ISRAEL JOURNAL OF MATHEMATICS **164** (2008), 19–59
DOI: 10.1007/s11856-008-0019-0

# LIFTING RESULTS FOR RATIONAL POINTS ON HURWITZ MODULI SPACES

BY

Anna Cadoret

*Laboratoire A2X, I.M.B., Univ. Bordeaux 1,*
*351 Cours de la libération, F-33405 Talence cedex, France*
*e-mail: anna.cadoret@math.u-bordeaux1.fr*

ABSTRACT

Hurwitz moduli spaces for G-covers of the projective line have two classical variants whether G-covers are considered modulo the action of $\mathrm{PGL}_2$ on the base or not. A central result of this paper is that, given an integer $r \geq 3$ there exists a bound $d(r) \geq 1$ depending only on $r$ such that any rational point $\mathbf{p}^{rd}$ of a reduced (i.e., modulo $\mathrm{PGL}_2$) Hurwitz space can be lifted to a rational point $\mathbf{p}$ on the nonreduced Hurwitz space with $[\kappa(\mathbf{p}) : \kappa(\mathbf{p}^{rd})] \leq d(r)$. This result can also be generalized to infinite towers of Hurwitz spaces. Introducing a new Galois invariant for G-covers, which we call the base invariant, we improve this result for G-covers with a nontrivial base invariant. For the sublocus corresponding to such G-covers the bound $d(r)$ can be chosen depending only on the base invariant (no longer on $r$) and $\leq 6$. When $r = 4$, our method can still be refined to provide effective criteria to lift $k$-rational points from reduced to nonreduced Hurwitz spaces. This, in particular, leads to a rigidity criterion, a genus 0 method and, what we call an expansion method to realize finite groups as regular Galois groups over $\mathbb{Q}$. Some specific examples are given.

## Introduction

Given a field $k$ of characteristic 0, we write $\Gamma_k$ for its absolute Galois group. Also, given a $k$-variety $X$ and a $\overline{k}$-rational point $\mathbf{p} \in X(\overline{k})$, we write $\kappa(\mathbf{p})$ for the field of definition of $\mathbf{p}$ that is the fixed field in $\overline{k}$ of the stabilizer of $\mathbf{p}$ under $\Gamma_k$.

Received October 14, 2005 and in revised form September 16, 2006.

Fix a finite group $G$, an integer $r \geq 3$ and consider the groupoid of G-covers with group $G$ and degree $r$ ramification divisor. The projective general linear group $\mathrm{PGL}_2$ acts naturally on G-covers by composition; taking this action into account yields a new groupoid of G-covers — the groupoid of $\mathrm{G}/\mathrm{PGL}_2$-covers — with an enlarged set of isomorphisms. Both groupoids of G-covers and $\mathrm{G}/\mathrm{PGL}_2$-covers admit coarse moduli spaces defined over $\mathbb{Q}$, called Hurwitz spaces, $\mathcal{H}_{r,G}$, and reduced Hurwitz spaces, $\mathcal{H}^{rd}_{r,G}$, respectively. The map $\Pi : \mathcal{H}_{r,G} \to \mathcal{H}^{rd}_{r,G}$ can then be identified with the quotient map of $\mathrm{PGL}_2$ acting on $\mathcal{H}_{r,G}$ naturally; in particular, $\dim(\mathcal{H}^{rd}_{r,G})=\dim(\mathcal{H}_{r,G}) - 3 = r - 3$.

The main motivation for studying these objects is the regular inverse Galois problem which, basically, reduces to finding $\mathbb{Q}$-rational points on nonreduced Hurwitz spaces. The case $r = 4$ is particularly worth considering since, then reduced Hurwitz spaces are curves and, in some cases, one can find geometrically irreducible components of them which are birational over $\mathbb{Q}$ to the projective line $\mathbb{P}^1_{\mathbb{Q}}$. But, in general, a $\mathbb{Q}$-rational point on $\mathcal{H}^{rd}_{r,G}$ does not lift to a $\mathbb{Q}$-rational point on $\mathcal{H}_{r,G}$. The aim of this paper is to study this lifting problem, and, in particular, to find subsets $U \subset \mathcal{H}^{rd}_{r,G}(\overline{\mathbb{Q}})$ where any point $\mathbf{p}^{rd} \in U$ can be lifted to a point $\mathbf{p} \in \mathcal{H}_{r,G}$ with $\kappa(\mathbf{p}^{rd}) = \kappa(\mathbf{p})$.

