Séminaires & Congrès
5, 2001, p. 1–26

THÉORIE DE GALOIS ET GÉOMÉTRIE : UNE INTRODUCTION

par

Pierre Dèbes

Résumé. — La question centrale de la théorie inverse de Galois est le problème inverse de Galois : tout groupe fini est-il le groupe de Galois d'une extension du corps des rationnels ? Des progrès importants ont été réalisés ces trente dernières années grâce à un point de vue géométrique : revêtements, groupes fondamentaux, espaces de modules, déformations, etc. Nous proposons ici un survol du domaine.

***Abstract* (Galois Theory and Geometry).** — The central question of inverse Galois theory is the inverse Galois problem: is each finite group the Galois group of an extension of the field of the rationals? There has been some significant progress in the last thirty years thanks to a geometric approach: covers, fundamental groups, moduli spaces, deformations, etc. We offer here a survey of this area.

La théorie de Galois, sujet classique, renvoie à un domaine de recherches aux contours indistincts. Le mot « géométrie » dans le titre précise un peu le champ de cet exposé : nous nous intéresserons à la théorie de Galois des *corps de fonctions* ou si on préfère, des *revêtements*; la présence d'indéterminées sera le signe de reconnaissance. Cela laisse de côté tout un pan de la théorie de Galois, où les questions et les méthodes relèvent plus de la théorie des nombres. Dans ce cadre géométrique, nous nous limiterons de plus à la théorie de Galois dite classique, par opposition à la théorie de Galois différentielle.

Même ainsi réduit, le domaine reste vaste et le choix d'un point de départ assez arbitraire. Nous avons choisi de motiver notre présentation par des questions de théorie *inverse* de Galois, qui ont été à l'origine de progrès importants ces 30 dernières années. Pour préciser, disons que le type général des problèmes qui nous guideront est de construire des revêtements algébriques, de la droite projective $\mathbb{P}^1$ principalement, vérifiant certaines propriétés galoisiennes et avec contrôle du corps de définition. Nous

***Classification mathématique par sujets* (2000).** — 12F12, 14H30, 14G32, 12E30, 14D15, 14D10, 14H05, 14H10, 14Gxx, 14Kxx, 11Gxx.

Mots clefs. — Théorie de Galois, problème inverse, corps de fonctions, revêtements, groupes fondamentaux, familles de revêtements, espaces de modules, espaces de Hurwitz, programme de Noether, déformation, recollement, réduction, questions de rationalité, corps de définition.

essaierons cependant de dépasser le cadre de la théorie inverse pour donner un aperçu global du domaine.

Un résultat fondateur est le théorème d'existence de Riemann. Grâce à lui, on sait résoudre la plupart des problèmes envisagés si le corps de base est $\mathbb{C}$, ou plus généralement, un corps algébriquement clos de caractéristique 0. Le cas d'un corps de base plus petit, le corps $\mathbb{Q}$ par exemple, devient un problème de *descente*. En quelque sorte, en caractéristique 0, tout commence avec le théorème d'existence de Riemann. Cela fait du cas de caractéristique $p > 0$, pour lequel on ne connaît pas d'analogue, un problème bien distinct. Nous lui avons réservé une section spécifique (section 4). Avant cette section, l'exposé est composé comme suit. Dans la section 1, nous présentons les problèmes et les conjectures du domaine. La section 2 est consacrée aux principaux résultats. La section 3 rentre un peu plus dans le cœur du sujet en expliquant les diverses approches et leurs ramifications.

Nous remercions le rapporteur dont les commentaires nous ont permis de beaucoup améliorer le texte.

1. Problèmes et conjectures

1.1. Problèmes inverses de Galois. — Une motivation importante pour l'étude arithmétique des revêtements de $\mathbb{P}^1$ réside dans le problème inverse de Galois. Classiquement la théorie de Galois associe à tout polynôme $P(Y) \in \mathbb{Q}[Y]$ irréductible, ou, si on préfère, à toute extension galoisienne $E/\mathbb{Q}$, un groupe fini, le groupe de Galois du polynôme, ou de l'extension. Le problème inverse, qui concerne la réciproque, est une question fondamentale encore ouverte de la théorie de Galois.

Problème inverse de Galois (GAL/INV). — *Étant donné*

– un groupe fini G

il existe une extension galoisienne $E/\mathbb{Q}$ de corps telle que $\mathrm{Gal}(E/\mathbb{Q}) = G$.

L'approche privilégiée aujourd'hui utilise une stratégie due à Hilbert. Étant donné un groupe fini G, elle consiste à introduire une indéterminée T et *réaliser* d'abord G comme groupe de Galois d'une extension $E_T/\mathbb{Q}(T)$ (ou si on préfère d'un polynôme irréductible $P(T,Y) \in \mathbb{Q}(T)[Y]$), puis à *spécialiser* T en un nombre $t_o \in \mathbb{Q}$. D'après le *théorème d'irréductibilité* de Hilbert ([FrJa86] [La83]), le groupe de Galois de l'extension spécialisée $E_{t_o}/\mathbb{Q}$, (ou du polynôme spécialisé $P(t_o, x)$) reste égal à G pour une infinité de $t_o \in \mathbb{Q}$.

On demande de plus à l'extension $E_T/\mathbb{Q}(T)$ d'être *régulière* sur $\mathbb{Q}$, *i.e.*, de vérifier $E_T \cap \overline{\mathbb{Q}} = \mathbb{Q}$. Alors elle correspond, par le foncteur « corps des fonctions », à un revêtement(1) algébrique galoisien $f : X \to \mathbb{P}^1$ de groupe d'automorphismes G, défini sur $\mathbb{Q}$ ainsi que ses automorphismes(2) : la courbe X est simplement un modèle projectif lisse de la courbe $P(t,y) = 0$ et f un prolongement à X de la projection $(t,y) \mapsto t$ sur cette courbe. Le problème est ainsi replacé dans un cadre géométrique. C'est dans ce cadre que nous nous situerons ici. Le problème inverse *géométrique* correspond à la conjecture suivante ; d'après Hilbert, pour $K = \mathbb{Q}$, elle entraîne l'énoncé (GAL/INV).

Forme régulière du problème inverse de Galois (GAL/INV/RÉG)

Étant donnés

– un corps K,

– un groupe fini G,

il existe

– une extension galoisienne régulière $E_T/K(T)$ telle que $\mathrm{Gal}(E_T/K(T)) = G$*, ou, en d'autres termes,*

– un G-revêtement galoisien $f : X \to \mathbb{P}^1$ défini sur K tel que $\mathrm{Aut}(X/\mathbb{P}^1) = G$

Le corps de base K (qui généralise $\mathbb{Q}$) est *a priori* arbitraire ; on ne connaît pas de corps K où l'énoncé (GAL/INV/RÉG) est faux, contrairement à l'énoncé (GAL/INV) qui le devient si $\mathbb{Q}$ est remplacé par exemple par $\mathbb{C}$, ou $\mathbb{Q}_p$, etc. La propriété de régularité de $E_T/K(T)$ entraîne que le groupe de Galois ne change pas par extension des scalaires, *i.e.*, $\mathrm{Gal}(E_T/K(T)) = \mathrm{Gal}(kE_T/k(T))$ pour tout corps $k \supset K$. On peut donc se limiter aux corps premiers dans l'énoncé ci-dessus.

1.2. Forme régulière forte. — Il existe une forme forte de (GAL/INV/RÉG) qui s'exprime en termes de *problèmes de plongement*. Essentiellement un problème de plongement (fini) pour un corps k consiste en la donnée d'une suite exacte de groupes finis $1 \to N \to G \to H \to 1$ et d'une extension galoisienne E_H/k telle que $\mathrm{Gal}(E_H/k) = H$; le problème est de plonger la H-extension E_H/k dans une G-extension, *i.e.*, de construire une extension E_G/E_H, galoisienne sur k, telle que $\mathrm{Gal}(E_G/k) = G$ et $\mathrm{Gal}(E_G/E_H) = N$.

D'après un théorème d'Iwasawa [FrJa86 ; Ch. 24], si pour un corps k (dénombrable), tout problème de plongement a une solution, alors le groupe de Galois absolu $\mathrm{G}_k = \mathrm{Gal}(k_{\mathrm{s}}/k)$ est pro-libre, *i.e.*, libre dans la catégorie des groupes profinis. Ce n'est

(1)par « revêtement », nous entendons revêtement éventuellement ramifié ; nous préciserons « non ramifié » dans le cas opposé. De plus, sauf mention du contraire, les revêtements considérés sont connexes.

(2)Nous suivrons l'usage et parlerons de « G-revêtement de groupe G » (ou de « G-revêtement ») pour indiquer que les automorphismes font partie de la donnée. Par opposition, les revêtements non nécessairement galoisiens et considérés sans leurs automorphismes sont appelés « revêtements purs ».

pas le cas par exemple pour $k = \mathbb{Q}$ puisque, au contraire de tout groupe pro-libre, le groupe $\mathrm{G}_{\mathbb{Q}}$ a des éléments de torsion (ceux induits par la conjugaison complexe). On conjecture cependant que, sur $\mathbb{Q}$ (ou plus généralement sur tout corps k *hilbertien*(3)), il existe une solution à tout problème de plongement *scindé*, *i.e.*, tel que l'épimorphisme $G \to H$ possède une section. Comme plus haut, on préfère la conjecture suivante qui ne dépend pas du corps de base.

Galois inverse/forme régulière forte (Gal/Inv/Rég/+). — *Étant donnés*
– *un corps K,*
– *un problème de plongement scindé pour le corps $K(T)$,*
il existe une solution régulière.

« Solution régulière » signifie ici que la solution $E_G/K(T)$ vérifie $E_G \cap \overline{K} = E_H \cap \overline{K}$ (*i.e.*, les constantes dans l'extension solution E_G sont celles qui figuraient déjà dans l'extension donnée E_H). La conjecture (Gal/Inv/Rég) correspond au cas particulier de (Gal/Inv/Rég/+) où le groupe H est trivial. Une autre conséquence notable est la

Conjecture de Shafarevich (Sha). — *Le groupe de Galois absolu* $\mathrm{G}_{\mathbb{Q}^{\mathrm{ab}}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}^{\mathrm{ab}})$ *de* $\mathbb{Q}^{\mathrm{ab}}$ *est pro-libre.*

En effet, en appliquant la conjecture (Gal/Inv/Rég/+) à $K = \mathbb{Q}^{\mathrm{ab}}$, on obtient, par spécialisation de T (le corps $\mathbb{Q}^{\mathrm{ab}}$ est hilbertien d'après un résultat de Kuyk ([Ku70], [FrJa86 ; § 15])), que tout problème de plongement scindé pour $\mathbb{Q}^{\mathrm{ab}}$ a une solution. Mais le fait que $\mathrm{cd}(\mathbb{Q}^{\mathrm{ab}}) \leqslant 1$(4) entraîne que la même conclusion est vraie, sans le mot « scindé » [Se73 ; ch.I § 5.9]. Le théorème d'Iwasawa, mentionné plus haut, conclut l'argument. Pour plus de détails sur ces conjectures et leurs relations, nous renvoyons à l'article [DeDes97] où l'énoncé (Gal/Inv/Rég/+) est présenté comme la conjecture unifiante du domaine.

