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 $G \subset \mathrm{GL}_d$) :