+1]}$ est le plus petit sous-groupe fermé normal de G contenu dans $G^{[n]}$ tel que $G^{[n]}/G^{[n+1]}$ soit ℓ -élémentaire abélien et contenu dans le centre de $G/G^{[n+1]}$.

Pour notre propos, nous avons une certaine liberté dans le choix de la filtration : on aurait aussi bien pu considérer, par exemple, la filtration de Frattini itérée $\Phi^n G$, où $\Phi(H) = \overline{H^\ell(H, H)} \subseteq F(H)$. À ce sujet, signalons que la filtration de Frattini itérée $\Phi^n G$ et la filtration ℓ -centrale descendante $F^n G$ définie ci-dessus sont équivalentes au sens où il existe une fonction $\tau(d, n)$ (explicitement calculable, et même, primitivement récursive) telle que $F^{\tau(d,n)} G \subseteq \Phi^n G \subseteq F^n G$ si G a d générateurs (comme pro- ℓ -groupe). (Esquisse de démonstration : l'inclusion $\Phi^n G \subseteq F^n G$ est évidente. L'inclusion $F^{\tau(d,n)} G \subseteq \Phi^n G$ se montre en combinant le (i) du lemme 6.1 ci-dessous avec un l'analogue du (ii) pour la filtration $\Phi^n G$. Cet analogue du (ii) revient à majorer l'ordre de $L/\Phi^n L$ où L est le pro- ℓ -groupe libre à d générateurs : ceci peut se faire par récurrence sur n en utilisant le fait que $\#(L/\Phi L) = \ell^d$ et le théorème de l'indice de Schreier [Lubotzky et Segal 2003, proposition 16.4.5] pour calculer le nombre de générateurs de $\Phi^n L$.)

Signalons également que si G est topologiquement de type fini, le passage à l'adhérence est superflu, les sous-groupes considérés étant déjà fermés, tant pour F que pour Φ [Dixon et al. 1999, corollaire 1.20].

3.2. Revêtements et topos associés.

3.2.1. Soient X un schéma *connexe*, séparé de type fini sur un corps algébriquement clos k , x un point géométrique, ℓ un nombre premier inversible sur k et π_X le groupe fondamental pro- ℓ de (X, x) . Ce groupe est topologiquement de type fini, par finitude de $H^1(X, \mathbb{F}_\ell) = \text{Hom}(\pi_X, \mathbb{F}_\ell)$, si bien que le morphisme canonique $\pi_X \rightarrow \lim_n \pi_X^{(n)}$ est un isomorphisme (voir par exemple [Neukirch, Schmidt et Wingberg 2000, 3.8.2], ou [Dixon et al. 1999, proposition 1.16 (iii)]).

Pour chaque entier $n \geq 1$, notons $X^{[n]} \rightarrow X$ un revêtement étale de X correspondant au sous-groupe d'indice fini $\pi_X^{[n]}$ de π_X ; nous dirons que c'est un *revêtement ℓ -étale n -approché universel* de X . On note $X_{\ell\text{ét}}^{(n)}$, voire simplement $X^{(n)}$, le topos des faisceaux sur $X_{\ell\text{ét}}$ trivialisés par le revêtement étale $X^{[n]} \rightarrow X$. Le morphisme

naturel $X_{\ell\acute{e}t} \rightarrow X_{\ell\acute{e}t}^{(n)}$ s'identifie au morphisme de topos $B\pi_X \rightarrow B\pi_X^{(n)}$ déduit de la surjection $\pi_X \rightarrow \pi_X^{(n)}$: l'image inverse est le foncteur des $\pi_X^{(n)}$ -ensembles vers les π_X -ensembles continus (obtenu par composition) et l'image directe est le foncteur « invariants sous $\pi_X^{[n]}$ » ; cf. p. ex. [SGA 4_I 1972, IV.4.5.1]. (On laisse le soin au lecteur de définir $X_{\ell\acute{e}t}^{(n)}$ sous des hypothèses plus générales ; nous n'en aurons pas usage.) Par construction, pour chaque $n \geq 2$, le topos $X_{\ell\acute{e}t}^{(n)}$ est ponctuel si et seulement si π_X est trivial, c'est-à-dire si X ne possède pas de revêtement étale connexe d'ordre ℓ .

3.2.2. *Mutatis mutandis*, les définitions précédentes s'étendent au cas d'un schéma (algébrique sur un corps algébriquement clos) *non nécessairement connexe*. Pour définir $X^{[n]}$, on écrit X comme coproduit de ses composantes connexes (ouvertes) et l'on procède de manière évidente : si $X = \coprod_{c \in \pi_0(X)} X_c$, on pose

$$X^{[n]} := \coprod_{c \in \pi_0(X)} X_c^{[n]}.$$

La définition du topos $X^{(n)}$ est inchangée et celle du groupe $\pi_X^{(n)}$ devrait être remplacée par la définition d'un *groupoïde* $\Pi_X^{(n)}$.

Notons que $X_{\ell\acute{e}t}^{(1)}$ est le topos discret des faisceaux sur l'ensemble (fini) $\pi_0(X)$.

3.2.3. Donnons une description alternative de $X^{(n)}$. Commençons par observer qu'il est équivalent au topos des faisceaux sur le site *ℓ -étale n -approché* de X dont les objets sont les $U \rightarrow X$ finis étales qui sont, composante connexe par composante connexe, quotients d'un revêtement *ℓ -étale n -approché* universel de X ; une famille est couvrante si son image recouvre X . Fixons un revêtement *ℓ -étale n -approché* universel $X^{[n]}$ de X , et notons $\Pi_{X^{[n]}/X}$ le groupoïde totalement discontinu (au sens de [Gabriel et Zisman 1967, 6.1.4]) dont les objets sont les $c \in \pi_0(X)$, de groupe d'automorphismes $\text{Aut}_{X_c}(X_c^{[n]})$. Le foncteur $\mathcal{F} \mapsto \mathcal{F}(X^{[n]})$ induit une équivalence entre le topos $X^{(n)}$ et le topos des préfaisceaux sur $\Pi_{X^{[n]}/X}$. Les foncteurs $\mathcal{F} \mapsto \mathcal{F}(X_c^{[n]})$ sont des *points* du topos $X^{(n)}$. (Noter qu'un schéma $X_c^{[n]}$ n'est pas nécessairement local au sens de la topologie *ℓ -étale n -approchée* considérée.)

3.2.4. Nous dirons qu'un faisceau d'ensembles constructible \mathcal{F} sur $X^{(n)}$ (resp. un morphisme $\mathcal{F} \rightarrow \mathcal{G}$) est *calculable* (en fonction des données) s'il en est ainsi du X -schéma *ℓ -étale n -approché* $X^{\mathcal{F}}$ (resp. du morphisme $X^{\mathcal{F}} \rightarrow X^{\mathcal{G}}$) qui le représente (ce schéma ou morphisme étant lui-même décrit au sens de la [section 16](#)) ; si le faisceau \mathcal{F} est abélien, on demande de plus que les X -morphisms $+$: $X^{\mathcal{F}} \times_X X^{\mathcal{F}} \rightarrow X^{\mathcal{F}}$ (addition), $[-1]$: $X^{\mathcal{F}} \rightarrow X^{\mathcal{F}}$ (opposé) et e : $X \rightarrow X^{\mathcal{F}}$ (neutre) soient calculables. L'ensemble des sections sur un ouvert *ℓ -étale n -approché* donné U d'un faisceau calculable \mathcal{F} , ainsi que les flèches de functorialité, sont calculables : il suffit de calculer l'ensemble des sections du morphisme fini étale de schémas $X^{\mathcal{F}} \rightarrow X$

au-dessus de U , et les flèches induites ; cf. 17.3. Réciproquement, l'action de la monodromie sur $\mathcal{F}(X^{[n]})$ permet de reconstruire $X^{\mathcal{F}}$.

3.2.5. Il résulte immédiatement de ce qui précède que l'on peut calculer le noyau d'un morphisme calculable $\mathcal{F} \rightarrow \mathcal{G}$ de faisceaux constructibles abéliens. Il en est de même du conoyau : il est représenté par le plus grand quotient X' de $X^{\mathcal{G}}$ tel que le morphisme de schémas en groupes $X^{\mathcal{F}} \rightarrow X'$ se factorise à travers la section nulle $X \rightarrow X'$.

3.2.6. Nous dirons qu'un faisceau d'ensembles constructible \mathcal{F} sur $X^{(n)}$ est *induit* s'il est isomorphe à un faisceau image directe étale $\pi_{\text{ét}\star} E$, où π est le morphisme (fini étale) $X^{[n]} \rightarrow X$ et E est un faisceau constant constructible sur chaque composante connexe. Tout faisceau d'ensemble constructible \mathcal{F} sur $X^{(n)}$ est sous-objet d'un faisceau induit : l'unité $\mathcal{F} \rightarrow \pi_{\text{ét}\star} \pi_{\text{ét}}^* \mathcal{F}$ est un monomorphisme. Si \mathcal{F} est *calculable*, il en est de même de l'injection précédente.

Rappelons que l'image inverse d'un faisceau représentable est représentée par le produit fibré évident et que si \mathcal{G} est un faisceau d'ensembles constructible sur un schéma X' , représenté par un X' -schéma Y' , le faisceau étale image directe $f_{\text{ét}\star} \mathcal{G}$ par un morphisme *fini étale* $f : X' \rightarrow X$ est représenté par même schéma Y' , vu sur X . On utilise ici l'égalité $f_{\text{ét}\star} = f_{\text{ét}!}$ et la description de ce dernier foncteur faite par exemple en [SGA 4₁ 1972, IV.11.3.1].

3.3. Calculabilité de $X^{[n]}$.

3.3.1. Soient k un corps algébriquement clos et X un k -schéma algébrique *normal*, non nécessairement connexe. Comme précédemment, on a fixé un nombre premier ℓ inversible sur k . On se propose de montrer que l'on peut calculer un revêtement ℓ -étale n -approché universel $X^{[n]}$ de X . Une décomposition de X en composantes connexes étant calculable (cf. 16.6), on suppose dorénavant le schéma X connexe. Observons maintenant qu'une fois calculé $X^{[n]} \rightarrow X$, on peut en déduire $\pi_X^{(n)}$ qui est isomorphe au groupe d'automorphismes $\text{Aut}_X(X^{[n]})$, lui-même en bijection avec $\pi_0(X^{[n]} \times_X X^{[n]})$ par son action sur la composante connexe diagonale (cf. 17.3 ou 16.6). Réciproquement, si $\pi_X^{(n)}$ — ou même simplement son cardinal — est connu, on peut construire $X^{[n]}$, au pire par recherche non bornée (12.8) d'un revêtement étale ayant le bon groupe de Galois. Ci-dessous, nous allons donc nous contenter de calculer le groupe $\pi_X^{(n)}$ dans le cas où X est normal connexe (en fait, il n'est pas difficile de se convaincre qu'on construit bien $X^{[n]}$).

Remarque 3.3.2. Par « calcul » d'un groupe fini, on entend la détermination du cardinal et d'une table de multiplication du groupe. (En particulier, on peut en déterminer des générateurs — par exemple, le groupe tout entier — et, pour tout ensemble fini de générateurs, une présentation finie associée.)

3.3.3. $n = 2$. Comme signalé ci-dessus, le groupe abélien $\pi_X^{(2)}$ est isomorphe au dual du \mathbb{F}_ℓ -espace vectoriel de dimension finie $H^1(X, \mathbb{F}_\ell)$. D’après le [théorème 2.1](#), on peut calculer le rang de cet espace vectoriel. En particulier, si π_X est un pro- ℓ -groupe libre de type fini, on peut calculer son rang (nombre minimal de générateurs).

3.3.4. Réurrence sur n . On suppose que l’on sait calculer le groupe $\pi_X^{(n)}$ et par conséquent un revêtement ℓ -étale n -approché universel $X^{[n]} \rightarrow X$. Considérons maintenant un revêtement ℓ -étale 2-approché universel $X^{[n][2]}$ de $X^{[n]}$. C’est également un revêtement galoisien de X car le sous-groupe de Frattini $\Phi(\pi_X^{[n]})$ est caractéristique dans π_X donc distingué. Notons G le groupe de Galois de $X^{[n][2]}$ sur X , que l’on peut calculer : c’est le groupe d’automorphismes d’un X -schéma explicite. Abstraitement, il est isomorphe à $\pi_X / \Phi(\pi_X^{[n]})$; le groupe $\pi_X^{(n+1)} = \pi_X / \pi_X^{[n+1]}$ — que l’on cherche à calculer — en est donc un quotient. Plus précisément, par functorialité [[Dixon et al. 1999](#), proposition 1.16 (i)], $\pi_X^{(n+1)} = G^{(n+1)}$. Ceci permet de conclure.

3.4. Functorialité. De même que l’on ne peut associer à un espace topologique (connexe localement simplement connexe) un revêtement universel de façon fonctorielle, on ne peut espérer choisir $X^{[n]}$ fonctoriellement en X . Tout comme $X \rightsquigarrow X_{\text{ét}}$ (cf. p. ex. [[SGA 4₂ 1972](#), VII.1.4]), la construction $X \rightsquigarrow X_{\text{ét}}^{(n)}$ définit seulement un *pseudo-foncteur* ([[SGA 1 2003](#), VI, §8] ou [[Borceux 1994](#), 7.5.1]) covariant de la catégorie des schémas vers la 2-catégorie des topos.

3.4.1. Soit $f : (X, x) \rightarrow (Y, y)$ un morphisme de schémas pointés, entre k -schémas algébriques, où k est un corps algébriquement clos sur lequel un nombre premier ℓ fixé est inversible. (On ne suppose pas que le morphisme f est un k -morphisme.) Soient $n \geq 1$ un entier et $X^{[n]}$ (resp. $Y^{[n]}$) un revêtement ℓ -étale n -approché universel de X (resp. Y). Il résulte de la théorie des revêtements et de la functorialité de $G \mapsto G^{(n)}$ qu’il existe un morphisme $f^{[n]} : X^{[n]} \rightarrow Y^{[n]}$ au-dessus de $f : X \rightarrow Y$, c’est-à-dire rendant commutatif le diagramme suivant :

$$\begin{array}{ccc} X^{[n]} & \xrightarrow{f^{[n]}} & Y^{[n]} \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

Si X et Y sont connexes, ce morphisme $f^{[n]}$ est unique à translation près par $\text{Aut}_Y(Y^{[n]})$. Si f est un k -morphisme explicite entre schémas normaux, on peut le calculer.

Rigidification : choisissons des points géométriques $x^{[n]} \rightarrow X^{[n]}$ et $y^{[n]} \rightarrow Y^{[n]}$ au-dessus de x et y respectivement. Alors, il existe un *unique* morphisme pointé

$f_{xy}^{[n]} : (X^{[n]\circ}, x^{[n]}) \rightarrow (Y^{[n]\circ}, y^{[n]})$ au-dessus de f , où le terme de gauche d'une paire (Z°, z) désigne la composante connexe de Z contenant z .

3.4.2. Version simpliciale. Soit X_\bullet un k -schéma algébrique simplicial tronqué — c'est-à-dire un foncteur d'une catégorie $\mathbf{\Delta}_{\leq r}$ ⁶ ($r \in \mathbb{N}$) vers les k -schémas algébriques — et $P_\bullet \rightarrow X_\bullet$ un morphisme simplicial (tronqué), tel que chaque P_i soit coproduit fini de points géométriques. Il existe pour chaque i un relèvement de $P_i \rightarrow X_i$ à un revêtement ℓ -étale n -approché universel $X_i^{[n]\circ}$ de X_i . Notons $X_{P_i}^{[n]\circ}$ le coproduit $\coprod_{p_i \in P_i} X_{p_i}^{[n]\circ}$, où $X_{p_i}^{[n]\circ}$ désigne la composante connexe de $X_i^{[n]\circ}$ contenant l'image de p_i . D'après le paragraphe précédent, les $X_{P_i}^{[n]\circ}$ s'organisent *de façon unique* en un schéma simplicial $X_{P_\bullet}^{[n]\circ}$ de telle sorte que $P_\bullet \rightarrow X_{P_\bullet}^{[n]\circ}$ soit une factorisation simpliciale de $P_\bullet \rightarrow X_\bullet$.

En d'autres termes, quitte à introduire des « multiplicités », on peut relever simplicialement les points géométriques d'un schéma à un revêtement ℓ -étale n -approché universel.

4. Cohomologie ℓ -étale n -approchée d'un schéma simplicial

On vérifie ici le fait — énoncé en 4.3.1 et intuitivement évident compte tenu de ce qui précède (3.3) — que l'on sait calculer la cohomologie des topos obtenus à partir d'un schéma simplicial tronqué par application du pseudo-foncteur $S \rightsquigarrow S^{(n)}$ (cf. ¶ 3.4). Il est logiquement possible, et peut-être préférable, de ne lire cette section qu'après la section 8. Pour un raccourci, cf. 4.2.3.

4.1. Généralités. Nous renvoyons le lecteur à [Illusie 1972, VI, §5.1 et §6.2] ou [SGA 4₂ 1972, VI, §7] pour les détails, et [Deligne 1974, §5.1] pour un résumé (qui est le point de départ de la théorie) dans le cas des espaces topologiques.

4.1.1. Cohomologie d'un topos simplicial. Soient X_\bullet un k -schéma algébrique simplicial et n un entier ≥ 1 . Notons $X_\bullet^{(n)}$ le topos simplicial (c'est-à-dire fibré sur $\mathbf{\Delta}$) qui s'en déduit par application du pseudo-foncteur $S \rightsquigarrow S^{(n)}$ et $\text{Tot } X_\bullet^{(n)}$ le topos total associé, noté $\text{Top} X_\bullet^{(n)}$ dans [Illusie 1972, VI, §5.1]. On peut voir un objet \mathcal{F}_\bullet de $\text{Tot } X_\bullet^{(n)}$ comme la donnée pour chaque ouvert U d'un X_i (ouvert : objet du site ℓ -étale n -approché défini en 3.2.3) d'un ensemble $\mathcal{F}_\bullet(U) = \mathcal{F}_i(U)$, fonctoriellement en un sens que nous ne répétons pas ([Illusie 1972, VI, §5.2] ou [Deligne 1974, 5.1.7] ; essentiellement, la fonctorialité est « cosimpliciale en i et faisceautique en U »).

Rappelons par contre un procédé de calcul de la cohomologie de $\text{Tot } X_\bullet^{(n)}$ à valeurs dans un faisceau abélien \mathcal{F}_\bullet . Le cas du H^0 (sections globales) est particulièrement

6. C'est la catégorie des ensembles $\{0, \dots, s\} \subseteq \mathbb{N}$, où $s \leq r$, munis des applications croissantes ; elle est notée $(\mathbf{\Delta})_r$ dans [Deligne 1974, 5.1.1].

simple : c'est

$$\lim_{i \in \Delta} \Gamma(X_i^{(n)}, \mathcal{F}_i) = \text{Ker}(\Gamma(X_0^{(n)}, \mathcal{F}_0) \rightrightarrows \Gamma(X_1^{(n)}, \mathcal{F}_1)).$$

Soit $u_\bullet : P_\bullet \rightarrow X_\bullet^{(n)}$ un morphisme simplicial tel que pour chaque étage i , le topos P_i soit discret (c'est-à-dire coproduit de topos ponctuels) et le morphisme $u_i : P_i \rightarrow X_i^{(n)}$ d'image inverse conservative. Notons $\mathcal{F}_i^\bullet = (\mathcal{F}_i^j)$ la résolution flasque (« de Godement ») du faisceau \mathcal{F}_i associée. Le système des $\Gamma(X_i^{(n)}, \mathcal{F}_i^j)$ est cosimplicial en i et différentiel gradué en j ; il fournit un complexe double, la différentielle en i étant la somme alternée usuelle. La cohomologie cherchée est celle du complexe simple associé :

$$\text{R}\Gamma(\text{Tot } X_\bullet^{(n)}, \mathcal{F}_\bullet) \simeq \text{Tot } \Gamma(X_i^{(n)}, \mathcal{F}_i^j).$$

Le terme $\Gamma(X_i^{(n)}, \mathcal{F}_i^j)$ de droite n'est autre que l'ensemble des sections globales de \mathcal{F}_i^j , vu comme faisceau étale sur le schéma X_i .

On en déduit notamment que $\tau_{<r} \text{R}\Gamma(\text{Tot } X_\bullet^{(n)}, \mathcal{F}_\bullet)$ ne dépend que du schéma simplicial tronqué $X_{\leq r}$ et de la restriction de \mathcal{F}_\bullet correspondante. Bien que cela ne soit pas absolument nécessaire pour les résultats de cet article, nous précisons en 4.1.2 ci-dessous cette observation.

4.1.2. Variante tronquée (cf. [Gabber 2001]). Pour tout $r \in \mathbb{N} \cup \{+\infty\}$ et tout faisceau abélien $F_{\leq r}$ sur $\Delta_{\leq r}^{\text{op}}$ (c'est-à-dire : groupe abélien cosimplicial tronqué $\Delta_{\leq r} \rightarrow \text{Ab}$), les sections globales dérivées $\text{R}\Gamma(\Delta_{\leq r}^{\text{op}}, F_{\leq r})$ sont calculées par le complexe normalisé $NF_{\leq r} \in \text{Ob } C^{[0,r]}(\text{Ab})$ de la correspondance de Dold–Kan. Pour une définition de ce complexe dans un contexte non tronqué, cf. par exemple [Dold et Puppe 1961, §3]. Les sections globales dérivées d'un *complexe* (de groupes abéliens cosimpliciaux tronqués) se calculent en prenant le *complexe simple* obtenu par ce procédé. Si $X_{\leq r}$ est un k -schéma algébrique tronqué et $\mathcal{F}_{\leq r}$ est un faisceau sur $\text{Tot } X_{\leq r}^{(n)}$, on en déduit en poussant par $X_{\leq r}^{(n)} \rightarrow \Delta_{\leq r}$ que pour toute résolution $\mathcal{F}_{\leq r}^\bullet$ à $\mathcal{F}_{i \leq r}^j$ acycliques sur $X_i^{(n)}$, on a

$$\text{R}\Gamma(\text{Tot } X_{\leq r}^{(n)}, \mathcal{F}_{\leq r}^\bullet) = \text{Tot } N_i \Gamma(X_{i \leq r}^{(n)}, \mathcal{F}_i^j),$$

où, pour chaque j , on note $N_i \Gamma(X_{i \leq r}^{(n)}, \mathcal{F}_i^j)$ le complexe normalisé déduit du groupe cosimplicial tronqué $i \mapsto \Gamma(X_{i \leq r}^{(n)}, \mathcal{F}_i^j)$. Ceci est compatible avec la description non « normalisée » du paragraphe précédent par le théorème d'Eilenberg–Mac Lane, [Dold et Puppe 1961, 3.22].

Si X_\bullet (resp. \mathcal{F}_\bullet) est une extension de $X_{\leq r}$ (resp. de $\mathcal{F}_{\leq r}$) en un k -schéma simplicial non tronqué (resp. en un faisceau sur $\text{Tot } X_\bullet^{(n)}$), on a donc un triangle distingué

$$(\text{complexe dans } D^{>r}(\mathbb{Z})) \rightarrow \text{R}\Gamma(\text{Tot } X_\bullet^{(n)}, \mathcal{F}_\bullet) \rightarrow \text{R}\Gamma(\text{Tot } X_{\leq r}^{(n)}, \mathcal{F}_{\leq r}^\bullet) \xrightarrow{+1}$$

de sorte qu'en particulier la flèche

$$H^d(\mathrm{Tot} X_{\bullet}^{(n)}, \mathcal{F}_{\bullet}) \rightarrow H^d(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \mathcal{F}_{\bullet \leq r})$$

est un isomorphisme pour $d < r$ et injective pour $d = r$.

4.2. Résolution de Godement explicite. Montrons maintenant que les considérations précédentes permettent de calculer les $H^i(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \mathcal{F}_{\bullet \leq r})$ lorsque les objets sont donnés explicitement.

4.2.1. On reprend les notations de 4.1.1 et l'on suppose chacun des étages X_i de $X_{\bullet \leq r}$ normaux, afin de pouvoir appliquer les résultats de 3.3. Observons tout d'abord que, si P est un point géométrique d'un des X_i (obtenu par exemple par le procédé décrit en 16.10), l'ensemble de ses images par toutes les composées de morphismes de bord et de dégénérescence est fini, de cardinal borné par celui de l'ensemble de toutes les applications croissantes $\{0, \dots, m\} \rightarrow \{0, \dots, n\}$ avec $m, n \leq r$. On peut donc choisir un ensemble fini $\{P_j\}$ de points géométriques formant un morphisme simplicial $P_{\bullet \leq r} \rightarrow X_{\bullet \leq r}$ et tel que chaque composante connexe de chacun des X_i contienne au moins un des P_j . Comme expliqué en 3.4.2, on peut relever $P_{\bullet \leq r}$ en un morphisme de schémas simpliciaux $P_{\bullet \leq r} \rightarrow X_{P_{\bullet \leq r}}^{[n]^\circ}$, qui nous permet de calculer les images directes et inverses par le morphisme de topos simpliciaux $u_{\bullet \leq r} : P_{\bullet \leq r} \rightarrow X_{\bullet \leq r}^{(n)}$, où l'on voit maintenant (abusivement) les P_i comme des topos discrets. Le calcul de l'image inverse $u_i^* \mathcal{F}$ d'un faisceau \mathcal{F} sur $X_i^{(n)}$ est évident : sa fibre en p_i est $\mathcal{F}(X_{p_i}^{[n]^\circ})$. L'image directe $u_{i*} E$, pour la topologie ℓ -étale n -approchée, est le faisceau induit (3.2.6) image directe usuelle (= étale) par le morphisme fini étale $X_{P_i}^{[n]^\circ} \rightarrow X_i$ du faisceau constant sur chaque composante connexe correspondant à E . Donné E , ce faisceau est calculable, étant représenté par un coproduit explicite $X_{P_i, E}^{[n]^\circ}$ de copies de $X_{P_i}^{[n]^\circ}$. De plus, on peut calculer les X -morphismes (addition, neutre, opposé) faisant de $X_{P_i, E}^{[n]^\circ}$ un X -schéma en groupes fini.

4.2.2. Pour tout faisceau $\mathcal{F}_{\bullet \leq r} \in \mathrm{Ob} \mathrm{Tot} X_{\bullet \leq r}^{(n)}$, le morphisme d'adjonction $\mathcal{F}_{\bullet \leq r} \rightarrow \mathcal{G}_{\bullet \leq r} := u_{\bullet \leq r*} u_{\bullet \leq r}^* \mathcal{F}_{\bullet \leq r}$ est le début de la résolution flasque de Godement considérée ci-dessus. Supposons $\mathcal{F}_{\bullet \leq r}$ calculable, c'est-à-dire représentable par un schéma simplicial tronqué en groupes abéliens finis $X_{\bullet \leq r}^{\mathcal{F}}$ au-dessus de $X_{\bullet \leq r}$ qui est calculable (cf. 3.2.4). Comme expliqué ci-dessus, le faisceau $\mathcal{G}_{\bullet \leq r}$ — induit étage par étage — est également calculable, ainsi que la flèche $\mathcal{F}_{\bullet \leq r} \rightarrow \mathcal{G}_{\bullet \leq r}$. D'après 3.2.5, le conoyau de cette flèche est calculable : on a montré que, donné $\mathcal{F}_{\bullet \leq r}$ — et les données auxiliaires, non canoniques, $P_{\bullet \leq r}$, etc. — on peut calculer une résolution « de Godement » $\mathcal{C}_P^{(n)}(\mathcal{F}_{\bullet \leq r})$ jusqu'à des degrés arbitrairement grands.

4.2.3. Variante par recherche non bornée. Si l'on s'autorise à être moins explicite (et perdre l'éventuelle primitive récursivité), on peut procéder plus simplement, c'est-à-dire sans avoir recourt aux schémas simpliciaux $P_{\bullet \leq r}$ et $X_{P_{\bullet \leq r}}^{[n]^\circ}$. Fixons

comme ci-dessus un corps k , un nombre premier ℓ , un schéma simplicial tronqué $X_{\bullet \leq r}$, un anneau Λ , et deux entiers n et d . Il existe une résolution tronquée par un complexe d'induits \mathcal{F}_i^j (cosimplicial en $i \leq r$, différentiel gradué en $j \leq d$) du faisceau constant de valeur Λ sur $X_{\bullet \leq r}$. Cette résolution tronquée est, par hypothèse, acyclique étage par étage et calcule la cohomologie tronquée : $\tau_{<d} \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \Lambda) = \tau_{j < d} \mathrm{Tot} N_i \Gamma(X_i, \mathcal{F}_i^j)$. Pour calculer la cohomologie de $\mathrm{Tot} X_{\bullet \leq r}^{(n)}$ à valeurs dans Λ en degrés strictement inférieurs à d , il suffit donc de parcourir les morphismes $\Lambda \rightarrow \mathcal{F}_i^j$, où \mathcal{F}_i^j est un complexe tronqué d'induits, et, si c'est une résolution tronquée (c'est-à-dire acyclique en degrés $\leq d$) — fait que l'on sait vérifier (cf. 3.2.5) —, de calculer le terme de droite correspondant. On peut procéder de même pour calculer les flèches de functorialité en n et en $X_{\bullet \leq r}$.

Remarque 4.2.4. Ce qui précède peut être vu comme une variante du fait bien connu que l'on sait calculer en chaque degré la cohomologie d'un groupe fini agissant sur un Λ -module explicite (voir par exemple la définition donnée en [Serre 1994, I, §2.2]). Sur le problème de la détermination de l'algèbre de cohomologie $H^*(G, \Lambda)$ d'un groupe fini G , voir par exemple [Carlson 2001]. (D'après le théorème de Venkov–Evens [Evens 1991, 7.4.6], c'est une Λ -algèbre de type fini.)

4.2.5. La construction précédente d'une résolution de Godement est fonctorielle en n en un sens évident : une fois choisi $P_{\bullet \leq r} \rightarrow X_{P_{\bullet \leq r}}^{[n]_0}$ comme ci-dessus, on a pour tout $m \leq n$ un choix naturel de $P_{\bullet \leq r} \rightarrow X_{P_{\bullet \leq r}}^{[m]_0}$, qui permet de calculer — jusqu'à des degrés arbitrairement grands — la flèche $\rho_m^* \mathcal{C}_P^{(m)}(\mathcal{F}_{\bullet \leq r}) \rightarrow \rho_n^* \mathcal{C}_P^{(n)}(\mathcal{F}_{\bullet \leq r})$, où ρ_j^* est le morphisme de topos $\mathrm{Tot} X_{\bullet \leq r} \rightarrow \mathrm{Tot} X_{\bullet \leq r}^{(?)}$.

4.2.6. Soit maintenant $f_{\bullet \leq r} : X_{\bullet \leq r} \rightarrow Y_{\bullet \leq r}$ un morphisme de k -schémas normaux simpliciaux tronqués. Expliquons brièvement comment calculer la flèche induite sur la cohomologie des topos totaux ℓ -étales n -approchés. On commence par produire une flèche simpliciale de points conservatifs $P_{\bullet \leq r}^X \rightarrow P_{\bullet \leq r}^Y$ au-dessus de $X_{\bullet \leq r} \rightarrow Y_{\bullet \leq r}$, que l'on relève arbitrairement aux schémas $X_i^{[n]}$ et $Y_i^{[n]}$, puis on construit l'unique morphisme simplicial $X_{P_{\bullet \leq r}^X}^{[n]} \rightarrow Y_{P_{\bullet \leq r}^Y}^{[n]}$ au-dessus de $X_{\bullet \leq r} \rightarrow Y_{\bullet \leq r}$ les respectant. On peut alors calculer un morphisme de résolution de Godement $\mathcal{C}_{P^Y}^{(n)}(\mathcal{F}_{\bullet \leq r}) \rightarrow \mathcal{C}_{P^X}^{(n)}(\mathcal{F}_{\bullet \leq r})$ au-dessus du morphisme de topos $\mathrm{Top} X_{\bullet \leq r}^{(n)} \rightarrow \mathrm{Top} Y_{\bullet \leq r}^{(n)}$.

4.3. Pour référence ultérieure, résumons les rappels et observations précédentes sous la forme suivante.

Proposition 4.3.1. *Soient k un corps algébriquement clos, ℓ un nombre premier inversible sur k , $r \geq 0$ un entier et $X_{\bullet \leq r}$ un k -schéma algébrique normal simplicial tronqué. Pour tout ℓ -groupe abélien fini Λ et tout triplet d'entiers $d \geq 0$, $n \geq m \geq 1$, on peut calculer le complexe $\tau_{\leq d} \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \Lambda)$ et la flèche*

$$\tau_{\leq d} \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet \leq r}^{(m)}, \Lambda) \rightarrow \tau_{\leq d} \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \Lambda).$$

De plus, donné un morphisme $X_{\bullet \leq r} \rightarrow Y_{\bullet \leq r}$ de k -schémas algébriques normaux simpliciaux tronqués, on peut calculer la flèche

$$\tau_{\leq d} R\Gamma(\text{Tot } Y_{\bullet \leq r}^{(n)}, \Lambda) \rightarrow \tau_{\leq d} R\Gamma(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda).$$

Par « calcul » d'un complexe ou d'une flèche, on entend par là que l'on peut trouver des représentants explicites au sens de 13.3.

Remarque 4.3.2. Considérant le cas particulier $m = 1$, on voit que l'on peut calculer les flèches

$$\tau_{\leq d} \check{R}\Gamma(X_{\bullet \leq r}, \Lambda) \rightarrow \tau_{\leq d} R\Gamma(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda),$$

où le terme de gauche est le tronqué du complexe associé au Λ -module cosimplicial tronqué des $\Gamma(X_i, \Lambda)$. Cela résulte du fait que $X_{\bullet \leq r}^{(1)} = \pi_0(X_{\bullet \leq r})$ (voir 3.2.2).