1.3. Problème de Beckmann-Black. — On peut, comme S. Beckmann et E. Black, s'interroger sur les arguments de spécialisation utilisés précédemment et plus particulièrement sur la stratégie de Hilbert : pour réaliser un groupe G sur $\mathbb{Q}$, n'est-ce pas se limiter que se restreindre aux extensions de $\mathbb{Q}$ qui s'obtiennent par spécialisation d'une extension $E_T/\mathbb{Q}(T)$? La conjecture suivante, formulée par E. Black, répond par la négative. Ici encore, le corps de base est arbitraire.

(3)c'est-à-dire, un corps où la *propriété de spécialisation* du théorème d'irréductibilité de Hilbert est vraie.
(4)ce qui résulte de la trivialité du groupe de Brauer de $\mathbb{Q}^{\mathrm{ab}}$ et de ses extensions finies [Se73 ; ch.II § 3.1].

Problème de Beckmann-Black (BB). — *Étant donnés*

– *un corps* K,

– *un groupe fini* G,

– *une extension galoisienne* E/K *de groupe* G,

il existe une extension galoisienne régulière $E_T/K(T)$ *de groupe* G *(i.e., un* G*-revêtement* $f : X \to \mathbb{P}^1$ *défini sur* K*) telle que*

| – *l'extension résiduelle* E_{t_o}/K, *ou, en d'autres termes,*
| – *la fibre (spécialisation)* X_{t_o}/K

en un point $t_o \in \mathbb{P}^1(K)$ *est la* G*-extension* E/K.

L'énoncé (BB) précise l'énoncé (GAL/INV/RÉG) : non seulement tout groupe fini G est *réalisable* sur $K(T)$, mais aussi toute G-extension de K (*cf.* [De99c]).

Par « G-extension de groupe G » (ou « G-extension »), nous entendons *a priori* « extension galoisienne de *corps*, de groupe G ». Le problème (BB) est parfois énoncé plus généralement avec E une K-*algèbre* galoisienne ; cela permet par exemple d'inclure le cas où E est l'extension totalement décomposée (dite triviale), *i.e.*, le produit de d copies de K. Dans la suite, nous préciserons « G-extension d'*algèbres* » quand E n'est pas forcément un corps.

1.4. Le programme de Noether. — L'énoncé (BB) permet de faire le lien avec une autre partie importante de la théorie inverse de Galois, qui part d'une idée de Noether. Le *programme de Noether* est le suivant : étant donnés un corps K et un groupe fini G plongé dans S_d (par la représentation régulière de G par exemple), le groupe G agit sur le corps $E = \mathbb{Q}(T_1, \ldots, T_d)$. Le corps des invariants E^G est une extension régulière de $\mathbb{Q}$, et donc peut être vu comme le corps des fonctions $\mathbb{Q}(U_G)$ d'une variété irréductible U_G définie sur $\mathbb{Q}$, laquelle est alors unirationnelle par construction (*i.e.*, $\mathbb{Q}(U_G)$ est contenu dans une extension transcendante pure). L'extension $E/\mathbb{Q}(U_G)$ est galoisienne de groupe G. En termes géométriques, ces données correspondent à un revêtement, dit de Noether, $V_G \to U_G$, que l'on peut supposer non ramifié, quitte à restreindre U_G à un ouvert. Plutôt qu'un plongement $G \subset S_d$, on peut aussi utiliser un plongement linéaire $G \subset \mathrm{GL}_d$; dans ce cas, on prend $V_G = \mathrm{GL}_d$ et $U_G = \mathrm{GL}_d/G$.

Si $\mathbb{Q}(U_G)$ est lui-même une extension transcendante pure $\mathbb{Q}(\theta_1, \ldots, \theta_d)$ (*i.e.*, U_G une variété $\mathbb{Q}$-rationnelle), le théorème d'irréductibilité de Hilbert s'applique : on peut spécialiser les indéterminées $\theta_1, \ldots, \theta_d$ dans $\mathbb{Q}$ et obtenir une extension galoisienne de $\mathbb{Q}$ de groupe G. C'est le cas pour $G = S_n$. Mais comme l'ont montré Swan [Sw69] et V. E. Voskresenskiĭ [Vos70], puis Lenstra [Le74] et Saltman [Sa82], le corps $\mathbb{Q}(U_G)$ n'est pas en général une extension transcendante pure (voir aussi [Vos98 ; ch.3]). D'après Saltman [Sa84], il existe même des p-groupes G (où p peut être un nombre premier arbitraire) pour lesquels ce n'est pas le cas sur le corps $\mathbb{C}$ (à la place de $\mathbb{Q}$). L'extension $E/\mathbb{Q}(U_G)$ satisfait cependant la propriété *verselle* de spécialisation (dans les deux situations $G \subset S_d$ et $G \subset \mathrm{GL}_d$) :

Toute G-extension d'algèbres d'un corps $k \supset \mathbb{Q}$ (ou plus généralement d'une algèbre semi-locale $k \supset \mathbb{Q}$) s'obtient par spécialisation de l'extension $E/\mathbb{Q}(U_G)$ en un point k-rationnel sur U_G (ou, si on préfère, est une fibre du revêtement $V_G \to U_G$ au-dessus d'un point k-rationnel de U_G).

Inversement, les points k-rationnels sur U_G fournissent des G-extensions E/k, où E est *a priori* une *k-algèbre* galoisienne. La conjecture suivante, due à Colliot-Thélène [Se92 ; Ch. 3], garantirait qu'il existe de telles extensions avec E un corps.

Conjecture (COLLIOT). — *Toute variété unirationnelle sur un corps de nombres K vérifie la propriété de spécialisation de Hilbert.*

En liaison avec le programme de Noether, D. Saltman a introduit la notion d'*extension générique* pour un groupe G sur un corps K (qui remplace $\mathbb{Q}$) : il s'agit d'une extension $E/K(B)$ vérifiant la propriété *verselle* de spécialisation mentionnée ci-dessus et où $K(B)$ est une extension transcendante pure de type fini sur K (ou si on préfère, où B est une variété K-rationnelle). Par exemple, si, dans le programme de Noether, le corps $\mathbb{Q}(U_G) = E^G$ est une extension transcendante pure, $E/\mathbb{Q}(U_G)$ est une extension générique pour G. E. Black a montré d'autre part que si G a une extension générique sur K alors l'énoncé (BB) est vrai pour le groupe G et le corps K [Bl99a].

Rappelons aussi la conjecture suivante formulée dans [De99c], également dans le contexte du programme de Noether. Elle est équivalente à la conjecture (GAL/INV/RÉG) ; et elle est vraie dans le cas où la variété B ci-dessous est rationnelle.

Conjecture des Réalisations Linéairement Disjointes (RÉAL/LIN/DISJ)

Étant donnés
- *un corps K,*
- *une K-variété B de dimension > 0,*
- *un groupe G,*
- *une extension galoisienne $E/K(B)$ de groupe G régulière sur K,*

il existe une extension galoisienne $E'/K(B)$ de groupe G, régulière sur K et telle que les extensions $\overline{K}E'/\overline{K}(B)$ et $\overline{K}E/\overline{K}(B)$ soient linéairement disjointes.

1.5. Récapitulatif. — Le diagramme suivant résume les liens entre les conjectures.

$$\begin{tikzcd}
 & \text{GAL/INV/RÉG/+} \arrow[r, Rightarrow] \arrow[d, Rightarrow] & \text{SHA} \\
 & \text{GAL/INV/RÉG} \arrow[r, Rightarrow] \arrow[d, Leftrightarrow] & \text{GAL/INV} \\
\text{BB} \arrow[r, Rightarrow] & \text{RÉAL/LIN/DISJ} & \text{COLLIOT} \arrow[u, Rightarrow]
\end{tikzcd}$$

2. Principaux résultats

2.1. Les travaux de Riemann. — L'approche géométrique de la théorie inverse de Galois est motivée par le fait fondamental que les conjectures énoncées sont vraies si $K = \mathbb{C}$. Cela résulte du

Théorème d'existence de Riemann. — *Étant donnés*

- *un groupe fini G,*
- *un entier $r > 0$,*
- *r points distincts $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$,*

il existe une correspondance bijective entre

l'ensemble des extensions		*l'ensemble des revêtements*
de corps $E/\mathbb{C}(T)$		*topologiques connexes*
– ramifiées en $t_1, \ldots, t_r$	*et*	*– de $\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$*
– galoisiennes de groupe G		*– galoisiens de groupe G*
modulo les $\mathbb{C}(T)$-isomorphismes		*modulo l'équivalence des revêtements*

En particulier, un groupe fini G est groupe de Galois d'une extension $E/\mathbb{C}(T)$ si et seulement si G est quotient du groupe (libre) $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\})$, c'est-à-dire, si et seulement si G est de rang $\leqslant r - 1$.

Corollaire. — *La forme régulière du problème inverse de Galois ainsi que ses variantes (version forte et* (BB)*) sont vraies si $K = \mathbb{C}$.*

Pour la partie qui nous intéresse, la méthode est sommairement la suivante. Si $\mathrm{rg}(G) \leqslant r - 1$ (*i.e.*, si r est assez grand), le groupe G donné est quotient du groupe libre à $r-1$ générateurs et donc du groupe fondamental $\pi_1(\mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\})$, et donc peut être réalisé comme groupe d'automorphismes d'un revêtement topologique galoisien connexe $f : \mathcal{X} \to \mathbb{P}^1(\mathbb{C}) \setminus \{t_1, \ldots, t_r\}$. On peut ensuite prolonger f au-dessus des points manquants $t_1, \ldots, t_r$ et obtenir un revêtement analytique (ramifié) $\overline{f} : \overline{\mathcal{X}} \to \mathbb{P}^1(\mathbb{C})$ entre surfaces de Riemann compactes. La dernière étape consiste à montrer que le corps $M(\overline{\mathcal{X}})$ des fonctions méromorphes sur $\overline{\mathcal{X}}$ est une extension galoisienne finie de $\mathbb{C}(\overline{f})$ de groupe G.[5]

Le théorème d'existence de Riemann est plus largement un résultat d'équivalence de catégories, qui identifie les divers points de vue (topologique, analytique, algébrique) de la théorie des revêtements. Un exposé de ce volume est consacré à ce résultat [De01a].

[5] Il serait important de pouvoir démontrer le théorème d'existence de Riemann de manière algébrique (et éventuellement adaptée au cas de la caractéristique $p > 0$). Dans cette direction, indiquons l'article [Ko00] de Kollár qui fournit une preuve entièrement algébrique de son corollaire fondamental, à savoir, (Gal/Inv/Rég) sur un corps algébriquement clos de caractéristique 0. Sa méthode, qui ne passe pas par $\mathbb{C}$, utilise des techniques de déformation de Kollár-Miyaoka-Mori. (Voir aussi section 3.5).

