Astérisque

JEAN-PIERRE SERRE

Revêtements de courbes algébriques

Astérisque, tome 206 (1992), Séminaire Bourbaki,
exp. n° 749, p. 167-182

<http://www.numdam.org/item?id=SB_1991-1992__34__167_0>

Séminaire BOURBAKI Novembre 1991
44ème année, 1991/92, n° 749

REVÊTEMENTS DE COURBES ALGÉBRIQUES

par Jean-Pierre SERRE

1. INTRODUCTION

1.1. Le problème

Soit k un corps algébriquement clos. Soit C une courbe algébrique sur k, supposée irréductible et lisse. On a :

$$C = \overline{C} - S,$$

où $\overline{C}$ est une courbe projective lisse, et S un sous-ensemble fini de $\overline{C}(k)$.

Quels sont les revêtements galoisiens (non ramifiés) *de* C ?

On peut préciser cette question de deux façons :

(a) On se donne un groupe fini G. On demande à quelle condition il existe un revêtement galoisien connexe $C' \to C$ de groupe G.

(b) Soit $\pi_C = \pi_1^{\text{alg}}(C, x)$ le groupe fondamental (algébrique) de la courbe C relativement à un point-base x. Ce groupe est un groupe profini. On demande de déterminer sa structure.

Remarque.— 1) Noter que (b) est plus précis que (a) : un groupe fini G satisfait à la condition (a) si et seulement si G est isomorphe à un quotient de π_C.

2) Lorsque l'on remplace le corps de base k par une extension algébriquement close k', le groupe π_C ne change pas, si la caractéristique est 0. Il n'est va plus de même en caractéristique $p > 0$: il existe des familles non

constantes de revêtements. Toutefois, les quotients finis de π_C sont les mêmes sur k et sur k', comme le montre un argument de spécialisation. La question (a) est donc "indépendante" du corps de base choisi (pourvu, bien sûr, qu'il soit algébriquement clos).

1.2. Le cas complexe

Lorsque $k = \mathbf{C}$, le *théorème d'existence de Riemann* dit que tout revêtement fini (au sens topologique) de la surface $C(\mathbf{C})$ possède une structure algébrique et une seule compatible avec sa projection sur $C(\mathbf{C})$ (*cf.* par exemple [5], chap. VI). Cela permet de répondre aux questions (a) et (b) ci-dessus. Pour (b), la réponse est la suivante : si g est le genre de $\overline{C}$, et $s = |S|$, le groupe π_C est le *complété profini* (*i.e.* le complété pour la topologie des sous-groupes d'indice fini) du groupe défini par $2g + s$ générateurs a_i, b_i $(i = 1, \cdots, g)$ et c_j $(j = 1, \cdots, s)$ liés par la relation

$$a_1\, b_1\, a_1^{-1}\, b_1^{-1} \cdots a_g\, b_g\, a_g^{-1}\, b_g^{-1}\, c_1 \cdots c_s = 1\,.$$

Lorsque $S \neq \emptyset$ (*i.e.* lorsque C est affine), ce groupe est un groupe libre de rang $2g + s - 1$. Dans ce cas, la réponse à la question (a) du n° 1.1 s'énonce très simplement : un groupe fini G convient si et seulement si il peut être engendré par $2g + s - 1$ éléments.

(La théorie de Riemann donne en fait un résultat plus précis : les éléments $c_1, \cdots, c_s$ peuvent être choisis de telle sorte qu'ils engendrent des groupes d'inertie au-dessus des points de S.)

1.3. Le cas de caractéristique 0

Lorsque la caractéristique de k est 0, le principe de Lefschetz, combiné avec des arguments de spécialisation, montre que *les résultats du* n° 1.2 *restent valables sans changement.*

Noter que, bien que ces résultats s'énoncent algébriquement, la seule démonstration que l'on en ait repose sur la théorie transcendante pour $k = \mathbf{C}$ (le point essentiel est de montrer qu'une surface de Riemann compacte a suffisamment de fonctions méromorphes).

Une tentative pour attaquer "algébriquement" la classification des revêtements avait été faite par Weil en 1938 (*cf.* [21], p. 84-86, ainsi que V.

Nori, *Comp. Math.* **33** (1976), p. 29-41). Son point de départ est le suivant : tout revêtement galoisien $C' \to C$ de groupe G, donne naissance (par l'intermédaire des représentations linéaires de G) à des *fibrés vectoriels* sur C, qui ont la propriété de satisfaire à des équations algébriques vis-à-vis de la somme directe et du produit tensoriel. Si l'on pouvait expliciter la structure des *variétés de modules* de fibrés vectoriels avec assez de précision, on pourrait en déterminer les éléments algébriques et remonter de là aux revêtements galoisiens. Cette approche "tannakienne" du problème est intéressante, mais n'a jusqu'à présent abouti à rien de concret ; même le cas élémentaire $g = 1$, $s = 0$, semble difficile à traiter par cette méthode.

