ISSN 0012-9593

quatrième série - tome 51 *fascicule 1* *janvier-février 2018*

ANNALES SCIENTIFIQUES de L'ÉCOLE NORMALE SUPÉRIEURE

Pierre DÈBES

Groups with no parametric Galois realizations

SOCIÉTÉ MATHÉMATIQUE DE FRANCE

Annales Scientifiques de l'École Normale Supérieure

Publiées avec le concours du Centre National de la Recherche Scientifique

Rédaction / *Editor*

Annales Scientifiques de l'École Normale Supérieure,
45, rue d'Ulm, 75230 Paris Cedex 05, France.
Tél. : (33) 1 44 32 20 88. Fax : (33) 1 44 32 20 80.
`annales@ens.fr`

Édition / *Publication*

Société Mathématique de France
Institut Henri Poincaré
11, rue Pierre et Marie Curie
75231 Paris Cedex 05
Tél. : (33) 01 44 27 67 99
Fax : (33) 01 40 46 90 96

Abonnements / *Subscriptions*

Maison de la SMF
Case 916 - Luminy
13288 Marseille Cedex 09
Fax : (33) 04 91 41 17 51
email : `smf@smf.univ-mrs.fr`

Tarifs

Europe : 540 €. Hors Europe : 595 € ($893). Vente au numéro : 77 €.

ISSN 0012-9593

Directeur de la publication : Stéphane Seuret
Périodicité : 6 nos / an

Ann. Scient. Éc. Norm. Sup.
4^{e} série, t. 51, 2018, p. 143 à 179

GROUPS WITH NO PARAMETRIC GALOIS REALIZATIONS

BY Pierre DÈBES

Abstract. – We disprove a strong form of the Regular Inverse Galois Problem: there exist finite groups G which do not have a $\mathbb{Q}(U)$-parametric extension, i.e., a regular realization $F/\mathbb{Q}(T)$ that induces all Galois extensions $L/\mathbb{Q}(U)$ of group G by specializing T to $f(U) \in \mathbb{Q}(U)$. A much weaker Lifting Property is even disproved for these groups: two realizations $L/\mathbb{Q}(U)$ exist that cannot be induced by realizations with the same ramification type. Our examples of such groups G include symmetric groups S_n, $n \geq 6$, infinitely many $\mathrm{PSL}_2(\mathbb{F}_p)$, the Monster.

Two variants of the question with $\mathbb{Q}(U)$ replaced by $\mathbb{C}(U)$ and $\mathbb{Q}$ are answered similarly, the second one under a diophantine "working hypothesis" going back to a problem of Fried-Schinzel.

We introduce two new tools: a comparison theorem between the invariants of an extension $F/\mathbb{C}(T)$ and those obtained by specializing T to $f(U) \in \mathbb{C}(U)$; and, given two regular Galois extensions of $k(T)$, a finite set of $k(U)$-curves that say whether these extensions have a common specialization E/k.

Résumé. – Nous réfutons une forme forte du problème inverse de Galois régulier: il existe des groupes finis G qui n'ont pas de réalisation régulière $F/\mathbb{Q}(T)$ induisant toutes les extensions galoisiennes $L/\mathbb{Q}(U)$ de groupe G par spécialisation de T en $f(U) \in \mathbb{Q}(U)$. Une propriété de relèvement bien plus faible est même infirmée pour ces groupes: deux réalisations $L/\mathbb{Q}(U)$ existent qui ne peuvent être induites par des réalisations ayant le même type de ramification. Nos exemples de tels groupes G incluent les groupes symétriques S_n, $n \geq 6$, une infinité de $\mathrm{PSL}_2(\mathbb{F}_p)$, le Monstre.

Deux variantes de la question, où $\mathbb{Q}(U)$ est remplacé par $\mathbb{C}(U)$ et $\mathbb{Q}$, ont une réponse similaire, la seconde sous une « hypothèse de travail » liée à un problème de Fried-Schinzel.

Nous introduisons deux nouveaux outils: un théorème de comparaison entre les invariants d'une extension $F/\mathbb{C}(T)$ et ceux de celle obtenue en spécialisant T en $f(U) \in \mathbb{C}(U)$; et, étant données deux extensions régulières galoisiennes de $k(T)$, un ensemble fini de $k(U)$-courbes qui disent si ces extensions ont une spécialisation commune E/k.

