

Calculabilité de la cohomologie étale modulo 1

David A. MADORE and Fabrice ORGOGOZO



Institut des Hautes Études Scientifiques
35, route de Chartres
91440 – Bures-sur-Yvette (France)

Mars 2014

IHES/M/14/13

CALCULABILITÉ DE LA COHOMOLOGIE ÉTALE MODULO ℓ

David A. Madore et Fabrice Orgogozo

RÉSUMÉ. Soient X un schéma algébrique sur un corps algébriquement clos et ℓ un nombre premier inversible sur X . D'après des résultats classiques (dus notamment à A. Grothendieck, M. Artin, et P. Deligne), 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 de M. 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 \mathbf{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. Enfin, dans la troisième partie, on présente un formalisme de calcul « universel » sur les éléments d'un corps.

ABSTRACT. Let X be an algebraic scheme over an algebraically closed field and ℓ a prime number invertible on X . According to classical results (due essentially to A. Grothendieck, M. Artin and P. Deligne), the étale cohomology groups $H^i(X, \mathbb{Z}/\ell\mathbb{Z})$ are finite-dimensional. Using an ℓ -adic variant of M. 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 \mathbf{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-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. Finally, in the third part, we present a "universal" formalism for computation on the elements of a field.

TABLE DES MATIÈRES

Introduction	2
I. Cohomologie étale	5
1. $K(\pi, 1)$ pro- ℓ	5
2. Calculabilité du H^1	13
3. Série ℓ -centrale descendante et groupe fondamental	14
4. Cohomologie ℓ -étale n -approchée d'un schéma simplicial	17
5. Systèmes essentiellement constants	20
6. Approximation d'un pro- ℓ -groupe par ses quotients finis	22
7. Calcul de la cohomologie d'une polycourbe ℓ -élémentaire	24
8. Descente	26
9. Functorialité	26
10. Structure de l'algorithme	28
11. Compléments	28
II. Algèbre commutative et géométrie algébrique effectives	34
12. Corps et extensions de corps	34
13. Modules de type fini sur une k -algèbre de type fini	38
14. Algèbres de type fini sur un corps : description algorithmique	41
15. Algèbre commutative effective	43
16. Schémas de type fini sur un corps : description algorithmique	47
17. Géométrie algébrique effective	50
III. Modèle de calcul « universel »	51
Motivation	51

18. Types et parties constructibles	52
19. Fonctions F-rationnelles	54
20. Fonctions partielles calculables	55
21. Équivalence avec le modèle « boîte noire »	57
22. Fonctions totales	59
23. Élimination des quantificateurs	61
24. Sélection d'un élément unique	63
25. Factorisation dans le modèle de calcul	64
26. Indépendance de la caractéristique (esquisse)	68
Bibliographie	69

INTRODUCTION

L'objet principal de ce texte est de démontrer le théorème suivant, ainsi que la variante relative **0.8**.

0.1. Théorème. *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 functorialité 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 (et nous présentons dans la partie **III** un modèle de calcul « universel » qui permet d'obtenir des stratifications explicites comme expliqué en **0.6**); voir aussi **0.9 infra**. Calculer le groupe $H^i(X, \mathbb{F}_\ell)$ signifie 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 le rang, et, si $Y = X$, une matrice. (Voir §9 pour des précisions.)

L'énoncé précédent répond notamment à la question posée en [POONEN, TESTA et LUIJK 2012, hypothèse 7.4] et également considérée dans [EDIXHOVEN et COUVEIGNES 2011, chap. 1 et chap. 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 [C. SIMPSON 2008, corollaire 2.5] ou [POONEN, TESTA et LUIJK 2012, §7.2]). 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, indicé 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 $\mathbf{X}_\alpha = \pi_0(X_\alpha/X)$ l'ensemble simplicial des composantes connexes des produits fibrés itérés de X_α au-dessus de X . Comme à tout ensemble simplicial, on peut lui associer des groupes de cohomologie, notés $H^i(\mathbf{X}_\alpha, \mathbb{Z}/\ell\mathbb{Z})$ (ou $\check{H}^i(X_\alpha/X, \mathbb{Z}/\ell\mathbb{Z})$) : considérer le \mathbb{F}_ℓ -module cosimplicial naturellement associé puis le complexe dont les dérivations sont les sommes alternées des faces (cf. [SGA 4, 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 $H^i(\mathbf{X}_\alpha, \mathbb{Z}/\ell\mathbb{Z})$. 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 $H^i(X, \mathbb{Z}/\ell\mathbb{Z}) = \text{Im}(H^i(\mathbf{X}_\alpha, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^i(\mathbf{X}_\beta, \mathbb{Z}/\ell\mathbb{Z}))$ (ces entiers existent car le système inductif $H^i(\mathbf{X}_\alpha, \mathbb{Z}/\ell\mathbb{Z})$ 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 4, XI]) et Gerd Faltings ([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 $H^i(\mathbf{X}_\alpha, \mathbb{Z}/\ell\mathbb{Z})$ — il s'agit maintenant de cohomologie de ℓ -groupes — est « explicitement »

essentiellement constant. La technique utilisée pour résoudre (ou plutôt d'ignorer) les divers problèmes d'extension que l'on rencontre est semblable à celle de [SCHÖN 1991, chap. I-II] (également connue, indépendamment de [ibid.], 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.

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. Remarque. 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.

0.5. 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 $\mathbb{Z}/\ell^n\mathbb{Z}$. Pour d'autres compléments, et quelques questions, voir §11.

0.6. Stratifications. La première des affirmations suivantes, où ℓ est un nombre premier fixé, inversible sur les schémas considérés, découle immédiatement du modèle de calcul « universel » décrit dans la partie III (cf. 22.4), et la seconde d'une généralisation facile de celui-ci (cf. §26 et notamment 26.6) :

- 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, donné un morphisme $\mathcal{X} \rightarrow \mathbb{A}^r$, on peut calculer une partition de \mathbb{A}^r en un nombre fini de parties constructibles sur chacune desquelles $H^i(X, \mathbb{F}_\ell)$ a une dimension fixée, qu'on peut calculer, où X désigne une fibre en un point géométrique de la partie ; il en va de même, par exemple, du rang de $H^i(X, \mathbb{F}_\ell) \rightarrow H^i(Y, \mathbb{F}_\ell)$ (pour un morphisme $\mathcal{X} \rightarrow \mathcal{Y}$ sur \mathbb{A}^r) ;
- si X est défini sur un ouvert de $\text{Spec } \mathbb{Z}$, on peut calculer un p_0 tel que la dimension de $H^i(X_p, \mathbb{F}_\ell)$ 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 rang de $H^i(X_p, \mathbb{F}_\ell) \rightarrow H^i(Y_p, \mathbb{F}_\ell)$.

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 observé par Olivier Wittenberg ([POONEN, TESTA et LUIJK 2012, prop. 8.3]), le théorème 0.1 (étendu au cas des coefficients $\mathbb{Z}/\ell^n\mathbb{Z}$) a le corollaire suivant.

0.7. Corollaire. *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. [ibid.]) Notons par contre, qu'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. 11.4).

On déduira du théorème 0.1 le résultat suivant (voir 11.3).

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

(Idéalement, on aimerait plutôt déduire **0.1** du théorème **0.8**, démontré par dévissage.)

0.9. 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** doit se comprendre au sens 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 **0.10** 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 $\mathbf{P}(m, n)$ elle-même calculable, alors la fonction $\mu_n \mathbf{P}$ qui à m associe le plus petit n vérifiant $\mathbf{P}(m, n)$ 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 ¶**11.5** plus bas.

0.10. Remarques générales sur les corps calculables et la géométrie algébrique effective. Nous considérons dans cet article deux points de vue très liés, mais néanmoins différents, sur la calculabilité des opérations algébriques :

- Selon le premier point de vue, qui est le plus classique, on dispose de la notion de *corps calculable* (rappelée en **12.1**, et qui contient notamment une clôture algébrique de \mathbb{F}_p ou de $\mathbb{F}_p(T_1, \dots, T_r)$), c’est-à-dire de corps dont les éléments sont codés par des entiers naturels et sur lequel on suppose qu’une machine de Turing puisse effectuer les opérations algébriques. Nous expliquons dans la partie **II** comment, donné un corps calculable k (disposant d’un algorithme de factorisation et d’une p -base finie explicite, cf. **12.7**), on peut algorithmiquement manipuler les k -schémas algébriques de type fini et leurs morphismes (§16) et calculer ou tester la plupart des opérations et propriétés classiques de la géométrie algébrique. Si on adopte ce point de vue, on peut ignorer complètement la partie **III** de cet article.
- L’autre point de vue, que nous appellerons « modèle de calcul “universel” », dont l’exposition fait l’objet de la partie **III**, consiste à considérer un corps k algébriquement clos *quelconque* et des machines qui peuvent manipuler (outre, évidemment, les entiers naturels) les éléments de k sous forme de « boîtes noires » sur lesquelles elles peuvent effectuer les opérations algébriques et le test d’égalité. L’intérêt de ce point de vue est triple. D’abord, il se passe d’hypothèses sur le corps, et revient à travailler sur tous les corps algébriquement clos de caractéristique fixée. Ensuite, il garantit que les fonctions calculables sont *uniquement* celles qui s’obtiennent par des opérations algébriques sur les corps (et pas, par exemple, celles qui pourraient dépendre du détail du codage d’un élément du corps par tel ou tel entier naturel : cf. **21.5**) : on observera donc au cours de la lecture de la partie **II**, que tous les algorithmes décrits sont de cette nature. Enfin, ce modèle de calcul donne automatiquement des stratifications « universelles », comme en **0.6**, sur lesquelles les fonctions calculables prennent des valeurs constantes — c’est d’ailleurs la manière dont on définit ce modèle de calcul (cf. **20.1**).

0.11. Leitfaden. Des efforts ont été faits pour rendre la lecture de chacune des trois parties largement indépendantes des deux autres. L'ordre logique est $\text{III} \rightarrow \text{II} \rightarrow \text{I}$, mais comme on vient de l'expliquer on peut ignorer la partie III si on ne s'intéresse pas à des résultats tels que **0.6**, et par ailleurs 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, et la partie III décrit un formalisme indépendant de tout ce qui précède.

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 Luc Illusie, Jean Lannes, Ronald van Luijk, 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).

I. Cohomologie étale

1. $K(\pi, 1)$ PRO- ℓ

Les résultats de cette section, essentiellement dus à Ofer Gabber^①, 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**. Nous laissons le soin au lecteur qui le souhaite d'éliminer les hypothèses noethériennes.

1.1. Champs ℓ -monodromiques : définitions.

1.1.1. Soit \mathcal{C} un champ en groupoïdes sur un schéma localement noethérien 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

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

– c'est aussi le faisceau des *sous-gerbes maximales* ([ibid., 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 $\text{Aut}(c_U)$ 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, 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 $\varphi : \text{Isom ex}(p_1^* G', p_2^* G')$, 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 torsseurs sous un S -faisceau en groupes G , son lien est celui naturellement associé à G , représenté par le triplet ($S' = S, G' = G, \varphi = \text{Id}$). Le faisceau des automorphismes de ce lien est le faisceau des automorphismes *extérieurs* de G et l'ensemble des classes d'isomorphisme de liens *localement* représentés par le S -schéma en groupes G est naturellement isomorphe à $H^1(S, \text{Aut ex}(G))$.

^①Les auteurs sont bien entendu seuls responsables des éventuelles imprécisions ou erreurs dans l'exposition.

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].)

1.1.5. Définition. 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 le $\text{Aut ex}(G)$ -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 champ ℓ -monodromique ne provient pas nécessairement par image inverse du topos $S_{\text{ét}}$ considéré en 1.4.3; cela reflète le fait qu'une classe dans $H^2(S, Z(\ell\mathbb{Z}))$ n'est pas nécessairement tuée par un revêtement galoisien d'ordre une puissance de ℓ (cf. 1.1.4). C'est cependant vrai pour les faisceaux, c'est-à-dire pour les champs en catégories discrètes.

1.1.7. Remarque. 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 ℓ -adique des fibres d'un morphisme de type fini.

1.2. Champs ℓ -monodromiques : sorites.

1.2.1. Une extension de faisceaux abéliens ℓ -monodromiques est également ℓ -monodromique. La lissité (locale constance et constructibilité) résulte de [SGA 4, IX, 2.1(ii) et 2.6(ii)]. Que la monodromie soit un ℓ -groupe est conséquence immédiate du fait qu'un élément unipotent de $\text{GL}_n(\mathbb{Z}/\ell^r\mathbb{Z})$ est de ℓ -torsion, c'est-à-dire annulé par une puissance de ℓ .

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

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

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 $\text{Aut ex}(G_s)$ 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 $N_\sigma \trianglelefteq \text{Aut}(\sigma) = \pi_1(\mathcal{G}, \sigma)$ 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 $\text{Hom}_{\mathcal{G}'}(\sigma, \tau) := \text{Hom}_{\mathcal{G}}(\sigma, \tau)/N_\sigma$. 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 $Z_\sigma = Z(\text{Aut}(\sigma))$ 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 s est une section globale de la gerbe quotient \mathcal{G}/Z , la gerbe $\mathcal{K}(s)$ des relèvements de s à \mathcal{G} ([GIRAUD 1971, IV.2.5.1,2.5.4]) est naturellement une Z -gerbe (cf. [ibid., 2.5.6.(ii)]). Rappelons que $\mathcal{K}(s)$ est triviale si et seulement si la section s se relève à \mathcal{G} .

1.2.4. Lemme. Soient ℓ un nombre premier, G un ℓ -groupe fini et \mathcal{G} une gerbe 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{H} la gerbe quotient de \mathcal{G} par son centre (cf. 1.2.3). Cette gerbe est localement isomorphe à BH , où H est le quotient de G par son centre Z (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{K} de ses relèvements à \mathcal{G} (cf. loc. cit.) a une classe dans $H^2(S, Z)$ (1.1.4), nécessairement nulle par hypothèse. Il en résulte que la gerbe \mathcal{K} est triviale et, par conséquent, que la section globale de \mathcal{H} considérée se relève à la gerbe \mathcal{G} , qui est donc également triviale. \square

1.2.5. Lemme. Soit $\iota : \mathcal{H} \hookrightarrow \mathcal{G}$ 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{H} .

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{H} , le morphisme ι induit une injection $\text{Aut}_{\mathcal{H}}(h) \hookrightarrow \text{Aut}_{\mathcal{G}}(\iota h)$. Il en résulte que, localement, le morphisme $\text{lien}(\iota) : \text{lien}(\mathcal{H}) \rightarrow \text{lien}(\mathcal{G})$ 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 :

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

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 $\pi_1(S, s) \rightarrow \text{Aut ex}(H)$. CQFD. \square

1.3. Courbes et polycourbes ℓ -élémentaires. Rappelons les définitions [SGA 4, 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

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

satisfaisant aux conditions suivantes :

- (i) j est une immersion ouverte et $X = \overline{X} - D$;
- (ii) \overline{f} est une courbe (relative) projective lisse, à fibres géométriquement connexes;
- (iii) g est un revêtement étale (en particulier : chaque fibre de g est non vide).

Donnés un morphisme projectif \overline{f} et une immersion fermée i , les conditions (i)-(iii) sont algorithmiquement testables : pour la lissité de \overline{f} et g , utiliser 17.2; pour la connexité géométrique (resp. non vacuité) des fibres de \overline{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 $\overline{f}_* \underline{\mathbb{Z}}$ (resp. $g_* \underline{\mathbb{Z}}$) 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 4, XI]. (Voir aussi [GROTHENDIECK 197?, 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 4, 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 4, 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, XIII.2.9] pour $i \leq 1$, seul cas utilisé dans cet article); 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 $\text{GL}(H^1(X_{\bar{s}}, \mathbb{Z}/\ell\mathbb{Z}))$ 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.

1.3.5. Lemme. *Soient X/S une courbe 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 $Y \rightarrow S'$.*

Démonstration. Soit \bar{X}/S une compactification comme en 1.3.1. Par modération et le lemme d'Abhyankar relatif ([SGA 1, 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 ([GROTHENDIECK et MURRE 1971, 1.3.9.c]). Celui-ci est unique à isomorphisme unique près, sa source est lisse sur S et l'image inverse réduite de D est étale sur S . 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. Ses fibres ne sont pas nécessairement géométriquement connexe mais sa factorisation de Stein répond à la question. (Rappelons que d'après [ÉGA III₂, 7.8.10], la factorisation de Stein d'un morphisme propre et réduit est un revêtement *étale*.) □

1.3.6. Lemme. *Soient $X \rightarrow S$ une courbe élémentaire, ℓ un nombre premier inversible sur S et \mathcal{E} un champ en groupoïdes sur X . Si S est strictement local et si \mathcal{E} est ℓ -monodromique, il existe un ℓ -revêtement étale $X' \rightarrow X$ tel que $\mathcal{E}' = (X' \rightarrow X)^* \mathcal{E}$ 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 et l'hypothèse sur le champ \mathcal{E} , on peut supposer $\pi_0(\mathcal{E})$ constant. Quitte à remplacer \mathcal{E} 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 toiseurs et l'on pourra conclure par 1.2.2. L'existence d'une section résulte de 1.2.4 et du fait que, par modération et changement de base, les groupes $H^2(X', \mathbb{Z}/\ell\mathbb{Z})$ sont nuls pour tout ℓ -revêtement X' de X . \square

1.3.7. Proposition. *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 le lemme précédent, on se ramène au cas particulier où \mathcal{C} est une gerbe de toiseurs 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, XIII.§2]) et résulte d'ailleurs de la démonstration ci-dessous.

Montrons que pour tout champ \mathcal{C} comme dans l'énoncé, le faisceau $\pi_0(f_*\mathcal{C})$ est ℓ -monodromique. Traitons 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 $S_{\text{ét}}$ 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, chap. 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. prop. 23]). Or, on a la suite exacte (Leray)

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

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 $R^1f_*\mathbb{Z}/\ell\mathbb{Z}$ est constant sur S (par hypothèse sur f) de sorte que $H^0(S, R^1f_*\mathbb{Z}/\ell\mathbb{Z}) = H^1(X \times_S S_{(s)}, \mathbb{Z}/\ell\mathbb{Z})$. Considérons maintenant le cas d'un champ ℓ -monodromique général ; d'après ce qui précède, on peut supposer – quitte à faire un ℓ -revêtement de S – le faisceau $f_*\pi_0(\mathcal{C})$ constant et, enfin, que le champ considéré est une gerbe (ℓ -monodromique) \mathcal{G} . Soit \mathcal{G}' son quotient par le centre Z de \mathcal{G} (1.2.3). Notons $\mathcal{L} = \pi_0(f_*\mathcal{G})$ et $\mathcal{L}' = \pi_0(f_*\mathcal{G}')$. Rappelons ([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, le groupe abélien $H^1(X, Z)$ agit sur $H^1(X, G)$ par produit contracté, c'est-à-dire par $[T] \cdot [P] = [T \overset{Z}{\wedge} P]$, et l'application $H^1(X, Z) \backslash H^1(X, G) \rightarrow H^1(X, G')$, de source le quotient à gauche de $H^1(X, G)$ par $H^1(X, Z)$, est injective. En faisceautisant, on obtient : le faisceau en groupes abéliens R^1f_*Z agit sur le morphisme (localement constant) canonique $\mathcal{L} \rightarrow \mathcal{L}'$ et l'action est transitive sur les fibres : $(R^1f_*Z) \backslash \mathcal{L} \rightarrow \mathcal{L}'$ est injective. Procédant par récurrence, on peut supposer \mathcal{L}' et R^1f_*Z constants. 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 1.2.5. On vérifie en effet que le morphisme $f^*\mathcal{G} \rightarrow \mathcal{G}$ 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 4, 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 $\text{Id} \rightarrow \text{R}\rho_{\star}\rho^{\star}$ 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 $\mathcal{L}_f \rightarrow \text{R}\rho_{\star}\rho^{\star}\mathcal{L}_f$ 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 $\text{R}\Gamma(\pi_1(X, x), \mathcal{L}_x) \rightarrow \text{R}\Gamma(X, \mathcal{L})$ est un isomorphisme. La réciproque est vraie lorsque 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 est, sur chaque composante connexe, 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 4, IX.1.1]) \mathcal{L}_{ℓ} sur $X_{\ell\text{ét}}$, l'unité d'adjonction $\mathcal{L}_{\ell} \rightarrow \text{R}\rho_{\ell\star}\rho_{\ell}^{\star}\mathcal{L}_{\ell}$ 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 $\text{R}\Gamma(\pi_1^{\text{pro-}\ell}(X, x), \mathcal{L}_x) \simeq \text{R}\Gamma(X, \mathcal{L})$ 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 $\text{Id} \rightarrow \text{R}\rho_{\ell\star}\rho_{\ell}^{\star}$ est un isomorphisme en degré ≤ 1 pour les faisceaux de ℓ -torsion.)

1.4.7. Proposition. 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

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

est *exacte*. (On omet ici la notation de points bases.) L'exactitude à droite résulte de la surjection $\pi_1(X) \rightarrow \pi_1(Y)$ ([SGA 1, XIII.4.1]). Soit G un ℓ -groupe fini. Rappelons (cf. par exemple [SGA 4, 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, 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} : à une classe $c \in H^0(Y, R^1f_*G)$ 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 $c|_V \in H^0(V, R^1f_*G)$. 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 $f_*\mathbf{B}G$.) D'après 1.2.4, 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, 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 $R\Gamma(\pi_1^{\text{pro-}\ell}(Y, \bar{\eta}), (Rf_*\mathcal{F})_{\bar{\eta}}) \simeq R\Gamma(Y, Rf_*\mathcal{F})$ (cf. 1.4.6) et enfin de l'isomorphisme $(Rf_*\mathcal{F})_{\bar{\eta}} = R\Gamma(X_{\bar{\eta}}, \mathcal{F}) \leftarrow R\Gamma(\pi_1^{\text{pro-}\ell}(X_{\bar{\eta}}), \mathcal{F})$, obtenu par récurrence sur la dimension relative. \square

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 4, 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.

1.4.9. Proposition. *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 [A. J. DE JONG 1996, 4.1], il est localement (par une altération) lisse sur k . D'après [SGA 4, XI.3.3]

(rappelé en 1.3.3), on peut donc supposer 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 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.) 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.

$$\begin{array}{ccccc}
 X & \longleftarrow & X' & \longleftarrow & X'' \\
 f \downarrow & & \square & f' \downarrow & \square & \downarrow f'' \\
 Y & \xleftarrow{h} & Y' & \xleftarrow{\quad} & Y'' \\
 g \downarrow & & \swarrow g' & & \searrow g'' \\
 \text{Spec}(k) & \longleftarrow & & &
 \end{array}$$

□

1.4.10. Notons que l'utilisation du théorème de A. J. de Jong fait perdre l'éventuelle primitive récursivité de notre algorithme (puisque l'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. 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 4, XI.§2-3].

1.4.11. Si k est algébrique séparable sur ${}_0k$ 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 ${}_0k$. 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 . (Les indices sont mis à gauche pour éviter la confusion avec les indices simpliciaux utilisés ci-dessous.)

Nous utiliserons la proposition précédente sous la forme suivante (cf. [SGA 4, V^{bis}.5.1] ou bien [DELIGNE 1974, 5.3.3.1 et §6.2]).

1.4.12. Corollaire. 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 $\text{R}\Gamma(X_{\text{ét}}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow \text{R}\Gamma(\text{Tot } X_{\text{ét}}, \mathbb{Z}/\ell\mathbb{Z})$ 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 $X_{\leq r} \rightarrow X$ provient par extension des scalaires d'une flèche ${}_0X_{\leq r} \rightarrow {}_0X$.