1.4. Le cas de caractéristique $p > 0$

Ce cas est resté longtemps inexploré. Voici ce qu'en disait Weil en 1946, dans [22] :

"... avant d'aborder la détermination des extensions de corps de nombres par leurs propriétés locales, il conviendrait peut-être de résoudre le problème analogue, déjà fort difficile, au sujet des fonctions algébriques d'une variable sur un corps de base fini, c'est-à-dire d'étendre à ces fonctions les théorèmes d'existence de Riemann. Pour ne citer qu'un cas particulier, le groupe modulaire, dont la structure détermine les corps de fonctions d'une variable complexe ramifiés en trois points seulement, joue-t-il le même rôle, tout au moins en ce qui concerne les extensions de degré premier à la caractéristique, quand le corps de base est fini ? Il n'est pas impossible que toutes les questions de ce genre puissent se traiter par une méthode uniforme, qui permettrait, d'un résultat une fois établi (par exemple par voie topologique) pour la caractéristique 0, de déduire le résultat correspondant pour la caractéristique p; la découverte d'un tel principe constituerait un progrès de la plus grande importance..."

Ce texte suggérait deux choses :

(i) Pour les groupes d'ordre premier à p, la théorie est la même qu'en caractéristique zéro;

(ii) Il doit être possible de passer de la caractéristique zéro à la caractéristique p (et inversement).

L'assertion (i) a été précisée en 1956 par Abhyankar ([1]) sous la forme de la conjecture suivante :

(i') Soit π'_C le plus grand quotient de π_C dont l'ordre (comme groupe profini) soit premier à p. Alors π'_C est isomorphe au groupe correspondant pour une courbe sur $\mathbf{C}$ ayant mêmes invariants g et s.

2. THÉORÈMES DE GROTHENDIECK ET CONJECTURES D'ABHYANKAR

2.1. Les théorèmes de Grothendieck

L'un des premiers succès de la théorie des schémas de Grothendieck a été la démonstration, en 1958, de la conjecture (i') du n° 1.4 (*cf.* [7], p. 182-27 ainsi que [8], p. 392) ; sa méthode consiste à se ramener à la caractéristique 0 conformément à ce qu'avait prédit Weil.

De façon plus précise, choisissons un anneau de valuation discrète complet A, de corps résiduel k, et dont le corps des fractions K est de caractéristique 0. On procède en trois étapes :

(2.1.1) *On peut "relever"* la k-courbe projective $\overline{C}$ en un schéma $\overline{C}_A$ projectif et lisse sur A (ce qui donne une courbe $\overline{C}_K$ sur K ayant bonne réduction).

Ce résultat est presque évident lorsque g est < 5, mais il ne l'est pas pour des valeurs plus grandes de g. Grothendieck le démontre en relevant d'abord $\overline{C}$ en un *schéma formel*, puis en montrant que ce schéma est algébrique puisqu'il possède un fibré de rang 1 qui est ample (à savoir le fibré défini par un point). La démonstration utilise les théorèmes de comparaison "formel $\Longleftrightarrow$ algébrique", *i.e.* "GAGA formel".

(2.1.2) Une fois choisi $\overline{C}_A$, soit S_K un relèvement de S dans $\overline{C}_A(A) = \overline{C}_K(K)$. Si $C' \to C$ est un revêtement galoisien de C, de groupe G, qui est *modéré* en tous les points de S, on peut relever C' de façon unique en un revêtement de $C_K - S_K$: cela se démontre en utilisant encore "GAGA formel".

(2.1.3) Inversement, soit $C'_K \to \overline{C}_K - S_K$ un revêtement galoisien absolument irréductible de groupe de Galois G, et supposons que l'ordre de G soit premier à p. On montre alors que, après remplacement éventuel de A par un anneau plus ramifié, le revêtement C'_K "se réduit bien", *i.e.* se prolonge

en un revêtement de $\overline{C}_A - S_K$, et définit donc un revêtement de C. (La démonstration utilise le *lemme d'Abhyankar* ainsi que le *théorème de pureté.*)

En combinant ces résultats, on voit que :

(*) Si p ne divise pas $|G|$, les G-revêtements *sont les mêmes* en caractéristique p et en caractéristique 0, *cf.* (2.1.2) et (2.1.3).

C'est là un résultat très satisfaisant — à cela près que la condition "p ne divise pas $|G|$" est très restrictive : si $p = 2$, elle n'est satisfaite que par des groupes résolubles, d'après Feit-Thompson.

