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 : 519 €. Hors Europe : 548 €. 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).

0012-9593/01/© 2018 Société Mathématique de France. Tous droits réservés doi:10.24033/asens.2352

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.

which is weaker than the middle condition in the above chain of implications, already fails for $N = 2$. The variant of $(\mathrm{LP}_N(G))$ requiring further $f_1 = \cdots = f_N$ is stronger, so fails too. This is interesting as this variant is close to another Arithmetic Lifting Property, for the field $\mathbb{C}(U)$ [(4)] and that only two counter-examples to this property are known, due to Colliot-Thélène [4], for $\mathbb{Z}/8\mathbb{Z}$ over some number field and for some p-group over some "ample field".

1.3. Comparison result and pre-order for extensions of $\mathbb{C}(T)$

We will first focus on the situation $K = k(U)$ with $k \subset \mathbb{C}$. Results mentioned above follow from a general criterion (criterion 2.9) for some set of k-regular Galois extensions $L/k(U)$ of group G not to be $k(U)$-specializations of k-regular Galois extensions $F/k(T)$ of group G and given ramification type $(r, \mathbf{C})$. A main point is that

(*) *the branch point number of an extension* [(5)] $F/\mathbb{C}(T)$ *cannot drop under specialization of* T *in* $\mathbb{C}(U) \setminus \mathbb{C}$, *unless* $F/\mathbb{C}(T)$ *is one from a list of exceptional extensions with* F *of genus* 0 (see Theorem 2.1 (a)).

Despite its basic nature, this did not seem to be known; the difficulty is that the group may drop and that the ramification of the specialization point $T_0 \in \mathbb{C}(U)$ may cancel some of the ramification of $F/\mathbb{C}(T)$ [(6)]. We prove a more precise version (Theorem 3.1) giving better estimates of the branch point number and other invariants of specialized extensions $F_{T_0}/\mathbb{C}(U)$ which could be interesting beyond this paper.

The situation $K = \mathbb{C}(U)$ has another interesting feature: specialized extensions $F_{T_0}/\mathbb{C}(U)$ with $T_0 \in \mathbb{C}(U)$ remain extensions of the rational function field in one indeterminate, as the initial extension $F/\mathbb{C}(T)$; in other words, pull-backs of a cover of $\mathbb{P}^1_{\mathbb{C}}$ along covers $\mathbb{P}^1_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ still are covers of $\mathbb{P}^1_{\mathbb{C}}$. The specialization process induces a (partial) pre-order on the set of Galois extensions $L/\mathbb{C}(T)$. We will show that this is in fact an order on a big subset (see Theorem 2.1 (b)), with this consequence:

(*) *for "most" groups* G (*e.g., all groups of rank* $\geq$ 4), *there is at most one* $\mathbb{C}(U)$*-parametric extension* $F/\mathbb{C}(T)$ *of group* G.

The pre-order that we use to investigate the minimal elements raises further questions about the ordered structure of Galois extensions of $\mathbb{C}(T)$ that are certainly worthwhile being studied.

[(4)] In the Arithmetic Lifting Property for $\mathbb{C}(U)$, the lifting covers $f_1, \dots, f_N$ from $(\mathrm{LP}_N(G))$ are replaced by *one* cover, of $\mathbb{P}^1_{\mathbb{C}(U)}$, instead of $\mathbb{P}^1_{\mathbb{C}}$. Disproving it would consist in showing the variant of (*) from §1.2 above concluding that $L_1\mathbb{C}/\mathbb{C}(U)$ and $L_2\mathbb{C}/\mathbb{C}(U)$ are not $\mathbb{C}(U)$-specializations of *any one* $\mathbb{C}(U)$*-regular Galois extension* $\mathcal{F}/\mathbb{C}(U)(T)$ *of group* G (and not just of anyone coming from an extension $F/\mathbb{C}(T)$). Footnote 6 explains however that a main point of our approach, statement (*) from 1.3 below, does not extend to these general $\mathbb{C}(U)$-extensions $\mathcal{F}/\mathbb{C}(U)(T)$.

[(5)] The extension $F/\mathbb{C}(T)$ need not be assumed to be Galois in this statement.

[(6)] Statement (*) in fact becomes false for general $\mathbb{C}(U)$-extensions $\mathcal{F}/\mathbb{C}(U)(T)$ (not just those coming from extensions $F/\mathbb{C}(T)$). Take $\mathcal{F} = \mathbb{C}(U)(\sqrt{H(U,T)})$ with

$$H(U,T) = T(T - (U^2 - (U - a_1)^2)) \cdots (T - (U^2 - (U - a_s)^2))(T - 1)$$

and $a_1, \dots a_s \in \mathbb{C} \setminus \{0\}$ pairwise distinct. The extension $\mathcal{F}/\mathbb{C}(U)(T)$ has $s + 2$ branch points but for $T_0(U) = U^2$, we have $H(U, T_0(U)) = U^2(U - a_1)^2 \cdots (U - a_s)^2(U^2 - 1)$ and the extension $\mathcal{F}_{T_0}/\mathbb{C}(U)$ has only 2 branch points.

1.4. The twisted polynomial

Our results in the situation that $k = K$ is a number field will be obtained from those with $K = k(U)$ by specialization, but of the indeterminate U this time. To this end we will generalize a tool introduced in [7] as the "self-twisted cover". Theorem 2.16, the concrete statement around this specialization approach, is interesting for its own sake: given two k-regular Galois extensions $F/k(T)$, $L/k(T)$ of group G, it provides a finite list of families of covers $\widetilde{X}_U \to \mathbb{P}^1_{k(U)}$ parametrized by $U \in \mathbb{P}^1$ which have the answer to the question of whether $F/k(T)$ and $L/k(T)$ have a common specialization:

(*) *for all but finitely many $u_0 \in k$ and all $t_0 \in k$ not a branch point of $F/k(T)$, we have $L_{u_0}/k = F_{t_0}/k$ if and only if for at least one family $\widetilde{X}_U$, the u_0-curve $\widetilde{X}_{u_0}$ has an unramified k-rational point above t_0,*

and a similar statement holds with u_0 the generic point U of $\mathbb{P}^1_U$.

The working hypothesis alluded to in §1.1 is stated in § 2.4.2: it connects the absence of $k(U)$-rational points on each of the curves $\widetilde{X}_U$ with the absence, for infinitely many $u_0 \in k$, of k-rational points on each of the curves $\widetilde{X}_{u_0}$. It relates to some diophantine problem of Fried-Schinzel and somehow extends Hilbert's Irreducibility Theorem. It has no known counter-example.

Acknowledgments. – I wish to express special thanks to the anonymous referee for his/her valuable suggestions and notably for his/her remark that the original results about $\mathbb{C}(U)$-parametric extensions could be extended with no extra work to results about $\mathbb{C}(U)$-parametric ramification types. I also wish to thank Lior Bary-Soroker, Joachim Koenig, François Legrand, Razvan Litcanu and Danny Neftin for many interesting and helpful discussions about this work.

The paper is organized as follows. § 2 presents in full detail the results of our paper. We reduce their proofs to that of three main statements: the comparison Theorem 2.1, the twisting Theorem 2.16 and the genus zero Proposition 2.4. We state them and explain their implications. Their proofs, which are independent, are given in § 3 and § 4. Finally § 5 is an appendix which collects a few classical results that enter in our proofs and that we have rephrased to fit our field arithmetic set-up; § 5 is used in § 3 and in § 4. We start below with some basic terminology.

Basic terminology. – (For more details, see [8] or [10].)

The base field k is always assumed to be of characteristic 0. Is also fixed a big algebraically closed field containing the complex field $\mathbb{C}$ and the indeterminates that will be used and in which all field compositum should be understood.

Given a field k, an extension $F/k(T)$ is said to be *k-regular* if $F \cap \overline{k} = k$. We make no distinction between a k-regular extension $F/k(T)$ and the associated k-regular cover $f : X \to \mathbb{P}^1$: f is the normalization of $\mathbb{P}^1_k$ in F and F is the function field $k(X)$ of X. The "field extension" viewpoint is mostly used in this paper.

We also use *affine equations*: we mean the irreducible polynomial $P \in k[T, Y]$ of a primitive element of $F/k(T)$, integral over $k[T]$.

By *group* and *branch point set* of a k-regular extension $F/k(T)$, we mean those of the extension $F\overline{k}/\overline{k}(T)$: the group of $F\overline{k}/\overline{k}(T)$ is the Galois group of its Galois closure. The branch point set of $F\overline{k}/\overline{k}(T)$ is the (finite) set of points $t \in \mathbb{P}^1(\overline{k})$ such that the associated discrete valuations are ramified in $F/\overline{k}(T)$.

The field k being of characteristic 0, we also have the *inertia canonical invariant* $\mathbf{C}$ of the k-regular extension $F/k(T)$, defined as follows. If $\mathbf{t} = \{t_1, \dots, t_r\}$ is the branch point set of f, then $\mathbf{C}$ is a r-tuple $(C_1, \dots, C_r)$ of conjugacy classes of the group G of f: for $i = 1, \dots, r$, C_i is the conjugacy class of the distinguished [7] generators of the inertia groups $I_{\mathfrak{P}}$ above t_i in the Galois closure $\widehat{F}/k(T)$ of $F/k(T)$. The couple $(r, \mathbf{C})$ is called the *ramification type* of $F/k(T)$. More generally, given a finite group G, we say that a couple $(r, \mathbf{C})$ is *a ramification type* for G over k if it is the ramification type of at least one k-regular Galois extension $F/k(T)$.

We also use the notation $\mathbf{e} = (e_1, \dots, r_r)$ for the r-tuple with ith entry the ramification index $e_i = |I_{\mathfrak{P}}|$ of primes above t_i; e_i is also the order of elements of C_i, $i = 1, \dots, r$.

We say that two k-regular extensions $F/k(T)$ and $L/k(T)$ are *isomorphic* if there is a field isomorphism $F \to L$ that restricts to an automorphism $\chi : k(T) \to k(T)$ equal to the identity on k and that they are *$k(T)$-isomorphic* if in addition χ is the identity on $k(T)$.

Given a Galois extension $F/k(T)$ and $t_0 \in \mathbb{P}^1(k)$, the *specialized extension F_{t_0}/k of $F/k(T)$ at t_0* is the Galois extension defined as follows. Consider the localized ring $A_{t_0} = k[T]_{\langle T - t_0 \rangle}$ of $k[T]$ at t_0, the integral closure B_{t_0} of A_{t_0} in F. Then F_{t_0}/k the residue extension of an arbitrary prime ideal of B_{t_0} above $\langle T - t_0 \rangle$. (As usual use the local ring $k[1/T]_{\langle 1/T \rangle}$ and its ideal $\langle 1/T \rangle$ if $t_0 = \infty$).

If $P \in k[T, Y]$ is an affine equation of $F/k(T)$ and $\Delta_P \in k[T]$ is its discriminant w.r.t. Y, then for every $t_0 \in k$ such that $\Delta_P(t_0) \neq 0$, t_0 is not a branch point of $F/k(T)$ and the specialized extension F_{t_0}/k is the splitting field over k of $P(t_0, Y)$.

If K is a field containing k and $t_0 \in \mathbb{P}^1(K)$, the *specialized extension F_{t_0}/K of $F/k(T)$ at t_0* is the extension $(FK)_{t_0}/K$. If $K = k(U)$, $T_0 \in K(U)$ is a non-constant rational function [8] and $P \in K[T, Y]$ is an affine equation of $F/K(T)$, then $\Delta_P(T_0) \neq 0$ and so $P(T_0(U), Y)$ is an affine equation of the specialized extension $F_{T_0}/K(U)$.

If the extension $F/k(T)$ is not Galois, the above definition leads to several specializations F_{t_0}/k: the prime ideals of B_{t_0} above $\langle T - t_0 \rangle$ are not conjugate in general. When we use this extended definition (only once in Theorem 3.1 (a)), we will talk about *a* specialization instead of *the* specialization F_{t_0}/k.

Recall the *Riemann Existence Theorem* (RET), a fundamental tool of the paper and of the surrounding theory of covers of $\mathbb{P}^1$ (viewed here as field extensions of $\mathbb{C}(T)$): it allows turning questions about covers into combinatorics and group theory considerations.

RIEMANN EXISTENCE THEOREM. – *Given a group G, an integer $r \geq 2$, a subset $\mathbf{t} \subset \mathbb{P}^1(\overline{k})$ of r points and an r-tuple $\mathbf{C} = (C_1, \dots, C_r)$ of nontrivial conjugacy classes of G, there is a Galois extension $F/\overline{k}(T)$ of group G, branch point set $\mathbf{t}$ and inertia canonical invariant $\mathbf{C}$ iff there exists $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \dots, g_r \rangle = G$. Furthermore the number of such extensions $F/\overline{k}(T)$ (in a fixed algebraic closure $\overline{k(T)}$) equals*

[7] "distinguished" means that these generators correspond to the e_ith root $e^{2i\pi/e_i}$ of 1 in the canonical isomorphism $I_{\mathfrak{P}} \to \mu_{e_i} = \langle e^{2i\pi/e_i} \rangle$.

[8] We use a capital letter for the specialization point T_0 to stress that it is a function $T_0(U)$ contrary to the situation for which it is a point in the ground field and the notation t_0 is preferred.

the number of r-tuples $(g_1, \dots, g_r)$ as above, counted modulo component-wise conjugation by an element of G.

The RET shows that a couple $(r, \mathbf{C})$ is a ramification type for G over $\overline{k}$ if the set, traditionally called the *Nielsen class*, of all $(g_1, \dots, g_r) \in C_1 \times \cdots \times C_r$ such that $g_1 \cdots g_r = 1$ and $\langle g_1, \dots, g_r \rangle = G$ is nonempty.

We will notably use the RET to construct Galois extensions of given group G and with an inertia canonical invariant $\mathbf{C}$ only formed with some given conjugacy classes $C_1, \dots, C_N$ of G, possibly repeated. This is possible if the union $\bigcup_{i=1}^N C_N$ contains a generating set $\{g_1, \dots, g_t\}$ of G.

This generating assumption on the set $\{C_1, \dots, C_N\}$ is satisfied in the following situations: (a) $C_1, \dots, C_N$ are the respective classes of elements $g_1, \dots, g_N$ forming a generating set for G ; (b) $C_1, \dots, C_N$ are all non-trivial conjugacy classes of G (any N-tuple $(g_1, \dots, g_N)$ with $g_i \in C_i$, $i = 1, \dots, N$, is a generating set thanks to a classical lemma of Jordan [19]); (c) G is a simple group and $C_1, \dots, C_N$ consist of a single non-trivial conjugacy class of G. Situations (a) and (b) will be used in Corollary 2.10 and (c) is alluded to around Problem 2.14.

2. Main results

We present our main results: the specialization process and the associated order in the situation $k = \mathbb{C}$ and $K = \mathbb{C}(U)$ (§ 2.1), some new examples of groups with a $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$ (§ 2.2), a method to produce groups with no $k(U)$-parametric ramification type (§ 2.3), our "twisted polynomial" $\widetilde{P}_F^L(U, T, Y)$ and its use towards the construction of groups with no k-parametric extension $F/k(T)$ (§ 2.4).

2.1. $\mathbb{C}(U)$-specializations of Galois extensions $F/\mathbb{C}(T)$

This subsection gives the main definitions and our first main tool (Theorem 2.1).

2.1.1. *Comparison theorem.* – Given an extension $F/\mathbb{C}(T)$, we use the following notation for its *invariants*: G_F for the group, r_F for the branch point number, $\mathbf{C}_F$ for the inertia canonical invariant, g_F for the genus of F; they are invariant inside the isomorphism class of $F/\mathbb{C}(T)$.

Given two Galois extensions $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$, we write

$$F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$$

if $L/\mathbb{C}(U)$ is the specialized extension $F_{T_0}/\mathbb{C}(U)$ of $F/\mathbb{C}(T)$ at some non-constant rational function $T_0 \in \mathbb{C}(U)$.

For a conjugacy class C of a group G, set $C^{\mathbb{Z}} = \bigcup_{\alpha \in \mathbb{Z}} C^\alpha$. This *powered conjugacy class* $C^{\mathbb{Z}}$ is also the conjugacy class of the cyclic subgroup generated by any element of C.

Given tuples $\mathbf{C} = (C_1, \dots, C_r)$ and $\mathbf{C}' = (C'_1, \dots, C'_{r'})$ of conjugacy classes of G and G', write $\mathbf{C} \prec \mathbf{C}'$ if for every $j \in \{1, \dots, r'\}$, there exists $i \in \{1, \dots, r\}$ such that $C'_j \subset C_i^{\mathbb{Z}}$.

THEOREM 2.1. – (a) *Let $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$ be two finite Galois extensions. Assume $g_F \geq 1$. Then we have:*

$$F/\mathbb{C}(T) \prec L/\mathbb{C}(T) \Rightarrow (G_F, r_F, \mathbf{C}_F) \prec (G_L, r_L, \mathbf{C}_L)$$

where the right-hand side condition means that $G_F \supset G_L$, $r_F \leq r_L$ and $\mathbf{C}_F \prec \mathbf{C}_L$. If in addition $G_F = G_L$, the implication also holds if $g_F = 0$; and we have $g_F \leq g_L$ if $r_F \geq 4$.