2.2. Le point des résultats. — Le théorème d'existence de Riemann fait de l'étude des conjectures précédentes un problème de descente : on va chercher à démontrer le corollaire ci-dessus sur des sous-corps de $\mathbb{C}$, idéalement $\mathbb{Q}$. L'état actuel des connaissances est résumé par les théorèmes 2.1 et 2.2 ci-dessous.

Théorème 2.1. — *La forme régulière du problème inverse de Galois ainsi que ses variantes (version forte et* (BB)*) sont vraies si le corps de base K est un corps ample.*

Définition. — Un corps K est dit ample si pour toute K-courbe lisse C géométriquement irréductible, on a $C(K) \neq \varnothing \Rightarrow C(K)$ infini.

Exemples de corps amples

– Les corps pseudo algébriquement clos (PAC) : c'est-à-dire, les corps K pour lesquels $C(K) \neq \varnothing$ pour toute K-courbe lisse C géométriquement irréductible. Les corps algébriquement clos (et plus généralement séparablement clos) sont PAC. Il existe de nombreux autres exemples de corps PAC : voir [FrJa86], en particulier § 6.9 et § 16.6 ; le corps $\mathbb{Q}^{\mathrm{tr}}(\sqrt{-1})$ (voir la définition de $\mathbb{Q}^{\mathrm{tr}}$ ci-dessous) est un autre exemple de corps PAC.

– Les corps valués complets : $\mathbb{Q}_p$, $\mathbb{R}$, $k((x))$, etc.

– Les corps $\mathbb{Q}^{\mathrm{t}p}$: pour p premier fixé, le corps $\mathbb{Q}^{\mathrm{t}p}$ des nombres algébriques totalement p-adiques peut être défini comme l'extension galoisienne maximale de $\mathbb{Q}$ contenue dans $\mathbb{Q}_p$. Le corps $\mathbb{Q}^{\mathrm{t}\infty}$ des nombres algébriques totalement réels est plus traditionnellement noté $\mathbb{Q}^{\mathrm{tr}}$. Il y a des généralisations naturelles de ces corps qui sont aussi des corps amples : $\mathbb{Q}$ peut être remplacé par un corps de nombres K, le nombre premier p par un ensemble fini de places de K.

– Les extensions algébriques de corps amples.

Le théorème 2.1 correspond à la réunion de plusieurs travaux. Citons quelques contributions, qui ont semblé des étapes importantes à l'auteur :

– (GAL/INV/RÉG) : Harbater [Har84], [Har87], Dèbes-Fried [DeFr94], Dèbes [De95], Pop [Po96], Colliot-Thélène [Co00], Kollár [Ko00].

– (GAL/INV/RÉG/+) : Fried-Völklein [FrVo92], Fried-Haran-Völklein [FrHaVo93], Harbater [Har95], Pop [Po93] [Po96].

– (BB) : Dèbes [De99c], Colliot-Thélène [Co00], Moret-Bailly [Mo00].

La technique-clé a été la méthode de recollement pour les corps valués complets ; elle est due à D. Harbater. Pour certains corps amples (PAC, etc.), on peut utiliser alternativement la théorie des espaces de Hurwitz de M. Fried. Depuis la mise en œuvre par Colliot-Thélène des techniques de déformation de Kollár, on dispose encore d'une nouvelle approche, pour les corps amples de caractéristique 0. Les travaux de Fried-Völklein et de F. Pop sur la forme forte en termes de problèmes de plongement ont également marqué une évolution importante du problème. On doit aussi à Pop le passage aux corps amples.

Nous aurons l'occasion de préciser ces contributions en section 3 où nous reviendrons sur les différentes approches.

Dans le second énoncé les résultats sont d'un autre type : les problèmes sont résolus sur le corps $\mathbb{Q}$ mais pour des groupes G fixés.

Théorème 2.2

(a) *La forme régulière du problème inverse de Galois est vraie sur* $K = \mathbb{Q}$ *pour de nombreux groupes : les groupes abéliens,* S_d*,* A_d *(*$d > 0$*),* $\mathrm{GL}_n(\mathbb{F}_q)$*, de nombreuses familles classiques de groupes simples telles que* $\mathrm{PSL}_n(\mathbb{F}_q)$*,* $\mathrm{PSU}_n(\mathbb{F}_q)$*,* $\mathrm{PSp}_n(\mathbb{F}_q)$ *avec éventuellement des conditions sur* n *et* q*,* 25 *des* 26 *groupes simples sporadiques (manque le groupe de Mathieu* M_{23}*), etc.*

(b) *L'énoncé* (BB) *est vrai sur* $K = \mathbb{Q}$ *(et en fait sur tout corps* K[6]*) pour les groupes suivants :* S_d*,* A_d *(*$d > 0$*), les groupes abéliens, les groupes diédraux d'ordre impair et ceux d'ordre* 2^m *avec* $m \leqslant 4$*.*

La plupart des résultats dans (a) ont été obtenus par la méthode de *rigidité* et ses développements ; nous y revenons plus bas. Nous renvoyons à [MaMat99] pour un point plus précis et pour des références. Nombre de ces résultats sont dûs à Malle, Matzat et l'école d'Heidelberg ; citons aussi Belyi, Thompson, Völklein, etc. Les résultats du (b) sur le problème (BB) sont dus pour beaucoup à E. Black [Bl98], [Bl99a], [Bl99b], [Bl00] ; citons aussi Beckmann [Be94], Dèbes [De99c], Mestre [Me90], etc.

3. Les diverses approches

3.1. La rigidité. — Le théorème d'existence de Riemann permet de résoudre le problème (GAL/RÉG/INV) ainsi que ses variantes sur $K = \overline{\mathbb{Q}}$ (voir [De01a ; § 12] pour la descente de $\mathbb{C}$ à $\overline{\mathbb{Q}}$). Poursuivre la descente (idéalement jusqu'à $\mathbb{Q}$) est plus difficile. On souhaite montrer que sous certaines conditions les revêtements donnés par le théorème d'existence de Riemann sont définis sur $\mathbb{Q}$. La difficulté est de contrôler l'action de $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ sur un revêtement qui a *a priori* une origine topologique. On a cependant un bon contrôle de cette action sur les *invariants* du revêtement : le groupe, les points de branchement, l'invariant canonique de l'inertie (voir [De01a ; § 2]). On peut faire en sorte que l'action de $\mathrm{G}_{\mathbb{Q}}$ soit triviale sur les invariants mais cela ne suffit pas en général pour garantir que le revêtement est défini sur $\mathbb{Q}$. Cependant cela suffit parfois : dans certaines situations, les invariants déterminent la classe d'isomorphisme du revêtement ; si l'action de $\mathrm{G}_{\mathbb{Q}}$ est triviale sur ces invariants, alors le revêtement est défini sur $\mathbb{Q}$. Les conditions qui définissent ces situations s'appellent les conditions de *rigidité* : ce sont des conditions de théorie des groupes portant sur le groupe G à réaliser et des classes de conjugaison $C_1, \dots, C_r$ de G. La condition principale demande qu'il n'existe qu'une seule classe d'isomorphisme de G-revêtements

[6] Pour A_d avec $d > 5$, le résultat ne semble être connu que pour K de caractéristique 0.

ayant r points de branchement $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{Q})$ fixés et les « générateurs distingués de l'inertie » dans $C_1, \ldots, C_r$; cela correspond à la transitivité de l'action de G par conjugaison sur l'ensemble

$$\left\{ (g_1, \ldots, g_r) \in G^r \;\middle|\; \begin{array}{l} -\ g_1 \cdots g_r = 1 \\ -\ \langle g_1, \ldots, g_r \rangle\ = G \\ -\ g_i \in C_i \end{array} \right\}$$

Les conditions de rigidité sont assez contraignantes mais elles sont satisfaites pour certains groupes. Nous renvoyons à [Se92] et [MaMat99] pour plus de détails, des exemples et des références sur ce sujet.

Pour certains groupes, la méthode de rigidité ne donne pas le résultat désiré sur $\mathbb{Q}$ mais sur un corps de nombres explicite, en général une extension abélienne de $\mathbb{Q}$. Outre la rigidité, d'autres méthodes ont donné des résultats de réalisation de groupes sur $\mathbb{Q}$ ou des extensions contrôlées de $\mathbb{Q}$. L'idée est d'utiliser une action classique de $\mathrm{G}_{\mathbb{Q}}$ pour en déduire un morphisme surjectif $\mathrm{G}_{\mathbb{Q}} \twoheadrightarrow G$ sur un groupe classique. Par exemple, Shih utilise l'action de $\mathrm{G}_{\mathbb{Q}}$ sur les points de torsion des courbes elliptiques et arrive à en déduire dans certains cas des réalisations du groupe $\mathrm{PSL}_2(\mathbb{F}_q)$ ([Sh74], [Sh78], [Se92]).

3.2. Familles de revêtements. — La théorie de la rigidité a relancé le sujet dans les années 70. Deux autres méthodes ont permis ensuite des avancées plus marquantes encore, pour aboutir aux théorèmes 2.1 et 2.2 : la théorie des espaces de Hurwitz, due à M. Fried, qu'on peut voir comme un développement de la théorie de la rigidité, et les méthodes dites de recollement, dues à D. Harbater. Assez distinctes, elles reposent cependant sur une stratégie commune : travailler avec des *familles* de revêtements. Plus précisément, cela consiste à construire un revêtement défini sur une extension *transcendante régulière* F de $\mathbb{Q}$ et à chercher ensuite des spécialisations $\mathbb{Q}$-rationnelles du corps F ; en termes plus géométriques, cela revient à construire une famille de revêtements paramétrée par une variété $\mathcal{H}$ définie sur $\mathbb{Q}$ et chercher des points rationnels sur $\mathcal{H}$; le corps de fonctions $\mathbb{Q}(\mathcal{H})$ correspond à l'extension transcendante régulière F. En quelque sorte, on cherche à effectuer la descente, de $\mathbb{C}$ à $\mathbb{Q}$, en passant par les extensions transcendantes régulières (plutôt que par les sous-extensions « purement algébriques » $F \subset \overline{\mathbb{Q}}$).