(**) Si p divise $|G|$, mais si l'on se borne aux revêtements *modérément ramifiés* en tous les points de S, il y a au plus autant (et en général strictement moins) de tels revêtements en caractéristique p qu'en caractéristique 0.

(Pour des formulations plus précises de (*) et (**) en termes de *spécialisation du groupe fondamental*, voir [8].)

2.2. Le cas où C est une courbe complète

C'est le cas $S = \emptyset$. Tous les revêtements de C sont modérés. D'après (**) ci-dessus, le groupe π_C est un quotient du groupe fondamental correspondant en caractéristique 0. *Quel est ce quotient* ? On ne sait le déterminer explicitement que si $g = 0$ ou 1, auquel cas il est commutatif :

pour $g = 0$, on a $\pi_C = \{1\}$;

pour $g = 1$, π_C est isomorphe à $\prod_{\ell \neq p}(\mathbf{Z}_\ell \times \mathbf{Z}_\ell)$ ou à $\mathbf{Z}_p \times \prod_{\ell \neq p}(\mathbf{Z}_\ell \times \mathbf{Z}_\ell)$, suivant que la courbe C est supersingulière ou ordinaire.

Pour $g \geq 2$, on n'a pas de théorème de structure, même conjecturalement. On a seulement des renseignements cohomologiques. On les obtient en remarquant que la cohomologie de π_C est isomorphe à la cohomologie étale de C, tout comme si le "revêtement universel" de C était contractile (cela se démontre en utilisant la suite spectrale de Cartan-Leray pour les revêtements, *cf.* [14], p. 105, th. 2.20). D'où, d'après [4], exposés IX, X :

$\mathrm{cd}_p(\pi_C) = 1$ et $\dim H^1(\pi_C, \mathbf{Z}/p\mathbf{Z}) \leq g$;

$\mathrm{cd}_\ell(\pi_C) = 2$, $\dim H^1(\pi_C, \mathbf{Z}/\ell\mathbf{Z}) = 2g$ et $\dim H^2(\pi_C, \mathbf{Z}/\ell\mathbf{Z}) = 1$ si $\ell \neq p$.

(Rappelons que $\mathrm{cd}_p(\pi)$ désigne la *p-dimension cohomologique* du groupe profini π, *cf.* [18], p. I-17. L'assertion $\mathrm{cd}_p(\pi_C) \leq 1$ équivaut à dire que les

p-groupes de Sylow de π_C sont des *pro-p-groupes libres* ; ces groupes sont non triviaux d'après Raynaud [16], cor. 4.3.2).

2.3. Le cas où C est une courbe affine : conjecture d'Abhyankar

C'est le cas $S \neq \emptyset$; sur $\mathbf{C}$, le groupe fondamental correspondant est libre de rang $2g + s - 1$, *cf.* n° 1.2.

Soit G un groupe fini. Soit $p(G) = O^{p'}(G)$ le sous-groupe de G engendré par ses p-groupes de Sylow. Le groupe $G/p(G)$ est le plus grand quotient de G d'ordre premier à p. Si G est quotient de π_C, il en est de même de $G/p(G)$ et, d'après Grothendieck (*cf.* (2.1.2)), $G/p(G)$ est quotient du groupe analogue à π_C en caractéristique 0, autrement dit peut être engendré par $2g + s - 1$ éléments. Dans [1], Abhyankar conjecture que cette condition est suffisante :

Conjecture 2.3.1.— *Un groupe fini G est quotient de π_C si et seulement si le quotient $G/p(G)$ peut être engendré par $2g + s - 1$ éléments.*

Si cette conjecture était vraie, elle donnerait une réponse satisfaisante à la question (a) du n° 1.1 (mais pas à la question (b)).

Remarque.— Ici encore, la cohomologie de π_C s'identifie à la cohomologie étale de C, et l'on en déduit :

$$\mathrm{cd}_\ell(\pi_C) = 1 \text{ pour tout } \ell\,, \text{ et } \dim H^1(\pi_C, \mathbf{Z}/\ell\mathbf{Z}) = \begin{cases} \mathrm{Card}(k) & \text{si } \ell = p \\ 2g + s - 1 & \text{sinon.} \end{cases}$$

En particulier (*cf.* [18], p. I-74), π_C possède la *propriété de relèvement* : si $f : \widetilde{G} \to G$ est un homomorphisme surjectif de groupes finis, et si φ est un homomorphisme de π_C dans G, il existe $\widetilde{\varphi} : \pi_C \to \widetilde{G}$ tel que $f \circ \widetilde{\varphi} = \varphi$. (Mais si φ est surjectif, on ne peut pas toujours choisir $\widetilde{\varphi}$ surjectif, même si $\widetilde{G}$ satisfait à la condition de (2.3.1).)