Le dernier point résulte de l'observation 1.4.11 et de la construction des hyperrecouvrements rapée ci-dessous, effectuée sur ${}_0k$. Pour la définition du topos total $\text{Tot } X_{\text{ét}}$, 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 4, 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 degré : la construction décrite en [SGA 4, V^{bis}.5.1.3] (voir aussi [DELIGNE 1974, prop. 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 que tout hyperrecouvrement X_\bullet de X peut être dominé par un hyperrecouvrement (calculable en tout degré) X'_\bullet à composantes des coproduits de polycourbes ℓ -élémentaires. 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 :

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

D'après [SGA 4, 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.

2.1. Théorème. *Soient X un schéma normal, de type fini sur un corps algébriquement clos calculable 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 $\varphi \in \text{Hom}(\pi, G)$, on peut construire explicitement le G -torseur $A_\varphi = \text{Hom}_{\pi\text{-Ens}}(G, L)$ 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/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 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.

2.4.2. Remarque. 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 \overline{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. [HEB 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, chap. 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. ^① 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. [A. J. DE JONG 1996, 4.11-12].) Il résulte de ce qui précède – appliqué à la courbe $X_{\overline{\eta}}$ où $\overline{\eta}$ est un point générique géométrique de S – qu'il existe un S -schéma étale S' intègre 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 $\kappa(\overline{\eta})$ 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 $H^1(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$. Il en résulte que la flèche $H^0(S, R^1 f_* \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^1(X_{\overline{\eta}}, \mathbb{Z}/\ell\mathbb{Z})$ est une injection et, par conséquent, que tout $\mathbb{Z}/\ell\mathbb{Z}$ -torseur sur X trivialisé par $X_{\overline{\eta}}$ provient de S . (Voir aussi 1.3.7 et 1.4.7.) Ceci achève la démonstration du théorème 2.1.

2.7. Remarque. 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, A. SCHMIDT et WINGBERG

^①Cette méthode nous a été suggérée par Ofer Gabber.

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 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 $G^{[n]}$ en §6.

3.1.2. Remarques. 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 $\Phi(H) = \overline{H}^\ell(H, H) \subseteq F(H)$. 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, 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) . 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 , le nombre premier ℓ étant sous-entendu. 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 $X_{\ell\text{ét}} \rightarrow X_{\ell\text{ét}}^{(n)}$ s'identifie au morphisme de topos $\mathbf{B}\pi_X \rightarrow \mathbf{B}\pi_X^{(n)}$ déduit de la surjection $\pi_X \twoheadrightarrow \pi_X^{(n)}$: 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, IV.4.5.1]. (On laisse le soin au lecteur de définir $X_{\ell\text{ét}}^{(n)}$ sous des hypothèses plus générales; nous n'en aurons pas usage.) Par construction, pour chaque $n \geq 2$, le topos $X_{\ell\text{ét}}^{(n)}$ 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* $\Pi_X^{(n)}$.

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 $\text{Aut}_X(X_c^{[n]})$. 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 4, IV.11.3.1].

3.3. Calculabilité de $X^{[n]}$.

3.3.1. Soient k un corps algébriquement clos calculable 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 $X^{[n]}$).

3.3.2. Remarque. 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 pro-générateurs).

3.3.4. Récurrence 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, 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 functorielle, on ne peut espérer choisir $X^{[n]}$ functoriellement en X . Plus abstraitement, ceci est lié au fait que, comme $X \rightsquigarrow X_{\text{ét}}$ (cf. p. ex. [SGA 4, VII.1.4]), la construction $X \rightsquigarrow X_{\ell\text{ét}}^{(n)}$ définit seulement un *pseudo*-foncteur ([SGA 1, VI.§8] ou [BORCEUX 1994, 7.5.1]) 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 $n \geq 2$ 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 $\Delta_{\leq r}^{\circledast}$ ($r \in \mathbb{N}$) 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 $X_i^{[n]}$ 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 $X_i^{[n]}$ 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 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 1971-1972, VI, §5.1 et §6.2] ou [SGA 4, 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 ≥ 2 . Notons $X_\bullet^{(n)}$ le topos simplicial (c'est-à-dire fibré sur Δ) 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 1971-1972, §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) d'un ensemble $\mathcal{F}_\bullet(U) = \mathcal{F}_i(U)$, functoriellement en un sens que nous ne répétons pas ([ibid., §5.2] ou [DELIGNE 1974, 5.1.7]).

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 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

^①C'est la catégorie des ensembles $\{0, \dots, s\} \subseteq \mathbb{N}$, où $s \leq r$, munis des applications croissantes ; elle est notée (Δ) , dans [DELIGNE 1974, 5.1.1].

fournit un complexe double, la différentielle en i étant la somme alternée usuelle. La cohomologie cherchée est celle du complexe simple associé :

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

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 $\tau_{<r} \mathrm{R}\Gamma(\mathrm{Tot} X_{\bullet}^{(n)}, \mathcal{F}_{\bullet})$ ne dépend que du schéma simplicial tronqué $X_{\bullet \leq r}$ 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 $F_{\bullet \leq r}$ sur $\Delta_{\leq r}^{\mathrm{op}}$ (c'est-à-dire : groupe abélien cosimplicial tronqué $\Delta_{\leq r} \rightarrow \mathrm{Ab}$), les sections globales dérivées $\mathrm{R}\Gamma(\Delta_{\leq r}^{\mathrm{op}}, F_{\bullet \leq r})$ sont calculées par le complexe normalisé $NF_{\bullet \leq r} \in \mathrm{Ob} C^{[0,r]}(\mathrm{Ab})$ 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 $X_{\bullet \leq r}$ est un k -schéma algébrique tronqué et $\mathcal{F}_{\bullet \leq r}$ est un faisceau sur $\mathrm{Tot} X_{\bullet \leq r}^{(n)}$, on en déduit en poussant par $X_{\bullet \leq r}^{(n)} \rightarrow \Delta_{\leq r}$ que pour toute résolution $\mathcal{F}_{\bullet \leq r}^{\star}$ à $\mathcal{F}_{i \leq r}^j$ acycliques sur $X_i^{(n)}$, on a

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

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, [ibid., 3.22].

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

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

de sorte qu'en particulier la flèche

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

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 $\mathrm{H}^i(\mathrm{Tot} X_{\bullet \leq r}^{(n)}, \mathcal{F}_{\bullet \leq r})$ lorsque les objets sont donnés explicitement.

4.2.1. On reprend les notations de 4.1.1 et l'on suppose chacun des étales 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 $u_{i \star} E$, 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 $\mathcal{F}_{\bullet \leq r} \in \text{Ob Tot } X_{\bullet \leq r}^{(n)}$, le morphisme d'adjonction $\mathcal{F}_{\bullet \leq r} \rightarrow \mathcal{G}_{\bullet \leq r} := u_{\bullet \leq r} \star u_{\bullet \leq r}^* \mathcal{F}_{\bullet \leq r}$ 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 : $\tau_{< d} \text{RG}(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda) = \tau_{j < d} \text{Tot } N_i \Gamma(X_i, \mathcal{F}_i^j)$. Pour calculer la cohomologie de $\text{Tot } X_{\bullet \leq r}^{(n)}$ 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 $X_{\bullet \leq r}$.

4.2.4. Remarque. 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 functorielle en n en un sens évident : une fois choisi $P_{\bullet \leq r} \rightarrow X_{P_{\bullet \leq r}}^{[n]^\circ}$ comme ci-dessus, on a pour tout $m \leq n$ un choix naturel de $P_{\bullet \leq r} \rightarrow X_{P_{\bullet \leq r}}^{[m]^\circ}$, 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 $\text{Tot } X_{\bullet \leq r} \rightarrow \text{Tot } X_{\bullet \leq r}^{(?)}$.

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 $\text{Top } X_{\bullet \leq r}^{(n)} \rightarrow \text{Top } Y_{\bullet \leq r}^{(n)}$.

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

4.3. Proposition. Soient k un corps algébriquement clos calculable, 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 $d \geq 0$, $n \geq m \geq 2$, on peut calculer le complexe $\tau_{\leq d} \text{RG}(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda)$ et la flèche $\tau_{\leq d} \text{RG}(\text{Tot } X_{\bullet \leq r}^{(m)}, \Lambda) \rightarrow \tau_{\leq d} \text{RG}(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda)$. 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 $\tau_{\leq d} \text{RG}(\text{Tot } Y_{\bullet \leq r}^{(n)}, \Lambda) \rightarrow \tau_{\leq d} \text{RG}(\text{Tot } X_{\bullet \leq r}^{(n)}, \Lambda)$.

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.

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} indicé 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 *noëthérien*, il existe un j tel que $A(j, \infty) = A_\infty$; si de plus A_j est *noëthérien*, il existe un $k \geq j$ tel que $A(j, k) \simeq A(j, \infty) = A_\infty$.

5.2. Définition. 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} , indicé 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 $\varphi : \mathbb{N}_{\geq i_0} \rightarrow \mathbb{N}$ une fonction telle que $\varphi(j) \geq j$ pour tout $j \in \mathbb{N}_{\geq i_0}$. On dit qu’un système inductif $A_{\bullet \geq i_0}$ est ***(N, φ)-essentiellement constant*** si :

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

Explicitement : (i) $\text{Ker}(A_j \rightarrow A_{\varphi(j)}) \simeq \text{Ker}(A_j \rightarrow A_k)$ pour $k \geq \varphi(j)$ et (ii) $\text{Im}(A_N \rightarrow A_{\varphi(j)}) \simeq \text{Im}(A_j \rightarrow A_{\varphi(j)})$ 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 *noëthériens* et à colimite *noëthérienne*, 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]^①.

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. [ibid., 8.6.11]).

5.6. Proposition. 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 $m \geq \varphi(n)$ s’annule en particulier dans A_m (d’après la même condition sur (A_n)) donc s’annule dans $A_{\varphi(n)}$ donc dans $A'_{\varphi(n)}$. Soit maintenant $N' = \varphi''(N)$ (qui est supérieur ou égal à N) : si x appartient à A'_n , son image dans $A'_{\varphi(n)}$ vue dans $A_{\varphi(n)}$ 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 $A''_{\varphi(n)}$, c’est-à-dire appartient à $\text{Ker}(A''_N \rightarrow A''_{\varphi(n)})$, 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 $A'_{\varphi(n)}$ que l’élément

^①Nous remercions Luc Illusie de nous avoir communiqué cette référence.

x qu'on s'était fixé. On a donc montré que le système (A'_n) était (N', φ) -essentiellement constant (pour $N' = \varphi''(N)$).

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 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 $A'_{\varphi'(m)}$; alors $y' := y - x_0$ (vu comme élément de A_n) a une image nulle dans $A_{\varphi'(m)}$: donc l'image de y' dans $A_{\varphi(n)}$ est déjà nulle (d'après la première condition sur (A_n)), mais ceci implique que l'image de z dans $A''_{\varphi(n)}$ est nulle. Ceci montre la première condition pour (A''_n) , pour la fonction φ'' égale à $\max(\varphi, N')$. 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 $A_{\varphi(n)}$, et alors l'image \tilde{z} de \tilde{y} dans A''_N a la même image que z dans $A''_{\varphi(n)}$. On a donc montré que le système (A''_n) était (N, φ'') -essentiellement constant (pour $\varphi'' = \max(\varphi, N')$).

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 $A''_{\varphi''(n)}$ (d'après la première propriété sur (A''_n)) ; donc l'image de y dans $A_{\varphi(n)}$ provient d'un élément x de $A'_{\varphi''(n)}$; si $m \geq \varphi''(n)$, l'image de x dans A'_m s'annule et s'annule donc déjà (d'après la première propriété sur (A'_n)) dans $A'_{\varphi'(\varphi''(n))}$. Ceci montre la première condition sur (A_n) pour la fonction $\varphi : n \mapsto \varphi'(\varphi''(n))$. Enfin, soit $y \in A_n$: son image dans A''_n a la même image dans $A''_{\varphi''(n)}$ 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 $A_{\varphi(n)}$, donc la différence entre ces images provient d'un élément $x \in A'_{\varphi''(n)}$; ce dernier a la même image dans $A'_{\varphi(n)} = A'_{\varphi'(\varphi''(n))}$ 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 $A_{\varphi(n)}$ est la même que celle de y . On a donc montré que le système (A_n) était (N, φ) -essentiellement constant pour $\varphi = \varphi' \circ \varphi''$ 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 (indiqué 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, 0_{III}-§11.1], on considère que cet objet filtré de \mathcal{A} fait partie de la donnée.)

5.8. Corollaire. 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.* \square

5.9. Proposition. Soient $\mathbf{A} \rightarrow \mathbf{B}$, un morphisme de systèmes inductifs et $\tau : \mathbb{N} \rightarrow \mathbb{N}$ une fonction strictement croissante. Supposons qu'il existe un diagramme commutatif

$$\begin{array}{ccc} \mathbf{A}_\bullet & \longrightarrow & \mathbf{B}_\bullet \\ \downarrow & \searrow^{h_\bullet} & \downarrow \\ \mathbf{A}_{\tau(\bullet)} & \longrightarrow & \mathbf{B}_{\tau(\bullet)} \end{array}$$

Alors, si \mathbf{B}_\bullet est (N, φ) -essentiellement constant, le système inductif \mathbf{A}_\bullet est $(\tau N, \tau \varphi)$ -essentiellement constant. En particulier, lorsque τ est calculable, le système inductif \mathbf{A}_\bullet est explicitement essentiellement constant si \mathbf{B}_\bullet l'est.

Démonstration. Soit j un entier. Remplaçons, dans le carré commutatif de l'énoncé, le système inductif \mathbf{A}_\bullet (resp. \mathbf{B}_\bullet , etc.) par le système $\mathbf{A}'_\bullet := \mathbf{A}(j, \bullet \geq \varphi(j))$ – à morphismes de transition épimorphiques – (resp. $\mathbf{B}'_\bullet := \mathbf{B}(j, \bullet \geq \varphi(j))$ – constant par hypothèse –, etc.). La commutativité du diagramme montre alors que h'_\bullet est un isomorphisme ; le système inductif $(\mathbf{A}'_k)_{k \geq \varphi(j)}$ est donc constant

pour $k \geq \tau\varphi(j)$. Posons $\psi = \tau\varphi$. Le même argument, appliqué à $A_j'' := A(j, \psi(j))_j$, etc. montre que ce système est constant pour $j \geq \tau(N)$. (On utilise le fait que B est (N, ψ) -essentiellement constant car $\psi \geq \varphi$.) \square

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).

6.1. Lemme. *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 $\psi_\ell(d, n) = \ell^{(d+1)^n}$ convient.

Démonstration. Pour ce qui est de φ : il n'existe qu'un nombre fini de groupes d'ordre $\leq n$ (et en particulier, de ℓ -groupes d'ordre $\leq n$), de sorte qu'il est possible de les énumérer effectivement. Comme pour chaque ℓ -groupe fini on peut trouver un r tel que $F^r\pi = 1$ (cf. [NEUKIRCH, A. SCHMIDT et WINGBERG 2000, proposition 3.8.2]), on peut trouver un r qui convient pour tous.

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 $N = F^rL$ et par récurrence sur r on en déduit $(L : F^rL) \leq \ell^{(d+1)^r}$ (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 $L/F^nL \twoheadrightarrow \pi$, 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 $L^{(\leq n)}$ et un système compatible de d générateurs.

6.3. Proposition (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 $z * x = s(z)x s(z)^{-1}$, et $\pi = \pi' \rtimes_* \pi''$.

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 $(\pi'/F^n \pi') = (\pi'/F^n \pi') \rtimes_{\ast} \pi''$ 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 \ast) 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, A. 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 $\varphi(\psi(d', n)!) \equiv 1$ 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 $(\pi'/F^n \pi')/s(F^m \pi'') = (\pi'/F^n \pi') \rtimes_{\ast} (\pi''/F^m \pi'')$ pour cette action quotientée.

Notons $\bar{\pi}$ ce ℓ -groupe fini $\pi/((F^n \pi') \cdot s(F^m \pi'')) = (\pi'/F^n \pi') \rtimes_{\ast} (\pi''/F^m \pi'')$. Son ordre est majoré par $\psi(d', n) \times \psi(d'', m)$ (et rappelons que $m = \varphi(\psi(d', n)!) \equiv 1$ convient).

Il existe alors $N \geq n, m$ tel que $F^N \bar{\pi} = 1$: précisément, $\varphi(\psi(d', n) \times \psi(d'', m)) \equiv 1$ 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. \square

6.4. Corollaire. *On reprend les hypothèses et les notations de la proposition. Soient $\tilde{\pi}^{(n)} = \pi'/(F^n \pi')$ 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)

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

et de 5.9. \square

6.5. Proposition. *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 $\varphi = \text{Id}$. (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 $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ telle que $H^i(L^{(n)}, V) \rightarrow H^i(L^{(\varphi(n))}, V)$ 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.

□

6.6. Remarque. 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.

Notons qu'il serait intéressant de calculer la plus petite fonction φ telle que les flèches $H^i(L^{(n)}, \mathbb{Z}/\ell\mathbb{Z}) \rightarrow H^i(L^{(\varphi(d,i,n))}, \mathbb{Z}/\ell\mathbb{Z})$ soient nulles. Lorsque $d = 1$ (cas d'un pro- ℓ -groupe abélien libre) ou bien lorsque $i = 2$, on peut vérifier que la fonction $n \mapsto n + 1$ convient (cf. [SERRE 2013] pour le dernier cas).

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 calculable, 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. L'objectif de cette section est de montrer que pour chaque ℓ -groupe abélien fini Λ et chaque $d \geq 0$ on peut déterminer (N_d, φ_d) tels que le système inductif $(H^d(\pi^{(n)}, \Lambda))_{n \geq 0}$ — dont $H^d(X, \Lambda)$ est la colimite — est (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 $\varphi : \mathbb{N} \rightarrow \mathbb{N}$ tels que $(V_n)_n$ soit (N, φ) -essentiellement constant; en particulier, le morphisme $(V_n)_{n \geq N} \rightarrow (V_{\varphi(n)})_{n \geq N}$ se factorise à travers le morphisme $(V_n)_n \rightarrow (V_n)_n$, où $(V_n)_n$ est le système inductif constant de valeur V . Passant à la cohomologie, on en déduit un diagramme commutatif

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

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

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

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

que l'on approxime par

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

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

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

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 :

$$\begin{array}{ccccccc} \pi = \pi^{(0)} & & \pi^{(1)} & & \dots & & \pi^{(m-2)} & & \pi^{(m-1)} \\ \\ \begin{array}{c} X_m \\ \downarrow \\ X_{m-1} \\ \vdots \\ \downarrow \\ X_1 \\ \downarrow \pi''^{(0)} \\ \text{Spec } k \end{array} & & \begin{array}{c} X_{m-1}^{(1)} \\ \downarrow \\ X_{m-2}^{(1)} \\ \vdots \\ \downarrow \pi''^{(1)} \\ \text{Spec } k^{(1)} \end{array} & & \dots & & \begin{array}{c} X_2^{(m-2)} \\ \downarrow \\ X_1^{(m-2)} \\ \downarrow \pi''^{(m-2)} \\ \text{Spec } k^{(m-2)} \end{array} & & \begin{array}{c} X_1^{(m-1)} \\ \downarrow \pi''^{(m-1)} = \pi^{(m-1)} \\ \text{Spec } k^{(m-1)} \end{array} \end{array}$$

Si $X = X_m \rightarrow X_{m-1} \rightarrow \cdots \rightarrow X_1 \rightarrow \text{Spec } k$ est la polycourbe ℓ -élémentaire de départ, on appelle $X_{m-i}^{(i)} \rightarrow X_{m-i-1}^{(i)} \rightarrow \cdots \rightarrow X_1^{(i)} \rightarrow \text{Spec } k^{(i)}$ 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 calculable, 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 :

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

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 1971-1972, 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) $X_{\leq r}$ 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 « $\ell\text{ét}$ » et « ét ».

Pour chaque entier $\lambda \geq 2$, on a une suite spectrale ([ibid., VI.6.2.3.2])

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

où les topos $X_i^{(\lambda)}$ sont comme définis en 3.2. Il résulte donc de l'exactitude des colimites filtrantes ([ÉGA III₁, 0.11.1.8]) et des isomorphismes $\text{colim}_\lambda H^j(X_i^{(\lambda)}, \Lambda) \simeq H^j(X_i, \Lambda)$, 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 $(N_\infty, \varphi_\infty)$ tels que le système inductif $H^d(\text{Tot } X_\bullet^{(\lambda)}, \Lambda)$ soit $(N_\infty, \varphi_\infty)$ -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 $H^d(\text{Tot } X_\bullet^{(\mu)}, \Lambda) \simeq H^d(\text{Tot } X_{\leq \mu}^{(\mu)}, \Lambda)$, 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.

9. FONCTORIALITÉ

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

9.1.1. Soient k un corps algébriquement clos calculable, $f : Y \rightarrow X$ 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

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

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

9.1.3. 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 $H^n(f_i, \Lambda)$ relativement à de *mêmes* présentations explicites de $H^n(X, \Lambda)$ et $H^n(Y, \Lambda)$. Il résulte en effet de 1.4.12 et 1.4.13 qu'il existe pour chaque $\alpha \in \{1, \dots, r\}$ un morphisme $Y_{\alpha} \rightarrow X_{\alpha}$ comme en *loc. cit.* au-dessus de f_{α} . En considérant le produit fibré des Y_{α} 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 α* . La conclusion en résulte aussitôt.

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. Compte-tenu de notre description de la cohomologie de X et de l'énoncé 1.4.12, notre problème se ramène au suivant : calculer, pour chaque entier n , l'action de $\text{Gal}(k/{}_0k)$ sur le complexe $\tau_{<d}\text{R}\Gamma(\text{Tot } X_{\leq r}^{(n)}, \Lambda)$, où d et r sont des entiers arbitraires et $X_{\leq r}$ est un schéma simplicial tronqué explicite de k -schémas de type fini normaux, provenant par extension des scalaires d'un ${}_0k$ -schéma simplicial tronqué ${}_0X_{\leq r}$. D'après 4.2, on peut calculer (ou produire par recherche non bornée, cf. 4.2.3) une injection $\Lambda \hookrightarrow \mathcal{F} = \mathcal{F}_{\leq r}$, où les \mathcal{F}_i sont des faisceaux induits sur X_i (3.2.6). Il existe une extension finie (nécessairement étale) ${}_1k$ de ${}_0k$ telle que $\Lambda \hookrightarrow \mathcal{F}$ se descende en $\Lambda \hookrightarrow {}_1\mathcal{F}$, où ${}_1\mathcal{F}$ est un faisceau sur le topos total *étale* de ${}_1X_{\leq r}$; on peut calculer ${}_1k$ et ${}_1\mathcal{F}$, par exemple en passant au schéma simplicial tronqué représentant \mathcal{F} .