Formellement une famille de revêtements est un morphisme $\mathcal{F} : \mathcal{T} \to \mathcal{H} \times \mathbb{P}^1$ fini et plat de variétés quasi-projectives tel que pour tout $h \in \mathcal{H}$ la fibre $\mathcal{F}_h : \mathcal{T}_h \to \mathbb{P}^1$ soit un revêtement. Birationnellement parlant, la variété $\mathcal{T}$ peut être vue comme une hypersurface $F(t_1, \ldots, t_r, \theta, t, y) = 0$ où $t_1, \ldots, t_r, \theta$ sont les fonctions coordonnées de l'espace des paramètres $\mathcal{H}$ et où, à paramètre $h = (t_1^o, \ldots, t_r^o, \theta^o)$ fixé, le revêtement $\mathcal{F}_h$ est le revêtement associé à l'équation $F(h, t, y) = 0$. Les fonctions coordonnées $t_1, \ldots, t_r, \theta$ satisfont les équations $\underline{h}(t_1, \ldots, t_r, \theta) = 0$ définissant la variété $\mathcal{H}$; on peut choisir $t_1, \ldots, t_r$ algébriquement indépendants sur $\mathbb{C}$. Le diagramme suivant résume la situation.

$$\begin{tikzcd}
F(t_1,\ldots,t_r,\theta,t,y)=0 \quad \mathcal{T} \arrow[d, "\mathcal{F}"'] & \mathcal{T}_h \arrow[l, hook'] \arrow[d, "\mathcal{F}_h"] \quad F(t_1^o,\ldots,t_r^o,\theta^o,t,y)=0 \\
\mathcal{H}\times\mathbb{P}^1 \arrow[d] & h\times\mathbb{P}^1 \arrow[l, hook'] \arrow[d] \\
\underline{h}(t_1,\ldots,t_r,\theta)=0 \quad \mathcal{H} & h \arrow[l, hook'] \quad =(t_1^o,\ldots,t_r^o,\theta^o)
\end{tikzcd}$$

Supposons que la famille soit définie sur $\mathbb{Q}$. S'il existe un point $h=(t_1^o,\ldots,t_r^o,\theta^o)\in\mathcal{H}(\mathbb{Q})$, le revêtement-fibre $\mathcal{F}_h:\mathcal{T}_h\to\mathbb{P}^1$ est défini sur $\mathbb{Q}$. Cette présentation s'adapte à la situation des G-revêtements. Pour démontrer la forme régulière du problème inverse sur $\mathbb{Q}$ (*i.e.*, l'énoncé (GAL/INV/RÉG)) pour G sur $\mathbb{Q}$, il suffit alors de montrer que $\mathcal{H}(\mathbb{Q})\neq\varnothing$.

Historiquement, deux types de constructions de familles se sont distingués : le premier correspond à une approche *modulaire* (ci-dessous), le second utilise des méthodes de *recollement* (section 3.4).

3.3. L'approche modulaire

3.3.1. Espaces de Hurwitz et problème inverse. — Cette première construction, due à M. Fried ([Fr77], [FrVo91]), repose sur la théorie des espaces de modules de revêtements — les espaces de Hurwitz. La construction de ces espaces est le fait fondamental. Précisément, si on fixe le nombre r de points de branchement et le groupe G du revêtement, on montre qu'il existe un espace de modules $\mathcal{H}_{r,G}$ pour la catégorie $\mathcal{C}_{r,G}$ des revêtements de $\mathbb{P}^1$ définis sur $\mathbb{C}$, avec r points de branchement et de groupe $G\subset S_d$: l'espace $\mathcal{H}_{r,G}$ est une variété algébrique lisse définie sur $\mathbb{Q}$ dont les points complexes correspondent bijectivement aux classes d'isomorphisme d'objets de la catégorie $\mathcal{C}_{r,G}$. De plus, si G est de centre trivial(7), il existe une famille de revêtements (au sens précédent) paramétrée par $\mathcal{H}_{r,G}$. Et cette famille est alors universelle ; $\mathcal{H}_{r,G}$ est un espace de modules *fin*.

Il s'agit ensuite, pour obtenir des applications au problème inverse de Galois, de trouver des points rationnels sur les espaces $\mathcal{H}_{r,G}$. On ne dispose pas d'une description assez bonne de ces espaces, qui ont eux aussi une origine topologique, pour traiter cette question en général. Dans certaines situations cependant, cela est possible. À ce niveau, on fixe, en plus de r et de G, le r-uplet $\mathbf{C}=(C_1,\ldots,C_r)$ des classes de conjugaison dans G des « générateurs distingués de l'inertie » au-dessus des points de branchement ; les sous-espaces correspondants $\mathcal{H}_{r,G}(\mathbf{C})\subset\mathcal{H}_{r,G}$ contiennent les composantes irréductibles de $\mathcal{H}_{r,G}$. Les espaces $\mathcal{H}_{r,G}(\mathbf{C})$ peuvent être parfois étudiés

(7)Pour le problème inverse, cette hypothèse n'est pas restrictive car tout groupe fini est quotient d'un groupe de centre trivial [FrVo91].

et décrits assez explicitement. Par exemple, pour $r = 4$, G un groupe diédral et $C_1, \dots, C_4$ égales à la classe des involutions de G, les espaces $\mathcal{H}_{r,G}(\mathbf{C})$ sont reliés assez naturellement à des courbes modulaires [DeFr94].

L'application principale au problème inverse de Galois utilise un critère de *rationalité* des espaces de Hurwitz[(8)], dû à M. Fried [Fr77]. Ce critère fait intervenir les courbes $\mathcal{C}$ tracées sur $\mathcal{H}'_{r,G}(\mathbf{C})$, dont les points h correspondent à des revêtements dont on a fixé $r-1$ des r points de branchement, disons $t_2, \dots, t_r$; le « $'$ » (dans $\mathcal{H}'_{r,G}(\mathbf{C})$) signifie qu'il faut travailler sur l'espace de Hurwitz des revêtements *avec* points de branchement *adjoints*. La condition principale du critère est que le genre g de ces courbes soit nul. Or ce genre g (qui est un invariant topologique) se déduit par la formule de Riemann-Hurwitz de la monodromie du revêtement de $\mathbb{P}^1$ associé à la correspondance $h \to t_1$ (pour h dans une courbe $\mathcal{C}$ comme ci-dessus) : le calcul se réduit à celui des orbites d'une certaine action d'un *groupe de tresses*. Il faut s'assurer préalablement que $\mathcal{H}'_{r,G}(\mathbf{C})$ est connexe, ce qui se voit aussi en regardant (la transitivité d')une action d'un groupe de tresses. La vérification des conditions du critère est donc un pur calcul de théorie des groupes. Dans les situations favorables[(9)], la monodromie du revêtement $h \to t_1$ fournit également, un point rationnel sur (le modèle projectif lisse de) $\mathcal{C}$, ce qui permet de conclure que $\mathcal{C} \simeq \mathbb{P}^1$ et $\mathcal{H}'_{r,G}(\mathbf{C}) \simeq \mathbb{P}^r$ (birationnellement, sur tout corps de définition de $\mathcal{H}'_{r,G}(\mathbf{C})$).

En utilisant et développant ce critère, Matzat a résolu le problème inverse pour de nombreux groupes ; la plupart des résultats du théorème 2.2(a) proviennent de cette méthode. Elle est cependant vraisemblablement insuffisante pour traiter la totalité du problème : le genre g n'est pas borné [DeFr94 ; § 3] ; on ne peut pas espérer que $\mathcal{H}'_{r,G}(\mathbf{C})$ soit une variété rationnelle en général. Mais Fried n'exclut pas qu'on puisse, sous certaines hypothèses sur G et $\mathbf{C}$ et pour r assez grand, obtenir des conclusions d'*unirationalité*.

L'approche modulaire fournit aussi des résultats en direction du théorème 2.1. Nous les indiquons au § 3.4.3 où nous les comparons à ceux que donnent les méthodes de recollement.

3.3.2. Familles de Hurwitz et théorie de la descente. — L'utilité des espaces de Hurwitz dépasse le simple cadre du problème inverse de Galois. D'une façon générale, les espaces de modules reflètent les propriétés des objets qu'ils paramètrent. Par exemple, l'étude du « bord » des espaces de Hurwitz donne des indications sur la dégénérescence des revêtements étudiés, ce qui, à son tour, par le principe que les singularités géométriques sont « reconnues par Galois », a des incidences arithmétiques. Un autre exemple vient de la *théorie de la descente*. Dans la recherche des plus petits corps de

(8) c'est-à-dire, pour qu'un espace de Hurwitz soit birationnel à un espace projectif
(9) C'est le cas par exemple si les cycles de ramification au-dessus d'un des trois points de ramification t_2, t_3, t_4 sont de longueurs distinctes, ou plus généralement si le nombre de cycles de longueur donnée est impair.

définition d'un revêtement donné, le *corps des modules*, *i.e.*, le corps de définition du point correspondant sur l'espace de modules, est un point de repère naturel. Le corps des modules *est* le plus petit corps de définition si par exemple $\mathcal{H}_{r,G}$ est un espace de modules fin, et plus généralement s'il existe une famille de revêtements paramétrée par l'espace $\mathcal{H}_{r,G}$ — une famille de Hurwitz. Quand ce n'est pas le cas, des extensions éventuelles du corps des modules sont nécessaires pour obtenir un corps de définition, qui correspondent aux revêtements étales de $\mathcal{H}_{r,G}$ au-dessus desquelles il existe des familles de Hurwitz. De nombreux résultats dans cette direction ont été obtenus ces dernières années (voir notamment [DeDoEm00]), qui montrent que les espaces de modules sont un cadre naturel pour le développement des outils fondamentaux de descente (cocycles d'obstruction, gerbes, etc.) forgés par Weil [We56] et Grothendieck [Gr60]. L'énoncé suivant, qui combine des énoncés de [DeDo97], [DeDo98], [DeDo99], [DeHar98], [Em99] et [DeDoMo00], est une illustration des progrès réalisés.

Théorème 3.1. — *Soit $f : X \to \mathbb{P}^1$ un $\overline{\mathbb{Q}}$-revêtement de corps des modules $\mathbb{Q}$.*

(a) *Le revêtement f est défini sur $\mathbb{Q}^{\mathrm{t}p}$ (donc en particulier sur $\mathbb{Q}_p$), pour tout p sauf éventuellement si p est l'un des « mauvais » premiers liés au revêtement, i.e., si p divise l'ordre du groupe du revêtement ou si les points de branchement deviennent égaux modulo p.*

(b) *Si f est un* G*-revêtement, f est défini sur $\mathbb{Q}$ ssi f est défini sur $\mathbb{Q}_p$ pour tout p.*

Le théorème 3.1 s'étend au cas où $\mathbb{Q}$ est plus généralement un corps de nombres K. Pour le (b), on doit cependant supposer que le corps K n'est pas une exception au théorème de Grunwald-Wang (*cf.* [DeDo97 ; § 3.5]).

Pour une introduction aux questions de descente en liaison avec les espaces de modules, nous renvoyons à [De01b]. À propos des espaces de Hurwitz en général et leurs applications, il y a une littérature abondante. Un exposé de ce volume de M. Emsalem [Em01] est consacré à ce sujet. Il en donne une présentation moderne, en termes de champs. Pour une présentation plus classique, nous renvoyons à [De99a].