5. Systèmes essentiellement constants

5.1. Soit \mathcal{A} une catégorie abélienne satisfaisant les conditions AB3 et AB5 [Grothendieck 1957, I] — qui garantissent l'existence et l'exactitude des colimites filtrantes — et $A_\bullet = (A_i)$ un système inductif de \mathcal{A} indexé par \mathbb{N} . Notons A_∞ la colimite de A_\bullet et, pour chaque $j \leq k$ dans $\mathbb{N} \cup \{\infty\}$, posons $A(j, k) := \text{Im}(A_j \rightarrow A_k)$. Si $j^- \leq j \leq k \leq k^+$, on a naturellement des flèches $A(j^-, k) \hookrightarrow A(j, k) \twoheadrightarrow A(j, k^+)$. Si A_∞ est *nœthérien*, il existe un j tel que $A(j, \infty) = A_\infty$; si de plus A_j est *nœthérien*, il existe un $k \geq j$ tel que $A(j, k) \xrightarrow{\sim} A(j, \infty) = A_\infty$.

Définition 5.2. Soient \mathcal{A} une catégorie abélienne, i_0 un entier, et $c : \mathbb{N}_{\geq i_0} \rightarrow \mathbb{N} \times \mathbb{N}$ une fonction. On dit qu'un système inductif $A_\bullet = (A_i)$ de \mathcal{A} , indexé par $\mathbb{N}_{\geq i_0}$, est *c-essentiellement constant* si la colimite $A_\infty = \text{colim}_i A_i$ est représentable dans \mathcal{A} et si pour chaque $i \in \mathbb{N}_{\geq i_0}$, tel que $c(i) = (j, k)$, l'inégalité $i \leq j \leq k$ est satisfaite et la flèche canonique $A(j, k) \rightarrow A_\infty$ est un *isomorphisme*.

5.3. Variante : soient $N \geq i_0$ deux entiers et $\phi : \mathbb{N}_{\geq i_0} \rightarrow \mathbb{N}$ une fonction telle que $\phi(j) \geq j$ pour tout $j \in \mathbb{N}_{\geq i_0}$. On dit qu'un système inductif $A_{\geq i_0}$ est (N, ϕ) -*essentiellement constant* si :

- (i) pour chaque j , le système inductif $A(j, k)_{k \geq \phi(j)}$, à flèches de transition *a priori* épimorphiques, est constant ;
- (ii) le système inductif $A(j, \phi(j))_{j \geq N}$, à flèches de transition *a priori* monomorphiques, est constant.

Explicitement : (i) $\text{Ker}(A_j \rightarrow A_{\phi(j)}) \xrightarrow{\sim} \text{Ker}(A_j \rightarrow A_k)$ pour $k \geq \phi(j)$ et (ii) $\text{Im}(A_N \rightarrow A_{\phi(j)}) \xrightarrow{\sim} \text{Im}(A_j \rightarrow A_{\phi(j)})$ pour $j \geq N$.

Nous laissons le soin au lecteur de vérifier que, donné c , on peut calculer une paire (N, ϕ) telle que tout système inductif c -essentiellement constant soit (N, ϕ) -essentiellement et que, réciproquement, donnée (N, ϕ) , on peut calculer un c .

5.4. Il résulte des observations précédentes que si A_\bullet est un système inductif constitué d'objets \mathfrak{N} ethériens et à colimite \mathfrak{N} ethérienne, il existe une telle fonction. Nous dirons, de façon un peu vague, qu'un système inductif est *explicitement essentiellement constant* s'il est (N, φ) -essentiellement constant pour un entier N et une fonction φ calculables en fonction des données. Cette notion apparaît, avec un but semblable, dans [Schön 1991], puis [Rubio et Sergeraert 2002, §2.1], où un tel système inductif est appelé « module de Schön ». Voir également [Grothendieck 1956, p. 3].⁷

5.5. Notons qu'un tel système inductif est essentiellement constant au sens usuel : il appartient à l'image essentielle du plongement de \mathcal{A} dans la catégorie abélienne (cf. p. ex. [Kashiwara et Schapira 2006, 8.6.5(i)]) des ind-objets $\text{Ind}(\mathcal{A})$. La proposition clef suivante est le pendant « explicite », du fait que la catégorie \mathcal{A} est naturellement une sous-catégorie épaisse de $\text{Ind}(\mathcal{A})$ (cf. p. ex. [Kashiwara et Schapira 2006, 8.6.11]).

Proposition 5.6. *Soit $0 \rightarrow A'_\bullet \rightarrow A_\bullet \rightarrow A''_\bullet \rightarrow 0$ une suite exacte de systèmes inductifs. Si deux des trois termes sont explicitement essentiellement constants, il en est de même du troisième.*

Cette proposition est élémentaire et bien connue (cf. [Schön 1991, lemme 5, p. 4] ou [Rubio et Sergeraert 2002, théorème 2.3]). Pour la commodité du lecteur, nous en donnons une démonstration, dans le cas d'une catégorie de modules pour simplifier l'exposition.

Démonstration. Supposons d'abord que (A_n) et (A''_n) soient respectivement (N, ϕ) -et (N'', ϕ'') -essentiellement constants. La première condition de 5.3 est vérifiée de (A'_n) pour la fonction ϕ : en effet, un élément de A'_n qui s'annule dans A'_m pour $m \geq \phi(n)$ s'annule en particulier dans A_m (d'après la même condition sur (A_n)) donc s'annule dans $A_{\phi(n)}$ donc dans $A'_{\phi(n)}$. Soit maintenant $N' = \phi''(N)$ (qui est supérieur ou égal à N) : si x appartient à A'_n , son image dans $A'_{\phi(n)}$ vue dans $A_{\phi(n)}$ est l'image d'un élément y de A_N (d'après la deuxième condition sur le système (A_n)) : l'image de ce y dans A''_N s'annule dans $A''_{\phi(n)}$, c'est-à-dire appartient à $\text{Ker}(A''_N \rightarrow A''_{\phi(n)})$, et la première condition sur (A''_n) entraîne que cette image s'annule dans $A''_{N'}$, donc l'image de y dans $A_{N'}$ provient d'un élément de $A'_{N'}$, qui par construction a la même image dans $A'_{\phi(n)}$ que l'élément x qu'on s'était fixé. On a donc montré que le système (A'_n) était (N', ϕ) -essentiellement constant (pour $N' = \phi''(N)$).

Supposons maintenant que (A_n) et (A'_n) soient respectivement (N, ϕ) -et (N', ϕ') -essentiellement constants. Soit $z \in A''_n$ avec $n \geq N'$, et soit $m \geq n$ tel que l'image de z s'annule dans A''_m : alors, si y est un relèvement quelconque de z à A_n , l'image

7. Nous remercions Luc Illusie de nous avoir communiqué cette référence.

de y dans A_m'' s'annule, donc l'image de y dans A_m provient d'un $x \in A_m'$; puisque (A_n') est essentiellement constant, il existe $x_0 \in A_n'$ tel que x_0 et x aient même image dans $A_{\phi'(m)}'$; alors $y' := y - x_0$ (vu comme élément de A_n) a une image nulle dans $A_{\phi'(m)}$: donc l'image de y' dans $A_{\phi(n)}$ est déjà nulle (d'après la première condition sur (A_n)), mais ceci implique que l'image de z dans $A_{\phi(n)}''$ est nulle. Ceci montre la première condition pour (A_n'') , pour la fonction ϕ'' égale à $\max(\phi, N')$. S'agissant de la seconde condition, si $z \in A_n''$ et si y en est un relèvement quelconque à A_n , il existe un \tilde{y} dans A_N tel que y et \tilde{y} aient la même image dans $A_{\phi''(n)}$, et alors l'image \tilde{z} de \tilde{y} dans A_N'' a la même image que z dans $A_{\phi''(n)}''$. On a donc montré que le système (A_n'') était (N, ϕ'') -essentiellement constant (pour $\phi'' = \max(\phi, N')$).

Enfin, supposons que (A_n') et (A_n'') soient respectivement (N', ϕ') - et (N'', ϕ'') -essentiellement constants. Soit $y \in A_n$ qui s'annule dans A_m pour $m \geq n$: alors en particulier son image dans A_m'' s'annule, donc elle s'annule déjà dans $A_{\phi''(n)}''$ (d'après la première propriété sur (A_n'')); donc l'image de y dans $A_{\phi(n)}$ provient d'un élément x de $A_{\phi''(n)}'$; si $m \geq \phi''(n)$, l'image de x dans A_m' s'annule et s'annule donc déjà (d'après la première propriété sur (A_n')) dans $A_{\phi'(\phi''(n))}'$. Ceci montre la première condition sur (A_n) pour la fonction $\phi: n \mapsto \phi'(\phi''(n))$. Enfin, soit $y \in A_n$: son image dans A_n'' a la même image dans $A_{\phi''(n)}''$ qu'un certain élément $\tilde{z} \in A_{N''}$, donc si \tilde{y} est un relèvement quelconque de \tilde{z} à $A_{N''}$, les éléments y et \tilde{y} (de A_n et $A_{N''}$ respectivement) ont même image dans $A_{\phi''(n)}$, donc la différence entre ces images provient d'un élément $x \in A_{\phi''(n)}'$; ce dernier a la même image dans $A_{\phi(n)}' = A_{\phi'(\phi''(n))}'$ qu'un certain élément $\tilde{x} \in A_{N'}$: si on appelle N le maximum de N' et N'' alors la somme des images de \tilde{x} et \tilde{y} dans $A_{\phi(n)}$ est la même que celle de y . On a donc montré que le système (A_n) était (N, ϕ) -essentiellement constant pour $\phi = \phi' \circ \phi''$ et $N = \max(N', N'')$. \square

5.7. Soient \mathcal{A} une catégorie abélienne, et $(E_{r,\lambda}^{\star,\star})_{\lambda \in \mathbb{N}}$ un système inductif (indexé par λ) de suites spectrales ($r \geq r_0$) d'objets de \mathcal{A} , supposées dans le premier quadrant, dont on note, pour chaque indice λ , l'aboutissement E_λ^\star . (Suivant p. ex. [ÉGA III₁ 1961, 0, §11.1], on considère que cet objet filtré de \mathcal{A} fait partie de la donnée.)

Corollaire 5.8. Soit m un entier tel que les systèmes inductifs $(E_{r_0,\lambda}^{p,q})_\lambda$ soient explicitement essentiellement constants pour chaque paire d'entiers p, q d'entiers tels que $p + q \leq 2m + 1$. Alors, pour chaque $0 \leq d \leq m$, le système inductif $(E_\lambda^d)_\lambda$ est explicitement essentiellement constant.

Démonstration. Pour chaque indice λ , le calcul de $E_{r,\lambda}^{p,q}$ ne fait intervenir que des flèches entre sous-quotients de $E_{r_0,\lambda}^{p',q'}$ avec $p' + q' \leq p + q + (r - r_0)$. Comme d'autre part $E_{\infty,\lambda}^{p,q} = E_{r,\lambda}^{p,q}$ si $r > p + q + 1$, il résulte de la proposition précédente (5.6) que les systèmes inductifs $(E_{\infty,\lambda}^{p,q})_\lambda$ pour $p + q < m$ sont explicitement essentiellement constants. Enfin, comme pour chaque $0 \leq d \leq m$ l'aboutissement E_λ^d est une

extension itérée de ces $E_{\infty, \lambda}^{p, q}$ la conclusion résulte d'une nouvelle application de *loc. cit.* □

Proposition 5.9. *Soient $A_{\bullet} \rightarrow B_{\bullet}$ un morphisme de systèmes inductifs et $\tau : \mathbb{N} \rightarrow \mathbb{N}$ une fonction strictement croissante. Supposons qu'il existe un diagramme commutatif*

$$\begin{array}{ccc}
 A_{\bullet} & \longrightarrow & B_{\bullet} \\
 \downarrow & \swarrow h_{\bullet} & \downarrow \\
 A_{\tau(\bullet)} & \longrightarrow & B_{\tau(\bullet)}
 \end{array}$$

Alors, si B_{\bullet} est (N, ϕ) -essentiellement constant, le système inductif A_{\bullet} est $(\tau N, \tau \phi)$ -essentiellement constant. En particulier, lorsque τ est calculable, le système inductif A_{\bullet} est explicitement essentiellement constant si B_{\bullet} l'est.

Démonstration. Soit j un entier. Remplaçons, dans le carré commutatif de l'énoncé, le système inductif A_{\bullet} (resp. B_{\bullet} , etc.) par le système $A'_{\bullet} := A(j, \bullet \geq \phi(j))$ — à morphismes de transition épimorphiques — (resp. $B'_{\bullet} := B(j, \bullet \geq \phi(j))$ — constant par hypothèse —, etc.). La commutativité du diagramme montre alors que h'_{\bullet} est un isomorphisme ; le système inductif $(A'_k)_{k \geq \phi(j)}$ est donc constant pour $k \geq \tau \phi(j)$. Posons $\psi = \tau \phi$. Le même argument, appliqué à $A''_{\bullet} := A(j, \psi(j))_j$, etc. montre que ce système est constant pour $j \geq \tau(N)$. (On utilise le fait que B est (N, ψ) -essentiellement constant car $\psi \geq \phi$.) □

6. Approximation d'un pro- ℓ -groupe par ses quotients finis

Pour π un ℓ -groupe fini, on rappelle qu'on a défini en §3 la filtration ℓ -centrale descendante par $F^1 \pi = \pi$ et $F^{n+1} \pi = (F^n \pi)^{\ell} \cdot (\pi, F^n \pi)$ (groupe topologiquement engendré).

Lemme 6.1. *Il existe deux fonctions calculables φ_{ℓ} et ψ_{ℓ} telles que :*

- (i) *si π est un ℓ -groupe fini d'ordre $\leq n$ alors $F^{\varphi_{\ell}(n)} \pi = 1$, et*
- (ii) *si π est un ℓ -groupe fini à d générateurs tel que $F^n \pi = 1$, alors $\#\pi \leq \psi_{\ell}(d, n)$.*

Il résulte de la démonstration que $\ell^{(d+1)^n}$ convient pour $\psi_{\ell}(d, n)$, et que 1 plus la valuation ℓ -adique de n convient pour $\varphi_{\ell}(n)$.

Démonstration. Pour ce qui est de φ : pour chaque ℓ -groupe fini il existe un r tel que $F^r \pi = 1$ (cf. [Neukirch, Schmidt et Wingberg 2000, proposition 3.8.2]) ; or comme $F^{i+1} \pi$ est défini en fonction de π et de $F^i \pi$, deux termes consécutifs de la suite $F^i \pi$ ne peuvent pas être égaux sauf à ce que cette suite stationne, et on vient de dire que ceci ne se produit que pour $F^i \pi = 1$: il en résulte que la valuation ℓ -adique de l'ordre de $F^i \pi$ doit décroître strictement jusqu'à atteindre 0, donc la valuation ℓ -adique de n (plus 1, puisque la filtration $F^i \pi$ est numérotée à partir de 1) convient pour $\varphi_{\ell}(n)$.

Pour ce qui est de ψ : d'après [Lubotzky et Segal 2003, théorème 3.5.1], si L est le pro- ℓ -groupe libre sur $d \geq 2$ générateurs et N un sous-groupe distingué ouvert de L d'indice $\ell^s > 1$, si on note $N' = N^\ell \cdot (N, L)$, on a $(N : N') \leq \ell^{(d-1)s+1}$, de sorte que $(L : N') \leq \ell^{ds+1} \leq \ell^{(d+1)s}$; en appliquant ceci à $N = F^r L$ et par récurrence sur r on en déduit $(L : F^r L) \leq \ell^{(d+1)^r}$ (on vérifie immédiatement que cette inégalité fonctionne encore pour $d = 1$ et $r = 1, 2$). Par conséquent, si π est un ℓ -groupe fini à d générateurs tel que $F^n \pi = 1$, en considérant $L \twoheadrightarrow \pi$ la surjection donnée par ces d générateurs, on a une surjection $L/F^n L \twoheadrightarrow \pi$, donc $\#\pi \leq \ell^{(d+1)^n}$. \square

6.2. Il résulte de ce lemme que pour chaque ℓ et chaque d , on peut calculer (au sens de 3.3.2) le ℓ -groupe fini $L^{(n)}$ quotient du pro- ℓ groupe libre L à d générateurs : parmi les groupes π comme en (ii) ci-dessus, c'est celui ayant le plus gros cardinal. (Notons qu'ici, il est *a priori* trivial de déterminer une présentation finie de $L^{(n)}$: c'est le quotient du pro- ℓ -groupe libre L par $L^{[n]}$. Par Frattini, le nombre minimal de générateurs de $L^{(n)}$ est d ; par Golod–Šafarevič [Serre 1994, I, §4.4], le nombre de relations entre ces générateurs est $> \frac{1}{4}d^2$.) En conséquence, on peut — pour chaque entier n — déterminer explicitement le système projectif tronqué $L^{(\bullet \leq n)}$ et un système compatible de d générateurs.

Proposition 6.3 (lemme d'Artin–Rees–Frattini effectif). *Il existe une fonction τ_ℓ calculable telle que, si $1 \rightarrow \pi' \rightarrow \pi \rightarrow \pi'' \rightarrow 1$ est une suite exacte courte de pro- ℓ -groupes, où π', π'' ont respectivement d', d'' générateurs, on a $F^{\tau_\ell(d', d'', n)} \pi \cap \pi' \subseteq F^n \pi' \subseteq F^n \pi \cap \pi'$ pour tout n .*

Démonstration. Il est évident que $F^n \pi' \subseteq F^n \pi \cap \pi'$. On souhaite montrer que, réciproquement, $F^n \pi' \supseteq F^{\tau(n)} \pi \cap \pi'$ pour une certaine fonction τ explicitement calculable (dépendant du nombre d', d'' de générateurs de π', π'' , mais pas d'autres données).

Expliquons pourquoi on peut supposer que π'' est libre (en tant que pro- ℓ -groupe) : il existe en tout cas un morphisme surjectif $L \twoheadrightarrow \pi''$ où L est le pro- ℓ -groupe libre sur d'' générateurs ; et quitte à relever à π les images par ce morphisme de chacun des générateurs, on peut le factoriser comme la composée d'un morphisme $s : L \rightarrow \pi$ et de la surjection donnée $\pi \twoheadrightarrow \pi''$. Soit $\hat{\pi} = \pi \times_{\pi''} L$ l'ensemble des éléments de $\pi \times L$ dont les deux composantes ont même image dans π'' (la première projection est donc un morphisme surjectif $\hat{\pi} \twoheadrightarrow \pi$ qui se restreint à l'identité sur π') : ce $\hat{\pi}$, qui s'inscrit dans une suite exacte $1 \rightarrow \pi' \rightarrow \hat{\pi} \rightarrow L \rightarrow 1$, se décrit aussi comme le produit semidirect $\hat{\pi} = \pi' \rtimes_* L$ par l'action de L sur π' donnée par $z * x = s(z) x s(z)^{-1}$. Si on a montré la conclusion voulue pour la suite exacte $1 \rightarrow \pi' \rightarrow \hat{\pi} \rightarrow L \rightarrow 1$, la même vaut encore pour $1 \rightarrow \pi' \rightarrow \pi \rightarrow \pi'' \rightarrow 1$ (puisque l'image de $F^N \hat{\pi}$ dans π est contenue dans, et même égale à, $F^N \pi$).

On peut donc bien supposer que π'' est libre, et qu'il existe une section $s : \pi'' \rightarrow \pi$, qui fait de π le produit semidirect $\pi = \pi' \rtimes_* \pi''$ où $*$ désigne l'action de π'' sur π' définie par $z * x = s(z) x s(z)^{-1}$.

Fixons n . On veut montrer qu'il existe N tel que $F^n \pi' \supseteq F^N \pi \cap \pi'$, et expliquer pourquoi N se calcule sous la forme $\tau(d', d'', n)$ en fonction de d', d'' et n .

L'action de π'' sur π' stabilise $F^n \pi'$, donc définit une action sur $\pi' / F^n \pi'$, et on a $(\pi / F^n \pi') = (\pi' / F^n \pi') \rtimes_* \pi''$ pour cette action quotient.

Comme $\pi' / F^n \pi'$ est fini, $\text{Aut}(\pi' / F^n \pi')$ est lui-même fini, et comme $\pi'' \rightarrow \text{Aut}(\pi' / F^n \pi')$ (donné par $*$) est continu, et que les $F^m \pi''$ forment un système fondamental de voisinages de l'unité dans π'' , il existe m tel que $F^m \pi''$ agisse trivialement sur $\pi' / F^n \pi'$ (cf. [Neukirch, Schmidt et Wingberg 2000, proposition 3.8.2]). On peut être plus précis : on a $\#(\pi' / F^n \pi') \leq \psi(d', n)$ avec les notations du lemme, donc $\#\text{Aut}(\pi' / F^n \pi') \leq \psi(d', n)!$, donc $\varphi(\psi(d', n)!) \pi''$ convient (en considérant l'image de π'' dans $\text{Aut}(\pi' / F^n \pi')$) — ce qui nous importe est qu'un m qui convient puisse être calculé en fonction de d' et n .

L'action de π'' sur $\pi' / F^n \pi'$ passe donc au quotient par $F^m \pi''$, c'est-à-dire définit une action de $\pi'' / F^m \pi''$ sur $\pi' / F^n \pi'$, et on a $(\pi / F^n \pi') / s(F^m \pi'') = (\pi' / F^n \pi') \rtimes_* (\pi'' / F^m \pi'')$ pour cette action quotientée.

Notons $\bar{\pi}$ ce ℓ -groupe fini $\pi / ((F^n \pi') \cdot s(F^m \pi'')) = (\pi' / F^n \pi') \rtimes_* (\pi'' / F^m \pi'')$. Son ordre est majoré par $\psi(d', n) \times \psi(d'', m)$ (et rappelons que $m = \varphi(\psi(d', n)!) \pi''$ convient).

Il existe alors $N \geq n, m$ tel que $F^N \bar{\pi} = 1$: précisément, $\varphi(\psi(d', n) \times \psi(d'', m))$ convient pour N . On a alors $F^N \pi \subseteq (F^n \pi') \cdot s(F^m \pi'')$, donc $F^N \pi \cap \pi' \subseteq F^n \pi'$, ce qu'on voulait démontrer. □

Corollaire 6.4. *On reprend les hypothèses et les notations de la proposition. Soient $\tilde{\pi}'^{(n)} = \pi' / (\pi' \cap \pi^{[n]})$ le noyau de la surjection naturelle $\pi^{(n)} \twoheadrightarrow \pi''^{(n)}$ et Λ un groupe abélien. Pour tout entier j , si le système inductif $H^j(\pi'^{(n)}, \Lambda)$ est explicitement essentiellement constant, il en est de même de $H^j(\tilde{\pi}'^{(n)}, \Lambda)$. (La fonction explicitant ce fait fait intervenir uniquement d', d'' et celle explicitant le fait que $H^j(\pi'^{(n)}, \Lambda)$ est essentiellement constant.)*

Démonstration. Cela résulte de la proposition précédente, réécrite sous la forme d'un diagramme commutatif (pour chaque n)

$$\begin{array}{ccc}
 \tilde{\pi}'^{(n)} & \longleftarrow & \pi'^{(n)} \\
 \uparrow & \nearrow & \uparrow \\
 \tilde{\pi}'^{(\tau n)} & \longleftarrow & \pi'^{(\tau n)}
 \end{array}$$

et de 5.9. □

Proposition 6.5. Soient L un pro- ℓ -groupe libre à d générateurs topologiques, $n_0 \geq 1$ un entier, Λ un ℓ -groupe abélien fini et V un Λ -module de type fini muni d'une action explicite de $L^{(n_0)}$. Pour tout entier i , le système inductif $H^i(L^{(n)}, V)$, $n \geq n_0$, est explicitement essentiellement constant.

Par « action explicite », on entend la donnée d'une présentation explicite (13.3) de V et de d éléments de $\text{Aut}(V)$ (13.4) satisfaisant des relations explicites décrivant $L^{(n_0)}$ (cf. 6.2). Le module V est naturellement muni, pour chaque $n \geq n_0$, de l'action de $L^{(n)}$ déduite de la surjection $L^{(n)} \twoheadrightarrow L^{(n_0)}$.

Démonstration. Distinguons trois cas :

$i = 0$. Le système inductif $H^0(L^{(n)}, V)$ étant constant, il est (n_0, Id) -essentiellement constant (5.3).

$i = 1$. Rappelons (cf. p. ex. [Serre 1994, I, §2.6(b)]) que les flèches $H^1(L^{(n)}, V) \rightarrow H^1(L^{(n+1)}, V)$ sont injectives, de sorte que la propriété 5.3 (i) est satisfaite pour $\phi = \text{Id}$. (Notons que V est fixe par $L^{[n]}/L^{[n+1]}$.) Il reste à trouver $N \geq n_0$ tel que la flèche (injective) $H^1(L^{(N)}, V) \rightarrow H^1(L, V)$ soit un isomorphisme ou, de façon équivalente, tel que l'on ait l'égalité $\#H^1(L^{(N)}, V) = \#H^1(L, V)$. La conclusion résulte du fait que ces cardinaux sont calculables. Pour le terme de gauche c'est clair : on sait calculer le système projectif $L^{(n)}$; pour le terme de droite, rappelons [Ogg 1962, p. 188] que l'on a une suite exacte

$$0 \rightarrow H^0(L, V) \rightarrow V \rightarrow V^d \rightarrow H^1(L, V) \rightarrow 0$$

si bien que l'on a l'égalité (formule « d'Euler–Poincaré », due à Ogg et Šafarevič) $\#H^1(L, V) = (\#V)^{d-1} \times \#H^0(L, V)$.

$i \geq 2$. La colimite $H^i(L, V)$ étant nulle (cf. [Serre 1994, I, §3.4]), il suffit de trouver $\phi : \mathbb{N} \rightarrow \mathbb{N}$ telle que $H^i(L^{(n)}, V) \rightarrow H^i(L^{(\phi(n))}, V)$ soit nulle pour chaque $n \geq n_0$ et de poser, par exemple, $N = n_0$. Une telle fonction ϕ existe et est calculable car les objets et les flèches le sont. \square

Remarque 6.6. Bien que cela ne soit pas nécessaire — sauf pour ne pas perdre la primitive récursivité — signalons que l'on peut être plus précis. Avec les notations de l'énoncé, on a pour chaque $N \geq n \geq n_0$ un morphisme de la suite exacte

$$0 \rightarrow H^1(L^{(n)}, V) \rightarrow H^1(L, V) \rightarrow H^1(L^{[n]}, V)$$

vers la suite exacte

$$0 \rightarrow H^1(L^{(N)}, V) \rightarrow H^1(L, V) \rightarrow H^1(L^{[N]}, V),$$

où $L^{[n]}$ (resp. $L^{[N]}$) agit trivialement sur V et les flèches sont les flèches de functorialité évidentes. Par chasse au diagramme, l'injection $H^1(L^{(N)}, V) \hookrightarrow H^1(L, V)$

est un isomorphisme si la flèche « verticale » $H^1(L^{[n]}, V) \rightarrow H^1(L^{[N]}, V)$ est nulle. Il suffit pour cela que l'on ait l'inclusion $L^{[N]} \subseteq L^{[n][2]}$. À n fixé, un tel N peut être obtenu à partir de la suite exacte

$$1 \rightarrow L^{[n]} \rightarrow L \rightarrow L^{(n)} \rightarrow 1$$

par application de la proposition 6.3 et de l'estimation du rang du groupe libre $L^{[n]}$ par la formule de l'indice de Schreier ([Serre 1977, I, §3.4] ou [Rotman 1995, théorème 11.45]). Considérons maintenant le cas $i \geq 2$. La suite spectrale de Hochschild–Serre associée à la suite exacte précédente dégénère en E_3 , car $H^j(L^{[n]}, V)$ est nul pour $j > 1$. Comme l'aboutissement est nul — pour la même raison — en degré cohomologique > 1 , la flèche

$$d_2 : H^{i-2}(L^{(n)}, H^1(L^{[n]}, V)) \rightarrow H^i(L^{(n)}, V)$$

est surjective pour chaque $i \geq 2$. Ceci est bien entendu valable pour chaque $N \geq n$. Il en résulte que pour tuer la flèche $H^i(L^{(n)}, V) \rightarrow H^i(L^{(N)}, V)$, il suffit de tuer $H^1(L^{[n]}, V) \rightarrow H^1(L^{[N]}, V)$. C'est ce que l'on a fait ci-dessus.

Remarque 6.7. Il serait intéressant de calculer la plus petite fonction ϕ telle que les flèches $H^i(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^i(L^{(\phi(d,i,n))}, \mathbb{Z}/\ell\mathbb{Z})$ soient nulles. (Lorsque $d = 1$ — cas d'un pro- ℓ -groupe abélien libre — la fonction $n \mapsto n + 1$ convient.) Nous ignorons la réponse à cette question, mais nous indiquons un argument, duquel nous sommes redevables à Jean-Pierre Serre, qui montre que si $i = 2$ et si $L^{[n]}$ désigne maintenant la filtration de Frattini itérée $\Phi^n L$ plutôt que la filtration $F^n L$ considérée ci-dessus (cf. 3.1.2 à ce sujet), et bien sûr $L^{(n)} = L/\Phi^n L$, alors la fonction $n \mapsto n + 1$ convient. Autrement dit, la flèche $H^i(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^i(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est nulle.

En comparant les suites spectrales de Hochschild–Serre associées aux suites exactes $1 \rightarrow L^{[n]} \rightarrow L \rightarrow L^{(n)} \rightarrow 1$ et $1 \rightarrow L^{[n]}/L^{[n+1]} \rightarrow L^{(n+1)} \rightarrow L^{(n)} \rightarrow 1$, le morphisme évident de la seconde suite spectrale vers la première donne :

$$\begin{array}{ccccc} H^0(L^{(n)}, H^1(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z})) & \longrightarrow & H^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & H^2(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z}) \\ & & & & \downarrow \\ & \downarrow & & \parallel & \\ H^0(L^{(n)}, H^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z})) & \longrightarrow & H^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) & \longrightarrow & H^2(L, \mathbb{Z}/\ell\mathbb{Z}) = 0 \end{array}$$

Or la flèche canonique de $H^1(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z}) = \text{Hom}(L^{[n]}/L^{[n+1]}, \mathbb{Z}/\ell\mathbb{Z})$ vers

$$H^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z}) = \text{Hom}(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z})$$

est un isomorphisme puisque nous avons pris la filtration où $L^{[n+1]}$ est le Frattini de $L^{[n]}$. Comme tout élément de $H^2(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z})$ se relève à $H^0(L^{(n)}, H^1(L^{[n]}, \mathbb{Z}/\ell\mathbb{Z}))$, on en conclut que son image dans $H^2(L^{(n+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est nulle.

7. Calcul de la cohomologie d'une polycourbe ℓ -élémentaire

7.1. Soit X une polycourbe ℓ -élémentaire sur $\text{Spec}(k)$, où k est un corps algébriquement clos, que l'on peut supposer factorisée en courbes ℓ -élémentaires ($X = X_m \rightarrow X_{m-1} \rightarrow \dots \rightarrow X_1 \rightarrow \text{Spec } k$ où $\dim X_i = i$). D'après 1.4.7, c'est un $K(\pi, 1)$ pro- ℓ , où π est le pro- ℓ complété du groupe fondamental de X , qui est extension itérée de pro- ℓ groupes libres de type fini. En particulier, pour chaque ℓ -groupe abélien fini Λ et chaque entier $d \geq 0$ le groupe $H^d(X, \Lambda)$ est canoniquement isomorphe à $H^d(\pi, \Lambda)$ qui s'identifie, d'après l'égalité $\pi = \lim_n \pi^{(n)}$ (3.2.1) et [Serre 1994, I, §2.2, proposition 8], à la colimite des $H^d(\pi^{(n)}, \Lambda)$.

L'objectif de cette section est de montrer que l'on peut déterminer une paire (N_d, ϕ_d) telle que ce système inductif $H^d(\pi^{(n)}, \Lambda)$, $n \geq 0$, soit (N_d, ϕ_d) -essentiellement constant au sens de 5.3.

7.2. Dévissage. On raisonne par récurrence sur la dimension m de X . Par hypothèse (cf. 1.4.7, démonstration), le groupe π s'insère dans une suite exacte

$$1 \rightarrow \pi' \rightarrow \pi \rightarrow \pi'' \rightarrow 1,$$

où π'' est un pro- ℓ groupe libre (non abélien) et π' est une extension itérée de tels groupes. Cette suite exacte est d'origine géométrique, c'est-à-dire déduite de morphismes calculables de schémas (normaux connexes) comme ci-dessous, par application du foncteur « groupe fondamental pro- ℓ ».

$$\begin{array}{ccccc}
 \pi & X & \longleftarrow & X_{\bar{\eta}} & \pi' \\
 & \downarrow & & \downarrow & \\
 [\text{pro-}\ell\text{-libre}] \pi'' & Y & \longleftarrow & \bar{\eta} & \\
 & \downarrow & & & \\
 & k & & &
 \end{array}$$

(où $Y = X_1$ est une courbe ℓ -élémentaire et $\bar{\eta}$ un point générique géométrique de celle-ci ; soulignons que $X_{\bar{\eta}} \rightarrow \bar{\eta}$ est encore une polycourbe ℓ -élémentaire, cette fois de dimension $m - 1$). Notons que l'on peut calculer le nombre de pro-générateurs (3.3.3) de π'' et π' , qui apparaissent dans le lemme d'Artin-Rees-Frattini effectif 6.3. (Pour π' , on peut procéder par récurrence ou bien utiliser la calculabilité du H^1 .)

Fixons j . D'après 3.3 et 3.4.1, on peut calculer pour chaque $n \geq 1$ la suite exacte $1 \rightarrow \tilde{\pi}^{(n)} \rightarrow \pi^{(n)} \rightarrow \pi''^{(n)} \rightarrow 1$ (de groupes finis) considérée en 6.4 et, en particulier, calculer $\tilde{\pi}^{(n)} = \pi' / (\pi' \cap \pi^{[n]})$. L'hypothèse de récurrence permet d'affirmer que le système inductif $H^j(\pi^{(n)}, \Lambda)$ est explicitement essentiellement constant. D'après *loc. cit.*, il en est de même de $V_n := H^j(\tilde{\pi}^{(n)}, \Lambda)$. (Comme rappelé en 4.2.4, on sait calculer chacun de ces différents groupes de cohomologie.)