To carry out this study, we associate to any G-cover $f$ a new Galois invariant $\mathcal{E}_f$ we call the **base invariant** of $f$; for a given $r$, there are only finitely many possible values for $\mathcal{E}_f$. This base invariant, when nontrivial, encodes most of the lifting problem; it also encodes whether the prestack of models of $f$ over $k$ is a stack or not (Proposition 2.5). Assume $f$ has field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover, we use $\mathcal{E}_f$ to construct a **cohomological obstruction** $I_k(f) \subset \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ which vanishes (i.e., contains the trivial class) over an extension $K/k$ if and only if $f$ is $\mathrm{G}/\mathrm{PGL}_2$-isomorphic to a G-cover with field of moduli $K$ as G-cover. In other words, $I_k(f)$ vanishes over $K/k$ if and only if the $k$-rational point corresponding to $f$ on $\mathcal{H}^{rd}_{r,G}$ can be lifted to a $K$-rational point on $\mathcal{H}_{r,G}$. Using this cohomological obstruction and nonabelian Galois cohomology, we obtain a precise answer to the original problem (Corollaries 3.9 and 3.11) and its profinite generalization (Corollary 3.15). To sum it up, denote by $\mathcal{H}^{rd}_{r,G}(\mathcal{E}) \subset \mathcal{H}^{rd}_{r,G}(\overline{\mathbb{Q}})$ the subset corresponding to G-covers with base invariant $\mathcal{E}$. Then we have the following

THEOREM: (1) *If $\mathcal{E}$ is nontrivial then there is an integer $d(\mathcal{E})$ depending only on $\mathcal{E}$ and equal to* 1, 2 *or* 6 *such that any point $\mathbf{p}^{rd} \in \mathcal{H}^{rd}_{r,G}(\mathcal{E})$ can be lifted to a point $\mathbf{p} \in \mathcal{H}_{r,G}$ with $[\kappa(\mathbf{p}) : \kappa(\mathbf{p}^{rd})] \leq d(\mathcal{E})$.*

(2) *In general, there is an integer $d(r)$ depending on $r$ such that any point $\mathbf{p}^{rd} \in \mathcal{H}^{rd}_{r,G}(\mathcal{E})$ can be lifted to a point $\mathbf{p} \in \mathcal{H}_{r,G}$ with $[\kappa(\mathbf{p}) : \kappa(\mathbf{p}^{rd})] \leq d(r)$.*

We also show that if $k$ is a field with 2-cohomological dimension $\mathrm{cd}_2(k) \leq 1$ then $\mathcal{H}_{r,G}(k)$ maps surjectively onto $\mathcal{H}^{rd}_{r,G}(k)$. This yields, for instance, that for $\mathbf{p}^{rd} \in \mathcal{H}^{rd}_{r,G}(\overline{\mathbb{Q}})$ the field $\kappa(\mathbf{p}^{rd})$ is the intersection of all the fields $\kappa(\mathbf{p})$ with $\mathbf{p} \in \Pi^{-1}(\mathbf{p}^{rd})$.

Finally, we explain how topological methods give a group-theoretical description of the base-invariant (Section 4). Combining this and a refined version of the above theorem when $r = 3$, 4 (Corollary 5.1) yields effective criteria to find $\mathbb{Q}$-rational points on nonreduced Hurwitz spaces from $\mathbb{Q}$-rational points on reduced Hurwitz spaces: a rigidity criterion (Corollary 5.3), a genus 0 criterion (Corollary 5.5) and what we call an expansion method (proposition 5.7). Using the Braid program [21], [30], we obtain, for instance, regular realizations of $\mathrm{L}_2(19)$ over $\mathbb{Q}$ with 4 copies of the conjugacy class of order 3 elements as inertia canonical invariant (genus 0) or of $\mathrm{L}_2(25)$ over $\mathbb{Q}$ with 42 copies of the conjugacy class of order 3 elements as inertia canonical invariant (expansion). These groups have already been realized regularly over $\mathbb{Q}$ via the classical rigidity method, but not with these inertia canonical invariants.

ACKNOWLEDGEMENT. I would like to thank A. Tamagawa for discussions and several improvements of my original work, H. Völklein for devoting time to explain to me the Braid program and G. Wiesend for his interest in the cohomological part of this work. I am also very grateful to Pierre Dèbes for his re-readings of this paper and his constructive suggestions.

## 1. Preliminaries

1.1. HURWITZ SPACES AND REDUCED HURWITZ SPACES. The central objects of this paper are G-covers of the projective line in characteristic 0. Recall that, given a finite group $G$ and a field $k$ of characteristic 0, a G-cover of the projective line over $k$ with group $G$ is a pair $(f : X \to \mathbb{P}^1_k, \alpha)$ where $f : X \to \mathbb{P}^1_k$ is a Galois cover and $\alpha : \mathrm{Aut}(f) \tilde{\to} G$ a group isomorphism. In the following, we will almost always drop the $\alpha$ in our notation though it remains part of the data.

One can define two categories (fibered in groupoids above $\mathrm{spec}(\mathbb{Q})_{et}$) of G-covers of the projective line: the **category of G-covers** and the **category of $\mathrm{G/PGL_2}$-covers**. In both categories objects are G-covers. In the usual category of G-covers a morphism from $(f_1 : X_1 \to \mathbb{P}^1_k, \alpha_1)$ to $(f_2 : X_2 \to \mathbb{P}^1_k, \alpha_2)$ is an isomorphism $u : X_1 \tilde{\to} X_2$ such that $f_2 \circ u = f_1$ and $\alpha_1(g_1) = \alpha_2(ug_1u^{-1})$, $g_1 \in \mathrm{Aut}(f_1)$ whereas in the category of $\mathrm{G/PGL_2}$-covers a morphism from $(f_1 : X_1 \to \mathbb{P}^1_k, \alpha_1)$ to $(f_2 : X_2 \to \mathbb{P}^1_k, \alpha_2)$ is a pair of isomorphisms $(u : X_1 \tilde{\to} X_2, v : \mathbb{P}^1 \tilde{\to} \mathbb{P}^1)$ such that $f_2 \circ u = v \circ f_1$ and $\alpha_1(g_1) = \alpha_2(ug_1u^{-1})$, $g_1 \in \mathrm{Aut}(f_1)$.