3. LA CONJECTURE D'ABHYANKAR POUR LA DROITE AFFINE

3.1. Conjecture et résultats

On se restreint maintenant au cas où C est la droite affine $D = \operatorname{Spec} k[X]$, le corps k étant algébriquement clos de caractéristique $p > 0$.

On a alors $g = 0$ et $s = 1$, d'où $2g + s - 1 = 0$, et la conjecture 2.3.1 prend la forme suivante :

Conjecture 3.1.1.— *Un groupe fini G est quotient de π_D si et seulement si l'on a $G = p(G)$, i.e. si et seulement si G est engendré par ses p-groupes de Sylow.*

Un groupe G tel que $G = p(G)$ sera appelé un *quasi-p-groupe.*

Exemple.— Un groupe simple dont l'ordre est divisible par p est un quasi-p-groupe. La conjecture (3.1.1) implique donc que tout groupe simple non abélien est quotient de π_D si $p = 2$.

On verra ci-après que (3.1.1) a été démontrée dans de nombreux cas particuliers :

G est le groupe des points rationnels d'un groupe algébrique semi-simple simplement connexe sur un corps fini de caractéristique p (Nori [10]) ;

G est le groupe alterné A_n, $n \geq p > 2$, ou le groupe symétrique S_n, $n \geq p = 2$ (Abhyankar [2]) ;

G est résoluble ([19]) ;

G est engendré par des sous-groupes vérifiant certaines conditions restrictives (Harbater [9], Raynaud [17]).

Remarque.— La droite D joue un rôle en quelque sorte universel pour les revêtements de variétés affines. De façon plus précise, soit V une variété affine irréductible sur k, de dimension > 0, et soit G un groupe fini qui soit quotient de π_D. Il existe alors un revêtement galoisien connexe $V' \to V$ de groupe de Galois G, *cf.* [19], n° 2.

3.2. Les exemples de Nori

Soit q une puissance de p, et soit Σ un groupe algébrique semi-simple simplement connexe sur $\mathbf{F}_q$. Soit $G = \Sigma(\mathbf{F}_q)$ le groupe des $\mathbf{F}_q$-points de Σ.

Le groupe G est un quasi-p-groupe.

THÉORÈME 3.2.1 (Nori).— *Le groupe G est quotient de π_D.*

COROLLAIRE.— *La conjecture* 3.1.1 *est vraie pour les groupes* $\mathbf{SL}_n(\mathbf{F}_q)$, $\mathbf{Sp}_{2n}(\mathbf{F}_q), \cdots, E_8(\mathbf{F}_q)$.

Démonstration (d'après G. Laumon).— Soient B^+ et B^- des sous-groupes de Borel opposés de Σ, et soient U^+ et U^- leurs radicaux unipotents. L'application produit $U^+ \times U^- \to \Sigma$ est un isomorphisme de $U^+ \times U^-$ sur une sous-variété fermée V de Σ (le fait que V soit fermée n'interviendra d'ailleurs pas). Soit $f : \Sigma \to \Sigma$ *l'isogénie de Lang*, définie par :

$$f(x) = x^{-1} \,.\, F(x),$$

où F est l'endomorphisme de Frobenius de Σ relativement à $\mathbf{F}_q$. Cette isogénie définit un *revêtement galoisien connexe* de Σ, de groupe de Galois G. Soit $W = f^{-1}(V)$. *La variété W est connexe.* En effet, soit W^0 la composante connexe de W contenant 1, et soit G^0 le sous-groupe de G qui stabilise W^0. Comme W^0 contient U^+, le groupe G^0 contient $U^+(\mathbf{F}_q)$; de même, il contient $U^-(\mathbf{F}_q)$. Mais on sait (*cf.* [20], lemme 64) que G est engendré par $U^+(\mathbf{F}_q)$ et $U^-(\mathbf{F}_q)$. On a donc $G = G^0$, ce qui montre que W est connexe. On a donc obtenu un revêtement galoisien connexe $W \to V$ de groupe de Galois G. Mais V est isomorphe à $U^+ \times U^-$, donc est un espace affine de dimension > 0 (sauf si $\Sigma = \{1\}$, auquel cas il n'y a rien à démontrer). En restreignant le revêtement $W \to V$ à une droite Δ de V, on obtient un revêtement de Δ de groupe de Galois G. D'après une variante du théorème de Bertini, ce revêtement est *connexe* si Δ est assez générale. D'où le résultat cherché, puisque Δ est isomorphe à D.

Remarque.— La démonstration s'applique aussi aux groupes "tordus" du type Suzuki et Ree en caractéristique 2 et 3.