7.3. Cas d'une courbe. Soit $V = \text{colim}_n V_n$; c'est un Λ -module de type fini. Il résulte du caractère explicitement essentiellement constant de la colimite que l'on peut calculer V ainsi que l'action induite d'un quotient explicite $\pi''^{(n_0)}$ de π'' . Fixons i . D'après 6.5, on peut calculer un couple (M, ψ) tel que le système $H^i(\pi''^{(n)}, V)$, $n \geq n_0$, soit (M, ψ) -essentiellement constant. On veut montrer que, quitte à changer M et ψ , il en est de même du système inductif $H^i(\pi''^{(n)}, V_n)$. Par hypothèse, il existe un entier $N \geq n_0$ et une fonction strictement croissante $\phi : \mathbb{N} \rightarrow \mathbb{N}$ tels que $(V_n)_n$ soit (N, ϕ) -essentiellement constant ; en particulier, le morphisme $(V_n)_{n \geq N} \rightarrow (V_{\phi(n)})_{n \geq N}$ se factorise à travers le morphisme $(V_n)_n \rightarrow (V)_n$, où $(V)_n$ est le système inductif constant de valeur V . Passant à la cohomologie, on en déduit un diagramme commutatif

$$\begin{array}{ccc}
 H^i(\pi''^{(\bullet)}, V_{\bullet}) & \longrightarrow & H^i(\pi''^{(\bullet)}, V) \\
 \downarrow & \swarrow h_{\bullet} & \downarrow \\
 H^i(\pi''^{(\phi(\bullet))}, V_{\phi(\bullet)}) & \longrightarrow & H^i(\pi''^{(\phi(\bullet))}, V)
 \end{array}$$

D'après 5.9, le système inductif $H^i(\pi''^{(\bullet)}, V_{\bullet})$ est $(\phi M, \phi \psi)$ -essentiellement constant.

7.4. Suite spectrale de Hochschild–Serre. Revenons maintenant au calcul de la cohomologie du schéma X . On a

$$\text{R}\Gamma(X, \Lambda) = \text{R}\Gamma(\pi, \Lambda) = \text{R}\Gamma(\pi'', \text{R}\Gamma(\pi', \Lambda)),$$

que l'on approche par

$$\text{R}\Gamma(\pi^{(n)}, \Lambda) = \text{R}\Gamma(\pi''^{(n)}, \text{R}\Gamma(\tilde{\pi}''^{(n)}, \Lambda)).$$

D'après [Serre 1994, I, §2.6], on a pour chaque entier $\lambda \geq 1$ une suite spectrale

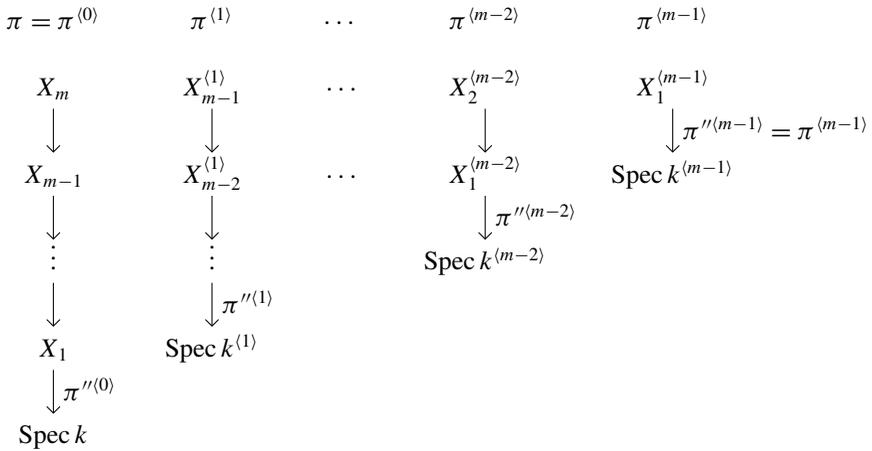
$$E_{2,\lambda}^{i,j} = H^i(\pi''^{(\lambda)}, H^j(\tilde{\pi}''^{(\lambda)}, \Lambda)) \implies H^{i+j}(\pi^{(\lambda)}, \Lambda).$$

Il résulte de 5.8 et de ce qui précède que pour chaque entier $d \geq 0$ on peut calculer (N_d, ϕ_d) tels que le système inductif $H^d(\pi^{(\bullet)}, \Lambda)$ soit (N_d, ϕ_d) -essentiellement constant. En particulier, on peut trouver deux entiers $\alpha \leq \beta$ tels que

$$H^d(\pi, \Lambda) = \text{Im}(H^d(\pi^{(\alpha)}, \Lambda) \rightarrow H^d(\pi^{(\beta)}, \Lambda)).$$

Ces objets sont donc algorithmiquement calculables.

7.5. Synthèse. Résumons la situation de cette section sous la forme du diagramme suivant avec des notations légèrement différentes pour expliciter la récurrence :



Si $X = X_m \rightarrow X_{m-1} \rightarrow \dots \rightarrow X_1 \rightarrow \text{Spec } k$ est la polycourbe ℓ -élémentaire de départ, on appelle $X_{m-i}^{(i)} \rightarrow X_{m-i-1}^{(i)} \rightarrow \dots \rightarrow X_1^{(i)} \rightarrow \text{Spec } k^{(i)}$ sa fibre au-dessus d'un point générique géométrique de X_i , et $\pi^{(i)}$ le groupe fondamental pro- ℓ de cette fibre $X_{m-i}^{(i)}$, ainsi que $\pi''^{(i)}$ celui de $X_1^{(i)}$. Les $\pi''^{(i)}$ sont des groupes pro- ℓ -libres dont on peut calculer le nombre de générateurs ; les $\pi^{(i)}$ s'inscrivent dans des suites exactes $1 \rightarrow \pi^{(i+1)} \rightarrow \pi^{(i)} \rightarrow \pi''^{(i)} \rightarrow 1$, permettant de calculer leur nombre de générateurs, et des fonctions explicitant le fait que les $H^d(\pi^{(i)}, \Lambda)$ sont essentiellement constants.

8. Descente

8.1. Soient k un corps algébriquement clos, X un k -schéma algébrique (supposé décrit comme en 16.2), et ℓ un nombre premier inversible sur k . D'après 1.4.12, il existe un X -schéma simplicial X_\bullet calculant la cohomologie étale de X à coefficients dans le ℓ -groupe abélien fini Λ , et dont les constituants sont des coproduits de polycourbes ℓ -élémentaires. Par descente cohomologique et 1.4.4, les flèches ci-dessous sont des isomorphismes :

$$\text{R}\Gamma(X_{\text{ét}}, \Lambda) \xrightarrow{\sim} \text{R}\Gamma(\text{Tot } X_{\bullet, \text{ét}}, \Lambda) \xleftarrow{\sim} \text{R}\Gamma(\text{Tot } X_{\bullet, \ell \text{ét}}, \Lambda),$$

où $\text{Tot } X_{\bullet, \text{ét}}$ (resp. $\text{Tot } X_{\bullet, \ell \text{ét}}$) désigne le topos total associé au système simplicial des topos $X_{i \text{ét}}$ (resp. $X_{i \ell \text{ét}}$), $i \geq 0$. Le second isomorphisme résulte du fait que les images directes entre topos simpliciaux se calculent étage par étage, si bien que l'adjonction est un isomorphisme si elle l'est sur chaque étage (cf. [Deligne 1974, 5.2.5] ou [Illusie 1972, VI.5.8.1 (iii)]).

8.2. Fixons un entier $d \geq 0$ puis un entier $r > d$. D'après les observations précédentes et 1.4.13, il existe un X -schéma simplicial X_\bullet , à tronqué (= squelette) $X_{\bullet, \leq r}$ calculable, tel que $H^d(X_{\text{ét}}, \Lambda) = H^d(\text{Tot } X_{\bullet, \ell \text{ét}}, \Lambda)$ et tel que les X_i soient des

coproduits finis de k -polycourbes ℓ -élémentaires.

Pour alléger les notations, on omet dorénavant les indices « ℓ ét » et « ét ».

Pour chaque entier $\lambda \geq 2$, on a une suite spectrale [Illusie 1972, VI.6.2.3.2]

$$E_{1,\lambda}^{i,j} = H^j(X_i^{(\lambda)}, \Lambda) \implies H^{i+j}(\text{Tot } X_{\bullet}^{(\lambda)}, \Lambda),$$

où les topos $X_i^{(\lambda)}$ sont comme définis en 3.2. Il résulte donc de l'exactitude des colimites filtrantes [ÉGA III₁ 1961, 0.11.1.8] et des isomorphismes

$$\text{colim}_{\lambda} H^j(X_i^{(\lambda)}, \Lambda) \xrightarrow{\sim} H^j(X_i, \Lambda),$$

que la cohomologie de $\text{Tot } X_{\bullet}$ est colimite de la cohomologie des $\text{Tot } X_{\bullet}^{(\lambda)}$. D'autre part, d'après les résultats de §7 (cas d'une polycourbe ℓ -élémentaire), on peut calculer (N_1, ϕ_1) tels que les systèmes inductifs $(E_{1,\lambda}^{i,j})_{\lambda}$ soient (N_1, ϕ_1) -essentiellement constants pour chaque $i, j \geq 0$ tels que $i + j \leq 2d + 1$. Il en résulte (5.8) que l'on peut calculer $(N_{\infty}, \phi_{\infty})$ tels que le système inductif $H^d(\text{Tot } X_{\bullet}^{(\lambda)}, \Lambda)$ soit $(N_{\infty}, \phi_{\infty})$ -essentiellement constants ; en particulier, on peut calculer deux entiers $\mu \leq \nu$ tels que l'on ait

$$H^d(X, \Lambda) = \text{Im}(H^d(\text{Tot } X_{\bullet}^{(\mu)}, \Lambda) \rightarrow H^d(\text{Tot } X_{\bullet}^{(\nu)}, \Lambda)).$$

Comme expliqué en 4.1.2, on a $H^d(\text{Tot } X_{\bullet}^{(\mu)}, \Lambda) \xrightarrow{\sim} H^d(\text{Tot } X_{\bullet \leq r}^{(\mu)}, \Lambda)$, et de même pour ν . Que l'on puisse trouver une présentation explicite (13.3) de $H^d(X, \Lambda)$ résulte alors de la proposition 4.3.1.

8.3. Hyper-Čech.

8.3.1. Soit $X'_{\bullet} \rightarrow X$ un hyperrecouvrement pour la topologie des altérations. Vérifions que l'on peut calculer les morphismes $\check{H}^d(X'_{\bullet}, \Lambda) \rightarrow H^d(X, \Lambda)$, comme annoncé en 0.4.

D'après le lemme 1.4.13, on peut calculer (en tout étage) un hyperrecouvrement $X_{\bullet} \rightarrow X$ comme ci-dessus, se factorisant à travers un morphisme $X_{\bullet} \rightarrow X'_{\bullet}$. Fixons $d \geq 0$. On sait que la flèche $\check{H}^d(X'_{\bullet}, \Lambda) \rightarrow H^d(X, \Lambda)$ est la composée des flèches $\check{H}^d(X'_{\bullet}, \Lambda) \rightarrow \check{H}^d(X_{\bullet}, \Lambda)$ et $\check{H}^d(X_{\bullet}, \Lambda) \rightarrow H^d(X, \Lambda)$, la première étant trivialement calculable pour des schémas simpliciaux donnés (par calculabilité fonctorielle du π_0). On est donc ramené au cas particulier où $X'_{\bullet} = X_{\bullet}$. La conclusion résulte alors d'une part du fait que, comme observé en 4.3.2, on a $\check{H}^d(X_{\bullet}, \Lambda) = H^d(\text{Tot } X_{\bullet \leq r}^{(1)}, \Lambda)$ pour $r > d$ et, d'autre part, de la calculabilité des flèches $H^d(\text{Tot } X_{\bullet \leq r}^{(\mu)}, \Lambda) \rightarrow H^d(\text{Tot } X_{\bullet \leq r}^{(\nu)}, \Lambda)$ pour $\mu \leq \nu \leq \infty$.

8.3.2. Il résulte de ce qui précède que, donnés deux hyperrecouvrements $X'_{\bullet} \rightarrow X_{\bullet}$ de X pour la topologie des altérations, on sait vérifier si la flèche $\check{H}^d(X_{\bullet}, \Lambda) \rightarrow H^d(X, \Lambda)$ identifie la cohomologie de X au quotient de $\check{H}^d(X_{\bullet}, \Lambda)$ par le noyau (calculable) de $\check{H}^d(X_{\bullet}, \Lambda) \rightarrow \check{H}^d(X'_{\bullet}, \Lambda)$. (D'autre part, on sait qu'il existe deux tels

hyperrecouvrements.) En particulier, si les X_{α_\bullet} sont comme en 0.2, le système inductif $\check{H}^d(X_{\alpha_\bullet}, \Lambda)$ est explicitement essentiellement constant (mais le « explicitement » utilise une recherche non bornée).

Remarque 8.3.3. Notons que si $V \rightarrow U$ est un morphisme de k -schémas algébriques se factorisant à travers un revêtement ℓ -étale n -approché universel $U^{[n]}$ de U , le morphisme de topos $V^{(n)} \rightarrow U^{(n)}$ se factorise à travers $V^{(n)} \rightarrow V^{(1)}$, dont le but est naturellement équivalent au topos discret des faisceaux sur $\pi_0(V)$. D'autre part, pour chaque X_\bullet comme en 8.2 et chaque entier $n \geq 1$, on devrait sans aucun doute pouvoir fabriquer en utilisant les techniques usuelles de construction d'hyperrecouvrements (cf. 1.4.13 et 4.2.1) — donc, en particulier, sans nouvelle recherche non bornée — un hyperrecouvrement \check{X}_\bullet de X au-dessus de X_\bullet tel que les $\check{X}_i \rightarrow X_i$ se factorisent par un revêtement n -approché universel de X_i . Que $R\Gamma(X_\bullet^{(n)}, \Lambda) \rightarrow R\Gamma(X, \Lambda)$ se factorise à travers $\check{R}\Gamma(\check{X}_\bullet, \Lambda) \rightarrow R\Gamma(X, \Lambda)$ entraîne que l'on peut obtenir (sans nouvelle recherche non bornée) des cocycles hyper-Čech pour une base des $H^i(X, \Lambda)$.

8.4. Calcul de $R\Gamma(X, \Lambda)$.

8.4.1. Soient X et Λ comme ci-dessus et X_{α_\bullet} un système projectif (indexé par les entiers)⁸ d'hyperrecouvrements de X tel que pour chaque entier i , on ait l'égalité $\text{colim}_\alpha \check{H}^i(X_{\alpha_\bullet}, \Lambda) \xrightarrow{\sim} H^i(X, \Lambda)$, ou encore un quasi-isomorphisme $\text{hocolim}_\alpha \check{R}\Gamma(X_{\alpha_\bullet}, \Lambda) \xrightarrow{\sim} R\Gamma(X, \Lambda)$, où $\check{R}\Gamma(X_{\alpha_\bullet}, \Lambda)$ est le complexe de Čech déduit du Λ -module cosimplicial $\Gamma(X_{\alpha_\bullet}, \Lambda)$. (Rappelons que dans une catégorie abélienne satisfaisant la condition AB5 de Grothendieck, la cohomologie d'une colimite homotopique est la colimite des groupes de cohomologie.) Le complexe $R\Gamma(X, \Lambda)$ appartenant à $D_c^b(\Lambda)$, il résulte du lemme classique [SGA 4 $\frac{1}{2}$ 1977, Rapport, 4.7] qu'il existe un complexe \mathcal{H} de Λ -modules de type fini, concentré en degrés $[0, 2 \dim(X)]$ et, pour α suffisamment grand, un morphisme de (vrais) complexes $\mathcal{H} \rightarrow \check{R}\Gamma(X_{\alpha_\bullet}, \Lambda)$ tel que la flèche composée $\mathcal{H} \rightarrow R\Gamma(X, \Lambda)$ soit un quasi-isomorphisme. Pour calculer un tel \mathcal{H} , il suffit de parcourir les morphismes $\mathcal{H} \rightarrow \check{R}\Gamma(X_{\alpha_\bullet}, \Lambda)$ et de s'arrêter lorsqu'on en a trouvé un induisant le quasi-isomorphisme recherché (en degré $0 \leq i \leq 2 \dim(X)$). C'est possible car on sait calculer les flèches $\check{H}^i(X_{\alpha_\bullet}, \Lambda) \rightarrow H^i(X, \Lambda)$.

8.4.2. La remarque précédente devrait même permettre de calculer $R\Gamma(X, \Lambda)$ sans plus de recherches non bornées que celles faites jusqu'à 8.2.

8. Lorsque k est dénombrable, ce qui suffit pour notre propos, l'existence d'un tel système projectif est élémentaire (voir [Deligne 1980, 5.2.2], cité en 0.2). Pour k quelconque, on peut améliorer le résultat classique selon lequel la catégorie des hyperrecouvrements à homotopie près est cofiltrante (cf. p. ex. [Artin et Mazur 1969, 8.13]) en la « rigidifiant » ([Friedlander 1982, §4]; comparer avec 3.4.2). D'après O. Gabber (communication personnelle) on a des résultats semblables pour des sites généraux, sans hypothèse de finitude (ni, notamment, d'existence de suffisamment de points).

9. Fonctorialité

9.1. Fonctorialité sur $\text{Spec}(k)$.

9.1.1. Soient k un corps algébriquement clos, $f : Y \rightarrow X$ un morphisme de k -schémas algébriques (supposé décrit comme en 16.2), et Λ un ℓ -groupe abélien fini, avec ℓ inversible sur k . D’après 1.4.12, il existe un morphisme simplicial $Y_\bullet \rightarrow X_\bullet$ au-dessus de f , calculable jusqu’à des étages arbitrairement élevés (et dépendant de ℓ mais pas de Λ), donnant lieu à un diagramme commutatif

$$\begin{array}{ccccc}
 \text{R}\Gamma(\text{Tot } X_{\bullet, \ell\text{ét}}, \Lambda) & \xrightarrow{\sim} & \text{R}\Gamma(\text{Tot } X_{\bullet\text{ét}}, \Lambda) & \longrightarrow & \text{R}\Gamma(\text{Tot } Y_{\bullet\text{ét}}, \Lambda) & \xleftarrow{\sim} & \text{R}\Gamma(\text{Tot } Y_{\bullet, \ell\text{ét}}, \Lambda) \\
 & & \uparrow \sim & & \uparrow \sim & & \\
 & & \text{R}\Gamma(X, \Lambda) & \longrightarrow & \text{R}\Gamma(Y, \Lambda) & &
 \end{array}$$

D’après ce qui précède (§8), il existe deux entiers explicites $\mu \leq \nu$ tels que pour chaque $d \leq 2 \max\{\dim(X), \dim(Y)\} < r$, on ait

$$\text{H}^d(Z, \Lambda) = \text{Im}(\text{H}^d(\text{Tot } Z_{\bullet, \leq r}^{(\mu)}, \Lambda) \rightarrow \text{H}^d(\text{Tot } Z_{\bullet, \leq r}^{(\nu)}, \Lambda))$$

pour $Z = X$ ou Y . Le morphisme $\text{H}^d(\text{Tot } X_{\bullet, \leq r}^{(\nu)}, \Lambda) \rightarrow \text{H}^d(\text{Tot } Y_{\bullet, \leq r}^{(\nu)}, \Lambda)$ étant calculable (cf. 4.2.6), on peut trouver une présentation explicite du morphisme $\text{H}^d(f, \Lambda) : \text{H}^d(X, \Lambda) \rightarrow \text{H}^d(Y, \Lambda)$ (au sens de 13.3). Si Λ est le corps $\mathbb{Z}/\ell\mathbb{Z}$, cela revient bien entendu à calculer le rang de $\text{H}^d(f, \mathbb{Z}/\ell\mathbb{Z})$.

Notons que l’on pourrait bien entendu utiliser la présentation tirée de 8.3, pour obtenir le même résultat (voir aussi 9.2).

9.1.2. Amélioration. Vérifions maintenant que pour toute collection finie f_1, \dots, f_r de k -morphisms explicites $Y \rightarrow X$, on peut calculer des présentations explicites des $\text{H}^d(f_i, \Lambda)$ relativement à de *mêmes* présentations explicites de $\text{H}^d(X, \Lambda)$ et $\text{H}^d(Y, \Lambda)$. Il résulte en effet de 1.4.12 et 1.4.13 qu’il existe pour chaque $\alpha \in \{1, \dots, r\}$ un morphisme $Y_{\alpha\bullet} \rightarrow X_\bullet$ comme en *loc. cit.* au-dessus de f_α . En considérant le produit fibré des $Y_{\alpha\bullet}$ au-dessus de Y et en réappliquant la construction de *loc. cit.*, on en déduit qu’il existe un diagramme commutatif

$$\begin{array}{ccc}
 Y_\bullet & \begin{array}{c} \xrightarrow{f_{1\bullet}} \\ \vdots \\ \xrightarrow{f_{r\bullet}} \end{array} & X_\bullet \\
 \downarrow & & \downarrow \\
 Y & \begin{array}{c} \xrightarrow{f_1} \\ \vdots \\ \xrightarrow{f_r} \end{array} & X
 \end{array}$$

où les flèches verticales *ne dépendent pas de l’indice* $\alpha \in \{1, \dots, r\}$. La conclusion en résulte aussitôt.

(En particulier, donnés deux morphismes $f, g : Y \rightarrow X$, on peut décider si $H^d(g, \Lambda) = H^d(f, \Lambda)$.)

Notons que si $Y = X$, on peut supposer que les Λ -modules explicites $H^d(X, \Lambda)$ et $H^d(Y, \Lambda)$ sont *égaux*. Pour s'en convaincre, il suffit par exemple de rajouter l'identité $Y \rightarrow X$ aux morphismes f_1, \dots, f_r et de composer avec l'inverse de l'isomorphisme $H^d(X, \Lambda) \rightarrow H^d(Y, \Lambda)$ qui s'en déduit.

On peut reformuler la functorialité établie sous la forme suivante.

9.1.3. Soit \mathcal{G} un graphe fini orienté avec arêtes multiples possibles. Supposons donné un étiquetage de \mathcal{G} par la catégorie des k -schémas algébriques, c'est-à-dire un étiquetage de ses sommets par des k -schémas algébriques et un étiquetage des arêtes par des k -morphisms (entre les schémas correspondants). On peut calculer un étiquetage du graphe opposé \mathcal{G}^{op} par la catégorie des Λ -modules finis, déduit du précédent par application du foncteur $H^d(-, \Lambda)$.

On peut déduire cet énoncé du précédent en considérant le coproduit

$$X = \text{Spec}(k) \amalg \coprod_s X_s,$$

où X_s parcourt les étiquettes des sommets s de \mathcal{G} , et les endomorphismes $X \rightarrow X$ envoyant chaque $X_{s'}$, sauf un X_s , sur $\text{Spec}(k)$ et déterminé par l'étiquette d'une arête sur ce dernier X_s .

9.2. Action galoisienne.

9.2.1. Soient ${}_0k$ un corps (calculable et disposant d'un algorithme de factorisation et d'une p -base finie explicite : cf. 12.7) et ${}_0X$ un ${}_0k$ -schéma algébrique explicite. Fixons une clôture algébrique k de ${}_0k$ et notons X le k -schéma obtenu par extension des scalaires. Nous allons montrer que l'on peut calculer une extension finie galoisienne ${}_1k/{}_0k$ telle que l'action du groupe de Galois de ${}_0k$ sur $H^*(X, \Lambda)$ se factorise à travers $\Gamma = \text{Gal}({}_1k/{}_0k)$ et calculer la représentation du groupe fini correspondante. Toute extension étale de la clôture parfaite de ${}_0k$ dans k se descendant explicitement à ${}_0k$, on peut supposer le corps ${}_0k$ parfait (12.5(v)).

9.2.2. Fixons d . Comme on l'a vu en 8.3, il existe un hyperrecouvrement tronqué pour la topologie des altérations $X_{\bullet \leq r} \rightarrow X$ tel que $\check{H}^d(X_{\bullet \leq r}, \Lambda) \rightarrow H^d(X, \Lambda)$ soit *surjective*; par cofinalité (observée en 1.4.11), il existe un tel hyperrecouvrement *défini sur* ${}_0k$. La calculabilité de l'action du groupe de Galois sur $H^d(X, \Lambda)$ se déduit donc de celle de l'action sur $\check{H}^d(X_{\bullet \leq r}, \Lambda)$ et de la calculabilité de la flèche. Plus précisément, si $c \in H^d(X, \Lambda)$ est l'image d'une d -chaîne $z \in H^0(X_d, \Lambda)$, la classe de cohomologie $\gamma \cdot c$, où $\gamma \in \text{Gal}(k/{}_0k)$, est l'image de la d -chaîne $\gamma \cdot z$ déduite de l'action du groupe de Galois sur $\pi_0(X_d) = \pi_0({}_0X_d \otimes_{{}_0k} k)$.

Notons que l'hyperrecouvrement tronqué $X_{\bullet \leq r} \rightarrow X$ est défini sur une sous-extension galoisienne finie ${}_1k/{}_0k$, et l'action précédente se factorise à travers le quotient fini $\Gamma = \text{Gal}({}_1k/{}_0k)$. Ce dernier est calculable car ${}_0k$ est un corps calculable avec un algorithme de factorisation [Fried et Jarden 2008, 19.3.2].

10. Structure de l'algorithme et exemple simple

10.1. Structure générale. Récapitulons brièvement comment les différents éléments qui ont été présentés s'emboîtent pour fournir, en principe, un algorithme permettant de calculer $H^d(X, \Lambda)$ pour X un schéma algébrique sur un corps algébriquement clos de caractéristique différente de ℓ et Λ un ℓ -groupe abélien fini.

Dans un premier temps, on calcule, jusqu'à un certain niveau r , un hyperrecouvrement X_\bullet de X tel qu'explicité en 1.4.12. Plus exactement, on calcule $X_0 \rightarrow X$ qui recouvre X et dont les composantes sont des polycourbes ℓ -élémentaires (et en particulier, des $K(\pi, 1)$ pro- ℓ) : ceci se fait au moyen de la proposition 1.4.9 (compte tenu des remarques qui suivent au sujet de la constructivité) ; puis de même $X_1 \rightarrow X_0 \times_X X_0$ et ainsi de suite comme expliqué en 1.4.13. Cette construction des X_i doit être menée pour $i \leq r$ avec r qui dépend uniquement du degré en lequel on veut calculer la cohomologie (comme expliqué en 4.1.2, en fait $r = d + 1$ suffit).

D'après les résultats de la section 3, et s'appuyant sur la calculabilité du nombre de $\mathbb{Z}/\ell\mathbb{Z}$ -torseurs établie en 2.1, on sait calculer, pour chaque niveau d'approximation fini $\lambda \geq 1$, et pour tout k -schéma algébrique normal Y , un revêtement ℓ -étale λ -approché universel $Y^{[\lambda]}$, ainsi que le groupe de Galois correspondant $\pi_Y^{[\lambda]}$ si Y est connexe.

D'après §4, on sait calculer, pour chaque niveau d'approximation fini $\lambda \geq 1$, le groupe $H^d(\text{Tot } X_\bullet^{(\lambda)}, \Lambda)$ (isomorphe à $H^d(\text{Tot } X_{\bullet \leq r}^{(\lambda)}, \Lambda)$ puisque r a été choisi assez grand), et même la flèche $H^d(\text{Tot } X_\bullet^{(\mu)}, \Lambda) \rightarrow H^d(\text{Tot } X_\bullet^{(\nu)}, \Lambda)$ pour deux entiers $\mu \leq \nu$.

Il s'agit donc de calculer de tels entiers pour que l'image de cette flèche soit le groupe $H^d(X, \Lambda)$ recherché. Comme expliqué en §8, ceci résulte de 5.8 appliqué à la suite spectrale $E_{1,\lambda}^{i,j} = H^j(X_i^{(\lambda)}, \Lambda) \Rightarrow H^{i+j}(\text{Tot } X_\bullet^{(\lambda)}, \Lambda)$, une fois connus des fonctions explicitant, pour chaque i et j , le fait que $H^j(X_i^{(\lambda)}, \Lambda)$ est essentiellement constant. De telles bornes sont obtenues en §7.

10.2. Esquisse d'exemple. Pour illustrer la manière dont l'algorithme s'exécuterait, nous esquissons le calcul de $H^i(\mathbb{P}_k^1, \mathbb{Z}/\ell\mathbb{Z})$ pour les petits i en en suivant les différentes étapes. (Le cas encore plus simple d'une courbe affine lisse X consiste essentiellement à calculer $X^{[\lambda]}$ par 3.3 pour des petites valeurs de λ et à appliquer la proposition 6.5 : de toute façon, on est ramené à §2.)

Notons $U = \mathbb{P}_k^1 \setminus \{\infty\}$ et $U' = \mathbb{P}_k^1 \setminus \{0\}$ deux ouverts de Zariski qui recouvrent \mathbb{P}_k^1 et

dont on note $V := U \times_{\mathbb{P}_k^1} U'$ l'intersection. Soit $X_0 := U \amalg U' \rightarrow \mathbb{P}_k^1$, vu comme un \mathbb{P}_k^1 -schéma simplicial 0-tronqué ; son cosquelette est donné par $X_p = X_0 \times_{\mathbb{P}_k^1} \cdots \times_{\mathbb{P}_k^1} X_0$ (avec $p + 1$ facteurs), qui est le coproduit $U \amalg V \amalg \cdots \amalg V \amalg U'$ de U , U' et $2^{p+1} - 2$ copies de V qu'on imaginera étiquetés par les 2^{p+1} mots binaires w de longueur $p + 1$, et pour $0 \leq i \leq p + 1$, le morphisme $X_{\delta_{p,i}} : X_{p+1} \rightarrow X_p$ envoie par le morphisme évident la composante $X_{p+1,w}$ étiquetée w sur celle $X_{p,w'}$ étiquetée par le mot w' égal à w privé de son i -ième bit. Il s'agit manifestement d'un hyperrecouvrement. Comme U, U', V sont des (poly)courbes ℓ -élémentaires sur $\text{Spec } k$, il est possible que la recherche de courbes élémentaires effectuée par l'algorithme retourne cet hyperrecouvrement.

Examinons maintenant comment se déroulerait le calcul de la cohomologie de $\text{Tot } X_{\bullet}^{(\lambda+1)}$ (en fonction d'un entier $\lambda + 1 \geq 1$) à valeurs dans le faisceau constant $\mathbb{Z}/\ell\mathbb{Z}$. Comme $V = \mathbb{G}_m$, le topos $V^{(\lambda+1)}$ est le topos des $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ -ensembles, tandis que $U^{(\lambda+1)}$ et $U'^{(\lambda+1)}$ sont, bien sûr, celui des ensembles. (Et pour un λ donné, l'algorithme est capable d'effectuer ce calcul en suivant 3.3.) Un faisceau abélien de $\text{Tot } X_{\bullet}^{(\lambda+1)}$ est donc (cf. 4.1.1) la donnée pour chaque mot binaire w de longueur $p + 1$ (pour $p \geq 0$) d'un groupe abélien $A_{p,w}$, muni d'une action de $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ sauf si w est l'un des mots $00 \cdots 0$ ou $11 \cdots 1$, ainsi que de morphismes $A_{p,w} \rightarrow A_{p+1,w'}$ pour chaque mot w' obtenu en insérant un bit dans w , vérifiant les compatibilités évidentes. Si comme topos discret utilisé en §4 on prend $P_{\bullet} = X_{\bullet}^{(1)}$, alors un faisceau abélien de $\text{Tot } P_{\bullet}$ correspond à de telles données sans l'action de $\mathbb{Z}/\ell^\lambda\mathbb{Z}$: à un tel objet est associé un complexe de différentielle

$$\bigoplus_{w \in \{0,1\}^{p+1}} A_{p,w} \rightarrow \bigoplus_{w \in \{0,1\}^{p+2}} A_{p+1,w} \tag{†}$$

somme alternée des morphismes $A_{p,w} \rightarrow A_{p+1,w'}$.

Les foncteurs u^* associant à un $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ -ensemble son ensemble sous-jacent, et u_* son adjoint à droite $X \mapsto \text{Hom}_{\text{Ens}}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, X)$, définissent pour tout $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ -module une résolution de Godement, analogue (et quasi-isomorphe) à l'une des résolutions habituelles définissant la cohomologie des groupes (par exemple [Serre 1994, I, §2.2] ou [Neukirch, Schmidt et Wingberg 2000, I, §2]). Ces foncteurs forment un morphisme $\text{Tot } P_{\bullet} \rightarrow \text{Tot } X_{\bullet}^{(\lambda+1)}$. À partir du faisceau constant $A_{p,w} = \mathbb{Z}/\ell\mathbb{Z}$, l'algorithme (4.2) va donc calculer, en bas degrés, le complexe double dont les colonnes sont sommes de copies de la résolution qu'on vient de dire (et pour $w = 00 \cdots 0, 11 \cdots 1$, de la résolution triviale), et dont les différentielles horizontales sont données par (†). Le calcul du $H^i(\text{Tot } X_{\bullet}^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z})$ est alors donné par la cohomologie du complexe simple associé à ce complexe double.

On peut prédire quel sera le résultat de ce calcul en utilisant la suite spectrale de descente décrite en 8.2 (et qui est la « première » suite spectrale associée au complexe double décrit ci-dessus) : il est facile de se convaincre que cette suite

spectrale dégénère en E_2 , les seuls termes non nuls étant $E_2^{0,0} = \mathbb{Z}/\ell\mathbb{Z}$ et $E_2^{1,q} = H^q(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$ si $q \geq 2$. Ainsi, $H^n(\text{Tot } X_\bullet^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z})$ vaut $\mathbb{Z}/\ell\mathbb{Z}$ si $n=0$, 0 si $n=1$, et $H^{n-1}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$ si $n \geq 2$ (c'est-à-dire $\mathbb{Z}/\ell\mathbb{Z}$ dès que $\lambda \geq 1$). Pour $\lambda \leq \mu$, les flèches $H^n(\text{Tot } X_\bullet^{(\lambda+1)}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^n(\text{Tot } X_\bullet^{(\mu+1)}, \mathbb{Z}/\ell\mathbb{Z})$ correspondent bien aux morphismes fonctoriels (d'inflation) $H^{n-1}(\mathbb{Z}/\ell^\lambda\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^{n-1}(\mathbb{Z}/\ell^\mu\mathbb{Z}, \mathbb{Z}/\ell\mathbb{Z})$, et grâce à 6.5–6.7 on sait que cette flèche sera un isomorphisme pour $n \leq 2$ et nulle pour $n \geq 3$ dès que $1 \leq \lambda < \mu$. Muni de cette borne, l'algorithme calcule $H^n(\mathbb{P}_k^1, \mathbb{Z}/\ell\mathbb{Z})$ comme l'image de $H^n(\text{Tot } X_\bullet^{(2)}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^n(\text{Tot } X_\bullet^{(3)}, \mathbb{Z}/\ell\mathbb{Z})$, ce qui donne bien le résultat attendu.