From now on, given a field $k$ of characteristic 0, we will always assume a compatible system $(\zeta_n)_{n\geq 1}$ of primitive roots of unity is given in the algebraic closure $\overline{k}$ of $k$ (that is, $\zeta_{nm}^n = \zeta_m$, $n, m \geq 1$). With this convention, two classical invariants can be associated to a given G-cover $f : X \to \mathbb{P}^1_{\overline{k}}$ of the projective line over $\overline{k}$ with group $G$ : the ramification divisor $\mathbf{t} \in \mathcal{U}_r$, where $\mathcal{U}_r$ denotes the fine moduli space for $r$ unordered marked points on the (fixed) projective line and the inertia canonical invariant $\mathbf{C} = (C_t)_{t\in\mathbf{t}}$[1].

Given a finite group $G$ and an $r$-tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in $G$, both categories of G-covers and $\mathrm{G/PGL_2}$-covers with group $G$ and inertia canonical invariant $\mathbf{C}$ admit coarse moduli spaces called **inner Hurwitz spaces** and **reduced inner Hurwitz spaces** respectively. Inner Hurwitz spaces have been studied by many authors and there exist various constructions of them. See [14] for a good survey of them. Classical references include [16], [32], [33], etc. Reduced inner Hurwitz spaces appear for instance in [1] and [5]. The two following paragraphs sum up the properties that will be needed further. In section 4, the topological aspect will be dealt with more precisely.

1.1.1. *Hurwitz spaces.* Fix a finite group $G$ and a $r$-tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in $G$. Denote by $H(\mathbf{C})$ the set of all G-isomorphism classes of G-covers defined over $\mathbb{C}$ with invariants $G$, $\mathbf{C}$ and by

[1] Recall that $\mathbf{C} = (C_t)_{t\in\mathbf{t}}$ is defined as follows. For each $t \in \mathbf{t}$, choose a place $P_t$ in $\overline{k}(X)$ above $t$ and let $I_{P_t}$ be the corresponding inertia group, which is cyclic of order $e_t$. Any uniformizing parameter $u \in P_t$ induces a well-defined (independent of the uniformizing parameter $u$) group monomorphism $\phi_{P_t} : I_{P_t} \hookrightarrow \overline{k}^\times$, $\omega \to \omega(u)/u \bmod P_t$. The element $\omega_{P_t} := \alpha(\phi_{P_t}^{-1}(\zeta_{e_t})) \in G$ (where $\zeta_{e_t}$ is our distinguished $e_t$th root of unity) is called **the distinguished generator of** $I_{P_t}$. The set of all $\omega_{P_t}$ for places $P_t$ above $t$ is a full conjugacy class $C_t$ in $G$.

$\Psi : H(\mathbf{C}) \to \mathcal{U}_r(\mathbb{C})$ the ramification divisor map, sending the G-isomorphism class of a G-cover $f$ to its ramification divisor $\mathbf{t}$. By Riemann's Existence Theorem, this map has finite fibers in (noncanonical) bijection with the **Nielsen class** $\overline{\mathrm{ni}}(\mathbf{C})$ that is, the quotient set modulo the componentwise action of the inner automorphism group $\mathrm{Inn}(G)$ of

$$\mathrm{ni}(\mathbf{C}) = \left\{ (g_1, \ldots, g_r) \in G^r \;\middle|\; \begin{array}{l} (1)\ G = \langle g_1, \ldots, g_r \rangle \\ (2)\ g_1 \cdots g_r = 1 \\ (3)\ g_i \in C_{\sigma(i)},\ \ i = 1, \ldots, r \text{ for some } \sigma \in S_r \end{array} \right\}.$$

The (noncanonical) isomorphism $\Psi^{-1}(\mathbf{t}) \simeq \overline{\mathrm{ni}}(\mathbf{C})$ depends on the choice of a topological bouquet for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ and it is given by the monodromy. The set $H(\mathbf{C})$ can be equipped in a unique way with a topology and an analytic structure such that $\Psi$ becomes an analytic cover. Then, invoking results of G.A.G.A. type, one obtains the following theorem.