3.4. Méthodes de recollement et de déformation

3.4.1. Le résultat central. — C'est ici le

Théorème d'Harbater. — *La forme régulière du problème inverse de Galois, i.e., l'énoncé* (GAL/INV/RÉG)*, est vraie sur tout corps K valué complet.*

Il y a maintenant plusieurs démonstrations de ce résultat. Une idée souvent présente est de construire des revêtements par recollements de revêtements élémentaires, cycliques par exemple. C'est en gros ce que l'on faisait sur le corps des complexes où la topologie permet de couper et coller des bouts de surfaces de Riemann. Sur un corps valué complet, on peut également effectuer ces opérations, en se plaçant dans le contexte de la géométrie formelle ou celui essentiellement équivalent de la géométrie rigide, mis en place respectivement par A. Grothendieck et J. Tate. Des théorèmes type GAGA garantissent que les revêtements ainsi construits ont une structure algébrique. La preuve initiale d'Harbater [Har87] utilise la géométrie formelle (formal patching) ; le point de vue rigide a été développé par Serre [Se92], Liu [Li95] et Pop [Po96] ; un point de vue plus algébrique (algebraic patching), a été proposé ensuite par Haran, Jarden et Völklein ([HaVo96], [HaJa98a], [HaJa98b], [HaJa00]).

Le mécanisme de recollement comporte deux étapes, qui apparaissent nettement dans [Mo00], où l'auteur démontre (GAL/INV/RÉG) et (BB) sur un corps ample. La première consiste à *assembler* des revêtements élémentaires : elle conduit à un K-revêtement d'une « chaîne de $\mathbb{P}^1$ », qui est connexe si on identifie convenablement certaines fibres des revêtements élémentaires. L'espace-base de cet assemblage est une courbe singulière. Une seconde étape est nécessaire pour *déformer* ce revêtement en un revêtement d'une courbe lisse. La déformation de la base s'appuie sur les résultats de Deligne-Mumford [DelMu69] ; la déformation du revêtement, ensuite, utilise un travail de Harbater-Stevenson [HarSt99].

Cette technique de construction de revêtements par recollement s'est révélée féconde, pour de nombreux problèmes d'existence de revêtements. Elle a notamment permis des avancées significatives en caractéristique $p > 0$ où elle sert de palliatif en l'absence du théorème d'existence de Riemann (*cf.* section 4). C'est ainsi une technique de base dans la preuve de la conjecture d'Abhyankar, par Raynaud et Harbater. Un exposé de ce volume, de Q. Liu [Li01], est consacré à ce type de techniques ; nous y renvoyons.

Plus récemment, une nouvelle approche du théorème d'Harbater a été proposée par Colliot-Thélène [Co00], puis Kollár [Ko00]. Nous y revenons dans la sous-section 3.5.

3.4.2. Construction de familles de revêtements via les méthodes de recollement

L'idée de départ est d'utiliser le théorème d'Harbater sur le corps $k((x))$ des séries formelles à coefficients dans un corps k (arbitraire). Un revêtement galoisien $f : X \to \mathbb{P}^1$ défini sur $k((x))$ de groupe G donné (comme fourni par le théorème d'Harbater) peut être vu comme une famille de G-revêtements paramétrée par une variété $\mathcal{H}$: on prend pour $\mathcal{H}$ une variété dont le corps des fonctions $k(\mathcal{H})$ est un sous-corps de type fini de $k((x))$ sur lequel f est défini. De plus, comme $k(\mathcal{H}) \subset k((x))$, la variété $\mathcal{H}$ est définie sur k. (Voir [DeDes97] pour plus de détails sur cet argument).

3.4.3. Quelques résultats. — Comme dans l'approche modulaire, toute la question est de trouver des points rationnels sur $\mathcal{H}$. Et on voit là une différence entre les deux approches. La variété $\mathcal{H}$ de ce paragraphe est obtenue de façon abstraite et il semble difficile d'étudier les points rationnels sur $\mathbb{Q}$ ou sur des corps de nombres spécifiques. Par contre, $\mathcal{H}$ a par construction des points $k((x))$-rationnels. Les espaces de Hurwitz sont plus concrets ; il est parfois possible d'y trouver des points rationnels, éventuellement sur le corps $\mathbb{Q}$. Mais on ne dispose pas de résultat général d'existence, même sur les corps $k((x))$.

D'après un résultat de Pop [Po96], si le corps k est ample on peut déduire que $\mathcal{H}$ possède des points k-rationnels (l'énoncé précis est que les corps amples sont *existentiellement clos* dans $k((x))$ (et réciproquement)). On obtient ainsi, comme conséquence de cette sous-section, le problème inverse de Galois (forme régulière) sur les corps amples. Les variantes (version forte et (BB)) procèdent des mêmes principes ; elles sont dues, pour le cas général des corps amples, à Pop [Po96] (pour (GAL/INV/RÉG/+)) et à Moret-Bailly (pour (BB)).

Pour le cas particulier des corps PAC de caractéristique 0, on peut aussi obtenir les trois formes du problème inverse, *i.e.*, le théorème 2.1, par l'approche modulaire. C'est ce que font Fried et Völklein dans [FrVo92] (voir aussi [De99c] pour (BB) dans ce contexte). B. Deschamps [Des95] a aussi montré, *via* l'approche modulaire, qu'étant donné un groupe fini G, il existe une variété irréductible $\mathcal{H}$ (en fait une infinité) définie sur $\mathbb{Q}$ et telle que

– $\mathcal{H}(\mathbb{Q}) \neq \varnothing$ entraîne que G est groupe de Galois (régulièrement) sur $\mathbb{Q}(T)$ (et *idem* pour tout corps $k \supset \mathbb{Q}$ à la place de $\mathbb{Q}$), et

– $\mathcal{H}(\mathbb{Q}_p) \neq \varnothing$ pour tout premier p (y compris $p = \infty$).

Dans la preuve de Deschamps, $\mathcal{H}$ est un espace de Hurwitz. On sait aussi démontrer ce résultat par la seconde approche [DeDes97], comme conséquence de (GAL/INV/RÉG) sur $\mathbb{Q}((x))$; on peut même alors demander que $\mathcal{H}$ soit une courbe (mais elle est moins explicite que l'espace $\mathcal{H}$ de Deschamps). J-L. Colliot-Thélène [Co00] a également noté que l'énoncé (GAL/INV/RÉG) pour un groupe G donné sur le corps $\mathbb{Q}((x))$ entraîne l'existence de corps de nombres $k_1, \ldots, k_n$ de degrés $[k_i : \mathbb{Q}]$ relativement premiers dans leur ensemble et tels que G est groupe de Galois sur $k_i(T)$ régulièrement, $i = 1, \ldots, n$.

3.5. Autour du programme de Noether

3.5.1. Variétés rationnellement connexes. — On peut aussi voir le revêtement de Noether, et plus généralement les extensions génériques, comme des familles de G-extensions (ou de G-torseurs). Nous gardons les notations introduites dans la section 1.4. Par revêtement de Noether, nous entendrons un des deux revêtements suivants, que nous noterons $V_G \to U_G$ dans les deux cas :

$$\left|\begin{array}{l} \bullet\ \mathbb{A}^d \to \mathbb{A}^d/G \text{ avec } G \subset S_d \\ \bullet\ \mathrm{GL}_d \to \mathrm{GL}_d/G \text{ avec } G \subset \mathrm{GL}_d \end{array}\right.$$

où G est un groupe fixé d'ordre d.

La propriété verselle de ce revêtement en fait un outil appréciable. Étant donné un corps K, les points K-rationnels [resp. les points $K(T)$-rationnels] correspondent aux G-extensions d'*algèbres* de K [resp. de $K(T)$]. Pour retrouver le contexte des G-revêtements, on peut par exemple fixer une G-extension E/K de *corps* et s'intéresser aux points $K(T)$-rationnels sur U_G, autrement dit aux courbes K-rationnelles tracées sur U_G et passant, d'une part par un point $u_1 \in U_G(K)$ correspondant à la G-extension

E/K et d'autre part par un point $u_o \in U_G(K)$ correspondant à la G-extension d'algèbre triviale (d copies de K). Une telle courbe K-rationnelle C correspond alors à un G-revêtement connexe de $\mathbb{P}^1$ défini sur K et se spécialisant en l'extension E/K en un point $t_1 \in \mathbb{P}^1(K)$ et en l'extension triviale en un autre $t_o \in \mathbb{P}^1(K)$ (ces deux spécialisations assurant que l'algèbre $E/K(T)$ associée à la courbe C est respectivement un corps et une extension régulière de K). L'existence de telles courbes C est liée à la propriété de *connexité rationnelle* de U_G sur K, qui demande que deux K-points sur U_G puissent *toujours* être liés par une courbe K-rationnelle[(10)] [Co99]. Or, la variété U_G étant unirationnelle, cette propriété est vraie sur $\overline{K}$; U_G est *rationnellement connexe* sur $\overline{K}$.

3.5.2. L'approche de Colliot-Thélène et Kollár. — En appliquant à la variété de Noether $U_G = \mathrm{GL}_d/G$ des techniques de déformation dans les variétés *rationnellement connexes* dues à Kollár-Miyaoka-Mori[(11)], Colliot-Thélène [Co00] a obtenu une nouvelle preuve du théorème d'Harbater. De plus sa méthode a permis de démontrer (BB) sur les corps amples de caractéristique 0. Dans un article ultérieur [Ko00], Kollár obtient même, comme produit de la méthode, l'existence pour tout groupe fini G, d'un $\overline{\mathbb{Q}}$-revêtement galoisien de groupe G (pour ce point Colliot-Thélène invoque le théorème d'existence de Riemann).

Comme dans le § 3.4, on peut distinguer dans la méthode les deux étapes d'assemblage et de déformation. Ainsi [Co00] part d'un $\overline{K}$-revêtement galoisien de $\mathbb{P}^1$ de groupe G donné, qui est vu comme comme une $\overline{K}$-courbe rationnelle tracée sur la variété de Noether U_G. On peut s'arranger pour que cette courbe passe par un point K-rationnel u de U_G (correspondant par exemple à la G-extension de K donnée dans (BB)). L'ensemble (ou l'assemblage) des conjugués de cette courbe sous G_K fournit, après éclatement du point commun u, une K-courbe paramétrée par un « K-arbre singulier » de $\mathbb{P}^1$s. La seconde étape utilise les techniques de Kollár : par déformation de cet arbre, on obtient sur U_G *une* K-courbe rationnelle irréductible et lisse, c'est-à-dire, un K-G-revêtement d'*un seul* $\mathbb{P}^1$.

3.5.3. Connexité rationnelle sur les corps amples. — En termes de la variété de Noether U_G et pour G groupe fini fixé, la propriété (BB) est satisfaite si par tout K-point donné u_1 de U_G, on peut faire passer une K-courbe rationnelle sur laquelle le revêtement de Noether induise un revêtement par une K-courbe *absolument irréductible.* Pour un corps ample K, on peut se demander si on peut améliorer (BB) en montrant qu'il existe une K-courbe rationnelle passant par u_1 et le point $u_0 \in U_G(K)$ correspondant à la G-extension d'algèbre triviale (d copies de K). La réponse est négative

(10) De façon précise, la définition demande que les deux points puissent être liés par une *chaîne* de courbes rationnelles. Mais on peut montrer que sur un corps ample (ce à quoi nous nous bornerons ici), *une seule* courbe suffit [Mo01].