3.3. Les exemples d'Abhyankar

THÉORÈME 3.3.1 (Abhyankar [2]).— *Les groupes ci-dessous sont quotients de* π_D :

le groupe alterné A_n *si* $p \neq 2$ *et* $n \geq p$;

le groupe symétrique S_n *si* $p = 2$.

La méthode consiste à écrire explicitement des équations de degré n qui définissent des revêtements étales de degré n de D, et à montrer que les clôtures galoisiennes de ces revêtements ont pour groupe de Galois un sous-groupe de S_n qui est A_n ou S_n suivant les cas ; cela se fait en prouvant que le groupe en question est suffisamment transitif (dans certains cas, Abhyankar est amené à utiliser le "théorème de classification" des groupes finis simples).

L'une des équations qu'il utilise est la suivante :

$$Y^n - X \cdot Y^t + 1 = 0, \tag{I}$$

avec $n = p + t$, $t \geq 1$ et $t \not\equiv 0 \pmod{p}$.

Il montre (*cf.* [2], [3]) que le groupe de Galois de cette équation est :

$\mathbf{PSL}_2(\mathbf{F}_p)$	si	$t = 1$;
$\mathbf{SL}_2(\mathbf{F}_8)$	si	$t = 2$, $p = 7$;
A_n	si	$t = 2$, $p \neq 2, 7$;
A_n	si	$t > 2$, $p \neq 2$;
S_n	si	$p = 2$.

Donnons la démonstration dans le cas le plus simple, qui est celui où $t \geq 3$. Soit G le groupe de Galois de (I). C'est un sous-groupe de S_n jouissant des propriétés suivantes :

il est transitif ;

il contient un cycle c d'ordre p (à cause de l'inertie en $X = \infty$, $Y = \infty$) ;

il contient un élément d'ordre premier à p qui permute circulairement les t points fixes du cycle c (inertie en $X = \infty$, $Y = 0$).

Comme $n = p + t$, et $(p, t) = 1$, on vérifie facilement que les propriétés ci-dessus entraînent que G est *primitif*. Comme G contient un cycle d'ordre

premier $\leq n-3$, on a $G = S_n$ ou A_n d'après un théorème de Jordan (*cf.* [23], p.39). Si $p = 2$, le fait que G contienne une transposition entraîne $G = S_n$. Si $p \neq 2$, le fait que soit un quasi-p-groupe entraîne $G \neq S_n$, donc $G = A_n$, d'où le résultat cherché.

Remarques.— 1) La méthode employée ne semble pas donner le cas de A_n, $n \geq 5$, lorsque $p = 2$. Toutefois Raynaud m'a fait observer que ce cas peut se traiter par "recollement" de groupes A_5 en utilisant le th. 1.1 de [17] (voir n° 3.5).

2) Certaines équations explicites, conduisant à des groupes de Galois intéressants, peuvent s'obtenir par réduction $(\mathrm{mod}\, p)$ à partir d'équations connues en caractéristique zéro. Par exemple :

(a) On sait depuis Fricke (*cf.* [6], [24]) qu'il existe un revêtement galoisien de la droite projective de groupe $G = \mathbf{SL}_2(\mathbf{F}_8)$, ramifié en trois points avec ramification d'ordre 2, 3, 7, et défini sur le corps $\mathbf{Q}(\cos(2\pi/7))$; la courbe correspondante est de genre 7. Si l'on représente G comme sous-groupe transitif de A_9, cela conduit à un revêtement de degré 9 de la droite projective dont l'équation a été écrite par Goursat (*cf.* [6]). En réduisant cette équation en caractéristique 7 (après des changements de variables convenables), on obtient l'équation $Y^9 - X \,.\, Y^2 + 1 = 0$ d'Abhyankar, et l'on retrouve ainsi le résultat principal de [3].

(b) En réduisant en caractéristique 11 une équation donnée par Matzat [13], on voit que l'équation

$$Y^{11} + 2Y^9 + 3Y^8 - X^8 = 0 \qquad (p = 11)$$

définit un revêtement étale de degré 11 de D dont le groupe de Galois est le groupe de Mathieu M_{11}.

(c) En caractéristique 23, l'équation :

$$Y(Y-1)^2\,(Y+1)^4\,(Y^2+17Y+4)^8 - X^8 = 0 \qquad (p = 23)$$

définit un revêtement étale de degré 23 de D. Il semble que le groupe de Galois de ce revêtement soit le groupe de Mathieu M_{23} ; il serait intéressant de le démontrer.