THEOREM 1.1 ([16, Theorem 1]): *The analytic space $H(\mathbf{C})$ can be equipped in a unique way with an algebraic structure of affine variety $\mathcal{H}(\mathbf{C})$ (defined over an explicitly computable cyclotomic number field $\mathbb{Q}_{\mathbf{C}}$ which depends only on $\mathbf{C}$) such that the analytic cover $\Psi$ is induced by a finite etale cover $\Psi : \mathcal{H}(\mathbf{C}) \to \mathcal{U}_r$ defined over $\mathbb{Q}_{\mathbf{C}}$. Furthermore, we have the following properties:*

(1) COARSE MODULI: *For any algebraically closed field $k$ of characteristic 0 the set of $k$-rational points $\mathcal{H}(\mathbf{C})(k)$ is in bijection with the set of all $G$-isomorphism classes of $G$-covers defined over $k$ and with invariants $G$, $\mathbf{C}$.*

(2) GALOIS ACTION: *For any field extension $k/\mathbb{Q}_{\mathbf{C}}$ and for any $\sigma \in \Gamma_k$, $[f] \in \mathcal{H}(\mathbf{C})(\overline{\mathbb{Q}})$ we have ${}^{\sigma}[f] = [{}^{\sigma}f]$. So, in particular, the set of $k$-rational points $\mathcal{H}(\mathbf{C})(k)$ is in bijection with the set of all $G$-isomorphism classes of $G$-covers with field of moduli $k$ and invariants $G$, $\mathbf{C}$.*

(3) TOPOLOGICAL DESCRIPTION: *the geometrically irreducible components of $\mathcal{H}(\mathbf{C})$ are in bijection with the connected components of the associated topological space $\mathcal{H}(\mathbf{C})(\mathbb{C})^{\mathrm{top}}$ which, in turn, are in bijection with the orbits of the topological fundamental group $H_r$ of the base space $\mathcal{U}_r(\mathbb{C})$ on the fibers $\Psi^{-1}(\mathbf{t}) \simeq \overline{\mathrm{ni}}(\mathbf{C})$.*

1.1.2. *Reduced Hurwitz spaces.* Now, to define reduced Hurwitz spaces, consider the natural action of the projective general linear group $\mathrm{PGL}_2$ over $\mathcal{H}(\mathbf{C})$ and

$\mathcal{U}_r$, for which $\Psi$ is invariant. As $\mathrm{PGL}_2$ is an affine reductive algebraic $\mathbb{Q}$-group acting on affine algebraic $\mathbb{Q}$ (resp. $\mathbb{Q}_{\mathbf{C}}$)-varieties, it follows from [25, Theorem 1.1] that the quotient spaces, denoted by $\mathcal{H}^{rd}(\mathbf{C})$ and $\mathcal{J}_r$, exists in the category of affine algebraic $\mathbb{Q}$ (resp. $\mathbb{Q}_{\mathbf{C}}$)-varieties. More precisely, one obtains the following theorem.

THEOREM 1.2 ([1, Proposition 3.4 and Proposition 3.28]): *The quotient space exists in the category of $\mathbb{Q}_{\mathbf{C}}$-affine varieties*

$$\begin{array}{ccc} \mathcal{H}(\mathbf{C}) & \xrightarrow{\Pi} & \mathcal{H}^{rd}(\mathbf{C}) \\ \Big\downarrow{\scriptstyle \Psi} & & \Big\downarrow{\scriptstyle \Psi^{rd}} \\ \mathcal{U}_r & \xrightarrow{\Pi_r} & \mathcal{J}_r \end{array}$$

*and the reduced cover $\Psi^{rd}$ is ramified over the closed subvariety corresponding to $PGL_2$-orbits of divisors $\mathbf{t} \in \mathcal{U}_r$ with a nontrivial stabilizer. Furthermore, $\mathcal{H}^{rd}(\mathbf{C})$ has properties* (1) *and* (2) *of Theorem 1.1 with $G/PGL_2$-covers instead of $G$-covers and the geometrically irreducible components of $\mathcal{H}^{rd}(\mathbf{C})$ are in bijection with the geometrically irreducible components of $\mathcal{H}(\mathbf{C})$.*

1.2. THE LIFTING PROBLEM. The main motivation for this work is finding $\mathbb{Q}$-rational points on Hurwitz spaces. Indeed, by [16, Lemma 2], the regular inverse Galois problem over a field $k$ is equivalent to the following arithmetico-geometric conjecture.

CONJECTURE 1.3: *For any centerless finite group $G$ there exists a $r$-tuple $\mathbf{C}$ of nontrivial conjugacy classes of $G$ such that the inner Hurwitz space $\mathcal{H}(\mathbf{C})$ is defined over $k$ and carries $k$-rational points.*

Conjecture 1.3 was proved for ample fields, but it is still entirely open for number fields and $\mathbb{Q}^{ab}$. Over these fields, most of the results were obtained using rigidity [32], [22] or genus 0 methods over nonreduced Hurwitz spaces [23], [13].