As recalled in § 3.3, the excluded case $g_F = 0$ is known to only happen when $r_F \leq 3$ and G_F is a subgroup of $\mathrm{PGL}_2(\mathbb{C})$, i.e., one of these groups: $\mathbb{Z}/n\mathbb{Z}$ ($n \geq 1$), $(\mathbb{Z}/2\mathbb{Z})^2$, A_4, S_4, A_5, D_{2n} ($n \geq 3$). For each such group G_F, there is, up to isomorphism, only one Galois extension $F/\mathbb{C}(T)$ of group G_F and genus $g_F = 0$.

Theorem 2.1 will be deduced from Theorem 3.1 which offers more precise estimates, for example, the lower bound

$$(*) \qquad r_L \geq (N-4)r_F + 4$$

if $L/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$ with $T_0 \in \mathbb{C}(T)$ of degree N.

2.1.2. *The order $\prec$.* – These estimates will further show that, as stated below, the pre-order $\prec$ is antisymmetric on a big subset of all Galois extensions, regarded modulo isomorphisms.

Specifically, denote by $\mathcal{G}^*$ the set of groups that are

(*) (*of rank* ≥ 4) or (*or rank* 3 *and odd order*) or (*of rank* 2 *and order not divisible by* 2 *or* 3) or (*a subgroup of* $\mathrm{PGL}_2(\mathbb{C})$)

and by $\mathcal{E}^*$ the set of all Galois extensions $F/\mathbb{C}(T)$, viewed up to isomorphism such that $(G_F \in \mathcal{G}^*, G_F \not\subset \mathrm{PGL}_2(\mathbb{C}))$ *or* $(g_F = 0)$.

The notion of "parametric extensions" appearing below was introduced in § 1; the definition is recalled right next in § 2.1.3.

THEOREM 2.1. – (b) *The relation $\prec$ induces a* (*partial*) *order on $\mathcal{E}^*$. Consequently, for every group $G \in \mathcal{G}^*$, there is at most one Galois extension $F/\mathbb{C}(T)$ of group G that is $\mathbb{C}(U)$-parametric.*

The uniqueness part follows from the first part (and Remark 3.5, when $G_F \subset \mathrm{PGL}_2(\mathbb{C})$): the main point is that if an extension $F/\mathbb{C}(T)$ is $\mathbb{C}(U)$-parametric of group $G \in \mathcal{G}^*$, it is *the* smallest (for $\prec$) Galois extension $L/\mathbb{C}(T)$ of group G.[9]

We have no example of two non-isomorphic Galois extensions $F/\mathbb{C}(T)$ and $L/\mathbb{C}(T)$ such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$ and $L/\mathbb{C}(T) \prec F/\mathbb{C}(T)$, and in particular, no example of a group G that has two non-isomorphic $\mathbb{C}(U)$-parametric extensions $F/\mathbb{C}(T)$. In fact the groups that are known to have at least one $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$ are the finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$, and for them, uniqueness is part ot Theorem 2.1 (for the existence, see Corollary 2.5).

The proofs of the two parts of Theorem 2.1 are given in § 3.2 and § 3.4.

[9] For a Galois extension $L/\mathbb{C}(T)$ of group G, there is a Galois extension $F/\mathbb{C}(T)$ such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$ and $F/\mathbb{C}(T)$ is minimal (for $\prec$) among all Galois extensions of $\mathbb{C}(T)$ of group G, but several such extensions $F/\mathbb{C}(T)$ exist in general.

2.1.3. *Parametricity*. – Next definition extends the notion of parametric extension introduced by Legrand [20], [22], [21].

Definition 2.2. – Given a nonempty set H of k-regular Galois extensions $F/k(T)$ of group G and a nonempty set $\mathscr{R}$ of Galois extensions F/k of group contained in G, H is said to *k-specialize to all extensions in $\mathscr{R}$* if

(*) for every extension $L/k \in \mathscr{R}$, there exist $F/k(T) \in \mathsf{H}$ and $t_0 \in \mathbb{P}^1(k)$, not a branch point of $F/k(T)$, such that the specialized extension F_{t_0}/k is k-isomorphic to E/k.

The set H is said to be *k-parametric* if (*) holds with $\mathscr{R}$ the set of all Galois extensions L/k of group contained in G. Given a field $K \supset k$, H is said to be *K-parametric* if the set $\mathsf{H}_K = \{FK/K(T) | F/k(T) \in \mathsf{H}\}$ is K-parametric.

We have two typical situations in mind:

(a) $\mathsf{H} = \{F/k(T)\}$ consists of a single k-regular Galois extension. When H is K-parametric (for a field $K \supset k$), we say that *the extension $F/k(T)$ is K-parametric* and that G *has a K-parametric extension* $F/k(T)$. These definitions corresponds to those of Legrand.

The extension $\mathbb{Q}(\sqrt{T})/\mathbb{Q}(T)$ is the standard example of a K-parametric extension $F/\mathbb{Q}(T)$; it is for all fields $K \supset \mathbb{Q}$ and so is in fact *generic*. Recall that "generic" for a finite k-regular Galois extension $F/k(T)$ means "K-parametric for all fields $K \supset k$". See [18] for more on generic extensions and polynomials.

(b) Given a ramification type $(r, \mathbf{C})$ (for G over k), take $\mathsf{H} = \mathsf{H}_{r,G}(\mathbf{C})_k$ to be the set of all k-regular Galois extensions $F/k(T)$ with group G and ramification type $(r, \mathbf{C})$. This is also the set of k-points on the Hurwitz stack associated with $(r, \mathbf{C})$. When $\mathsf{H}_{r,G}(\mathbf{C})_k$ is K-parametric, we say that *the ramification type* $(r, \mathbf{C})$ *is K-parametric* and that G *has a K-parametric ramification type*.

Remark 2.3 (Transfer properties). – (a) *If a set* H *of k-regular Galois extensions $F/k(T)$ is $k(U)$-parametric, then it is k-parametric.*

Proof. – Let H be as above and E/k be a Galois extension of group $H \subset G$. As H is $k(U)$-parametric, there exist $F/k(T) \in \mathsf{H}$ and $T_0 \in k(U)$ such that the specialized extension $F_{T_0}/k(U)$ is $k(U)$-isomorphic to $E(U)/k(U)$. Hence for all but finitely many $u_0 \in \mathbb{P}^1(k)$, the extension, $(F_{T_0})_{u_0}/k$, obtained by specializing $F_{T_0}/k(U)$ at u_0 is E/k. The conclusion follows since, as explained below, for all but finitely many $u_0 \in \mathbb{P}^1(k)$, $(F_{T_0})_{u_0}/k$ is also the specialized extension $F_{T_0(u_0)}/k$.

This is clear if $T_0 \in k$. Assume $T_0 \notin k$ and let $P \in k[T, Y]$ be an affine equation of $F/k(T)$. Then F_{T_0} is the splitting field over $k(U)$ of $P(T_0(U), Y)$ and, as $F/k(T)$ is Galois, it is also the splitting field of any irreducible factor $Q \in k[U, Y]$ of $P(T_0(U), Y)$. Thus such a Q is an affine equation of the Galois extension $F_{T_0}/k(U)$. For all but finitely many $u_0 \in \mathbb{P}^1(k)$, the extension $(F_{T_0})_{u_0}/k$ is the splitting field over k of $Q(u_0, Y)$ and also of $P(T_0(u_0), Y)$. This concludes the argument as for all but finitely many $u_0 \in \mathbb{P}^1(k)$, $F_{T_0(u_0)}/k$ is also the splitting field over k of $P(T_0(u_0), Y)$. □

This argument applies inductively to show that condition "H is $k(U_1, \dots, U_s)$-parametric" is stronger and stronger as s gets bigger; it remains however always weaker than "generic".
(b) On the other hand, for the same set H of k-regular Galois extensions $F/k(T)$ and an algebraic extension E/K with $K \supset k$, the connection between "E-parametric" and "K-parametric" is not so clear. As we will see, our criterion to produce non $k(U)$-parametric sets of extensions is all the more efficient that there are more $k(U)$-regular realizations of the group G in question, and so will be more fruitful when k is algebraically closed. We however do not have any proof of any implication.

2.2. Groups with a $k(U)$-parametric extension $F/k(T)$

We will deduce such groups from the following statement (one of our three main statements with Theorems 2.1 and 2.16). It is proved in § 4.2.1.

PROPOSITION 2.4 (genus 0). – *If $F/\mathbb{C}(T)$ is a Galois extension of group G with F of genus* 0*, then $F/\mathbb{C}(T)$ is $\mathbb{C}(U)$-parametric.*

COROLLARY 2.5. – *All subgroups of* $\mathrm{PGL}_2(\mathbb{C})$*:*

$$\mathbb{Z}/n\mathbb{Z}\ (n \geq 1), \quad (\mathbb{Z}/2\mathbb{Z})^2, \quad A_4, \quad S_4, \quad A_5, \quad D_{2n}\ (n \geq 3)$$

have a $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$, with $g_F = 0$. Out of them, $\mathbb{Z}/n\mathbb{Z}$ with $n = 1, 2, 3$ and $D_6 = S_3$ have a $k(U)$-parametric extension for every field k of characteristic 0*.*

Theorem 2.1 (b) shows further that the $\mathbb{C}(U)$-parametric extension claimed to exist is unique up to isomorphism.

Whether other groups than the subgroups of $\mathrm{PGL}_2(\mathbb{C})$ have a $\mathbb{C}(U)$-parametric extension is not known.

Proof of Corollary 2.5. – Subgroups of $\mathrm{PGL}_2(\mathbb{C})$ have a classical realization $F/\mathbb{C}(T)$ with $g_F = 0$. Such an extension $F/\mathbb{C}(T)$ is automatically $\mathbb{C}(U)$-parametric from Proposition 2.4. As to the second part of Corollary 2.5 we note that the groups $\mathbb{Z}/n\mathbb{Z}$ with $n = 1, 2, 3$ and $D_6 = S_3$ are known to have a generic extension $F/\mathbb{Q}(T)$ [18]. □

Clearly if a k-regular Galois extension $F/k(T)$ is K-parametric, then so is its ramification type $(r, \mathbf{C})$. So the ramification types of the extensions $F/\mathbb{C}(T)$ from Corollary 2.5 are $\mathbb{C}(U)$-parametric. It would be interesting to provide other examples of parametric ramification types.

REMARK 2.6 (Parametricity and genericity). – Cyclic groups and dihedral groups D_{2n} with n odd were known to have a $\mathbb{C}(U)$-parametric extension as they have a generic extension $F/\mathbb{C}(T)$: for $\mathbb{Z}/d\mathbb{Z}$, take $F = \mathbb{C}(T^{1/d})/\mathbb{C}(T)$ $(d \geq 1)$; for D_{2n}, it is a result of Hashimoto-Miyake [17] (see also [18, Theorem 5.5.4]). These groups are the only ones to have a generic extension $F/\mathbb{C}(T)$ [2]. The other subgroups of $\mathrm{PGL}_2(\mathbb{C})$: $(\mathbb{Z}/2\mathbb{Z})^2$, A_4, S_4, A_5, D_{2n} with n even, have a $\mathbb{C}(U)$-parametric extension but no generic extension $F/\mathbb{C}(T)$. Whether subgroups of $\mathrm{PGL}_2(\mathbb{C})$ other than $\mathbb{Z}/n\mathbb{Z}$ with $n = 1, 2, 3$ and S_3 have a $\mathbb{Q}(U)$-parametric extension $F/\mathbb{Q}(T)$ is unclear. [10]

[10] Even if for some of these groups ($(\mathbb{Z}/2\mathbb{Z})^2$, S_4, D_{2n} with n even), the unique $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$ is defined over $\mathbb{Q}$ (§ 3.3), a $\mathbb{Q}$-model $F_0/\mathbb{Q}(T)$ is not guaranteed to be $\mathbb{Q}(U)$-parametric: although any

2.3. Groups with no $k(U)$-parametric ramification type

We explain how we use Theorem 2.1 to produce groups with no $k(U)$-parametric ramification type $(r, \mathbf{C})$, with k algebraically closed in § 2.3.2 and k non algebraically closed in § 2.3.3. We start with a general criterion in § 2.3.1. Assume $k \subset \mathbb{C}$; there is no loss of generality.

Our method leads to a better conclusion than "no $k(U)$-parametric ramification type". To this end we introduce this definition:

Definition 2.7. – Given nonempty sets H and $\mathscr{R}$ of k-regular Galois extensions of group G [11], the set H is said to *weakly $k(U)$-specialize to all extensions in* $\mathscr{R}$ if

(*) for every extension $L/k(U) \in \mathscr{R}$, there exist $F/k(T) \in \mathsf{H}$ and $T_0 \in \mathbb{P}^1(\mathbb{C}(U))$ such that the specialized extension $F_{T_0}/\mathbb{C}(U)$ is $\mathbb{C}(U)$-isomorphic to $L\mathbb{C}/\mathbb{C}(U)$ [12].

The set H is *weakly $k(U)$-parametric* if (*) holds with $\mathscr{R}$ the set of all k-regular Galois extensions $L/k(U)$ of group G. When one of these properties holds for $\mathsf{H} = \mathsf{H}_{r,G}(\mathbf{C})_k \neq \emptyset$, we say that the ramification type $(r, \mathbf{C})$ has the property (instead of H).

Obviously we have:

$$\mathsf{H} \text{ is } k(U)\text{-parametric} \Rightarrow \mathsf{H} \text{ is weakly } k(U)\text{-parametric.}$$

2.3.1. *General criterion.* – Given a subfield $k \subset \mathbb{C}$ and a finite group G, denote the set of all k-regular extensions $L/k(U)$ of group G by $\mathscr{R}_k(G)$. From Theorem 2.1, if the ramification type $(r, \mathbf{C})$ is weakly $k(U)$-parametric, we must have

$$(*) \qquad r \leq r_L \text{ and } \mathbf{C} \prec \mathbf{C}_L \text{ for every } L/k(T) \in \mathscr{R}_k(G).$$

The general idea is to show that for some groups G, this is possible for no ramification type $(r, \mathbf{C})$. Criterion 2.9 below uses the following additional notation.

Definition 2.8. – Say that two conjugacy classes C and C' of G are *incompatible*, and write then $C\#C'$ if there is no conjugacy class C_0 such $C \subset C_0^{\mathbb{Z}}$ and $C' \subset C_0^{\mathbb{Z}}$.

For example, if C is the conjugacy class of a generator of a maximal cyclic subgroup of G, then $C\#C'$ if and only if $C' \not\subset C^{\mathbb{Z}}$. In particular, if C' is also the conjugacy class of a generator of a maximal cyclic subgroup of G, then $C\#C'$ if and only if $C^{\mathbb{Z}} \neq (C')^{\mathbb{Z}}$, i.e., if the two maximal cyclic subgroups associated with C and C' are not conjugate in G. Many concrete examples appear in § 2.3.2 and § 2.3.3 below.

extension $L/\mathbb{Q}(U)$ of group $H \subset G$ is a specialization of $F/\mathbb{C}(T)$, the specialization point T_0, which is in $\mathbb{C}(U)$ may not be in $\mathbb{Q}(U)$. Anticipating on § 4.2, the issue relates to the following: a polynomial equation $P(U, T, Y) = 0$ with $P \in \mathbb{Q}[U, T, Y]$ may have a solution $(T_0(U), Y_0(U)) \in \mathbb{C}(U)^2$ but no solution in $\mathbb{Q}(U)^2$: think of $Y^2 + T^2 + U^2 + 1 = 0$.

[11] And not of group *contained in* G for $\mathscr{R}$ as in the original parametric context.

[12] While in the original parametric context, (*) should be true without extending the scalars from k to $\mathbb{C}$. Also note that necessarily $T_0 \notin \mathbb{C}$ if $L/k(U)$ is non-trivial, as a consequence of the k-regularity of $L/k(U)$.

Criterion 2.9. – *Let $\mathscr{R} \subset \mathscr{R}_k(G)$ be a nonempty subset. Let $\rho_{\mathscr{R}}$ be the minimum number r_L for some $L/k(T) \in \mathscr{R}$. Assume the list of conjugacy classes appearing in some tuple $\mathbf{C}_L$ with $L/k(T) \in \mathscr{R}$ has at least $\nu_{\mathscr{R}}$ of them that are pairwise incompatible, and that $\nu_{\mathscr{R}} > \rho_{\mathscr{R}}$. Then*

(*) *there is no ramification type $(r, \mathbf{C})$*
that weakly $k(U)$-specializes to all extensions $L/k(T)$ in $\mathscr{R}$.

In particular, G has no weakly $k(U)$-parametric ramification type and a fortiori no $k(U)$-parametric ramification type $(r, \mathbf{C})$.