3.4. Extensions par des groupes résolubles

Soit $1 \to N \to \widetilde{G} \to G \to 1$ une suite exacte de groupes finis. Supposons que $\widetilde{G}$ soit un *quasi-p-groupe*, et que N soit *résoluble*. Alors, *si la conjecture* 3.1.1 *est vraie pour* G, *elle l'est pour* $\widetilde{G}$. Autrement dit :

THÉORÈME 3.4.1 (*cf.* [19]).— *Sous les hypothèses ci-dessus, si* G *est quotient de* π_D, *il en est de même de* $\widetilde{G}$.

COROLLAIRE 1.— *La conjecture* 3.1.1 *est vraie pour les groupes résolubles : tout quasi-p-groupe résoluble est quotient de* π_D.

C'est le cas particulier $G = \{1\}$.

COROLLAIRE 2.— *Si* G *est quotient de* π_D, *il en est de même de toute extension de* G *par un p-groupe.*

En effet, une telle extension est un quasi-p-groupe, ce qui permet d'appliquer le th. 3.4.1.

Démonstration de (3.4.1).— On se ramène par dévissage au cas où N est un groupe abélien élémentaire de type $(\ell, \cdots, \ell)$, avec ℓ premier, l'action de G sur N étant irréductible.

Par hypothèse, il existe un morphisme surjectif $\varphi : \pi_D \to G$, et, d'après ce qui a été dit au n° 2.3, on peut relever φ en $\widetilde{\varphi} : \pi_D \to \widetilde{G}$. Lorsque $\widetilde{G}$ est une extension non scindée de G, $\widetilde{\varphi}$ est surjectif, et le théorème est démontré. Le cas où $\widetilde{G}$ est produit semi-direct de G par N est plus délicat. Si $\ell = p$, on montre que l'on peut choisir $\widetilde{\varphi}$ de telle sorte qu'il soit surjectif. Si $\ell \neq p$, ce n'est pas possible en général. Toutefois, dans ce cas, *on peut modifier* φ de façon à ce que cela devienne possible. De façon plus précise, choisissons un entier $m > 1$ premier à p. Le morphisme $D \to D$ défini par $X \mapsto X^m$ induit un endomorphisme $f_m : \pi_D \to \pi_D$ (on prend pour point-base le point 0). Cet endomorphisme est surjectif. Si on le compose avec φ, on obtient un homomorphisme $\varphi_m : \pi_D \to G$ qui est encore surjectif, mais qui est "plus ramifié" que φ (son invariant de Swan à l'infini est multiplié par m). On montre qu'il est possible de relever φ_m en un morphisme surjectif $\widetilde{\varphi}_m : \pi_D \to \widetilde{G}$ (la démonstration de ce fait repose sur une étude des modules

galoisiens fournis par l'homologie (mod ℓ) des revêtements, *cf.* [19], th. 2). D'où le théorème.

3.5. Les constructions de Harbater et Raynaud

Remarquons d'abord que la conjecture d'Abhyankar 3.1.1 résulterait (en raisonnant par récurrence sur $|G|$ et en se ramenant au cas où G est cyclique) de l'énoncé suivant :

(3.5.1?) *Si G est engendré par deux sous-groupes G_1 et G_2 qui sont quotients de π_D, alors G est quotient de π_D.*

Harbater [9] et Raynaud [17] démontrent (3.5.1?) sous diverses hypothèses restrictives. Par exemple :

THÉORÈME 3.5.2 ([9], th. 4 (i)).— *L'assertion* (3.5.1?) *est vraie si G_1 est un p-groupe contenant un p-groupe de Sylow de G_2.*

L'énoncé de Raynaud fait intervenir les groupes d'inertie à l'infini des revêtements considérés (groupes qui sont définis à conjugaison près) :

THÉORÈME 3.5.3 ([17], th. 1.1).— *Soit Q un p-sous-groupe de G. Supposons que, pour $i = 1, 2$, il existe un revêtement galoisien connexe $\widetilde{D}_i \to D_i = D$, de groupe G_i, ayant comme groupe d'inertie à l'infini un sous-groupe Q_i de Q. Il existe alors un revêtement galoisien connexe de D de groupe G ayant Q comme groupe d'inertie à l'infini.*

Les démonstrations de (3.5.2) et (3.5.3) utilisent respectivement "GAGA formel" et "GAGA rigide" — ce qui d'ailleurs revient à peu près à la même chose, *cf.* [15].