Now, fix a finite group $G$ and a $r$-tuple $\mathbf{C}$ of nontrivial conjugacy classes of $G$. The underlying principle of genus 0 methods is to consider curves $\mathcal{C}$ on nonreduced Hurwitz spaces $\mathcal{H}(\mathbf{C})$ obtained by lifting geometrically irreducible $\mathbb{Q}_{\mathbf{C}}$-rational curves $\mathcal{C}_0$ of the base space $\mathcal{U}_r$. For clever choices of $\mathcal{C}_0$, one can compute the ramification data of the projective normalization of the cover $\mathcal{C} \to \mathcal{C}_0$, hence the geometrically irreducible components $O_1, \ldots, O_n$ of $\mathcal{C}$ and, by

Riemann–Hurwitz, their respective genera $g_1, \dots, g_n$. Assume that one of these components, say $O$, has genus 0, is defined over $\mathbb{Q}_{\mathbf{C}}$ and carries a $\mathbb{Q}_{\mathbf{C}}$-rational divisor of odd degree. Then, by the Riemann–Roch theorem, $O$ is birational to $\mathbb{P}^1$ over $\mathbb{Q}_{\mathbf{C}}$ and, in particular, it has a dense subset of $\mathbb{Q}_{\mathbf{C}}$-rational points.

As the quotient $\Pi : \mathcal{H}(\mathbf{C}) \to \mathcal{H}^{rd}(\mathbf{C})$ is defined over $\mathbb{Q}_{\mathbf{C}}$, it should be easier to find $\mathbb{Q}_{\mathbf{C}}$-points on $\mathcal{H}^{rd}(\mathbf{C})$. For instance, when $r = 4$, $\mathcal{H}^{rd}(\mathbf{C})$ is a curve and $O$ can be regarded as a finite cover of some geometrically irreducible component $O^{rd}$ of $\mathcal{H}^{rd}(\mathbf{C})$. In particular, the genus of $O^{rd}$ will be often smaller than the genus of $O$. In addition, one can compute the ramification data of the projective normalization of $\Psi : \mathcal{H}^{rd}(\mathbf{C}) \to \mathcal{J}_4 \simeq \mathbb{P}^1 \setminus \{0, 1, \infty\}$ (cf. Theorem 5.2), hence the genus 0-argument described above can also be checked effectively for $\mathcal{H}^{rd}(\mathbf{C})$. However, in view of the regular inverse Galois problem, the significant Hurwitz spaces are not the reduced ones but the nonreduced ones. This motivates the following problem.

Problem (Lifting problem): Given a field $k$ and a $k$-rational point $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$, find a minimal upper bound for

$$\mathrm{m}_k(\mathbf{p}^{rd}) := \min\{[\kappa(\mathbf{p}) : k] \colon \ \mathbf{p} \in \Pi^{-1}(\mathbf{p}^{rd})\}.$$

In terms of G-covers, the lifting problem is equivalent to the following. Given a field $k$ and a G-cover $f$ with field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover, find a minimal upper bound for the degree over $k$ of the field of moduli as G-cover of $v \circ f$, when $v$ describes $\mathrm{PGL}_2(\overline{k})$.

To realize regularly finite groups over $k$, one has to prove that

$$\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$$

can be taken in such a way that $\mathrm{m}_k(\mathbf{p}^{rd}) = 1$. We give criteria for this when $r = 3, 4$ and $k$ is any field of characteristic 0 (in particular, $\mathbb{Q}$) in Section 5.2. This leads to three effective methods: a rigidity method (Corollary 5.3), which refines the usual rigidity argument by considering an additional Galois invariant — the base invariant, the genus 0 method described above (Corollary 5.5) and, what we call an expansion method (Proposition 5.7).

## 2. Cohomological obstruction

2.1. The base invariant. Given a G-cover $f : X \to \mathbb{P}^1_k$, we define the **base group** of $f$ to be the stabilizer $E_f$ of the G-isomorphism class of $f$ under $\mathrm{PGL}_2$,

that is the set of all $v \in \mathrm{PGL}_2(\overline{k})$ such that $f$ and $v \circ f$ are G-isomorphic. This is not an invariant of the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of $f$. That is why we introduce the **base invariant** of $f$, defined as the conjugacy class of $E_f$ in $\mathrm{PGL}_2(\overline{k})$ and we denote it by $\mathcal{E}_f$.

The base group $E_f$ is a subgroup of the stabilizer $S_{\mathbf{t}}$ of the ramification divisor $\mathbf{t}$ of $f$ in $\mathrm{PGL}_2(\overline{k})$. In particular, $|E_f|$ is finite provided $r \geq 3$, which we will always assume in the following. If, furthermore, we specify the inertia canonical invariant $\mathbf{C} = (C_t)_{t \in \mathbf{t}}$ and define a partition $\mathbf{t}_1, \ldots, \mathbf{t}_s$ of $\mathbf{t}$ in such a way that $C_t = C_i$, $t \in \mathbf{t}_i$ and $C_i \neq C_j$, $1 \leq i \neq j \leq s$ then $E_f$ is a subgroup of $S_{\mathbf{t}_1} \times \cdots \times S_{\mathbf{t}_s} \subset S_{\mathbf{t}}$. For instance, if $s = r$ then $E_f$ is trivial, if $s = r-1$ then $E_f$ is either trivial or $\mathbb{Z}/2\mathbb{Z}$, *etc.*

The finiteness of the base group implies that, for a given $r \geq 3$, the base invariant can only take finitely many possible values. This is a consequence of the following classification result for finite subgroups of $\mathrm{PGL}_2(\overline{k})$.