9.2.3. Rappelons que si $\pi : Y \rightarrow X$ est un morphisme fini étale, tout faisceau d'ensembles localement constant constructible \mathcal{L} sur un schéma Y se plonge dans un faisceau localement constant constructible \mathcal{M} défini sur X : considérer la flèche d'adjonction $\mathcal{L} \rightarrow \pi^! \pi_! \mathcal{L}$. Si \mathcal{L} est représenté par le Y -schéma Y' , le faisceau \mathcal{M} est représenté par $Y' \times_X Y$ et la flèche $\mathcal{L} \rightarrow \mathcal{M}$ correspond à la flèche évidente $Y' \rightarrow Y' \times_X Y$. Il résulte de cette observation (et de son caractère fonctoriel), appliquée aux morphismes ${}_1X_i \rightarrow {}_0X_i$ pour $i \leq r$ et aux faisceaux \mathcal{F}_i , que l'on peut supposer \mathcal{F} défini sur ${}_0X_{\leq r}$. On peut donc calculer une résolution tronquée $\Lambda \rightarrow \mathcal{F}_{\leq r}^{\leq d}$ définie sur ${}_0X_{\leq r}$ telle que $\tau_{<d}\text{R}\Gamma(\text{Tot } X_{\leq r}^{(n)}, \Lambda) = \tau_{<d} \text{Tot } N_i \Gamma(X_i, \mathcal{F}_i^j)$. L'action du groupe de Galois $\text{Gal}(k/{}_0k)$ sur le terme de gauche est donnée par l'action évidente et calculable de ce même groupe sur chacun des ensembles finis $\Gamma(X_i, \mathcal{F}_i^j)$. En particulier, on peut déterminer une extension étale ${}_1k$ de ${}_0k$ à travers laquelle cette action se factorise — il suffit que les sections $\Gamma(X_i, \mathcal{F}_i^j)$ soient définies sur ${}_1k$ —, et calculer l'action du quotient $\Gamma = \text{Gal}({}_1k/{}_0k)$. Rappelons que 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

Expliquons 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 – 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 $n \geq 2$, et pour tout k -schéma algébrique normal Y , un revêtement ℓ -étales n -approché universel $Y^{[n]}$, ainsi que le groupe de Galois correspondant $\pi_Y^{[n]}$.

D'après §4, on sait calculer, pour chaque niveau d'approximation fini $n \geq 2$, le groupe $H^d(\text{Tot } X_\bullet^{(n)}, \Lambda)$ (isomorphe à $H^d(\text{Tot } X_{\leq r}^{(n)}, \Lambda)$ 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.

11. COMPLÉMENTS

On considère ici quelques résultats qui sont des prolongements naturels de notre théorème principal et on énonce en 11.4 quelques questions, dont certaines sont probablement hors de portée. Cette section se termine (11.5) par quelques précisions sur la nature des algorithmes que l'on espère pouvoir obtenir.

Ci-dessous k est un corps algébriquement clos calculable (12.1) et Λ un anneau commutatif fini de cardinal inversible sur k .

11.1. Cohomologie d'un schéma simplicial. Soit X , un k -schéma algébrique simplicial. D'après [DELIGNE 1974, §6.4] et les résultats de §1.4, il existe un hyperrecouvrement $X_\bullet \rightarrow X$ par des polycourbes ℓ -élémentaires tel que $H^*(X_\bullet, \Lambda) = H^*(X, \Lambda)$. 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 ([ibid., 6.4.2.2] ou [ILLUSIE 1971-1972, I.§1.2]), on a $\text{RG}(X_\bullet, \Lambda) = \text{RG}(\delta X_\bullet, \Lambda)$, où δX_\bullet est le schéma simplicial *diagonal* déduit de X_\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).

11.2. Cohomologie relative. On présente ici deux constructions de la cohomologie relative : 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.

11.2.1. Cône d'un morphisme simplicial. Soit $f_\bullet : Y_\bullet \rightarrow X_\bullet$ un morphisme de topos simpliciaux (dont on notera $\text{Tot } f_\bullet : \text{Tot } Y_\bullet \rightarrow \text{Tot } X_\bullet$ 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_\bullet 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 $Cf_\varphi : Cf_m \rightarrow Cf_n$ déduit d'une application croissante $\varphi : [n] = \{0, \dots, n\} \rightarrow [m] = \{0, \dots, m\}$. 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 $\varphi_\mu : [\nu] \rightarrow [\mu]$ 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 . 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 $\varphi_\bullet : \mathcal{F}_\bullet \rightarrow \mathcal{G}_\bullet$ un f_\bullet -morphisme entre faisceaux abéliens \mathcal{F}_\bullet sur $\text{Tot } X_\bullet$ et \mathcal{G}_\bullet sur $\text{Tot } Y_\bullet$, c'est-à-dire un morphisme $f_\bullet^* \mathcal{F}_\bullet \rightarrow \mathcal{G}_\bullet$, un objet du topos flèche $\text{Fl}(\text{Tot } f_\bullet)$. 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 »^①, permettent de définir un faisceau abélien simplicial sur $\text{Tot } Cf_\bullet$, cône de φ_\bullet , que nous notons $C\varphi_\bullet$. (Notons que l'objet final de cette catégorie de paires est le faisceau nul sur e .)

11.2.2. La cohomologie relative de $\text{Tot } X_\bullet$, modulo $\text{Tot } Y_\bullet$, est un cas particulier de celle définie, pour tout morphisme $S \rightarrow T$ de topos, en [ILLUSIE 1971-1972, III.§4] (voir aussi [DELIGNE 1980, §4.3.4]). On la note $\text{R}\Gamma(\text{Tot } X_\bullet / \text{Tot } Y_\bullet, \varphi_\bullet)$; ce n'est en général *pas* la cohomologie de $\text{Fl}(\text{Tot } f_\bullet)$ à valeurs dans φ_\bullet . (Cette dernière étant isomorphe à $\text{R}\Gamma(\text{Tot } X_\bullet, \mathcal{F}_\bullet)$ d'après [ILLUSIE 1971-1972, III.4.2].) Implicite en [DELIGNE 1974, §6.3] est la formule suivante :

$$(\star) \quad \text{R}\Gamma(\text{Tot } X_\bullet / \text{Tot } Y_\bullet, \varphi_\bullet) = \text{R}\Gamma(\text{Tot } Cf_\bullet, C\varphi_\bullet).$$

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 $\text{Ker } H^0(\text{Tot } X_\bullet, \mathcal{F}_\bullet) \rightarrow H^0(\text{Tot } Y_\bullet, \mathcal{G}_\bullet)$.

11.2.3. Justifions brièvement (\star) . Notons \mathcal{R} le topos $\text{Fl}(\text{Tot } f_\bullet)$ et \mathcal{E} le topos $\text{Tot } Cf_\bullet$. Il n'y a pas de morphisme naturel $\mathcal{E} \rightarrow \mathcal{R}$ – comme on le voit par exemple en considérant l'unique endomorphisme du topos simplicial vide – mais un morphisme $a : \mathcal{E}^\times \rightarrow \mathcal{R}$, où \mathcal{E}^\times est le *sous-topos ouvert* de \mathcal{E} , défini par la condition : $i^\star = \emptyset$, où $i : \text{Fl}(e_\bullet) \rightarrow \mathcal{E}$ 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 $j : \mathcal{E}^\times \hookrightarrow \mathcal{E}$, on vérifie sans peine l'égalité $C\varphi_\bullet = j_! a^\star \varphi_\bullet$ 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** l'on peut calculer le groupe de cohomologie étale $H^i(X/Y, \Lambda)$: c'est $H^i(Cf_\bullet, C\Lambda_\bullet)$. 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 $U = X - F$:

$$H_c^i(U, \Lambda) = H^i(X/F, \Lambda).$$

11.2.5. Esquissons une autre approche du calcul de la cohomologie de X relative à un fermé F . Notons $Y = X \amalg_F X$ la somme amalgamée (pincement) de deux copies de X le long de F ; si $X = \text{Spec}(A)$ et $F = \text{Spec}(A/I)$, le schéma Y 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 Y , et i l'immersion fermée de F dans Y . 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

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

calcule la cohomologie $\text{R}\Gamma(Y, \Lambda)$ de Y (« 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 $\text{R}\Gamma(X, \Lambda) \oplus \text{R}\Gamma(X \text{ mod } F, \Lambda)$. La cohomologie de $X \text{ mod } F$ se déduit donc fonctoriellement de la cohomologie (usuelle) de X et de celle de $X \amalg_F X$.

^①Voir aussi [SGA 4, V^{bis}, 4.3.0].

11.3. 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 $R^i f_* \mathcal{F}$.

11.3.1. 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 4, IV.9.3]), description des générateurs ou cogénérateurs usuels ([SGA 4, IX 2.9 (ii) et 2.14 (ii)]), espaces algébriques ([ARTIN 1973, chap. VII], ou [MILNE 1980, chap. V, §1]). Cette dernière est probablement la plus économique.

11.3.2. Effaçabilité et dévissages. Soient S un schéma noethérien et $f : X \rightarrow S$ un morphisme de type fini. D'après une variante de [SGA 4½, 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 (dédue de l'unité de l'adjonction $\pi^* \dashv \pi_*$)

$$R^n f_* \Lambda \rightarrow R^n f'_* \Lambda,$$

soit nulle, où $f' = f \circ \pi'$.

11.3.3. Cas d'un morphisme propre. 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 $R^n f_* \Lambda$ et $R^n f'_* \Lambda$ 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 $R^n f_* \Lambda \rightarrow R^n f'_* \Lambda$ 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 0.8 dans le cas particulier où f est *propre*, ou bien lorsque $S = \text{Spec}(k)$.

11.3.4. 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 2011, §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

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

g g'

où :

- a est une altération effaçant la cohomologie de f : la flèche de functorialité $R^i f_{\star} \Lambda \rightarrow R^i g_{\star} \Lambda$ est nulle pour chaque $i > 0$;
- $\tilde{\pi}$ un morphisme fini surjectif effaçant la cohomologie du morphisme *propre* a : la flèche de functorialité $R^{\geq 1} a_{\star} \Lambda \rightarrow R^{\geq 1} b_{\star} \Lambda$ 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

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

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

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

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

11.3.5. Les observations précédentes et le théorème de résolution des singularités [A. J. 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

$$\begin{array}{ccc}
 X & \xleftarrow{a} & X' \\
 \downarrow j & \nearrow k & \downarrow j' \\
 \bar{X} & \xleftarrow{\bar{a}} & \bar{X}' \\
 \downarrow \bar{f} & \nearrow \bar{f}' & \\
 S & &
 \end{array}$$

(The diagram is enclosed in a large circle with arrows labeled f on the left and f' on the right, both pointing downwards.)

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

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

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 $R^n \bar{f}'_* \Lambda$; la conclusion est alors immédiate.

Comme au paragraphe précédent (11.3.4), il suffit de montrer que l'on peut calculer une altération \bar{a} effaçant $R^{\geq 1} j_* \Lambda$, c'est-à-dire telle que le morphisme $R^{\geq 1} j_* \Lambda \rightarrow R^{\geq 1} k_* \Lambda$ soit nul. En effet, on a sous cette hypothèse un diagramme commutatif et une factorisation

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

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

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

désiré. Pour effacer $R^{\geq 1} j_* \Lambda$, il suffit – par itération, cf. 11.3.4, premier paragraphe – de savoir effacer chaque $R^i j_* \Lambda$ 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 $R^i j_* \Lambda$. 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 $R^i j_* \Lambda \rightarrow R^i k_* \Lambda$ 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 0.8.

11.4. Questions.

11.4.1. Calculer la cohomologie d'espaces algébriques au sens d'Artin.

11.4.2. Déterminer la structure d'algèbre de $H^*(X, \Lambda)$.

11.4.3. Construire les morphismes « trace » et la « classe de cycle » dans le cas d'un schéma X lisse sur k .

11.4.4. (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 toute élément de $H^*(X_s, A)$ se relève à X_U .

11.4.5. Calculer $H^i(X, \mathcal{K})$ où \mathcal{K} est un complexe borné constructible de A -modules.

11.4.6. Calculer le *complexe* $R\Gamma(X, A)$, voire $R\Gamma(X, \mathcal{K})$ pour \mathcal{K} un complexe borné constructible de A -modules. Variante relative : étendre le théorème **0.8** au calcul de $Rf_{\star} \mathcal{K}$.

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

11.5. Primitive récursivité, ou existence de bornes algorithmiques. Comme nous l'avons signalé en **0.9** (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* : cf. [ODIFREDDI 1989, définition I.1.6 et proposition I.5.8] ; il revient au même de dire qu'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]. (Pour une description agréable à lire de la différence entre fonctions primitivement récursives et générales récursives, on pourra aussi consulter la discussion comparant les langages de programmation « BlooP » et « FlooP » dans [HOFSTADTER 1999, chapitre XIII].) Les fonctions que nous calculons sont vraisemblablement même « élémentaires » au sens de Kalmár, c'est-à-dire de temps d'exécution borné par une tour d'exponentielles, cf. [ODIFREDDI 1999, définition VIII.7.1].

Cette supposition est motivée, entre autres, par un slogan proposé par certains logiciens, cf. [AVIGAD 2003, « grand conjecture » page 258], selon lequel tout théorème mathématique « ordinaire », qui peut s'énoncer dans le langage de l'arithmétique, est en fait prouvable dans des systèmes formels très faibles qui, dès qu'ils prouvent qu'un algorithme termine, prouvent en fait que celui-ci appartient à une des classes citées ci-dessus (on pense notamment au système PRA, « Primitive Recursive Arithmetic », défini par exemple en [S. G. 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. [ibid., théorème 2.2 et remarque qui suit]) : si notre théorème (qui affirme 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 autant 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 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 4, XI.§2-3], le cas général nécessiterait aussi de revoir les résultats de [A. J. 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.

12. CORPS ET EXTENSIONS DE CORPS

12.1. Définition. 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 $(^{-1})_{\mathfrak{K}} : \{z \in \mathfrak{K} : z \neq 0_{\mathfrak{K}}\} \rightarrow \mathfrak{K}$, 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** 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 $y \in L$, décide s'il existe x tel que $f(x) \equiv_{\mathfrak{L}} y$ (et, cf. 12.8, on peut alors supposer^① qu'elle calcule ce x), alors on dit que K est un sous-corps calculable **reconnaissable** de L (ou que L est une extension calculable reconnaissable de K).

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

12.2. Remarques. (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{K} en tant que partie de \mathbb{N} — de chaque classe d'équivalence, on peut omettre la relation d'équivalence et demander directement que \mathfrak{K} soit une partie récursive de \mathbb{N} munie d'opérations qui en font un corps); celle proposée ci-dessus (équivalente à celle de [ibid., 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{K} 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 a un algorithme de factorisation.

^①Ce serait la bonne définition à prendre si on voulait remplacer la notion de calculabilité par celle de fonction primitivement récursive.

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 précédent 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]).

12.3. On rappelle (voir notamment [BOURBAKI 2007, V.§13] ou [ÉGA IV₁, 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).

12.4. Proposition. *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 $\sum_{\underline{i}} \xi_{\underline{i}} b_1^{i_1} \cdots b_r^{i_r}$ 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 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 :

12.4.1. Lemme. *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 :

12.5. Proposition. *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 ^①clôture 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 .

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).

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. [ibid., 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 ^②, 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. [ibid., lemme 2.7.3]).

^①On 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.

^②Il 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!

(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{Q} 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 $(e, a) \equiv_{\mathfrak{Q}} (e', a')$ (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 $(e, a) \in \mathfrak{Q}$ « canoniques », définis comme ceux pour lesquels $a \notin K^p$ si $e > 0$, convertir un couple $(e, a) \in \mathfrak{Q}$ 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 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

12.6. Remarque. 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 monogènes. 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 [ibid., 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).

12.7. Convention. 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, admettant un algorithme de factorisation (cf. 12.2) et une p -base finie explicite (12.4), l'opération en question est calculable. D'après le résultat qu'on vient de montrer, cette hypothèse n'est guère restrictive. En fait, il faudra même comprendre (ce qui est plus fort, cf. 21.4 et 21.5) que l'opération décrite est calculable au sens du modèle de calcul « universel » présenté dans la partie III.

12.8. Remarque. Le fait de considérer des fonctions récursives (générales, par opposition par exemple aux fonctions primitivement récursives) signifie que si $\mathbf{P}(m, n)$ est une propriété calculable (des entiers naturels) et que pour chaque m il existe n vérifiant $\mathbf{P}(m, n)$, alors la fonction $\mu_n \mathbf{P}$ qui à m associe le plus petit n vérifiant $\mathbf{P}(m, n)$ 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 $\mathbf{P}(m, n)$ 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 $(\cdot^{-1})_{\mathfrak{K}} : \{z \in \mathfrak{K} : z \neq 0_{\mathfrak{K}}\} \rightarrow \mathfrak{K}$ 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 $x \times_{\mathfrak{K}} y \equiv_{\mathfrak{K}} 1_{\mathfrak{K}}$). Notons d'ores et déjà que si on préfère à la notion de corps calculable le modèle de calcul « universel » présenté dans la partie III, bien qu'on ne puisse plus énumérer les « éléments de \mathbb{A}^1 », la possibilité d'effectuer des recherches subsiste grâce aux résultats de la section 23.

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 \mathbf{P} considérée. Ainsi, il découle du théorème de A. J. de Jong sur la résolution des singularités par altérations ([A. J. 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 11.5 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 $\mathbf{P}(m, n)$ 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 $\mathbf{P}(m, n)$ est vrai, sans imposer qu'elle termine quand $\mathbf{P}(m, n)$ n'est pas vrai — on peut alors calculer *un* n vérifiant $\mathbf{P}(m, n)$ (pas nécessairement le plus petit) en lançant en parallèle la vérification de tous les $\mathbf{P}(m, n)$ jusqu'à ce que l'une d'entre elles termine. (Ceci n'est néanmoins pas compatible avec l'invocation de 23 dans le cas du modèle de calcul universel, s'il s'agit d'énumérer des éléments du corps, mais ce type de recherche est surtout utile pour parcourir des entiers n ; nous n'utiliserons de toute façon pas cette opération.)

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 . Les bases de Gröbner permettent de 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 éléments de la base, dont 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]).

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 $P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$ 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 $P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$, 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 $P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$), 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. [ibid., 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. [ibid., §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. [ibid., 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 $P = \text{Coker}(G_P \xrightarrow{\varphi_P} F_P)$ et $Q = \text{Coker}(G_Q \xrightarrow{\varphi_Q} F_Q)$ sont deux R -modules explicitement présentés, on peut calculer une présentation explicite de $P \otimes_R Q$, à savoir $P \otimes_R Q = \text{Coker}((G_P \otimes F_Q) \oplus (F_P \otimes G_Q) \rightarrow F_P \otimes F_Q)$ 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 15.4].)

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 en calculer la troncation à un ordre quelconque d'une résolution libre : 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 de type fini. 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 [T. DE JONG 1998, §3], ou [LOMBARDI ET QUITTÉ 2011, exercice 6.6] dans le cas libre) :

13.6.1. Proposition. *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 $x_ix_j = b_0^{(i,j)} + b_1^{(i,j)}x_1 + \dots + b_n^{(i,j)}x_n$ 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 $T_i T_j$, disons $z = a T_i T_j e + u$ où $a \in A$, où e est un monôme et où u ne fait intervenir que des monômes plus petits que $T_i T_j e$: alors $z' := z + a e q_{i,j}$ 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'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).

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 $\text{Im } \varphi \cong A/\text{Ker } \varphi$ 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).

14.3. Lemme. *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 $A[\frac{1}{f}]$ la k -algèbre $A[T]/(Tf - 1)$ localisée de A en inversant f (et $B[\frac{1}{f}] = B \otimes_A A[\frac{1}{f}]$). Alors l'ensemble des $f \in A$ tels que le morphisme $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ 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 $A[\frac{1}{f}]$, donne $0 \rightarrow N[\frac{1}{f}] \rightarrow A[\frac{1}{f}] \rightarrow B[\frac{1}{f}] \rightarrow Q[\frac{1}{f}] \rightarrow 0$: on voit donc que l'ensemble des f tels que $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ soit injective (resp. surjective, resp. bijective) est l'ensemble des f tels que $N[\frac{1}{f}] = 0$ (resp. $Q[\frac{1}{f}] = 0$, resp. $N[\frac{1}{f}] = 0$ et $Q[\frac{1}{f}] = 0$). Or si M est un A -module, dire de $f \in A$ que $M[\frac{1}{f}] = 0$ 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

14.4. Proposition. *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 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 $A = k[X_1, \dots, X_m]/I$ et $B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$ où $I \subseteq \hat{J}$.

On a déjà expliqué qu'on pouvait 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 $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ soit injectif, soit $N[\frac{1}{f}] = 0$, 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 $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ 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 $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ soit surjectif. \square

Vu au niveau du morphisme de schémas $\text{Spec } B \rightarrow \text{Spec } A$, l'idéal des f tels que $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ 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 $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ 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] :

14.5. Lemme. 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 $A[\frac{1}{f}] \rightarrow B[\frac{1}{f}]$ 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 $A[\frac{1}{f_i}] \rightarrow B[\frac{1}{f_i}]$ 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 $A[\frac{1}{f_i}] \rightarrow B[\frac{1}{f_i}]$ 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 $A = k[X_1, \dots, X_m]/I$ et $B = k[X_1, \dots, X_m, Y_1, \dots, Y_n]/\hat{J}$ 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 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]. (Notons que 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 irredondante, 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 possède 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 possède 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 $f_{u_1} \dots f_{u_i} t^i \in J^i t^i$ sur la classe de $T_{u_1} \dots T_{u_i}$ 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 $\text{gr}_J(R) = (R/J) \oplus (J/J^2)t \oplus (J^2/J^3)t^2 \oplus \dots$ (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 $M[Jt] = M \oplus JMt \oplus J^2Mt^2 \oplus \dots$ comme module sur l'algèbre de Rees $R[Jt]$, ainsi donc que du gradué $\text{gr}_J(M) = (M/JM) \oplus (JM/J^2M)t \oplus \dots$ 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'avoir 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 noëthérien 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], [T. DE JONG 1998], [SINGH et SWANSON 2009] (en caractéristique positive uniquement) et les livres [VASCONCELOS 2005, chap. 6] et [HUNEKE et SWANSON 2006, chap. 15]. Pour la commodité du lecteur, nous rappelons ici brièvement un argument (tiré de [T. 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 $A' \rightarrow K$, $\varphi \mapsto \varphi(i)i^{-1}$, 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 [ibid., §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.

15.5.2. Proposition (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, rem. 1.5], où il est implicitement fait usage du théorème de normalisation de Noether « génériquement étale » ([EISENBUD 1995, cor. 16.18], [ZARISKI et SAMUEL 1975, V.§3, th. 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 ([DRIES et K. 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, th. 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, 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, prop. 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, §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 peut calculer une borne sur le nombre d'étapes pour rendre A régulier en codimension 1^①.

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

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 1971-1972, 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 [ibid., §5.4.5] et [ELKIK 1973, §0.2]

^①Cette technique nous a été suggérée par O. Gabber.

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.

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

15.7.2. Proposition. 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 $T f_i - 1$ 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 $V_{ii'}$ 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 $\varphi_{ii'} : V_{ii'} \rightarrow V_{i'i}$ 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 $\varphi_{ii'}$ 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 $V_{ii'}$ de U_i avec l'ouvert $V_{i'i}$ de $U_{i'}$ au moyen de $\varphi_{ii'}$. 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 de Z une description 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 [ÉGA I, 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 [ÉGA I, 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 $I' = \varphi(I)A'$ 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 [ibid., 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 : ces ouverts sont calculables algorithmiquement d'après ce qu'on vient de dire (il est clair que $F \cap U$ est calculable, au besoin d'après 16.3), ils recouvrent $X \amalg_F X$, et si U, U' sont deux ouverts affines de X , l'ouvert quasi-affine $(U \amalg_V U) \cap (U' \amalg_{V'}, U') = (U \cap U') \amalg_{V \cap V'} (U \cap U')$ se décrit comme réunion des $U'' \amalg_{V''} U''$ pour $U'' \subseteq U \cap U'$ et s'envoie vers $U \amalg_V U$ et $U' \amalg_{V'} U'$ par les morphismes de fonctorialité (cf. ci-dessus). Ceci fournit donc une description de $X \amalg_F X$ au sens de 16.2.