(11) Ces auteurs travaillent initialement sur un corps de base algébriquement clos. La généralisation aux corps amples est due à Kollár.

en général. En s'appuyant sur le contre-exemple de Wang au théorème de Grunwald, Colliot-Thélène [Co00] a donné un contre-exemple : il prend $K = \mathbb{Q}_2$, G le groupe cyclique C_8 et u_1 correspondant à la C_8-extension non ramifiée de $\mathbb{Q}_2$(12) ; en particulier, U_G n'est pas K-rationnellement connexe.

Il y a néanmoins des énoncés positifs. Ainsi, si le corps K est PAC, la propriété de connexité rationnelle est vraie sur K. En fait, toute G-extension d'algèbres E/K d'un corps PAC K de groupe donné G est spécialisation de *tout* G-revêtement de $\mathbb{P}^1$ défini sur K [De99c]. Depuis un travail récent de P. Gille [Gi01], complété par Moret-Bailly [Mo01], on dispose aussi du résultat suivant : si G est un groupe fini et p un nombre premier ne divisant pas $|G|$, alors la variété U_G est rationnellement connexe sur $\mathbb{Q}_p$; autrement dit, si p ne divise pas $|G|$, deux G-extensions d'algèbres de $\mathbb{Q}_p$ de groupe G sont spécialisations d'un $\mathbb{Q}_p$-revêtement de $\mathbb{P}^1$. Dans [Co99], Colliot-Thélène demande si une $\mathbb{Q}$-variété $\overline{\mathbb{Q}}$-rationnellement connexe est $\mathbb{Q}_p$-rationnellement connexe pour tout p sauf un nombre fini. D'après le résultat de Gille, c'est le cas pour la variété U_G.

3.5.4. Compléments sur le problème de Beckmann-Black. — Dans ce qui précède, le corps de base est un corps ample. Il existe aussi de nombreux résultats relatifs au problème (BB) sur le corps $\mathbb{Q}$, comme ceux énoncés dans le théorème 2.2. Les méthodes sont différentes et diverses. Dans [Be94], S. Beckmann propose des constructions explicites pour le cas des groupes abéliens et du groupe symétrique S_d. Pour un groupe abélien G, l'énoncé découle en fait de la propriété relativement classique suivante [De99b] : tout G-revêtement de $\mathbb{P}^1$ (ou d'une base plus générale) défini sur un corps K (arbitraire) peut être « tordu » en un autre K-modèle(13) ayant pour fibre une G-extension d'algèbres arbitraire donnée à l'avance. Pour le groupe alterné A_d, l'énoncé (BB) se déduit des réalisations régulières explicites de A_d données par J-F. Mestre [Me90]. Les résultats d'E. Black sur les groupes diédraux D_n nécessitent également une approche assez fine [Bl98] [Bl99a]. Dans un premier temps, elle se place sur un corps contenant suffisamment de racines de l'unité ; elle peut alors utiliser la théorie de Kummer et les travaux de Saltman pour traiter la partie cyclique C_n du groupe diédral. La précision de ces résultats est suffisante pour passer de C_n à D_n (un problème type problème de plongement) et pour redescendre ensuite sur le corps initial (sans les racines de l'unité). Dans le cas où $n = 2^m$ $(m > 0)$ et $K = \mathbb{Q}$, il y a cependant des difficultés techniques liées au contre-exemple de Wang.

3.6. Action de Belyi-Ihara et groupe de Grothendieck-Teichmüller

Dans notre présentation, le point de départ était de reposer les questions historiques (de *théorie des nombres*) sur $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (problème inverse sur $\mathbb{Q}$, conjecture

(12) Rappelons que le même exemple avait été utilisé par Saltman pour montrer que U_G n'est pas une variété rationnelle si $G = C_8$.

(13) Par K-modèle, nous entendons un G-revêtement de $\mathbb{P}^1$ défini sur K et isomorphe sur $\overline{K}$ au G-revêtement initial.

de Shafarevich) sous un angle *géométrique*, en ajoutant une indéterminée T. Cela a permis de nombreuses avancées, mais la méconnaissance de $\mathrm{G}_{\mathbb{Q}}$, ici dans son action sur les revêtements de $\mathbb{P}^1$, demeure le problème majeur en général. Même si dans certains cas (rigidité, etc.), les contraintes de la géométrie et de la théorie des groupes ont permis de contourner la difficulté en trivialisant la face arithmétique du problème, on peut penser qu'une étude plus systématique de $\mathrm{G}_{\mathbb{Q}}$ s'impose. Il s'agit évidemment d'une question fondamentale, à la croisée de multiples travaux. Par la théorie du corps de classes global, on accède à l'abélianisé de $\mathrm{G}_{\mathbb{Q}}$. Il y a aussi de nombreux travaux sur les représentations ℓ-adiques de $\mathrm{G}_{\mathbb{Q}}$, notamment celles qui proviennent de l'action de $\mathrm{G}_{\mathbb{Q}}$ sur la cohomologie ℓ-adique des extensions à $\overline{\mathbb{Q}}$ des $\mathbb{Q}$-variétés algébriques. On peut d'ailleurs replacer les travaux de Shih évoqués en section 2.1 dans ce courant. Dans les années 70, A. Grothendieck place le problème sur un terrain résolument géométrique en proposant de parvenir à $\mathrm{G}_{\mathbb{Q}}$ *via* son action sur les revêtements de $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ et plus généralement sur les espaces de modules de courbes avec r points marqués.

Plus précisément, notons $\widehat{\pi}_1$ le groupe fondamental de la $\overline{\mathbb{Q}}$-variété $\mathbb{P}^1\setminus\{0, 1, \infty\}$. On parle ici de la version *algébrique* du groupe fondamental qui classifie les $\overline{\mathbb{Q}}$-revêtements algébriques de $\mathbb{P}^1$ ramifiés au-dessus de $0, 1, \infty$ (au plus) ; il résulte du théorème d'existence de Riemann que $\widehat{\pi}_1$ est le complété profini du groupe fondamental topologique, c'est-à-dire du groupe libre $F(2)$ à 2 générateurs. L'action de $\mathrm{G}_{\mathbb{Q}}$ induit un homomorphisme

$$\mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{\pi}_1)$$

Un fait majeur est que ce morphisme est injectif. Cela résulte du théorème de Belyi ([Bel79], [Se89]), selon lequel toute $\overline{\mathbb{Q}}$-courbe algébrique peut être présentée comme revêtement de $\mathbb{P}^1$ ramifié seulement en 0, 1 et ∞. L'étape suivante est de mieux cerner l'image de ce morphisme. Cette action de $\mathrm{G}_{\mathbb{Q}}$ a été l'objet de nombreux travaux, notamment de G. Anderson, P. Deligne, Y. Ihara et A. Grothendieck (nous renvoyons à [Ih90] pour un exposé de survol et des références). Ainsi, les « dessins d'enfants » sont des représentations des revêtements de $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ destinés à mieux visualiser cette action. Un résultat significatif a été de montrer que l'image du morphisme ci-dessus est contenue dans un certain sous-groupe de $\widehat{\mathbb{Z}} \times \widehat{F(2)}'$ décrit par des formules explicites. Ce groupe, qui a été découvert par Drinfel'd dans un autre contexte, est noté $\widehat{\mathrm{GT}}$ et appelé groupe de Grothendieck-Teichmüller.

Plus généralement, pour $r \geqslant 3$, considérons la $\mathbb{Q}$-variété des r-uplets à coordonnées distinctes dans $\mathbb{P}^1$ et notons X_r son quotient par l'action de PGL_2. On a ainsi $X_3 \simeq \mathrm{Spec}(\mathbb{Q})$ et $X_4 \simeq \mathbb{P}^1 \setminus \{0, 1, \infty\}$. Le groupe fondamental topologique de X_r est un groupe classique, le *mapping class group* $M_{o,r}$, lequel est un quotient du *groupe des tresses* d'Artin B_r. L'action de $\mathrm{G}_{\mathbb{Q}}$ sur les revêtements de X_r induit un homomorphisme

$$\mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}(\widehat{M_{o,r}})$$

Il existe d'autre part des flèches $X_{r+1} \to X_r$ définies sur $\mathbb{Q}$ qui induisent des homomorphismes $\widehat{M_{o,r+1}} \to \widehat{M_{o,r}}$. On obtient en fait une action sur la tour de ces groupes fondamentaux

$$\mathrm{G}_{\mathbb{Q}} \to \mathrm{Aut}\begin{bmatrix} \vdots \\ \widehat{M_{o,r+1}} \\ \downarrow \\ \widehat{M_{o,r}} \\ \vdots \end{bmatrix}$$

On sait relier le groupe de droite au groupe de Grothendieck-Teichmüller de façon précise : moyennant quelques conditions techniques supplémentaires, on obtient exactement $\widehat{\mathrm{GT}}$ [LoSc94]. Il est évidemment naturel de demander quelle place occupe le groupe $\mathrm{G}_{\mathbb{Q}}$ à l'intérieur de $\widehat{\mathrm{GT}}$.

Pour une introduction plus détaillée à cette branche du domaine, nous renvoyons à [Ih90] et [Lo01].

4. Caractéristique $p > 0$

L'inséparabilité éventuelle des extensions, la possibilité de ramification sauvage, l'existence d'extensions cycliques non-kummeriennes, etc., sont autant de phénomènes spécifiques à la caractéristique $p > 0$ qui rendent ce cas plus difficile en général. Un fait fondamental résume la difficulté : on ne connaît pas d'analogue du théorème d'existence de Riemann en caractéristique $p > 0$. Donc, même sur des corps algébriquement clos, les questions considérées posent *a priori* des problèmes. Les techniques de recollement (section 3.4), qui permettent de construire des revêtements et qui sont valides en toute caractéristique, pallient cependant à ce manque et ont permis de réaliser des progrès importants. En fait, une forme faible du théorème d'existence de Riemann, indiquant que, sous certaines conditions, le π_1 en caractéristique $p > 0$, a pour quotient un quotient assez gros du π_1 en caractéristique 0, a été établie par F. Pop [Po94].