Soulignons sur cet exemple le fait suivant : si on remplace les coefficients $\mathbb{Z}/\ell\mathbb{Z}$ par le groupe μ_ℓ des racines ℓ -ièmes de l'unité (qui lui est non canoniquement isomorphe) et le groupe $\mathbb{Z}/\ell^\lambda\mathbb{Z}$ par le groupe μ_{ℓ^λ} (de nouveau non canoniquement isomorphe) des automorphismes du revêtement étale $\mathbb{G}_m \rightarrow \mathbb{G}_m$ donné par $z \mapsto z^{\ell^\lambda}$, on se convainc aisément que le calcul ne dépend plus d'aucun choix arbitraire (même si la description ci-dessus en utilise), et on voit donc $H^2(\mathbb{P}_k^1, \mu_\ell)$ comme $H^1(\mu_{\ell^\lambda}, \mu_\ell)$ (l'action de μ_{ℓ^λ} étant triviale), lui-même isomorphe à $\text{Hom}(\mu_{\ell^\lambda}, \mu_\ell) = \mathbb{Z}/\ell\mathbb{Z}$ sans faire de choix arbitraire.

11. Compléments

On considère ici quelques résultats qui sont des prolongements naturels de notre théorème principal et on énonce en 11.5 quelques questions, dont certaines sont probablement hors de portée. Cette section se termine (11.6) par quelques précisions métamathématiques sur la nature des algorithmes que l'on espère pouvoir obtenir.

Ci-dessous k est un corps algébriquement clos et Λ un anneau commutatif fini de cardinal inversible sur k .

11.1. Cohomologie d'un schéma simplicial. Soit X_\bullet un k -schéma algébrique simplicial. D'après [Deligne 1974, §6.4] et les résultats de §1.4, il existe un hyperrecouvrement $X_{\bullet\bullet} \rightarrow X_\bullet$ par des polycourbes ℓ -élémentaires tel que $H^*(X_{\bullet\bullet}, \Lambda) = H^*(X_\bullet, \Lambda)$. On peut donc procéder comme dans le cas non simplicial pour calculer le terme de gauche en tout degré donné à l'avance. Noter qu'il n'est pas absolument nécessaire d'utiliser une variante bisimpliciale de arguments précédents : d'après le théorème de Cartier–Eilenberg–Zilber ([Deligne 1974, 6.4.2.2] ou [Illusie 1971, I, §1.2]), on a $R\Gamma(X_{\bullet\bullet}, \Lambda) = R\Gamma(\delta X_{\bullet\bullet}, \Lambda)$, où $\delta X_{\bullet\bullet}$ est le schéma simplicial *diagonal* déduit de $X_{\bullet\bullet}$. Le même argument est valable si l'on veut calculer la cohomologie de X_\bullet à valeurs dans un faisceau à composantes localement constantes (étage par étage).

Tout espace algébrique (au sens d'Artin) étant localement pour la topologie étale un schéma, on peut probablement utiliser le résultat précédent pour en calculer la cohomologie étale.

11.2. Cohomologie relative. On présente ici deux constructions de la cohomologie relative d'un morphisme $Y \rightarrow X$: la première (simpliciale) est valable en toute généralité, la seconde (11.2.5) s'applique uniquement à la cohomologie relativement à un sous-schéma fermé.

Rappelons que la cohomologie relative s'inscrit dans un triangle distingué

$$\mathrm{R}\Gamma(X/Y, \Lambda) \rightarrow \mathrm{R}\Gamma(X, \Lambda) \rightarrow \mathrm{R}\Gamma(Y, \Lambda) \xrightarrow{+1} .$$

Lorsque Λ est un corps, la calculabilité de la dimension du groupe de cohomologie relative $H^i(X/Y, \Lambda)$ résulte donc immédiatement du **théorème 0.1** : c'est une extension de $\mathrm{Ker}(H^i(X, \Lambda) \rightarrow H^i(Y, \Lambda))$ par $\mathrm{Im}(H^{i-1}(X, \Lambda) \rightarrow H^{i-1}(Y, \Lambda))$.

11.2.1. Cône d'un morphisme simplicial. Soit $f_* : Y_* \rightarrow X_*$ un morphisme de topos simpliciaux (dont on notera $\mathrm{Tot} f_* : \mathrm{Tot} Y_* \rightarrow \mathrm{Tot} X_*$ le morphisme entre les topos totaux, cf. 4.1.1); on pourra penser au cas d'un morphisme déduit, par passage aux topos étales, d'un morphisme de k -schémas algébriques simpliciaux. Notons Cf_* son cône : $Cf_n = X_n \amalg Y_{<n}$, où $Y_{<n} = \coprod_{-1 \leq i < n} Y_i$ et, conformément à l'usage, Y_{-1} est le topos final e . Explicitons le morphisme de functorialité $Cf_\phi : Cf_m \rightarrow Cf_n$ déduit d'une application croissante $\phi : [n] = \{0, \dots, n\} \rightarrow [m] = \{0, \dots, m\}$. Sur le facteur X_m , c'est le morphisme composé $X_m \rightarrow X_n \hookrightarrow Cf_n$, la première flèche étant X_ϕ . Soit maintenant $-1 \leq \mu < m$ et considérons l'application $\phi_\mu : [\nu] \rightarrow [\mu]$ déduite de ϕ par changement de base $[\mu] \hookrightarrow [m]$. Sur le facteur Y_μ , le morphisme Cf_ϕ est le morphisme composé $Y_\mu \rightarrow Y_\nu \hookrightarrow Cf_n$, la première flèche étant Y_{ϕ_μ} si $\nu < n$, et $Y_\mu \rightarrow Y_\nu \rightarrow X_\nu \hookrightarrow Cf_n$, où $Y_\nu \rightarrow X_\nu$ est f_ν , si $\nu = n$. Par exemple, le morphisme face $d_i : Cf_{n+1} \rightarrow Cf_n$, déduit de l'unique injection croissante $[n] \rightarrow [n+1]$ d'image ne contenant pas i , est induit par les identités $Y_j \rightarrow Y_j$ pour $j < i$ (composée avec $Y_n \rightarrow X_n$ si $j = n$) et les faces $d_i : Y_l \rightarrow Y_{l-1}$ pour $i \leq l \leq n$ et $d_i : X_{n+1} \rightarrow X_n$.

Soit $\phi_* : \mathcal{F}_* \rightarrow \mathcal{G}_*$ un f_* -morphisme entre faisceaux abéliens \mathcal{F}_* sur $\mathrm{Tot} X_*$ et \mathcal{G}_* sur $\mathrm{Tot} Y_*$, c'est-à-dire un morphisme $f_*^* \mathcal{F}_* \rightarrow \mathcal{G}_*$, objet du topos flèche $\mathrm{Fl}(\mathrm{Tot} f_*)$. Les coproduits et les flèches du paragraphe précédent, calculés dans la catégorie des paires (X, \mathcal{F}) — cf. [Deligne 1974, 6.3.1.b], en remplaçant « espace topologique » par « topos »⁹ —, permettent de définir un faisceau abélien simplicial sur $\mathrm{Tot} Cf_*$, cône de ϕ_* , que nous notons $C\phi_*$. (Notons que l'objet final de cette catégorie de paires est le faisceau nul sur e .)

11.2.2. La cohomologie relative de $\mathrm{Tot} X_*$ modulo $\mathrm{Tot} Y_*$ est un cas particulier de celle définie, pour tout morphisme $S \rightarrow T$ de topos, en [Illusie 1971, III, §4] (voir aussi [Deligne 1980, §4.3.4]). On la note $\mathrm{R}\Gamma(\mathrm{Tot} X_*/\mathrm{Tot} Y_*, \phi_*)$; ce n'est en général pas la cohomologie de $\mathrm{Fl}(\mathrm{Tot} f_*)$ à valeurs dans ϕ_* . (Cette dernière étant isomorphe à $\mathrm{R}\Gamma(\mathrm{Tot} X_*, \mathcal{F}_*)$ d'après [Illusie 1971, III.4.2].) Implicite en [Deligne

9. Voir aussi [SGA 4₂ 1972, V^{bis}.4.3.0].

1974, §6.3] est la formule suivante :

$$\mathbf{R}\Gamma(\mathrm{Tot} X_{\bullet} / \mathrm{Tot} Y_{\bullet}, \phi_{\bullet}) = \mathbf{R}\Gamma(\mathrm{Tot} C f_{\bullet}, C \phi_{\bullet}). \quad (\star)$$

En degré cohomologique nul, cette formule résulte immédiatement de la description explicite de d_0 et d_1 , et du fait que le terme de gauche est $\mathrm{Ker}(\mathrm{H}^0(\mathrm{Tot} X_{\bullet}, \mathcal{F}_{\bullet}) \rightarrow \mathrm{H}^0(\mathrm{Tot} Y_{\bullet}, \mathcal{G}_{\bullet}))$. (On pourra aussi comparer à [Anderson 1987, §1], où le cas des ensembles simpliciaux et des coefficients constants est considéré.)

11.2.3. Justifions brièvement (\star) . Notons \mathcal{R} le topos $\mathrm{Fl}(\mathrm{Tot} f_{\bullet})$ et \mathcal{C} le topos $\mathrm{Tot} C f_{\bullet}$. Il n’y a pas de morphisme naturel $\mathcal{C} \rightarrow \mathcal{R}$ — comme on le voit par exemple en considérant l’unique endomorphisme du topos simplicial vide — mais un morphisme $a : \mathcal{C}^{\times} \rightarrow \mathcal{R}$, où \mathcal{C}^{\times} est le *sous-topos ouvert* de \mathcal{C} , défini par la condition : $i^{\star} = \emptyset$, où $i : \mathrm{Fl}(e_{\bullet}) \rightarrow \mathcal{C}$ est le morphisme évident. Le morphisme image inverse a^{\star} est la variante ensembliste du cône d’un morphisme de faisceau abélien considérée en 11.2.1 : sur chaque $Y_{-1} = e$, on considère le faisceau initial (= vide). Notant $j : \mathcal{C}^{\times} \hookrightarrow \mathcal{C}$, on vérifie sans peine l’égalité $C \phi_{\bullet} = j_! a^{\star} \phi_{\bullet}$ pour tout faisceau abélien sur \mathcal{R} . La formule (\star) résulte alors, par dérivation et exactitude de $j_! a^{\star}$, de la formule en degré cohomologique nul.

11.2.4. Soient $f : Y \rightarrow X$ un morphisme de k -schémas algébriques et $f_{\bullet} : Y_{\bullet} \rightarrow X_{\bullet}$ le morphisme induit entre les schémas simpliciaux constants. Il résulte de ce qui précède et de 11.1 que l’on peut calculer le groupe de cohomologie étale $\mathrm{H}^i(X/Y, \Lambda) : c$ ’est $\mathrm{H}^i(C f_{\bullet}, C \Lambda_{\bullet})$. Ceci s’applique en particulier au calcul de la cohomologie à support compact : si X est *propre* sur k , la cohomologie de X/F — où F est un fermé de X — est la cohomologie à support compact de $U = X - F$:

$$\mathrm{H}_c^i(U, \Lambda) = \mathrm{H}^i(X/F, \Lambda).$$

11.2.5. Esquissons une autre approche du calcul de la cohomologie de X relative à un fermé F . Notons $Z = X \amalg_F X$ la somme amalgamée (pincement) de deux copies de X le long de F ; si $X = \mathrm{Spec}(A)$ et $F = \mathrm{Spec}(A/I)$, le schéma Z est le spectre du sous-anneau $B = \{(a_1, a_2) \in A^2 : a_1 \equiv a_2 \pmod{I}\}$ de A^2 . Voir [Ferrand 2003, §5 et §7, notamment le théorème 7.1] pour une discussion de l’existence de coproduits sous des hypothèses bien plus générales et 16.4 pour une approche effective.

Notons i_1 et i_2 les deux immersions fermées canoniques de X dans Z , et i l’immersion fermée de F dans Z . Considérons les morphismes d’adjonctions $\rho_{\alpha} : i_{\alpha\star} \Lambda \rightarrow i_{\star} \Lambda$ (pour $\alpha \in \{1, 2\}$) et δ le morphisme « différence » $(i_{\star} \Lambda)^2 \rightarrow i_{\star} \Lambda$, $(a_1, a_2) \mapsto a_1 - a_2$. Le complexe concentré en degrés $[0, 1]$

$$[i_{1\star} \Lambda \oplus i_{2\star} \Lambda \xrightarrow{\delta \circ (\rho_1, \rho_2)} i_{\star} \Lambda]$$

calcule la cohomologie $\mathbf{R}\Gamma(Z, \Lambda)$ de Z (« Mayer–Vietoris »). Or, il est *isomorphe*

au complexe

$$[i_{1\star}\Lambda \oplus i_{2\star}\Lambda \xrightarrow{0 \oplus \rho_2} i_{\star}\Lambda]$$

dont la cohomologie est la somme directe $R\Gamma(X, \Lambda) \oplus R\Gamma(X/F, \Lambda)$. La cohomologie de X/F se déduit donc fonctoriellement de la cohomologie (usuelle) de X et de celle de $Z = X \amalg_F X$.

(Notons que la rétraction $Z = X \amalg_F X \rightarrow X = X \amalg_X X$ des deux inclusions $X \rightrightarrows Z$ induit la décomposition en somme directe ci-dessus.)

11.3. Structure d'algèbre graduée.

11.3.1. Soient X et Y deux k -schémas de type fini, Λ comme au début de la section 11 et i, j deux entiers. Comme expliqué en 8.3, on peut notamment construire deux hyperrecouvrements (étales) $X_{\bullet} \rightarrow X$ et $Y_{\bullet} \rightarrow Y$ tels que les flèches $\check{H}^i(X_{\bullet}, \Lambda) \rightarrow H^i(X, \Lambda)$ et $\check{H}^j(Y_{\bullet}, \Lambda) \rightarrow H^j(Y, \Lambda)$ soient *surjectives*. Utilisant la formule de Künneth triviale $\pi_0(X_{\bullet} \times_k Y_{\bullet}) = \pi_0(X_{\bullet}) \times \pi_0(Y_{\bullet})$ et l'existence d'un homotopisme d'Eilenberg–Zilber *explicite* [Mac Lane 1963, VIII, théorèmes 8.1 et 8.8]

$$\text{Hom}(\pi_0(X_{\bullet}), \Lambda) \otimes \text{Hom}(\pi_0(Y_{\bullet}), \Lambda) \rightarrow \text{Hom}(\pi_0(X_{\bullet} \times_k Y_{\bullet}), \Lambda),$$

on en déduit un morphisme

$$\check{H}^i(X_{\bullet}, \Lambda) \otimes \check{H}^j(Y_{\bullet}, \Lambda) \rightarrow \check{H}^{i+j}(X_{\bullet} \times_k Y_{\bullet}, \Lambda)$$

relevant le morphisme de Künneth $H^i(X, \Lambda) \otimes H^j(Y, \Lambda) \rightarrow H^{i+j}(X \times_k Y, \Lambda)$ ([Milne 1980, V.1.19]; comparer avec [Deligne 1974, 8.1.25]). Ce dernier est donc calculable compte tenu de ce qui précède. (On utilise le fait que la flèche naturelle $\check{H}^{i+j}(X_{\bullet} \times_k Y_{\bullet}, \Lambda) \rightarrow H^{i+j}(X \times_k Y, \Lambda)$ l'est.)

11.3.2. Lorsque $X = Y$, on en déduit la structure de Λ -algèbre graduée commutative sur $H^*(X, \Lambda)$ par composition avec la flèche de functorialité $H^*(X \times_k X, \Lambda) \rightarrow H^*(X, \Lambda)$ induite par la diagonale $X \rightarrow X \times_k X$: on peut donc calculer le produit

$$H^*(X, \Lambda) \otimes H^*(X, \Lambda) \rightarrow H^*(X, \Lambda), \quad c_1 \otimes c_2 \mapsto c_1 \smile c_2.$$

11.3.3. Le résultat précédent a une application immédiate aux cycles algébriques. Supposons dorénavant X propre, lisse, connexe de dimension d_X , et fixons un isomorphisme $t_X : H^{2d_X}(X, \Lambda) \xrightarrow{\sim} \Lambda$. Par la dualité de Poincaré, toute forme linéaire $\phi : H^i(X, \Lambda) \rightarrow \Lambda$ est de la forme $b \mapsto t_X(a_{\phi} \smile b)$ pour une unique classe $a_{\phi} \in H^{2d_X-i}(X, \Lambda)$, que l'on peut calculer. En particulier, tout morphisme $Z \rightarrow X$ de source une variété propre lisse connexe de dimension d_Z induit une classe $c_Z \in H^{2(d_X-d_Z)}(X, \Lambda)$, correspondant à la forme linéaire composée $H^{2d_Z}(X, \Lambda) \rightarrow H^{2d_Z}(Z, \Lambda) \xrightarrow{\sim} \Lambda$, où le dernier morphisme est un morphisme trace pour Z .

La classe de cycle c_Z est ainsi définie à multiplication par un élément de Λ^\times près (lié au choix arbitraire de traces pour X et Z), ambiguïté que l'on devrait pouvoir lever. Ceci nous permet cependant de répondre à la question : la classe d'un cycle algébrique lisse de X est-elle triviale ?

11.4. Images directes. On montre que pour tout morphisme $f : X \rightarrow S$ entre k -schémas algébriques, tout faisceau constructible \mathcal{F} de Λ -modules sur X et tout entier i , on peut calculer le faisceau $R^i f_* \mathcal{F}$, fonctoriellement en \mathcal{F} .

11.4.1. Il conviendrait de donner une description explicite de la catégorie des faisceaux constructibles sur un schéma (explicite) X et de vérifier que quelques opérations usuelles (noyau, conoyau, etc.) sont bien calculables. Signalons simplement que différentes approches sont possibles : stratifications et flèches de recollement (cf. [SGA 4₁ 1972, IV.9.3]), description des générateurs ou cogénérateurs usuels [SGA 4₃ 1973, IX 2.9(ii) et 2.14(ii)], espaces algébriques ([Artin 1973, chapitre VII], ou [Milne 1980, chapitre V, §1]). Cette dernière est probablement la plus économique.

11.4.2. Effaçabilité et dévissages. Soient S un schéma noëthérien et $f : X \rightarrow S$ un morphisme de type fini. D'après une variante de [SGA 4₂¹ 1977, Arcata, IV.3.5], les foncteurs $R^i f_*$ pour $i > 0$ sont *effaçables* dans la catégorie des faisceaux constructibles sur X : pour chaque faisceau (abélien) constructible \mathcal{F} sur X , il existe un plongement de \mathcal{F} dans un faisceau *constructible* $\tilde{\mathcal{F}}$ tel que le morphisme $R^i f_* \mathcal{F} \rightarrow R^i f_* \tilde{\mathcal{F}}$ soit nul. De plus, il est formel de vérifier que tout morphisme $\mathcal{F}_1 \rightarrow \mathcal{F}_2$ de faisceaux constructibles s'insère dans un diagramme

$$\begin{array}{ccc} \mathcal{F}_1 & \longrightarrow & \mathcal{F}_2 \\ \downarrow & & \downarrow \\ \tilde{\mathcal{F}}_1 & \longrightarrow & \tilde{\mathcal{F}}_2 \end{array}$$

où $\tilde{\mathcal{F}}_1$ et $\tilde{\mathcal{F}}_2$ effacent respectivement $R^i f_* \mathcal{F}_1$ et $R^i f_* \mathcal{F}_2$.

Fixons un entier $n > 1$ et supposons que l'on sache calculer, fonctoriellement en \mathcal{F} , les $R^i f_* \mathcal{F}$ pour chaque entier $i < n$, et chaque faisceau constructible \mathcal{F} de Λ -modules sur X . Considérons un faisceau constructible \mathcal{F} sur X et $\mathcal{F} \hookrightarrow \tilde{\mathcal{F}}$ un monomorphisme effaçant $R^n f_* \mathcal{F}$. Notant \mathcal{G} le faisceau quotient $\tilde{\mathcal{F}}/\mathcal{F}$, on a la suite exacte $R^{n-1} f_* \tilde{\mathcal{F}} \rightarrow R^{n-1} f_* \mathcal{G} \rightarrow R^n f_* \mathcal{F} \rightarrow 0$. La calculabilité (fonctorielle) de $R^n f_* \mathcal{F}$ se ramène donc à la détermination explicite d'un monomorphisme $\mathcal{F} \hookrightarrow \tilde{\mathcal{F}}$ comme ci-dessus. La possibilité de plonger tout Λ -faisceau constructible dans l'image directe par un morphisme fini d'un faisceau constant sur chaque composante connexe nous ramène au problème suivant : trouver un morphisme fini surjectif $\pi : X' \rightarrow X$ tel que la flèche de functorialité $R^n f_* \Lambda \rightarrow R^n f'_* \Lambda$ (déduite de l'unité de l'adjonction $\pi^* \dashv \pi_*$) soit nulle, où $f' = f \circ \pi'$.

11.4.3. Cas d'un morphisme propre. (Par la suite, S est de type fini sur k algébriquement clos.) Quitte à énumérer les morphismes π (pour faire une recherche non bornée : cf. 12.8), on se ramène au problème de *tester* la nullité d'une flèche comme ci-dessus. Or, on peut calculer une stratification explicite $S = \bigcup_i S_i$ (réunion disjointe) telle que les faisceaux $R^n f_\star \Lambda$ et $R^n f'_\star \Lambda$ ci-dessus soient lisses sur les S_i ; c'est un corollaire immédiat des démonstrations « géométriques » de la constructibilité des images directes. (Voir [Orgogozo 2013] pour des variantes sur ce thème.) Tester si $R^n f_\star \Lambda \rightarrow R^n f'_\star \Lambda$ est nulle revient donc à tester si sa fibre l'est en tout point géométrique $\bar{\eta}$ localisé en un point maximal η des S_i . Lorsque f est *propre* (ou simplement cohomologiquement propre pour les faisceaux de torsion), cette fibre n'est autre que la flèche de functorialité

$$H^n(X_{\bar{\eta}}, \Lambda) \rightarrow H^n(X'_{\bar{\eta}}, \Lambda).$$

D'après le [théorème 0.1](#), on peut décider si une telle flèche est nulle ou non ; la conclusion résulte alors du fait que les points maximaux η sont en nombre fini.

Ceci démontre le [théorème 0.9](#) dans le cas particulier où f est *propre*, ou bien lorsque $S = \text{Spec}(k)$.

11.4.4. Notons que l'on peut améliorer légèrement le résultat d'effaçabilité précédent : donné $f : X \rightarrow S$ propre (et Λ), on peut calculer $X' \rightarrow X$ fini surjectif

$$\begin{array}{ccc} X & \xleftarrow{\pi} & X' \\ f \downarrow & \swarrow f' & \\ S & & \end{array}$$

tel que le morphisme $R^{\geq 1} f_\star \Lambda \rightarrow R^{\geq 1} f'_\star \Lambda$ soit nul, où l'on note $R^{\geq 1} = \tau_{\geq 1} R$ pour simplifier. Il suffit d'itérer suffisamment la construction (cf. par exemple [Bhatt 2012, §2]).

Déduisons de cette observation que, si f n'est plus nécessairement propre (mais toujours de type fini), l'existence d'un morphisme *fini* surjectif $\pi : X' \rightarrow X$ tel que les $R^i f_\star \Lambda \rightarrow R^i f'_\star \Lambda$ soient nuls pour $i > 0$ se déduit de l'existence d'une *altération* a effaçant la cohomologie. Supposons en effet que l'on ait un diagramme commutatif

$$\begin{array}{ccc} \tilde{X} & \xleftarrow{\tilde{\pi}} & \tilde{X}' \\ a \downarrow & \swarrow b & \downarrow \\ X & \xleftarrow{\pi} & X' \\ f \downarrow & \swarrow f' & \\ S & & \end{array} \begin{array}{l} \curvearrowright g \\ \curvearrowright g' \end{array}$$

où :

- a est une altération effaçant la cohomologie de f : la flèche de functorialité $R^i f_* \Lambda \rightarrow R^i g_* \Lambda$ est nulle pour chaque $i > 0$;
- $\tilde{\pi}$ est un morphisme fini surjectif effaçant la cohomologie du morphisme propre a : la flèche de functorialité $R^{\geq 1} a_* \Lambda \rightarrow R^{\geq 1} b_* \Lambda$ est nulle ;
- $\tilde{X}' \rightarrow X' \rightarrow X$ est la *factorisation de Stein* de b ; en particulier, π est fini surjectif.

(D'après ce qui précède, donné a , on sait *calculer* un tel diagramme.) Il résulte de la seconde hypothèse que l'on a une factorisation diagonale du carré commutatif ci-dessous

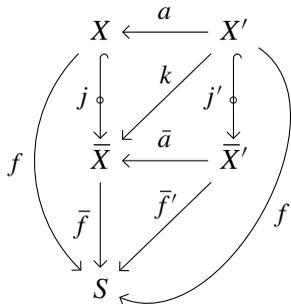
$$\begin{array}{ccc}
 \Lambda & \longrightarrow & R^0 b_* \Lambda = \pi_* \Lambda \\
 \downarrow & \nearrow \text{dotted arrow} & \downarrow \\
 R a_* \Lambda & \longrightarrow & R b_* \Lambda
 \end{array}$$

où l'égalité du coin supérieur droit est conséquence de la troisième hypothèse. Fixons $n > 0$ et appliquons le foncteur $R^n f_*$. Le carré précédent devient

$$\begin{array}{ccc}
 R^n f_* \Lambda & \longrightarrow & R^n f'_* \Lambda \\
 \downarrow 0 & \nearrow \text{dotted arrow} & \downarrow \\
 R^n g_* \Lambda & \longrightarrow & R^n g'_* \Lambda
 \end{array}$$

La nullité de la flèche verticale de gauche correspond à la première hypothèse. La flèche horizontale supérieure est donc nulle. CQFD.

11.4.5. Les observations précédentes et le théorème de résolution des singularités [de Jong 1996, 4.1] ramènent le calcul d'un morphisme fini surjectif effaçant la cohomologie d'un morphisme (non nécessairement propre) $f : X \rightarrow S$ au cas particulier où : X est le complémentaire d'un diviseur à croisements normaux stricts D dans un schéma projectif lisse \bar{X} sur k , et où l'on s'autorise à effacer par une *altération* a . Le cas propre étant déjà connu, il suffit de montrer que l'on peut calculer un diagramme commutatif



où \bar{a} est une altération et le carré commutatif ci-dessous

$$\begin{array}{ccc} \mathbf{R}^n \bar{f}_* \Lambda & \longrightarrow & \mathbf{R}^n \bar{f}'_* \Lambda \\ \downarrow & \nearrow & \downarrow \\ \mathbf{R}^n f_* \Lambda & \longrightarrow & \mathbf{R}^n f'_* \Lambda \end{array}$$

se factorise diagonalement comme indiqué. En effet, le cas propre appliqué au morphisme \bar{f}' permet de construire une altération (et même un morphisme fini surjectif) $\bar{X}'' \rightarrow \bar{X}'$ effaçant $\mathbf{R}^n \bar{f}'_* \Lambda$; la conclusion est alors immédiate.

Comme au paragraphe précédent (11.4.4), il suffit de montrer que l'on peut calculer une altération \bar{a} effaçant $\mathbf{R}^{\geq 1} j_* \Lambda$, c'est-à-dire telle que le morphisme $\mathbf{R}^{\geq 1} j_* \Lambda \rightarrow \mathbf{R}^{\geq 1} k_* \Lambda$ soit nul. En effet, on a sous cette hypothèse un diagramme commutatif et une factorisation

$$\begin{array}{ccccc} \Lambda & \longrightarrow & k_* \Lambda = \bar{a}_* \Lambda & \longrightarrow & \mathbf{R} \bar{a}_* \Lambda \\ \downarrow & & \nearrow & & \downarrow \\ \mathbf{R} j_* \Lambda & \longrightarrow & & \longrightarrow & \mathbf{R} k_* \Lambda \end{array}$$

induisant après application du foncteur $\mathbf{R}^n \bar{f}_*$ le diagramme commutatif

$$\begin{array}{ccccc} \mathbf{R}^n \bar{f}_* \Lambda & \longrightarrow & \mathbf{R}^n \bar{f}_*(\bar{a}_* \Lambda) & \longrightarrow & \mathbf{R}^n \bar{f}_*(\mathbf{R} \bar{a}_* \Lambda) = \mathbf{R}^n \bar{f}'_* \Lambda \\ \downarrow & & \nearrow & & \downarrow \\ \mathbf{R}^n f_* \Lambda & \longrightarrow & & \longrightarrow & \mathbf{R}^n f'_* \Lambda \end{array}$$

désiré. Pour effacer $\mathbf{R}^{\geq 1} j_* \Lambda$, il suffit — par itération, cf. 11.4.4, premier paragraphe — de savoir effacer chaque $\mathbf{R}^i j_* \Lambda$ pour $i > 0$ (en nombre fini). Pour tout entier $N > 0$, il existe un morphisme fini surjectif $\bar{X}' \rightarrow \bar{X}$ tel que, Zariski-localement sur \bar{X} , le tiré en arrière du diviseur $D = \bar{X} - X$ soit une puissance N -ième dans \bar{X}' . En effet, il est possible de trouver, Zariski-localement, une extension finie du corps des fractions de \bar{X} telle que la clôture intégrale de \bar{X} convienne (cf. [Deligne 1980, §1.7.9]) ; il suffit alors de considérer la clôture intégrale de \bar{X} dans une extension composée. Vérifions que $\bar{X}' \rightarrow \bar{X}$ efface les $\mathbf{R}^i j_* \Lambda$. Soit d un point géométrique de D , $U = X \times_{\bar{X}} \bar{X}'_{(d)}$ le complémentaire de $D_{(d)}$ dans le schéma régulier strictement local $\bar{X}'_{(d)}$ et V l'ouvert correspondant dans $\bar{X}'_{(d)} = \bar{X}'_{(d)} \times_{\bar{X}} \bar{X}'$. La fibre en d de $\mathbf{R}^i j_* \Lambda \rightarrow \mathbf{R}^i k_* \Lambda$ s'identifie à l'application de fonctorialité $H^i(U, \Lambda) \rightarrow H^i(V, \Lambda)$. Cette dernière est nulle par construction et pureté lorsque $N \cdot \Lambda = \{0\}$. Notons que l'on peut bien itérer cette construction car, quitte à altérer (ce qui est licite comme on l'a vu), on peut supposer que \bar{X}' est régulier et que l'ouvert X' image inverse de X est le complémentaire d'un diviseur à croisements normaux stricts. Ceci achève la démonstration du [théorème 0.9](#).

11.5. Questions. Nous terminons en suggérant quelques questions, de difficulté variée, qui nous paraissent être un prolongement naturel de ce travail, et que nous n'avons pas eu la patience ou le courage d'aborder.

11.5.1. Calculer $H^i(X, \mathcal{K})$, voire $\Gamma(X, \mathcal{K})$, pour \mathcal{K} un complexe borné constructible de Λ -modules. Variante relative : étendre le [théorème 0.9](#) au calcul de $Rf_*\mathcal{K}$.

11.5.2. (Théorème de changement de base propre effectif.) Donnés $X \rightarrow S$ un morphisme *propre* et $s \in S$, construire un voisinage étale U de s tel que tout élément de $H^*(X_s, \Lambda)$ se relève à X_U .

11.5.3. Calculer les cycles proches $\Psi_f(\Lambda)$ d'un morphisme $f: X \rightarrow S = \text{Spec}(k[t]_{(t)})$.

11.5.4. Calculer les nombres de Betti ℓ -adiques dans le cas non nécessairement propre et lisse.¹⁰

11.6. Primitive récursivité, ou existence de bornes algorithmiques. Comme nous l'avons signalé en [0.10](#) (voir aussi [12.8](#) pour une explication plus détaillée), la notion de « calculabilité » que nous avons utilisée est la notion classique de calculabilité au sens de Church–Turing, qui permet notamment d'effectuer des « recherches non bornées », c'est-à-dire énumérer des objets (toujours ramenables aux entiers naturels) jusqu'à en trouver un, si on sait qu'il existe, vérifiant une propriété algorithmiquement testable. L'utilisation de ce procédé, sans aucune borne *a priori* sur la longueur des recherches en question, fait perdre tout contrôle sur la complexité de nos algorithmes.

Il nous semble cependant plausible que de telles bornes puissent être trouvées. Plus exactement, nous pensons que les fonctions calculées algorithmiquement dans le présent article sont au moins *primitivement récursives*, c'est-à-dire calculables par un algorithme dont toutes les boucles peuvent être bornées *a priori* au sens où on doit avoir calculé un majorant sur le nombre d'exécutions de toute boucle avant d'entrer dans celle-ci : cf. [[Odifreddi 1989](#), définition I.1.6 et proposition I.5.8]. Ceci interdit l'utilisation des « recherches non bornées » et correspond à la façon la plus naturelle de les interdire.¹¹ (Pour rendre plus parlante la notion de fonction primitivement récursive, on peut décrire un langage de programmation qui ne permet

10. Ce problème nous semble actuellement hors de portée.

11. Il n'est malheureusement pas possible de dire que toute fonction intuitivement calculable sans recherche non bornée est primitivement récursive, car il existe différentes sortes de récursion garantissant la terminaison qui ne peuvent pas s'exprimer sous forme primitivement récursive : la fonction d'Ackermann en est un exemple ; on pourra consulter [[Odifreddi 1999](#), VIII.9, notamment les définitions VIII.9.1 et VIII.9.3] pour des notions plus générales. De toute manière, l'argument général du problème de l'arrêt (i.e., un principe diagonal) ne permet pas qu'on puisse formaliser la notion intuitive de « fonction calculable sans recherche non bornée » (donc en particulier, terminant toujours).

pas d'appels récursifs de fonctions et dans lequel toutes les boucles sont des boucles bornées par la valeur d'une variable à l'entrée de la boucle : tel est le langage « BlooP » décrit dans [Hofstadter 1979, chapitre XIII], qu'on pourra consulter pour une description agréable à lire de la différence entre fonctions primitivement récursives et générales récursives, ces dernières y étant définies par le langage « FlooP ».) Par ailleurs, les fonctions primitivement récursives sont une « classe de complexité » car une fonction primitivement récursive est une fonction qui peut être calculée algorithmiquement avec une complexité (en espace ou en temps) elle-même donnée par une fonction primitivement récursive : cf. [Odifreddi 1999, VIII.8.8].