The smaller the subset $\mathscr{R}$ is the stronger is conclusion (*), which, in the extreme case $\mathscr{R} = \mathscr{R}_k(G)$, is equivalent to G not having a weakly $k(U)$-parametric ramification type $(r, \mathbf{C})$.

Proof. – Assume that there is a ramification type $(r, \mathbf{C})$ that contradicts (*). It follows from Theorem 2.1 that $r \leq \rho_{\mathscr{R}}$ and $\mathbf{C} \prec \mathbf{C}_L$ for every $L/k(T) \in \mathscr{R}$. Hence if C, C' are two conjugacy classes appearing in the list of tuples $\mathbf{C}_L$ with $L/k(T) \in \mathscr{R}$, there are conjugacy classes C_i, C_j from $\mathbf{C}$ such that $C \subset C_i^{\mathbb{Z}}$ and $C' \subset C_j^{\mathbb{Z}}$. If $C \# C'$, then $C_i \neq C_j$. Hence $r \geq \nu_{\mathscr{R}}$ and $\rho_{\mathscr{R}} \geq \nu_{\mathscr{R}}$, a contradiction. □

2.3.2. *Groups with no $\mathbb{C}(U)$-parametric ramification type.* – Denote the number of conjugacy classes of maximal cyclic subgroups of a group G by $\nu(G)$ and the rank of G (minimal cardinality of a generating set) by $\mathrm{rk}(G)$.

Corollary 2.10. – *Assume k that is algebraically closed. If $\nu(G) \geq \mathrm{rk}(G) + 2$, there exist two extensions $L_1/k(T)$ and $L_2/k(T)$ such that no ramification type $(r, \mathbf{C})$ weakly $k(U)$-specializes to both. Consequently G has no weakly $k(U)$-parametric ramification type and a fortiori no $k(U)$-parametric ramification type $F/k(T)$.*

Proof. – This directly follows from criterion 2.9 applied with $\mathscr{R}$ consisting of two extensions $L_1/k(T)$ and $L_2/k(T)$ chosen so that $r_{L_1} = \mathrm{rk}(G)+1$ and $\mathbf{C}_{L_2}$ contains all non trivial conjugacy classes of G. Such extensions exist thanks to the RET (as recalled in *Basic Terminology*). □

Remark 2.11. – As pointed out by Legrand, the proof gives more: no two Galois extensions $F_1/k(T)$, $F_2/k(T)$ with group G and same branch point number r (but possibly different ramification types) can weakly $k(U)$-specialize to $L_1/k(T)$, $L_2/k(T)$, respectively. Namely, as in criterion 2.9, one should otherwise have $r \leq \mathrm{rk}(G) + 1$, but then $F_2/k(T)$ cannot specialize to $L_2/k(T)$ if $\nu(G) \geq \mathrm{rk}(G) + 2$. For $G = (\mathbb{Z}/2\mathbb{Z})^n$ with $n \geq 3$, one can even take $k = \mathbb{Q}$. Construct indeed $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$ as in the proof but also $\mathbb{Q}$-regular: take $L_1 = \mathbb{Q}(T)(\sqrt{T-1}, \ldots, \sqrt{T-n})$ and $L_2/\mathbb{Q}(T)$ can be obtained thanks to the rigidity theory.

As we check below, the groups in the following non exhaustive list satisfy the condition $\nu(G) \geq \mathrm{rk}(G) + 2$.

Corollary 2.12. – *Assume that k is algebraically closed. None of these groups:*

- *S_n and A_n, $n \geq 6$,*

- *non cyclic nilpotent groups G with abelianization G^{ab} different from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, in particular non cyclic nilpotent groups G of odd order,*
- *linear groups $\mathrm{PSL}_2(\mathbb{F}_p)$, $p > 7$ prime,*
- *all sporadic simple groups,*

has a weakly $k(U)$-parametric ramification type $(r, \mathbf{C})$. More precisely, for such groups G, there exist two Galois extensions $L_1/k(U)$ and $L_2/k(U)$ of group G such that no ramification type $(r, \mathbf{C})$ weakly $k(U)$-specializes to both.

On the other hand, all finite subgroups of $\mathrm{PGL}_2(\mathbb{C})$ can be double-checked not to satisfy $\nu(G) \geq \mathrm{rk}(G) + 2$ (which must also hold because they have a $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$). The quaternion group $\mathbb{H}_8$ is another example. The complete list of groups satisfying the condition remains to be established. It seems that it contains most simple groups (and not just the last two categories of examples).

Proof. – We use the standard notation for the conjugacy classes of S_n or A_n: $[1^{\ell_1} \cdots n^{\ell_n}]$ is the conjugacy class of elements of S_n that write as a product of ℓ_1 cycles of length 1, …, ℓ_n cycles of length n, all cycles having disjoint supports; if such a class is contained in A_n, it is a conjugacy class of A_n if and only if $\ell_q \geq 2$ or $\ell_{2q} \geq 1$ for some $q \in \{1, \dots, n\}$; otherwise $[1^{\ell_1} \cdots n^{\ell_n}]$ splits into two distinct conjugacy classes of A_n denoted by $[1^{\ell_1} \cdots n^{\ell_n}]_1$ and $[1^{\ell_1} \cdots n^{\ell_n}]_2$.

The symmetric groups S_n, $n \geq 6$, satisfy $\nu(G) \geq \mathrm{rk}(G) + 2$. Indeed $\mathrm{rank}(S_n) = 2$ and these 4 conjugacy classes are pairwise incompatible:

$$[n^1], \quad [(n-1)^1], \quad [(n-2)^1 2^1], \quad [(n-3)^1 3^1].$$

So do the alternating groups A_n with $n \geq 6$: note that $\mathrm{rank}(A_n) = 2$ and use the classes

$$\begin{cases} [n^1]_1, \quad [(n-3)^1 2^1 1^1], \quad [(n-2)^1 1^2], \quad [(n-4)^1 1^4] & \text{if } n \text{ odd} \\ [(n-1)^1 1^1]_1, \quad [(n-2)^1 2^1], \quad [(n-3)^1 1^3], \quad [(n-4)^1 2^1] & \text{if } n \text{ even.} \end{cases}$$

For the second class of examples, we start with the case G is abelian. If G of rank $s \geq 2$, it writes $G = \mathbb{Z}/d_1\mathbb{Z} \times \cdots \mathbb{Z}/d_s\mathbb{Z}$ with $s \geq 2$ and $d_1|d_2|\cdots|d_s$ in $\mathbb{Z}$. The s-tuples $(\varepsilon_1, \dots, \varepsilon_{s-1}, 1)$ with $\varepsilon_i \in \mathbb{Z}/d_i\mathbb{Z}$ ($i = 1, \dots, s-1$) generate non-conjugate maximal cyclic subgroups of G. There are $d_1 \cdots d_{s-1}$ such s-tuples, and so at least $s + 2$ unless ($s = 2$ and $d_1 \in \{2, 3\}$) or ($s = 3$ and $d_1 = d_2 = 2$). After checking separately the remaining special cases (use further non-conjugate maximal cyclic subgroups e.g., those generated by s-tuples $(\varepsilon_1, \dots, \varepsilon_{s-1}, k)$ with $k \in (\mathbb{Z}/d_s\mathbb{Z})^\times$), conclude that $\nu(G) \geq \mathrm{rk}(G) + 2$ unless $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Assume more generally that G is nilpotent. From the Burnside basis theorem, G and its abelianization G^{ab} have the same rank. On the other hand, we have $\nu(G) \geq \nu(G^{\mathrm{ab}})$. If G is non cyclic then so is G^{ab}. If G^{ab} is further assumed to be different from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then from the preceding case, we have $\nu(G^{\mathrm{ab}}) \geq \mathrm{rk}(G^{\mathrm{ab}}) + 2$. Inequality $\nu(G) \geq \mathrm{rk}(G) + 2$ follows.

All finite simple groups have rank 2 and their classification shows that many of them have at least 4 non-conjugate maximal cyclic subgroups of G. This includes all groups $\mathrm{PSL}_2(\mathbb{F}_p)$ ($p > 7$ prime) and all sporadic simple groups. □

Criterion 2.9 can be used in a slightly different way to lead to this variant of Corollary 2.10.

Corollary 2.13. – *If N is an integer $< \nu(G)/(\mathrm{rk}(G)+2)$, there do not exist N ramification types $(r_1, \mathbf{C}_1), \dots, (r_N, \mathbf{C}_N)$ such that this holds:*

(*) *every Galois extension $L/\mathbb{C}(U)$ of group G is a $\mathbb{C}(U)$-specialization of one of the ramification types $(r_i, \mathbf{C}_i)$, $i = 1, \dots, N$.*

Proof. – Let $g_1, \dots, g_{\nu(G)}$ be generators of $\nu(G)$ non-conjugate maximal cyclic subgroups and let $C_1, \dots, C_{\nu(G)}$ be their conjugacy classes. For $j = 1, \dots, \nu(G)$, construct a Galois extension $L_j/\mathbb{C}(U)$ such that C_j appears in $\mathbf{C}_{L_j}$, $r_{L_j} = \mathrm{rk}(G) + 2$[13], and in such a way that the constructed extensions are distinct; if some happen to be equal in a first stage, compose them with non-trivial automorphisms of $\mathbb{C}(U)$. Assume that N ramification types $(r_1, \mathbf{C}_1), \dots, (r_N, \mathbf{C}_N)$ exist that satisfy the conclusion of Corollary 2.13. Then there is an index $i \in \{1, \dots, N\}$ such that at least $\nu(G)/N$ of the constructed extensions $L_j/\mathbb{C}(U)$ $(j = 1, \dots, \nu(G))$ are $\mathbb{C}(U)$-specializations of extensions $F/\mathbb{C}(T)$ with ramification type $(r_i, \mathbf{C}_i)$. If $\mathscr{R}$ is the set of these $\nu(G)/N$ extensions, we have $\rho_{\mathscr{R}} = \mathrm{rk}(G) + 2$ and criterion 2.9 can be applied with $\nu_{\mathscr{R}} \geq \nu(G)/N$; this gives $\nu(G)/N \leq \mathrm{rk}(G) + 2$ and so $N \geq \nu(G)/(\mathrm{rk}(G) + 2)$. □

The following generalized problem was suggested by the referee.

Problem 2.14. – *Given m nontrivial conjugacy classes $C_1, \dots, C_m$ of a finite group G such that $\bigcup_{i=1}^m C_i$ contains a generating set of G, do there exist finitely many ramification types $(r_1, \mathbf{C}_1), \dots, (r_N, \mathbf{C}_N)$ with $\mathbf{C}_1, \dots, \mathbf{C}_N$ only supported by powers of $C_1, \dots, C_m$ such that this holds:*

(*) *every Galois extension $F/\mathbb{C}(T)$ of group G and with ramification type only supported by conjugacy class powers of $C_1, \dots, C_m$ is a $\mathbb{C}(U)$-specialization of one of the ramification type $(r_i, \mathbf{C}_i)$, $i = 1, \dots, N$?*

Corollary 2.13 shows that when $C_1, \dots, C_m$ consist of all non trivial conjugacy classes of G, one should have $N \geq \nu(G)/(\mathrm{rk}(G) + 2)$. The special case $m = 1$ is also interesting; G can be taken to be a simple group, a symmetric group S_n with C_1 the class of involutions, etc. However this case is not in the range of criterion 2.9 as the conjugacy classes involved in the ramification types of the extensions $F/\mathbb{C}(T)$ considered in (*) *are* all pairwise compatible; $\nu_{\mathscr{R}} = 1$ in this case.

2.3.3. *Groups with no $\mathbb{Q}(U)$-parametric ramification type.* – Here we apply criterion 2.9 over a non-algebraically closed field k.

Corollary 2.15. – *Let k be a subfield of $\mathbb{C}$. None of the groups*

- *S_n, $n \geq 6$ and A_n, $n \geq 7$,*
- *$\mathrm{PSL}_2(\mathbb{F}_p)$ with p a prime such that $(\frac{2}{p}) = (\frac{3}{p}) = -1$,*
- *the Fischer-Griess Monster M,*

[13] Take for $\mathbf{C}_{L_j}$ a tuple consisting of C_j and the conjugacy classes of elements of a minimal generating set and apply the RET as explained in *Basic Terminology*.

has a weakly $k(U)$-parametric ramification type and a fortiori they do not have a $k(U)$-parametric ramification type $(r, \mathbf{C})$. More precisely, except for the alternating groups A_n, there exist two extensions $L_1/k(U)$, $L_2/k(U)$ such that no ramification type $(r, \mathbf{C})$ weakly $k(U)$-specializes to both; for groups A_n, three extensions are needed.

The list is not exhaustive. This corollary is meant to show on examples how to apply Criterion 2.9 and how in some situations where it cannot be applied directly, one can still get the desired conclusion.

Proof. – Take $G = S_n, n \geq 6$. The group S_n is known to have $\mathbb{Q}$-regular realizations with the following inertia canonical invariants (see [27], [20, **B**-3] for the first one and [16] for the second one):

$$\begin{cases} \mathbf{C}_m = ([n^1], [m^1(n-m)^1], [2^1 1^{n-2}]) & \text{with } 1 \leq m \leq n,\ (m,n) = 1, \\ \mathbf{C} = ([(n-2)^1 1^2], [3^1 1^{n-3}], [2^{n/2}], 2^{(n-2)/2} 1^2]) & \text{if } n \geq 6 \text{ even.} \end{cases}$$

Apply criterion 2.9 with $\mathcal{R}$ consisting of the following two realizations:

- if n is odd, those above with inertia canonical invariants $\mathbf{C}_1$ and $\mathbf{C}_m$, with $m \neq 1, 2, n-1, n-2$; such an m exists as $n \geq 7$;
- if n is even, those above with inertia canonical invariants $\mathbf{C}_1$ and $\mathbf{C}$.

Then $\rho_{\mathcal{R}} \leq 3$ and $\nu_{\mathcal{R}} \geq 4$. Conclude that statement (*) from criterion 2.9 is satisfied for this $\mathcal{R}$.

Take $G = A_n, n \geq 7$. The group A_n is known to have $\mathbb{Q}$-regular realizations with the following inertia canonical invariant [20, **B**-3]:
if n is even:

$$([m^1(n-m)^1]_1, [m^1(n-m)^1]_2, [(n/2)^2]) \text{ with } 1 \leq m \leq n,\ (m,n) = 1$$

if n is odd:

$$([n^1]_1, [n^1]_2, [m^1((n-m)/2)^2]) \text{ with } m \text{ odd, } 1 \leq m \leq n,\ (m,n) = 1,$$
$$([n^1]_1, [n^1]_2, [(m/2)^2(n-m)^1]) \text{ with } m \text{ even, } 1 \leq m \leq n,\ (m,n) = 1.$$

One checks that for every $n \geq 7$, one can always find three such realizations with four pairwise incompatible conjugacy classes in the union of the three inertia canonical invariants. Criterion 2.9 concludes the proof in this case.

Take $G = \mathrm{PSL}_2(\mathbb{F}_p)$ with $p > 3$ a prime such that $(\frac{2}{p}) = (\frac{3}{p}) = -1$. [29, §8.3.3] gives two $\mathbb{Q}$-regular realizations $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$ of G with $r_{L_1} = r_{L_2} = 3$ and

$$\mathbf{C}_{L_1} = (2A, pA, pB) \text{ and } \mathbf{C}_{L_2} = (3A, pA, pB),$$

where $2A$ (resp. $3A$) is the unique conjugacy class of $\mathrm{PSL}_2(\mathbb{F}_p)$ of order 2 (resp. of order 3) and pA, pB are the two conjugacy classes of order p. Hence for $\mathcal{R} = \{L_1/\mathbb{Q}(T), L_2/\mathbb{Q}(T)\}$, we have $\rho_{\mathcal{R}} \leq 3$.

According to [15, Corollary 2.7], the maximal order of an element of $\mathrm{PSL}_2(\mathbb{F}_p)$ is $p+1$, so the conjugacy classes pA and pB are classes of generators of maximal cyclic subgroups. It follows that $2A \# pA$, $2A \# pB$, $3A \# pA$, $3A \# pB$. Furthermore $2A \# 3A$: indeed otherwise both classes would be contained in the conjugacy class of a cyclic subgroup $\langle \gamma_0 \rangle \subset \mathrm{PSL}_2(\mathbb{F}_p)$

of order 6. But then $\gamma_0 \in 3A$ or $(-\gamma_0) \in 3A$ and so $2A \subset (3A)^{\mathbb{Z}}$ or $2A \subset (-3A)^{\mathbb{Z}}$—a contradiction.

However pA and pB are not incompatible and criterion 2.9 cannot be applied directly. We use instead the following argument.

Assume there is a ramification type $(r, \mathbf{C})$ that weakly $k(U)$-specializes to both extensions $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$. From above we have $r = 3$ and, with $\mathbf{C} = (C_1, C_2, C_3)$, there should exist integers $a_i, b_i, c_i \in \mathbb{Z}$, $i = 1, 2$, such that

$$(C_1^{a_1}, C_2^{b_1}, C_3^{c_1}) = (2A, pA, pB) \text{ and } (C_1^{a_2}, C_2^{b_2}, C_3^{c_2}) = (3A, pA, pB).$$

Necessarily $C_2, C_3 \in \{pA, pB\}$, $2A \subset C_1^{\mathbb{Z}}$ and $3A \subset C_1^{\mathbb{Z}}$. This contradicts $2A\#3A$.