This work was supported in part by the Labex CEMPI (ANR-11-LABX-0007-01).

 doi:10.24033/asens.2353

1. Introduction

Given two fields $k \subset K$, a finite Galois extension $F/k(T)$ and a point $t_0 \in \mathbb{P}^1(K)$, there is a well-defined notion of *specialized extension* F_{t_0}/K (see *Basic terminology*). If F is the splitting field over $k(T)$ of a polynomial $P \in k[T,Y]$, monic in Y, irreducible in $\overline{k}[T,Y]$ and t_0 not a root of the discriminant $\Delta_P \in k[T]$ of P w.r.t Y, F_{t_0} is the splitting field over K of the polynomial $P(t_0, Y)$. We are mostly interested in the situations $K = k$ and $K = k(U)$ (with U a new indeterminate).

The specialization process has been much studied towards the *Hilbert irreducibility* issue of existence of specializations $t_0 \in k$ preserving the Galois group. Investigating the set, say $\mathcal{S}p_K(F/k(T))$, of all specialized extensions F_{t_0}/K with $t_0 \in \mathbb{P}^1(K)$ is a further goal. For $k = K = \mathbb{Q}$, [7] shows for example that the number of extensions $F_{t_0}/\mathbb{Q}$ of group $G = \mathrm{Gal}(F/\mathbb{Q}(T))$ and discriminant $|d_E| \leq y$ grows at least like a power of y, for some positive exponent, thereby proving for G the "lower bound part" of a conjecture of Malle.

Little was known on an even more fundamental question: whether $\mathcal{S}p_K(F/k(T))$ can contain all Galois extensions E/K of group contained in $G = \mathrm{Gal}(F/k(T))$; we then say that $F/k(T)$ is K-*parametric*, as for example $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$. Strikingly no group was known yet *not to have* a $\mathbb{Q}$-parametric or a $\mathbb{Q}(U)$-parametric extension $F/\mathbb{Q}(T)$ while only four: $\{1\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, S_3, are known to have one. No group with no $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$ was even known, while only a few more with one are: cyclic groups, dihedral groups D_{2n} with n odd.

1.1. Groups with no K-parametric extension $F/k(T)$

We produce many such groups:

(a) $k = \mathbb{C}$ *and* $K = \mathbb{C}(U)$*: non cyclic nilpotent groups* G *of odd order, symmetric and alternating groups* S_n *and* A_n *with* $n \geq 6$*, linear groups* $\mathrm{PSL}_2(\mathbb{F}_p)$ *with* $p > 7$ *prime, all sporadic groups, etc.*

(b) $k = \mathbb{Q}$ *and* $K = \mathbb{Q}(U)$*: the same* S_n *and* A_n *except* A_6*, the* $\mathrm{PSL}_2(\mathbb{F}_p)$ *with* $(\frac{2}{p}) = (\frac{3}{p}) = -1$*, the Monster* M*, etc.*

(c) $k = K = \mathbb{Q}$*: the same last groups, under some "working hypothesis".*

We say more about the "working hypothesis" in §1.4 below and full statements are in § 2.3-2.4.

Remark (parametric *vs.* generic). – Consequently the groups from §1.1 (a) do not have a *generic* extension $F/\mathbb{C}(T)$; generic is indeed a stronger notion meaning "L-parametric for all fields $L \supset \mathbb{C}$". This was known by a result of Buhler-Reichstein [2]: the only groups to have a generic extension $F/\mathbb{C}(T)$ are the cyclic groups and the dihedral groups D_{2n} with n odd. Our non $\mathbb{C}(U)$-parametric conclusion however is stronger: the extensions to be parametrized in the generic context include all Galois extensions E/L of group G with L *any field containing* $\mathbb{C}$ and it follows that G should then be a subgroup of $\mathrm{PGL}_2(\mathbb{C})$ [18, prop.8.14]. This reduction cannot be used if $F/\mathbb{C}(T)$ only parametrizes extensions of $L = \mathbb{C}(U)$. There exist in fact groups that have a $\mathbb{C}(U)$-parametric extension but no generic extension $F/\mathbb{C}(T)$ (Corollary 2.5).