4.1. Problème inverse en caractéristique $p > 0$. — Le théorème 2.1 sur le problème inverse et ses variantes sur les corps amples est démontré en toute caractéristique (*cf.* § 3.4). On obtient en particulier les énoncés (Gal/Inv/Rég) [Har84] et (Gal/Inv/Rég/+) [Har95], [Po93] sur un corps algébriquement clos. Le second signifie simplement que le groupe $\mathrm{G}_{\overline{K}(T)}$ est un groupe pro-libre (*via* le théorème de Tsen). L'énoncé (Gal/Inv/Rég) appliqué à un certain corps PAC construit comme ultraproduit de corps finis (une construction due initialement à J. Ax) permet de montrer qu'étant donné un groupe fini G, (Gal/Inv/Rég) est vrai pour G sur tout corps fini $\mathbb{F}_q$ sauf éventuellement un nombre fini ; ce résultat est initialement dû à Fried et Völklein [FrVo92], mais pour la variante un peu plus faible « sur tout corps fini premier $\mathbb{F}_p$ sauf éventuellement un nombre fini », le cas général a été établi ensuite par Pop [Po96]. Pour le corps premier $K = \mathbb{F}_p$, de nombreuses réalisations explicites de groupes classiques ont été obtenues par Abhyankar. Quant à l'énoncé (BB), comme les précédents, il a été établi sur tout corps ample (de caractéristique arbitraire) ; ce résultat est dû à Moret-Bailly [Mo00]. Le (b) du théorème 2.2, également relatif à l'énoncé (BB), est lui aussi valable en toute caractéristique (sauf pour le groupe A_d avec $d > 5$).

4.2. Groupes fondamentaux et conjecture d'Abhyankar. — On se place ici sur un corps de base k algébriquement clos de caractéristique $p > 0$.

4.2.1. Le cas affine. — En l'absence du théorème d'existence de Riemann, le groupe fondamental (algébrique) $\pi_1(X)$ de $X = \mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}$ $(r > 0)$, qui classifie les revêtements de $\mathbb{P}^1$ non ramifiés au-dessus de X, est encore mal connu. On sait cependant grâce au *théorème de spécialisation* de Grothendieck [Gr71-SGA1] que le $\pi_1^{p'}$ (*premier à* p) [resp le π_1^{t} (*modéré*)], qui classifie les revêtements de groupe d'ordre premier à p [resp. les revêtements modérément ramifiés (en $x_1, \ldots, x_r$)], est isomorphe à la p'-partie du π_1 en caractéristique 0 (*i.e.*, du groupe pro-libre à $r-1$ générateurs) [resp. est isomorphe à un quotient du π_1 en caractéristique 0]. Le cas général est plus complexe : par exemple, on sait que la structure de π_1 dépend de l'ensemble $\{t_1, \ldots, t_r\}$ et pas seulement de r comme en caractéristique 0.

À défaut de pouvoir décrire π_1 exactement, on connaît l'ensemble de ses quotients finis (noté π_A) ; on sait donc quels groupes sont groupes d'automorphismes d'un revêtement, non-ramifié au-dessus de $\mathbb{P}^1 \setminus \{t_1, \ldots, t_r\}$. La réponse est donnée par la

Conjecture d'Abhyankar. — *Un groupe G est quotient du π_1 si et seulement si chaque quotient de G d'ordre premier à p est quotient du π_1 en caractéristique* 0.

qui a été démontrée en 1992. Raynaud [Ra94] a d'abord traité le cas de la droite affine (X avec $r = 1$) ; Harbater [Har94] a déduit ensuite le cas général, encore grâce à des méthodes de recollement.

La condition de l'énoncé équivaut à demander que le quotient de G par le sous-groupe engendré par ses p-Sylow soit quotient du π_1 en caractéristique 0. Il y a *a priori* plus de revêtements en caractéristique p qu'en caractéristique 0 : par exemple, au contraire de la caractéristique 0, les p-groupes, et plus généralement les *quasi-p* groupes (*i.e.*, les groupes qui sont engendrés par leurs p-sous-groupes de Sylow) sont groupes de Galois de revêtements non ramifiés de la droite affine ; penser au revêtement d'Artin-Schreier.

4.2.2. Le cas projectif. — La conjecture d'Abhyankar est établie plus généralement avec $\mathbb{P}^1$ remplacé par une courbe projective $\overline{X}$ de genre g. Pour $g > 0$, on peut également regarder le cas $r = 0$, *i.e.*, le cas où $X = \overline{X}$ est une courbe projective. Le cas projectif est assez différent du cas affine. Ainsi, pour une courbe projective, le π_1 est déterminé par l'ensemble π_A de ses quotients finis[(14)]. L'étude du π_A est donc aussi difficile que celle du π_1. La considération des revêtements de groupe un p-groupe fournit une autre différence. En fait, la p-partie du π_1 d'une courbe projective $\overline{X}$ de genre g est connue, grâce un résultat de Shafarevich ; elle dépend essentiellement de p, de g et de l'invariant de Hasse-Witt $\gamma_{\overline{X}}$ de $\overline{X}$ (*i.e.*, la $\mathbb{F}_p$-dimension du sous-groupe de p-torsion de la jacobienne $J_{\overline{X}}$ de $\overline{X}$). Ainsi, pour qu'un p-groupe soit dans π_A, il doit être de rang $\leqslant \gamma_{\overline{X}}$. Il y a donc moins de revêtements en caractéristique $p > 0$ qu'en caractéristique 0 (contrairement au cas affine $r > 0$) : le groupe $(\mathbb{Z}/p\mathbb{Z})^2$ est groupe d'automorphismes d'un revêtement non ramifié d'une courbe elliptique en caractéristique 0 mais pas en caractéristique p (car $\gamma_{\overline{X}} \leqslant g = 1$). La condition de la conjecture d'Abhyankar pour qu'un groupe soit dans π_A n'est donc pas suffisante pour une courbe projective (on sait par Grothendieck qu'elle demeure nécessaire). Le cas « projectif » a beaucoup été étudié par K. Stevenson ([St96], [St98]). Elle a par exemple montré que tout groupe fini engendré par d éléments est quotient du π_1 de *presque toute* courbe projective $\overline{X}$ de genre $g \geqslant d$. Nous renvoyons à ses travaux.

4.2.3. Autres généralisations. — Un autre sujet de recherches dans cette direction est de chercher à généraliser la conjecture d'Abhyankar à des variétés de dimension supérieure. Des travaux d'Harbater vont dans ce sens. Il a récemment montré avec M. van der Put que la condition du cas des courbes ne s'étend pas telle quelle [HarvdP00].

4.3. Réduction et relèvement des revêtements. — La situation générale est la suivante. On se donne un anneau de valuation discrète (complet) R de corps résiduel k de caractéristique p. Un revêtement $f : X \to \mathbb{P}^1$ sur R étant donné, on peut s'intéresser au revêtement $\overline{f} : \overline{X} \to \mathbb{P}^1$ sur k obtenu par *réduction* ; on dit qu'il y a bonne réduction si $\overline{X}$ est irréductible et réduit. Inversement, un k-revêtement $\overline{f}$ étant donné, on dit qu'il se *relève* sur R s'il existe un R-revêtement f qui se réduit en $\overline{f}$.

Réduction et relèvement des revêtements, qui font le lien entre la caractéristique 0 et la caractéristique > 0, sont des questions beaucoup étudiées. La recherche du groupe fondamental des courbes en caractéristique $p > 0$ est une première motivation : la caractéristique 0 sert de modèle et de point de départ. On peut aussi avoir des motivations arithmétiques, l'idée générale étant que « Galois respecte les singularités » des revêtements, notamment en réduction. Ainsi, il y a un lien entre la bonne ou mauvaise réduction de f et la ramification de p dans le corps des modules de f.

Pour ces questions, il y a un premier cas que l'on maîtrise assez bien, en gros grâce au théorème de spécialisation de Grothendieck : le cas des revêtements de groupe d'ordre premier à p et plus généralement des revêtement modérément ramifiés. Les k-revêtements modérément ramifiés se relèvent en caractéristique 0. Un résultat de

[(14)] Cela résulte du théorème de spécialisation de Grothendieck (cas projectif) qui entraîne que le π_1 d'une courbe projective, quotient du π_1 en caractéristique 0, est un groupe pro-fini de type fini, combiné au fait qu'un tel groupe est déterminé par ses quotients finis [FrJa86 ; Prop. 15.4].

Fulton [Fu69], qui est un ingrédient-clé du théorème de spécialisation, précise la question de la réduction : si les points de branchement d'un R-revêtement f modérément ramifié demeurent distincts en réduction, alors il y a bonne réduction. Un résultat de Beckmann [Be89], également conséquence du théorème de Grothendieck, indique que si p est un *bon* premier, *i.e.*, si p ne divise pas l'ordre du groupe du revêtement et si les points de branchement demeurent distincts en réduction, alors p n'est pas ramifié dans le corps des modules de f.

On en connaît beaucoup moins sur le cas des revêtements de groupe d'ordre divisible par p, qui est plus complexe, mais aussi potentiellement plus instructif. Ainsi dans la preuve de la conjecture d'Abhyankar, les revêtements qu'il s'agit de construire s'obtiennent à partir de revêtements en caractéristique 0 dans une situation où il y a mauvaise réduction. Un outil important est la théorie de la *réduction semi-stable* : le travail consiste alors à étudier la mauvaise réduction des modèles semi-stables (qui existent en général). En utilisant la même démarche, Raynaud [Ra99] a obtenu, pour des revêtements galoisiens de $\mathbb{P}^1 \setminus \{0, 1, \infty\}$ de groupe d'ordre divisible par p, une borne pour l'indice de ramification de p dans son corps des modules, sous l'hypothèse de mauvaise réduction. *A contrario* cela fournit un critère de bonne réduction. En suivant l'approche de Raynaud, I. Bouw et S. Wewers [BoWe00] poursuivent ce travail en envisageant le cas de 4 points de branchement. M. Emsalem et S. Flon développent le résultat de Beckmann dans les situations potentielles de mauvaise réduction où p est un « mauvais » premier ; ils obtiennent des formules reliant les indices de ramification de p à d'autres invariants. Les questions de relèvement font également l'objet de nombreux travaux dans le cas non modéré. Une conjecture attribuée à F. Oort prédit que tout G-revêtement cyclique en caractéristique p se relève en caractéristique 0. Il y a plusieurs approches : voir les travaux de Green-Matignon, Saïdi, Henrio, Bertin-Mézard. Actuellement, on ne sait traiter que le cas d'un groupe d'ordre divisible par p^2 au plus. Là encore, les techniques de déformation des revêtements, ou de façon équivalente, des représentations de π_1, se révèlent utiles.

Pour plus de détails et plus de références sur cette partie, voir [Em01].

Références

[Be89] S. Beckmann, *Ramified primes in the field of moduli of a branched covering of curves*, J. Algebra, **125**, (1989), 236–255.

[Be94] S. Beckmann, *Is every extension of $\mathbb{Q}$ the specialization of a branched covering ?*, J. Algebra, **164**, (1994), 430–451.

[Bel80] G.V. Belyi, *On Galois extensions of a maximal cyclotomic field*, Math. USSR Izvestija, **14**, (1979), 247-256.

[Bl98] E. Black, *Arithmetic lifting of dihedral extensions*, J. Algebra, **203**, (1998), 12–29.

[Bl99a] E. Black, *Deformation of dihedral 2-group extensions of fields*, Transactions A.M.S., **351/8**, (1999).

[Bl99b] E. Black, *On semidirect products and arithmetic lifting property*, J. London Math. Soc., **60/2**, (1999), 677–688.