Finally take $G = M$ the Fischer-Griess Monster. We will use two known $\mathbb{Q}$-regular realizations $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$ of G, for which $r_{L_1} = r_{L_2} = 3$ and

$$\mathbf{C}_{L_1} = (2A, 3B, 29A) \text{ and } \mathbf{C}_{L_2} = (2A, 3C, 38A)$$

(where we use the standard notation from the Atlas of simple groups for the conjugacy classes of M). The extension $L_1/\mathbb{Q}(T)$ is the one originally produced by J. Thompson [30]; the main point is that $\mathbf{C}_{L_1}$ is a "rigid triple". Computer programs now exist to find other rigid tuples. The triple $\mathbf{C}_{L_2}$ was communicated to me by J. Koenig who checked that it is rigid, assuming that the current classification of all (certain and hypothetical) maximal subgroups of M is correct.

Assume there is a ramification type $(r, \mathbf{C})$ that weakly $k(U)$-specializes to both extensions $L_1/\mathbb{Q}(T)$ and $L_2/\mathbb{Q}(T)$. Then we have $r = 3$. Set $\mathbf{C} = (C_1, C_2, C_3)$. From the Atlas of simple groups, there is only one conjugacy class, $38A$, whose elements are of order a multiple of 38 (and this multiple is 38) and there are three conjugacy classes, $29A$, $87A$ and $87B$, whose elements are of order a multiple of 29 (and these multiples are 29, 87 and 87). One of C_1, C_2, C_3, say C_1, must be $38A$ and one, say C_2, should be $29A$ or $87A$ or $87B$. Furthermore $3B$ and $3C$ are not a power of $87A$ or $87B$. This leads to these possibilities for the triple $\mathbf{C}$ of ramification indices of $F/\mathbb{Q}(T)$:

$$\mathbf{C} = (38A, 29A, C_3) \text{ or } \mathbf{C} = (38A, 87A, C_3) \text{ or } \mathbf{C} = (38A, 87B, C_3)$$

with C_3 of order divisible by 3. But then the lower bound for the number r_{T_0} of branch points of a specialized extension $F_{T_0}/\mathbb{Q}(T)$ with $T_0 \in \mathbb{Q}(T)$ given in Theorem 3.1 (b-1) gives $r_{T_0} > 3$ and so neither $L_1/\mathbb{Q}(T)$ nor $L_2/\mathbb{Q}(T)$ can be a specialization of an extension $F/\mathbb{Q}(T)$ with inertia canonical invariant $\mathbf{C}$. □

2.4. Non $\mathbb{Q}$-parametric extensions $F/\mathbb{Q}(T)$

Assume k is a number field. The groups from Corollary 2.15 have no weakly $k(U)$-parametric ramification type $(r, \mathbf{C})$ and *a fortiori* no weakly $k(U)$-parametric extension $F/k(T)$. We show below how to deduce that they do not have a k-parametric extension $F/k(T)$ (Corollary 2.18). Our method is however conditional to some diophantine "working hypothesis" (§ 2.4.2) and does not lead to a non k-parametric ramification type conclusion.

2.4.1. *Main tool for producing non k-parametric extensions $F/k(T)$.* –

Theorem 2.16. – *Let $F/k(T)$ and $L/k(T)$ be two k-regular Galois extensions with respective groups G and H such that $H \subset G$. There exist $k(U)$-regular covers $\widetilde{f_i} : \widetilde{X_i} \to \mathbb{P}^1_{k(U)}$, $i = 1, \dots, N$ such that:*

(a) $\overline{k(U)}(\widetilde{X_i}) = F\overline{k(U)}$, $i = 1, \dots, N$.

(Equivalently, after scalar extension to $\overline{k(U)}$, each cover $\widetilde{f_i}$ becomes isomorphic to the k-cover of $\mathbb{P}^1_k$ corresponding to the extension $F/k(T)$).

(b) *For all but finitely many $u_0 \in k$ or for $u_0 = U$, the $k(U)$-covers $\widetilde{f_1}, \dots, \widetilde{f_N}$ have good reduction at $U = u_0$ and the reduced $k(u_0)$-covers, say $\widetilde{f_i}|_{u_0} : \widetilde{X_i}|_{u_0} \to \mathbb{P}^1_{k(u_0)}$ $(i = 1, \dots, N)$, have this property:*

(*) *for all $t_0 \in \mathbb{P}^1(k(u_0))$ not a branch point of $F/k(T)$, the specializations $L_{u_0}/k(u_0)$ and $F_{t_0}/k(u_0)$ are $k(u_0)$-isomorphic iff there exist $i \in \{1, \dots, N\}$ and an unramified $k(u_0)$-point on $\widetilde{X_i}|_{u_0}$ above t_0 (via $\widetilde{f_i}|_{u_0}$).*

Theorem 2.16 is proved in § 4.

2.4.2. *The working hypothesis.* – We will deduce some non k-parametric conclusions from Theorem 2.16 under this "working hypothesis":

(WH) *Let k be a number field and $f_i : X_i \to \mathbb{P}^1_{k(U)}$, $i = 1, \dots, N$, be $k(U)$-regular covers. Assume that none of the $k(U)$-curves $X_1, \dots, X_N$ have an unramified*[14] *$\mathbb{C}(U)$-rational point. Then for infinitely many $u_0 \in k$, the covers $f_1, \dots, f_N$ have good reduction at $U = u_0$ and none of the reduced curves $X_1|_{u_0}, \dots, X_N|_{u_0}$ have an unramified k-rational point.*

This is an extension of Hilbert's Irreducibility Theorem, which indeed corresponds to (WH), modified as follows: instead of "$k(U)$-regular covers of $\mathbb{P}^1_{k(U)}$ with no unramified $\mathbb{C}(U)$-rational point," consider "closed points of $\mathbb{P}^1_{k(U)}$ of degree ≥ 2 over $k(U)$"—one way of seeing irreducible polynomials $P \in k(U)[Y]$ with $\deg_Y(P) \geq 2$.

We make more comments on the hypothesis (WH) in § 2.4.4. Below we first explain how to combine it with Theorem 2.16.

2.4.3. *Main conclusions*

Proposition 2.17. – *Let k be a number field, assume that* (WH) *holds and let $F/k(T)$ be a k-regular Galois extension of group G.*

(a) *If a k-regular Galois extension $L/k(U)$ of group $H \subset G$ is such that $L\mathbb{C}/\mathbb{C}(U)$ is not a specialization of $F/k(T)$ at any $T_0 \in \mathbb{P}^1(\mathbb{C}(U))$, there are infinitely many $u_0 \in k$ such that the specialization L_{u_0}/k is not a specialization of $F/k(T)$ at any $t_0 \in k$, not a branch point of $F/k(T)$.*

(b) *If $F/k(T)$ is k-parametric then it is weakly $k(U)$-parametric.*

(c) *Every group with no weakly $k(U)$-parametric extension has no k-parametric extension.*

Corollary 2.18. – *Let k be a number field and assume* (WH) *holds. Every group as in Corollary 2.15 has no k-parametric extension $F/k(T)$.*

[14] By "unramified on X_i" we mean w.r.t. the cover $f_i : X_i \to \mathbb{P}^1_{k(U)}$; similarly below "unramified on $X_i|_{u_0}$" means w.r.t. the cover $f_i|_{u_0} : X_i|_{u_0} \to \mathbb{P}^1_k$, $i = 1, \dots, N$.

Proof of Proposition 2.17. – Let $F/k(T)$ and $L/k(U)$ be as in (a) and $\widetilde{f_1},\dots,\widetilde{f_N}$ be the $k(U)$-regular covers provided by Theorem 2.16. Combining its conclusion (b) for $u_0 = U$ and the assumption in (a) above yields that none of the $k(U)$-curves $\widetilde{X}_1,\dots,\widetilde{X}_N$ has an unramified $\mathbb{C}(U)$-rational point [15]. Apply (WH) to conclude that for infinitely many $u_0 \in k$, the covers $\widetilde{f_1},\dots,\widetilde{f_N}$ have good reduction at $U = u_0$ and that none of the reduced curves $\widetilde{X}_1|_{u_0},\dots,\widetilde{X}_N|_{u_0}$ have an unramified k-rational point. From Theorem 2.16, for these u_0, the specialization L_{u_0}/k, which is of Galois group contained in $H \subset G$, is not a specialization F_{t_0}/k with $t_0 \in k$, not a branch point of $F/k(T)$. Statements (b) and (c) follow straightforwardly from (a). □

REMARK 2.19. – (a) The proof shows that Proposition 2.17 and Corollary 2.18 still hold if (WH) is replaced by the weaker hypothesis (WH-$\flat$) for which the conclusion of (WH) solely holds for $k(U)$-regular covers $f_1,\dots,f_N$ which all become isomorphic to a $\overline{k(U)}$-regular Galois cover (the same for $i = 1,\dots,N$) after scalar extension to $\overline{k(U)}$.

(b) We can explain how, conditionally, Legrand's result (mentioned in § 1.1) can be deduced from ours. Assuming G is the group of some $\mathbb{Q}$-regular Galois extension $L/\mathbb{Q}(U)$, if $F/\mathbb{Q}(T)$ is another $\mathbb{Q}$-regular Galois extension of group G such that $L\mathbb{C}/\mathbb{C}(U)$ is not a $\mathbb{C}(U)$-specialization of $F/\mathbb{Q}(T)$, then it follows from Proposition 2.17 that, if G satisfies (WH-$\flat$), $F/\mathbb{Q}(T)$ is not $\mathbb{Q}$-parametric. [16]

For example, one can take for $F/\mathbb{Q}(T)$ a specialization $L_{U_0}/\mathbb{Q}(T)$ with $U_0(T) = a + T^5$ with $a \in \mathbb{Q}$. For all but finitely many $a \in \mathbb{Q}$, $\mathrm{Gal}(F/\mathbb{Q}(T)) = G$. From inequality (*) from § 2.1.1, the branch point number of $F\mathbb{C}/\mathbb{C}(T)$ is bigger than that of $L\mathbb{C}/\mathbb{C}(U)$. From Theorem 2.1, the latter is not a specialization of the former with $T_0 \in \mathbb{C}(U)$.

2.4.4. *Comments on the working hypothesis*

(a) The working hypothesis (WH) is a variant for covers of the following statement about curves, posed as a problem of Fried in [3], and which we call here the *Fried-Schinzel problem*:

(*) *given a family X_U of smooth projective k-curves parametrized by $U \in \mathbb{P}^1$, if there is no $k(U)$-rational point on X_U, then there are infinitely many $u_0 \in k$ such that there is no k-rational point on X_{u_0}.*

Schinzel proved that Fried's problem has an affirmative answer when X_U has genus 0 [26, Theorem 38]. A stronger conclusion even holds: the infinitely many u_0 can be chosen in the ring of integers of k. Our cover variant (WH) holds too for genus 0 curves, but for a different reason: the $k(U)$-curves that we consider should not have rational points over $\mathbb{C}(U)$; this is not possible if the genus is 0, due to Tsen's theorem.

Our working hypothesis (WH) was also shown to hold in this situation: $N = 1$ and $f_1 : X_1 \to \mathbb{P}^1_{T,k(U)}$ is the $k(U)$-cover corresponding to the polynomial $Y^n - U^m Q(T)$ with $n \geq 2$ dividing $\deg(Q)$, m relatively prime to n and $Q \in k[T] \setminus k$ a polynomial with integral

[15] To obtain this $\mathbb{C}(U)$-irrationality conclusion (instead of $k(U)$-irrationality), one uses the fact, shown by the proof of Theorem 2.16, that the covers $\widetilde{f_1},\dots,\widetilde{f_N}$ behave well under scalar extension from k to $\mathbb{C}$: the covers, with $\mathbb{C}$ as base field, are obtained from the original ones by scalar extension.

[16] Legrand in fact obtains a stronger conclusion: he can produce extensions $E/\mathbb{Q}$ that in addition to not being specializations of $F/\mathbb{Q}(T)$ are Galois of group G (and not only of group $H \subset G$).

coefficients such that the Galois group of Q has an element that fixes no root of Q (e.g., Q is irreducible in $k[T]$) [24].

(b) There is no known counter-example to the working hypothesis (WH) or to the Fried-Schinzel problem. The best attempts in this direction are due to Cassels, Lewis and Schinzel [25] [3] [27]. They produce two polynomials $Y^2 - f(U,T)$ with $f(U,T)$ taken to be

$$\begin{cases} f_1(U,T) = T^4 - (8U^2+5)^2, & \text{or} \\ f_2(U,T) = T(T^2 - (7U^4+7)^2) & \end{cases}$$

and show these properties: the $\mathbb{C}(U)$-curve $y^2 - f(U,t) = 0$ is of genus 1, the equation $y^2 - f(U,t) = 0$ has no unramified solution $(T_0(U), Y_0(U) \in \mathbb{Q}(U)^2$ and the equation $y^2 - f(u_0,t) = 0$ has a solution $(t_0, y_0) \in \mathbb{Q}^2$ for every $u_0 \in \mathbb{Z}$. This however does not make them counter-examples. First, the last conclusion is only established under a conjecture of Selmer [28]. Secondly, for $f = f_2$, the equation $y^2 - f(U,t) = 0$ has an unramified solution $(T_0(U), Y_0(U) \in \mathbb{C}(U)^2$ (contrary to the assumption in (WH))[(17)], and for $f = f_1$, it is not shown (even conjecturally) that the equation $y^2 - f(u_0,t) = 0$ has a solution $(t_0, y_0) \in \mathbb{Q}^2$ for every $u_0 \in \mathbb{Q}$ (it is only shown for every $u_0 \in \mathbb{Z}$)[(18)].

3. $\mathbb{C}(U)$-specializations of Galois extensions $F/\mathbb{C}(T)$

A main goal of this section is to establish Theorem 2.1.

Let $F/\mathbb{C}(T)$ be a degree d Galois extension of group G, with r branch points $t_1, \dots, t_r$, inertia canonical invariant $\mathbf{C} = (C_1, \dots, C_r)$ and associated ramification indices $\mathbf{e} = (e_1, \dots, e_r)$. Also set

$$\begin{cases} \varepsilon = \frac{1}{e_1} + \cdots + \frac{1}{e_r} \\ e_\infty = \max(e_1, \dots, e_r). \end{cases}$$

Let $T_0(U) = a(U)/b(U) \in \mathbb{C}(U) \setminus \mathbb{C}$ with $a, b \in \mathbb{C}[U]$ relatively prime and $b \neq 0$. Set

$$N = \deg(T_0) = \max(\deg(a), \deg(b)).$$

We will compare the invariants of $F/\mathbb{C}(T)$ to those of $F_{T_0}/\mathbb{C}(T)$.

Note that when $N = 1$, T_0 is a linear fractional transformation and the two extensions $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are isomorphic. More specifically, T_0 interprets as an automorphism of $\mathbb{P}^1(\mathbb{C})$ and if $f : X \to \mathbb{P}^1$ is the branched cover corresponding to $F/\mathbb{C}(T)$, then $F_{T_0}/\mathbb{C}(T)$ corresponds to the cover $f \circ T_0^{-1}$. In particular the invariants $G, r, d, g, \mathbf{C}$ are the same for the two extensions.

[(17)] The equation $y^2 - f_2(U,t) = 0$ also has the obvious ramified solution $y = t = 0$.

[(18)] And it is also actually stated that for infinitely $u_0 \in \mathbb{Q}$, the elliptic curve of equation $y^2 - f(u,t) = 0$ is of rank 0.

3.1. Invariants of the specialized extensions

Denote the invariants of the specialized extensions $F_{T_0}/\mathbb{C}(U)$ by G_{T_0}, $d_{T_0} = |G_{T_0}|$, g_{T_0} and $\mathbf{C}_{T_0}$. The following statement is the most precise of this section. We will in particular deduce Theorem 2.1 from it.

THEOREM 3.1. – *Consider the specialized extension $F_{T_0}/\mathbb{C}(U)$.*

(a) *We have $G_{T_0} \subset G$, equivalently $d_{T_0} \leq d$. Furthermore $d_{T_0} < d$ if and only if there is a subfield $L \subset F$, $L \neq \mathbb{C}(T)$, of genus* 0*, such that a specialization of it at T_0 is trivial: $L_{T_0} = \mathbb{C}(U)$.*

(b) *The branch point number r_{T_0} satisfies $r_{T_0} \leq rN$ and*

$$\text{(b-1)} \qquad r_{T_0} \geq \frac{(r-\varepsilon-2)N+2}{1-(1/e_\infty)} \quad \textit{if } r \geq 0$$

$$\text{(b-2)} \qquad r_{T_0} \geq (r-4)N+4 \quad \textit{if } r \geq 4$$

(c) *The inertia canonical invariant $\mathbf{C}_{T_0}$ of $F_{T_0}/\mathbb{C}(U)$ consists of conjugacy classes in G_{T_0} of powers g^α ($\alpha \in \mathbb{N}$) of elements of $C_1 \cup \cdots \cup C_r$.*

(d) *The genus g_{T_0} satisfies $g_{T_0} \leq N(g+d-1)$, and, if $G_{T_0} = G$,*

$$g_{T_0} - g \geq \frac{d}{4}(N-1)(r-4).$$

REMARK 3.2. – The lower and upper bounds for g_{T_0} in (d) are better than those that can be deduced from inequalities (b-1) or (b-2) by combining them with the usual ones given by Riemann-Hurwitz:

$$\frac{r}{2} + 1 - d \leq g \leq \frac{rd}{2} + 1 - d - \frac{r}{2}.$$

Proof. – (a) The first part of (a) is standard.