Voici un résumé (très incomplet) de la méthode esquissée par Raynaud dans [17] :

On utilise la géométrie rigide sur le corps local $K = k((T))$. Dans la droite projective $\mathbf{P}_1$ sur K, on choisit deux disques fermés Δ_1 et Δ_2, ne contenant pas ∞, et à distance > 0 l'un de l'autre (par exemple les disques $|z| \leq 1/p$ et $|z - 1| \leq 1/p$). On choisit des disques un peu plus grands Δ_i^+ les contenant, et satisfaisant aux mêmes conditions. On définit ensuite trois revêtements galoisiens (au sens rigide), de groupe G :

(a_1) Un revêtement de Δ_1^+ ;

(a_2) Un revêtement de Δ_2^+ ;

(a_3) Un revêtement de $\mathbf{P}_1 - \Delta_1 - \Delta_2 - \{\infty\}$, qui se prolonge en un revêtement ramifié à l'infini, de groupe d'inertie Q.

La construction des revêtements (a_1) et (a_2) se fait de la manière suivante : la "réduction mod T" du disque Δ_i peut être identifiée à la k-droite affine D_i. Le G_i-revêtement $\widetilde{D}_i \to D_i$ définit par relèvement à K un G_i-revêtement rigide de Δ_i, et l'on montre que ce revêtement se prolonge à un disque un peu plus grand. On obtient ainsi un G_i-revêtement, et par induction de G_i à G on obtient le revêtement (a_i) cherché. (Noter que ce revêtement n'est pas irréductible en général : ses composantes irréductibles sont en nombre égal à l'indice de G_i dans G.)

Quant à (a_3), on l'obtient par induction de Q à G à partir d'un Q-revêtement (algébrique) de $\mathbf{P}_1 - \{\infty\}$. On le choisit (*cf.* [17]) de telle sorte que la propriété suivante soit satisfaite :

(b) Pour $i = 1, 2$, la restriction du revêtement (a_3) à la couronne ouverte $\Delta_i^+ - \Delta_i$ est isomorphe à la restriction de (a_i) à cette couronne (du moins si les Δ_i^+ sont assez petits).

Cette propriété permet de *recoller* (au sens de la géométrie rigide) les trois revêtements (a_i) et l'on obtient ainsi un revêtement galoisien de $\mathbf{P}_1$, de groupe G, qui est ramifié seulement à l'infini, avec Q pour groupe d'inertie. Par "GAGA rigide" (*cf.* [11], [12]), ce revêtement est algébrique. De plus, sa construction montre qu'il est géométriquement irréductible (c'est là que sert l'hypothèse que G est engendré par G_1 et G_2). *A priori*, ce revêtement est défini sur K ; par spécialisation (*cf.* n° 1.1), on en déduit un revêtement sur k ayant les propriétés voulues.

COROLLAIRE 3.5.4.— *Si G est groupe de Galois d'un revêtement connexe de D, ce revêtement peut être choisi tel que les groupes d'inertie à l'infini soient les p-groupes de Sylow de G.*

Soit I un groupe d'inertie à l'infini. En utilisant le lemme d'Abhyankar (*i.e.* un changement de base $X \mapsto X^n$, avec n convenable), on peut supposer que I est un p-groupe. Soit P un p-groupe de Sylow de G contenant I. On applique alors le th. 3.5.3, avec $G_1 = G$, $G_2 = P$, $Q_1 = I$, $Q_2 = P$, $Q = P$ (c'est licite car on sait que tout p-groupe fini est quotient de π_D, *cf.* par

exemple [19]).

Compte tenu de ce résultat, on voit que (3.5.2) est un cas particulier de (3.5.3).

Compléments

Du th. 3.5.3, Raynaud déduit le résultat suivant :

Soit G un groupe fini qui soit un quasi-p-groupe, et soit P un p-groupe de Sylow de G. Il existe alors un sous-groupe H de G, contenant P, quotient de π_D, et *maximum* pour cette propriété. En particulier, H est stable par tout automorphisme de G préservant P. De plus, tout sous-groupe de G qui est quotient de π_D est conjugué d'un sous-groupe de H. Enfin, Raynaud démontre ([17], th. 1.5) que, si $P \neq G$, on a $H \neq P$ (ce qui permet souvent de prouver que $H = G$, autrement dit que la conjecture d'Abhyankar est vraie pour G).

Application

Indiquons à titre d'exemple comment on peut déduire du th. 3.5.3 le fait que *le groupe alterné* A_n, $n \geq 5$, *est quotient de* π_D *si* $p = 2$.

Soit P le 2-groupe de Sylow de A_4. On va montrer par récurrence sur $n \geq 5$ qu'il existe un revêtement galoisien connexe de D, de groupe A_n, pour lequel les groupes d'inertie à l'infini sont les conjugués de P. C'est vrai pour $n = 5$ car $A_5 = \mathbf{SL}_2(\mathbf{F}_4)$ et l'on applique 3.2.1 et 3.5.4 (on peut aussi, plus simplement, utiliser l'équation $Y^5 + X^3Y + 1 = 0$). Si $n \geq 6$, on applique 3.5.3 au groupe $G = A_n$, avec :

$G_1 = A_{n-1}$, fixateur de n dans A_n ;

$Q_1 = P$;

$G_2 =$ fixateur de $n-1$ dans A_n (on a $G_2 \simeq A_{n-1}$);

$Q_2 = P$;

$Q = P$.