Lemma 2.1 (Classification): *Let $k$ be a field of characteristic 0. Then,*

(1) Classification: *Any finite subgroup of $\mathrm{PGL}_2(\overline{k})$ is conjugate to one of the following groups.*

- $C_n = \left\{ \left(\begin{smallmatrix} \zeta_n^r & 0 \\ 0 & 1 \end{smallmatrix}\right), r = 0, \ldots, n-1 \right\}$, *where $\zeta_n$ is a primitive $n$-th root of unity, $n \geq 1$.*
- $D_{2n} = \left\{ \left(\begin{smallmatrix} \zeta_n^r & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \zeta_n^r \\ 1 & 0 \end{smallmatrix}\right), r = 0, \ldots, n-1 \right\}$, *where $\zeta_n$ is a primitive $n$-th root of unity, $n \geq 3$.*
- $V_4 = \left\{ \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \pm 1 \\ 1 & 0 \end{smallmatrix}\right) \right\}$.
- $\mathcal{A}_4 = \left\{ \left(\begin{smallmatrix} \pm 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \pm 1 \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} i^\nu & i^\nu \\ 1 & -1 \end{smallmatrix}\right), \left(\begin{smallmatrix} i^\nu & -i^\nu \\ 1 & i^\nu \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & i^\nu \\ 1 & -i^\nu \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & -i^\nu \\ 1 & -i^\nu \end{smallmatrix}\right), \nu = 1, 3 \right\}$.
- $\mathcal{S}_4 = \left\{ \left(\begin{smallmatrix} i^\nu & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & i^\nu \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} i^\nu & -i^{\nu+\nu'} \\ 1 & i^{\nu'} \end{smallmatrix}\right), \nu, \nu' = 0, 1, 2, 3 \right\}$.
- $\mathcal{A}_5 = \left\{ \left(\begin{smallmatrix} \zeta^r & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & \zeta^r \\ 1 & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} \zeta^r\omega & \zeta^{r-s} \\ 1 & -\zeta^s\omega \end{smallmatrix}\right), \left(\begin{smallmatrix} \zeta^r\overline{\omega} & \zeta^{r-s} \\ 1 & -\zeta^{-s}\overline{\omega} \end{smallmatrix}\right), r, s = 0, 1, 2, 3, 4 \right\}$,

*where $\omega = \frac{-1+\sqrt{5}}{2}$, $\overline{\omega} = \frac{-1-\sqrt{5}}{2}$ and $\zeta$ is a primitive 5-th root of unity.*

(2) Normalizers: - $\mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(C_n) = \overline{k}^\star \rtimes \mathbb{Z}/2$ *(with $1 \in \mathbb{Z}/2$ acting on $\alpha \in \overline{k}^\star$ via $(1,1)(\alpha, 0)(1,1) = (\alpha^{-1}, 0)$), $n \geq 2$).*
- $\mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(D_{2n}) = D_{4n}$, $n \geq 3$.
- $\mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(V_4) = \mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(\mathcal{A}_4) = \mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(\mathcal{S}_4) = \mathcal{S}_4$.
- $\mathrm{Nor}_{\mathrm{PGL}_2(\overline{k})}(\mathcal{A}_5) = \mathcal{A}_5$.

(3) Quotients galois modules: *If $E$ is one of the groups listed in (1) and $N$ is its normalizer then both $E$ and $N$ are globally $\Gamma_k$-invariant. Consequently,*

*the resulting quotient group $Q := N/E$ carries a natural structure of $\Gamma_k$-module.*
- $E = \mathcal{S}_4$, $\mathcal{A}_5$: $Q = \{1\}$.
- $E = \mathcal{A}_4$, $D_{2n}$, $n \geq 3$: $Q = \mathbb{Z}/2$.
- $E = C_n$, $n \geq 2$: $Q = \overline{k}^\star \rtimes \mathbb{Z}/2$.
- $E = V_4$: $Q = \mathbb{Z}/3 \rtimes \mathbb{Z}/2$.

*Proof.* For (1) and (2) we refer to [31]. As for (3), if $E = \mathcal{S}_4$, $\mathcal{A}_5$ then $E = N$ and $Q = \{1\}$. If $E = \mathcal{A}_4$, $D_{2n}$, $n \geq 3$ then $Q = \mathbb{Z}/2$ as a group and the only $\Gamma_k$-module structure on $\mathbb{Z}/2\mathbb{Z}$ is the trivial one. If $E = C_n$, $n \geq 2$ then consider the $\Gamma_k$-module epimorphism $p : \overline{k}^\star \rtimes \mathbb{Z}/2 \twoheadrightarrow \overline{k}^\star \rtimes \mathbb{Z}/2$ sending $(\alpha, 0)$ to $(\alpha^n, 0)$ and $(1, 1)$ to $(1, 1)$. Its kernel is $C_n$ thus $p$ identifies $Q$ with $\overline{k}^\star \rtimes \mathbb{Z}/2$. Finally, if $E = V_4$ then $N = \mathcal{S}_4$. Denote by $I$, $A_i$, $i = 1, 2, 3$ and $B$ the classes in $Q$ of, respectively, $\mathrm{I}_2$, $\left(\begin{smallmatrix} -1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & i \\ 1 & 0 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} i & -1 \\ 1 & -i \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & -i \\ 1 & i \end{smallmatrix}\right)$. This defines a canonical group isomorphism $Q \tilde{\to} \mathbb{Z}/3 \rtimes \mathbb{Z}/2$ sending $B$ to $(0, 1)$ and $A_1$ to $(1, 0)$. Finally, straightforward computations show that the classes $I$, $A_i$, $i = 1, 2, 3$, $B$ are $\Gamma_k$-invariant and, consequently, that $Q$ is the trivial $\Gamma_k$-module $\mathbb{Z}/3 \rtimes \mathbb{Z}/2$. ∎