Assume that there is a subfield $L \subset F$, $L \neq \mathbb{C}(T)$ with a trivial specialization: $L_{T_0} = \mathbb{C}(U)$. Then we have

$$d_{T_0} = [F_{T_0} : L_{T_0}]\,[L_{T_0} : \mathbb{C}(U)] \leq [F : L] < d.$$

For the converse, assume that $d_{T_0} < d$. A standard argument (e.g., [12, Lemma 13.1.2]) from the theory of Hilbertian fields (applied here to the field $\mathbb{C}(U)$) shows that there exists $\theta \in F \setminus \mathbb{C}(T)$ such that $\mathbb{C}(T,\theta)_{T_0} = \mathbb{C}(U)$: if $P(T,Y)$ is an affine equation of $F/\mathbb{C}(T)$, θ is a coefficient in $\overline{\mathbb{C}(T)}$ of a factorization $P(T,Y)$ in $\overline{\mathbb{C}(T)}[Y]$. The field $L = \mathbb{C}(T,\theta)$ is the desired field.

That L is of genus 0 follows from $L_{T_0} = \mathbb{C}(U)$. Indeed, if $Q(T,Y)$ is an affine equation for $L/\mathbb{C}(T)$, $L_{T_0} = \mathbb{C}(U)$ means that there exists $Y_0(U) \in \mathbb{C}(U)$ such that $Q(T_0(U), Y_0(U)) = 0$, which is a rational parametrization of the curve of equation $Q(T,Y)$. Hence its function field L is of genus 0.

(b) A first point of the proof is that

(*) *if $u \in \mathbb{P}^1(\mathbb{C})$ is a branch point of $F_{T_0}/\mathbb{C}(U)$, there exists a branch point t_i of $F/\mathbb{C}(T)$ such that $T_0(u) = t_i$ and, conversely, if $T_0(u) = t_i$, the associated inertia group is generated by some power g_i^α ($\alpha \in \mathbb{N}$) of an element $g_i \in C_i$.*

This statement, which in particular yields conclusion (c), follows from the Specialization Inertia Theorem (SIT) recalled in § 5. Specifically, we use it in the situation the Dedekind domain is $A = \mathbb{C}[U]$ (or $A = \mathbb{C}[1/U]$ for $u = \infty$), $K = \mathbb{C}(U)$, the K-regular extension is $F\mathbb{C}(U)/\mathbb{C}(U)(T)$ and $\mathfrak{p}$ is the ideal $\mathfrak{p} = \langle U - u\rangle$ if $u \in \mathbb{C}$ (and $\mathfrak{p} = \langle 1/U\rangle$ if $u = \infty$).

A few remarks on the assumptions from § 5 are in order:

(1) $|G| \notin \mathfrak{p}$ since $A/\mathfrak{p} = \mathbb{C}$ is of characteristic 0.
(2) *there is no vertical ramification at* $\mathfrak{p}$ *in the extension* $FK/K(T)$*:* indeed if $\mathcal{Y}$ is a primitive element of $F/\mathbb{C}(T)$, integral over A, then $1, \mathcal{Y}, \dots, \mathcal{Y}^{d-1}$ (with $d = |G|$) are integral over $A[T]$ and form a $K(T)$-basis of $FK/K(T)$. The discriminant of this basis is a non-zero element of $\mathbb{C} \subset A$, and so remains non-zero modulo $\mathfrak{p}$. This classically guarantees the content of our claim.
(3) *no two different branch points of* $F/K(T)$ *meet modulo* $\mathfrak{p}$: indeed the branch points are those of $F/\mathbb{C}(T)$ and their mutual differences $t_i - t_j$ or $(1/t_i) - (1/t_j)$ are non-zero elements of $\mathbb{C} \subset A$ and remain non-zero modulo $\mathfrak{p}$.
(4) *the ideal* $\mathfrak{p}$ *is unramified in* $K(t_1, \dots, t_r)/K = \mathbb{C}(U)/\mathbb{C}(U)$.
(5) t_i *and* $1/t_i$ *are integral over* $\widetilde{A}_{\mathfrak{p}}$: $t_i, 1/t_i \in \mathbb{C} \cup \{\infty\}$ $i = 1, \dots, r$.

The SIT concludes that if $u \in \mathbb{P}^1(\mathbb{C})$ is a branch point of $F_{T_0}/\mathbb{C}(U)$, there exists $i \in \{1, \dots, r\}$ such that T_0 meets t_i modulo $\mathfrak{p}$, which exactly means that $T_0(u) = t_i$, and, secondly, that, if $T_0(u) = t_i$, the inertia group of $F_{T_0}/\mathbb{C}(U)$ at u, is generated by an element of C_i^α with

$$\alpha = \mathrm{ord}_u(T_0(U) - t_i). \tag{**}$$

This concludes the proof of (*). To simplify the exposition of the rest of the proof, we first assume:

(H) *neither* ∞ *nor* $T_0(\infty)$ *is a branch point of* $F/\mathbb{C}(T)$.

and will explain afterwards how to reduce to this hypothesis.

For an element $u \in \mathbb{P}^1(\mathbb{C})$ such that $T_0(u) = t_i$ for some $i = 1, \dots, r$ to be a branch point of $F_{T_0}/\mathbb{C}(U)$, the integer α from (**) should not be a multiple of e_i. Note further that because of (H), $u \neq \infty$ and u is not a pole of T_0.

For each $i = 1, \dots, r$, label the roots in $\mathbb{C}$ of $a(U) - t_i b(U)$ as follows:

- $u_{i1}, \dots, u_{ip_i}$ are the p_i distinct simple roots,
- $v_{i1}, \dots, v_{iq_i}$ are the q_i distinct multiple roots of orders, say $m_{i1}, \dots, m_{iq_i}$, non divisible by e_i,
- $w_{i1}, \dots, v_{is_i}$ are the s_i distinct multiple roots of orders, say $n_{i1}, \dots, n_{iq_i}$, divisible by e_i.

Then we have

$$p_i + \sum_{j=1}^{q_i} m_{ij} + \sum_{j=1}^{s_i} n_{ij} = N, \quad i = 1, \dots, r, \tag{1}$$

$$\sum_{i=1}^{r} \left(\sum_{j=1}^{q_i} (m_{ij} - 1) + \sum_{j=1}^{s_i} (n_{ij} - 1) \right) \leq 2N - 2. \tag{2}$$

Equality (1) is clear. As to (2), it follows from the fact (left to the reader [19]) that if $u \in \mathbb{C}$ is root of $a(U) - t_i b(U)$ of order $m \geq 1$ for some $i = 1, \ldots, r$, then u is a root of order $m-1$ of the polynomial $a'b - ab'$, which is of degree $2N-2$. An alternate argument consists in applying the Riemann-Hurwitz formula to the branched cover $T_0 : \mathbb{P}^1 \to \mathbb{P}^1$ induced by the rational function $T_0(U)$: the left-hand side term from (2) is smaller than or equal to the term $\sum_P (e_P - 1)$ of this formula (where P ranges over all ramified points) and so is $\leq 2 \cdot 0 - 2 + 2\deg(T_0) = 2N - 2$.

Statement (*) gives

$$r_{T_0} = \sum_{i=1}^{r} (p_i + q_i).$$

Clearly $r_{T_0} \leq rN$ follows. Inequality (2), conjoined with (1), rewrites

$$\sum_{i=1}^{r} (N - p_i - q_i - s_i) \leq 2N - 2$$

so we obtain

$$r_{T_0} \geq (r-2)N + 2 - \sum_{i=1}^{r} s_i. \tag{***}$$

From (1), for $i = 1, \ldots, r$, we also have $p_i + q_i + e_i s_i \leq N$, whence

$$s_i \leq \frac{N}{e_i} - \frac{p_i + q_i}{e_i}.$$

The definition of e_∞ and ε leads to

$$r_{T_0} \geq rN - (2N-2) - \varepsilon N + \frac{1}{e_\infty} \sum_{i=1}^{r} (p_i + q_i)$$

and finally to inequality (b-1).

From (2) we can also deduce that

$$\sum_{i=1}^{r} s_i \leq 2N - 2$$

which conjoined with (***), yields inequality (b-2).

(d) Write the Riemann-Hurwitz formula for $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(U)$:

$$\begin{cases} 2g - 2 = -2d + \sum_F (e_{\mathscr{P}} - 1) \\ 2g_{T_0} - 2 = -2d_{T_0} + \sum_{F_{T_0}} (e_{\mathscr{P}} - 1) \end{cases}$$

where $\sum_F$ (resp. $\sum_{F_{T_0}}$) means that the sum ranges over all places of F (resp. of F_{T_0}) trivial on $\mathbb{C}$. The first claim from (d) comes from

$$g_{T_0} = 1 - d_{T_0} + \frac{1}{2} \sum_{F_{T_0}} (e_{\mathscr{P}} - 1) \leq \frac{N}{2} \sum_{F} (e_{\mathscr{P}} - 1) = N(g - 1 + d).$$

[19] With this hint: if $a^{(k)}(u) - t_i b^{(k)}(u) = 0$ for $k = 0, \ldots, m-1$, then $a^{(h)}(u) b^{(k)}(u) - a^{(k)}(u) b^{(h)}(u) = 0$ for $h, k = 0, \ldots, m-1$. The claim follows from the observation that every derivative $(a'b - ab')^{(h)}$ $(h = 0, \ldots, m-2)$ is a sum of terms of the form $a^{(h)} b^{(k)} - a^{(k)} b^{(h)}$ with $h, k = 0, \ldots, m-1$.

As $F/\mathbb{C}(T)$ is Galois, we also have

$$\sum_{F}(e_{\mathcal{P}}-1)=\sum_{i=1}^{r}\sum_{\mathcal{P}/t_i}(e_i-1)=\sum_{i=1}^{r}\left(d-\frac{d}{e_i}\right).$$

Assume $G_{T_0} = G$, so $d_{T_0} = d$. Our analysis of the branch points of the specialized extension $F_{T_0}/\mathbb{C}(U)$ yields:

$$\sum_{F_{T_0}}(e_{\mathcal{P}}-1)\geq\sum_{i=1}^{r}\left(d-\frac{d}{e_i}\right)p_i$$

whence

$$g_{T_0}-g\geq\frac{1}{2}\sum_{i=1}^{r}\left(d-\frac{d}{e_i}\right)(p_i-1).$$

Now we have, for each $i = 1,\dots,r$,

$$\begin{aligned}p_i&=N-\sum_{j=1}^{q_i}m_{ij}-\sum_{j=1}^{s_i}n_{ij}\\&\geq N-2\left(\sum_{j=1}^{q_i}(m_{ij}-1)+\sum_{j=1}^{s_i}(n_{ij}-1)\right).\end{aligned}$$

We deduce:

$$\begin{aligned}g_{T_0}-g&\geq\frac{1}{2}\sum_{i=1}^{r}(d-\frac{d}{e_i})\left(N-1-2(\sum_{j=1}^{q_i}(m_{ij}-1)+\sum_{j=1}^{s_i}(n_{ij}-1))\right)\\&\geq\frac{d}{4}\left(r(N-1)-2(2N-2)\right)\\&=\frac{d}{4}(N-1)(r-4).\end{aligned}$$

Finally we explain how to reduce to a situation for which assumption (H) is satisfied. Note first that the parameters $r, d, g, \mathbf{C}$ are unchanged if the extension $F/\mathbb{C}(T)$ is replaced by any extension $F_\chi/\mathbb{C}(T)$ with $\chi\in\mathbb{C}(T)$ of degree 1.

For some fixed $\theta_0\in\mathbb{C}\setminus\{t_1,\dots,t_r\}$, consider the linear fractional transformation χ defined by

$$\chi^{-1}(T)=\frac{\tau T+\mu}{T-\theta_0},$$

where τ,μ are chosen in $\mathbb{C}$ so that the complex numbers $\chi^{-1}(t_1),\dots,\chi^{-1}(t_r)$ are different from ∞; such a choice is possible as $\mathbb{C}$ is infinite. These r complex numbers are the branch points of the extension $F_\chi/\mathbb{C}(T)$, and so these branch points are different from ∞. Fix then a second linear fractional transformation χ' such that $T_0(\chi'(\infty))\notin\{t_1,\dots,t_r\}$. By construction the extension $F_\chi/\mathbb{C}(T)$ and the rational function $\chi^{-1}\circ T_0\circ\chi'$ satisfy the assumption (H). Therefore the conclusions from Theorem 3.1 comparing the ramification invariants of the specialized extension

$$(F_\chi)_{\chi^{-1}\circ T_0\circ\chi'}/\mathbb{C}(U)=F_{T_0\circ\chi'}/\mathbb{C}(U)$$

with those of $F_\chi/\mathbb{C}(T)$ are satisfied. These conclusions hold as well for the invariants of the specialized extension $F_{T_0}/\mathbb{C}(U)$ compared to those of $F/\mathbb{C}(T)$ since $F_{T_0}/\mathbb{C}(U)$ (resp. $F/\mathbb{C}(T)$) is obtained from $F_{T_0\circ\chi'}/\mathbb{C}(U)$ (resp. $F_\chi/\mathbb{C}(T)$) by composition with an automorphism of $\mathbb{C}(U)$ (resp. an automorphism of $\mathbb{C}(T)$). □

In the next subsections, we explain how Theorem 2.1 can be deduced from Theorem 3.1.

3.2. Proof of Theorem 2.1(a)

Assume $g \geq 1$ and let $L/\mathbb{C}(T)$ be a Galois extension such that $F/\mathbb{C}(T) \prec L/\mathbb{C}(T)$, i.e., there exists $T_0 \in \mathbb{C}(U) \setminus \mathbb{C}$ such that $L/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$. As in § 3.1 denote the invariants of $F_{T_0}/\mathbb{C}(T)$ by $G_{T_0}, r_{T_0}, g_{T_0}, \mathbf{C}_{T_0}$.

We already know that $G \supset G_{T_0}$ and $\mathbf{C} \prec \mathbf{C}_{T_0}$ (Theorem 3.1 (a), (c)).

Next we show that $r_{T_0} \geq r$. We may assume that $N \geq 2$.

A first case is when $r \geq 4$: $r_{T_0} \geq r$ follows from Theorem 3.1 (b-2).

From Theorem 3.1 (b-1), if $\varepsilon \leq (r-1)/2$ and $r \geq 3$ we have:

$$r_{T_0} > (r - \frac{r-1}{2} - 2)N + 2 \geq 2\left(\frac{r}{2} - \frac{3}{2}\right) + 2 = r - 1.$$

In particular, for $r = 3$, we have $r_{T_0} \geq r$ if $\varepsilon \leq 1$. A simple check shows that the following 3-tuples $\mathbf{e}$:

$$(2,2,2),\ (2,3,3),\ (2,3,4),\ (2,3,5),\ (2,2,e), \quad (e \geq 3)$$

are exactly those for which $\varepsilon > 1$ and that $g = 0$ in these cases.

We are left with the case $r = 2$. But then $F/\mathbb{C}(T)$ is a cyclic extension with two branch points and hence $g = 0$. This ends the proof of the inequality $(G, r, \mathbf{C}) \prec (G_{T_0}, r_{T_0}, \mathbf{C}_{T_0})$ when $g \geq 1$.

Assume next $G_{T_0} = G$. The above inequality then also holds if $g = 0$. The only non-trivial point is $r_{T_0} \geq r$. We know that $r_{T_0} < r$ possibly happens only when $r \leq 3$ and $g = 0$ and in this case $r_{T_0} < r$ means that either $r_{T_0} = 0$ in which case $F_{T_0} = \mathbb{C}(T)$ and then $G_{T_0} = \{1\} \neq G$, or, $r_{T_0} = 2$ in which case $F_{T_0}/\mathbb{C}(T)$ is cyclic, and then again $G_{T_0} \neq G$. Indeed, in this last case, G cannot be cyclic as $r = 3$, $g = 0$ and a cyclic group has no generating set $\{g_1, g_2, g_3\}$ such that $g_1g_2g_3 = 1$ and with respective orders those in one of the above triples $\mathbf{e}$. Finally it immediately follows from Theorem 3.1 (d) that $g_{T_0} \geq g$ if $r \geq 4$.