Les fonctions que nous calculons sont peut-être même « élémentaires » (ou « élémentairement récursives ») au sens de Kalmár, c'est-à-dire de temps d'exécution borné par une tour d'exponentielles, cf. [ibid., définition VIII.7.1]; de nouveau, il revient au même de dire qu'elle est calculable algorithmiquement avec une complexité elle-même élémentaire (cf. [ibid., théorème VIII.7.6]).

Cette supposition est motivée, entre autres, par un slogan proposé par certains logiciens, cf. [Friedman 1999, conjecture 1] ou [Avigad 2003, « grand conjecture » p. 258], selon lequel tout théorème mathématique « ordinaire », ¹² qui peut s'énoncer dans le langage de l'arithmétique, est en fait prouvable dans des systèmes formels faibles de l'arithmétique ; or, dès que ces systèmes prouvent qu'un algorithme termine, ils prouvent en fait qu'il appartient à une classe de complexité bien comprise. On pense notamment au système PRA, « Primitive Recursive Arithmetic » (défini par exemple en [Simpson 2009, IX, §3]) et qui démontre la terminaison précisément des fonctions primitivement récursives (cf. [Hájek et Pudlák 1998, corollaire IV.3.7]), et au système EA, « Elementary [fonction] Arithmetic », défini en [Avigad 2003, §2], et qui démontre la terminaison des fonctions Kalmár-élémentaires (cf. [Avigad 2003, théorème 2.2 et remarque qui suit]). Si notre théorème (affirmant qu'un certain algorithme termine en calculant la cohomologie étale) est démontrable dans ces systèmes faibles, c'est que l'algorithme est primitivement récursif voire Kalmár-élémentaire.

Pour s'en convaincre, il faudrait chercher à reprendre tous les résultats d'existence utilisés ici pour faire apparaître une borne explicite sur les objets construits (de manière à placer les algorithmes dans une des hiérarchies décrites dans [Odifreddi 1999, chapitre VIII]). Nous n'avons pas eu le courage de mener cet exercice, mais nous avons au moins cherché à limiter les appels aux « recherches non bornées » (notamment en 6.6, ou encore 15.5 pour le calcul de la normalisation). Il reste que nous n'avons pas réussi à l'éviter dans la construction d'un hyperrecouvrement

12. Il va de soi que l'affirmation est fautive sans le qualificatif « ordinaire », et que celui-ci ne peut pas être défini rigoureusement. Voir [Smoryński 1985] (ainsi que les autres articles de cet auteur dans le même recueil [Harrington et al. 1985]) pour un aperçu généraliste de ces questions, ou bien l'introduction de [Friedman 2011] pour une présentation plus systématique.

d'un schéma X par des polycourbes ℓ -élémentaires ([proposition 1.4.9](#) et suite) : s'il est probable que, dans le cas où X est lisse on puisse sans trop de mal construire explicitement les polycourbes en question en suivant la démonstration de [[SGA 4₃ 1973](#), XI, §2–3], le cas général nécessiterait aussi de revoir les résultats de [[de Jong 1996](#)] sous un angle algorithmique.

II. Algèbre commutative et géométrie algébrique effectives

L'objet de cette partie est de vérifier la calculabilité des propriétés et opérations algébriques et géométriques utilisées dans la première partie. Certains des résultats rassemblés ici, bien que connus, nous ont semblé difficiles à trouver dans la littérature, ou bien formulés dans un langage différent du nôtre, si bien que nous avons préféré, pour la commodité du lecteur, redémontrer certains faits, ou rappeler la manière dont ils se démontrent. (Ceci devrait en outre faciliter le travail de vérification du lecteur qui a commencé sa lecture par le texte [[Madore et Orgogozo 2014](#)] et qui souhaite vérifier que tout ce que nous utilisons est calculable dans le modèle de calcul qui y est exposé.)

12. Corps et extensions de corps

Définition 12.1. On appelle *corps calculable* la donnée d'une partie calculable (= récursive) \mathfrak{K} de \mathbb{N} , d'une relation d'équivalence calculable \equiv sur \mathfrak{K} , d'éléments $0_{\mathfrak{K}}$ et $1_{\mathfrak{K}}$ de \mathfrak{K} , et de fonctions calculables $(+)_{\mathfrak{K}}: \mathfrak{K} \times \mathfrak{K} \rightarrow \mathfrak{K}$ et $(-)_{\mathfrak{K}}: \mathfrak{K} \rightarrow \mathfrak{K}$ et $(\times)_{\mathfrak{K}}: \mathfrak{K} \times \mathfrak{K} \rightarrow \mathfrak{K}$ et $(^{-1})_{\mathfrak{K}}: \{z \in \mathfrak{K}: z \not\equiv 0_{\mathfrak{K}}\} \rightarrow \mathfrak{K}$, telles que ces opérations passent au quotient par \equiv et définissent sur \mathfrak{K}/\equiv une structure de corps. On notera généralement $K = (\mathfrak{K}/\equiv)$ et on dira abusivement que K « est » un corps calculable pour sous-entendre qu'on s'est donné une structure de corps calculable dont K est le quotient ; s'il faut désambiguïser, on pourra dire que \mathfrak{K} est l'ensemble d'*étiquettes*¹³ qui servent à décrire les éléments de K .

Une *extension calculable* $\mathfrak{K} \rightarrow \mathfrak{L}$ de corps calculables est la donnée d'une fonction calculable $f: \mathfrak{K} \rightarrow \mathfrak{L}$ telle que $x \equiv_{\mathfrak{K}} y$ implique $f(x) \equiv_{\mathfrak{L}} f(y)$ et que l'application $K \rightarrow L$ définie par passage au quotient soit une extension (un morphisme) de corps. (On dira aussi que K est un sous-corps calculable de L .) Si de plus K est une partie récursive de L , c'est-à-dire s'il existe une fonction calculable qui, donné $y \in \mathfrak{L}$, décide s'il existe x tel que $f(x) \equiv_{\mathfrak{L}} y$ (et, cf. [12.8](#), on peut alors supposer¹⁴ qu'elle calcule ce x), alors on dit que K est un sous-corps calculable *reconnaisable* de L (ou que L est une extension calculable reconnaissable de K).

13. Une autre terminologie possible serait d'appeler \mathfrak{K} un « corps calculé » et K un « corps calculable ».

14. Ce serait la bonne définition à prendre si on voulait remplacer la notion de calculabilité par celle de fonction primitivement récursive.

On dit qu'un corps calculable K admet un *algorithme de factorisation* lorsqu'il existe un algorithme qui, donné un polynôme à coefficients dans K en une variable, calcule sa factorisation¹⁵ en polynômes irréductibles.

Remarques 12.2. (0) Nous renvoyons notamment à [Fröhlich et Shepherdson 1956] et [Stoltenberg-Hansen et Tucker 1999] pour des généralités sur les corps calculables. Il existe différentes variantes autour de la définition, essentiellement sans importance dans le cadre dans lequel nous nous plaçons (par exemple, quitte à n'utiliser que le plus petit élément — pour l'ordre de \mathfrak{R} en tant que partie de \mathbb{N} — de chaque classe d'équivalence, on peut omettre la relation d'équivalence et demander directement que \mathfrak{R} soit une partie récursive de \mathbb{N} munie d'opérations qui en font un corps) ; celle proposée ci-dessus (équivalente à celle de [Stoltenberg-Hansen et Tucker 1999, 2.1.5]), nous semble la plus naturelle et celle qui se transpose le plus agréablement, par exemple, au cas où on remplacerait les fonctions récursives par des fonctions seulement primitivement récursives (cf. [Jacobsson et Stoltenberg-Hansen 1985, §1]).

Il est notamment utile de rappeler les faits suivants.

(1) Si K est un corps calculable, alors $K(T)$ (où T est une indéterminée), ainsi que $K[X]/(f)$ (où $f \in K[X]$ est un polynôme irréductible) sont des extensions calculables et reconnaissables de K . (C'est-à-dire qu'il y a une façon standard de faire de $K(T)$ ou de $K[X]/(f)$ des corps calculables et de l'extension une extension calculable reconnaissable, et c'est de cette structure qu'on parlera toujours ; par exemple, un élément de $K[X]/(f)$, si $d = \deg f$, est décrit comme un d -uplet (c_0, \dots, c_{d-1}) d'éléments de K , ou plus précisément de l'ensemble \mathfrak{R} d'étiquettes des éléments de K , représentant la classe modulo f du polynôme $\sum c_i X^i$, l'addition se faisant terme à terme et la multiplication se faisant en terminant par le reste de la division euclidienne par f , laquelle est évidemment calculable.)

(2) Si K est un corps calculable, alors « la » clôture algébrique de K est une extension calculable de K ([Rabin 1960, théorème 7] ; cf. [Stoltenberg-Hansen et Tucker 1999, corollaire 3.1.11]), mais non reconnaissable en général (cf. le point suivant). (3) L'existence d'un algorithme de factorisation pour un corps calculable K équivaut à l'existence d'un algorithme qui décide si un polynôme admet une racine, ou encore à l'existence d'un algorithme qui reconnaît si un élément de la clôture algébrique de K (calculable comme on vient de le dire en (2)) appartient à K ([Rabin 1960, théorème 8] ; cf. aussi [Stoltenberg-Hansen et Tucker 1999, proposition 3.2.2] et [Miller 2010, théorème 2.5(2)]). Bien entendu, (4) tout corps calculable algébriquement clos admet un algorithme de factorisation.

15. Plus exactement : donné une suite d'étiquettes représentant les coefficients d'un polynôme (en une variable) à factoriser, renvoie des suites d'étiquettes représentant les coefficients de ses facteurs irréductibles.

De plus, (5) si K est un corps calculable admettant un algorithme de factorisation, alors c'est aussi le cas de $K(T)$ (où T est une indéterminée) et de $K[X]/(f)$ si $f \in K[X]$ est un polynôme irréductible *séparable* (cf. [Stoltenberg-Hansen et Tucker 1999, théorèmes 3.2.3 et 3.2.4] ; et (6) la nécessité de l'hypothèse « séparable » pour le point précédent est montrée dans [Fröhlich et Shepherdson 1956, théorème 7.12]).

(7) Si K est un corps *parfait* calculable admettant un algorithme de factorisation (notamment si K est un corps calculable algébriquement clos), et si $K(x_1, \dots, x_n)$ est une extension de type fini de K , puisqu'on peut extraire de x_1, \dots, x_n une base de transcendance séparante [Matsumura 1989, remarque précédant le théorème 26.3], le point (5) montre que le corps calculable $K(x_1, \dots, x_n)$ admet lui aussi un algorithme de factorisation (cf. [Stoltenberg-Hansen et Tucker 1999, 3.2.6] ; ou bien [Lecerf 2013, théorème 4 de l'introduction] lorsque K est un corps premier).

En lien avec ce fait, rappelons que si un corps calculable admet un algorithme de factorisation (des polynômes en une variable), il en admet automatiquement un pour les polynômes en un nombre fini quelconque de variables : [Fried et Jarden 2008, lemme 19.1.3].

12.3. On rappelle (voir notamment [Bourbaki 1981, V, §13] ou [ÉGA IV₁ 1964, 0, §21] ou encore [Fried et Jarden 2008, §2.7]) qu'une p -base (resp. une famille p -libre) finie d'un corps K de caractéristique $p > 0$ (sous-entendu : sur K^p) est une famille $b_1, \dots, b_r \in K$ tels que les produits $b_1^{i_1} \cdots b_r^{i_r}$ pour $0 \leq i_u < p$ forment une base (resp. une famille libre) du K^p -espace vectoriel K ; il existe une p -base finie de K si et seulement si K est de degré fini sur K^p , auquel cas ce degré vaut p^r où r est le cardinal de la p -base : on appelle r le p -rang ou *exposant d'imperfection* de K (sous-entendu : sur K^p).

Proposition 12.4. *Soit K un corps calculable de caractéristique $p > 0$ et de p -rang fini. Il revient au même de se donner :*

- (i) le p -rang r de K et un algorithme décidant si des éléments a_1, \dots, a_s de K sont linéairement indépendants sur K^p ;
- (ii) le p -rang r de K et un algorithme décidant si des éléments a_1, \dots, a_s de K sont p -libres ;
- (iii) une p -base b_1, \dots, b_r de K ;
- (iv) une p -base b_1, \dots, b_r de K et un algorithme exprimant un élément x de K sous la forme $\sum_{\underline{i}} \xi_{\underline{i}}^p b_1^{i_1} \cdots b_r^{i_r}$ où $\xi_{\underline{i}} \in K$ pour $\underline{i} = (i_1, \dots, i_r)$ vérifiant $0 \leq i_u < p$ pour tout u .

« Il revient au même de se donner » signifie qu'on peut exprimer n'importe laquelle de ses données en fonction de n'importe quelle autre de façon algorithmique et uniforme — c'est-à-dire par un algorithme indépendant de K et des autres données.

(On pourra comparer ces équivalences avec [Richman 1981, théorème 1] qui en est l'analogie dans le cadre de l'algèbre constructive.)

On dira qu'on a sur un corps calculable une p -base finie explicite en référence à n'importe laquelle de ces données.

Démonstration. Il est évident que connaître (i) permet de connaître (ii) (tester la p -liberté revient, par définition de ce terme, à tester l'indépendance linéaire de certaines puissances). Connaissant (ii), on peut connaître (iii) en énumérant les éléments de K et en ajoutant ceux qui sont p -libres avec les précédents jusqu'à atteindre le p -rang de K . Connaissant (iii) on obtient (iv) en énumérant toutes les écritures possibles de x sur la p -base jusqu'à en obtenir une qui convient. Enfin, connaissant (iv), on a un isomorphisme explicite de K^p -espaces vectoriels entre K et $(K^p)^{\oplus p^r}$ (somme de p^r copies de K^p), ce qui permet donc facilement de tester l'indépendance linéaire d'une famille (il s'agit simplement de calculer des déterminants). \square

Comme on l'a souligné en 12.2(5–6), si K est un corps calculable admettant un algorithme de factorisation, ces propriétés valent pour $L := K[X]/(f)$ (avec $f \in K[X]$ irréductible) lorsque f est séparable, mais pas nécessairement dans le cas général. Si on fait l'hypothèse qu'on dispose sur K d'une p -base finie explicite, cette difficulté n'existe plus :

Lemme 12.4.1. *Soit K un corps calculable pour lequel on dispose d'un algorithme de factorisation et d'une p -base finie explicite. Soit $a \in K$ n'appartenant pas à K^p . Alors sur le corps $L := K(\sqrt[p]{a})$ (extension calculable reconnaissable de K comme rappelé en 12.2(1)), on dispose d'un algorithme de factorisation et d'une p -base finie explicite.*

Démonstration. Puisque $a \notin K^p$ (autrement dit, le singleton a est p -libre), d'après 12.4(ii), on peut explicitement construire une p -base de K contenant l'élément a (comme dans la démonstration du fait que (ii) permet de trouver (iii), en partant de a), disons a, b_2, \dots, b_r . Alors $a^{1/p}, b_2, \dots, b_r$ constitue une p -base explicite de L .

Pour montrer que L dispose d'un algorithme de factorisation, d'après [Fröhlich et Shepherdson 1956, 7.3] ou son amélioration citée dans [Stoltenberg-Hansen et Tucker 1999, 3.2.5], il suffit de montrer qu'on peut décider si un élément de L est une puissance p -ième : or d'après 12.4(iv) on sait l'écrire sur la p -base $a^{1/p}, b_2, \dots, b_r$, et il suffit de vérifier que seul le coefficient devant 1 est non nul dans cette écriture. \square

Le résultat suivant a pour objet de convaincre que tous les corps que nous serons amenés à considérer sont calculables avec un algorithme de factorisation :

Proposition 12.5. *Soit K un corps calculable pour lequel on dispose d'un algorithme de factorisation et (si K est de caractéristique $p > 0$) d'une p -base finie explicite. Soit L l'extension de K définie par l'une des opérations suivantes :*

- (i) *l'ajout d'un transcendant : $L = K(T)$ où T est une indéterminée,*
- (ii) *l'ajout d'un élément algébrique : $L = K[X]/(f)$ où $f \in K[X]$ est irréductible (non supposé séparable), donné,*
- (iii) *le passage à la ¹⁶ clôture algébrique $L = K^{\text{alg}}$ de K ,*
- (iv) *le passage à la clôture séparable $L = K^{\text{sép}}$ de K ,*
- (v) *(dans le cas où K est de caractéristique $p > 0$) le passage à la clôture parfaite $L = K^{1/p^\infty}$ de K ,*

alors L est une extension calculable reconnaissable de K , et on dispose d'un algorithme de factorisation et d'une p -base finie explicite pour L .

Plus précisément, on va esquisser des algorithmes explicites qui, donnés des algorithmes qui calculent les opérations sur K et la factorisation des polynômes de $K[X]$ et une p -base finie explicite de K , et donnés le cas où on se place, et le polynôme f dans le cas (ii), présentent L comme une extension calculable reconnaissable de K , permettent de factoriser les polynômes de $L[X]$, et fournissent une p -base de L .

(On pourra comparer avec [Mines et Richman 1982, théorème 3.9], analogue de (ii) ci-dessus mais dans le cadre de l'algèbre constructive.)

Démonstration. Traitons chacun des cas séparément.

(i) Le corps $L = K(T)$ est une extension calculable reconnaissable de K comme on l'a rappelé en 12.2(1), et dispose d'un algorithme de factorisation d'après 12.2(5). En ajoutant T à la p -base de K on obtient une p -base de L (cf. [Fried et Jarden 2008, lemme 2.7.2 et sa démonstration]).

Pour le cas (ii), on peut distinguer le cas où f est séparable et celui où il est purement inséparable : en effet, il est algorithmique d'écrire un polynôme irréductible $f \in K[X]$ sous la forme $h(X^{p^e})$ avec h irréductible et séparable, ce qui ramène l'extension $K[X]/(f)$ aux deux extensions $E := K[X]/(h)$ avec h séparable puis $L = E[X]/(X^{p^e} - a)$ avec a la classe de X modulo h . Par ailleurs, pour les extensions purement inséparables, on peut encore se ramener au cas où le polynôme est de la forme $X^p - a$ (quitte à écrire une racine (p^e)-ième comme extractions successives de racines p -ièmes).

16. On conviendra que, s'agissant d'un corps calculable, « la » clôture algébrique désigne celle qui est construite explicitement par l'algorithme de Rabin : cf. 12.2(2) ; et de même « la » clôture séparable désigne la clôture séparable dans cette clôture algébrique.

Dans le cas (ii) avec f séparable, le corps L est une extension calculable reconnaissable de K comme on l'a rappelé en 12.2(1), et dispose d'un algorithme de factorisation d'après 12.2(5). Une p -base de K est encore une p -base de L (cf. [Fried et Jarden 2008, lemme 2.7.3]).

Dans le cas (ii) avec f de la forme $X^p - a$ a été traité en 12.4.1.

(iii) La clôture algébrique L de K est une extension calculable de K comme on l'a rappelé en 12.2(2), et dispose d'un algorithme de factorisation (12.2(4)). La p -base vide convient pour L . De plus, comme K était supposé disposer d'un algorithme de factorisation, on peut reconnaître K dans L d'après 12.2(3).

(iv) La clôture séparable L de K se voit comme un sous-corps de la clôture algébrique : pour reconnaître si un élément de cette dernière appartient à L , il suffit de calculer son polynôme minimal sur K (quitte à énumérer tous les polynômes de $K[X]$ jusqu'à en trouver un qui annule l'élément considéré,¹⁷ cf. 12.8, puis le factoriser) et vérifier s'il est séparable. On dispose d'un algorithme de factorisation puisque, d'après 12.2(3), il suffit pour cela de savoir identifier un élément de L dans la clôture algébrique commune de K et L , et on vient d'expliquer que c'est possible. Enfin, une p -base de K est encore une p -base de L (cf. [Fried et Jarden 2008, lemme 2.7.3]).

(v) Si K est un corps calculable (sans autre hypothèse pour l'instant), alors on peut construire $L = K^{1/p^\infty}$ extension calculable de K explicitement selon sa définition : on définit \mathfrak{L} comme l'ensemble des couples (e, a) où $e \in \mathbb{N}$ et a est un élément de K : ce couple représente alors la racine (p^e) -ième de a dans L , et on peut définir $(e, a) \equiv_{\mathfrak{L}} (e', a')$ (disons pour $e' \geq e$) lorsque $a^{p^{e'-e}} = a'$ dans K , ce qui est bien une relation calculable. Pour ajouter ou multiplier (e, a) et (e', a') (disons pour $e' \geq e$), on remplace (e, a) par $(e', a^{p^{e'-e}})$ et on effectue l'opération entre $a^{p^{e'-e}}$ et a' , qui est calculable.

Avec l'hypothèse supplémentaire que K dispose d'un algorithme de factorisation, on peut tester si un élément de K a sa racine p -ième dans K (et le cas échéant la calculer) : on peut donc considérer uniquement les couples $(e, a) \in \mathfrak{L}$ « canoniques », définis comme ceux pour lesquels $a \notin K^p$ si $e > 0$, convertir un couple $(e, a) \in \mathfrak{L}$ quelconque en un couple « canonique », et on voit alors clairement que L est une extension calculable reconnaissable de K (c'est d'ailleurs essentiellement ce qui est fait dans [Steel 2005, §2.1]).

Pour montrer que L dispose d'un algorithme de factorisation, il suffit clairement de montrer qu'on peut factoriser dans L les polynômes f de $K[X]$ (quitte à appliquer l'isomorphisme entre K^{1/p^e} et K pour un e assez grand) : comme K a un algorithme de factorisation, on peut évidemment supposer f irréductible dans $K[X]$, et l'écrire

17. Il va de soi que sur une description réellement explicite de la clôture algébrique on n'aurait pas besoin de faire quelque chose d'aussi absurde !

sous la forme $h(X^{p^e})$ avec $h \in K[X]$ irréductible séparable : ceci se réécrit $(h_1(X))^{p^e}$ avec h_1 le polynôme de $L[X]$ dont les coefficients sont les racines (p^e) -ièmes de ceux de h ; en utilisant de nouveau l'isomorphisme entre K^{1/p^e} et K il est clair que h_1 est irréductible dans $L[X]$, et on a la factorisation voulue. Enfin, la p -base vide convient pour L . \square

Remarque 12.6. L'énoncé ci-dessus considère des extensions algébriques du type $L = K[X]/(f)$ avec f irréductible (i.e., (f) maximal dans $K[X]$). Il n'y aura pas de difficulté, dès qu'on saura manipuler les idéaux d'une algèbre de polynômes à plusieurs variables (§13), à y exprimer des extensions du type $L = K[Z_1, \dots, Z_d]/\mathfrak{m}$ avec \mathfrak{m} un idéal maximal de $K[Z_1, \dots, Z_d]$ comme une tour d'extensions mono-gènes. Il suffit en effet d'utiliser un algorithme d'élimination, cf. [Eisenbud 1995, §15.10.4], pour calculer les intersections $\mathfrak{m} \cap K[Z_1, \dots, Z_i]$, qui définissent autant d'extensions de corps $K_i \subseteq K_{i+1}$ avec $K_i = K[Z_1, \dots, Z_i]/(\mathfrak{m} \cap K[Z_1, \dots, Z_i])$, algébriques engendrées par un seul élément dont on connaît le polynôme minimal, et $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_d = L$.

Plus généralement, si \mathfrak{p} est un idéal premier de $K[Z_1, \dots, Z_d]$, l'extension $L := \text{Frac}(K[Z_1, \dots, Z_d]/\mathfrak{p})$ de K se ramène également explicitement à des extensions comme envisagées ci-dessus : en effet, il suffit de considérer un ensemble maximal E de variables Z_i telles que $\mathfrak{p} \cap K[E] = \{0\}$ (de nouveau calculable par élimination), si bien que $K(E) = \text{Frac}(K[E])$ est une extension transcendante pure de K et que L en est une extension algébrique du type considéré au paragraphe précédent (on peut aussi invoquer le lemme de normalisation de Noether [Eisenbud 1995, théorème 13.3] ou [Serre 1965, III(D)2, théorème 2], mais ce n'est pas nécessaire ici car on a recherché simplement la finitude générique, c'est-à-dire la finitude de l'extension de corps).

Convention 12.7. On fera souvent l'abus de langage consistant à écrire qu'une certaine opération algébrique ou géométrique est calculable sans autre précision sur le corps k dans lequel vivent les données : sauf mention du contraire, il faut en fait comprendre : pour tout corps k calculable, disposant d'un algorithme de factorisation (cf. 12.2) et une p -base finie explicite (12.4), l'opération en question est calculable. Lorsque k est algébriquement clos, bien entendu, seule l'hypothèse « calculable » est utile (cf. 12.2(4)) ; par ailleurs, d'après le résultat qu'on vient de montrer, les corps que nous sommes amenés à manipuler vérifient toujours les hypothèses qui viennent d'être dites.

(Dans le langage de l'algèbre constructive, l'analogue de nos hypothèses « calculable, disposant d'un algorithme de factorisation et une p -base finie explicite » serait les corps « discrets pleinement factoriels » : voir [Mines, Richman et Ruitenburg 1988, théorème VII.3.3].)

Remarque 12.8. Le fait de considérer des fonctions récursives (générales, par opposition par exemple aux fonctions primitivement récursives) signifie que si $P(m, n)$ est une propriété calculable (des entiers naturels) et que pour chaque m il existe n vérifiant $P(m, n)$, alors la fonction $\mu_n P$ qui à m associe le plus petit n vérifiant $P(m, n)$ est calculable (il s'agit de l'« opérateur μ de Kleene », cf. par exemple [Odifreddi 1989, définitions I.1.5 et I.1.7]). Concrètement, cela signifie que les fonctions calculables (= récursives, donc) peuvent effectuer des « recherches non bornées » dans les entiers naturels, c'est-à-dire parcourir tous les n jusqu'à en trouver un qui vérifie la propriété $P(m, n)$ demandée, même si on ne dispose d'aucune borne de complexité sur le temps qu'une telle recherche pourra prendre (on demande simplement qu'elle termine pour tout m si on veut que la fonction soit totale).

Comme les corps calculables (12.1) sont étiquetés par les entiers naturels, cette notion de « recherche non bornée » s'applique aussi bien à eux. C'est la raison pour laquelle, dans la définition d'un corps calculable, on pourrait par exemple se passer d'imposer que la fonction $(\cdot)^{-1}_{\mathfrak{K}} : \{z \in \mathfrak{K} : z \not\equiv 0_{\mathfrak{K}}\} \rightarrow \mathfrak{K}$ soit calculable (elle l'est automatiquement puisque pour calculer x^{-1} on peut parcourir tous les $y \in \mathfrak{K}$ jusqu'à en trouver un qui vérifie $x \times_{\mathfrak{K}} y \equiv_{\mathfrak{K}} 1_{\mathfrak{K}}$).

Une fois définis les schémas et autres objets géométriques en 16, on pourra effectuer de même ce type de « recherches non bornées » sur l'ensemble des schémas, morphismes de schémas, ou tout autre objet géométrique du même type : il s'agira d'énumérer toutes les données susceptibles de décrire, par exemple, un schéma, et pour chacune d'elles de tester si elle vérifie la propriété P considérée. Ainsi, il découle du théorème de A. J. de Jong sur la résolution des singularités par altérations [de Jong 1996, 4.1], et du fait que cette propriété soit algorithmiquement testable, qu'on peut en fait calculer une telle résolution ! Il va de soi que cette façon de procéder fait perdre toute utilisabilité pratique à nos algorithmes — et comme observé en 11.6 on *devrait* pouvoir s'en passer.

Sous-remarque : On pourrait même être un peu plus général dans les recherches par test non bornées : il n'est pas nécessaire que la propriété $P(m, n)$ soit décidable (= calculable, = récursive), il suffit qu'elle soit semi-décidable (= récursivement énumérable), autrement dit qu'il existe une machine de Turing qui termine en répondant « vrai » lorsque $P(m, n)$ est vrai, sans imposer qu'elle termine quand $P(m, n)$ n'est pas vrai — on peut alors calculer *un* n vérifiant $P(m, n)$ (pas nécessairement le plus petit) en lançant en parallèle la vérification de tous les $P(m, n)$ jusqu'à ce que l'une d'entre elles termine.

13. Modules de type fini sur une k -algèbre de type fini

Soit $S = k[Z_1, \dots, Z_d]$ où k est un corps calculable (nous n'utiliserons pas ici l'ensemble des hypothèses 12.7 puisque nous n'aurons jamais affaire à des

factorisations de polynômes : la simple calculabilité de k suffit). Le but de cette section est de montrer qu'on peut manipuler algorithmiquement les S -modules de type fini, et, plus généralement, les modules de type fini sur une algèbre quotient de S .

13.1. Algorithmes fondamentaux. Un morphisme $\varphi: S^m \rightarrow S^n$ de S -modules est représenté par une matrice $n \times m$ d'éléments de S . On sait (par exemple en utilisant des bases de Gröbner) répondre algorithmiquement aux deux questions fondamentales suivantes :

— (*Test d'appartenance à un sous-module.*) Donné $\varphi: S^m \rightarrow S^n$ et un élément $y \in S^n$, décider si y appartient à l'image M de φ et, le cas échéant, en calculer un antécédent. (Ou, de façon équivalente : donnés $x_1, \dots, x_m \in S^n$ et $y \in S^n$, décider si y peut être écrit comme combinaison linéaire de x_1, \dots, x_m et, le cas échéant, en trouver les coefficients. Pour le faire, on peut calculer une base de Gröbner du sous-module M engendré par x_1, \dots, x_m , cf. [Eisenbud 1995, algorithmes 15.7 et 15.9], [Decker et Lossen 2006, problème 2.16] ou [Becker et Weispfenning 1993, lemme 6.7 et discussion qui suit], cette base de Gröbner étant elle-même écrite comme combinaison des x_i , et ceci permet de décider si un élément y appartient à M et, le cas échéant, l'écrire comme combinaison des élément de la base, donc des x_1, \dots, x_m .)

— (*Calcul de syzygies.*) Donné $\varphi: S^m \rightarrow S^n$, calculer un ensemble de générateurs du noyau de φ (ou, si on préfère, donnés des éléments x_1, \dots, x_m de S^n , calculer un système de générateurs des syzygies entre eux, cf. [Eisenbud 1995, algorithme 15.10] ou [Becker et Weispfenning 1993, théorème 6.4]).

(De façon alternative, on pourra se référer à [Mines, Richman et Ruitenburg 1988, VIII.1.5 combiné à III.2.6] ou bien [Lombardi et Quitté 2011, VII.1.10] pour une présentation de ces faits en algèbre constructive et sans utiliser de bases de Gröbner.)

Soulignons que les algorithmes en question n'utilisent que des opérations rationnelles et des tests d'égalité dans le corps k .

13.2. Noyaux, conoyaux et images sur les anneaux de polynômes. Une *présentation explicite* d'un S -module M de type fini est la donnée d'un morphisme $\varphi: G \rightarrow F$, où F, G sont deux S -modules libres de type fini, tel que $M = \text{Coker } \varphi$ (concrètement, φ est fourni sous la forme d'une matrice $n \times m$ d'éléments de S où m et n sont les rangs de G et F respectivement).

Une *présentation explicite* d'un morphisme $\alpha: P \rightarrow Q$ de S -modules, où

$$P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P) \quad \text{et} \quad Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q) \quad (\ddagger)$$

sont deux S -modules explicitement présentés comme ci-dessus, est la donnée d'un morphisme $\alpha_F: F_P \rightarrow F_Q$ tel que α se déduise de α_F par passage au quotient (autrement dit, tel qu'il existe $\alpha_G: G_P \rightarrow G_Q$ vérifiant $\alpha_F \varphi_P = \varphi_Q \alpha_G$).

Dans le contexte ci-dessus, donnés les conoyaux P et Q de $G_P \xrightarrow{\varphi_P} F_P$ et $G_Q \xrightarrow{\varphi_Q} F_Q$, on sait tester si un $\alpha_F: F_P \rightarrow F_Q$ est la présentation explicite d'un morphisme $\alpha: P \rightarrow Q$; et de plus, on sait calculer algorithmiquement l'image, le conoyau, et le noyau, d'un morphisme explicitement présenté : les algorithmes à cet effet sont bien connus, mais nous les rappelons brièvement ci-dessous pour la commodité du lecteur.

- Pour tester si $\alpha_F: F_P \rightarrow F_Q$ passe au quotient et définit (une présentation explicite d'un) morphisme $\alpha: P \rightarrow Q$ (où P et Q sont encore donnés par (\ddagger)), il s'agit, grâce à l'algorithme de test d'appartenance évoqué en 13.1, de tester si les éléments images de la base de G_P par $\alpha_F \varphi_P$ sont dans l'image de φ_Q : cf. [Decker et Lossen 2006, problème 4.1 et début de §4.2].
- Donné $\alpha: L \rightarrow F$ un morphisme entre S -modules libres de type fini, on sait calculer une présentation explicite de $\text{Im } \alpha$ (sous la forme $\text{Im } \alpha = \text{Coker}(H \rightarrow L)$). En effet, ceci revient exactement à calculer des générateurs des syzygies entre les images par α des éléments de la base de L (c'est-à-dire, des colonnes de la matrice décrivant α), algorithme déjà évoqué en 13.1 comme calcul de syzygies.
- Si $\alpha: L \rightarrow Q$ est un morphisme de S -modules, où L est toujours libre mais cette fois Q est défini par une présentation explicite $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$, le morphisme α étant explicitement présenté par la donnée de $\alpha_F: L \rightarrow F_Q$, alors on peut encore calculer une présentation explicite de $\text{Im } \alpha$. En effet, il est isomorphe à $(\text{Im } \alpha_F + \text{Im } \varphi_Q) / \text{Im } \varphi_Q$, or $\text{Im } \alpha_F + \text{Im } \varphi_Q$ est l'image du morphisme $L \oplus G_Q \xrightarrow{(\alpha_F, \varphi_Q)} F_Q$ de modules libres, cas traité par le paragraphe précédent, et si $H \rightarrow L \oplus G_Q$ est la présentation de cette image, alors $H \rightarrow L$ définit la présentation de $\text{Im } \alpha$ recherchée (cf. [Decker et Lossen 2006, problème 4.2]).
- Donné un morphisme $\alpha: P \rightarrow Q$ explicitement présenté entre modules explicitement présentés $P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$, il est facile de calculer une présentation explicite de $\text{Coker } \alpha$, à savoir $\text{Coker } \alpha = \text{Coker}(F_P \oplus G_Q \xrightarrow{(\alpha_F, \varphi_Q)} F_Q)$ (cf. [Decker et Lossen 2006, §4.2.1]). Mais on peut également calculer une présentation de $\text{Im } \alpha$ sous la forme $\text{Coker}(H \rightarrow F_P)$ avec H libre (en effet, il s'agit de $\text{Im}(F_P \rightarrow Q)$, cas qu'on a traité au paragraphe précédent), et aussi de $\text{Ker } \alpha$ (il s'agit de l'image de $H \rightarrow P$, de nouveau le cas qu'on a traité). (cf. [Decker et Lossen 2006, problème 4.3] ou [Eisenbud 1995, proposition 15.32].)