We will use the following cohomological result several times. With the notation of (1) of Lemma 2.1, let

$$1 \longrightarrow K \longrightarrow G \underset{s}{\longrightarrow} \mathbb{Z}/2 \longrightarrow 1 \tag{1}$$

be one of the two split short exact sequences of $\Gamma_k$-modules

$$1 \longrightarrow C_n \longrightarrow D_{2n} \underset{s}{\longrightarrow} \mathbb{Z}/2 \longrightarrow 1,\ n \geq 2 \tag{2}$$

or

$$1 \longrightarrow D_{2n} \longrightarrow D_{4n} \underset{s}{\longrightarrow} \mathbb{Z}/2 \longrightarrow 1,\ n \geq 3 \text{ odd}. \tag{3}$$

where $s : \mathbb{Z}/2 \to G$ is the section sending 1 to $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ in (2) and to $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in (3). Then (1) yields in cohomology the following commutative diagram.

$$\begin{array}{ccc} \mathrm{H}^1(k, G) & \xrightarrow{\ i\ } & \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k})) \\ {\scriptstyle s}\,\big(\ \big\downarrow{\scriptstyle p} & \nearrow_{i \circ s} & \\ \mathrm{H}^1(k, \mathbb{Z}/2) & & \end{array} .$$

LEMMA 2.2: *The map $i \circ s : \mathrm{H}^1(k, \mathbb{Z}/2) \to \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ is trivial.*

*Proof.* Let $\chi \in \mathrm{H}^1(k, \mathbb{Z}/2)$ be any nontrivial element and let $L_\chi$ be the fixed field of $\ker(\chi)$ in $\overline{k}$. Then $L_\chi/k$ is a quadratic extension and, in particular, it admits a primitive element $x \notin k$ such that $x^2 \in k$.

Now, introducing $v_x := \left(\begin{smallmatrix} 1 & 1 \\ 1+x & 1-x \end{smallmatrix}\right) \in \mathrm{PGL}_2(\overline{k})$ when (1) is (2) and $v_x := \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}_2(\overline{k})$ when (1) is (3), one immediately checks that

$$v_x^{-1}\, {}^{\sigma}v_x = \chi_\sigma, \sigma \in \Gamma_k. \qquad \blacksquare$$

For technical matters, we will need the following notions. Given a G-cover $f : X \to \mathbb{P}^1_{\overline{k}}$, the representative $E_f^0$ of $\mathcal{E}_f$ which appears in (1) of Lemma 2.1 is the **normalized base group of** $f$; we will denote by $N_f^0$ and $Q_f^0 = N_f^0/E_f^0$ the corresponding normalizer and quotient $\Gamma_k$-module. A **normalized representative of** $f$ is a representative $f_0 : X_0 \to \mathbb{P}^1_{\overline{k}}$ of the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of $f$ with base group $E_{f_0} = E_f^0$; we will denote by $\mathcal{N}(f)$ the set of normalized representatives of $f$. Any choice of $f_0 \in \mathcal{N}(f)$ defines a bijection $Q_f^0 \tilde{\to} \mathcal{N}(f)$.

2.2. CONSTRUCTION OF THE COHOMOLOGICAL OBSTRUCTION. Given a G-cover $f : X \to \mathbb{P}^1_{\overline{k}}$ with field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover, let

$$f_0 : X_0 \to \mathbb{P}^1_{\overline{k}} \in \mathcal{N}(f)$$

be any of its normalized representatives. Then $f_0$ also has field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover that is, for any $\sigma \in \Gamma_k$ we have a commutative diagram

$$\begin{array}{ccc} {}^{\sigma}X_0 & \xrightarrow{u_\sigma} & X_0 \\ {\scriptstyle {}^{\sigma}f_0}\downarrow & & \downarrow{\scriptstyle f_0} \\ \mathbb{P}^1_{\overline{k}} & \xrightarrow[v_\sigma]{} & \mathbb{P}^1_{\overline{k}} \end{array}$$

where the horizontal arrows are isomorphisms. On the one hand, $E_{{}^{\sigma}f_0} = E_{v_\sigma^{-1} f_0} = v_\sigma^{-1} E_{f_0} v_\sigma$ and, on the other hand, $E_{{}^{\sigma}f_0} = {}^{\sigma}E_{f_0}$. But, as $f_0$ is a normalized representative, $E_{f_0} = E_f^0$ is $\Gamma_k$-invariant, which forces (and this is the key point) $v_\sigma \in N_f^0$. However, $v_\sigma$ is only defined up to composition by elements of the normalized base group $E_f^0$ so, the well-defined object is $v_\sigma$ mod $E_f^0 \in Q_f^0$. This leads to the following lemma.