16.5. Immersions ouvertes et isomorphismes de schémas. Donné 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 particulière : 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, 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, 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_{Spr}, 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], cf. aussi 23.1), 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, 5.4.1]), resp. une surjection ([ÉGA IV₁, 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 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 ALGÈBRE 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, 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, 2.5]). Rappelons ([SERRE 1955, ch. III, §4, ¶69, cor. 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 [ibid., ch. III, §3, ¶63, prop. 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 $H^0(X, \mathcal{O}_X) = H^0(\mathbb{P}_k^r, \mathcal{O}_{\mathbb{P}_k^r}/I)$. En particulier, on peut vérifier si la flèche naturelle $k \rightarrow H^0(X, \mathcal{O}_X)$ 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.

III. Modèle de calcul « universel »

MOTIVATION

Le but de cette partie est de présenter un formalisme permettant de définir le concept de fonction calculable sur un corps en évitant de passer par les corps calculables (12.1), et qui conduit à une notion plus restrictive (voir le corollaire 21.4 et la remarque 21.5) qui permet d'obtenir automatiquement des énoncés tels que 0.6.

Ce formalisme se passe d'hypothèse de type « calculabilité » sur les corps, et revient à travailler sur tous les corps algébriquement clos (ou même simplement parfaits) de caractéristique fixée : autrement dit, nous allons définir une notion de fonction calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$. On peut procéder de deux manières, dont nous prouverons l'équivalence.

L'une considère des machines semblables aux machines de Turing qui peuvent manipuler, outre les entiers naturels, les éléments d'un corps (parfait de caractéristique $p \geq 0$) dont elles ne savent rien, sous forme de « boîtes noires » sur lesquelles elles peuvent effectuer les opérations algébriques

(addition, soustraction, multiplication, inverse, Frobenius inverse) et le test d'égalité : c'est ce que nous verrons en 21. C'est cette approche qui permet de se convaincre que les fonctions qu'on a naturellement envie de qualifier de « calculables », et notamment celles qualifiées de telles dans la partie II, sont bien calculables au sens du modèle décrit ici.

L'autre approche (que nous utiliserons essentiellement comme définition en 20.1 et 20.4, et dont on peut trouver un énoncé simple pour les fonctions totales en 22.4) consiste à définir les fonctions calculables par une stratification calculable en parties constructibles de $\mathbb{A}_{\mathbb{F}_p}^n$ sur chacune desquelles la fonction prend une valeur constante (si elle doit renvoyer une valeur dans \mathbb{N}) ou définie par une fonction rationnelle composée avec Frob_p^{-i} (si elle doit renvoyer une valeur dans $\mathbb{A}_{\mathbb{F}_p}^1$). C'est ainsi que, par exemple, savoir calculer si une variété algébrique affine est, disons, géométriquement normale, revient exactement, pour le modèle de calcul ici décrit, à savoir calculer quelles fibres d'un morphisme entre variétés algébriques affines le sont.

Ceci fournit donc un point de vue effectif sur la constructibilité des propriétés géométriques tel qu'exposé en [ÉGA IV₃, §9] (voir notamment [ÉGA IV₃, corollaire 9.9.5]) : *le fait de montrer qu'une propriété géométrique est calculable (dans le sens présenté ici) montre automatiquement qu'elle est constructible* (au moins pour des schémas de type fini).

Les résultats de cette partie ne sont pas difficiles, et peuvent s'approcher soit par la géométrie algébrique classique soit par la théorie des modèles (le point central pouvant reposer sur la compacité de la topologie constructible sur $\mathbb{A}_{\mathbb{F}_p}^n$, cf. 18.3, ou sur le théorème de compacité de la logique du premier ordre ; de même, les résultats de la section 23 peuvent s'expliquer par le théorème de Chevalley ou l'élimination des quantificateurs dans la théorie des corps algébriquement clos). Nous avons cherché à évoquer les deux points de vue, qui se complètent. Chacun des deux serait d'ailleurs sans doute susceptible de généralisations (pour ne pas considérer uniquement des corps mais des schémas arbitraires ou des modèles d'une théorie quelconque qui réalise l'élimination des quantificateurs^①) : nous n'avons pas cherché à poursuivre cette piste mais montrons dans la dernière section (26) comment le modèle peut s'adapter au cas où on ne veut pas fixer la caractéristique p .

On rappelle que l'*exposant caractéristique* d'un corps désigne sa caractéristique lorsque celle-ci est différente de 0, et 1 lorsque la caractéristique est 0.

Nous attirons par ailleurs l'attention du lecteur sur le fait que, nous serons dans cet annexe fréquemment amenés à considérer des fonctions partielles^② : une fonction partielle $f : E \rightarrow F$ est simplement une fonction [totale] $E_0 \rightarrow F$ pour une partie $E_0 \subseteq E$, et on dit que $f(x)$ est *définie* (resp. non définie) si $x \in E_0$ (resp. $x \notin E_0$). Nous avons pris garde à utiliser l'adjectif « partiel » ou « total » pour qualifier les fonctions dès qu'il pouvait y avoir ambiguïté.

18. TYPES ET PARTIES CONSTRUCTIBLES

18.1. Définition. Soit p un nombre premier ou bien 1, et soit \mathbb{F}_p le corps premier de cet exposant caractéristique (c'est-à-dire le corps fini à p éléments si $p > 1$ et \mathbb{Q} lorsque p vaut 1). On appelle **formule booléenne** en les indéterminées X_1, \dots, X_n sur \mathbb{F}_p une combinaison booléenne, c'est-à-dire une combinaison par les connecteurs \wedge (et logique), \vee (ou logique) et \neg (négation logique) d'expressions de la forme $f(X_1, \dots, X_n) = 0$ où $f \in \mathbb{F}_p[X_1, \dots, X_n]$. On dira indifféremment qu'une telle formule est « vraie », « valide », « vérifiée » ou « satisfaite » en des éléments (x_1, \dots, x_n) d'un corps k d'exposant caractéristique p lorsque sa valeur de vérité évaluée sur les éléments en question est vraie.

À une telle formule ϕ on associe une **partie constructible** E_ϕ de l'ensemble $\mathbb{A}_{\mathbb{F}_p}^n$ des idéaux premiers de $\mathbb{F}_p[X_1, \dots, X_n]$ de la manière évidente : c'est-à-dire que la partie associée à $f(X_1, \dots, X_n) = 0$ est le fermé de Zariski ayant cette équation, et les parties associées à des combinaisons par les

^①Un exemple évident serait la théorie des corps réel-clos, correspondant aux fonctions calculables par des machines pouvant en manipuler les éléments dans des boîtes noires permettant les opérations algébriques et la comparaison pour l'ordre : le rôle de $\mathbb{A}_{\mathbb{F}_p}^n$ serait alors joué par l'espace des types de cette théorie.

^②Même si on s'intéresse finalement surtout aux fonctions calculables totales, ici définies en §22, toute définition raisonnable de calculabilité doit nécessairement considérer des fonctions calculables partielles, à cause de l'indécidabilité du problème de l'arrêt : cf. [ODIFREDDI 1989, prop. II.2.1].

connecteurs \wedge, \vee, \neg sont obtenues respectivement par intersection, union et complémentaire des parties associées aux formules connectées. De même, si k est un corps d'exposant caractéristique p , on associe à ϕ une partie (dite constructible) $E_\phi(k)$ de k^n définie de façon analogue : c'est l'ensemble des n -uplets d'éléments de k qui vérifient la formule ϕ .

Par analogie avec le cas de $x \in k^n$ pour k un corps d'exposant caractéristique p (où il y a par définition équivalence entre $x \in E_\phi(k)$ et $\phi(x)$), si $\mathfrak{x} \in \mathbb{A}_{\mathbb{F}_p}^n$ et si ϕ est une formule booléenne, on écrira parfois encore abusivement que \mathfrak{x} vérifie ϕ , ou que $\phi(\mathfrak{x})$ est vraie, pour dire $\mathfrak{x} \in E_\phi$.

On aura parfois tendance à identifier abusivement la partie constructible E_ϕ de $\mathbb{A}_{\mathbb{F}_p}^n$ et le foncteur de même nom qui à un corps k d'exposant caractéristique p (éventuellement supposé algébriquement clos) associe la partie $E_\phi(k)$ de k^n ; cette confusion est bénigne en raison de la proposition suivante :

18.2. Proposition. *Soient φ, ψ deux formules booléennes en les indéterminées X_1, \dots, X_n sur \mathbb{F}_p , soient E et F les parties constructibles de $\mathbb{A}_{\mathbb{F}_p}^n$ qu'elles définissent, et pour tout corps k d'exposant caractéristique p soient $E(k)$ et $F(k)$ les parties constructibles de k^n qu'elles définissent. Il y a équivalence entre :*

- (i) $E \subseteq F$ en tant que parties de $\mathbb{A}_{\mathbb{F}_p}^n$ (i.e., ensembles d'idéaux premiers de $\mathbb{F}_p[X_1, \dots, X_n]$),
- (ii) $E(k) \subseteq F(k)$ pour tout corps k d'exposant caractéristique p ,
- (ii') $E(k) \subseteq F(k)$ pour tout corps k algébriquement clos d'exposant caractéristique p ,
- (iii) l'énoncé $\forall x_1 \dots \forall x_n (\varphi \Rightarrow \psi)$ est un théorème de la théorie des corps d'exposant caractéristique p ,
- (iii') l'énoncé $\forall x_1 \dots \forall x_n (\varphi \Rightarrow \psi)$ est un théorème de la théorie des corps algébriquement clos d'exposant caractéristique p .

On a, bien sûr, les mêmes équivalences en remplaçant partout « \subseteq » par « $=$ » et « \Rightarrow » par « \Leftrightarrow ».

Pour le sens de l'expression «être un théorème de la théorie \mathcal{T} », et la définition des théories considérées, cf. par exemple [FRIED et JARDEN 2008, §8.1, exemple 7.3.1 et chapitre 9]. L'équivalence entre (ii) et (iii) (resp. entre (ii') et (iii')) découle du théorème de complétude de Gödel ([MARKER 2002, théorème 2.1.2] ou [FRIED et JARDEN 2008, corollaire 8.2.6]); les autres équivalences sont de démonstration immédiate.

Il sera souvent commode d'identifier une formule booléenne en n variables en la formule équivalente en $n' > n$ variables (ne faisant pas intervenir les nouvelles variables).

18.3. Les parties constructibles de $\mathbb{A}_{\mathbb{F}_p}^n$ sont la base d'ouverts d'une topologie sur $\mathbb{A}_{\mathbb{F}_p}^n$ plus fine que la topologie de Zariski (puisque tous les fermés de Zariski sont à la fois ouverts et fermés pour cette nouvelle topologie). Celle-ci s'appelle la **topologie constructible** (ou **topologie de Stone**) sur $\mathbb{A}_{\mathbb{F}_p}^n$, qui est alors dans la terminologie des logiciens l'**espace des types** (en n variables, et à coefficients dans \mathbb{F}_p) de la théorie des corps algébriquement clos d'exposant caractéristique p , et cette topologie est *compacte et totalement discontinue* : cf. [ÉGA IV₁, 1.9.15] et [MARKER 2002, lemme 4.1.8 et exemple 4.1.14]. Plus généralement, on peut associer à tout schéma affine $X = \text{Spec}(A)$, un schéma X^{cons} , naturellement isomorphe au spectre de l'anneau absolument plat universel $T(A)$ associé, dont l'espace topologique sous-jacent est l'ensemble X muni de la topologie constructible (cf. [OLIVIER 1966-1968, prop. 5]). Pour chaque $x \in X$, l'anneau local $\mathcal{O}_{X^{\text{cons}}, x}$ est naturellement isomorphe au corps résiduel de x .

18.4. Remarques. Il importe aussi de souligner que la notion de multiplicité n'existe pas ici : les formules booléennes $f = 0$ et $f^2 = 0$ sont toujours équivalentes en ce qu'elles définissent la même partie constructible. Un fermé de Zariski — sans notion de «multiplicité» ni structure de schéma — équivaut à une partie constructible définie par une formule booléenne *positive* (c'est-à-dire sans utiliser la négation logique) : en effet, quitte à utiliser la distributivité de \vee sur \wedge , une telle formule peut s'écrire comme une conjonction de disjonctions ($\bigwedge_i \bigvee_j f_{ij} = 0$, dite aussi «forme normale conjonctive»), or la disjonction $f_{i,1} = 0 \vee \dots \vee f_{i,s} = 0$ équivaut à $f_i := f_{i,1} \dots f_{i,s} = 0$ de sorte que la conjonction de ces clauses définit un fermé de Zariski $f_1 = \dots = f_r = 0$. (La réciproque est claire : le fermé $V(f_1, \dots, f_r)$ est défini par $\bigvee_i f_i = 0$.)

On peut reformuler le fait qu'une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^n$ est réunion finie de parties *localement fermées* (pour la topologie de Zariski) ainsi : toute formule booléenne comme disjonction de formules

purement conjonctives, c'est-à-dire de la forme $f_1 = 0 \wedge \dots \wedge f_r = 0 \wedge g_1 \neq 0 \wedge \dots \wedge g_s \neq 0$; on peut d'ailleurs supposer $s = 1$ quitte à remplacer la fin de la formule par $g_1 \dots g_s \neq 0$. On pourra cette fois parler de « forme normale disjonctive », et on peut réécrire une formule booléenne sous cette forme en utilisant la distributivité de \wedge sur \vee (ainsi que les lois de De Morgan pour traiter la négation).

18.5. Observation. Les formules booléennes sur \mathbb{F}_p peuvent être manipulées par une machine de Turing.

Il est algorithmique de décider si la partie constructible associée à une formule booléenne est vide : en effet, comme expliqué en 18.4, on peut se ramener à une formule purement conjonctive, c'est-à-dire de la forme $f_1 = 0 \wedge \dots \wedge f_r = 0 \wedge g_1 \neq 0 \wedge \dots \wedge g_s \neq 0$, or tester si une telle formule est universellement fautive revient, d'après le Nullstellensatz, à tester si l'un des g_j (ou 1 dans le cas $s = 0$) appartient au radical de l'idéal engendré par les f_i . Ou encore que l'idéal engendré par les f_i et les $1 - yg_j$ contienne 1, où y est une nouvelle variable. Ce fait est décidable, par exemple en utilisant les algorithmes de bases de Gröbner rappelés en 13.1.

Par conséquent, il est décidable de tester l'inclusion ou l'égalité entre deux telles parties constructibles et on peut considérer que les machines de Turing peuvent manipuler directement les parties constructibles (à coefficients dans \mathbb{F}_p).

19. FONCTIONS F-RATIONNELLES

Motivation. Même si le modèle de calcul élaboré ici s'intéresse surtout aux fonctions calculables à valeurs entières, qu'on va définir en 20.1, il est utile (et même indispensable pour pouvoir formuler l'approche « boîtes noires » en 21) de disposer d'une notion de fonctions calculables à valeurs dans $\mathbb{A}_{\mathbb{F}_p}^1$ (c'est-à-dire dans « le corps non spécifié sur lequel on travaille ») : pour cette notion (qui sera définie en 20.4), il est très commode (même si ce n'est pas absolument indispensable) d'admettre l'inverse du Frobenius comme opération calculable — ceci est justifié notamment par le souhait d'obtenir le lien simple entre fonctions à valeurs entières et fonctions à valeurs dans $\mathbb{A}_{\mathbb{F}_p}^1$ qui sera explicité en 24.3. C'est ce qui explique l'apparition de Frob_p^{-1} dans cette section et ailleurs.

19.1. Définition. Soit p un nombre premier ou bien 1. Si k est un corps d'exposant caractéristique p , on note $\text{Frob}_p : k \rightarrow k$ le morphisme $x \mapsto x^p$. Si k est parfait (et notamment si k est algébriquement clos), on note Frob_p^{-1} le morphisme réciproque de Frob_p .

Remarquons notamment que $\text{Frob}_p : \mathbb{F}_p(X_1, \dots, X_n) \rightarrow \mathbb{F}_p(X_1, \dots, X_n)$ (où $\mathbb{F}_p(X_1, \dots, X_n)$ désigne le corps des fractions rationnelles en n variables sur le corps premier \mathbb{F}_p) peut se voir soit comme l'élevation à la puissance p soit comme la composition par la substitution $(X_1, \dots, X_n) \mapsto (X_1^p, \dots, X_n^p)$.

On appellera **fonction F-rationnelle** (sous-entendu : à coefficients dans \mathbb{F}_p) un élément de la clôture parfaite de $\mathbb{F}_p(X_1, \dots, X_n)$, qui est aussi la colimite du système inductif indicé par \mathbb{N} dont le i -ième terme K_i est $\mathbb{F}_p(X_1, \dots, X_n)$, et les flèches sont les Frobenius itérés $(\text{Frob}_p)^{j-i} : K_i \rightarrow K_j$ si $i \leq j$.

Autrement dit, une fonction F-rationnelle est simplement une expression de la forme $\text{Frob}_p^{-i} \circ f$ où $f \in \mathbb{F}_p(X_1, \dots, X_n)$, avec les identifications évidentes, ou si on préfère une fraction rationnelle en les $X_1^{1/p^i}, \dots, X_n^{1/p^i}$ pour un certain i . La *valeur* d'une telle fonction F-rationnelle en $(x_1, \dots, x_n) \in k^n$, si k est un corps parfait d'exposant caractéristique p , est définie comme $\text{Frob}_p^{-i}(f(x_1, \dots, x_n))$ (c'est-à-dire qu'elle est définie si et seulement si $f(x_1, \dots, x_n)$ l'est, et lorsque c'est le cas elle a pour valeur $\text{Frob}_p^{-i}(f(x_1, \dots, x_n))$).

(Dans [MARKER 2002, définition 3.2.13], ces fonctions sont appelées « quasirationnelles ».)

Comme pour les formules booléennes, il sera souvent commode d'identifier une fonction F-rationnelle en n variables X_1, \dots, X_n en la fonction F-rationnelle de même expression en $n' > n$ variables (ne faisant pas intervenir les nouvelles variables).

19.2. Remarque. Le *graphe* Γ_u d'une fonction F-rationnelle $u = \text{Frob}_p^{-i} \circ f$ est la partie constructible (en fait, localement fermée) de $\mathbb{A}_{\mathbb{F}_p}^n \times \mathbb{A}_{\mathbb{F}_p}^1$ définie par l'équation $y^{p^i} = f(x_1, \dots, x_n)$ (c'est-à-dire $vy^{p^i} - u = 0$ et $v \neq 0$ où $f = uv$ est la forme irréductible de la fonction rationnelle f ; ici, x_1, \dots, x_n sont les coordonnées sur $\mathbb{A}_{\mathbb{F}_p}^n$ et y celle sur $\mathbb{A}_{\mathbb{F}_p}^1$).

Il est clair qu'une fonction F-rationnelle est complètement déterminée par son graphe (quitte à appliquer une puissance de Frob_p on se ramène au cas des fractions rationnelles).

Remarquons d'autre part (cf. [ÉGA IV₂, 2.4.5]) que la projection $\Gamma_u \rightarrow D_u$ où $D_u \subseteq \mathbb{A}_{\mathbb{F}_p}^n$ est l'ouvert de définition de u (ou de façon équivalente, de f) est un homéomorphisme universel de schémas (pour la topologie de Zariski) : ceci permet de voir une fonction F-rationnelle u comme une application ensembliste $D_u \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$, donc une fonction *partielle* $\mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$.

Si E est une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^n$, on appellera « fonction F-rationnelle sur E » la restriction à E d'une fonction F-rationnelle (ceci n'impose pas que la fonction soit définie sur tout E).

La proposition suivante a pour objet d'aider l'intuition du lecteur. Nous ne faisons qu'en esquisser la démonstration puisque nous ne l'utiliserons pas et que nous prouverons un résultat plus général (plus effectif) en 24.2.

19.3. Proposition. *Soit Z une partie localement fermée de $\mathbb{A}_{\mathbb{F}_p}^{n+1}$ (munie de la structure de schéma réduit induite) telle que la projection $\pi : Z \rightarrow \mathbb{A}_{\mathbb{F}_p}^n$ soit radicielle (c'est-à-dire que pour tout corps k d'exposant caractéristique p et tout $x \in \mathbb{A}_{\mathbb{F}_p}^n(k)$ il existe au plus un $z \in Z(k)$ se projetant en x). Alors on peut écrire $\pi(Z)$ comme réunion finie disjointe de parties localement fermées X_1, \dots, X_n telles que sur chacune d'entre elles la restriction $Z_i = \pi^{-1}(X_i)$ soit le graphe d'une fonction F-rationnelle sur X_i .*

Esquisse de démonstration. Le morphisme $\pi : Z \rightarrow \mathbb{A}_{\mathbb{F}_p}^n$ est quasi-fini : quitte à écrire son image comme réunion finie disjointe de localement fermés X_i , qu'on peut même supposer affine, on peut s'arranger pour que π soit fini (entier et de type fini) sur chaque X_i . On peut supposer qu'il n'y a qu'un seul X_i , notons-le X . Mettons que $X = \text{Spec } A$ et $Z = \text{Spec } B$, de sorte que B est une A -algèbre de type fini entière ; l'immersion fermée $Z \hookrightarrow X \times \mathbb{A}_{\mathbb{F}_p}^1$ définit une surjection de A -algèbres $A[t] \twoheadrightarrow B$, donc B est engendré par un unique élément y (image de t) qui vérifie une équation radicielle, $y^{p^j} = x$ pour $x \in A$ qu'on peut représenter par une fonction rationnelle. \square

(On pourra comparer avec [MARKER 2002, proposition 3.2.14].)

19.4. Observation. Il est clair que les fonctions F-rationnelles peuvent être manipulées par une machine de Turing (on peut par exemple le déduire de 12.5(i,v)) : il est algorithmique de calculer des sommes, différences, produits et quotients dans ce corps, ou de tester la nullité d'un élément, ou encore de calculer des composées (et notamment de tester si une composée est bien définie). On se convainc de même facilement qu'on peut par exemple calculer algorithmiquement le graphe d'une fonction F-rationnelle (comme partie constructible) ou tester l'égalité de deux fonctions F-rationnelles sur une partie constructible.

20. FONCTIONS PARTIELLES CALCULABLES

Nous cherchons maintenant à définir la notion de fonction partielle $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ calculable au sens de Church-Turing. L'intuition de la définition qui suit est que, pour évaluer une telle fonction f en des arguments $(i_1, \dots, i_r, x_1, \dots, x_n) \in \mathbb{N}^r \times k^n$ (où k est un corps quelconque d'exposant caractéristique p), une machine de Turing va produire une suite de fonctions booléennes φ_j (indicées par les entiers naturels j , et pouvant dépendre des paramètres entiers i_1, \dots, i_r) et de valeurs v_j , et la valeur de la fonction en x_1, \dots, x_n est la v_j accompagnant la première formule φ_j qui soit vraie en x_1, \dots, x_n . Formellement :

20.1. Définition. Soit p un nombre premier ou bien 1. On appelle **fonction partielle** $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ **calculable au sens de Church-Turing** la donnée d'une fonction partielle calculable au sens de Church-Turing (au sens usuel^①) qui à un $(r+1)$ -uplet d'entiers naturels $(i, j) = (i_1, \dots, i_r, j)$ associe une formule booléenne $\varphi_{i,j}$ sur \mathbb{F}_p en des indéterminées X_1, \dots, X_n ainsi qu'un entier naturel $v_{i,j}$.