On notera bien évidemment qu'on obtient non seulement une présentation explicite de l'image ou du noyau d'un morphisme explicitement présenté $\alpha: P \rightarrow Q$, mais

aussi une présentation explicite de l'inclusion canonique $\text{Im } \alpha \rightarrow Q$ ou $\text{Ker } \alpha \rightarrow P$. Ceci permettra aisément de se convaincre, par exemple, qu'on peut calculer des sommes ou intersections de sous-modules.

13.3. Modules sur les algèbres de type fini quelconques. Si $R = S/I$ est une algèbre de type fini sur un corps k où $S = k[Z_1, \dots, Z_d]$ et I l'idéal engendré par $h_1, \dots, h_r \in S$, un R -module n'est autre qu'un S -module annulé par I . On peut appeler *R -module explicitement présenté* le conoyau d'un morphisme $\varphi: R^m \rightarrow R^n$ (décrit par une matrice $n \times m$ d'éléments de R) ou, de façon équivalente, comme le conoyau d'un morphisme $\tilde{\varphi}: S^m \rightarrow S^n$ tel que $h_j e_i$ soit dans l'image de $\tilde{\varphi}$ pour tout $1 \leq j \leq r$ et tout $1 \leq i \leq n$ (en notant e_1, \dots, e_n la base canonique de S^n) : ce critère est algorithmiquement testable, et on passe de façon évidente d'une description à l'autre (dans un sens en reprenant la matrice de $\tilde{\varphi}$ comme matrice de φ , et dans l'autre en relevant de façon quelconque la matrice de φ et en ajoutant des colonnes $h_j e_i$). Les morphismes de R -modules sont simplement des morphismes de S -modules qui s'avèrent être des R -modules, et ce qui précède montre qu'on sait calculer l'image, le conoyau et le noyau d'un morphisme explicitement présenté de R -modules.

Notons par ailleurs que pour manipuler des *sous-modules* d'un module explicitement présenté, on peut représenter ceux-ci comme l'image d'un morphisme (ou, ce qui revient au même, par un ensemble d'éléments engendrant le sous-module) ou comme le noyau d'un morphisme : on a vu qu'on peut passer d'une représentation à l'autre. Dès lors, il est clair qu'on peut calculer des sommes ou intersections de sous-modules, de tester l'inclusion ou l'égalité entre deux sous-modules (tout se ramène facilement à tester la nullité d'un sous-module, ce qui est facile si on le décrit comme engendré par certains éléments).

(En particulier, on sait tester l'inclusion et l'égalité d'idéaux.)

13.4. Produits tensoriels et Hom de modules ; transporteurs et annulateurs. On continue de noter $R = S/I$ une k -algèbre de type fini où $S = k[Z_1, \dots, Z_d]$.

Si

$$P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P) \quad \text{et} \quad Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$$

sont deux R -modules explicitement présentés, on peut calculer une présentation explicite de $P \otimes_R Q$, à savoir $P \otimes Q = \text{Coker}((G_P \otimes F_Q) \oplus (F_P \otimes G_Q) \rightarrow F_P \otimes F_Q)$ où les produits tensoriels de modules libres sont triviaux à calculer et la flèche est $(\varphi_P \otimes \text{Id}) \oplus (\text{Id} \otimes \varphi_Q)$.

De même, grâce au fait qu'on sait calculer les noyaux, on peut calculer une présentation explicite du module $\text{Hom}_R(P, Q) = \text{Ker}(\text{Hom}_R(F_P, Q) \rightarrow \text{Hom}_R(G_P, Q))$ où $\text{Hom}_R(F_P, Q)$ admet la présentation explicite évidente $\text{Coker}(\text{Hom}_R(F_P, G_Q) \rightarrow \text{Hom}_R(F_P, F_Q))$ et de même pour $\text{Hom}_R(G_P, Q)$, et où la flèche entre eux est

donnée par le morphisme $\text{Hom}_R(F_P, F_Q) \rightarrow \text{Hom}_R(G_P, F_Q)$ de composition à gauche par φ_P .

Si N, N' sont des sous-modules d'un module M explicitement présenté, on peut calculer l'idéal « transporteur » $(N : N') := \{f \in R : fN' \subseteq N\}$ (c'est-à-dire, en calculer des générateurs) : en effet, on peut le voir comme le noyau du morphisme $R \rightarrow \text{Hom}_R(N', M/N)$. De même, si J est un idéal de R et N un sous-module de M , on peut calculer le sous-module $(N : J) := \{x \in M : Jx \subseteq N\}$ de M (car on peut le voir comme noyau de $M \rightarrow \text{Hom}_R(J, M/N)$). (Comparer [Eisenbud 1995, exercice 15.41].)

En particulier, on sait calculer l'idéal annulateur $(0 : M)$ d'un module M explicitement présenté.

13.5. Tor et Ext. On continue de noter $R = S/I$ une k -algèbre de type fini où $S = k[Z_1, \dots, Z_d]$.

Si M est un R -module défini par une présentation explicite $M = \text{Coker}(G \rightarrow F)$, on peut aisément calculer le tronqué à un ordre quelconque d'une résolution libre de M : en effet, il suffit de poser $F_0 = F$ et $F_1 = G$ et récursivement construire le noyau de $F_{i+1} \rightarrow F_i$ comme l'image d'un morphisme $F_{i+2} \rightarrow F_{i+1}$ de modules libres (par l'algorithme de syzygies de 13.1 si on est sur l'algèbre de polynômes S , ou par les techniques générales présentées ci-dessus).

Si F_i est une résolution libre d'un R -module P explicitement présenté, et si Q est un R -module explicitement présenté, en calculant le complexe $F_i \otimes_R Q$, puis l'homologie de celui-ci, on peut calculer $\text{Tor}_i^R(P, Q)$ pour i arbitraire (mais fixé). De même, en calculant la cohomologie du complexe $\text{Hom}_R(F_i, Q)$ on calcule $\text{Ext}_R^i(P, Q)$ pour i arbitraire (mais fixé).

13.6. Présentation d'une algèbre finie comme module. Soit A un anneau quelconque. Une A -algèbre de présentation finie en tant que A -module est, en particulier, de présentation finie en tant que A -algèbre : la proposition facile suivante explicite ce fait (on pourra comparer avec [de Jong 1998, §3], ou [Lombardi et Quitté 2011, exercice IV.15] dans le cas libre) :

Proposition 13.6.1. *Soit A un anneau et B une A -algèbre engendrée comme A -module par les éléments $1, x_1, \dots, x_n$ dont le module des syzygies (c'est-à-dire le sous- A -module N de A^{n+1} formé des $(c_0, \dots, c_n) \in A^{n+1}$ tels que $c_0 + c_1x_1 + \dots + c_nx_n = 0 \in B$) soit de type fini engendré par y_1, \dots, y_m .*

Soit $\Phi: A[T_1, \dots, T_n] \rightarrow B$ le morphisme de A -algèbres envoyant T_i sur x_i et J son noyau (c'est-à-dire l'idéal des relations algébriques entre x_1, \dots, x_n). On considère chaque y_i comme un élément de J en identifiant $(c_0, \dots, c_n) \in A^{n+1}$ au polynôme $c_0 + c_1T_1 + \dots + c_nT_n$ de degré 1. De plus, pour chaque $1 \leq i, j \leq n$, écrivons $x_i x_j = b_0^{(i,j)} + b_1^{(i,j)} x_1 + \dots + b_n^{(i,j)} x_n$ pour certains $b_u^{(i,j)} \in A$, et soit

$q_{i,j} = b_0^{(i,j)} + b_1^{(i,j)}T_1 + \dots + b_n^{(i,j)}T_n - T_iT_j$, polynôme de degré 2 appartenant à J (relation quadratique).

Alors J est engendré, en tant qu'idéal de $A[T_1, \dots, T_n]$, par les y_i et par les $q_{i,j}$.

Démonstration. Soit J' l'idéal de $A[T_1, \dots, T_n]$ engendré par les y_i et par les $q_{i,j}$. Fixons un ordre total quelconque sur les monômes en T_1, \dots, T_n qui raffine l'ordre partiel donné par le degré total (par exemple, l'ordre lexicographique gradué) : il s'agit donc d'un bon ordre sur les monômes. Soit z un élément de J n'appartenant pas à J' et dont le monôme initial (c'est-à-dire, le plus grand monôme intervenant dans z avec un coefficient non nul) soit le plus petit possible. Si z est de degré ≥ 2 , ce monôme initial est divisible par un T_iT_j , disons $z = aT_iT_je + u$ où $a \in A$, où e est un monôme et où u ne fait intervenir que des monômes plus petits que T_iT_je : alors $z' := z + aeq_{i,j}$ est congru à z modulo J' , donc appartient à J mais non à J' , et son monôme initial est strictement plus petit que celui de z , une contradiction. Si z est de degré ≤ 1 , alors z appartient à N donc z est engendré par y_1, \dots, y_m , de nouveau une contradiction. \square

13.6.2. En particulier, si $R = S/I$ est une algèbre de présentation finie sur un corps k et si B est un R -module explicitement présenté, et si on dispose sur B d'une multiplication décrite, par exemple, sous forme de tous les produits $x_i x_j$ pour x_i, x_j parcourant le système de générateurs donné par la présentation de B comme R -module, alors on peut calculer une présentation de B comme R -algèbre, et donc comme k -algèbre.

Ceci s'applique notamment pour montrer que si J est un idéal de R , on peut calculer une présentation de $\text{End}_R(J)$ en tant que R -algèbre ou en tant que k -algèbre.

14. Algèbres de type fini sur un corps : description algorithmique

Comme dans la section précédente, k est ici un corps calculable (nous n'utilisons pas ici l'ensemble des hypothèses 12.7 puisque nous n'aurons jamais affaire à des factorisations de polynômes : la simple calculabilité de k suffit).

14.1. Algèbres de type fini sur k . Une algèbre de type fini sur un corps k sera représentée comme un quotient $A = k[X_1, \dots, X_m]/I$ d'une algèbre de polynômes, c'est-à-dire par la donnée d'un ensemble (fini !) de générateurs de I . Un élément de R sera représenté par un polynôme dans $k[X_1, \dots, X_m]$ qui le relève : on peut ainsi calculer algorithmiquement les sommes et produits dans A , et le fait de pouvoir tester l'appartenance à I permet de tester la nullité, donc l'égalité, d'éléments de A . Remarquons aussi qu'on sait tester l'inversibilité (un $f \in R$ est inversible si et seulement si, pour n'importe quel $\tilde{f} \in k[X_1, \dots, X_m]$ le relevant, l'idéal $I + (\tilde{f})$ obtenu en adjoignant \tilde{f} aux générateurs décrivant I , est égal à l'idéal unité de $k[X_1, \dots, X_m]$, chose qu'on sait tester).

14.2. Morphismes entre algèbres de type fini. Si $A = k[X_1, \dots, X_m]/I$ et $B = k[Y_1, \dots, Y_n]/J$ sont deux algèbres de type fini sur k comme ci-dessus, on représentera un morphisme de k -algèbres $A \rightarrow B$ comme la donnée de m éléments h_1, \dots, h_m de B tels que $f_i(h_1, \dots, h_m) = 0$ pour tout i si f_1, \dots, f_r sont les générateurs choisis pour représenter I (cette condition est évidemment testable algorithmiquement).

Dans ces conditions, on peut aussi présenter B comme A -algèbre de la manière suivante : $B = A[Y_1, \dots, Y_n]/\tilde{J}$, où \tilde{J} est l'idéal $J + (x_i - h_i)$ décrit en adjoignant aux générateurs décrivant J les relations supplémentaires identifiant l'image x_i de X_i dans A avec l'élément h_i de B (ou plus exactement, n'importe quel polynôme dans $k[Y_1, \dots, Y_n]$ le relevant). Et réciproquement, donnée une présentation $B = A[Y_1, \dots, Y_n]/J$ où J est décrit par des générateurs, on peut écrire $B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$ où \hat{J} est l'idéal obtenu en relevant les générateurs décrivant J et en y adjoignant ceux de I ; et le morphisme $A \rightarrow B$ est alors évident. On pourra donc librement choisir entre la représentation d'un morphisme entre k -algèbres de type fini et celle d'une algèbre sur une autre algèbre.

Dans les conditions ci-dessus, on peut tester algorithmiquement si le morphisme $A \rightarrow B$ est *surjectif*. En effet, sur la description où $A = k[X_1, \dots, X_m]/I$ et $B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$, il s'agit de tester, pour chaque Y_i , si Y_i est congru modulo \hat{J} à un élément de $k[X_1, \dots, X_m]$, or ceci peut se faire testant, au moyen d'une base de Gröbner, si chaque Y_i appartient à l'idéal initial (cf. [Eisenbud 1995, §15.2]) de \hat{J} pour un ordre monomial pour lequel Y_i est supérieur à tout monôme en les X_1, \dots, X_m . (En effet, si pour chaque $i \in \{1, \dots, n\}$ il existe $u_i \in k[X_1, \dots, X_m]$ tel que $Y_i - u_i \in \hat{J}$ alors pour un tel ordre monomial le terme initial de $Y_i - u_i$, à savoir Y_i d'après l'hypothèse faite sur l'ordre monomial, appartient à l'idéal initial de \hat{J} ; et réciproquement, si chaque Y_i appartient à l'idéal initial de \hat{J} , disons que $Y_1 < \dots < Y_n$, alors chaque Y_i est congru modulo \hat{J} à un polynôme en $X_1, \dots, X_m, Y_1, \dots, Y_{i-1}$, donc en les X_1, \dots, X_m .)

On peut aussi tester algorithmiquement si le morphisme $A \rightarrow B$ est *injectif* ou même calculer son noyau (un idéal de A , qu'on peut représenter comme l'image d'un idéal de $k[X_1, \dots, X_m]$). En effet, si $A = k[X_1, \dots, X_m]/I$ et $B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$ où $I \subseteq \hat{J}$, le noyau du morphisme $A \rightarrow B$ est (l'image modulo I de) l'intersection $\hat{J} \cap k[X_1, \dots, X_m]$, laquelle se calcule par un algorithme d'élimination (cf. [Eisenbud 1995, §15.10.4]). Ceci permet naturellement de calculer aussi une présentation de l'image $\text{Im } \varphi \simeq A / \text{Ker } \varphi$ d'un morphisme $\varphi: A \rightarrow B$ (il n'y a pas redondance avec le paragraphe précédent, car cette présentation de l'image ne permet pas trivialement de savoir si elle est B tout entier sauf, justement, à utiliser ce qui précède).

Lemme 14.3. *Soit $\varphi: A \rightarrow B$ un morphisme de k -algèbres (où, ici, k est un anneau quelconque). Pour $f \in A$, on note comme d'habitude $A[1/f]$ la k -algèbre*

$A[T]/(Tf - 1)$ localisée de A en inversant f (et $B[1/f] = B \otimes_A A[1/f]$). Alors l'ensemble des $f \in A$ tels que le morphisme $A[1/f] \rightarrow B[1/f]$ déduit de φ soit injectif (resp. soit surjectif, resp. soit un isomorphisme) est un idéal de A .

Démonstration. Soient $N = \text{Ker } \varphi$ et $Q = \text{Coker } \varphi$, vus comme A -modules. La suite exacte $0 \rightarrow N \rightarrow A \rightarrow B \rightarrow Q \rightarrow 0$, tensorisée par le A -module plat $A[1/f]$, donne $0 \rightarrow N[1/f] \rightarrow A[1/f] \rightarrow B[1/f] \rightarrow Q[1/f] \rightarrow 0$: on voit donc que l'ensemble des f tels que $A[1/f] \rightarrow B[1/f]$ soit injective (resp. surjective, resp. bijective) est l'ensemble des f tels que $N[1/f] = 0$ (resp. $Q[1/f] = 0$, resp. $N[1/f] = 0$ et $Q[1/f] = 0$). Or si M est un A -module, dire de $f \in A$ que $M[1/f] = 0$ signifie que chaque élément de M est annulé par une puissance de f (pouvant dépendre de l'élément), c'est-à-dire que f est dans l'intersection des radicaux des annulateurs de tous les éléments $z \in M$ — sous cette forme, il est clair que l'ensemble des f en question est bien un idéal de A . \square

Proposition 14.4. *Dans les conditions du lemme ci-dessus (mais en reprenant pour k un corps calculable), si A et B sont des k -algèbres de type fini décrites par une présentation, alors on peut algorithmiquement calculer les idéaux indiqués par le lemme qui précède, à condition de savoir calculer le radical d'un idéal de A (ce qui sera possible d'après 15.2 au prix des hypothèses 12.7 sur le corps k).*

Démonstration. On note comme précédemment $N = \text{Ker } \varphi$ et $Q = \text{Coker } \varphi$, vus comme, respectivement, un idéal de A et un A -module (qui n'est pas, en général, de type fini). Par ailleurs, on suppose

$$A = k[X_1, \dots, X_m]/I \quad \text{et} \quad B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J},$$

où $I \subseteq \hat{J}$.

On a déjà expliqué qu'on peut calculer l'idéal $\hat{J} \cap k[X_1, \dots, X_m]$ de $k[X_1, \dots, X_m]$ par un algorithme d'élimination : les générateurs ainsi obtenus, lus modulo I , engendrent N , et fournissent donc une description de celui-ci comme idéal de A , ou en particulier, comme A -module de type fini. L'idéal des $f \in A$ tels que $A[1/f] \rightarrow B[1/f]$ soit injectif, soit $N[1/f] = 0$, est le radical de l'annulateur de N , qu'on peut calculer d'après 13.4 et l'hypothèse faite sur la calculabilité du radical.

Pour calculer l'idéal des $f \in A$ tels que $A[1/f] \rightarrow B[1/f]$ soit surjectif, on peut supposer que $A \xrightarrow{\varphi} B$ est injectif (quitte à quotienter par N , qu'on sait calculer, pour remplacer A par l'image de φ), autrement dit que $I = \hat{J} \cap k[X_1, \dots, X_m]$. Nous ferons donc cette hypothèse.

Pour chaque variable Y_i , dont on note y_i l'image dans B , on peut calculer l'idéal formé des $f \in A$ tels qu'il existe $r \geq 0$ pour lequel $f^r y_i \in A$: en effet, il s'agit du radical de l'idéal $(A : y_i)$ des $f \in A$ tels que $f y_i \in A$, et ce dernier est calculable en travaillant dans le sous- A -module de type fini de B engendré par 1 et y_i (dont les relations sont connues : c'est l'intersection de \hat{J} avec $k[X_1, \dots, X_m, Y_i]$). On peut

donc aussi calculer l'intersection de ces n idéaux, c'est-à-dire l'ensemble des $f \in A$ tels que pour chaque i il existe $r \geq 0$ vérifiant $f^r y_i \in A$. Mais il est clair que cet idéal est aussi l'idéal des $f \in A$ tels que pour chaque $h \in B$ il existe $r \geq 0$ vérifiant $f^r h \in A$: c'est bien l'idéal des $f \in A$ tels que $A[1/f] \rightarrow B[1/f]$ soit surjectif. \square

Vu au niveau du morphisme de schémas $\text{Spec } B \rightarrow \text{Spec } A$, l'idéal des f tels que $A[1/f] \rightarrow B[1/f]$ soit injectif définit le plus grand ouvert au-dessus duquel $\text{Spec } B \rightarrow \text{Spec } A$ est schématiquement dominant, tandis que l'idéal des f tels que $A[1/f] \rightarrow B[1/f]$ soit surjectif définit le plus grand ouvert au-dessus duquel $\text{Spec } B \rightarrow \text{Spec } A$ est une immersion fermée.

Nous tirons le lemme suivant de [Petersen 2010] :

Lemme 14.5. *Soit $\varphi: A \rightarrow B$ un morphisme de k -algèbres (où, ici, k est un anneau quelconque) : le morphisme $\text{Spec } B \rightarrow \text{Spec } A$ est une immersion ouverte si et seulement si l'idéal engendré dans B par l'idéal P des $f \in A$ tels que $A[1/f] \rightarrow B[1/f]$ soit un isomorphisme, est l'idéal unité de B . De plus, si c'est le cas, l'image de cette immersion est l'ouvert complémentaire du fermé de $\text{Spec } A$ défini par l'idéal P .*

Démonstration. Si $\text{Spec } B \rightarrow \text{Spec } A$ est une immersion ouverte, son image dans $\text{Spec } A$ est la réunion d'ouverts principaux $D(f_i)$ pour certains $f_i \in A$ (qui *a priori* pourraient ne pas être en nombre fini), pour chacun d'entre eux $A[1/f_i] \rightarrow B[1/f_i]$ est un isomorphisme puisque le morphisme de schémas correspondant en est un, et comme les $D(f_i)$ recouvrent $\text{Spec } B$, les images des f_i dans B engendrent l'idéal unité de B .

Réciproquement, supposons donnés un certain nombre (que cette fois on peut d'emblée supposer fini) de f_i dans A qui engendrent l'idéal unité de B et tels que les $A[1/f_i] \rightarrow B[1/f_i]$ soient des isomorphismes : alors le morphisme $\text{Spec } B \rightarrow \text{Spec } A$ est un isomorphisme au-dessus de chacun des ouverts principaux $D(f_i)$ de $\text{Spec } A$, et leurs images réciproques recouvrent $\text{Spec } B$: il s'agit donc d'un isomorphisme de $\text{Spec } B$ sur l'ouvert réunion des $D(f_i)$ dans A . Cet ouvert est bien le complémentaire du fermé défini par les f_i . \square

En particulier, si A et B sont des k -algèbres de type fini décrites par une présentation, alors on peut algorithmiquement tester si φ définit une immersion ouverte $\text{Spec } B \rightarrow \text{Spec } A$.

14.6. Morphismes finis. Soit

$$A = k[X_1, \dots, X_m]/I \quad \text{et} \quad B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$$

avec $I \subseteq \hat{J}$ (comme en 14.2) la présentation d'un morphisme $A \rightarrow B$ entre k -algèbres de type fini. Alors on peut tester algorithmiquement si ce morphisme est fini (c'est-à-dire si B est un A -module de type fini). En effet, c'est le cas si et

seulement si les images modulo \hat{J} de chacun des Y_i sont entières sur A , ce qui d'une part permet de se ramener au cas où ($n = 1$, c'est-à-dire) $B = k[X_1, \dots, X_m, Y]/\hat{J}$, et d'autre part c'est le cas si et seulement si \hat{J} contient un polynôme dont le monôme initial, pour un ordre monomial pour lequel Y est supérieur à tout monôme en les X_1, \dots, X_m , est une puissance de Y . Autrement dit, sous ces hypothèses, c'est le cas lorsque l'idéal initial de \hat{J} (pour un tel ordre ; c'est-à-dire l'idéal engendré par les monômes initiaux des éléments de \hat{J}) contient une puissance de Y . Or les monômes initiaux de la base de Gröbner de \hat{J} (pour l'ordre considéré) engendrent son idéal initial : il s'agit donc simplement de tester si la base contient un élément dont le monôme initial est une puissance de Y .

Notons qu'on a alors une présentation explicite de B comme un A -module de type fini, dont les générateurs sont les monômes sur les Y_i . Dans le cas où $n = 1$, il suffit d'aller jusqu'à la puissance donnée par le degré de l'équation entière satisfaite par Y , moins 1).

15. Algèbre commutative effective

Dans cette section (en fait, à partir de 15.2) et dans la suite de cette partie, même si elles ne sont pas partout indispensables, nous ferons implicitement les hypothèses 12.7 sur le corps k auquel on a affaire.

15.1. Fonction de Hilbert et dimension. Soit $S = k[Z_1, \dots, Z_d]$ où k est un corps, que nous voyons comme une k -algèbre graduée (par le degré total). Si $M = \text{Coker}(G \rightarrow F)$ est un S -module gradué explicitement présenté (c'est-à-dire que F et G sont des modules libres de type fini gradués, i.e. des sommes directes finies de $S[n_i]$ où $S[n_i]$ désigne l'algèbre S où le degré est décalé de n_i ; et où la flèche $G \rightarrow F$ qui décrit M est homogène de degré 0), alors on sait algorithmiquement calculer la fonction de Hilbert de M (qui à n associe la dimension sur k de l'espace vectoriel des éléments de M homogènes de degré n) : c'est-à-dire que non seulement on sait calculer sa valeur en chaque degré n donné, mais on sait aussi calculer un rang à partir duquel cette fonction est un polynôme, et quel est ce polynôme. (Pour ce fait, nous renvoyons à [Eisenbud 1995, théorème 15.26] et [Cox, Little et O'Shea 2007, chapitre 9, §2–3].)

Dans ce même contexte, on sait calculer une résolution libre graduée *finie* de M (c'est-à-dire de la forme $0 \rightarrow F_r \rightarrow \dots \rightarrow F_2 \rightarrow F_1 \rightarrow F_0 \rightarrow 0$ avec F_i libre de type fini gradué et les flèches homogènes de degré 0) : cf. [Eisenbud 1995, corollaire 15.11]. (Ce calcul ne fait pas appel à des recherches non bornées : notamment, la longueur r de la résolution est majorée par le nombre d de variables.)

Si $S = R/I$ où I est un idéal homogène de R , la fonction de Hilbert d'un S -module gradué M est celle du R -module gradué sous-jacent à M . (En revanche, il n'existe pas en général de résolution libre finie de M comme S -module.)

15.2. Décomposition primaire. Dans cette section, où on se penche sur la calculabilité d'une décomposition primaire d'un idéal I (dans un anneau de polynômes), on entend par ce terme le calcul de couples (M_i, \mathfrak{p}_i) d'idéaux (du même anneau) tels que $I = \bigcap_i M_i$, l'intersection étant irrédundante, avec \mathfrak{p}_i des idéaux premiers deux à deux distincts et M_i (pour chaque i) un idéal \mathfrak{p}_i -primaire. Nous cherchons donc à la fois à calculer les M_i (qui ne sont pas uniques) et les \mathfrak{p}_i (qui le sont). Remarquons en particulier que la décomposition primaire recouvre le calcul du radical d'un idéal (intersection des \mathfrak{p}_i), et permet de tester si un idéal est radical, ou s'il est premier.

15.2.1. Dimension zéro. Soit k un corps (dont, conformément à la convention 12.7, on suppose qu'il est calculable et dispose d'un algorithme de factorisation et une p -base finie explicite). Alors, si I est un idéal de $k[Z_1, \dots, Z_d]$ de dimension 0 (voir la section suivante pour le cas plus général), on peut algorithmiquement calculer le radical, et plus généralement une décomposition primaire, de I : pour cela, on renvoie soit à [Gianni, Trager et Zacharias 1988, §6], ou bien, pour une présentation peut-être plus simple, à [Becker et Weispfenning 1993, théorème 8.22] combiné à [Steel 2005] pour lever les difficultés liées à l'inséparabilité (cette dernière référence se place dans un cas plus restreint, mais il est aisé de voir que ces hypothèses additionnelles ne servent que pour obtenir celle que nous avons faite de factorisation dans les extensions finies).

15.2.2. Dimension arbitraire. Soit k un corps (dont, comme dans le paragraphe précédent, et conformément à la convention 12.7, on suppose qu'il est calculable et dispose d'un algorithme de factorisation et une p -base finie explicite). Alors, si I est un idéal de $k[Z_1, \dots, Z_d]$, on peut algorithmiquement calculer une décomposition primaire de I en ramenant ce problème à celui de la dimension 0 : on renvoie pour cela à [Gianni, Trager et Zacharias 1988, §8 et §9] et [Becker et Weispfenning 1993, théorème 8.101] (cf. aussi [Steel 2005, §5.3]).

(On pourra remarquer au passage que l'algorithme IDEALDIV2 décrit en [Becker et Weispfenning 1993, p. 268], est primitivement récursif.)

15.3. Algèbre de Rees et gradué associé. Soit R une k -algèbre de type fini, disons $R = S/I$ où $S = k[Z_1, \dots, Z_d]$ est un anneau de polynômes, et soit J un idéal de R engendré par des éléments $f_1, \dots, f_r \in R$.

L'algèbre de Rees associée à cette situation est la sous-algèbre $R[Jt] = R \oplus Jt \oplus J^2t^2 \oplus \dots$ de l'algèbre $R[t]$ des polynômes en une indéterminée t sur R formée des polynômes dont le coefficient de degré i appartient à J^i . On peut calculer une présentation de $R[Jt]$ comme R -algèbre, donc aussi comme k -algèbre, de la manière suivante. Soit L l'idéal de $S[T_1, \dots, T_r]$ défini comme l'intersection de ce dernier avec l'idéal de $S[T_1, \dots, T_r, t]$ engendré par I et par les $T_i - f_i t$: alors on sait calculer L par un algorithme d'élimination (cf. [Eisenbud 1995, §15.10.4]).

Or $R[Jt]$ est isomorphe au quotient $S[T_1, \dots, T_r]/L$, l'isomorphisme envoyant $a \in R$ sur la classe modulo L de n'importe quel $\hat{a} \in S$ qui le représente (remarquer que L contient I), et $f_{u_1} \cdots f_{u_i} t^i \in J^i t^i$ sur la classe de $T_{u_1} \cdots T_{u_i}$ modulo L . (Cf. [Vasconcelos 2005, proposition 1.5].)

Le quotient de l'algèbre de Rees $R[Jt]$ par l'idéal J de R définit l'*algèbre graduée associée* à J dans R , soit $\text{gr}_J(R) = (R/J) \oplus (J/J^2)t \oplus (J^2/J^3)t^2 \oplus \cdots$ (les t^i , qui servent simplement à étiqueter les degrés, sont souvent omis de cette description). D'après ce qui précède, on peut aussi en calculer une présentation comme (R/J) -algèbre ou comme k -algèbre, à savoir $S[T_1, \dots, T_r]/(L + (f_1, \dots, f_r))$.

Expliquons comment ceci s'adapte au cas d'un R -module M explicitement présenté (cf. 13.3) pour obtenir une présentation explicite de $M[Jt] = M \oplus JMt \oplus J^2Mt^2 \oplus \cdots$ comme module sur l'algèbre de Rees $R[Jt]$, ainsi donc que du gradué $\text{gr}_J(M) = (M/JM) \oplus (JM/J^2M)t \oplus \cdots$ comme module sur $\text{gr}_J(R)$. À partir d'une présentation $M = S^n/Q$ de M comme S -module (où $Q \subseteq S^n$ contient I^n), on définit encore le $S[T_1, \dots, T_r]$ -module L — tel que $M[Jt]$ soit isomorphe à $S[T_1, \dots, T_r]^n/L$ — comme l'intersection de $S[T_1, \dots, T_r]^n$ avec le sous- $S[T_1, \dots, T_r, t]$ -module de $S[T_1, \dots, T_r, t]^n$ engendré par Q et les produits de $T_i - f_i t$ par les éléments de la base canonique de $S[T_1, \dots, T_r, t]^n$. On peut calculer une présentation de L car la théorie de l'élimination fonctionne encore pour les sous-modules des modules libres de type fini sur les anneaux de polynômes [Eisenbud 1995, remarque suivant la proposition 15.29 et exercice 15.37].

15.4. Calculs de longueurs et de multiplicités. Soit comme dans la section précédente (15.3) R une k -algèbre de type fini, et soit maintenant \mathfrak{p} un idéal *premier* de R . (On rappelle que grâce à 15.2 on sait tester si un idéal de R est premier.) Remarquons que le corps $\kappa_{\mathfrak{p}} := R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}} = \text{Frac}(R/\mathfrak{p})$ est calculable, et on a même les propriétés (12.7) d'admettre un algorithme de factorisation et une p -base finie explicite en vertu de 12.5 et des remarques 12.6. Si M est un R -module explicitement présenté, on a obtenu ci-dessus une présentation explicite de $\text{gr}_{\mathfrak{p}} R$ comme algèbre de type fini sur R/\mathfrak{p} et de $\text{gr}_{\mathfrak{p}} M$ comme module sur $\text{gr}_{\mathfrak{p}} R$: ceci donne donc également une présentation explicite de $\text{gr}_{\mathfrak{p}} R_{\mathfrak{p}}$ comme algèbre de type fini sur $\kappa_{\mathfrak{p}}$ et de $\text{gr}_{\mathfrak{p}} M_{\mathfrak{p}}$ comme module sur cette algèbre de type fini. D'après 15.1, on peut calculer la fonction de Hilbert de $\text{gr}_{\mathfrak{p}} M_{\mathfrak{p}}$, c'est-à-dire la fonction $\dim_{\kappa_{\mathfrak{p}}} \mathfrak{p}^i M_{\mathfrak{p}}/\mathfrak{p}^{i+1} M_{\mathfrak{p}}$ (« calculer » au sens où on peut à la fois calculer le polynôme avec lequel cette fonction coïncide pour i assez grand, et expliciter une borne à partir de laquelle elle coïncide avec lui).

En particulier, on sait calculer la *multiplicité* $\text{mult}_{R_{\mathfrak{p}}}(\mathfrak{p}, M_{\mathfrak{p}})$ de \mathfrak{p} dans $M_{\mathfrak{p}}$ (cf. [Serre 1965, V(A)2] et [Eisenbud 1995, remarque suivant le corollaire 12.5]).