[Bl00] E. Black, *Arithmetic lifting of wreath products*, à paraître dans Proc. Amer. Math. Soc.

[BoWew00] I. Bouw and S. Wewers, *Reduction of covers and Hurwitz spaces*, (preprint), (2000).

[Co99] J-L. Colliot-Thélène, *Points rationnels sur les variétés non de type général*, Cours spécialisé, IHP, Paris, (1999).

[Co00] J-L. Colliot-Thélène, *Rational connectedness and Galois covers of the projective line*, Ann. Math, **151**, (2000), 359–373.

[De95] P. Dèbes, *Covers of* $\mathbb{P}^1$ *over the* p*-adics*, in *Recent developments in the Inverse Galois Problem*, M. D. Fried ed., Contemp. Math., **186**, (1995), 217–238.

[De99a] P. Dèbes, *Arithmétique et espaces de modules de revêtements*, in *Number Theory in Progress*, Proceedings of the Number Theory conference in Zakopane, (K. Gyory, H. Iwaniec and J. Urbanowicz ed.), Walter de Gruyter, (1999), 75–102.

[De99b] P. Dèbes, *Some arithmetic properties of algebraic covers*, in *Aspects of Galois Theory*, London Math. Soc. Lecture Note Series, **256**, H. Völklein, P. Mueller, D. Harbater and J. G. Thompson ed., Cambridge University Press, (1999), 66–84.

[De99c] P. Dèbes, *Galois covers with prescribed fibers : the Beckmann-Black problem*, Ann. Scuola Norm. Sup. Pisa, Cl. Sci. (4), **28**, (1999), 273–286.

[De01a] P. Dèbes, *Méthodes topologiques et analytiques en théorie inverse de Galois — théorèmes d'existence de Riemann*, ce volume.

[De01b] P. Dèbes, *Descent theory for algebraic covers*, (preprint), (2000).

[DeDes97] P. Dèbes and B. Deschamps, *The Inverse Galois problem over large fields*, in *Geometric Galois Action*, London Math. Soc. Lecture Note Series, Cambridge University Press, **243**, (1997), 119–138.

[DeDo97] P. Dèbes and J-C. Douai, *Algebraic covers : field of moduli versus field of definition*, Ann. Sci. E.N.S., **30**, (1997), 303–338.

[DeDo98] P. Dèbes and J-C. Douai, *Local-global principles for algebraic covers*, Israel J. Math., **103**, (1998), 237–257.

[DeDo99] P. Dèbes and J-C. Douai, *Gerbes and Covers*, Comm. in Algebra, **27/2**, 577–594, (1999).

[DeDoEm00] P. Dèbes, J-C. Douai et M. Emsalem, *Familles de Hurwitz et cohomologie non abélienne*, Ann. Inst. Fourier, **50/1**, (2000), 1001–1037.

[DeDoMo00] P. Dèbes, J-C. Douai and L. Moret-Bailly, *Descent varieties for algebraic covers*, (preprint), (2000).

[DeFr94] P. Dèbes and M. Fried, *Non rigid situations in constructive Galois Theory*, Pacific J. Math., **163**, (1994), 81–122.

[DeHar98] P. Dèbes and D. Harbater, *Field of definition of* p*-adic covers*, J. fur die reine und angew. Math., **498**, (1998), 223–236.

[DelMu69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, I.H.E.S., Publ. mathématiques, **36**, (1969), 75–109

[Des95] B. Deschamps, *Existence de points* p*-adiques sur des espaces de Hurwitz pour tout* p, in *Recent developments in the Inverse Galois Problem*, Contemp. Math., **186**, (1995), 239–247.

[Em99] M. Emsalem, *On reduction of covers of arithmetic surfaces*, in *Applications of Curves over Finite Fields*, M. D. Fried ed., Contemp. Math., **245**, (1999), 117–132.

[Em01] M. Emsalem, *Sur les espaces de Hurwitz*, ce volume.

[Fr77] M. Fried, *Fields of definition of function fields and Hurwitz families, Groups as Galois groups,* Comm. in Alg., **1**, (1977), 17–82.

[FrHaVo93] M. Fried, D. Haran and H. Völklein, *Absolute Galois group of the totally real numbers*, C.R. Acad. Sc. Paris, Série I, **317**, (1993), 995–999.

[FrJa86] M. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, (1986).

[FrVo91] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann., **290**, (1991), 771-800.

[FrVo92] M. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Ann. Math., **135**, (1992), 469–481.

[Fu69] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Ann. Math., **90**, (1969), 542–575.

[Gi01] P. Gille, *R-équivalence sur les G-revêtements sur les corps locaux non archimédiens*, J. Number Theory, (à paraître).

[Gr60] A. Grothendieck, *Technique de descente et théorèmes d'existence en géométrie algébrique. 1. Descente par morphisme fidèlement plats*, Séminaire Bourbaki, (Déc. 1959), (1960).

[Gr71-SGA1] A. Grothendieck et al., *Revêtements étales et groupe fondamental*, (Séminaire de Géométrie algébrique (1960/61)), Lecture Notes in Math., **224**, (1971).

[HaJa98a] D. Haran and M. Jarden, *Regular split embedding problems over function fields of one variable over ample fields*, Forum math. **10**, (1998), 329–351.

[HaJa98b] D. Haran and M. Jarden, *Regular split embedding problems over complete valued fields*, Forum math. **10**, (1998), 329–351.

[HaJa00] D. Haran and M. Jarden, *Regular liftings of covers over ample fields*, preprint, (2000).

[HaVo96] D. Haran and H. Völklein, *Galois groups over complete valued fields.*, Israel J. Math., **93**, (1996), 9–27.

[Har84] D. Harbater, *Mock covers and Galois extensions*, J. Algebra, **91**, (1984), 281–293.

[Har87] D. Harbater, *Galois covering of the arithmetic line*, Lecture Notes in Math., **1240**, (1987), 165–195.

[Har94] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Invent. Math., **117**, (1994), 1–25

[Har95] D. Harbater, *Fundamental groups and embedding problems in characteristic p*, in *Recent developments in the Inverse Galois Problem*, M. D. Fried ed., Contemp. Math., **186**, (1995), 353–369

[HarSt99] D. Harbater and K. Stevenson, *Module and thickening problems*, J. Algebra, **212**, (1999), 272–304.

[HarvdP00] D. Harbater and M. van der Put, *Valued fields and covers in characteristic p*, (preprint), (2000).

[Ih90] Y. Ihara, *Braids, Galois groups and some arithmetic functions*, Proceedings of the ICM (Kyoto 1990), Springer-Verlag, (1991), 99–120

[Ko00] J. Kollár, *Fundamental groups of rationally connected varieties*, Michigan Math. J, **48**, (2000), 359–368.

[Ku70] W. Kuyk, *Extensions de corps hilbertiens*, J. Algebra, **14**, (1970), 112–124.

[La83] S. Lang, *Fundamentals of Diophantine Geometry*, Springer-Verlag, (1983).

[Le74] H.W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math., **25**, (1974), 299–325.

[Li95] Q. Liu, *Tout groupe fini est groupe de Galois sur* $\mathbb{Q}_p(T)$, in *Recent developments in the Inverse Galois Problem*, M. D. Fried ed., Contemp. Math., **186**, (1995), 261–265.

[Li01] Q. Liu, *Une mini-introduction à la géométrie analytique rigide*, ce volume.

[Lo01] P. Lochak, *Some elements of Grothendieck-Teichmüller theory*, (preprint).

[LoSc94] P. Lochak and L. Schneps, *The Grothendieck-Teichmüller group and automorphisms of braid groups*, in *The Grothendieck theory of Dessins d'Enfants*, L. Schneps ed., London Math. Soc. Lecture Note Series, Cambridge University Press, **200**, (1994), 323–358.

[MaMat99] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer-Verlag, (1999).

[Me90] J-F. Mestre, *Extensions régulières de* $\mathbb{Q}(T)$ *de groupe de Galois* $\widetilde{A}_n$, J. Algebra, **131**, (1990), 483–495.

[Mo00] L. Moret-Bailly, *Constructions de revêtements de courbes pointées*, J. Algebra, (to appear).

[Mo01] L. Moret-Bailly, *R-équivalence simultanée de torseurs : un complément à l'article de P. Gille*, (preprint).

[Po93] F. Pop, *The geometric case of a conjecture of Shafarevich —* $G_{\overline{\kappa}(t)}$ *is profinite free —*, Heidelberg-Mannheim Preprint Series "Arithmetik", Heft 8, (1993)

[Po94] F. Pop, *Half Riemann's existence theorem*, in *Algebra and Number Theory*, G. Frey and J. Ritter, eds, de Gruyter Proceedings in Mathematics, (1994)

[Po96] F. Pop, *Embedding problems over large fields*, Ann. Math., **144**, 1–35, (1996).

[Ra94] M. Raynaud, *Revêtement de la droite affine en caractéristique p et conjecture d'Abhyankar*, Invent. Math., **116**, (1994), 425–462

[Ra99] M. Raynaud, *Spécialisation des revêtements en caractéristique p*, Ann. Sci. E.N.S., **32**, (1999), 87–126.

[Sa82] D.J. Saltman, *Generic Galois extensions and problems in field theory*, Advances in Math., **43**, (1982), 250–283.

[Sa84] D.J. Saltman, *Noether's problem over an algebraically closed field*, Invent.Math., **77**, (1984), 71–84.

[Se73] J.-P. Serre, *Cohomologie Galoisienne*, LNM 5, Springer-Verlag, 4ème édition, (1973).

[Se92] J.-P. Serre, *Topics in Galois theory*, Jones and Bartlett Publ., Boston, (1992).

[Sh74] K-y. Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann, **207**, (1974), 99–120.

[Sh78] K-y. Shih, *p-division points on certain elliptic curves*, Comp. Math., **36**, (1978), 113–129.

[St96] K. Stevenson, *Galois groups of étale covers of projective curves in characteristic p*, J. Algebra, **182**, (1996), 770–804.

[St98] K. Stevenson, *Conditions related to* π_1 *of projective curves*, J. Number Theory, **69/1**, (1998), 62–79.

[Sw69] R. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math., **7**, (1969), 148–158.

[Vos70] V. E. Voskresenskiĭ, *On the question of the structure of the field of invariants of a cyclic group of automorphisms of the field* $\mathbb{Q}(x_1, \ldots, x_n)$, Izv. Akad. Nauk SSSR, **34**, (1970), 370–375 (= Math. USSR Izv., **4**, (1970), 371–380).

[Vos98] V. E. Voskresenskiĭ, *Algebraic groups and their birational invariants*, Translations of math. monographs, **179**, AMS, (1998)

[We56] A. Weil, *The field of definition of a variety*, *Œuvres complètes (Collected papers)* **II**, Springer-Verlag, 291–306.

P. Dèbes, Université de Lille I, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France
E-mail : Pierre.Debes@univ-lille1.fr