Si (x_1, \dots, x_n) sont des éléments d'un corps k quelconque d'exposant caractéristique p , ou bien une notation abusive pour un point de $\mathbb{A}_{\mathbb{F}_p}^n$, et si (i_1, \dots, i_r) sont des entiers naturels, alors la *valeur* de f en $(i_1, \dots, i_r, x_1, \dots, x_n)$ est définie comme valant $v_{i,j}$, où j est le plus petit entier naturel tel que

^①C'est-à-dire définie, par exemple, par une machine de Turing, avec la convention que lorsque l'exécution de la machine de Turing sur l'entrée fournit ne termine pas, la fonction n'est pas définie : [ODIFREDDI 1989, définition II.1.1, théorème II.1.8 et discussion p. 132–133].

- la formule $\varphi_{i,j}$ est définie, et $\varphi_{i,j}(x_1, \dots, x_n)$ est vraie, et
- pour tout $j' < j$, la formule $\varphi_{i,j'}$ est définie, et $\varphi_{i,j'}(x_1, \dots, x_n)$ n'est pas vraie.

Si un tel j n'existe pas, alors la valeur de f n'est pas définie en ces points.

(Pour alléger la notation, on omettra souvent les indices i_1, \dots, i_r sur φ et v , notant ainsi simplement φ_j et v_j .)

On définit aussi la notion de fonction partielle $f : \mathbb{N}^r \times (\prod_{n=0}^{+\infty} \mathbb{A}_{\mathbb{F}_p}^n) \rightarrow \mathbb{N}$ calculable au sens de Church-Turing : il s'agit d'une fonction partielle calculable qui à un $(r + 2)$ -uplet (i_1, \dots, i_r, n, j) d'entiers naturels associe un couple (φ_j, v_j) , la valeur de f en $(i_1, \dots, i_r, (x_1, \dots, x_n))$ étant définie de la même manière.

Il faut comprendre cette définition de la manière suivante : pour définir une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$, on donne une machine de Turing qui produit, pour chaque valeur des paramètres entiers (i_1, \dots, i_r) , une suite récursive de couples (φ_j, v_j) qui signifient « si les paramètres (x_1, \dots, x_n) vérifient φ_j (et aucune formule précédente), alors retourner la valeur v_j ». (Si pour un certain j la machine de Turing ne termine pas, ou bien sûr si elle renvoie autre chose qu'un couple formé d'une formule booléenne et d'un entier naturel, la valeur de la fonction est considérée comme indéfinie, sauf pour les valeurs qui ont déjà été attrapées par les $\varphi_{j'}$ précédents. De même, si aucune formule n'est vérifiée, la fonction n'est pas définie au point considéré.) Pour une fonction $f : \mathbb{N}^r \times (\prod_{n=0}^{+\infty} \mathbb{A}_{\mathbb{F}_p}^n) \rightarrow \mathbb{N}$, la dimension n doit également être passée en paramètre à la machine de Turing.

À titre d'exemple trivial (avec $r = 0$ et $n = 1$), la machine de Turing qui à $j = 0$ associe le couple $(“x = 0”, 0)$ et à $j = 1$ le couple $(“\neg(x = 0)”, 1)$ définit une fonction $\mathbb{A}_{\mathbb{F}_p}^1 \rightarrow \mathbb{N}$ qui, sur n'importe quel corps, vaut (l'entier naturel) 0 en (l'élément du corps) 0 et 1 ailleurs. On verra en 22.1 que cette fonction est « totale » : dans le cas des fonctions totales, la définition des fonctions calculables se simplifie considérablement, comme on le verra en 22.4.

20.2. Remarque. Pour être plus rigoureux, la définition faite en 20.1 est celle de la *description* d'une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$: on considérera que deux fonctions calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ sont égales lorsque leurs valeurs sont les mêmes en tout $(i_1, \dots, i_r, x_1, \dots, x_n)$ pour n'importe quel corps k d'exposant caractéristique p – d'après 18.2 il revient au même de faire cette hypothèse pour k algébriquement clos, ou encore pour tout $(i_1, \dots, i_r, x) \in \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n$. On peut donc bien considérer les fonctions partielles calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ comme des fonctions partielles $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ particulières.

20.3. Remarque. Dans la définition 20.1, on peut, si on le souhaite, supposer que les φ_j sont deux à deux exclusives (c'est-à-dire que les parties constructibles qu'elles définissent sont deux à deux disjointes) : en effet, il suffit pour cela de remplacer φ_j par sa conjonction avec la négation de tous les $\varphi_{j'}$ antérieurs. (Cette transformation est évidemment algorithmique.)

De même, si on le souhaite, et de nouveau par une transformation algorithmique, on peut supposer que les φ_j sont des formules purement conjonctives (donc définissent des parties localement fermées, cf. 18.4). On se convainc même qu'on peut faire ces deux hypothèses simultanément (car toute formule booléenne peut se réécrire – algorithmiquement – comme disjonction *exclusive* de formules purement conjonctives, quitte à distinguer tous les cas possibles d'égalité ou de non-égalité à 0 des polynômes qui y interviennent).

La notion de fonction partielle calculable à valeurs dans $\mathbb{A}_{\mathbb{F}_p}^1$ est définie de façon analogue à celle de fonction partielle calculable à valeurs dans \mathbb{N} , mais cette fois les valeurs v_j retournées par la machine de Turing sont des fonctions F-rationnelles qui sont évaluées en (x_1, \dots, x_n) . Précisément :

20.4. Définition. On appelle **fonction partielle** $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ **calculable au sens de Church-Turing** une fonction comme en 20.1 mais où cette fois les v_j sont censés être des fonctions F-rationnelles (cf. 19.1) en n variables X_1, \dots, X_n ; la valeur de la fonction f en $(i_1, \dots, i_r, x_1, \dots, x_n)$, où x_1, \dots, x_n appartiennent à un corps parfait k d'exposant caractéristique p , est alors définie comme la valeur en (x_1, \dots, x_n) de la fonction F-rationnelle v_j (et indéfinie si v_j n'est pas définie en (x_1, \dots, x_n)).

On définit de même les fonctions partielles calculables $f : \mathbb{N}^r \times (\prod_{n=0}^{+\infty} \mathbb{A}_{\mathbb{F}_p}^n) \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$. Et on définit sans difficulté les fonctions partielles calculables à valeurs dans $\mathbb{N}^s \times \mathbb{A}_{\mathbb{F}_p}^m$ (ou même vers $\prod_{m=0}^{+\infty} \mathbb{A}_{\mathbb{F}_p}^m$, en convenant que pour spécifier un élément de celui-ci on spécifie un m et une valeur dans $\mathbb{A}_{\mathbb{F}_p}^m$, c'est-à-dire un m -uplet de fonctions F-rationnelles).

En particulier, les fonctions F-rationnelles elles-mêmes sont des fonctions calculables.

Comme on l'a convenu en 20.2 pour les fonctions partielles calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$, les fonctions partielles calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ sont définies par leurs valeurs (on remarquera que c'est le cas pour les fonctions F-rationnelles : cf. 19.2).

20.5. Remarque. Dans le contexte de la définition 20.4, il pourra parfois être commode de supposer que la fonction F-rationnelle v_j est nécessairement définie quand on cherche à l'évaluer (autrement dit, que la non-définition de la fonction f ne peut être due qu'aux formules $\varphi_{j'}$) : ceci est très simple à assurer, il suffit de remplacer φ_j par sa conjonction avec la formule qui assure que le dénominateur de v_j ne s'annule pas.

21. ÉQUIVALENCE AVEC LE MODÈLE « BOÎTE NOIRE »

Le modèle de calcul que nous venons de définir a l'avantage qu'il définit automatiquement des fonctions valables à la fois sur tous les corps d'exposant caractéristique p (remarquons au passage que si la fonction dispose de $n = 0$ variables d'entrées dans le corps, alors la seule sortie qu'elle puisse produire est un élément de \mathbb{F}_p).

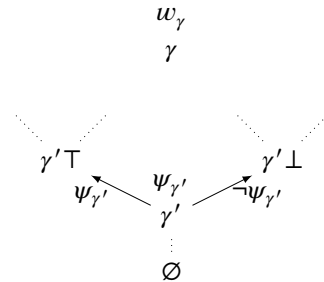
Il n'est cependant peut-être pas évident que cette notion de calcul soit naturelle et décrive bien toutes les manipulations qu'on souhaite pouvoir effectuer algorithmiquement sur les éléments d'un corps. Pour répondre à cette crainte, nous allons à présent montrer que les fonctions partielles calculables dans le modèle qu'on vient de définir coïncident précisément avec celles qui sont calculables par une machine de Turing qui manipulerait les éléments d'un corps non spécifié comme des « boîtes noires » sur lesquelles elle peut effectuer uniquement les opérations du corps (addition, opposé, multiplication, inverse, comparaison à zéro).

Montrons d'abord un lemme qui énonce le fait que dans les définitions 20.1 et 20.4, il revient au même de supposer que la machine de Turing qui produit la valeur finale v_j de la fonction peut poser des questions sur la satisfaction de formules booléennes des variables, y compris en fonction des réponses aux questions précédemment posées (c'est-à-dire, sur la base d'un arbre de décision) :

21.1. Lemme. *On obtient des définitions équivalentes à 20.1 et 20.4 si la machine de Turing considérée prend en entrée un multi-index $\underline{i} = (i_1, \dots, i_r)$ et un mot fini γ sur l'alphabet $\{\top, \perp\}$ et renvoie soit une formule booléenne ψ_γ soit une valeur finale w_γ (qui est un entier naturel ou bien une fonction F-rationnelle selon le type censé être retourné par f), la valeur de f en $(i_1, \dots, i_r, x_1, \dots, x_n)$ étant alors définie comme w_γ où γ est l'unique mot tel que*

- la machine renvoie pour γ une valeur finale (qui est w_γ), et
- pour tout préfixe strict γ' de γ , la machine renvoie une formule $\psi_{\gamma'}$, et le symbole suivant immédiatement γ' dans γ est \top ou \perp selon que $\psi_{\gamma'}(x_1, \dots, x_n)$ est vraie ou fausse.

(La donnée de la machine qui à γ associe une formule ou une valeur finale comme ci-dessus s'appellera un **arbre de décision** pour la fonction qu'elle calcule. Plus exactement, le mot vide s'appelle la **racine** de l'arbre de décision, à chaque fois que la machine renvoie une valeur w_γ , le mot γ est appelé une **feuille** de l'arbre de décision, tandis que si elle renvoie une formule ψ_γ , on dira que γ est un **nœud** ayant pour fils les deux mots obtenus en concaténant respectivement \top et \perp à la fin de γ .)



Démonstration. Il est clair que cette nouvelle définition est au moins aussi puissante que la précédente : donnée une suite (φ_j, v_j) calculée comme en 20.1 ou 20.4, on définit une machine M qui

calcule la même fonction pour la définition du présent lemme : si γ est un mot formé de j signes \perp suivi d'un signe \top alors M renvoie pour γ une valeur $w_\gamma = v_j$, et si γ est formé de j signes \perp alors M renvoie pour γ une formule $\psi_\gamma = \varphi_j$ (et pour tout mot γ qui n'est pas formé d'une suite de \perp puis d'un éventuel signe \top , ce que renvoie M est sans importance).

Réciproquement, donnons-nous une machine M qui pour tout mot γ renvoie soit une formule ψ_γ soit une valeur w_γ comme dans l'énoncé du présent lemme. Il s'agit de définir une nouvelle machine de Turing M' qui énumère une suite (φ_j, v_j) en fonction de ce que renvoie la machine M calculant les ψ_γ ou w_γ . Pour cela, on va effectuer un parcours en parallèle de l'arbre de tous les calculs possibles par M . Précisément, la machine M' commence par exécuter M sur le mot vide, puis, si celle-ci termine et renvoie une formule booléenne, exécute M en parallèle sur les deux mots \top et \perp , et ainsi de suite récursivement : à chaque fois qu'une exécution de M sur un mot γ termine en renvoyant une formule booléenne, la machine M' exécute en parallèle M sur les deux mots obtenus en ajoutant à γ un symbole \top ou \perp à la fin ; en revanche, si la machine M termine en produisant une valeur finale w_γ , alors la machine M' énumère pour prochaine valeur j (c'est-à-dire, le premier j qui n'ait pas encore été utilisé) le couple (φ_j, v_j) où $v_j = w_\gamma$ et φ_j est la conjonction de toutes les formules $\psi_{w'}$ qui ont été calculées par M sur les préfixes stricts w' de w . \square

21.2. Proposition. *Les fonctions partielles calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ et $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ au sens des définitions 20.1 et 20.4 :*

- contiennent les fonctions constantes (à valeurs dans les entiers ou les éléments de \mathbb{F}_p);
- contiennent la fonction successeur $i \mapsto i + 1$ sur les entiers naturels, la fonction de test à zéro (qui vaut l'entier naturel 0 en $0 \in \mathbb{A}_{\mathbb{F}_p}^1$ et 1 ailleurs), ainsi que les opérations d'addition $((x, x') \mapsto x + x')$, opposée $(x \mapsto -x)$, multiplication $((x, x') \mapsto xx')$ et inverse $(x \mapsto x^{-1}$ non définie en 0), et la fonction Frob_p^{-1} ;
- contiennent les projections vers n'importe quelle variable d'entrée;
- sont stables par composition : si h et g_1, \dots, g_N sont calculables et que la composition a un sens, alors $h(g_1, \dots, g_N)$ est calculable;
- sont stables par récursion primitive : si g et h sont calculables, le premier argument de h étant un entier naturel, alors la fonction f , dont le premier argument est un entier naturel, définie par $f(0, \dots) = g(\dots)$ et $f(u + 1, \dots) = h(u, f(u, \dots), \dots)$, est calculable — ici, les points de suspension désignent n'importe quelle combinaison de sortes de variables;
- sont stables par recherche non bornée (ou «opérateur μ de Kleene») : si f est calculable, son premier argument étant un entier naturel, alors la fonction qui à des paramètres d'entrée (\dots) associe le plus petit u tel que $f(u, \dots) = 0$ et que $f(u', \dots) \neq 0$ pour tout $u' < u$ (ce qui sous-entend que toutes ces valeurs $f(u', \dots)$ sont définies), est calculable.

(Comparer avec [ODIFREDDI 1989, définition II.1.1]. Voir la proposition suivante pour la réciproque.)

Démonstration. Les trois premiers points sont évidents.

Les suivants découlent du lemme précédent, car il est facile de fabriquer les arbres de décision des fonctions décrites d'après ceux des fonctions qui les définissent.

Par exemple, pour la composée $h \circ g$, on fabrique l'arbre de décision de $h \circ g$ en attachant à la chaque feuille de l'arbre de décision de g (c'est-à-dire, dans la notation du lemme, à chaque fois qu'au mot γ il affecte une valeur finale w_γ et non une formule) une copie de l'arbre de décision de h , dans lequel les formules et éventuelles fonctions booléennes ont été composées par w_γ (ce qui signifie, si g renvoie des entiers, qu'on a calculé l'arbre de décision de h pour cet entier w_γ , et si $g = (g_1, \dots, g_N)$ prend ses valeurs dans $\mathbb{A}_{\mathbb{F}_p}^N$, qu'on a composé toutes les formules booléennes, et éventuellement valeurs de retour si ce sont des fonctions F-rationnelles, dans cet arbre, par la fonction w_γ). \square

21.3. Proposition. *Les fonctions partielles calculables $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ et $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ au sens des définitions 20.1 et 20.4 sont le plus petit ensemble de telles fonctions qui possèdent les stabilités énumérées à la proposition précédente.*

Ces fonctions pourraient donc également être appelées **fonctions calculables à partir des opérations de corps et Frob_p^{-1} comme boîtes noires**.

Démonstration. On vient de voir une implication. Il s'agit maintenant de montrer que les fonctions calculables au sens des définitions 20.1 et 20.4 sont effectivement calculables à partir des opérations de corps et Frob_p^{-1} comme boîtes noires.

Mais les fonctions calculables en ce dernier sens contiennent au moins les fonctions calculables au sens de Church-Turing, et par ailleurs contiennent toutes les fonctions F-rationnelles et les formules booléennes (considérées comme fonctions à valeurs dans $\{0, 1\}$). Il reste donc simplement à montrer qu'à partir d'une suite réursive (φ_j, v_j) on peut calculer la valeur finale de f : mais c'est clair en utilisant la primitive récursion et la recherche (du plus petit j tel que φ_j soit vrai et tous les précédents soient faux). \square

On en déduit que les fonctions partielles calculables dans notre modèle sont calculables quand on les applique à n'importe quel « corps calculable » :

21.4. Corollaire. *Si \mathfrak{K} est un corps calculable (cf. 12.1) d'exposant caractéristique p , alors pour toute fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathfrak{K}}^n \rightarrow \mathbb{N}$ (resp. $\mathbb{N}^r \times \mathbb{A}_{\mathfrak{K}}^n \rightarrow \mathbb{A}_{\mathfrak{K}}^1$ en supposant \mathfrak{K} parfait) au sens des définitions 20.1 ou 20.4, la fonction partielle $\mathbb{N}^r \times \mathfrak{K}^n \rightarrow \mathbb{N}$ qu'elle définit est calculable (au sens usuel) (resp. il existe une fonction calculable $\mathbb{N}^r \times \mathfrak{K}^n \rightarrow \mathfrak{K}$ qui la représente).*

Démonstration. Il s'agit simplement de voir que les fonctions énumérées en 21.2 sont calculables sur \mathfrak{K} . Le seul cas qui n'est pas totalement évident est celui de Frob_p^{-1} : mais comme pour le cas de fonctions $\mathbb{N}^r \times \mathbb{A}_{\mathfrak{K}}^n \rightarrow \mathbb{A}_{\mathfrak{K}}^1$ on a supposé \mathfrak{K} parfait, et que dans le cas de fonctions $\mathbb{N}^r \times \mathbb{A}_{\mathfrak{K}}^n \rightarrow \mathbb{N}$ on peut construire et travailler dans la clôture parfaite de \mathfrak{K} d'après le début de la démonstration de 12.5(v)), on peut calculer Frob_p^{-1} (au pire ^① d'après 12.8). \square

21.5. Remarque. La réciproque n'est pas vraie. Par exemple, si on considère la clôture algébrique $\mathbb{F}_p(T)^{\text{alg}}$ de $\mathbb{F}_p(T)$ construite de la façon habituelle (cf. 12.5), la fonction qui à x associe 0 si x est algébrique sur \mathbb{F}_p et 1 si x est transcendant, sera calculable (ceci n'est pas surprenant : il est en effet facile, en considérant l'écriture d'une fonction algébrique sur \mathbb{F}_p , de voir si l'indéterminée apparaît réellement); en revanche, la fonction $\mathbb{A}_{\mathbb{F}_p}^1 \rightarrow \mathbb{N}$ qui répond à la même définition n'est pas calculable au sens de la définition 20.1, comme il résultera par exemple du corollaire 22.4 (l'ensemble des éléments transcendants sur \mathbb{F}_p n'étant, de toute évidence, pas une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^1$). Plus généralement, la différence entre la notion de fonction calculable sur un corps calculable \mathfrak{K} et celle de fonction calculable au sens « universel » défini dans la présente partie est que les premières peuvent utiliser les détails du codage des éléments de \mathfrak{K} alors que les « boîtes noires » ne permettent de réaliser que des opérations algébriques.

22. FONCTIONS TOTALES

22.1. Définition. On dit qu'une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ (au sens des définitions 20.1 et 20.4) est **totale** lorsque sa valeur est définie pour toutes valeurs $(i_1, \dots, i_r, x_1, \dots, x_n)$, les x_1, \dots, x_n appartenant à n'importe quel corps parfait k d'exposant caractéristique p .

En vertu de 18.2, il revient au même de demander que la valeur soit définie pour toutes valeurs $(i_1, \dots, i_r, x_1, \dots, x_n)$, les x_1, \dots, x_n appartenant à n'importe quel corps algébriquement clos k d'exposant caractéristique p , ou encore, en tout point de $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n$ où $\mathbb{A}_{\mathbb{F}_p}^n$ est vu comme l'ensemble des idéaux premiers de $\mathbb{F}_p[X_1, \dots, X_n]$.

22.2. Contre-exemple : La fonction qui à $x \in \mathbb{A}_{\mathbb{F}_p}^1$ associe le degré de x sur \mathbb{F}_p , c'est-à-dire le plus petit degré d'un polynôme $f \in \mathbb{F}_p[X]$ tel que $f(x) = 0$, est partielle calculable (il suffit de produire une machine de Turing qui énumère les polynômes irréductibles f_j sur \mathbb{F}_p , et renvoie le couple formé de la formule booléenne $f_j = 0$ et l'entier $\deg f_j$), mais même si elle est définie sur tout élément de $\mathbb{F}_p^{\text{alg}}$, elle n'est pourtant pas totale, car appliquée à l'élément transcendant T de $\mathbb{F}_p(T)$ elle n'est pas définie (ou, si on préfère voir $\mathbb{A}_{\mathbb{F}_p}^1$ comme l'ensemble des idéaux premiers de $\mathbb{F}_p[T]$, la fonction n'est

^①Si on voulait remplacer la notion de calculabilité par celle de fonction primitivement réursive, la bonne notion de corps « primitivement récursivement parfait » supposerait, bien sûr, que Frob_p^{-1} fait partie des opérations de corps.

pas définie au point générique). Il résulte de la proposition qui suit (ou de son corollaire) qu'il n'existe aucune manière de prolonger cette fonction en une fonction calculable totale.

22.3. Proposition. (A) Pour qu'une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ soit totale, il (faut et il) suffit qu'elle soit définie pour toutes les valeurs $(i_1, \dots, i_r, x_1, \dots, x_n)$, où les x_1, \dots, x_n appartiennent à une clôture algébrique fixée de $\mathbb{F}_p(T_1, \dots, T_n)$.

(B) De plus, pour une fonction totale, dans la définition 20.1 ou 20.4, il existe un N (dépendant de i_1, \dots, i_r et, évidemment, de la fonction considérée) telle qu'on puisse tronquer la suite (φ_j, v_j) à partir de N sans changer la fonction ainsi définie.

Démonstration. Le point (A) est conséquence du fait que les corps résiduels des points de $\mathbb{A}_{\mathbb{F}_p}^n$ sont de degré de transcendance au plus n sur \mathbb{F}_p . Détaillons dans le cas d'une fonction $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$; le cas d'une fonction $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ ne présentant pas de difficulté supplémentaire grâce à la remarque 20.5. Si la fonction n'est pas totale, il existe $(i_1, \dots, i_r) \in \mathbb{N}^r$ et un n -uplet (x_1, \dots, x_n) d'éléments d'un certain corps k d'exposant caractéristique p , qu'on peut certainement supposer algébriquement clos, tels que (1) pour un certain j_0 , les $\varphi_0, \dots, \varphi_{j_0-1}$ soient définis et faux (=non vérifiés) pour (x_1, \dots, x_n) mais que φ_{j_0} ne soit pas défini (la machine censée le produire ne termine pas), ou bien (2) les φ_j soient définis pour tout j et tous faux pour (x_1, \dots, x_n) . (Dans le cas inintéressant, c'est-à-dire (1), définissons comme $0 = 1$ tous les φ_j pour $j \geq j_0$.) Par hypothèse et construction, l'intersection des parties constructibles $E_j := E_{\neg\varphi_j}$ est non vide. Le corps résiduel d'un point quelconque de cette intersection se plonge dans le corps de l'énoncé.