Expliquons comment, dans le cas où \mathfrak{a} est seulement supposé être un idéal \mathfrak{p} -primaire de R (avec \mathfrak{p} un idéal premier), on peut *majorer* la multiplicité $\text{mult}_{R_{\mathfrak{p}}}(\mathfrak{a}, M_{\mathfrak{p}})$

(nous n'aurons pas besoin d'un calcul exact). En calculant la fonction de Hilbert de $\text{gr}_{\mathfrak{p}} R/\mathfrak{a}$, on calcule (sans effectuer de recherche non bornée) un r assez grand pour que $\mathfrak{p}^r \subseteq \mathfrak{a}$, ce qui entraîne $\mathfrak{p}^{ri} M \subseteq \mathfrak{a}^i M$ pour tout i : la longueur sur $R_{\mathfrak{p}}$ de $M_{\mathfrak{p}}/\mathfrak{a}^i M_{\mathfrak{p}}$ est donc majorée par celle de $M_{\mathfrak{p}}/\mathfrak{p}^{ri} M_{\mathfrak{p}}$, or les paragraphes précédents montrent qu'on sait calculer la longueur sur $R_{\mathfrak{p}}$ de $\mathfrak{p}^j M_{\mathfrak{p}}/\mathfrak{p}^{j+1} M_{\mathfrak{p}}$ (qui est la dimension de ce $\kappa_{\mathfrak{p}}$ -espace vectoriel), donc de $M_{\mathfrak{p}}/\mathfrak{p}^j M_{\mathfrak{p}}$.

15.5. Normalisation.

15.5.1. Soient A un anneau noethérien réduit, K son anneau total des fractions et \tilde{A} le normalisé de A dans K . La détermination constructive de \tilde{A} est un problème classique, qui fait l'objet d'une littérature abondante : citons notamment les articles [Stolzenberg 1968], [de Jong 1998], [Singh et Swanson 2009] (en caractéristique positive uniquement) et les livres [Vasconcelos 2005, chapitre 6 ; Huneke et Swanson 2006, chapitre 15]. Pour la commodité du lecteur, nous rappelons ici brièvement un argument (tiré de [de Jong 1998]). Soit I un idéal de A contenant un élément i non diviseur de zéro et posons $A' = \text{End}_A(I)$. Le morphisme évident $A \rightarrow A'$ est entier ; il est injectif, de même que le morphisme $A' \rightarrow K$, $\phi \mapsto \phi(i)i^{-1}$, qui est indépendant du choix de i . Notons que la structure d'anneau de A' est facilement explicitable, d'abord comme A -module puis comme anneau ; cf. 13.4 et 13.6.2 ou bien [de Jong 1998, §3]. Il résulte de ce qui précède que si A est normal, le morphisme $A \rightarrow A'$ est un isomorphisme. On a la réciproque suivante, moyennant des hypothèses supplémentaires.

Proposition 15.5.2 (Grauert–Remmert). *Soient k un corps parfait et*

$$A = k[x_1, \dots, x_n]/(f_1, \dots, f_r)$$

un anneau intègre de normalisé \tilde{A} dans son corps des fractions. Notons I le radical de l'idéal de Fitting $J = \text{Fitt}_d(\Omega_{A/k}^1)$ engendré par l'image dans A des déterminants des sous-matrices jacobiniennes de taille $n - d$. Alors :

- (i) *l'idéal J est non nul et inclus dans l'idéal conducteur $\mathfrak{c} := \text{Ann}_A(\tilde{A}/A)$;*
- (ii) *le morphisme $A \rightarrow \text{End}_A(I)$ est un isomorphisme si et seulement si A est normal.*

Pour (i), voir par exemple [Singh et Swanson 2009, remarque 1.5], où il est implicitement fait usage du théorème de normalisation de Noether « génériquement étale » [Eisenbud 1995, corollaire 16.18 ; Zariski et Samuel 1975, V, §3, théorème 8]. (Voir aussi [Huneke et Swanson 2006, exercice 12.12].) Pour (ii), voir par exemple [Grauert et Remmert 1984, VI, §5],

L'anneau A étant japonais, la suite croissante $A \subseteq A' \subseteq A'' \subseteq \dots$ obtenue en itérant la construction $A \mapsto \text{End}_I(A)$, pour $I = \sqrt{\text{Fitt}(\Omega_{A/k}^1)}$, est stationnaire. D'après (ii), sa limite est le normalisé \tilde{A} que l'on souhaite calculer.

15.5.3. La méthode précédente ne dit rien sur le nombre d'opérations à faire : on s'arrête simplement lorsque le morphisme d'inclusion d'un terme dans le suivant est un isomorphisme, condition que l'on sait tester (14.2). L'existence de bornes *a priori*, mais non calculables, est connue [van den Dries et Schmidt 1984, §3] mais inutile ici. On se propose ici de montrer que l'on peut contrôler cette terminaison par un calcul de multiplicité et ainsi calculer la normalisation sans faire de recherche non bornée.

Rappelons [Serre 1965, IV, théorème 11] qu'un anneau est normal si et seulement si il est R_1 , c'est-à-dire régulier en codimension 1, et satisfait la condition S_2 de Serre [ÉGA IV₂ 1965, 5.7.2].

La condition S_2 est facile à satisfaire : si P est une sous- k -algèbre de polynômes de A telle que $P \rightarrow A$ soit fini, et que l'on note $D(-) = \text{Hom}_P(-, P)$, le bidual $B = D(D(A))$ est S_2 et est la S_2 -ification de A , c'est-à-dire que $A \rightarrow B$ est la plus petite extension finie contenue dans l'anneau total des fractions de A qui soit S_2 . Voir [Vasconcelos 2005, proposition 6.21 ; Huneke et Swanson 2006, démonstration du théorème 15.3.3 et exercices 15.9 et 15.12]. (La multiplication sur B utilisée ici provient de son plongement dans le corps des fractions de A ; mais elle peut aussi se définir de façon intrinsèque : si $\xi, \eta \in D(D(A))$ sont vues comme des formes P -linéaires sur $D(A)$, leur produit est la forme P -linéaire sur $D(A)$ qui à $\varphi \in D(A)$ associe $\eta(x \mapsto \xi(y \mapsto \varphi(xy)))$ — cette multiplication du bidual, appelée « multiplication d'Arens » par les analystes dans le contexte des algèbres de Banach, cf. [Palmer 1974], n'est pas commutative en général, mais il est facile de se convaincre qu'elle l'est, et qu'elle coïncide bien avec la restriction de la multiplication sur $\text{Frac}(A)$, dans le cas où on s'est placé, cf. [Madore 2014].) Voir aussi [ÉGA IV₂ 1965, §5.10] et [Achar et Sage 2009] pour une présentation intrinsèque de S_2 -ification. Or P est calculable en utilisant une démonstration explicite du lemme de normalisation de Noether ([Eisenbud 1995, théorème 13.3 en utilisant le lemme 13.2(a)] ou [Serre 1965, III(D)2, théorème 2]), on sait décrire explicitement A comme un P -module de type fini d'après la remarque faite en 14.6, on peut en déduire la structure de B comme P -module d'après 13.4, et bien sûr comme algèbre (13.6.1, puisque la multiplication sur $D(D(A))$ est calculable).

D'autre part, si A est R_1 , il en est de même de B (en fait, $A \rightarrow DD(A)$ est un isomorphisme en codimension 1 ; cf. [Huneke et Swanson 2006, exercice 15.11]).

Ceci nous ramène donc à normaliser (= régulariser) en codimension 1. D'après la proposition précédente (i), on peut trouver un élément non nul f dans le conducteur \mathfrak{c} . Notons $\mathfrak{p} \in \text{Spec}(A)$ un point maximal (de codimension 1) de $V(f)$, calculé par décomposition primaire de f . Soit B le localisé de A en \mathfrak{p} et notons \tilde{B} le normalisé de B . La longueur de toute chaîne strictement croissante $B \subsetneq B' \subsetneq \dots \subsetneq \tilde{B}$ est majorée par l'entier $\text{long}_B(\tilde{B}/B)$ lui-même inférieur ou égal à $\text{long}_B(\tilde{B}/\mathfrak{c})$. Rappelons que ce dernier est égal à la multiplicité $\text{mult}(\mathfrak{c}, B)$ de \mathfrak{c} dans B , à son tour inférieur ou égal à $\text{mult}((f), B)$, que l'on sait majorer (cf. 15.4). Ceci montre

que l'on a peut calculer une borne sur le nombre d'étapes pour rendre A régulier en codimension 1. ¹⁸

Justifions brièvement l'égalité $\text{long}_B(\tilde{B}/c) = \text{mult}(c, B)$. Soit $n \geq 1$ un entier ; on a $\text{long}_B(\tilde{B}/c^n) = \sum_q [\kappa(q) : \kappa(p)] \cdot \text{long}_{\tilde{B}_q}(\tilde{B}_q/c^n)$, où q parcourt le spectre maximal (fini) de l'anneau de Dedekind semi-local \tilde{B} . Par régularité des anneaux \tilde{B}_q et nouvelle application de cette formule (pour $n = 1$), on obtient l'égalité $\text{long}_B(\tilde{B}/c^n) = n \cdot \text{long}_B(\tilde{B}/c)$ d'où $\text{mult}(c, \tilde{B}) = \text{long}_B(\tilde{B}/c)$. Comme d'autre part $\text{long}_B(\tilde{B}/B)$ est finie, on a $\text{mult}(c, \tilde{B}) = \text{mult}(c, B)$.

15.6. Lissité et étalitude. Soient A un anneau, $P = A[X_1, \dots, X_n]$ un anneau de polynômes sur A et B le quotient de P par un idéal de type fini I . Considérons le B -module $\text{Ext}_B^1(\mathbb{L}_{B/A}, I/I^2)$, où $\mathbb{L}_{B/A}$ est le complexe cotangent. D'après [Illusie 1971, III.1.2.9.1], ce module est naturellement isomorphe au quotient $\text{End}_B(I/I^2)/d^* \text{Hom}_P(\Omega_{P/A}^1, I/I^2)$, où d désigne la dérivation $I/I^2 \rightarrow \Omega_{P/A}^1 \otimes_P B$. On peut donc en déterminer la structure (cf. 13.4). Notons $H_A(P, I)$ son idéal annulateur en tant que P -module ; d'après une variante du critère jacobien [Gabber et Ramero 2003, 5.4.2], le lieu lisse (à la source) du morphisme $\text{Spec}(B) \rightarrow \text{Spec}(A)$ est l'ouvert complémentaire du fermé Σ défini par l'idéal image de $H_A(P, I)$ dans B . (Un avantage de cette description est que, contrairement à la description plus classique du lieu singulier par un idéal de Fitting du B -module $\Omega_{B/A}^1$ (cf. 15.5), elle ne fait pas d'hypothèse d'équidimensionalité ou de platitude.) On trouve en [Gabber et Ramero 2003, §5.4.5] et [Elkik 1973, §0.2] une variante moins intrinsèque mais plus explicite qui, donnés des générateurs $\{f_1, \dots, f_r\}$ de I , produit — par dérivation de ces générateurs et opérations élémentaires sur les idéaux de P (cf. 13.2 et 13.3) — un idéal contenu dans $H_A(P, I)$ et définissant également le fermé Σ .

Il résulte de ce qui précède que l'on peut tester si le morphisme de présentation finie $\text{Spec}(B) \rightarrow \text{Spec}(A)$ est *lisse*, par exemple lorsque A est une algèbre de type fini sur un corps. Pour vérifier s'il est *étale*, il suffit de vérifier si les fibres au-dessus des points maximaux de $\text{Spec}(A)$ (c'est-à-dire les points génériques des composantes irréductibles, calculables d'après 15.2) sont vides ou de dimension nulle.

15.7. Présentation d'un pincement.

Définition 15.7.1. Soit A un anneau et I un idéal de A . On définit une A -algèbre B en munissant le A -module $A \oplus I$ de la multiplication donnée par $(a, u) \cdot (b, v) = (ab, av + bu + uv)$. On dit que B est la A -algèbre obtenue par *pincement de A le long de I* .

Remarquons que B peut aussi se voir comme la A -algèbre $A \times_{A/I} A$ — en identifiant le couple (a, u) de $A \oplus I$ à $(a, a + u)$ de $A \times_{A/I} A$ — ou comme la

18. Cette technique nous a été suggérée par O. Gabber.

A -algèbre obtenue en ajoutant une unité à l'idéal I vu comme une A -algèbre-non-unitaire.

Proposition 15.7.2. *Soient k un corps, $A = k[t_1, \dots, t_d]/(u_1, \dots, u_q)$ une k -algèbre de type fini explicitement présentée et I l'idéal de A engendré par des éléments x_1, \dots, x_r de A , images d'éléments $\hat{x}_1, \dots, \hat{x}_r$ de $k[t_1, \dots, t_d]$. Alors on peut trouver algorithmiquement une présentation explicite de l'algèbre $B = A \oplus I$ obtenue par pincement de A le long de I (cf. 15.7.1).*

Démonstration. Le A -module B est engendré par $1, x_1, \dots, x_r$. D'après 13.3, on sait trouver algorithmiquement des générateurs y_1, \dots, y_s des relations linéaires entre les x_1, \dots, x_r (donc entre les $1, x_1, \dots, x_r$). Quitte à écrire chaque $x_i x_j$ comme combinaison de x_1, \dots, x_r , on trouve également des relations quadratiques $q_{i,j}$ telles que définies en 13.6.1, qui assure alors que les relations y_i et les $q_{i,j}$ définissent l'algèbre B comme un quotient de $A[t'_1, \dots, t'_r]$, donc, quitte à prendre leur relèvement et y ajouter les u_1, \dots, u_q , comme un quotient de $k[t_1, \dots, t_d, t'_1, \dots, t'_r]$. \square

16. Schémas de type fini sur un corps : description algorithmique

On rappelle que les hypothèses 12.7 sont implicitement faites sur le corps k . Par ailleurs, nous ne parlerons ici que de schémas de type fini sur k , omettant fréquemment les mots « de type fini ».

16.1. Schémas affines et quasi-affines, morphismes entre iceux. On représentera un schéma affine (sous-entendu : de type fini) X sur un corps k par une algèbre de type fini R dont il est le spectre, cette algèbre R étant elle-même représentée comme un quotient $k[Z_1, \dots, Z_d]/I$ d'une algèbre de polynômes, c'est-à-dire par la donnée d'un ensemble (fini !) de générateurs de I , équations de X dans l'espace affine \mathbb{A}_k^d . Remarquons qu'on peut tester algorithmiquement si un tel schéma est vide (il s'agit exactement de tester si I est l'idéal unité).

On représentera un morphisme $X \rightarrow Y$ de k -schémas affines, où $X = \text{Spec}(R)$ et $Y = \text{Spec}(S)$ sont les spectres de deux k -algèbres de type fini R, S , comme un morphisme $S \rightarrow R$ de k -algèbres (cf. 14.2).

On représentera un schéma quasi-affine, c'est-à-dire un ouvert U d'un schéma affine X , au moyen d'un fermé dont il est le complémentaire (décrit par des équations f_i de ce fermé : ceci revient à écrire U comme la réunion des ouverts principaux $D(f_i)$). Remarquons que, à l'intérieur d'un schéma affine X fixé, on sait tester l'inclusion ou l'égalité entre des ouverts (cela revient à tester l'inclusion entre les radicaux des idéaux définissant les fermés : cf. 15.2 pour le calcul du radical).

Un morphisme d'un schéma affine X vers un schéma quasi-affine V ouvert complémentaire de Z dans un schéma affine Y sera décrit comme un morphisme $X \rightarrow Y$ qui se factorise par V : ce fait est testable algorithmiquement en testant

si l'image réciproque de Z par $X \rightarrow Y$ est vide (c'est-à-dire si l'algèbre produit tensoriel de celles de X et Z au-dessus de celle de Y est nulle).

Un morphisme d'un schéma quasi-affine U ouvert d'un schéma affine X , vers un schéma quasi-affine V , sera décrit comme une collection de morphismes $U_i \rightarrow V$ qui coïncident sur $U_i \cap U_j$, où les U_i sont les ouverts affines principaux recouvrant U (c'est-à-dire les $D(f_i)$ avec f_i parcourant des équations d'un fermé dont U est le complémentaire dans X : on sait écrire des équations de $D(f_i)$ comme schéma affine en le considérant comme une hypersurface d'équation $Tf_i - 1$ au-dessus de X , où T est une nouvelle indéterminée ; et on peut représenter l'ouvert affine $U_i \cap U_j$ comme $D(f_i f_j)$). De nouveau, on peut calculer la composée de tels morphismes entre schémas quasi-affines, et tester l'égalité de deux d'entre eux (même si le quasi-affine U de départ n'est pas représenté par le même recouvrement par des $D(f_i)$: il suffit de prendre un raffinement commun entre deux recouvrements, ce qui est facile).

16.2. Description des schémas et de leurs morphismes. On représentera un schéma (sous-entendu : de type fini) X sur un corps k par la donnée d'un nombre fini de schémas affines U_i et, pour chacun, d'un recouvrement $V_{i'}$ par des ouverts quasi-affines (les variables i et i' parcourent ici le même ensemble fini) et, pour chaque paire i, i' , d'un morphisme $\varphi_{i' i} : V_{i'} \rightarrow V_i$ vérifiant la condition de compatibilité que ($V_{ii} = U_i$ et $\varphi_{ii} = \text{Id}_{U_i}$ et que) $\varphi_{i_2 i_3} \circ \varphi_{i_1 i_2}$ et $\varphi_{i_1 i_2}$ coïncident là où tous deux sont définis (en particulier, les $\varphi_{i' i}$ sont des isomorphismes). Toutes ces conditions sont bien testables algorithmiquement, et le schéma X défini est alors le recollement des U_i en identifiant l'ouvert $V_{i'}$ de U_i avec l'ouvert $V_{i'}$ de $U_{i'}$ au moyen de $\varphi_{i' i}$. On dit aussi que les U_i (avec les autres données les accompagnant) constituent un atlas affine de X . Un raffinement d'un tel atlas est un atlas obtenu en remplaçant chaque U_i par un recouvrement de celui-ci par des ouverts affines principaux U_{ij} (ici le j parcourt un ensemble fini qui peut dépendre de i), avec les données évidemment déduites de ce recouvrement.

On représentera un morphisme de schémas $X \rightarrow Y$, décrits par des atlas U_i pour X et V_j pour Y , en se donnant un raffinement U_{ij} de l'atlas initial de X et des morphismes $U_{ij} \rightarrow V_j$ de schémas affines, qui se recollent aux intersections décrites par l'atlas.

Notons qu'on peut algorithmiquement calculer la composée de morphismes de schémas ainsi décrits, et par ailleurs que, donnés deux morphismes $X \rightarrow Y$ entre les deux mêmes schémas décrits par les mêmes atlas, on peut tester leur égalité (ceci se fait en prenant un raffinement commun aux deux atlas de X qui décrivent les morphismes à comparer, ce qu'on peut faire puisqu'il s'agit de raffiner des recouvrements de mêmes schémas affines U_i).

Remarquons aussi que si dans la définition d'un schéma on ne suppose plus les U_i affines mais que ce sont des schémas plus généraux (autrement dit, si on cherche

à recoller un atlas formé de schémas non nécessairement affines), on peut encore se ramener algorithmiquement à la situation où ils sont affines (quitte à remplacer chaque schéma U_i par un atlas affine qui le décrit).

Nous ne prétendons pas qu'il soit possible de tester l'égalité (l'isomorphisme) de deux schémas décrits par des atlas (ceci sera néanmoins possible dans le cas étale : cf. 17.3 ci-dessous). Remarquons à ce sujet que dans la suite si nous écrivons par exemple « si Z est affine » il faut comprendre « si on s'est donné une description de Z comme schéma affine » et pas « si on s'est donné une description de Z comme un schéma général, et qu'il s'avère que Z est affine [chose qu'on ne sait pas tester] » : ceci ne devrait pas prêter à confusion.

En fait, à ce stade de la description, nous ne savons même pas encore tester si un morphisme *donné* entre schémas est un isomorphisme (ceci, en revanche, sera bien décidable : cf. 16.5).

16.3. Produits fibrés de schémas. Donnés X, Y, Z trois schémas (i.e., k -schémas de type fini) décrits comme précédemment, et donnés $X \rightarrow Z$ et $Y \rightarrow Z$ deux morphismes, on peut algorithmiquement calculer le produit fibré $X \times_Z Y$. En effet, si X, Y, Z sont affines (disons $X = \text{Spec } R, Y = \text{Spec } S$ et $Z = \text{Spec } A$), il s'agit de calculer un produit tensoriel de k -algèbres de type fini, or on a vu en 14.2 qu'on pouvait calculer des présentations finies de R et S comme A -algèbres, auquel cas leur produit tensoriel se calcule simplement en réunissant les générateurs et les relations. La démonstration dans le cas général suit celle de [ÉGAI 1960, 3.2.6] : si Z est toujours supposé affine mais que X, Y ne le sont plus, on obtient un atlas de $X \times_Z Y$ comme en [ÉGAI 1960, 3.2.6.3], en prenant les $U_i \times_Z V_j$ pour U_i parcourant un atlas de X et V_j de Y ; si Z n'est plus supposé affine, étant donné un atlas W_i de Z , la donnée même des morphismes $X \rightarrow Z$ et $Y \rightarrow Z$ fournit des atlas de X et Y appropriés à les représenter, c'est-à-dire par des $U_i \rightarrow W_i$ où U_i est un ouvert de X (non nécessairement affine, mais réunion d'ouverts affines) et $V_i \rightarrow W_i$ de même, on peut donc calculer les produits fibrés $U_i \times_{W_i} V_i$ comme on vient de le dire, et les recoller à leur tour.

Dans le cas où $X = Y$, en recollant les morphismes $R \otimes_A R \rightarrow R$ (de multiplication, qui ne posent pas de difficulté à décrire algorithmiquement), on obtient une description de la diagonale $X \rightarrow X \times_Z X$ d'un morphisme $X \rightarrow Z$ quelconque.

16.4. Pincement (cas non nécessairement affine). On renvoie à [Ferrand 2003] pour la question générale de l'existence des pincements dans la catégorie des schémas, dont on tire notamment (théorème 7.1(B)) le fait que la somme amalgamée (= « pincement ») $X \amalg_F X$ est représentable dans la catégorie des schémas lorsque X est un schéma et F un sous-schéma fermé de X , et plus exactement, représentée par la même somme amalgamée dans la catégorie des espaces annelés.

On a vu en 15.7.2 comment calculer algorithmiquement ce pincement si X est un schéma affine de type fini sur un corps k (si $X = \text{Spec } A$ et $F = \text{Spec}(A/I)$ avec I un idéal de A , alors $X \amalg_F X = \text{Spec}(A \oplus I)$ où $A \oplus I$ est muni de la structure d'algèbre décrite en 15.7.1). Remarquons par ailleurs que la construction est fonctorielle : si $\varphi : A \rightarrow A'$ est un morphisme d'algèbres et $I' = \varphi(I)$ l'idéal engendré dans A' par l'image de l'idéal I de A , alors $(A \oplus I) \rightarrow (A' \oplus I')$ défini par $(a, u) \mapsto (\varphi(a), \varphi(u))$ est bien un morphisme d'algèbres.

Si X est un schéma de type fini sur k et U un ouvert affine de X , alors d'après [Ferrand 2003, lemme 4.4] $U \amalg_V U$ est un ouvert de $X \amalg_F X$, où V désigne l'ouvert $F \cap U$ de $F : \text{ces ouverts sont calculables algorithmiquement d'après ce qu'on vient de dire (il est clair que } F \cap U \text{ est calculable, au besoin d'après 16.3), ils recouvrent } X \amalg_F X, \text{ et si } U, U' \text{ sont deux ouverts affines de } X, \text{ l'ouvert quasi-affine } (U \amalg_V U) \cap (U' \amalg_{V'} U') = (U \cap U') \amalg_{V \cap V'} (U \cap U') \text{ se décrit comme réunion des } U'' \amalg_{V''} U'' \text{ pour } U'' \subseteq U \cap U' \text{ et s'envoie vers } U \amalg_V U \text{ et } U' \amalg_{V'} U' \text{ par les morphismes de functorialité (cf. ci-dessus). Ceci fournit donc une description de } X \amalg_F X \text{ au sens de 16.2.}$

16.5. Immersions ouvertes et isomorphismes de schémas. Donn e un schéma X décrit par un atlas d'ouverts affines $U_i = \text{Spec } R_i$ (dont on notera $V_{ij} = U_i \cap U_j$ les intersections deux à deux que l'atlas identifie) et un schéma Y que nous supposons dans un premier temps affine $Y = \text{Spec } S$, on peut tester algorithmiquement si un morphisme $X \rightarrow Y$ est une immersion ouverte : en effet, pour ceci, il faut et il suffit que chacun des $U_i \rightarrow Y$ soient des immersions ouvertes, et que l'intersection (dans Y) des images de U_i et U_j coïncide avec V_{ij} en tant qu'ouvert de U_i ; or d'après 14.5 on sait tester si $U_i \rightarrow Y$ est une immersion ouverte, on peut calculer $U_i \cap U_j$ dans Y comme $\text{Spec}(R_i \otimes_S R_j)$, et tester si l'ouvert en question de $U_i = \text{Spec } R_i$ coïncide bien avec V_{ij} .

Le cas où le schéma Y cible n'est plus supposé affine ne pose pas de difficulté : le morphisme est décrit dans des atlas adaptés, et il est une immersion ouverte si et seulement si sa restriction à chaque carte de la cible est une immersion ouverte.

On peut également tester algorithmiquement si un morphisme $X \rightarrow Y$ de schémas est un isomorphisme et, le cas échéant, calculer sa réciproque. En effet, en considérant d'abord le cas où Y est affine, ceci se fait en testant d'abord s'il s'agit d'une immersion ouverte comme décrit par le pénultième paragraphe dont nous reprenons les notations, puis, si c'est bien le cas, en vérifiant que les U_i recouvrent Y , ce qui se fait en calculant (toujours par 14.5) un fermé complémentaire de U_i dans Y , ce qui permet de tester si l'intersection de ces fermés est vide (les équations qui les décrivent engendrent l'idéal unité de S) ; le cas échéant, les ouverts principaux dont les U_i sont écrits comme réunion forment un atlas de Y pour lequel l'écriture de l'isomorphisme réciproque est claire. Le cas où Y n'est pas affine ne présente pas

de difficulté nouvelle (il s'agit, de nouveau, d'être un isomorphisme en restriction à chaque carte de la cible).

16.6. Réduit, composantes irréductibles, composantes connexes. On peut tester algorithmiquement si un schéma est réduit, ou bien calculer son réduit : en effet, X est réduit si et seulement si chacun des ouverts affines constituant un atlas de X l'est, ce qui ramène à tester si une k -algèbre de type fini est réduite, donc si un idéal d'un anneau de polynômes est radical (cf. 15.2) ; et réduire X se fait en réduisant chaque carte d'un atlas de X (les morphismes de recollement passent au réduit grâce à la fonctorialité de celui-ci).

De même, on peut tester algorithmiquement si un schéma est irréductible, ou bien calculer ses composantes irréductibles.

Enfin, en testant parmi les composantes irréductibles celles dont l'intersection est vide (on a déjà observé ci-dessus qu'on pouvait tester si un schéma est vide), on peut calculer algorithmiquement les composantes connexes d'un schéma.

16.7. Image fermée, immersions fermées. Si $X \rightarrow Y$ est un morphisme de schémas, on peut en calculer algorithmiquement l'image fermée schématique (c'est-à-dire, [ÉGA I 1960, 9.5], le plus petit sous-schéma fermé Y' de Y par lequel le morphisme $X \rightarrow Y$ se factorise, et bien sûr on cherche aussi à calculer la factorisation en question) : en effet, si on suppose d'abord que $Y = \text{Spec } S$ est affine, et si X est décrit par un atlas d'ouverts affines $U_i = \text{Spec } R_i$, alors $Y' = \text{Spec}(S/N)$ où N est l'intersection des noyaux de tous les $S \rightarrow R_i$ décrivant le morphisme (cf. [ÉGA I 1960, 9.5.2]). Si Y n'est plus supposé affine, de nouveau, il suffit d'effectuer cette construction localement.

Grâce à cette construction, on peut tester si un morphisme de schémas $X \rightarrow Y$ est une immersion fermée : en effet, cela revient à tester si la factorisation $X \rightarrow Y'$, où Y' est l'image fermée schématique décrite ci-dessus, est un isomorphisme, et on a vu comment tester ce fait.

On peut également tester si un morphisme de schémas est dominant (c'est-à-dire d'image dense), puisque cela signifie précisément que son réduit est schématiquement dominant (c'est-à-dire que son image fermée schématique, définie ci-dessus, est toute la cible).

16.8. Image d'un morphisme, surjectivité. Si $X \rightarrow Y$ est un morphisme de schémas, on peut tester algorithmiquement s'il est surjectif, ou même calculer son image (une partie constructible de Y , décrite comme combinaison booléenne de fermés de Y). En effet, cette image est caractérisée par l'ensemble de ses points à valeurs dans la clôture algébrique de k (on rappelle que nous ne considérons ici que des schémas de type fini sur k ; cf. [ÉGA I 1971, proposition 7.1.8 et sa démonstration]), or pour k algébriquement clos il est algorithmique de calculer l'image d'une partie

constructible de k^n par la projection sur un sous-ensemble de ses coordonnées [Fried et Jarden 2008, théorème 9.3.1], ce qui suffit à calculer l'image de $X(k)$ par f comme la projection du graphe de f .

16.9. Morphismes et schémas séparés, radiciels. On peut tester si un morphisme de schémas est séparé, resp. radiciel, en testant si sa diagonale (qu'on sait calculer d'après 16.3) est une immersion fermée [ÉGA I 1960, 5.4.1], resp. une surjection [ÉGA IV₁ 1964, 1.8.7.1], ce qu'on sait tester d'après 16.7, resp. 16.8.

16.10. Détection de points. Expliquons brièvement pourquoi, donné un schéma X non vide sur k , on peut algorithmiquement en expliciter un point géométrique, c'est-à-dire un point sur « la » clôture algébrique de k . Comme il suffit de trouver un point d'un ouvert affine de X , on peut évidemment supposer que X est affine. Le cas où X est un fermé de la droite affine \mathbb{A}_k^1 est trivial (s'il est décrit comme l'ensemble $\{f = 0\}$ des zéros d'un polynôme f , on considère une racine de f dans la clôture algébrique de k), et le cas où X est un ouvert de \mathbb{A}_k^1 ne l'est pas moins (si l'ouvert en question est d'écrit comme $\{f \neq 0\}$, on peut considérer le fermé $\{f = 1\}$ qui y est contenu, se ramenant ainsi au cas précédent). Dans le cas général, on procède par récurrence sur la dimension de l'espace affine dans lequel X est inclus : si π est la projection sur une coordonnée, alors $\pi(X)$ est calculable d'après 16.8, on peut trouver un point géométrique de $\pi(X) \subseteq \mathbb{A}_k^1$ d'après ce qui vient d'être dit, et on est ramené au même problème dans la fibre de π au-dessus de ce point.

16.11. Passage à la limite. Soient k_0 un corps, X_0 un k_0 -schéma séparé de type fini et k/k_0 une extension algébrique (non nécessairement finie). On note X le produit fibré $X_0 \times_{k_0} k$ et on suppose donné un morphisme de type fini $f : T \rightarrow X$. Alors, on peut construire une extension finie k_1/k_0 et un morphisme $f_1 : T_1 \rightarrow X_1 = X_0 \times_{k_0} k_1$ induisant le morphisme f par changement de base : il suffit de considérer le sous-corps de k engendré des coefficients définissant f . Si f est étale, on peut supposer qu'il en est de même de k_1/k_0 (par invariance topologique du site étale).

17. Géométrie algébrique effective

On rappelle que les hypothèses 12.7 sont implicitement faites sur le corps k , et que les schémas sur k sont supposés de type fini.

17.1. Dimension. Grâce au calcul de la fonction de Hilbert (cf. 15.1), il est possible de calculer la dimension d'un schéma (cf. [Cox, Little et O'Shea 2007, §9.3]), ou la dimension de ses composantes connexes et irréductibles.

17.2. Lissité et étalitude. Les propriétés d'être lisse ou étale étant locales, le fait de pouvoir tester cette propriété sur un morphisme d'algèbres (15.6) permet de tester si un morphisme de schémas est lisse, resp. étale.

17.3. Sections et isomorphismes de morphismes étales. On peut décider algorithmiquement si un morphisme étale séparé $X \rightarrow S$ admet une section. En effet, d'après [ÉGA IV₄ 1967, 17.4.9] (ou bien [Milne 1980, corollaire I.3.12]), c'est le cas si et seulement si sa restriction à une réunion de composantes connexes de X est un isomorphisme.

Par conséquent, on peut aussi décider si deux morphismes étales finis $X \rightarrow S$ et $Y \rightarrow S$ sont S -isomorphes. Pour s'en convaincre, constatons d'abord qu'on peut calculer le morphisme $\underline{\text{Isom}}_S(X, Y) \rightarrow S$ où $\underline{\text{Isom}}$ est le schéma paramétrant les S -isomorphismes $X \rightarrow Y$: ses équations s'écrivent explicitement en fonction de celles de X et Y . Plus exactement, on peut décrire $\underline{\text{Isom}}_S(X, Y)$ comme le fermé des $(u, v) \in \underline{\text{Hom}}_S(X, Y) \times_S \underline{\text{Hom}}_S(Y, X)$ défini par les équations $v \circ u = \text{Id}_X$ et $u \circ v = \text{Id}_Y$, où $\underline{\text{Hom}}_S(X, Y)$ (aussi noté $\mathfrak{R}_{X/S}(Y \times_S X)$, où \mathfrak{R} désigne la restriction à la Weil) est le schéma paramétrant les morphismes $X \rightarrow Y$: voir [Bosch, Lütkebohmert et Raynaud 1990, §7.6, notamment théorème 4], dont la démonstration fournit une description explicite de ce schéma (cf. aussi [Debarre 2001, chapitre 2]). Comme $\underline{\text{Isom}}_S(X, Y) \rightarrow S$ est lui-même étale fini quand X et Y le sont, et que savoir si X et Y sont isomorphes sur S revient à savoir s'il a une section, ce qui nous ramène à la question précédente.