Vu l'hypothèse de récurrence, toutes les conditions nécessaires sont satisfaites.

BIBLIOGRAPHIE

[1] S. ABHYANKAR - *Coverings of algebraic curves*, Amer. J. Math. **79** (1957), 825-856.

[2] S. ABHYANKAR - *Galois theory on the line in nonzero characteristic*, Bull. A.M.S. **27** (1992), 68-133.

[3] S. ABHYANKAR - *Square-root parametrization of plane curves*, Purdue Univ., 1991.

[4] M. ARTIN, A. GROTHENDIECK et J.-L. VERDIER - *Théorie des Topos et Cohomologie Étale des Schémas* (SGA 4), vol. 3, Lect. Notes in Math. **305**, Springer-Verlag (1973).

[5] R. et A. DOUADY - *Algèbre et théories galoisiennes* ; 2) *théories galoisiennes*, CEDIC, F. Nathan, Paris (1979).

[6] R. FRICKE - *Ueber eine einfache Gruppe von 504 Operationen*, Math. Ann. **52** (1899), 321-339.

[7] A. GROTHENDIECK - *Géométrie formelle et géométrie algébrique*, Sém. Bourbaki, exposé n° 182, volume 1958/1959, Benjamin (1966).

[8] A. GROTHENDIECK - *Revêtement étales et groupe fondamental* (SGA 1), Lect. Notes in Math. **224**, Springer-Verlag (1971).

[9] D. HARBATER - *Formal patching and adding branch points*, prépublication (1991).

[10] T. KAMBAYASHI - *Nori's construction of Galois coverings in positive characteristics*, Algebraic and Topological Theories, Tokyo (1985), 640-647.

[11] R. KIEHL - *Der Endlichkeitssatz für eigentliche Abbildungen in der nichtarchimedischen Funktionentheorie*, Inv. Math. **2** (1967), 191-214.

[12] U. KÖPF - *Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen*, Schriftenreihe Univ. Münster, 2 Serie, Heft 7 (1974).

[13] B.H. MATZAT - *Konstruktion von Zahlkörpern mit der Galoisgruppe* M_{11} *über* $\mathbf{Q}(\sqrt{-11})$, Man. Math. **27** (1979), 103-111.

[14] J. MILNE - *Etale Cohomology*, Princeton Math. Series 33, Princeton (1980).

[15] M. RAYNAUD - *Géométrie analytique rigide, d'après Tate, Kiehl, ...*, Bull. Soc. math. France, Mémoire 39-40 (Table ronde anal. non-archim. 1972), 319-327.

[16] M. RAYNAUD - *Sections des fibrés vectoriels sur une courbe*, Bull. Soc. math. France **110** (1982), 103-125.

[17] M. RAYNAUD - *Autour d'une conjecture d'Abhyankar*, manuscrit non publié (1991).

[18] J.-P. SERRE - *Cohomologie galoisienne*, 4ème édit., Lect. Notes in Math. **5**, Springer-Verlag (1973).

[19] J.-P. SERRE - *Construction de revêtements étales de la droite affine en caractéristique p*, C.R. Acad. Sci. Paris **311** (1990), série I, 341-346.

[20] R. STEINBERG - *Lectures on Chevalley groups*, Notes prepared by John Faulkner and Robert Wilson, Yale University (1967).

[21] A. WEIL - *Généralisation des fonctions abéliennes*, J. Liouville **17** (1938), 47-87 (= *Oe.* [1938a]).

[22] A. WEIL - *L'avenir des mathématiques*, Les Grands Courants de la Pensée Mathématique, éd. F. Le Lionnais, Cahiers du Sud, 1947, 307-320 (= *Oe.* [1947a]).

[23] H. WIELANDT - *Finite Permutation Groups*, Acad. Press, New York (1964).

[24] K. WOHLFAHRT - *Macbeath's curve and the modular group*, Glasgow Math. J. **27** (1985), 239-247 ; *Corrigendum, ibid.* **28** (1986), 241.

(Note ajoutée en septembre 1992) La conjecture d'Abhyankar pour la droite affine (3.3.1) a été démontrée par M. Raynaud. Voir M. Raynaud, *Revêtements de la droite affine en caractéristique $p > 0$ et conjecture d'Abhyankar*, à paraître à Inv. Math.

Jean-Pierre SERRE

Collège de France
3, rue d'Ulm
F-75005 PARIS