Montrons (B) : le fait que la fonction soit totale implique qu'il n'existe pas de n -uplet (x_1, \dots, x_n) d'éléments d'un corps algébriquement clos d'exposant caractéristique p qui vérifieraient $\neg\varphi_j$ pour tout j . Autrement dit, l'intersection des parties constructibles $E_j = E_{\neg\varphi_j}$ est vide. L'espace topologique $\mathbb{A}_{\mathbb{F}_p}^{n \text{ cons}}$ étant compact et les E_j fermés, il existe un N tel que $\bigcap_{j < N} E_j = \emptyset$. On peut alors omettre tous les φ_j pour $j \geq N$ dans la définition de la fonction car l'une des conditions φ_j , $j < N$ est toujours satisfaite. \square

Notons, bien que nous n'en ferons pas usage que si dans (A) l'entier n n'est pas fixé, on peut tester si une fonction est totale en considérant des variables à valeurs dans une clôture algébrique de $\mathbb{F}_p(T_i, i \in \mathbb{N})$ ^①.

22.4. Corollaire. Une fonction totale calculable $\mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ est exactement la donnée d'une fonction continue $\mathbb{A}_{\mathbb{F}_p}^{n \text{ cons}} \rightarrow \mathbb{N}$, c'est-à-dire d'une partition de $\mathbb{A}_{\mathbb{F}_p}^n$ en un nombre fini de parties constructibles, sur chacune desquelles la fonction prend une valeur constante entière (en particulier, la fonction est bornée).

Une fonction totale calculable $\mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^m$ est exactement la donnée d'une partition de $\mathbb{A}_{\mathbb{F}_p}^n$ en un nombre fini de parties constructibles, sur chacune desquelles la fonction coïncide avec une certaine fonction F -rationnelle (définie partout sur la partie en question).

Une fonction totale calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^m$ est exactement la donnée d'une fonction calculable au sens usuel qui à toute valeur (i_1, \dots, i_r) des r premiers paramètres associe une donnée comme décrite dans les deux paragraphes précédents.

Démonstration. Ceci découle de manière simple du (B) de la proposition précédente. On notera que le N de cet énoncé peut être calculé en fonction de (i_1, \dots, i_r) en vertu de l'observation 18.5 (car on sait tester si $E_{\varphi_1} \cup \dots \cup E_{\varphi_N}$ recouvrent $\mathbb{A}_{\mathbb{F}_p}^n$). \square

(On pourra comparer avec [MARKER 2002, proposition 3.2.14].)

22.5. Remarque. La proposition et son corollaire valent également (*mutatis mutandis*) pour des fonctions calculables totales définies sur $\mathbb{N}^r \times E$ où E est une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^n$, ou même

^①Une autre approche à (A), utilisant la théorie des modèles, repose sur le théorème de Löwenheim-Skolem ([MARKER 2002, théorème 2.3.7]) : avec les notations de la démonstration, la suite $\neg\varphi_0, \neg\varphi_1, \neg\varphi_2, \dots$, réunie à la théorie des corps algébriquement clos d'exposant caractéristique p , admet un modèle de degré de transcendance \aleph_0 sur \mathbb{F}_p , qui permet de tester si une fonction est totale. Pour (B), on pourrait substituer au théorème de compacité de $\mathbb{A}_{\mathbb{F}_p}^{n \text{ cons}}$ celui de la logique du premier ordre ([ibid., théorème 2.1.4]).

sur une partie E de $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n$ dont la fonction indicatrice est calculable (on pourrait dire une partie réursive-constructible de $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n$). En effet, il suffit d'appliquer ce qu'on a dit à la fonction qui coïncide avec la fonction considérée sur la partie E et qui, ailleurs que sur E , prend une valeur spéciale.

On pourra donc considérer que la fonction $x \mapsto x^{-1}$ est « totale » si besoin est, puisqu'elle est totale sur une partie constructible (le complémentaire de $\{0\}$) : les fonctions « essentiellement partielles » (celles qu'on ne peut pas trivialement considérer comme totales) sont celles pour lesquelles on est réellement confronté à un calcul qui pourrait ne pas terminer en temps fini, ne serait-ce que le contre-exemple présenté en 22.2.

23. ÉLIMINATION DES QUANTIFICATEURS

Commençons par rappeler un fait bien connu, dont on trouvera par exemple une démonstration dans [FRIED et JARDEN 2008, théorème 9.3.1], et pour lequel notre modèle de calcul fournira une preuve différente :

23.1. Proposition. *Si Z est une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^{n+1}$ alors sa projection sur $\mathbb{A}_{\mathbb{F}_p}^n$ est encore constructible, et, de plus, une formule booléenne la définissant se calcule algorithmiquement en fonction d'une formule booléenne définissant Z .*

Démonstration. Comme remarqué en 18.4, on peut supposer que Z est une partie localement fermée, définie par une formule purement conjonctive, c'est-à-dire la conjonction de $f_1 = \dots = f_r = 0$ et de $g \neq 0$ (où f_1, \dots, f_r et g sont des polynômes en x_1, \dots, x_n, y).

Observons maintenant le fait suivant : si cette fois f_1, \dots, f_r et g sont des polynômes en une seule variable Y sur un corps k algébriquement clos d'exposant caractéristique p , il existe un algorithme décidant si les équations $f_1 = \dots = f_r = 0$ ont une solution commune telle que $g \neq 0$. En effet, il suffit pour cela de calculer le PGCD u (unitaire) de f_1, \dots, f_r selon l'algorithme d'Euclide, et de vérifier qu'il ne divise pas $g^{\deg(u)}$ (l'exposant $\deg u$ garantit que les racines de u dans une clôture algébrique sont un sous-ensemble de celles de g si et seulement si u divise $g^{\deg u}$).

Cet algorithme n'utilise manifestement que des opérations des corps et des tests d'égalité à 0, donc en vertu des résultats de la section 21, il est, en fait, calculable dans notre sens « universel », et comme la fonction calculée est totale, d'après 22.4, ceci signifie qu'il existe une fonction calculable totale qui à des entiers naturels r, D associe la formule d'une partie constructible Π de l'espace affine $\mathbb{A}_{\mathbb{F}_p}^{(r+1)(D+1)}$ telle que des polynômes $f_i = c_{i,0} + c_{i,1}Y + \dots + c_{i,D}Y^D$ et $g = c'_0 + c'_1Y + \dots + c'_D Y^D$ dans un corps k algébriquement clos d'exposant caractéristique p admettent une solution à $f_1 = \dots = f_r = 0$ et $g \neq 0$ si et seulement si $(c_{0,0}, \dots, c'_D) \in \Pi$.

On obtient alors une formule pour la projection de Z en remplaçant les coefficients en Y de nos f_1, \dots, f_r, g de départ dans la formule booléenne définissant Π (pour un D assez grand). \square

Autrement dit, ceci signifie que donnée une formule booléenne φ on peut trouver, algorithmiquement, une formule booléenne (donc sans quantificateur !) qui équivaut sur tout corps algébriquement clos d'exposant caractéristique p à la formule avec quantificateur $\exists y(\varphi(y, \dots))$.

(Rappelons que l'existence d'une telle formule sans quantificateur est conséquence du théorème de Chevalley : l'image d'un morphisme $\text{Spec}(B) \rightarrow \text{Spec}(A)$ de présentation finie est constructible ; cf. par exemple [ÉGA IV₁, §1.8] ou [OLIVIER 1966-1968, §3].)

Naturellement, ceci permet aussi de dire que la partie représentée par $\forall y(\varphi(y, \dots))$, qui est le complémentaire de la projection du complémentaire de la partie définie par φ , se calcule aussi effectivement.

La proposition suivante assure que, si une fonction f ($\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$) est calculable, alors il est possible de tester toutes les valeurs d'une de ses variables y (toutes, c'est-à-dire dans n'importe quel corps algébriquement clos d'exposant caractéristique p contenant les autres variables) pour détecter si l'une ou toutes les valeurs de la fonction f vaut 0 ; néanmoins, si une des valeurs n'est pas définie, alors la fonction résultante ne sera pas non plus définie. Précisément :

23.2. Proposition. *Si f est une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ et y une des coordonnées de $\mathbb{A}_{\mathbb{F}_p}^{n+1}$ intervenant dans f , alors il existe une fonction partielle calculable*

$f^{\forall y}$ (resp. $f^{\exists y}$) $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{N}$ (manifestement unique) telle que, si k est un corps algébriquement clos d'exposant caractéristique p , et si $\underline{z} \in \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n(k)$, alors $f^{\forall y}(\underline{z})$ (resp. $f^{\exists y}(\underline{z})$) vaut :

- 0 si, pour tout y dans n n'importe quel corps algébriquement clos k' contenant k , la valeur $f(\underline{z}, y)$ est définie et vaut toujours 0 (resp. et prend au moins une fois la valeur 0),
- 1 si, pour tout y dans n n'importe quel corps algébriquement clos k' contenant k , la valeur $f(\underline{z}, y)$ est définie et prend au moins une fois une valeur $\neq 0$ (resp. et ne prend que des valeurs $\neq 0$),
- non définie si pour au moins un y dans un corps algébriquement clos k' contenant k , la valeur $f(\underline{z}, y)$ n'est pas définie.

(Ces fonctions $f^{\forall y}$ et $f^{\exists y}$ sont évidemment totales quand f l'est. Par ailleurs, on peut bien sûr remplacer les mots « algébriquement clos » par « parfait » partout dans tout cet énoncé, et pour une fonction $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ on peut les omettre.)

Démonstration. On peut évidemment supposer que f est à valeurs dans \mathbb{N} (quitte à la composer par la fonction de test à zéro, qu'on sait être calculable). Mettons qu'on cherche à représenter $f^{\forall y}$ (le cas de $f^{\exists y}$ étant complètement analogue). Soient (φ_j, v_j) définissant f avec les notations habituelles (20.1). Comme on l'a signalé en 20.3, quitte à remplacer φ_j par sa conjonction avec la négation de tous les $\varphi_{j'}$, antérieurs, on peut supposer que les parties constructibles qu'elles définissent sont deux à deux disjointes.

On parcourt la liste des (φ_j, v_j) en calculant, au fur et à mesure, deux suites (ψ_j) et $(\psi_j^{(0)})$ de formules booléennes en n variables. (L'idée est que la partie constructible de $\mathbb{A}_{\mathbb{F}_p}^n$ définie par ψ_j sera celle sur laquelle on sait que f est définie pour tout y , et celle définie par $\psi_j^{(0)}$ sera celle sur laquelle on sait que f est définie et vaut 0 pour tout y .) Précisément, pour chaque j , on calcule (d'après ce qu'on a rappelé en 23.1) une formule booléenne ψ_j équivalente à $\forall y(\varphi_1(\dots, y) \vee \dots \vee \varphi_j(\dots, y))$ et une autre formule booléenne $\psi_j^{(0)}$ équivalente à $\forall y(\varphi_{j_1}(\dots, y) \vee \dots \vee \varphi_{j_s}(\dots, y))$ où les j_u sont les indices entre 1 et j tels qu'on ait $v_{j_u} = 0$. Enfin, pour représenter $f^{\forall y}$, on énumère alternativement $(\psi_j^{(0)}, 0)$ et $(\psi_j \wedge \neg \psi_j^{(0)}, 1)$.

Si pour un certain \underline{z} , la fonction $f(\underline{z}, y)$ est définie pour tous les y , c'est-à-dire que \mathbb{A}_k^1 est la réunion des parties constructibles définies par les φ_j (où \underline{z} a été substitué par sa valeur), par compacité de la topologie constructible il existe un j tel que les parties constructibles définies par $\varphi_1, \dots, \varphi_j$ suffisent à recouvrir \mathbb{A}_k^1 , autrement dit, \underline{z} vérifie ψ_j , et la fonction $f^{\forall y}$ est bien définie en \underline{z} et y a manifestement la bonne valeur. \square

Exactement comme en 22.3(A), on peut éviter d'avoir à considérer des éléments dans un corps k' plus gros que k en ne considérant qu'un seul corps K , fixé une fois pour toutes, algébriquement clos d'exposant caractéristique p et de degré de transcendance infini (cf. [MARKER 2002, proposition 4.3.4 et exemple 4.3.10]). (Dans le cas de fonctions calculables totales, on peut se contenter d'un corps algébriquement clos d'exposant caractéristique p quelconque.)

23.3. Corollaire. Si f est une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ et y une des coordonnées de $\mathbb{A}_{\mathbb{F}_p}^{n+1}$ intervenant dans f , et $\max_y f$ (resp. $\min_y f$) désigne la fonction qui à $\underline{z} \in \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n$ associe le maximum (resp. minimum) des $f(\underline{z}, y)$ si ceux-ci sont définis pour tout y , alors $\max_y f$ et $\min_y f$ sont calculables. (Elles sont évidemment totales quand f l'est.)

Démonstration. La fonction $\max_y f$ peut se définir comme le plus petit u tel que $\forall y(f(\underline{z}, y) \leq u)$, or la fonction qui à u associe la valeur de vérité de $\forall y(f(\underline{z}, y) \leq u)$ est calculable d'après la proposition, et d'après 21.2 (stabilité par recherche), la fonction qui calcule le plus petit u pour lequel cette valeur de vérité est vraie est elle-même calculable. \square

23.4. Remarque. Dans la lignée de la remarque 22.5, on peut calculer le maximum d'une fonction calculable pour y parcourant les éléments d'une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^n$. (En effet, on peut définir modifier la fonction pour valoir $-\infty$ en-dehors de cette partie constructible, ou adapter facilement la ou les démonstrations ci-dessus.)

Le même procédé (soit en imitant la preuve de la proposition 23.2, soit en l'appliquant comme dans le corollaire qui précède), permet de montrer la calculabilité de toutes sortes de fonctions où

on parcourt l'ensemble de tous les y pour vérifier une propriété, par exemple on pourrait facilement construire une fonction calculable $f^{-1}y$, comme dans l'énoncé de la proposition 23.2, qui teste l'existence d'un unique y pour lequel $f(\underline{z}, y) = 0$. Dans la section qui suit, on va voir qu'on peut, en fait, retourner la valeur de ce y .

24. SÉLECTION D'UN ÉLÉMENT UNIQUE

Le résultat suivant a pour objet d'éclaircir le lien entre fonctions calculables au sens de 20.1 et 20.4 en ramenant les secondes aux premières. Trivialement, si $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ (partielle ou totale) est calculable, alors la fonction $h : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ (partielle ou totale selon ce que f est) définie par $h(i_1, \dots, i_r, x_1, \dots, x_n, y) = 1$ lorsque $y = f(i_1, \dots, i_r, x_1, \dots, x_n, y)$ et $= 0$ sinon (et non définie si f ne l'est pas), est calculable. La proposition suivante, à rapprocher de 19.3, et son corollaire, montrent que la réciproque est vraie en un certain sens ; on commence par montrer un lemme facile qui est un cas particulier de ce qu'on veut prouver :

24.1. Lemme. *La fonction (totale) qui à des polynômes univariés $f_1, \dots, f_r, g \in k[Y]$ à coefficients dans un corps algébriquement clos d'exposant caractéristique p associe $(1, \xi)$ s'il existe un unique $\xi \in k$ tel que $f_1(\xi) = \dots = f_r(\xi) = 0$ et $g(\xi) \neq 0$, et $(0, 0)$ sinon, est une fonction calculable totale, au sens du modèle de calcul universel (c'est-à-dire de la définition 20.4).*

(Il faut bien sûr comprendre qu'on prend en entrée un couple $(r, D) \in \mathbb{N}^2$, où r est le nombre de polynômes et D une borne sur leurs degrés, ainsi que leurs coefficients vus comme un élément de $\mathbb{A}_{\mathbb{F}_p}^{(r+1)(D+1)}$, et on renvoie le couple annoncé – ou, si on veut, qu'on dispose de deux fonctions, l'une qui teste s'il existe un ξ unique comme indiqué et l'autre qui renvoie sa valeur.)

Démonstration. Le raisonnement est analogue à celui dans la démonstration de 23.1 : on effectue le calcul suivant dans notre modèle de calcul universel.

Donnés des polynômes univariés $f_1, \dots, f_r, g \in k[Y]$ à coefficients dans un corps k d'exposant caractéristique p , on calcule le PGCD unitaire u de f_1, \dots, f_r (au moyen de l'algorithme d'Euclide), ce qui fournit un polynôme dont les racines sont les racines communes à f_1, \dots, f_r . Puis on calcule le quotient v de u par le PGCD unitaire de u avec $g^{\deg(u)}$, ce qui fournit un polynôme dont les racines sont celles de u qui ne sont pas des racines de g (comme dans la démonstration de 23.1, l'exposant $\deg u$ sert à garantir qu'il est « assez grand »).

Puis on répète (au plus $\deg(v)$ fois) la boucle suivante : si le degré de v vaut 0, on renvoie $(0, 0)$; si v est de degré 1 et vaut $aY + b$ on renvoie $(1, -b/a)$. Si la dérivée v' de v vaut 0, on remplace v par sa racine p -ième (qu'on peut calculer car notre modèle de calcul permet d'effectuer Frob_p^{-1} ; remarquons que seuls les coefficients de degré multiple de p sont non-nuls ici) ; sinon, on remplace v par le quotient de celui-ci par le PGCD de v et v' ; si ces différentes opérations ne changent pas le polynôme (c'est-à-dire qu'il est à racines simples et de degré > 1), on renvoie $(0, 0)$. Il est clair que ces opérations renvoient bien l'unique racine ξ de v lorsque celle-ci existe et est unique. \square

24.2. Proposition. *Si h est une fonction partielle calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$, alors il existe une fonction partielle calculable $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ telle que, si k est un corps algébriquement clos d'exposant caractéristique p , et si pour $(\underline{i}, \underline{x}) \in \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n(k)$ il existe un unique y tel que $h(\underline{i}, \underline{x}, y) = 1$, alors $f(\underline{i}, \underline{x})$ vaut y (toute autre valeur de f est non spécifiée).*

Démonstration. Soient (φ_j, v_j) définissant h avec les notations habituelles. Comme on l'a signalé en 20.3, on peut supposer que les φ_j sont mutuellement exclusives et sont des formules purement conjonctives, et on le fera.

On énumère successivement les (φ_j, v_j) en ignorant celles pour lesquelles $v_j \neq 1$. Considérons maintenant une formule φ_j pour laquelle $v_j = 1$. Comme remarqué en 18.4, on peut supposer qu'elle s'écrit comme la conjonction de $f_1 = 0, \dots, f_r = 0$ et de $g \neq 0$ (où f_1, \dots, f_r et g sont des polynômes en x_1, \dots, x_n, y). D'après le lemme (et le corollaire 22.4), on peut calculer un nombre fini (disons s) de parties constructibles disjointes de l'espace affine (de dimension $(r+1)(D+1)$ où D est une borne sur les degrés des polynômes) et de fonctions F-rationnelles sur chacune d'elles, qui, sur n'importe quel corps k algébriquement clos d'exposant caractéristique p , si des polynômes univariés ont un

unique zéro commun qui ne soit pas zéro d'un autre, *calculent* le zéro en question. On substitue dans les équations de ces parties et fonctions les coefficients de nos f_1, \dots, f_r en la variable y (qui sont des polynômes en x_1, \dots, x_n) : ceci définit les $(\psi_{j,1}, w_{j,1}), \dots, (\psi_{j,s}, w_{j,s})$ qui participent à la définition de la fonction f . \square

24.3. Corollaire. *Une fonction (partielle ou totale) $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^n \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$ est calculable, si et seulement si la fonction $h : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{n+1} \rightarrow \mathbb{N}$ (partielle ou totale selon ce que f est) définie par $h(i_1, \dots, i_r, x_1, \dots, x_n, y) = 1$ lorsque $y = f(i_1, \dots, i_r, x_1, \dots, x_n)$ et $= 0$ sinon (et non définie si f ne l'est pas), est calculable*

Démonstration. On a déjà remarqué que l'implication « seulement si » est triviale. Pour ce qui est du « si », il découle facilement de la proposition (sauf éventuellement que f pourrait être définie en trop de points, mais il suffit d'évaluer $h(\underline{i}, \underline{x}, 0)$ avant de faire tout autre calcul pour éviter ce phénomène). \square

25. FACTORISATION DANS LE MODÈLE DE CALCUL

25.1. Remarque. Dans le cadre de la proposition 23.2, le modèle de calcul que nous avons adopté permet de tester l'existence d'un x tel que $f(x, \underline{z}) = 0$, mais ne permet pas, *stricto sensu*, d'en calculer un. Par exemple, si f (fonction d'une seule variable x , et à valeurs entières) est définie comme valant 0 si $x^2 + 1 = 0$ et 1 si $x^2 + 1 \neq 0$, alors $\exists x(f(x) = 0)$ est toujours vérifié, c'est-à-dire que la fonction $f^{\exists x}$ est égale à la constante 0, et pourtant, en caractéristique 0 ou bien $\equiv 3 \pmod{4}$, aucun élément du corps premier, donc aucune fonction calculable constante (cf. 22.4), ne peut témoigner de ce fait. Ceci est raisonnable si on pense que notre modèle de calcul ne « sait » rien du corps sur lequel il travaille (autrement que sa caractéristique), même pas si ce corps est algébriquement clos.

Les résultats qui vont suivre ont pour objet de montrer que, même si le modèle de calcul ne permet pas de factoriser un polynôme (comme l'illustre l'exemple de la remarque ci-dessus), il permet cependant de calculer tout ce qu'on pourrait calculer à partir d'une factorisation.

Nous commençons par considérer l'action de \mathfrak{S}_n (groupe symétrique sur n objets) sur $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ (dont les coordonnées seront notées $Z_1, \dots, Z_m, X_1, \dots, X_n$) par permutation des n dernières coordonnées. Cette action correspond à une action sur $\mathbb{F}_p[Z_1, \dots, Z_m, X_1, \dots, X_n]$ par permutation des variables X_i : on dira comme d'habitude qu'un polynôme est « totalement symétrique » en les n dernières variables lorsqu'il est invariant par cette action : on sait bien alors qu'il peut s'écrire, de façon unique, comme un polynôme en Z_1, \dots, Z_m et en les fonctions symétriques élémentaires de X_1, \dots, X_n . Nous montrons deux lemmes cruciaux quoique intuitivement évidents.

25.2. Lemme. *Soit F un fermé de Zariski de $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ tel que $\sigma(F) = F$ pour tout $\sigma \in \mathfrak{S}_n$, où le groupe \mathfrak{S}_n symétrique sur n objets opère en permutant les n dernières coordonnées. Alors F peut être défini par la formule $f_1 = \dots = f_r = 0$ où les f_i sont eux-mêmes totalement symétriques en les n dernières variables. De plus, on peut calculer les f_i algorithmiquement en fonction d'équations définissant F .*

Rappelons qu'un « fermé de Zariski » n'est pas un *sous-schéma* fermé mais bien une *partie* constructible définie par une formule booléenne positive, cf. 18.3.

Démonstration. Soient $g_1 = \dots = g_r = 0$ les équations initiales de F . Quitte à ajouter à ces équations toutes celles qui s'obtiennent en permutant de manière arbitraire les n dernières variables d'un des g_i , on peut supposer que l'ensemble des g_i est stable par \mathfrak{S}_n (agissant par permutation des n dernières variables). Soient f_1, \dots, f_r les r fonctions symétriques élémentaires appliquées à g_1, \dots, g_r (i.e., $f_1 = g_1 + \dots + g_r$, $f_2 = g_1 g_2 + g_1 g_3 + \dots + g_{r-1} g_r$, ..., $f_r = g_1 \dots g_r$). Alors les f_i sont manifestement totalement symétriques en les r dernières variables, et les équations $f_1 = \dots = f_r = 0$ sont équivalentes (ensemblément!) à $g_1 = \dots = g_r = 0$. \square

(On aurait bien sûr pu formuler ce lemme dans un contexte beaucoup plus général. Remarquons par ailleurs qu'il n'est plus vrai avec des multiplicités : le fermé $X_1 = \dots = X_n = 0$ de $\mathbb{A}_{\mathbb{F}_p}^n$ ne peut pas être défini par des équations totalement symétriques en les X_i .)