17.4. Proj. Soient r un entier, k un corps et S l'algèbre graduée de polynômes $k[x_0, \dots, x_r]$, où les variables x_i sont de degré 1. On va montrer que pour chaque un S -module gradué de type fini M , on peut calculer le k -module de type fini $H^0(\mathbb{P}_k^r, \mathcal{M})$, où \mathcal{M} désigne le faisceau quasi-cohérent naturellement associé à M [ÉGA II 1961, 2.5]. Rappelons [Serre 1955, chapitre III, §4, ¶ 69, corollaire 2], que l'on a $H^0(\mathbb{P}_k^r, \mathcal{M}) = \text{colim}_v \text{Hom}_S((x_0^v, \dots, x_r^v), M)_0$. (L'indice 0 indique que l'on ne considère que les morphismes de degré nul.) Étant donné une résolution libre (de type fini) L_\bullet de M — que l'on peut déduire d'une présentation de M comme conoyau d'un morphisme $L_1 \rightarrow L_0$ entre S -modules gradués libres de type fini —, il résulte de [Serre 1955, chapitre III, §3, ¶ 63, proposition 3(a)] que l'on a égalité $H^0(\mathbb{P}_k^r, \mathcal{M}) = \text{Hom}_S((x_0^v, \dots, x_r^v), M)_0$ dès que $v+r$ est supérieur à chaque entier n tel que $S(-n)$ apparaisse comme facteur direct des L_i . Rappelons qu'un S -module gradué libre est somme directe de modules $S(n)$, où $n \in \mathbb{Z}$ et $S(n)$ est le S -module S muni de la graduation $S(n)_i = S_{n+i}$. (Un tel v est aussi lié à la « régularité », au sens de Mumford–Castelnuovo, de M , cf. [Bayer et Mumford 1993, définition 3.2].)

Pour le calcul d'une résolution libre, cf. 15.1.

17.5. Application. Soient k un corps et $X = V(I) \subseteq \mathbb{P}_k^r$ un schéma projectif. Il résulte de ce qui précède (et des résultats de la section 13) que l'on peut calculer $H^0(X, \mathbb{C}_X) = H^0(\mathbb{P}_k^r, \mathbb{C}_{\mathbb{P}_k^r}/I)$. En particulier, on peut vérifier si la flèche naturelle $k \rightarrow H^0(X, \mathbb{C}_X)$ est un isomorphisme : ceci fournit une approche alternative à 16.6 pour le calcul des composantes connexes géométriques d'une variété projective.

La même approche, en remplaçant k par une k -algèbre A de type fini (qu'on peut supposer être une algèbre de polynômes) permettrait de calculer la factorisation de Stein d'un morphisme projectif $f : Y \rightarrow \text{Spec } A$ en calculant la A -algèbre $f_*\mathcal{O}_Y$: on pourrait en déduire la même chose pour $f : Y \rightarrow X$ sur une base non nécessairement affine.

Remerciements

Nous remercions chaleureusement Ofer Gabber auquel nous sommes redevables de plusieurs arguments importants et pour ses suggestions particulièrement utiles. À divers titres nous remercions également Pierre Deligne, Luc Illusie, Jean Lannes, Grégoire Lecerf, Henri Lombardi, Ronald van Luijk, Jean-Pierre Serre, Lenny Taelman, et Olivier Wittenberg. Le second auteur sait également gré à Ahmed Abbes et Weizhe Zheng (郑维喆) de leurs invitations, respectivement à l'IHÉS et au centre Morningside (晨兴数学中心).

Bibliographie

- [Abbes et Gros 2011] A. Abbes et M. Gros, “Topos co-évanescents et généralisations”, prépublication, 2011. [arXiv 1107.2380v3](#)
- [Achar et Sage 2009] P. N. Achar et D. S. Sage, “Perverse coherent sheaves and the geometry of special pieces in the unipotent variety”, *Adv. Math.* **220**:4 (2009), 1265–1296. [MR 2010a:20093](#) [Zbl 1168.20018](#)
- [Anderson 1987] G. W. Anderson, “Torsion points on Fermat Jacobians, roots of circular units and relative singular homology”, *Duke Math. J.* **54**:2 (1987), 501–561. [MR 89g:14012](#)
- [Anderson 2002] G. W. Anderson, “Abelians and their application to an elementary construction of Jacobians”, *Adv. Math.* **172**:2 (2002), 169–205. [MR 2004c:14056](#) [Zbl 1065.14035](#)
- [Artin 1971] M. Artin, “On the joins of Hensel rings”, *Advances in Math.* **7** (1971), 282–296. [MR 44 #6690](#) [Zbl 0242.13021](#)
- [Artin 1973] M. Artin, *Théorèmes de représentabilité pour les espaces algébriques*, Séminaire de Mathématiques Supérieures **44**, Presses de l'Université de Montréal, 1973. [MR 53 #10794](#) [Zbl 0323.14001](#)
- [Artin et Mazur 1969] M. Artin et B. Mazur, *Étale homotopy*, Lecture Notes in Mathematics **100**, Springer, Berlin, 1969. [MR 39 #6883](#) [Zbl 0182.26001](#)
- [Avigad 2003] J. Avigad, “Number theory and elementary arithmetic”, *Philos. Math.* (3) **11**:3 (2003), 257–284. [MR 2004g:03099](#) [Zbl 1050.03005](#)
- [Bayer et Mumford 1993] D. Bayer et D. Mumford, “What can be computed in algebraic geometry?”, pp. 1–48 dans *Computational algebraic geometry and commutative algebra* (Cortona, 1991), édité par D. Eisenbud et L. Robbiano, Symposia Mathematica **34**, Cambridge Univ. Press, New York, 1993. [MR 95d:13032](#) [Zbl 0846.13017](#)
- [Becker et Weispfenning 1993] T. Becker et V. Weispfenning, *Gröbner bases: a computational approach to commutative algebra*, Graduate Texts in Mathematics **141**, Springer, New York, 1993. [MR 95e:13018](#) [Zbl 0772.13010](#)
- [Bhatt 2012] B. Bhatt, “Derived splinters in positive characteristic”, *Compos. Math.* **148**:6 (2012), 1757–1786. [MR 2999303](#) [Zbl 1291.14036](#)

- [Borceux 1994] F. Borceux, *Handbook of categorical algebra, I: Basic category theory*, Encyclopedia of Mathematics and its Applications **50**, Cambridge Univ. Press, 1994. MR 96g:18001a Zbl 0803.18001
- [Bosch, Lütkebohmert et Raynaud 1990] S. Bosch, W. Lütkebohmert et M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer, Berlin, 1990. MR 91i:14034 Zbl 0705.14001
- [Bourbaki 1981] N. Bourbaki, *Éléments de mathématique: Algèbre, chapitres 4 à 7*, Deuxième éd., Masson, Paris, 1981. MR 84d:00002 Zbl 1139.12001
- [Bürgisser, Clausen et Shokrollahi 1997] P. Bürgisser, M. Clausen et M. A. Shokrollahi, *Algebraic complexity theory*, Grundlehren der Mathematischen Wissenschaften **315**, Springer, Berlin, 1997. MR 99c:68002 Zbl 1087.68568
- [Carlson 2001] J. F. Carlson, “Calculating group cohomology: tests for completion”, *J. Symbolic Comput.* **31**:1-2 (2001), 229–242. MR 2002c:20083 Zbl 0979.20047
- [Conrad 2003] B. Conrad, “Cohomological Descent”, notes, 2003, voir <http://math.stanford.edu/~conrad/papers/hypercover.pdf>.
- [Cox, Little et O’Shea 2007] D. Cox, J. Little et D. O’Shea, *Ideals, varieties, and algorithms*, Troisième éd., Springer, New York, 2007. MR 2007h:13036 Zbl 1118.13001
- [Debarre 2001] O. Debarre, *Higher-dimensional algebraic geometry*, Springer, New York, 2001. MR 2002g:14001 Zbl 0978.14001
- [Decker et Lossen 2006] W. Decker et C. Lossen, *Computing in algebraic geometry*, Algorithms and Computation in Mathematics **16**, Springer, Berlin, 2006. MR 2007b:14129 Zbl 1095.14001
- [Deligne 1974] P. Deligne, “Théorie de Hodge, III”, *Inst. Hautes Études Sci. Publ. Math.* **44** (1974), 5–77. MR 58 #16653b Zbl 0237.14003
- [Deligne 1980] P. Deligne, “La conjecture de Weil, II”, *Inst. Hautes Études Sci. Publ. Math.* **52** (1980), 137–252. MR 83c:14017 Zbl 0456.14014
- [Deligne et al. 1982] P. Deligne, J. S. Milne, A. Ogus et K.-y. Shih, *Hodge cycles, motives, and Shimura varieties*, Lecture Notes in Mathematics **900**, Springer, Berlin-New York, 1982. MR 84m:14046 Zbl 0465.00010
- [Dixon et al. 1999] J. D. Dixon, M. P. F. du Sautoy, A. Mann et D. Segal, *Analytic pro- p groups*, Deuxième éd., Cambridge Studies in Advanced Mathematics **61**, Cambridge Univ. Press, 1999. MR 2000m:20039 Zbl 0934.20001
- [Dold et Puppe 1961] A. Dold et D. Puppe, “Homologie nicht-additiver Funktoren: anwendungen”, *Ann. Inst. Fourier Grenoble* **11** (1961), 201–312. MR 27 #186 Zbl 0098.36005
- [van den Dries et Schmidt 1984] L. van den Dries et K. Schmidt, “Bounds in the theory of polynomial rings over fields: a nonstandard approach”, *Invent. Math.* **76**:1 (1984), 77–91. MR 85i:12016 Zbl 0539.13011
- [Edixhoven et Couveignes 2011] B. Edixhoven et J.-M. Couveignes (éditeurs), *Computational aspects of modular forms and Galois representations*, Annals of Mathematics Studies **176**, Princeton Univ. Press, 2011. MR 2849700 Zbl 1216.11004
- [ÉGA I 1960] A. Grothendieck, “Éléments de géométrie algébrique, I: Le langage des schémas”, *Inst. Hautes Études Sci. Publ. Math.* **4** (1960), 5–228. Rédigés avec la collaboration de Jean Dieudonné. MR 29 #1207 Zbl 0118.36206
- [ÉGA I 1971] A. Grothendieck et J. A. Dieudonné, *Éléments de géométrie algébrique, I*, Grundlehren der Mathematischen Wissenschaften **166**, Springer, Berlin, 1971. MR 3075000 Zbl 0203.23301

- [ÉGA II 1961] A. Grothendieck, “Éléments de géométrie algébrique, II: Étude globale élémentaire de quelques classes de morphismes”, *Inst. Hautes Études Sci. Publ. Math.* **8** (1961), 5–222. Rédigés avec la collaboration de Jean Dieudonné. MR 0163909 Zbl 0118.36206
- [ÉGA III₁ 1961] A. Grothendieck, “Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, I”, *Inst. Hautes Études Sci. Publ. Math.* **11** (1961), 5–167. Rédigés avec la collaboration de Jean Dieudonné. MR 0163910 Zbl 0118.36206
- [ÉGA III₂ 1963] A. Grothendieck, “Éléments de géométrie algébrique, III: Étude cohomologique des faisceaux cohérents, II”, *Inst. Hautes Études Sci. Publ. Math.* **17** (1963), 5–91. Rédigés avec la collaboration de Jean Dieudonné. MR 0163911 Zbl 0122.16102
- [ÉGA IV₁ 1964] A. Grothendieck, “Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, I”, *Inst. Hautes Études Sci. Publ. Math.* **20** (1964), 5–259. Rédigés avec la collaboration de Jean Dieudonné. MR 173675 Zbl 0136.15901
- [ÉGA IV₂ 1965] A. Grothendieck, “Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, II”, *Inst. Hautes Études Sci. Publ. Math.* **24** (1965), 5–231. Rédigés avec la collaboration de Jean Dieudonné. MR 0199181 Zbl 0135.39701
- [ÉGA IV₄ 1967] A. Grothendieck, “Éléments de géométrie algébrique, IV: Étude locale des schémas et des morphismes de schémas, IV”, *Inst. Hautes Études Sci. Publ. Math.* **32** (1967), 5–361. Rédigés avec la collaboration de Jean Dieudonné. MR 0238860 Zbl 153.22301
- [ÉGA V] A. Grothendieck, “Pré-notes ÉGA V”, 197?, voir <http://www.jmilne.org/math/Documents/EGA-V.pdf>.
- [Eisenbud 1995] D. Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics **150**, Springer, New York, 1995. MR 97a:13001 Zbl 0819.13001
- [Elkik 1973] R. Elkik, “Solutions d’équations à coefficients dans un anneau hensélien”, *Ann. Sci. École Norm. Sup. (4)* **6** (1973), 553–603. MR 49 #10692 Zbl 0327.14001
- [Evens 1991] L. Evens, *The cohomology of groups*, Clarendon Press, Oxford Univ. Press, New York, 1991. MR 93i:20059 Zbl 0742.20050
- [Faltings 1988] G. Faltings, “ p -adic Hodge theory”, *J. Amer. Math. Soc.* **1:1** (1988), 255–299. MR 89g:14008 Zbl 0764.14012
- [Ferrand 2003] D. Ferrand, “Conducteur, descente et pincement”, *Bull. Soc. Math. France* **131:4** (2003), 553–585. MR 2005a:13016 Zbl 1058.14003
- [Fried et Jarden 2008] M. D. Fried et M. Jarden, *Field arithmetic*, Troisième éd., Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **11**, Springer, Berlin, 2008. MR 2009j:12007 Zbl 1145.12001
- [Friedlander 1982] E. M. Friedlander, *Étale homotopy of simplicial schemes*, Annals of Mathematics Studies **104**, Princeton Univ. Press, 1982. MR 84h:55012 Zbl 0538.55001
- [Friedman 1999] H. Friedman, “Foundations of mathematics: grand conjectures”, courriel à la liste de diffusion *Foundations of Mathematics*, 16 avril 1999, voir <http://cs.nyu.edu/pipermail/fom/1999-April/003014.html>.
- [Friedman 2011] H. Friedman, “Boolean relation theory and incompleteness”, prépublication, 2011, voir <http://u.osu.edu/friedman.8/files/2014/01/0EntireBook061311-wh0yjj.pdf>. À paraître dans *Lecture Notes in Logic*, Cambridge Univ. Press.
- [Fröhlich et Shepherdson 1956] A. Fröhlich et J. C. Shepherdson, “Effective procedures in field theory”, *Philos. Trans. Roy. Soc. London. Ser. A* **248** (1956), 407–432. MR 17,570d Zbl 0070.03502
- [Gabber 2001] O. Gabber, Lettre à F. Orgogozo, 28 décembre 2001.
- [Gabber et Ramero 2003] O. Gabber et L. Ramero, *Almost ring theory*, Lecture Notes in Mathematics **1800**, Springer, Berlin, 2003. MR 2004k:13027 Zbl 1045.13002

- [Gabriel et Zisman 1967] P. Gabriel et M. Zisman, *Calculus of fractions and homotopy theory*, *Ergebnisse der Mathematik und ihrer Grenzgebiete* **35**, Springer, New York, 1967. [MR 35 #1019](#) [Zbl 0186.56802](#)
- [Gianni, Trager et Zacharias 1988] P. Gianni, B. Trager et G. Zacharias, “Gröbner bases and primary decomposition of polynomial ideals”, *J. Symbolic Comput.* **6**:2-3 (1988), 149–167. [MR 90f:68091](#) [Zbl 0667.13008](#)
- [Giraud 1971] J. Giraud, *Cohomologie non abélienne*, *Grundlehren der mathematischen Wissenschaften* **179**, Springer, Berlin-New York, 1971. [MR 49 #8992](#) [Zbl 0226.14011](#)
- [Grauert et Remmert 1984] H. Grauert et R. Remmert, *Coherent analytic sheaves*, *Grundlehren der Mathematischen Wissenschaften* **265**, Springer, Berlin, 1984. [MR 86a:32001](#) [Zbl 0537.32001](#)
- [Grothendieck 1956] A. Grothendieck, “Théorèmes de finitude pour la cohomologie des faisceaux”, *Bull. Soc. Math. France* **84** (1956), 1–7. [MR 18,327c](#) [Zbl 0071.17403](#)
- [Grothendieck 1957] A. Grothendieck, “Sur quelques points d’algèbre homologique”, *Tôhoku Math. J. (2)* **9** (1957), 119–221. [MR 21 #1328](#) [Zbl 0118.26104](#)
- [Grothendieck et Murre 1971] A. Grothendieck et J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, *Lecture Notes in Mathematics* **208**, Springer, Berlin-New York, 1971. [MR 47 #5000](#) [Zbl 0216.33001](#)
- [Haiman et Sturmfels 2004] M. Haiman et B. Sturmfels, “Multigraded Hilbert schemes”, *J. Algebraic Geom.* **13**:4 (2004), 725–769. [MR 2005d:14006](#) [Zbl 1072.14007](#)
- [Hájek et Pudlák 1998] P. Hájek et P. Pudlák, *Metamathematics of first-order arithmetic*, Springer, Berlin, 1998. [MR 2000m:03003](#) [Zbl 0889.03053](#)
- [Harrington et al. 1985] L. A. Harrington, M. D. Morley, A. Ščedrov et S. G. Simpson (éditeurs), *Harvey Friedman’s research on the foundations of mathematics*, *Stud. Logic Found. Math.* **117**, North-Holland, Amsterdam, 1985. [MR 87b:03004](#) [Zbl 0588.03001](#)
- [Hess 2002] F. Hess, “Computing Riemann–Roch spaces in algebraic function fields and related topics”, *J. Symbolic Comput.* **33**:4 (2002), 425–445. [MR 2003j:14032](#) [Zbl 1058.14071](#)
- [Hofstadter 1979] D. R. Hofstadter, *Gödel, Escher, Bach: an eternal golden braid*, Basic Books, New York, 1979. [MR 80j:03009](#) [Zbl 1014.03005](#)
- [Huneke et Swanson 2006] C. Huneke et I. Swanson, *Integral closure of ideals, rings, and modules*, *London Math. Soc. Lecture Note Series* **336**, Cambridge Univ. Press, 2006. [MR 2008m:13013](#) [Zbl 1117.13001](#)
- [Illusie 1971] L. Illusie, *Complexe cotangent et déformations, I*, *Lecture Notes in Mathematics* **239**, Springer, Berlin-New York, 1971. [MR 58 #10886a](#) [Zbl 0224.13014](#)
- [Illusie 1972] L. Illusie, *Complexe cotangent et déformations, II*, *Lecture Notes in Mathematics* **283**, Springer, Berlin-New York, 1972. [MR 58 #10886b](#) [Zbl 0238.13017](#)
- [Illusie, Laszlo et Orgogozo 2014] L. Illusie, Y. Laszlo et F. Orgogozo, *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**, Société mathématique de France, Paris, 2014. Avec la collaboration de Frédéric Déglise, Alban Moreau, Vincent Pilloni, Michel Raynaud, Joël Riou, Benoît Stroh, Michael Temkin et Weizhe Zheng. [MR 3329778](#) [Zbl 1297.14003](#)
- [Jacobsson et Stoltenberg-Hansen 1985] C. Jacobsson et V. Stoltenberg-Hansen, “Poincaré–Betti series are primitive recursive”, *J. London Math. Soc. (2)* **31**:1 (1985), 1–9. [MR 87e:03103](#) [Zbl 0584.03032](#)
- [de Jong 1996] A. J. de Jong, “Smoothness, semi-stability and alterations”, *Inst. Hautes Études Sci. Publ. Math.* **83** (1996), 51–93. [MR 98e:14011](#) [Zbl 0916.14005](#)

- [de Jong 1998] T. de Jong, “An algorithm for computing the integral closure”, *J. Symbolic Comput.* **26**:3 (1998), 273–277. [MR 99d:13007](#) [Zbl 0932.13021](#)
- [Kashiwara et Schapira 2006] M. Kashiwara et P. Schapira, *Categories and sheaves*, Grundlehren der Mathematischen Wissenschaften **332**, Springer, Berlin, 2006. [MR 2006k:18001](#) [Zbl 1118.18001](#)
- [Katz et Laumon 1985] N. M. Katz et G. Laumon, “Transformation de Fourier et majoration de sommes exponentielles”, *Inst. Hautes Études Sci. Publ. Math.* **62** (1985), 361–418. [MR 87i:14017](#) [Zbl 0603.14015](#)
- [Lecerf 2013] G. Lecerf, “Factorisation des polynômes à plusieurs variables”, *Les cours du CIRM* **3**:1 (2013), exposé no. 2.
- [Lombardi et Quitté 2011] H. Lombardi et C. Quitté, *Algèbre commutative: méthodes constructives*, Calvage et Mounet, Paris, 2011. [Zbl 1242.13002](#)
- [Lubotzky et Segal 2003] A. Lubotzky et D. Segal, *Subgroup growth*, Progress in Mathematics **212**, Birkhäuser, Basel, 2003. [MR 2004k:20055](#) [Zbl 1071.20033](#)
- [Mac Lane 1963] S. Mac Lane, *Homology*, Grundlehren der Mathematischen Wissenschaften **114**, Springer, Berlin, 1963. [MR 28 #122](#) [Zbl 0133.26502](#)
- [Madore 2014] D. Madore, “Commutative algebras whose bidual is commutative”, question sur MathOverflow, 2014, voir <http://mathoverflow.net/q/156091>.
- [Madore et Orgogozo 2014] D. Madore et F. Orgogozo, “Un modèle de calcul universel sur les éléments des corps” (titre provisoire), prépublication, 2014. Partie III de [arXiv 1304.5376v3](#)
- [Matsumura 1989] H. Matsumura, *Commutative ring theory*, Deuxième éd., Cambridge Studies in Advanced Mathematics **8**, Cambridge Univ. Press, 1989. [MR 90i:13001](#) [Zbl 0666.13002](#)
- [Miller 2010] R. Miller, “Is it harder to factor a polynomial or to find a root?”, *Trans. Amer. Math. Soc.* **362**:10 (2010), 5261–5281. [MR 2011e:12003](#) [Zbl 1215.12005](#)
- [Milne 1980] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series **33**, Princeton Univ. Press, 1980. [MR 81j:14002](#) [Zbl 0433.14012](#)
- [Mines et Richman 1982] R. Mines et F. Richman, “Separability and factoring polynomials”, *Rocky Mountain J. Math.* **12**:1 (1982), 43–54. [MR 84e:03075](#) [Zbl 0499.12019](#)
- [Mines, Richman et Ruitenburg 1988] R. Mines, F. Richman et W. Ruitenburg, *A course in constructive algebra*, Springer, New York, 1988. [MR 89d:03066](#) [Zbl 0725.03044](#)
- [Mochizuki 1999] S. Mochizuki, “Extending families of curves over log regular schemes”, *J. Reine Angew. Math.* **511** (1999), 43–71. [MR 2000f:14041](#) [Zbl 0933.14012](#)
- [Mumford 1975] D. Mumford, *Curves and their Jacobians*, University of Michigan Press, Ann Arbor, MI, 1975. [MR 54 #7451](#) [Zbl 0316.14010](#)
- [Neukirch, Schmidt et Wingberg 2000] J. Neukirch, A. Schmidt et K. Wingberg, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften **323**, Springer, Berlin, 2000. [MR 2000j:11168](#) [Zbl 0948.11001](#)
- [Odifreddi 1989] P. Odifreddi, *Classical recursion theory*, Studies in Logic and the Foundations of Mathematics **125**, North-Holland, Amsterdam, 1989. [MR 90d:03072](#) [Zbl 0661.03029](#)
- [Odifreddi 1999] P. G. Odifreddi, *Classical recursion theory, II*, Studies in Logic and the Foundations of Mathematics **143**, North-Holland, Amsterdam, 1999. [MR 2001b:03040](#) [Zbl 0931.03057](#)
- [Ogg 1962] A. P. Ogg, “Cohomology of abelian varieties over function fields”, *Ann. of Math. (2)* **76** (1962), 185–212. [MR 27 #5758](#) [Zbl 0121.38002](#)
- [Orgogozo 2003] F. Orgogozo, “Altérations et groupe fondamental premier à p ”, *Bull. Soc. Math. France* **131**:1 (2003), 123–147. [MR 2004e:14034](#) [Zbl 1083.14506](#)

- [Orgogozo 2013] F. Orgogozo, “[Sur les propriétés d’uniformité des images directes en cohomologie étale](#)”, prépublication, 2013, voir <http://fabrice.orgogozo.perso.math.cnrs.fr/articles/uniformite.pdf>.
- [Palmer 1974] T. W. Palmer, “[Arens multiplication and a characterization of \$w^*\$ -algebras](#)”, *Proc. Amer. Math. Soc.* **44** (1974), 81–87. MR 49 #5872 Zbl 0284.46041
- [Petersen 2010] D. Petersen, “[Ring-theoretic characterization of open affines?](#)”, réponse à une question sur MathOverflow, 2010, voir <http://mathoverflow.net/a/20790/17064>.
- [Poonen, Testa et van Luijk 2015] B. Poonen, D. Testa et R. van Luijk, “[Computing Néron–Severi groups and cycle class groups](#)”, *Compos. Math.* **151**:4 (2015), 713–734. MR 3334893 Zbl 06437570
- [Rabin 1960] M. O. Rabin, “[Computable algebra, general theory and theory of computable fields](#)”, *Trans. Amer. Math. Soc.* **95** (1960), 341–360. MR 22 #4639 Zbl 0156.01201
- [Richman 1981] F. Richman, “[Seidenberg’s condition \$P\$](#) ”, pp. 1–11 dans *Constructive mathematics* (Las Cruces, NM, 1980), édité par F. Richman, Lecture Notes in Mathematics **873**, Springer, Berlin–New York, 1981. MR 84k:12017 Zbl 0461.03016
- [Rotman 1995] J. J. Rotman, *An introduction to the theory of groups*, Quatrième éd., Graduate Texts in Mathematics **148**, Springer, New York, 1995. MR 95m:20001 Zbl 0810.20001
- [Rubio et Sergeraert 2002] J. Rubio et F. Sergeraert, “[Constructive algebraic topology](#)”, *Bull. Sci. Math.* **126**:5 (2002), 389–412. MR 2003g:55001 Zbl 1007.55019
- [Schön 1991] R. Schön, *Effective algebraic topology*, vol. 92, Mem. Amer. Math. Soc. **451**, Amer. Math. Soc., Providence, RI, 1991. MR 92h:55002 Zbl 0731.55015
- [Sergeraert 1994] F. Sergeraert, “[The computability problem in algebraic topology](#)”, *Adv. Math.* **104**:1 (1994), 1–29. MR 95c:55017 Zbl 0823.55011
- [Serre 1955] J.-P. Serre, “[Faisceaux algébriques cohérents](#)”, *Ann. of Math. (2)* **61** (1955), 197–278. MR 16,953c Zbl 0067.16201
- [Serre 1965] J.-P. Serre, *Algèbre locale: multiplicités*, Deuxième éd., Lecture Notes in Mathematics **11**, Springer, Berlin–New York, 1965. MR 34 #1352 Zbl 0142.28603
- [Serre 1975] J.-P. Serre, *Groupes algébriques et corps de classes*, Deuxième éd., Actualités Scientifiques et Industrielles **1264**, Hermann, Paris, 1975. MR 57 #6032 Zbl 0318.14004
- [Serre 1977] J.-P. Serre, *Arbres, amalgames, SL_2* , Astérisque **46**, Société Mathématique de France, Paris, 1977. MR 57 #16426 Zbl 0369.20013
- [Serre 1978–79] J.-P. Serre, “[Groupes finis](#)”, notes d’un cours à l’ÉNSJF, 1978–79. arXiv 0503154v6
- [Serre 1994] J.-P. Serre, *Cohomologie galoisienne*, Cinquième éd., Lecture Notes in Mathematics **5**, Springer, Berlin, 1994. MR 96b:12010 Zbl 0812.12002
- [SGA 1 2003] A. Grothendieck, *Revêtements étales et groupe fondamental* (Séminaire de Géométrie Algébrique du Bois Marie 1960–1961), Documents Mathématiques (Paris) **3**, Société Mathématique de France, Paris, 2003. MR 2017446 Zbl 1039.14001
- [SGA 4₁ 1972] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 1: Théorie des topos, Exposés I–IV* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **269**, Springer, Berlin, 1972. MR 50 #7130 Zbl 0234.00007
- [SGA 4₂ 1972] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 2: Exposés V–VIII* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **270**, Springer, Berlin, 1972. MR 50 #7131 Zbl 0237.00012
- [SGA 4₃ 1973] M. Artin, A. Grothendieck et J. L. Verdier, *Théorie des topos et cohomologie étale des schémas, Tome 3: Exposés IX–XIX* (Séminaire de Géométrie Algébrique du Bois Marie 1963–1964), Lecture Notes in Mathematics **305**, Springer, Berlin, 1973. MR 50 #7132 Zbl 0245.00002

- [SGA 4 $\frac{1}{2}$ 1977] P. Deligne, *Cohomologie étale* (Séminaire de Géométrie Algébrique du Bois Marie), Lecture Notes in Mathematics **569**, Springer, Berlin, 1977. Avec la collaboration de J.-F. Boutot, A. Grothendieck, L. Illusie et J.-L. Verdier. MR 57 #3132 Zbl 0349.14008
- [Simpson 2008] C. Simpson, “Algebraic cycles from a computational point of view”, *Theoret. Comput. Sci.* **392**:1-3 (2008), 128–140. MR 2008m:14021 Zbl 1134.14005
- [Simpson 2009] S. G. Simpson, *Subsystems of second order arithmetic*, Deuxième éd., Cambridge Univ. Press, Association for Symbolic Logic, Poughkeepsie, NY, 2009. MR 2010e:03073 Zbl 1181.03001
- [Singh et Swanson 2009] A. K. Singh et I. Swanson, “An algorithm for computing the integral closure”, *Algebra Number Theory* **3**:5 (2009), 587–595. MR 2011b:13022 Zbl 1180.13010
- [Smoryński 1985] C. Smoryński, “The varieties of arboreal experience [Math. Intelligencer 4:4 (1982), 182–189]”, pp. 381–397 dans *Harvey Friedman’s research on the foundations of mathematics*, édité par L. A. Harrington et al., Stud. Logic Found. Math. **117**, North-Holland, Amsterdam, 1985. MR 835269 Zbl 0588.03001
- [Steel 2005] A. Steel, “Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic”, *J. Symbolic Comput.* **40**:3 (2005), 1053–1075. MR 2006f:13023 Zbl 1120.13026
- [Stoltenberg-Hansen et Tucker 1999] V. Stoltenberg-Hansen et J. V. Tucker, “Computable rings and fields”, pp. 363–447 dans *Handbook of computability theory*, édité par E. R. Griffor, Stud. Logic Found. Math. **140**, North-Holland, Amsterdam, 1999. MR 2000g:03100 Zbl 0944.03040
- [Stolzenberg 1968] G. Stolzenberg, “Constructive normalization of an algebraic variety”, *Bull. Amer. Math. Soc.* **74** (1968), 595–599. MR 37 #201 Zbl 0164.04202
- [Szamuely 2009] T. Szamuely, *Galois groups and fundamental groups*, Cambridge Studies in Advanced Mathematics **117**, Cambridge Univ. Press, 2009. MR 2011b:14064 Zbl 1189.14002
- [Vasconcelos 2005] W. Vasconcelos, *Integral closure*, Springer, Berlin, 2005. MR 2006m:13007 Zbl 1082.13006
- [Wingberg 1984] K. Wingberg, “Ein Analogon zur Fundamentalgruppe einer Riemannschen Fläche im Zahlkörperfall”, *Invent. Math.* **77**:3 (1984), 557–584. MR 86e:11104 Zbl 0563.12008
- [Zariski et Samuel 1975] O. Zariski et P. Samuel, *Commutative algebra, I*, Graduate Texts in Mathematics **28**, Springer, Berlin, 1975. MR 52 #5641 Zbl 0313.13001

Communicated by Bjorn Poonen

Received 2014-10-16

Revised 2015-04-16

Accepted 2015-04-28

david+math@madore.org

INFRES/CNRS LTCI, Institut Mines-Télécom, Télécom
ParisTech, 75013 Paris, France

fabrice.orgogozo+math@normalesup.org

Centre de mathématiques Laurent Schwartz,
CNRS, École polytechnique, 91128 Palaiseau, France

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Georgia Benkart	University of Wisconsin, Madison, USA	Susan Montgomery	University of Southern California, USA
Dave Benson	University of Aberdeen, Scotland	Shigefumi Mori	RIMS, Kyoto University, Japan
Richard E. Borcherds	University of California, Berkeley, USA	Raman Parimala	Emory University, USA
John H. Coates	University of Cambridge, UK	Jonathan Pila	University of Oxford, UK
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Anand Pillay	University of Notre Dame, USA
Brian D. Conrad	Stanford University, USA	Victor Reiner	University of Minnesota, USA
Hélène Esnault	Freie Universität Berlin, Germany	Peter Sarnak	Princeton University, USA
Hubert Flenner	Ruhr-Universität, Germany	Joseph H. Silverman	Brown University, USA
Sergey Fomin	University of Michigan, USA	Michael Singer	North Carolina State University, USA
Edward Frenkel	University of California, Berkeley, USA	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Andrew Granville	Université de Montréal, Canada	J. Toby Stafford	University of Michigan, USA
Joseph Gubeladze	San Francisco State University, USA	Ravi Vakil	Stanford University, USA
Roger Heath-Brown	Oxford University, UK	Michel van den Bergh	Hasselt University, Belgium
Craig Huneke	University of Virginia, USA	Marie-France Vignéras	Université Paris VII, France
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Kei-Ichi Watanabe	Nihon University, Japan
János Kollár	Princeton University, USA	Efim Zelmanov	University of California, San Diego, USA
Yuri Manin	Northwestern University, USA	Shou-Wu Zhang	Princeton University, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne		

PRODUCTION

production@msp.org

Silvio Levy, Scientific Editor

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US \$255/year for the electronic version, and \$440/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW[®] from MSP.

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2015 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 9 No. 7 2015

<i>Singular moduli that are algebraic units</i>	1515
PHILIPP HABEGGER	
<i>Irreducibility of the Gorenstein loci of Hilbert schemes via ray families</i>	1525
GIANFRANCO CASNATI, JOACHIM JELISIEJEW and ROBERTO NOTARI	
<i>p-adic heights of Heegner points on Shimura curves</i>	1571
DANIEL DISEGNI	
<i>Calculabilité de la cohomologie étale modulo ℓ</i>	1647
DAVID A. MADORE and FABRICE ORGOGOZO	