Our first conclusions fit in the framework of Inverse Galois Theory. A prominent open problem is the *Regular Inverse Galois Problem*: is every finite group the Galois group of some extension $F/\mathbb{Q}(T)$, Galois and $\mathbb{Q}$-*regular* (i.e., $F \cap \overline{\mathbb{Q}} = \mathbb{Q}$)? Possessing a $\mathbb{Q}(U)$-parametric extension $F/\mathbb{Q}(T)$ is for a group G a strong variant. Our results show that this strong variant fails and conditionally so does the weaker $\mathbb{Q}$-parametric analog. This sets welcome boundaries for inverse Galois theory over $\mathbb{Q}$, a topic where few general statements were available. Narrowing these boundaries further, e.g., removing "conditionally" in the version over $\mathbb{Q}$, still remains desirable. We note this weaker but unconditional result [(1)] of Legrand [23]: every non trivial group that has at least one $\mathbb{Q}$-regular realization $F/\mathbb{Q}(T)$ has one that is not $\mathbb{Q}$-parametric [(2)].

1.2. Non parametric ramification type & the Lifting Property

Our main result is in fact stronger than §1.1. Assume that G is a group as in list (a) above if $k = \mathbb{C}$, or, as in list (b) if $k \subset \mathbb{C}$. Then not only G does not have a $k(U)$-parametric extension $F/k(T)$ but *it does not even have a* $k(U)$*-parametric ramification type* $(r, \mathbf{C})$. By this we mean that if $r \geq 2$ is any integer and $\mathbf{C} = (C_1, \dots, C_r)$ any r-tuple of nontrivial conjugacy classes of G, the k-regular Galois extensions $F/k(T)$ with group G, r branch points and inertia classes $C_1, \dots, C_r$ are not enough to obtain all regular Galois extensions $L/k(U)$ of group G by specialization of T in $k(U)$. Thus in the chain of implications:

G has a $k(U)$-parametric extension $F/k(T)$

$\Rightarrow$ G has a $k(U)$-parametric ramification type

$\Rightarrow$ G is a regular Galois group over k,

not only the first condition fails, but also the second one.

Our most precise results (corollaries 2.12 and 2.15) say even more, and are more informative, in that they show better the obstruction to having $k(U)$-parametrizations, which is not the absence of regular realizations $F/k(T)$ but the existence of several that cannot be obtained by specialization from some with the same ramification type:

(*) *For a group G as above, excluding $G = A_n$ if $k \neq \mathbb{C}$* [(3)]*, there exist two regular Galois extensions $L_1/k(U)$, $L_2/k(U)$ of group G such that $L_1\mathbb{C}/\mathbb{C}(U)$ and $L_2\mathbb{C}/\mathbb{C}(U)$ are not $\mathbb{C}(U)$-specializations of regular Galois extensions of $k(T)$ of group G with the same ramification type.*

We view indistinctly a k-regular extension $F/k(T)$ as the corresponding k-cover of the line $X \to \mathbb{P}^1_k$. In these more geometrical terms, $k(U)$-specializations interpret as pull-backs along genus 0 covers $\mathbb{P}^1_k \to \mathbb{P}^1_k$. Statement (*) shows that the following *Lifting Property*:

($\mathrm{LP}_N(G)$) *any N k-G-Galois covers $g_1, \dots g_N$ of $\mathbb{P}^1_k$ of group G can be, after scalar extension to $\mathbb{C}$, obtained by pull-back along genus 0 covers $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ from k-G-Galois covers $f_1, \dots, f_N$ of $\mathbb{P}^1_k$ with group G and the same ramification type,*

(1) Remark 2.19 explains how Legrand's result can be deduced from ours under our working hypothesis.
(2) Legrand has also just told me about a promising joint work with Koenig which could lead to unconditional existence of groups with no $\mathbb{Q}$-parametric extension $F/\mathbb{Q}(T)$.
(3) For $G = A_n$ and $k \neq \mathbb{C}$, the two extensions $L_1/k(U)$ and $L_2/k(U)$ from (*) should be replaced by three.