Montrons maintenant le résultat pour des combinaisons booléennes non nécessairement positives :

25.3. Lemme. Soit φ une formule booléenne (cf. 18.1) en les indéterminées $Z_1, \dots, Z_m, X_1, \dots, X_n$ qui soit totalement symétrique en les n dernières variables, c'est-à-dire que φ soit équivalente à $\varphi(Z_1, \dots, Z_m, X_{\sigma(1)}, \dots, X_{\sigma(n)})$ pour toute permutation $\sigma \in \mathfrak{S}_n$. Alors on peut écrire φ comme combinaison booléenne de formules de la forme $f = 0$ où chaque f est lui-même symétrique en les n dernières variables. De plus, cette transformation peut être faite de manière algorithmique.

Démonstration. Soit P l'ensemble de tous les polynômes qui apparaissent (positivement ou négativement) dans la formule booléenne φ , ainsi que tous les polynômes obtenus en appliquant un $\sigma \in \mathfrak{S}_n$ quelconque à l'un de ceux-ci (c'est-à-dire en permutant ses n dernières variables par σ). Ainsi, \mathfrak{S}_n opère sur P , et donc aussi sur l'ensemble des parties de cet ensemble (en préservant, évidemment, le cardinal des parties).

Pour chaque partie I de P , on définit deux formules booléennes : π_I sera la conjonction de tous les $f = 0$ pour $f \in I$, et δ_I sera la conjonction de tous les $f = 0$ pour $f \in I$ et des $f \neq 0$ pour $f \notin I$. Il est ainsi évident que les δ_I sont deux à deux exclusifs (la conjonction de deux d'entre eux est fausse) et recouvrent tous les cas possibles (leur disjonction est vraie); intuitivement, les δ_I représentent tous les cas possibles de nullité ou non-nullité des f (donc tous les cas de figure auxquels on sera éventuellement amenés à avoir affaire), mais il se peut, bien sûr, que certains des δ_I soient universellement faux.

Remarquons que π_I peut s'écrire comme $\delta_I \vee \bigvee_J \delta_J$ où la disjonction $\bigvee_J \delta_J$ est prise sur toutes les J contenant strictement I .

Il est clair que φ peut s'écrire comme disjonction des δ_I pour l'ensemble \mathcal{C} de parties de I telles que $\delta_I \Rightarrow \varphi$ au sens de 18.2 : il est également clair qu'on peut calculer \mathcal{C} algorithmiquement. Naturellement, \mathfrak{S}_n opère sur \mathcal{C} , c'est-à-dire que ce dernier est une réunion d'orbites.

Si \mathcal{X} est une réunion d'orbites de \mathfrak{S}_n agissant sur les parties de P , on notera encore $\pi_{\mathcal{X}}$ (resp. $\delta_{\mathcal{X}}$) la disjonction des π_I (resp. des δ_I) pour $I \in \mathcal{X}$. D'après le lemme précédent, les $\pi_{\mathcal{X}}$ (puisqu'ils définissent des fermés de Zariski invariants par \mathfrak{S}_n) peuvent s'écrire comme conjonction de formules de la forme $f = 0$ avec f symétrique en les X_i , et on peut calculer ces f algorithmiquement.

Montrons maintenant que si \mathcal{X} est une réunion d'orbites de \mathfrak{S}_n agissant sur les parties de P , alors $\delta_{\mathcal{X}}$ est une combinaison booléenne de formules de la forme $f = 0$ avec f symétrique en les X_i (en appliquant à $\mathcal{X} = \mathcal{C}$, ceci donnera le résultat voulu, vu que $\delta_{\mathcal{C}} = \varphi$). Pour cela, d'après ce qu'on vient de dire, il suffit de montrer que $\delta_{\mathcal{X}}$ est une combinaison booléenne des $\pi_{\mathcal{Y}}$. On peut évidemment supposer que \mathcal{X} est une unique orbite. On procède alors par récurrence décroissante sur le cardinal commun s des éléments de \mathcal{X} .

En écrivant $\pi_{\mathcal{X}} = \bigvee_{I \in \mathcal{X}} \pi_I$ et chaque π_I comme $\delta_I \vee \bigvee_J \delta_J$ (comme expliqué ci-dessus), on fait apparaître $\pi_{\mathcal{X}}$ comme la disjonction (exclusive!) de $\delta_{\mathcal{X}}$ et de certains δ_J pour J , tous de cardinal $> s$, parcourant un \mathcal{L} qui est une réunion d'orbites. Par l'hypothèse de récurrence, $\delta_{\mathcal{L}}$ s'écrit comme combinaison booléenne des $\pi_{\mathcal{Y}}$, donc il en va de même de $\delta_{\mathcal{X}} = \pi_{\mathcal{X}} \wedge \neg \delta_{\mathcal{L}}$. \square

25.4. Proposition. Soit $h : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{m+n} \rightarrow \mathbb{N}$ une fonction partielle calculable au sens de la définition 20.1, et telle que pour toute permutation $\sigma \in \mathfrak{S}_n$ on ait $h(i_1, \dots, i_r, z_1, \dots, z_m, x_1, \dots, x_n) = h(i_1, \dots, i_r, z_1, \dots, z_m, x_{\sigma(1)}, \dots, x_{\sigma(n)})$.

Pour k un corps algébriquement clos (variable) d'exposant caractéristique p , considérons l'application partielle f_k qui à $(i_1, \dots, i_r, z_1, \dots, z_m, c_1, \dots, c_n) \in \mathbb{N}^r \times k^{m+n}$ associe $h(i_1, \dots, i_r, z_1, \dots, z_m, \xi_1, \dots, \xi_n)$, où ξ_1, \dots, ξ_n sont les racines, avec multiplicités, du polynôme $X^n + c_1 X^{n-1} + \dots + c_n \in k[X]$. Alors les f_k définissent une fonction partielle calculable $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{m+n} \rightarrow \mathbb{N}$ (évidemment unique : cf. 20.2).

Démonstration. Suivant la définition 20.1, la fonction h est définie par une suite (énumérée par une machine de Turing) de parties constructibles $H_j = \{\phi_j\}$ de $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ et de valeurs $v_j \in \mathbb{N}$ associées. Quitte à remplacer ϕ_j par la disjonction des $\phi_j(z_1, \dots, z_m, x_{\sigma(1)}, \dots, x_{\sigma(n)})$ pour $\sigma \in \mathfrak{S}_n$ (ce qui ne change pas la valeur de h) d'après l'hypothèse faite sur celle-ci), on peut supposer que H_j vérifie $\sigma(H_j) = H_j$ pour tout $\sigma \in \mathfrak{S}_n$ (où σ opère sur $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ en permutant les n dernières coordonnées).

Il s'agit donc de voir que si H est une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ telle que $\sigma(H) = H$ pour tout $\sigma \in \mathfrak{S}_n$, alors le foncteur F qui à un corps k algébriquement clos d'exposant caractéristique p associe l'ensemble des $(z_1, \dots, z_m, c_1, \dots, c_n) \in k^n$ tels que $(z_1, \dots, z_m, \xi_1, \dots, \xi_n) \in H(k)$ où ξ_1, \dots, ξ_n

sont les racines, avec multiplicité, du polynôme $X^n + c_1 X^{n-1} + \dots + c_n \in k[X]$, définit bien une partie constructible de $\mathbb{A}_{\mathbb{F}_p}^{m+n}$ et que, de plus, cette partie constructible F se calcule effectivement en fonction de H (c'est-à-dire qu'on peut décrire une machine de Turing qui, en fonction d'une formule définissant H , produit une formule définissant F).

Or, en vertu des lemmes qui précèdent, on peut se ramener au cas où H est un fermé de Zariski défini par une unique équation $g = 0$ avec g un polynôme totalement symétrique en les n dernières variables. On sait alors algorithmiquement écrire g comme un polynôme (à coefficients dans \mathbb{F}_p) en les Z_1, \dots, Z_m et les fonctions symétriques élémentaires en X_1, \dots, X_n , ce qui donne les équations du fermé F recherché. \square

25.5. Proposition. *Le même énoncé que 25.4 vaut pour une fonction $h : \mathbb{N}^r \times \mathbb{A}_{\mathbb{F}_p}^{m+n} \rightarrow \mathbb{A}_{\mathbb{F}_p}^1$.*

Démonstration. Il suffit d'appliquer 24.3 pour se ramener à 25.4. \square

25.6. Remarque. Dans ces deux propositions, la fonction h est supposée vérifier $h(i_1, \dots, i_r, z_1, \dots, z_m, x_1, \dots, x_n) = h(i_1, \dots, i_r, z_1, \dots, z_m, x_{\sigma(1)}, \dots, x_{\sigma(n)})$ pour toute permutation σ des n dernières variables. On peut évidemment se passer de cette hypothèse si on n'exige d'avoir $f(i_1, \dots, i_r, z_1, \dots, z_m, c_1, \dots, c_n) = h(i_1, \dots, i_r, z_1, \dots, z_m, \xi_1, \dots, \xi_n)$ que lorsque le membre de droite ne dépend pas de la permutation des ξ_i — en effet, il suffit de remplacer, le cas échéant, la fonction h par une fonction h' qui calcule $h(i_1, \dots, i_r, z_1, \dots, z_m, x_{\sigma(1)}, \dots, x_{\sigma(n)})$ pour tout σ , renvoie la valeur commune si toutes ces valeurs sont toutes égales, et renvoie 42 si elles ne le sont pas.

On peut donc résumer ces résultats ainsi : dans le contexte de notre modèle de calcul universel, *on peut supposer qu'une fonction calculable peut calculer les racines d'un polynôme $X^n + c_1 X^{n-1} + \dots + c_n \in k[X]$ lorsque les calculs qu'elle fait avec ces racines sont invariants par toute permutation de celles-ci.*

25.7. Factorisation par simulation. Expliquons une autre manière de comprendre ces résultats, qui en fournit une démonstration différente, dans l'optique de la présentation « boîte noire » du modèle de calcul. Il s'agit donc d'expliquer pourquoi le fait d'ajouter à une machine de Turing, qui manipule dans des boîtes noires les éléments d'un corps k (parfait d'exposant caractéristique $p \geq 1$) non spécifié, la faculté de factoriser un polynôme dans sa clôture algébrique, n'augmente pas les fonctions qu'elle est capable de calculer.

Imaginons donc une machine de Turing qui effectue des calculs en manipulant les éléments de k dans des boîtes noires et qui dispose, en plus de la possibilité de calculer des additions, soustractions, multiplications, divisions, et Frobenius inverse (comme en 21), de la faculté de factoriser un polynôme. On souhaite expliquer comment effectuer les mêmes calculs sans cette faculté : il s'agit donc de simuler la possibilité de factoriser les polynômes. Dans la discussion qui suit, on appellera « programme simulé » la machine de Turing qui possède la faculté de factoriser les polynômes, et « simulateur » celui que nous décrivons, qui doit effectuer la même tâche sans factoriser de polynômes.

Le simulateur maintient une k -algèbre artinienne (c'est-à-dire de dimension finie comme k -espace vectoriel) et étale (c'est-à-dire géométriquement réduite, ou, ce qui revient au même puisque k est un corps parfait, réduite), que nous appellerons « algèbre courante » : celle-ci est vue comme quotient d'une algèbre de polynômes sur k par un idéal de celle-ci, et décrit par exemple par une base de Gröbner (cf. 13.1); au cours de l'exécution du simulateur, on pourra ajouter des indéterminées à cette « algèbre courante », ou des relations (c'est-à-dire faire grossir l'idéal), mais il y aura toujours un morphisme naturel de l'ancienne algèbre courante vers la nouvelle. Les éléments manipulés par le programme simulé (sous forme de boîtes noires) sont représentés, dans le simulateur, par des éléments de cette algèbre courante (et si l'algèbre courante est modifiée par l'ajout de nouvelles indéterminées ou de nouvelles relations, les éléments en question sont transportés par le morphisme naturel, c'est-à-dire qu'ils sont représentés par les mêmes polynômes dans les anciennes indéterminées).

Initialement, l'algèbre courante ne comporte pas d'indéterminées et pas de relations (elle est donc égale à k). Lorsque le programme simulé effectue une somme, une différence, ou un produit, le simulateur effectue la même opération dans l'algèbre courante.

Lorsque le programme simulé demande à calculer l'inverse d'un élément, représenté dans le simulateur par un élément x de l'algèbre courante, le simulateur ajoute une nouvelle indéterminée Y à

l'algèbre courante, et la relation $xY - 1 = 0$ (c'est-à-dire ajoute l'élément $xY - 1$ à ceux qui engendrent l'idéal des relations de l'algèbre courante), et il renvoie l'élément représenté par l'indéterminée Y . (Remarquons que l'algèbre courante peut devenir nulle, si x valait 0 : on s'apercevra ci-dessous du problème.)

Lorsque le programme simulé demande à calculer Frob_p^{-1} d'un élément représenté dans le simulateur par un élément x de l'algèbre courante, le simulateur ajoute une nouvelle indéterminée Y et la relation $Y^p - x = 0$; puis il calcule le réduit de cette algèbre (cf. par exemple [BECKER et WEISPFENNING 1993, théorème 8.22], qui utilise le « lemme 92 » de Seidenberg, [ibid., lemme 8.13]; on utilise bien sûr ici le fait que k est parfait et que le simulateur peut calculer Frob_p^{-1} dans k), et renvoie la classe de Y dans l'algèbre courante.

Lorsque le programme simulé demande à tester la nullité d'un élément représenté dans le simulateur par un élément x de l'algèbre courante, le simulateur ajoute une nouvelle indéterminée Y et la relation $Y - x = 0$ à l'algèbre courante, puis il calcule le polynôme $h \in k[Y]$ obtenu par l'élimination de toutes les autres variables de l'algèbre courante, c'est-à-dire le polynôme qui engendre l'intersection de $k[Y]$ avec l'idéal de $k[Y, \dots]$ définissant l'algèbre courante (où les points de suspension représentent d'autres indéterminées) : cf. [EISENBUD 1995, §15.10.4] pour un tel algorithme. Si le degré de h vaut 0 , cela signifie que l'algèbre courante est nulle, ce qui ne peut se produire que si le programme simulé a fait calculer l'inverse de 0 : dans ce cas, le simulateur exécute une boucle infinie (de façon à ne pas terminer). Sinon, et si h est de la forme Y^r (i.e., Y est nilpotent dans l'algèbre courante), le simulateur ajoute la relation $Y = 0$ et répond que x vaut 0 ; sinon, le simulateur ajoute la relation $h(Y)/Y^r = 0$ où r est l'ordre (=la valuation en Y) de h et répond que x ne vaut pas 0 . De même, si le programme simulé retourne x comme valeur finale, le simulateur effectue la même opération d'élimination : si le polynôme h est de degré 1 , le simulateur retourne son unique zéro comme valeur finale; s'il est de degré 0 (on a effectué une division par 0) ou > 1 (le programme simulé a violé la promesse de calculer une valeur qui ne dépende pas de la numérotation des racines des polynômes factorisés), le simulateur ne termine pas.

Enfin, si le programme simulé demande à factoriser un polynôme $P = X^n + c_1 X^{n-1} + \dots + c_n$, on ajoute à l'algèbre courante les indéterminées et relations de l'algèbre « de décomposition universelle » de P (cf. par exemple [LOMBARDI et QUITTÉ 2011, §III.4 et §VII.4]), c'est-à-dire l'algèbre A (finie sur k) quotient de $k[Z_1, \dots, Z_n]$ par les relations du type $e_i(Z_1, \dots, Z_n) - (-1)^i c_i$ où les e_i sont les fonctions symétriques élémentaires. (Rappelons que si $P = \prod_{i=1}^n (X - \xi_i)$, avec les ξ_i deux à deux distincts, est un polynôme séparable sur un corps, alors A est, en fait, isomorphe à $k^{\mathfrak{S}_n}$ par l'isomorphisme qui envoie Z_i sur l'ensemble des $\sigma(\xi_i)$ pour tous les $\sigma \in \mathfrak{S}_n$.) Puis on réduit l'algèbre courante, comme expliqué pour le calcul de Frob_p^{-1} . Le simulateur renvoie comme racines de P les indéterminées Z_1, \dots, Z_n qui viennent d'être ajoutées.

Pour montrer la correction de cet algorithme, il suffit de considérer les points de l'algèbre courante sur une clôture algébrique de k : il s'agit d'un nombre fini de tuples de valeurs de cette clôture algébrique, à savoir les valeurs que peuvent prendre les indéterminées pour une certaine numérotation des racines des polynômes factorisés. Dès lors que le programme simulé calcule une valeur ne dépend pas de cette numérotation, le simulateur effectue bien le calcul voulu.

25.8. Extensions de corps dans le modèle de calcul. Si k est un corps algébriquement clos d'exposant caractéristique $p \geq 1$, dont les éléments sont manipulés sous forme de « boîtes noires » (c'est-à-dire dans le cadre du modèle de calcul développé ici), on peut encore manipuler les éléments de tous les corps obtenus à partir de k par itération des extensions énumérées en 12.5, à savoir

- (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 » 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 ,

en utilisant essentiellement les mêmes algorithmes qu'expliqués en *loc. cit.* L'algorithme de Rabin pour construire la clôture algébrique n'est pas applicable tel quel, mais on peut le remplacer par celui,

essentiellement équivalent, décrit en 25.7 qui permet de manipuler les éléments de «la» clôture algébrique d'un corps K (ou plutôt, de toutes ses clôtures algébriques simultanément) si on sait manipuler ceux de K (la construction suppose K parfait, mais ceci n'est pas une difficulté puisqu'on peut de toute façon passer d'abord à la clôture parfaite de K).

26. INDÉPENDANCE DE LA CARACTÉRISTIQUE (ESQUISSE)

Toute la description faite jusqu'ici du modèle de calcul «universel» supposait fixée la caractéristique du corps manipulé. Esquissions maintenant la manière dont il faudrait modifier les choses pour obtenir l'uniformité en p . L'intuition sous-jacente, dans la présentation «boîte noire» est que la machine qui manipule des boîtes noires ne peut jamais être sûre d'être en caractéristique 0, elle peut seulement tester si $p \neq 0$ pour différentes valeurs de p , et donc minorer la caractéristique; par ailleurs, elle ne peut appliquer Frob_p^{-1} qu'à condition que la caractéristique vaille effectivement p (sous peine que la fonction ne soit pas définie).

26.1. Types et parties constructibles. On appelle formule booléenne en X_1, \dots, X_n sur \mathbb{Z} une combinaison booléenne d'expressions de la forme $f(X_1, \dots, X_n) = 0$ où $f \in \mathbb{Z}[X_1, \dots, X_n]$; on lui associe une partie constructible de $\mathbb{A}_{\mathbb{Z}}^n$, ou de k^n pour k un corps quelconque, de la façon évidente. L'analogue de 18.2 vaut encore, en remplaçant « \mathbb{F}_p » par « \mathbb{Z} » et en supprimant les mots «d'exposant caractéristique p ». On remarquera, par exemple, que la formule $p = 0$ définit la partie pleine sur les corps de caractéristique p et la partie vide sur les corps de caractéristique $\neq p$.

26.2. Fonctions F-rationnelles. On définit la notion de «fonction F-rationnelle sur \mathbb{Z} » de façon stupide : une telle fonction est soit la donnée d'une fonction rationnelle sur \mathbb{Q} (c'est-à-dire le quotient de deux polynômes à coefficients dans \mathbb{Z} , qu'on peut supposer sans facteur premier non trivial), auquel cas elle est définie aux points où son dénominateur réduit ne s'annule pas, soit la donnée d'une fonction F-rationnelle sur \mathbb{F}_p pour un $p > 0$ (c'est-à-dire pouvant faire intervenir Frob_p^{-1}), auquel cas elle n'est définie que sur les corps de caractéristique p . Pour déplaisante que soit cette définition, la notion de fonction calculable qui en résulte est raisonnable.

26.3. Fonctions partielles calculables. On définit la notion de fonction partielle calculable $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$ ou $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{A}_{\mathbb{Z}}^1$ comme dans les définitions 20.1 et 20.4, en remplaçant « \mathbb{F}_p » par « \mathbb{Z} » et en supprimant les mots «d'exposant caractéristique p ».

À titre d'exemple, la fonction (*partielle!*) qui renvoie la caractéristique du corps k si celle-ci est non nulle, et non définie si k est de caractéristique nulle, est calculable : il suffit d'énumérer les formules $p = 0$ (pour p parcourant les nombres premiers) et la valeur p (autrement dit, la machine teste successivement les nombres premiers et retourne la valeur p si elle constate que $p = 0$).

L'équivalence avec le modèle «boîte noire» se montre alors sans difficulté nouvelle : on souligne que la machine peut appliquer une fonction Frob_p^{-1} pour n'importe quel p (mais dès qu'elle le fait, la fonction cesse d'être définie si la caractéristique ne valait pas p).

26.4. Fonctions totales. On dira qu'une fonction partielle calculable $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$ ou $f : \mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{A}_{\mathbb{Z}}^1$ est **totale** lorsque sa valeur est définie pour toutes valeurs $(i_1, \dots, i_r, x_1, \dots, x_n)$, les x_1, \dots, x_n appartenant à n'importe quel corps parfait k (quelle que soit sa caractéristique).

L'analogue de 22.3(A) est qu'une fonction est totale lorsque, pour chaque $p \geq 1$, elle est définie en tous les $(i_1, \dots, i_r, x_1, \dots, x_n)$ où x_1, \dots, x_n appartenant à K_p , corps algébriquement clos d'exposant caractéristique p et de degré de transcendance infini sur \mathbb{F}_p . L'énoncé 22.3(B) reste valable sans modification. Le corollaire 22.4 devient l'énoncé suivant (exactement analogue, mais suffisamment notable pour être répété intégralement) :

26.5. Corollaire. *Une fonction totale calculable $\mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$ est exactement la donnée d'une partition de $\mathbb{A}_{\mathbb{Z}}^n$ en un nombre fini de parties constructibles, sur chacune desquelles la fonction prend une valeur constante entière (en particulier, la fonction est bornée).*

Une fonction totale calculable $\mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{A}_{\mathbb{Z}}^m$ est exactement la donnée d'une partition de $\mathbb{A}_{\mathbb{Z}}^n$ en un nombre fini de parties constructibles, sur chacune desquelles la fonction coïncide avec une certaine fonction F-rationnelle (définie partout sur la partie en question : donc soit une fonction rationnelle sur \mathbb{Q} , soit une fonction F-rationnelle sur \mathbb{F}_p uniquement sur une partie constructible du fermé $\mathbb{A}_{\mathbb{F}_p}^n$ de $\mathbb{A}_{\mathbb{Z}}^n$).

Une fonction totale calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$ ou $\mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{A}_{\mathbb{Z}}^m$ est exactement la donnée d'une fonction calculable au sens usuel qui à toute valeur (i_1, \dots, i_r) des r premiers paramètres associe une donnée comme décrite dans les deux paragraphes précédents.