Remark 3.3. – If F is of genus 0 and $G_{T_0} \neq G$, $r_{T_0} < r$ may happen. One may then have $G_{T_0} = \{1\}$ or not (see Example 3.3.2).

3.3. The exceptional genus 0 cases

The Riemann-Hurwitz formula

$$2g-2=-2d+\sum_{i=1}^{r}(e_i-1)\frac{d}{e_i}$$

where $d=|G|$, in a Galois situation yields

$$2g-2=d(r-2-\varepsilon).$$

As $\varepsilon\le r/2$ we have $2g-2\ge d(\frac{r}{2}-2)$, and if $\varepsilon\le(r-1)/2$, we have $2g-2\ge\frac{d}{2}(r-3)$. Hence if $g=0$, then ($r=3$ and $\varepsilon>1$) or ($r\le 2$).

Conclude that if $g=0$ we necessarily are in one of these cases:

(1) $r=3$ *and* $\mathbf{e}\in\{(2,2,2),(2,3,3),(2,3,4),(2,3,5),(2,2,n),\ (n\ge 3)\}$
with corresponding groups $(\mathbb{Z}/2\mathbb{Z})^2$, A_4, S_4, A_5, D_{2n} $(n\ge 3)$.
(2) $r\le 2$ *then* $F/\mathbb{C}(T)$ *is a cyclic extension.*

Namely, a simple calculation shows that the tuples $\mathbf{e}$ are the indicated ones. Concerning the corresponding groups, note first that, as F is of genus 0, G must be a subgroup of $\mathrm{PGL}_2(\mathbb{C})$ and so one of the proposed list. The case $r=2$ is clear. Assume $r=3$. Then G cannot be cyclic. For $\mathbf{e}=(2,2,2)$, G is generated by two involutions with product an involution, so $G=(\mathbb{Z}/2\mathbb{Z})^2$. Similarly one obtains D_{2n} (dihedral group of order $2n$) if $\mathbf{e}=(2,2,n)$ $(n\ge 3)$. If $\mathbf{e}=(2,3,4)$ G must be S_4 as it cannot be any of the others. We obtain similarly that $G=A_4$ if $\mathbf{e}=(2,3,3)$ and $G=A_5$ if $\mathbf{e}=(2,3,5)$.

Next we show that in all these cases, if r distinct points $t_1,\dots,t_r\in\mathbb{P}^1(\mathbb{C})$ are fixed ($r=2$ or $r=3$), there is one and only one Galois extension $F/\mathbb{C}(T)$ of group G, ramification indices $\mathbf{e}=(e_1,\dots,e_r)$ and branch points $t_1,\dots,t_r$. Furthermore, as PGL_2 is 3-transitive on $\mathbb{P}^1(\mathbb{C})$, up to isomorphism, there is exactly one extension $F/\mathbb{C}(T)$ in each case.

From Proposition 2.4, this unique extension $F/\mathbb{C}(T)$ of group G in each case is $\mathbb{C}(U)$-parametric.

Concerning uniqueness, one checks first that up to some (anti-)isomorphism of G (which does not change the Galois extension $F/\mathbb{C}(T)$), there is, for each r-tuple $\mathbf{e}$, a unique possible r-tuple $\mathbf{C}=(C_1,\dots,C_r)$ and second, that this r-tuple is *rigid*, that is: there is a unique r-tuple $(g_1,\dots,g_r)\in C_1\times\cdots\times C_r$ such that $\langle g_1,\dots g_r\rangle=G$ and $g_1\cdots g_r=1$, up to component-wise conjugation by an element of G. It then classically follows from the Riemann Existence Theorem that there is one and only one Galois extension $F/\mathbb{C}(T)$ as desired if in addition the branch points are fixed.

Below we produce in each case an example of an extension $F/\mathbb{C}(T)$ with the given invariants.

3.3.1. – $r=2$, $G=\mathbb{Z}/d\mathbb{Z}$ with $d\ge 1$: $\mathbb{C}(\sqrt[d]{T})/\mathbb{C}(T)$ is a Galois extension of group $\mathbb{Z}/d\mathbb{Z}$ branched at 0 and ∞ with ramification indices d.

3.3.2. – $\mathbf{e} = (2,2,2)$, $G = (\mathbb{Z}/2\mathbb{Z})^2$: for $F = \mathbb{C}(\sqrt{T}, \sqrt{T-1})$, $F/\mathbb{C}(T)$ is a Galois extension of group $(\mathbb{Z}/2\mathbb{Z})^2$. A primitive element of $F/\mathbb{C}(T)$ is for example $\sqrt{T} + \sqrt{T-1}$. An affine equation is the polynomial $Y^4 + 2(1-2T)Y^2 + 1$. There are three branch points: 0, 1 and ∞, which all are of index 2. For $T_0 = T^2$, we have $F_{T_0} = \mathbb{C}(T, \sqrt{T^2-1})$ whose branch points are 1 and -1.

For the other cases, we produce a generating set of G of 3 elements g_1, g_2, g_3 of orders e_1, e_2, e_3 and such that $g_1g_2g_3 = 1$.

3.3.3. – $\mathbf{e} = (2,3,3)$, $G = A_4$: take

$$g_1 = (12)(34),\ g_2 = (123),\ g_3 = (234).$$

3.3.4. – $\mathbf{e} = (2,3,4)$, $G = S_4$: take

$$g_1 = (12),\ g_2 = (234),\ g_3 = (4321).$$

(The conjugacy classes of g_1, g_2, g_3 in S_4 being "rational," a standard argument shows further that, if one fixes the three branch points in $\mathbb{P}^1(\mathbb{Q})$, the unique corresponding extension $F/\mathbb{C}(T)$ is defined over $\mathbb{Q}$.)

3.3.5. – $\mathbf{e} = (2,3,5)$, $G = A_5$: take

$$g_1 = (15)(34),\ g_2 = (124),\ g_3 = (54321).$$

3.3.6. – $\mathbf{e} = (2,2,n)$, $e \geq 3$, $G = D_{2n}$: take g_1, g_2 two involutions with $g_1g_2 = g_3^{-1}$ generating the normal cyclic subgroup. For n odd, an explicit example is the Galois extension $F/\mathbb{C}(T)$ with affine equation $Y^{2n} - TY^n + 1$ which is branched at 2, -2, ∞ with ramification indices 2, 2 and n. As it is $\mathbb{C}(U)$-parametric, it follows from the uniqueness conclusion of Theorem 2.1 (b) that it is isomorphic to the Hashimoto-Mihake generic extension for D_{2n} mentioned in Remark 2.6.

3.4. Theorem 2.1 (b)

3.4.1. *A preliminary lemma.* – Retain the notation already introduced for Theorem 2.1 (a).

LEMMA 3.4. – *When $N = \deg(T_0) > 1$, we have $r_{T_0} > r$ in each of the following cases:*

(a) *$r \geq 5$,*
(b) *$F \neq \mathbb{C}(T)$ and $\varepsilon \leq (r-2)/2$,*
(c) *$N \geq 4$, $r = 4$ and $\varepsilon \leq 3/2$,*
(d) *$N \geq 4$, $r = 3$ and $\varepsilon \leq 3/4$.*

Proof. – Assume $N > 1$. If $r \geq 5$ as in (a), Theorem 3.1 (b-2) gives

$$r_{T_0} \geq (r-4)N + 4 \geq 2r - 4 > r$$

From Theorem 3.1 (b-1), we have

$$(*) \qquad r_{T_0} > (r - \varepsilon - 2)N + 2.$$

Under the assumptions of (b), we deduce

$$r_{T_0} > (\frac{r}{2} - 1)N + 2 \geq (\frac{r}{2} - 1)2 + 2 = r.$$

Finally $r_{T_0} > r$ easily follows from (*) above in the last two cases (c) and (d). □

3.4.2. *Proof of Theorem 2.1 (b)*. – The only non-trivial point is the antisymmetry of $\prec$. Let $F/\mathbb{C}(T)$ and $F'/\mathbb{C}(T)$ be two non-isomorphic extensions in the set $\mathcal{E}^*$ such that $F/\mathbb{C}(T) \prec F'/\mathbb{C}(T)$ and $F'/\mathbb{C}(T) \prec F/\mathbb{C}(T)$. Let $T_0, T_0' \in \mathbb{C}(T)$ such that $F'/\mathbb{C}(T) = F_{T_0}/\mathbb{C}(T)$ and $F/\mathbb{C}(T) = F'_{T_0'}/\mathbb{C}(T)$ with $\deg(T_0) \geq 2$ and $\deg(T_0') \geq 2$. From Theorem 2.1 (a), $F/\mathbb{C}(T)$ and $F'/\mathbb{C}(T)$ have the same group G, the same branch point number r, the same powered conjugacy classes $C_1^{\mathbb{Z}}, \dots, C_r^{\mathbb{Z}}$ and, as a consequence, the same ramification indices $\mathbf{e}$ and the same genus g. We also have $F_{T_0T_0'}/\mathbb{C}(T) = F/\mathbb{C}(T)$.

Recall that $F/\mathbb{C}(T) \in \mathcal{E}^*$ means one of the following situations holds:

(a) G is of rank ≥ 4,
(b) G is of rank 3 and of odd order,
(c) G is of rank 2 and order non divisible by 2 or 3,
(d) F is of genus $g = 0$.

Each of the first three conditions further implies that

$$(*) \qquad r \geq 5 \text{ or } (r = 4 \text{ and } \varepsilon \leq \frac{4}{3} \leq \frac{3}{2}) \text{ or } (r = 3 \text{ and } \varepsilon \leq \frac{3}{5} \leq \frac{3}{4}).$$

In the three cases, Lemma 3.4 (applied with $N = \deg(T_0T_0') \geq 4$) yields a contradiction to $r_{T_0T_0'} = r$.

Suppose as in (d) that F is of genus 0. Then $F/\mathbb{C}(T)$ is one of the exceptional extensions described in § 3.3. But then so is $F'/\mathbb{C}(T)$ as it has the same invariants G, r, $\mathbf{e}$, g, and again from § 3.3, it must be isomorphic to $F/\mathbb{C}(T)$, a contradiction.

Remark 3.5. – This last argument also shows the uniqueness conclusion for $\mathbb{C}(U)$-parametric extensions $F/\mathbb{C}(T)$ when $G \subset \mathrm{PGL}_2(\mathbb{C})$: since G has a realization $F/\mathbb{C}(T)$ with $g_F = 0$ and that such a realization is $\mathbb{C}(U)$-parametric (Proposition 2.4), the argument gives that any other $\mathbb{C}(U)$-parametric extension $F'/\mathbb{C}(T)$ of G (which satisfies $F'/\mathbb{C}(T) \prec F/\mathbb{C}(T)$ and $F/\mathbb{C}(T) \prec F'/\mathbb{C}(T)$) is isomorphic to $F/\mathbb{C}(T)$.

Finally fix a group $G \in \mathcal{G}^*$ but not a subgroup of $\mathrm{PGL}_2(\mathbb{C})$. Then all Galois extensions $L/\mathbb{C}(T)$ of group G are in $\mathcal{E}^*$ and a $\mathbb{C}(U)$-parametric extension $F/\mathbb{C}(T)$ of group G is the smallest such extension for the order $\prec$, hence is unique.

3.4.3. *An example*. – Here is an example for which we have

$$(G, r, g, \mathbf{C}) = (G_{T_0}, r_{T_0}, g_{T_0}, \mathbf{C}_{T_0})$$

but $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are not isomorphic, and so $N > 1$. We do not know whether an example exists for which $F/\mathbb{C}(T)$ could additionally be shown to be a specialization of $F_{T_0}/\mathbb{C}(T)$ (which would show that the pre-order $\prec$ is not an order).

Take $G = D_{2n}$ with n odd and $F/\mathbb{C}(T)$ a Galois extension of group G with branch points $0, 1, -1, \lambda$ with $\lambda \in \mathbb{C} \setminus \{0, \pm 1\}$ and ramification indices $\mathbf{e} = (2, 2, 2, 2)$; such an extension exists from the RET and the easy construction of a generating set of G of four elements $g_1, \dots, g_4$ of order 2 and such that $g_1 \cdots g_4 = 1$.

Take $T_0(U) = U^2/(2U^2 - 2U + 1)$. One checks that $T_0(u) = 0$ has a double root, $u = 0$, and that $T_0(u) = 1$ has a double root, $u = 1$. It follows that both $T_0(u) = -1$ and $T_0(u) = \lambda$ have two distinct roots (because of inequality (2) of the proof of Theorem 3.1). From the analysis of the ramification in specialized extensions in the proof of Theorem 3.1

(more particularly from (*) and (**)), we obtain that $F_{T_0}/\mathbb{C}(T)$ has $r_{T_0} = 4$ branch points, with ramification indices 2.

The extensions $F/\mathbb{C}(T)$ and $F_{T_0}/\mathbb{C}(T)$ are not isomorphic. Otherwise the cross-ratio of their branch points would be equal, up to the sign. The cross-ratio of $0, 1, -1, \lambda$ is $(\lambda - 1)/(2\lambda)$. The branch points of $F_{T_0}/\mathbb{C}(T)$ are the simple roots of $T_0(u) = 1$ and $T_0(u) = \lambda$. Take for example $\lambda = 1/5$. These four points are then $(1 \pm \sqrt{-2})/3$, -1 and $1/3$. A final computation shows the corresponding cross-ratio is $(16 + 4\sqrt{-2})/9$ while $(\lambda - 1)/(2\lambda) = -2$.

Assume $G_{T_0} \neq G$. From Theorem 3.1 (a), there exists a sub-extension $L/\mathbb{C}(T)$ of $F/\mathbb{C}(T)$ such that $L \neq \mathbb{C}(T)$, $L_{T_0} = \mathbb{C}(T)$ and L of genus 0. Write $L = \mathbb{C}(\theta)$ for some $\theta \in F$ and $T = A(\theta)/B(\theta)$ with $A, B \in \mathbb{C}[X]$ relatively prime, $B \neq 0$. The irreducible polynomial of θ over $\mathbb{C}(T)$ is $A(Y) - TB(Y)$. Then $L_{T_0} = \mathbb{C}(U)$ means that $A(Y) - T_0(U)B(Y)$ has a root $Y_0(U) \in \mathbb{C}(U)$. But then we have $T_0(U) = A(Y_0(U))/B(Y_0(U))$. As we explain in the last paragraph, T_0 is indecomposable so necessarily $A/B = T_0$ and so L does not depend on λ. The next paragraph provides a contradiction by showing that L is ramified over λ.

The Galois group $\mathrm{Gal}(F/L)$ cannot be a subgroup of the cyclic subgroup of order n of D_{2n}: otherwise, with $d_L = [L : \mathbb{C}(T)]$, the Riemann-Hurwitz formula yields $-2 = -2d_L + 4d_L/2$, a contradiction. Therefore L is the fixed field in F of some involution of D_{2n}. The Riemann-Hurwitz formula gives: $-2 = -2n + R$ where R is the number of ramified primes. Conclude that above each of $0, 1, -1, \lambda$, the number of ramified points is the maximum possible: $(n - 1)/2$.

That T_0 is indecomposable is an exercise for which we only indicate the main steps. Deduce from $T_0(U) = A(Y_0(U))/B(Y_0(U))$ that $A(Y_0(U)) = K(U)U^2$ and $B(Y_0(U)) = K(U)(2U^2 - 2U + 1)$ for some $K \in \mathbb{C}(U)$. Writing $Y_0(U) = \alpha(U)/\beta(U)$ with $\alpha, \beta \in \mathbb{C}[U]$ relatively prime, show next that necessarily $Y_0(U) \in \mathbb{C}[U]$ and $K(U) \in \mathbb{C}$. The desired conclusion easily follows.

4. Twisting regular Galois extensions in families

Here k-regular extensions $F/k(T)$ are viewed as fundamental group representations, as recalled in § 4.1. § 4.2 recalls the twisting operation on covers and the twisting lemma (§ 4.2.1). § 4.3 explains how the twisting lemma can be used "in family". § 4.4 states Theorem 4.2, which is the main result of this section; Theorem 2.16 is a special case. Theorem 4.2 is proved in § 4.5.

4.1. Fundamental groups representations

The absolute Galois group of a field K is denoted by G_K. If E/K is a Galois extension of group G, an epimorphism $\varphi : \mathrm{G}_K \to G$ such that E is the fixed field of $\ker(\varphi)$ in $\overline{K}$ is a called a G_K-*representation* of E/K.

Given a finite subset $\mathbf{t} \subset \mathbb{P}^1(\overline{K})$ invariant under G_K, the K-fundamental group of $\mathbb{P}^1 \setminus \mathbf{t}$ is denoted by $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$; here t denotes a fixed *base point*, which corresponds to choosing an embedding of $K(T)$ in an algebraically closed field Ω. The (geometric) $\overline{K}$-fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ is defined as the Galois group of the maximal algebraic extension $\Omega_{\mathbf{t},K}/\overline{K}(T)$ (inside Ω) unramified above $\mathbb{P}^1 \setminus \mathbf{t}$ and the (arithmetic) K-fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ as the group of the Galois extension $\Omega_{\mathbf{t},k}/K(T)$.