À titre d'exemple, la fonction qui calcule la caractéristique de k n'est pas calculable (puisque'elle est totale et ne répond pas aux conditions de ce corollaire); en revanche, la fonction qui calcule la caractéristique de k si celle-ci est $\leq p_0$ (pour un certain p_0), et 0 si la caractéristique est $> p_0$, est bien calculable.

Notons la conséquence immédiate suivante :

26.6. Corollaire. Soit f une fonction totale calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$, et soient $i_1, \dots, i_r \in \mathbb{N}$ et $x_1, \dots, x_n \in \mathbb{Z}$. Alors il existe p_0 tel que la valeur de f en $(i_1, \dots, i_r, x_1, \dots, x_n)$ ne dépende pas de p si $p \geq p_0$ ou $p = 1$, où on considère x_1, \dots, x_n comme des éléments d'un corps d'exposant caractéristique p (cette valeur ne dépend pas non plus du corps choisi). De plus, ce p_0 peut être calculé algorithmiquement.

On a un résultat analogue pour une fonction totale calculable $\mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{A}_{\mathbb{Z}}^m$: pour tous $i_1, \dots, i_r \in \mathbb{N}$ et $x_1, \dots, x_n \in \mathbb{Z}$, il existe p_0 , calculable algorithmiquement, et des rationnels y_1, \dots, y_m dont le dénominateur n'est divisible par aucun nombre premier $\geq p_0$, tel que la valeur de f en $(i_1, \dots, i_r, x_1, \dots, x_n)$, où on considère x_1, \dots, x_n comme des éléments d'un corps d'exposant caractéristique p , soit égale à \underline{y} modulo p si $p \geq p_0$, et à \underline{y} si $p = 1$.

Démonstration. Considérons le cas d'une fonction $\mathbb{N}^r \times \mathbb{A}_{\mathbb{Z}}^n \rightarrow \mathbb{N}$. L'évaluation de f en $(i_1, \dots, i_r, x_1, \dots, x_n)$ définit une fonction calculable totale de 0 variables, c'est-à-dire $\mathbb{A}_{\mathbb{Z}}^0 \rightarrow \mathbb{N}$ (ici, évidemment, $\mathbb{A}_{\mathbb{Z}}^0$ est $\text{Spec } \mathbb{Z}$) elle est donc décrite, comme ci-dessus, par une partition de $\text{Spec } \mathbb{Z}$ en un nombre fini de parties constructibles, calculables algorithmiquement : il suffit de renvoyer un p_0 plus grand que tous les p intervenant dans les formules booléennes (qui ne peuvent être que $p = 0$) décrivant ces parties constructibles.

Le second cas est complètement analogue : la donnée d'une fonction calculable $\mathbb{A}_{\mathbb{Z}}^0 \rightarrow \mathbb{A}_{\mathbb{Z}}^m$ revient à se donner des rationnels sur un nombre fini de parties constructibles de $\text{Spec } \mathbb{Z}$. \square

Bibliographie

SIGLES

- ÉGA I Alexander GROTHENDIECK (1960). « Éléments de géométrie algébrique. I. Le langage des schémas ». *Publications mathématiques de l'IHÉS* 4. Rédigés avec la collaboration de Jean Dieudonné, 5–228.
- ÉGA II Alexander GROTHENDIECK (1961a). « Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes ». *Publications mathématiques de l'IHÉS* 8. Rédigés avec la collaboration de Jean Dieudonné, 5–222.
- ÉGA III₁ Alexander GROTHENDIECK (1961b). « Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents (Première partie) ». *Publications mathématiques de l'IHÉS* 11. Rédigés avec la collaboration de Jean Dieudonné, 5–167.
- ÉGA III₂ Alexander GROTHENDIECK (1963). « Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents (Seconde partie) ». *Publications mathématiques de l'IHÉS* 17. Rédigés avec la collaboration de Jean Dieudonné, 5–91.
- ÉGA I_{Spr} Alexander GROTHENDIECK et Jean DIEUDONNÉ (1971). *Éléments de géométrie algébrique. I*. Grundlehren der mathematischen Wissenschaften 166. Springer-Verlag.
- ÉGA IV₁ Alexander GROTHENDIECK (1964). « Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Première partie) ». *Publications mathématiques de l'IHÉS* 20. Rédigés avec la collaboration de Jean Dieudonné, 5–259.
- ÉGA IV₂ Alexander GROTHENDIECK (1965). « Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Seconde partie) ». *Publications mathématiques de l'IHÉS* 24. Rédigés avec la collaboration de Jean Dieudonné, 5–231.
- ÉGA IV₃ Alexander GROTHENDIECK (1966). « Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Troisième partie) ». *Publications mathématiques de l'IHÉS* 28. Rédigés avec la collaboration de Jean Dieudonné, 5–255.






- ÉGA IV₄ Alexander GROTHENDIECK (1967). « Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas (Quatrième partie) ». *Publications mathématiques de l'IHÉS* **32**. Rédigés avec la collaboration de Jean Dieudonné, 5–361.
- SGA 1 Alexander GROTHENDIECK (2003). *Revêtements étales et groupe fondamental. Séminaire de géométrie algébrique du Bois-Marie 1960–1961 (SGA 1)*. Documents mathématiques **3**. Réédition LNM 224. Soc. math. France.
- SGA 4 Michael ARTIN, Alexander GROTHENDIECK et Jean-Louis VERDIER (1972–1973). *Théorie des topos et cohomologie étale des schémas. Séminaire de géométrie algébrique du Bois-Marie 1963–1964 (SGA 4)*. Lecture Notes in Mathematics **269, 270, 305**. Springer-Verlag.
- SGA 4½ Pierre DELIGNE (1977). *Cohomologie étale*. Lecture Notes in Mathematics **569**. Avec la collaboration de J.-F. Boutot, A. Grothendieck, L. Illusie et J.-L. Verdier. Springer-Verlag, iv+312 pages.

RÉFÉRENCES

- ABBES, Ahmed et Michel GROS (2011). « Topos co-évanescents et généralisations ». Prépublication, [arXiv:1107.2380v2](https://arxiv.org/abs/1107.2380v2) (↑ p. 10).
- ACHAR, Pramod N. et Daniel S. SAGE (2009). « Perverse coherent sheaves and the geometry of special pieces in the unipotent variety ». *Adv. Math.* **220**(4). [DOI](#), 1265–1296 (↑ p. 46).
- ANDERSON, Greg W. (2002). « Abelianities and their application to an elementary construction of Jacobians ». *Adv. Math.* **172**(2). [DOI](#), 169–205 (↑ p. 3, 14).
- ARTIN, Michael (1971). « On the joins of Hensel rings ». *Advances in Math.* **7**, 282–296 (↑ p. 2).
– (1973). *Théorèmes de représentabilité pour les espaces algébriques*. Les presses de l'université de Montréal, 282 pages (↑ p. 30).
- AVIGAD, Jeremy (2003). « Number theory and elementary arithmetic ». *Philos. Math.* **11**(3). [DOI](#), 257–284 (↑ p. 33).
- BAYER, Dave et David MUMFORD (1993). « What can be computed in algebraic geometry? ». Dans [EISENBUD et ROBBIANO 1993, pages 1–48] (↑ p. 51).
- BECKER, Thomas et Volker WEISPFENNING (1993). *Gröbner bases*. Graduate Texts in Mathematics **141**. Springer-Verlag, xxii+574 pages (↑ p. 38, 44, 67).
- BHATT, Bhargav (2011). « Derived splinters in positive characteristic ». Prépublication, [arxiv:1109.0354v1](https://arxiv.org/abs/1109.0354v1) (↑ p. 31).
- BORCEUX, Francis (1994). *Handbook of categorical algebra 1. Basic category theory*. Encyclopedia of Mathematics and its Applications **50**. Cambridge University Press, xvi+345 pages (↑ p. 16).
- BOSCH, Siegfried, Werner LÜTKEBOHMERT et Michel RAYNAUD (1990). *Néron models*. Springer-Verlag, x+325 pages (↑ p. 51).
- BOURBAKI, Nicolas (2007). *Éléments de mathématique. Algèbre, chapitres 4 à 7*. Réimpression inchangée de la deuxième édition (Masson, 1981). Springer-Verlag, vii+422 pages (↑ p. 35).
- CARLSON, Jon F. (2001). « Calculating group cohomology: tests for completion ». *J. Symbolic Comput.* **31**(1-2). [DOI](#), 229–242 (↑ p. 19).
- CONRAD, Brian (2003). « Cohomological Descent ». [DOI](#) (↑ p. 11, 12).
- COX, David, John LITTLE et Donal O'SHEA (2007). *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra*. Troisième édition. Undergraduate Texts in Mathematics. Springer, xvi+551 pages (↑ p. 43, 50).
- DE JONG, Aise Johan (1996). « Smoothness, semi-stability and alterations ». *Publications mathématiques de l'IHÉS* **83**, 51–93 (↑ p. 11, 14, 31, 33, 38).
- DE JONG, Theo (1998). « An algorithm for computing the integral closure ». *J. Symbolic Comput.* **26**(3). [DOI](#), 273–277 (↑ p. 40, 45).
- DEBARRE, Olivier (2001). *Higher-dimensional algebraic geometry*. Universitext. Springer-Verlag, xiv+233 pages (↑ p. 51).
- DECKER, Wolfram et Christoph LOSSEN (2006). *Computing in algebraic geometry: A quick start using SINGULAR*. Algorithms and Computation in Mathematics **16**. Springer-Verlag, xvi+327 pages (↑ p. 38, 39).
- DELIGNE, Pierre (1974). « Théorie de Hodge. III ». *Publications mathématiques de l'IHÉS* **44**, 5–77 (↑ p. 11–13, 17, 26, 28, 29).

- (1980). «La conjecture de Weil. II». *Publications mathématiques de l’IHÉS* **52**, 137–252 (↑ p. 2, 29, 32).
- DELIGNE, Pierre et al. (1982). *Hodge cycles, motives, and Shimura varieties*. Lecture Notes in Mathematics **900**. Springer-Verlag, ii+414 pages (↑ p. 5, 6).
- DIXON, John D. et al. (1999). *Analytic pro- p groups*. Seconde édition. Cambridge Studies in Advanced Mathematics **61**. Cambridge University Press, xviii+368 pages (↑ p. 14–16).
- DOLD, Albrecht et Dieter PUPPE (1961). «Homologie nicht-additiver Funktoren. Anwendungen». *Ann. Inst. Fourier* **11**, 201–312 (↑ p. 18).
- DRIES, Lou van den et K. SCHMIDT (1984). «Bounds in the theory of polynomial rings over fields. A nonstandard approach». *Invent. math.* **76**(1), 77–91 (↑ p. 46).
- EDIXHOVEN, Bas et Jean-Marc COUVEIGNES, éd. (2011). *Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujan’s tau at a prime*. Annals of Mathematics Studies **176**. Princeton University Press, xii+425 pages (↑ p. 2).
- EISENBUD, David (1995). *Commutative algebra, with a view toward algebraic geometry*. Graduate Texts in Mathematics **150**. Springer-Verlag, xvi+785 pages (↑ p. 37–46, 67).
- EISENBUD, David et Lorenzo ROBBIANO, éd. (1993). *Computational algebraic geometry and commutative algebra (Cortona, 1991)*. Symposia Mathematica **34**. Cambridge University Press, x+298 pages (↑ p. 70).
- ELKIK, Renée (1973). «Solutions d’équations à coefficients dans un anneau hensélien». *Ann. sci. École norm. sup.* **6**, 553–603 (↑ p. 46).
- EVENS, Leonard (1991). *The cohomology of groups*. Oxford Mathematical Monographs. Oxford University Press, xii+159 pages (↑ p. 19).
- FALTINGS, Gerd (1988). « p -adic Hodge theory». *J. Amer. Math. Soc.* **1**(1), 255–299 (↑ p. 2).
- FERRAND, Daniel (2003). «Conducteur, descente et pincement». *Bull. Soc. math. France* **131**(4), 553–585 (↑ p. 29, 49).
- FRIED, Michael D. et Moshe JARDEN (2008). *Field arithmetic*. Troisième édition. Ergebnisse der Mathematik und ihrer Grenzgebiete **11**. Springer-Verlag, xxiv+792 pages (↑ p. 27, 35, 36, 50, 53, 61).
- FRIEDLANDER, Eric M. (1982). *Étale homotopy of simplicial schemes*. Annals of Mathematics Studies **104**. Princeton University Press, vii+190 pages (↑ p. 5, 8).
- FRÖHLICH, Albrecht et John C. SHEPHERDSON (1956). «Effective procedures in field theory». *Philos. Trans. Roy. Soc. London. Ser. A.* **248**, 407–432 (↑ p. 34, 35).
- GABBER, Ofer (2001). «Lettre à F. Orgogozo (2001-12-28)» (↑ p. 18).
- GABBER, Ofer et Lorenzo RAMERO (2003). *Almost ring theory*. Lecture Notes in Mathematics **1800**. Springer-Verlag (↑ p. 46).
- GABRIEL, Peter et Michel ZISMAN (1967). *Calculus of fractions and homotopy theory*. Ergebnisse der Mathematik und ihrer Grenzgebiete **35**. Springer-Verlag, x+168 pages (↑ p. 15).
- GIANNI, Patrizia, Barry TRAGER et Gail ZACHARIAS (1988). «Gröbner bases and primary decomposition of polynomial ideals». *J. Symbolic Comput.* **6**(2-3), 149–167 (↑ p. 44).
- GIRAUD, Jean (1971). *Cohomologie non abélienne*. Grundlehren der mathematischen Wissenschaften **179**. Springer-Verlag, ix+467 pages (↑ p. 5–7, 9, 11, 13).
- GRAUERT, Hans et Reinhold REMMERT (1984). *Coherent analytic sheaves*. Grundlehren der mathematischen Wissenschaften **265**. Springer-Verlag, xviii+249 pages (↑ p. 45).
- GRIFFOR, Edward R., éd. (1999). *Handbook of computability theory*. Studies in Logic and the Foundations of Mathematics **140**. North-Holland Publishing Co., xii+727 pages (↑ p. 73).
- GROTHENDIECK, Alexander (1956). «Théorèmes de finitude pour la cohomologie des faisceaux». *Bull. Soc. math. France* **84**, 1–7 (↑ p. 20).
- (1957). «Sur quelques points d’algèbre homologique». *Tôhoku Math. J.* **9**, 119–221 (↑ p. 20).
- (197?). «Pré-notes ÉGA V» (↑ p. 8).
- GROTHENDIECK, Alexander et Jakob Pieter MURRE (1971). *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*. Lecture Notes in Mathematics **208**. Springer-Verlag (↑ p. 8).
- HAIMAN, Mark et Bernd STURMFELS (2004). «Multigraded Hilbert schemes». *J. Algebraic Geom.* **13**(4), 725–769 (↑ p. 3).

- HÁJEK, Petr et Pavel PUDLÁK (1998). *Metamathematics of first-order arithmetic*. Perspectives in Mathematical Logic. Springer-Verlag, xiv+460 pages (↑ p. 33).
- HEß, Florian (2002). « Computing Riemann-Roch spaces in algebraic function fields and related topics ». *J. Symbolic Comput.* **33**(4). [DOI](#), 425–445 (↑ p. 14).
- HOFSTADTER, Douglas R. (1999). *Gödel, Escher, Bach: an Eternal Golden Braid*. Basic Books, 23+xxi+777 pages (↑ p. 33).
- HUNEKE, Craig et Irena SWANSON (2006). *Integral closure of ideals, rings, and modules*. London Mathematical Society Lecture Note Series **336**. Cambridge University Press, xiv+431 pages (↑ p. 45, 46).
- ILLUSIE, Luc (1971-1972). *Complexe cotangent et déformations*. **239, 283**. Lecture Notes in Mathematics. Springer-Verlag (↑ p. 17, 26, 28, 29, 46).
- JACOBSSON, Carl et Viggo STOLTENBERG-HANSEN (1985). « Poincaré-Betti series are primitive recursive ». *J. London Math. Soc.* **31**(1). [DOI](#), 1–9 (↑ p. 34).
- KASHIWARA, Masaki et Pierre SCHAPIRA (2006). *Categories and sheaves*. Grundlehren der mathematischen Wissenschaften **332**. Springer-Verlag, x+497 pages (↑ p. 20).
- KATZ, Nicholas M. et Gérard LAUMON (1985). « Transformation de Fourier et majoration de sommes exponentielles ». *Publications mathématiques de l’IHÉS* **62**, 361–418 (↑ p. 3).
- LOMBARDI, Henri et Claude QUITTÉ (2011). *Algèbre commutative (Méthodes constructives)*. Mathématiques en devenir. Calvage & Mounet, xxxi+991 pages (↑ p. 40, 67).
- LUBOTZKY, Alexander et Dan SEGAL (2003). *Subgroup Growth*. Progress in Mathematics **212**. Birkhäuser, xxii+453 pages (↑ p. 22).
- MADORE, David (2014). <http://mathoverflow.net/q/156091/17064> (↑ p. 46).
- MARKER, David (2002). *Model Theory: An Introduction*. Graduate Texts in Mathematics **217**. Springer-Verlag (↑ p. 53–55, 60, 62).
- MATSUMURA, Hideyuki (1989). *Commutative ring theory*. Cambridge Studies in Advanced Mathematics **8**. Cambridge University Press, xiv+320 pages (↑ p. 35).
- MILLER, Russell (2010). « Is it harder to factor a polynomial or to find a root? ». *Trans. Amer. Math. Soc.* **362**(10). [DOI](#), 5261–5281 (↑ p. 34).
- MILNE, James S. (1980). *Étale cohomology*. Princeton University Press, xiii+323 pages (↑ p. 2, 30, 51).
- MOCHIZUKI, Shinichi (1999). « Extending families of curves over log regular schemes ». *J. reine angew. Math.* **511**, 43–71 (↑ p. 8).
- MUMFORD, David (1975). *Curves and their Jacobians*. The University of Michigan Press, vi+104 pages (↑ p. 3).
- NEUKIRCH, Jürgen, Alexander SCHMIDT et Kay WINGBERG (2000). *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften **323**. Springer-Verlag, xvi+699 pages (↑ p. 14, 22, 23).
- ODIFREDDI, Piergiorgio (1989). *Classical recursion theory*. Studies in Logic and the Foundations of Mathematics **125**. North-Holland, xviii+668 pages (↑ p. 4, 33, 37, 52, 55, 58).
- (1999). *Classical recursion theory. II*. Studies in Logic and the Foundations of Mathematics **143**. North-Holland, xvi+949 pages (↑ p. 33).
- OGG, Andrew Pollard (1962). « Cohomology of abelian varieties over function fields ». *Ann. of Math.* **76**, 185–212 (↑ p. 23).
- OLIVIER, Jean-Pierre (1966-1968). « Anneaux absolument plats universels et épimorphismes à buts réduits ». *Séminaire Samuel. Algèbre commutative 2*. exp. 6 (↑ p. 53, 61).
- ORGOGOZO, Fabrice (2003). « Altérations et groupe fondamental premier à p ». *Bull. Soc. math. France* **131**, 123–147 (↑ p. 5, 6).
- (2013). « Sur les propriétés d’uniformité des images directes en cohomologie étale ». Prépublication (↑ p. 3, 30).
- PALMER, Theodore W. (1974). « Arens multiplication and a characterization of W^* -algebras ». *Proc. Amer. Math. Soc.* **44**, 81–87 (↑ p. 46).
- PETERSEN, Dan (2010). <http://mathoverflow.net/a/20790/17064> (↑ p. 42).
- POONEN, Bjorn, Damiano TESTA et Ronald van LUIJK (2012). « Computing Néron–Severi groups and cycle class groups ». Prépublication, [arXiv:1210.3720v3](https://arxiv.org/abs/1210.3720v3) (↑ p. 2, 3).

- RABIN, Michael O. (1960). « Computable algebra, general theory and theory of computable fields ». *Trans. Amer. Math. Soc.* **95**, 341–360 (↑ p. 34).
- ROTMAN, Joseph J. (1995). *An introduction to the theory of groups*. Quatrième édition. Graduate Texts in Mathematics **148**. Springer-Verlag, xvi+513 pages (↑ p. 15, 24).
- RUBIO, Julio et Francis SERGERAERT (2002). « Constructive algebraic topology ». *Bull. sci. math.* **126**(5). , 389–412 (↑ p. 20).
- SCHÖN, Rolf (1991). « Effective algebraic topology ». *Mem. Amer. Math. Soc.* **92**(451), vi+63 (↑ p. 3, 20).
- SERGERAERT, Francis (1994). « The computability problem in algebraic topology ». *Adv. Math.* **104**(1). , 1–29 (↑ p. 2).
- SERRE, Jean-Pierre (1955). « Faisceaux algébriques cohérents ». *Ann. of Math.* **61**, 197–278 (↑ p. 51).
- (1965). *Algèbre locale. Multiplicités*. Lecture Notes in Mathematics **11**. Springer-Verlag, vii+188 pages (↑ p. 37, 45, 46).
 - (1975). *Groupes algébriques et corps de classes*. Seconde édition. Actualités scientifiques et industrielles, 1264. Hermann, 207 pages (↑ p. 14).
 - (1977). *Arbres, amalgames, SL_2* . Astérisque **46**. Société mathématique de France, 189 pp. pages (↑ p. 24).
 - (1978-79). « Groupes finis ». Notes d’un cours à l’ÉNSJF ; [arXiv:0503154v6](https://arxiv.org/abs/0503154v6) (↑ p. 15).
 - (1994). *Cohomologie galoisienne*. Cinquième édition révisée et complétée. Lecture Notes in Mathematics **5**. Springer-Verlag (↑ p. 9, 19, 22, 23, 25).
 - (2013). Lettre à F. Orgogozo (2013-3-19) (↑ p. 24).
- SIMPSON, Carlos (2008). « Algebraic cycles from a computational point of view ». *Theoret. Comput. Sci.* **392**(1-3). , 128–140 (↑ p. 2).
- SIMPSON, Stephen G. (2009). *Subsystems of second order arithmetic*. Seconde édition. Perspectives in Logic. Cambridge University Press, xvi+444 pages (↑ p. 33).
- SINGH, Anurag K. et Irena SWANSON (2009). « An algorithm for computing the integral closure ». *Algebra Number Theory* **3**(5). , 587–595 (↑ p. 45).
- STEEL, Allan (2005). « Conquering inseparability: primary decomposition and multivariate factorization over algebraic function fields of positive characteristic ». *J. Symbolic Comput.* **40**(3), 1053–1075 (↑ p. 37, 44).
- STOLTENBERG-HANSEN, Viggo et John V. TUCKER (1999). « Computable rings and fields ». Dans [GRIFFOR 1999, chapitre 12], 363–447 (↑ p. 34, 35).
- STOLZENBERG, Gabriel (1968). « Constructive normalization of an algebraic variety ». *Bull. Amer. Math. Soc.* **74**, 595–599 (↑ p. 45).
- SZAMUELY, Tamás (2009). *Galois groups and fundamental groups*. Cambridge Studies in Advanced Mathematics **117**. Cambridge University Press, x+270 pages (↑ p. 9).
- VASCONCELOS, Wolmer (2005). *Integral closure. Rees algebras, multiplicities, algorithms*. Springer Monographs in Mathematics. Springer-Verlag, xii+519 pages (↑ p. 44–46).
- WINGBERG, Kay (1984). « Ein Analogon zur Fundamentalgruppe einer Riemann’schen Fläche im Zahlkörperfall ». *Invent. math.* **77**(3). , 557–584 (↑ p. 10).
- ZARISKI, Oscar et Pierre SAMUEL (1975). *Commutative algebra*. **28, 29**. Graduate Texts in Mathematics. Springer-Verlag, xi+329, x+414 pages (↑ p. 45).