Degree d K-regular extensions $F/K(T)$ (resp. K-regular Galois extensions $F/K(T)$ of group G) with branch points in $\mathbf{t}$ correspond to transitive homomorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to S_d$ (resp. to epimorphisms $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_K, t) \to G$), with the extra regularity condition that the restriction of ϕ to $\pi_1(\mathbb{P}^1 \setminus \mathbf{t})_K, t)_{\overline{K}}$ remains transitive (resp. remains onto). These corresponding homomorphisms are called the *fundamental group representations* (or π_1*-representations* for short) of the K-regular (resp. K-regular Galois) extension $F/K(T)$.

Each K-rational point $t_0 \in \mathbb{P}^1(K)\setminus\mathbf{t}$ naturally provides a section $\mathsf{s}_{t_0} : \mathrm{G}_K \to \pi_1(\mathbb{P}^1\setminus\mathbf{t}, t)_K$ to the exact sequence

$$1 \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to \mathrm{G}_K \to 1$$

which is uniquely defined up to conjugation by an element in the fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$.

If $\phi : \pi_1(\mathbb{P}^1\setminus\mathbf{t}, t)_K \to G$ represents a K-regular Galois extension $F/K(T)$, the morphism $\phi\circ\mathsf{s}_{t_0} : \mathrm{G}_K \to G$ is the *specialized representation* of ϕ at t_0. The fixed field in $\overline{K}$ of $\ker(\phi\circ\mathsf{s}_{t_0})$ is the specialized extension F_{t_0}/K of $F/K(T)$ at t_0.

4.2. Twisting regular Galois extensions

For this subsection, we refer to [9].

4.2.1. *The twisting lemma.* – Fix a field K and a K-regular Galois extension $\mathcal{F}/K(T)$ of group G, also viewed as a K-regular Galois cover $f : X \to \mathbb{P}^1$. Recall how it can be twisted by a Galois extension E/K of group $H \subset G$. Formally this is done in terms of the associated π_1-and G_K-representations.

Let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to G$ be a π_1-representation of $\mathcal{F}/K(T)$ and $\varphi : \mathrm{G}_K \to G$ be a G_K-representation of the Galois extension E/K.

Denote the right-regular (resp. left-regular) representation of G by $\delta : G \to S_d$ (resp. by $\gamma : G \to S_d$) where $d = |G|$. Consider the map

$$\widetilde{\phi}^{\varphi} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to S_d$$

defined by the following formula, where R is the restriction map $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to \mathrm{G}_K$ and $\times$ is the multiplication in the symmetric group S_d:

$$\widetilde{\phi}^{\varphi}(\Theta) = \gamma(\phi(\Theta)) \times \delta(\varphi(R(\Theta))^{-1}) \qquad (\Theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K). \tag{*}$$

The map $\widetilde{\phi}^{\varphi}$ is a group homomorphism with the same restriction on $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ as ϕ. It is called the *twisted representation* of ϕ by φ.

The associated K-regular extension is denoted by $\widetilde{\mathcal{F}}^{\varphi}/K(T)$ and called the *twisted extension* of $\mathcal{F}/K(T)$ by φ. The field $\widetilde{\mathcal{F}}^{\varphi}$ is the fixed field in $\Omega_{\mathbf{t},K}$ of the subgroup $\Gamma \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ of all Θ such that $\widetilde{\phi}^{\varphi}(\Theta)$ fixes the neutral element of G[20]. Finally the corresponding K-regular cover, the *twisted cover* of f by φ, is denoted by $\widetilde{f}^{\varphi} : \widetilde{X}^{\varphi} \to \mathbb{P}^1$.

The following statement is the main property of the twisted cover.

Twisting lemma 4.1. – *Let* $t_0 \in \mathbb{P}^1(K) \setminus \mathbf{t}$. *The specialization representation* $\phi \circ \mathsf{s}_{t_0} : \mathrm{G}_K \to G$ *is conjugate in* G *to* $\varphi : \mathrm{G}_K \to G$ *if and only if there exists* $x_0 \in \widetilde{X}^{\varphi}(K)$ *such that* $\widetilde{f}^{\varphi}(x_0) = t_0$.

[20] Taking any other element of G gives the same field up to $K(T)$-isomorphism.

As a first illustration, we can prove Proposition 2.4, which we have used several times.

Proof of Proposition 2.4. – Let $F/\mathbb{C}(T)$ be a Galois extension of group G with F of genus 0 and $L/\mathbb{C}(U)$ be a Galois extension of group $H \subset G$. Let $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\mathbb{C}(U)} \to G$ be a π_1-representation of $F\mathbb{C}(U)/\mathbb{C}(U)(T)$ and $\varphi : \mathrm{G}_{\mathbb{C}(U)} \to H \subset G$ be a $\mathrm{G}_{\mathbb{C}(U)}$-representation of the Galois extension $L/\mathbb{C}(U)$. Set $\mathscr{F} = F\mathbb{C}(U)$ and consider the twisted extension $\widetilde{\mathscr{F}}^{\varphi}/\mathbb{C}(U)(T)$ and the associated twisted cover $\widetilde{X}^{\varphi} \to \mathbb{P}^1$. The extension $\mathscr{F}\overline{\mathbb{C}(U)}/\overline{\mathbb{C}(U)}(T)$ and $F\overline{\mathbb{C}(U)}/\overline{\mathbb{C}(U)}(T)$ are $\overline{\mathbb{C}(U)}(T)$-isomorphic. Consequently $\widetilde{X}^{\varphi}$ is of genus 0. From Tsen's theorem, $\widetilde{X}^{\varphi}$ has a $\mathbb{C}(U)$-rational point and is isomorphic to $\mathbb{P}^1$ over $\mathbb{C}(U)$. Conclude thanks to Lemma 4.1 that $L/\mathbb{C}(U)$ is a $\mathbb{C}(U)$-specialization of $F/\mathbb{C}(T)$. □

It is a similar argument that proves that if K is a Pseudo Algebraically Closed field, then every K-regular Galois extension $F/K(T)$ is K-parametric [5, §3.3.1].

4.3. Twisting in families

Consider the twisted extension $\widetilde{\mathscr{F}}^{\varphi}/K(T)$ when $K = k(U)$ with k a field and U some indeterminate.

4.3.1. *Description of the twisted extension.* – Every element Θ in the K-fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$ uniquely writes $\Theta = \chi \mathsf{s}_U(\sigma)$ with $\chi \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$ and $\sigma \in \mathrm{G}_K$. Whence

$$\begin{cases} \phi(\Theta) = \phi(\chi)\phi(\mathsf{s}_U(\sigma)) \\ \varphi(R(\Theta)) = \varphi(\sigma) \end{cases}$$

and the following formula, where, by $\mathrm{conj}(g)$ ($g \in G$), we denote the permutation of G induced by the conjugation $x \to gxg^{-1}$:

$$\widetilde{\phi}^{\varphi}(\Theta) = \gamma(\phi(\chi)\phi(\mathsf{s}_U(\sigma))\varphi(\sigma)^{-1}) \times \mathrm{conj}(\varphi(\sigma)).$$

Conclude that the field $\widetilde{\mathscr{F}}^{\varphi}$ is the fixed field in $\Omega_{\mathbf{t},K}$ of the following subgroup $\Gamma \subset \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K$:

$$\Gamma = \{\chi \mathsf{s}_U(\sigma) \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K | \phi(\chi) = \varphi(\sigma)\phi(\mathsf{s}_U(\sigma))^{-1}\}.$$

4.3.2. *The fiber-twisted cover at u_0.* – The two extensions $\mathscr{F}/K(T)$ and $\widetilde{\mathscr{F}}^{\varphi}/K(T)$ are K-regular. From the Grothendieck good reduction theorem (§ 5), for every $u_0 \in k$ but in a finite subset $\mathscr{E}$, they specialize at $U = u_0$ to respective extensions $\mathscr{F}|_{u_0}/k(T)$ and $(\widetilde{\mathscr{F}}^{\varphi})|_{u_0}/k(T)$ that are k-regular of degree

$$[\widetilde{\mathscr{F}}^{\varphi} : k(U)(T)] = [\mathscr{F} : K(T)] = d,$$

have branch point set $\mathbf{t}_{u_0}$ and have the same genus as the common genus of the function fields $\mathscr{F}$ and $\widetilde{\mathscr{F}}^{\varphi}$. More specifically, one can take for $\mathscr{E}$ the set of $u_0 \in k$ that are bad for $\mathscr{F}/k(U)(T)$ or ramified in the extension $E/k(U)$ [21].

Using the embedding of $\overline{k(U)}$ in the field of Puiseux series in $U - u_0$ and coefficients in $\overline{k}$, we have a natural monomorphism

$$\mathsf{s}_{u_0} : \mathrm{G}_k \to \mathrm{G}_K.$$

[21] Assumption (1) from § 5 is satisfied as k is of characteristic $\mathbf{0}$ and u_0 unramified in $E/k(U)$ guarantees that u_0 is good for $\widetilde{\mathscr{F}}^{\varphi}/k(U)(T)$ if it is good for $\mathscr{F}/k(U)(T)$.

The morphism $\varphi \circ \mathsf{s}_{u_0} : \mathrm{G}_k \to G$ is well-defined and so is the twisted extension

$$\left(\widetilde{\mathscr{F}|_{u_0}}\right)^{\varphi \circ \mathsf{s}_{u_0}} / k(T).$$

We call it the *fiber-twisted extension* at u_0. If $\phi|_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \to G$ is a π_1-representation of the k-regular Galois extension $\mathscr{F}|_{u_0}/k(T)$, then a π_1-representation of the twisted extension above is

$$\widetilde{\phi|_{u_0}}^{\varphi \circ \mathsf{s}_{u_0}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \to S_d.$$

Every element $\theta \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_k$ uniquely writes $\theta = x\mathsf{s}_{u_0}(\tau)$ with $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{k}}$ and $\tau \in \mathrm{G}_k$. Similarly as in §4.3.1 we obtain:

$$\widetilde{\phi|_{u_0}}^{\varphi \circ \mathsf{s}_{u_0}}(\theta) = \gamma\left(\phi|_{u_0}(x)\phi|_{u_0}(\mathsf{s}_{u_0}(\tau)\right)\varphi(\mathsf{s}_{u_0}(\tau))^{-1}) \times \mathrm{conj}(\varphi(\mathsf{s}_{u_0}(\tau))).$$

The field $\left(\widetilde{\mathscr{F}|_{u_0}}\right)^{\varphi \circ \mathsf{s}_{u_0}}$ is the fixed field in $\Omega_{\mathbf{t}_{u_0},k}$ of the following subgroup Γ_{u_0} of $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k$:

$$\Gamma_{u_0} = \{x\mathsf{s}_{u_0}(\tau) | \phi|_{u_0}(x) = \varphi(\mathsf{s}_{u_0}(\tau))\phi|_{u_0}(\mathsf{s}_{u_0}(\tau))^{-1}\}.$$

4.4. Comparison statement and proof of Theorem 2.16

THEOREM 4.2. – *For all but finitely many $u_0 \in k$, the two extensions*

$$(\widetilde{\mathscr{F}^{\varphi}})|_{u_0}/k(T) \text{ and } \left(\widetilde{\mathscr{F}|_{u_0}}\right)^{\varphi \circ \mathsf{s}_{u_0}}/k(T)$$

are well-defined and are $k(T)$-isomorphic.

Before giving the proof (in §4.5), we explain how to deduce Theorem 2.16 from Theorem 4.2.

Proof of Theorem 2.16. – Consider the two k-regular Galois extensions $F/k(T)$ and $L/k(T)$ given in Theorem 2.16. Let then $\mathscr{F}/K(T)$ be the K-regular extension deduced from $F/k(T)$ by scalar extension from k to $K = k(U)$. Denote the K-cover corresponding to $\mathscr{F}/K(T)$ by $f : X \to \mathbb{P}^1_K$, a π_1-representation by $\phi : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_K \to G$ and let $\varphi : \mathrm{G}_K \to H \subset G$ be a G_K-representation of the extension E/K obtained by specializing $LK/K(T)$ at $T = U \in K$.

Denote the distinct automorphisms of the group H by $\chi_1, \dots, \chi_N$ and set $\varphi_i = \chi_i \circ \varphi : \mathrm{G}_K \to H \subset G$, $i = 1, \dots, N$. We will prove Theorem 2.16 with $\widetilde{f_i} : \widetilde{X_i} \to \mathbb{P}^1_{k(U)}$ taken to be twisted cover $\widetilde{f}^{\varphi_i} : \widetilde{X}^{\varphi_i} \to \mathbb{P}^1_{k(U)}$, $i = 1, \dots, N$. By construction, conclusion (a) from Theorem 2.16 holds.

Fix an element $u_0 \in k$ not in the finite list of exceptions for Theorem 4.2; the case $u_0 = U$ is even easier. Fix a $t_0 \in \mathbb{P}^1(k)$ not a branch point of $F/k(T)$. The extension L_{u_0}/k is k-isomorphic to the specialized extension F_{t_0}/k if and only if the two G_k-representations $\varphi_i \circ \mathsf{s}_{u_0}$ and $\phi|_{u_0} \circ \mathsf{s}_{t_0}$ are conjugate in G for some index $i = 1, \dots, N$. From the twisting Lemma 4.1, this is equivalent to existence of a k-rational point x on $(\widetilde{X|_{u_0}})^{\varphi_i \circ \mathsf{s}_{u_0}}$ above t_0; this point x is necessarily unramified in the cover $(\widetilde{f|_{u_0}})^{\varphi_i \circ \mathsf{s}_{u_0}}$ as the branch point set remains the original set $\mathbf{t}$. Theorem 4.2 concludes the proof: the k-cover $(\widetilde{X|_{u_0}})^{\varphi_i \circ \mathsf{s}_{u_0}} \to \mathbb{P}^1_k$ is equivalent to the k-cover $(\widetilde{X}^{\varphi_i})|_{u_0} \to \mathbb{P}^1_k$, $i = 1, \dots, N$. □

4.5. Proof of Theorem 4.2

Let $\mathscr{E}$ be the finite subset introduced in § 4.3.2 for the application of the Grothendieck good reduction theorem. Fix $u_0 \in k \setminus \mathscr{E}$. The two extensions from the statement of Theorem 4.2 are well-defined and have the same branch point set, namely $\mathbf{t}_{u_0}$. We will show that they are $k(T)$-isomorphic by showing that they have the same π_1-representations. We need to compare $\widetilde{\phi|_{u_0}}^{\varphi \circ \mathsf{s}_{u_0}}$ from § 4.3.2 and some π_1-representation, say

$$\widetilde{\phi}^{\varphi}|_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_k \to S_d$$

of the k-regular extension $(\widetilde{\mathscr{F}}^{\varphi})|_{u_0}/k(T)$.

As a first step, consider the restrictions of these π_1-representations to the geometric fundamental group $\pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_{\overline{k}}$. Recall that from the addendum to the Grothendieck good reduction theorem (§ 5), we have a specialization isomorphism

$$\mathrm{sp}_{u_0} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{u_0}, t)_{\overline{k}}$$

and that for all $x \in \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}}$, we have

$$\begin{cases} \phi|_{u_0}(x) = \phi \circ \mathrm{sp}_{u_0}^{-1}(x) \\ \widetilde{\phi}^{\varphi}|_{u_0}(x) = \widetilde{\phi}^{\varphi} \circ \mathrm{sp}_{u_0}^{-1}(x). \end{cases}$$

Using § 4.2.1 (*), we obtain

$$\widetilde{\phi}^{\varphi}|_{u_0}(x) = \gamma(\phi(\mathrm{sp}_{u_0}^{-1}(x))) = \gamma(\phi|_{u_0}(x)) = \widetilde{\phi|_{u_0}}^{\varphi \circ \mathsf{s}_{u_0}}(x).$$

To compare the restrictions to G_k of the two π_1-representations, first show the following.

Lemma 4.3. – *For all but finitely many $u_0 \in k$ and all $\tau \in \mathrm{G}_k$, we have*

$$\phi|_{u_0}(\mathsf{s}_{u_0}(\tau)) = \phi(\mathsf{s}_U \circ \mathsf{s}_{u_0}(\tau)).$$

Proof. – Namely, with $\mathscr{Y}_1$ a primitive element of $\mathscr{F}/K(T)$, which we may assume to be integral over $k[U, T]$, the right-hand side term corresponds to the action of $\mathsf{s}_{u_0}(\tau) \in \mathrm{G}_K$ on the d different K-conjugates

$$\mathscr{Y}_i = \sum_{n=0}^{\infty} b_{in}(U)(T - U)^n, \quad j = 1, \dots, d$$

of $\mathscr{Y}_1$, viewed in $\overline{K}((T - U))$; the action of $\mathsf{s}_{u_0}(\tau)$ is given by the action on the coefficients $b_{in}(U) \in \overline{K}$ $(n \geq 0)$.

From the Eisenstein theorem, there exists a polynomial $E(U) \in k[U]$, $E(U) \neq 0$, such that $E(U)^{n+1} b_{in}(U) \in k[U]$ for every $n \geq 0$, $i = 1, \dots, d$. Enlarge the set $\mathscr{E}$ to contain the roots of $E(U)$. Then $\mathscr{Y}_1, \dots, \mathscr{Y}_d$ can be specialized at $U = u_0$ to yield d formal power series in $\overline{k}[[T - u_0]]$

$$\mathscr{Y}_i|_{u_0} = \sum_{n=0}^{\infty} b_{in}(u_0)(T - u_0)^n, \quad j = 1, \dots, d.$$

If $\mathcal{E}$ is again enlarged to contain the roots of the bad prime divisor of the irreducible polynomial $P \in k[U,T,Y]$ of $\mathcal{Y}_1$ over $k(U,T)$ (§ 5), then $P(u_0,T,Y)$ is irreducible in $\overline{k}[T,Y]$; it is the irreducible polynomial of $\mathcal{Y}_1|_{u_0}$ and the extension $k(T,\mathcal{Y}_1|_{u_0})/k(T)$ is $k(T)$-isomorphic to the extension $\mathcal{F}|_{u_0}/K(T)$.

The left-hand side term $\phi|_{u_0}(\mathsf{s}_{u_0}(\tau))$ of the claimed formula corresponds to the action of $\tau \in \mathrm{G}_k$ on the d different $k(T)$-conjugates $\mathcal{Y}_1|_{u_0},\dots,\mathcal{Y}_d|_{u_0}$, with τ acting on the coefficients $b_{in}(u_0) \in \overline{k}$ $(n \geq 0)$. Clearly we have

$$\big(\mathsf{s}_{u_0}(\tau)(b_{in}(U))\big)|_{u_0} = \tau(b_{in}(u_0)), \quad (i = 1,\dots,d,\ n \geq 0)$$

and so

$$(\mathsf{s}_{u_0}(\tau)(\mathcal{Y}_i)|_{u_0} = \tau(\mathcal{Y}_i|_{u_0}), \quad (i = 1,\dots,d),$$

which corresponds to the claim. □

Lemma 4.3, applied with $\widetilde{\phi}^{\varphi}$ replacing ϕ also gives

$$\widetilde{\phi}^{\varphi}|_{u_0}(\mathsf{s}_{u_0}(\tau)) = \widetilde{\phi}^{\varphi}(\mathsf{s}_U \circ \mathsf{s}_{u_0}(\tau))$$

Using § 4.2.1 (*), we obtain

$$\begin{aligned}\widetilde{\phi}^{\varphi}|_{u_0}(\mathsf{s}_{u_0}(\tau)) &= \gamma(\phi(\mathsf{s}_U \circ \mathsf{s}_{u_0}(\tau))\delta(\varphi(\mathsf{s}_{u_0}(\tau))\\ &= \gamma(\phi|_{u_0}(\mathsf{s}_{u_0}(\tau))\delta(\varphi(\mathsf{s}_{u_0}(\tau))\\ &= \widetilde{\phi|_{u_0}}^{\varphi\circ\mathsf{s}_{u_0}}(\mathsf{s}_{u_0}(\tau)).\end{aligned}$$

This concludes the proof of $\widetilde{\phi|_{u_0}}^{\varphi\circ\mathsf{s}_{u_0}} = \widetilde{\phi}^{\varphi}|_{u_0}$ and so of Theorem 4.2.

5. Appendix: Good reduction & specializations of covers

This appendix recalls some classical results essentially due to Grothendieck about the good reduction of K-regular extensions and the inertia in their specializations. We have adjusted to our situation the original statements which hold in a bigger generality; in particular our statements are phrased in field extension terms rather than in a scheme theoretic language.

Assume K is the fraction field of a Dedekind domain A; typically $K = k(U)$ and $A = k[U]$ with U a new indeterminate.

Given a non-zero prime ideal $\mathfrak{p} \subset A$ (typically $\mathfrak{p} = \langle U - u_0\rangle$ with $u_0 \in k$ when $A = k[U]$), denote the residue field by $\kappa_{\mathfrak{p}}$, the completion of A (resp. of K) at $\mathfrak{p}$ by $\widetilde{A}_{\mathfrak{p}}$ (resp. by $\widetilde{K}_{\mathfrak{p}}$), the algebraic closure of $\widetilde{K}_{\mathfrak{p}}$ by $C_{\mathfrak{p}}$ and fix an embedding $\overline{K} \subset C_{\mathfrak{p}}$.

Let $F/K(T)$ be a K-regular extension of group G, with branch point set $\mathbf{t} = \{t_1,\dots,t_r\}$, inertia canonical invariant $\mathbf{C} = (C_1,\dots,C_r)$ and associated ramification indices $\mathbf{e} = (e_1,\dots,e_r)$. Let $\mathfrak{p} \subset A$ be a non-zero prime ideal. The results we recall are about

(a) the good reduction of $F/K(T)$ modulo the prime ideal $\mathfrak{p}$, and,
(b) the ramification above the prime ideal $\mathfrak{p}$ in specializations F_{t_0}/K at points $t_0 \in \mathbb{P}^1(K)$.

The classical references are some general results of Grothendieck [14], [13] and more specific versions by Beckmann for regular extensions $F/K(T)$ over number fields [1]. Regarding (b), we follow here Legrand's variant [22, §2] extending Beckmann's statement to the situation the ground field is the fraction field of an arbitrary Dedekind domain. For (a) we follow the variant given in [6].

Classical assumptions. – We first list some classical assumptions involved in these statements; we refer to the articles cited above for more details about them. The main point we will use is that each of them is satisfied for all but finitely many primes $\mathfrak{p}$.

(1) $|\mathcal{G}| \notin \mathfrak{p}$.
(2) *There is no vertical ramification at* $\mathfrak{p}$ *in the extension* $F/K(T)$.
(3) *No two different branch points of* $F/K(T)$ *meet modulo* $\mathfrak{p}$.
(4) *The ideal* $\mathfrak{p}$ *is unramified in the extension* $K(t_1, \dots, t_r)/K$.
(5) t_i *and* $1/t_i$ *are integral over* $\widetilde{A_{\mathfrak{p}}}$, $i = 1, \dots, r$.

We will say that $\mathfrak{p}$ is a *good prime of the extension* $F/K(T)$ if conditions (2), (3) hold [22] and that it is *bad* otherwise.

We also recall the related notion of *good/bad primes of a non-constant polynomial* $P \in A[T, Y]$, irreducible in $\overline{K}[T, Y]$ and monic in Y, defined in [6]: a non-zero element $\mathcal{B}_P \in A$ is constructed and called the bad prime divisor of P; it is essentially the discriminant w.r.t T of some "reduced form" of the discriminant $\Delta_P(T)$ of P w.r.t. Y. A prime $\mathfrak{p}$ is said to be a *good prime of P* if

(6) $\mathcal{B}_P \notin \mathfrak{p}$.

Again there are only finitely many *bad primes* for the polynomial P. The two notions compare as follows: if $\mathfrak{p}$ is good for P then it is also good for the extension $K(T)[Y]/\langle P\rangle$ of $K(T)$.

Let B be the integral closure of $\widetilde{A_{\mathfrak{p}}}[T]$ in the field $F\widetilde{K_{\mathfrak{p}}}$.

GROTHENDIECK GOOD REDUCTION THEOREM. – *Assume that* $\mathfrak{p}$ *is a good prime of* $F/K(T)$ *and that assumption* (1) *holds. Then the extension* $F/K(T)$ *has* good reduction *at* $\mathfrak{p}$*, i.e.,* $\mathfrak{p}B$ *is a prime ideal of* B *and the fraction field* ε *of* $B/\mathfrak{p}B$ *is a separable extension of* $\kappa_{\mathfrak{p}}(T)$ *and satisfies*

$$[\varepsilon : \kappa_{\mathfrak{p}}(T)] = [\overline{\kappa_{\mathfrak{p}}}\varepsilon : \overline{\kappa_{\mathfrak{p}}}(T)] = [F : K(T)] = \deg_Y(P).$$

The extension $\varepsilon/\kappa_{\mathfrak{p}}(T)$ is called the (*good*) *reduction* of $F/K(T)$ at $\mathfrak{p}$ and denoted by $F|_{\mathfrak{p}}/\kappa_{\mathfrak{p}}(T)$ — $F|_{u_0}/k(T)$ when $\mathfrak{p} = \langle U - u_0\rangle \subset A = k[U]$. The vertical bar in the notation is meant to distinguish the reduction from the specialization. The extension $F|_{\mathfrak{p}}/\kappa_{\mathfrak{p}}(T)$ is $\kappa_{\mathfrak{p}}$-regular and its branch point set is the reduction, denoted by $\mathbf{t}_{\mathfrak{p}}$, of the set $\mathbf{t}$ modulo an (arbitrary) prime ideal above $\mathfrak{p}$ of the integral closure of $A_{\mathfrak{p}}$ in $K_{\mathfrak{p}}(\mathbf{t})$.

When the residue field $\kappa_{\mathfrak{p}}$ is algebraically closed, we have this more precise addendum. Its statement uses the notion of fundamental group representation of an extension $F/\overline{K}(T)$; it is recalled in § 4.1.

[22] Legrand also includes (1) and (4). For consistency with other good/bad prime notions, we prefer to stick to (2) and (3) and repeat (1) and (4) when necessary.

ADDENDUM TO GROTHENDIECK GOOD REDUCTION THEOREM. – *Under the same assumptions, there is a specialization isomorphism*

$$\mathrm{sp}_{\mathfrak{p}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \to \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{\mathfrak{p}}, t)_{\overline{\kappa_{\mathfrak{p}}}}$$

which has this further property: if $\phi_{\overline{K}} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}, t)_{\overline{K}} \to G \subset S_d$ *is a* π_1*-representation of the extension* $F\overline{K}/\overline{K}(T)$*, then the morphism*

$$\phi_{\overline{K}} \circ \mathrm{sp}_{\mathfrak{p}}^{-1} : \pi_1(\mathbb{P}^1 \setminus \mathbf{t}_{\mathfrak{p}}, t)_{\overline{\kappa_{\mathfrak{p}}}} \to G \subset S_d$$

is a π_1*-representation of the reduction* $F|_{u_0}/\kappa_{\mathfrak{p}}(T)$*.*

Let $P \in A[T, Y]$ be a non-constant polynomial, irreducible in $\overline{K}[T, Y]$, monic in Y, e.g., an affine equation of the K-regular extension $F/K(T)$.

POLYNOMIAL FORM OF THE GROTHENDIECK GOOD REDUCTION THEOREM

Assume that $\mathfrak{p}$ *is a good prime of* P *and that assumption* (1) *holds. Then the polynomial "*P *modulo* $\mathfrak{p}$*" in* $\kappa_{\mathfrak{p}}[T, Y]$ *is irreducible in* $\overline{\kappa_{\mathfrak{p}}}[T, Y]$ *and of group* G*.*

As explained in [6], this polynomial conclusion is more precise than the field extension conclusion from GRT; the assumption is however also stronger. Finally we recall the conclusions from [22] about the inertia in specializations.

SPECIALIZATION INERTIA THEOREM. – *Let* $t_0 \in \mathbb{P}^1(K) \setminus \mathbf{t}$*.*

(a) *If* $\mathfrak{p}$ *ramifies in* F_{t_0}/K*, then* $F/K(T)$ *has vertical ramification at* $\mathfrak{p}$ *(i.e., condition* (2) *holds) or* t_0 *meets some branch point modulo* $\mathfrak{p}$*.*

(b) *Assume that* $\mathfrak{p}$ *is a good prime of* $F/K(T)$ *and assumptions* (1), (4), (5) *holds.*

If for some $i \in \{1, \dots, r\}$*,* t_0 *and* t_i *meet modulo* $\mathfrak{p}$*, then the inertia group of* F_{t_0}/K *at* $\mathfrak{p}$ *is conjugate in* G *to the cyclic group*

$$\langle g_i^{I_{\mathfrak{p}}(t_0, t_i)} \rangle$$

where g_i *is any element of the conjugacy class* C_i *and* $I_{\mathfrak{p}}(t_0, t_i)$ *is the intersection multiplicity of* t_0 *and* t_i*.*

In the special case $A = k[T]$ and $K = k(T)$, these conclusions correspond to quite concrete statements about pull-backs of covers of $\mathbb{P}^1$ along genus 0 covers $\mathbb{P}^1 \to \mathbb{P}^1$, which were probably known before Grothendieck; they are used for example in [11].

BIBLIOGRAPHY

[1] S. BECKMANN, On extensions of number fields obtained by specializing branched coverings, *J. reine angew. Math.* **419** (1991), 27–53.

[2] J. BUHLER, Z. REICHSTEIN, On the essential dimension of a finite group, *Compos. math.* **106** (1997), 159–179.

[3] J. W. S. CASSELS, A. SCHINZEL, Selmer's conjecture and families of elliptic curves, *Bull. London Math. Soc.* **14** (1982), 345–348.

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

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

[6] P. Dèbes, Reduction and specialization of polynomials, *Acta Arith.* **172** (2016), 175–197.

[7] P. Dèbes, On the Malle conjecture and the self-twisted cover, *Israel J. Math.* **218** (2017), 101–131.

[8] P. Dèbes, J.-C. Douai, Algebraic covers: field of moduli versus field of definition, *Ann. Sci. École Norm. Sup.* **30** (1997), 303–338.

[9] P. Dèbes, N. Ghazi, Galois covers and the Hilbert-Grunwald property, *Ann. Inst. Fourier (Grenoble)* **62** (2012), 989–1013.

[10] P. Dèbes, F. Legrand, Specialization results in Galois theory, *Trans. Amer. Math. Soc.* **365** (2013), 5259–5275.

[11] M. Fried, On a theorem of Ritt and related Diophantine problems, *J. reine angew. Math.* **264** (1973), 40–55.

[12] M. D. Fried, M. Jarden, *Field arithmetic*, 2nd ed., Ergebn. Math. Grenzg. **11**, Springer, Berlin, 2004.

[13] A. Grothendieck, J. P. Murre, *The tame fundamental group of a formal neighbourhood of a divisor with normal crossings on a scheme*, Lecture Notes in Math. **208**, Springer, Berlin-New York, 1971.

[14] A. Grothendieck, *Revêtements étales et groupe fondamental*, Lecture Notes in Math. **224**, Springer, 1971.

[15] S. Guest, J. Morris, C. E. Praeger, P. Spiga, On the maximum orders of elements of finite almost simple groups and primitive permutation groups, *Trans. Amer. Math. Soc.* **367** (2015), 7665–7694.

[16] E. Hallouin, E. Riboulet-Deyris, Computation of some moduli spaces of covers and explicit $\mathscr{S}_n$ and $\mathscr{A}_n$ regular $\mathbb{Q}(T)$-extensions with totally real fibers, *Pacific J. Math.* **211** (2003), 81–99.

[17] K.-I. Hashimoto, K. Miyake, Inverse Galois problem for dihedral groups, in *Number theory and its applications (Kyoto, 1997)*, Dev. Math. **2**, Kluwer Acad. Publ., Dordrecht, 1999, 165–181.

[18] C. U. Jensen, A. Ledet, N. Yui, *Generic polynomials*, Mathematical Sciences Research Institute Publications **45**, Cambridge Univ. Press, Cambridge, 2002.

[19] C. Jordan, Recherches sur les substitutions, *J. Liouville* **17** (1872), 351–367.

[20] F. Legrand, Spécialisations de revêtements et théorie inverse de Galois, thèse de doctorat, Université de Lille 1, 2013.

[21] F. Legrand, Parametric Galois extensions, *J. Algebra* **422** (2015), 187–222.

[22] F. Legrand, Specialization results and ramification conditions, *Israel J. Math.* **214** (2016), 621–650.

[23] F. Legrand, On parametric extensions over number fields, preprint arXiv:1602.06706, to appear in *Ann. Sc. Nor. Sup. di Pisa Cl. di Sci.*

[24] F. Legrand, Twists of super elliptic curves without rational points, to appear in *Int. Math. Res. Not*.

[25] D. J. Lewis, A. Schinzel, Quadratic Diophantine equations with parameters, *Acta Arith.* **37** (1980), 133–141.

[26] A. Schinzel, *Selected topics on polynomials*, University of Michigan Press, Ann Arbor, Mich., 1982.

[27] A. Schinzel, *Polynomials with special regard to reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge Univ. Press, Cambridge, 2000.

[28] E. S. Selmer, A conjecture concerning rational points on cubic curves, *Math. Scand.* **2** (1954), 49–54.

[29] J.-P. Serre, *Topics in Galois theory*, Research Notes in Math. **1**, Jones and Bartlett Publishers, Boston, MA, 1992.

[30] J. G. Thompson, Some finite groups which appear as Gal L/K, where $K \subseteq \mathbf{Q}(\mu_n)$, *J. Algebra* **89** (1984), 437–499.

(Manuscrit reçu le 30 mai 2016 ;
accepté, après révision, le 17 octobre 2016.)

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