LEMMA 2.3: *The map $\overline{c}_{f_0} : \Gamma_k \to Q_f^0$ sending $\sigma$ to $v_\sigma \bmod E_f^0$ is a well-defined 1-cocycle. Furthermore the corresponding cohomological class $[\overline{c}_{f_0}] \in \mathrm{H}^1(k, Q_f^0)$ is independent of the choice of the normalized representative $f_0 \in \mathcal{N}(f)$; we denote it by $[\overline{c}]_f$.*

*Proof.* First, it is readily checked that the definition of $\overline{c}_{f_0}$ does not depend on the $v_\sigma$, $\sigma \in \Gamma_k$. Likewise, it is a 1-cocycle since for any $\sigma, \tau \in \Gamma_k$, we have

$$v_{\sigma\tau} \circ f_0 \simeq {}^{\sigma\tau} f_0 \simeq {}^{\sigma}(v_\tau \circ f_0) \simeq {}^{\sigma} v_\tau \, {}^{\sigma} f_0 \simeq {}^{\sigma} v_\tau \circ v_\sigma \circ f_0 = (v_\sigma \, {}^{\sigma} v_\tau) \circ f_0,$$

where all the above isomorphisms are G-covers isomorphisms. So $v_{\sigma\tau}^{-1} v_\sigma \, {}^{\sigma} v_\tau \in E_f^0$ or, in other words, $v_{\sigma\tau} \bmod E_f^0 = v_\sigma \bmod E_f^0 \, {}^{\sigma}(v_\tau \bmod E_f^0)$. Finally, if $f_0^1, f_0^2 \in \mathcal{N}(f)$ are two normalized representatives then there exists $v_0 \in \mathrm{PGL}_2(\overline{k})$ such that $f_0^1$ and $v_0 \circ f_0^2$ are G-isomorphic. But $E_{f_0^1} = E_{f_0^2} = E_f^0$ forces $v_0 \in N_f^0$ and a straightforward computation shows that $\overline{c}_{f_0^1}(\sigma) = v_0^{-1} \overline{c}_{f_0^2}(\sigma) \, {}^{\sigma} v_0$, $\sigma \in \Gamma_k$. ∎

Let $k_0/k$ be a field extension. A sufficient condition for $f$ to be $\mathrm{G}/\mathrm{PGL}_2$-isomorphic to a G-cover with field of moduli $k_0$ as G-cover is that $\mathrm{Res}_k^{k_0}([\overline{c}]_f)$ be the trivial class in $\mathrm{H}^1(k_0, Q_f^0)$. Indeed, if $\mathrm{Res}_k^{k_0}([\overline{c}]_f)$ is trivial in $\mathrm{H}^1(k_0, Q_f^0)$ then there exists $v_0 \in N_f^0$ such that for any $\sigma \in \Gamma_{k_0}$ we have a commutative diagram

$$\begin{array}{ccc} {}^{\sigma} X_{0,\overline{k}_0} & \xrightarrow{u_\sigma} & X_{0,\overline{k}_0} \\ \downarrow{\scriptstyle {}^{\sigma} f_{0,\overline{k}_0}} & & \downarrow{\scriptstyle f_{0,\overline{k}_0}} \\ \mathbb{P}^1_{\overline{k}_0} & \xrightarrow[e_\sigma \circ (v_0^{-1} \, {}^{\sigma} v_0)]{} & \mathbb{P}^1_{\overline{k}_0} \end{array}$$

with $e_\sigma \in E_f^0$ thus, up to replacing $u_\sigma$ by $\epsilon_\sigma^{-1} \circ u_\sigma$ where $\epsilon_\sigma$ is any automorphism of $X_{0,\overline{k}_0}$ lifting $e_\sigma$, we get

$$\begin{array}{ccccc} X_{0,\overline{k}_0} & \xrightarrow{f_{0,\overline{k}_0}} & \mathbb{P}^1_{\overline{k}_0} & & \\ \uparrow{\scriptstyle \epsilon_\sigma^{-1} u_\sigma} & & \uparrow{\scriptstyle v_0^{-1} \, {}^{\sigma} v_0} & \searrow^{v_0} & \\ {}^{\sigma} X_{0,\overline{k}_0} & \xrightarrow[{}^{\sigma} f_{0,\overline{k}_0}]{} & \mathbb{P}^1_{\overline{k}_0} & \xrightarrow[{}^{\sigma} v_0]{} & \mathbb{P}^1_{\overline{k}_0} \end{array}$$

that is, $v_0 \circ f_{0,\overline{k}_0}$ has field of moduli $k_0$ as G-cover. However, this imposes that $v_0 \circ f_{0,\overline{k}_0}$ is also a normalized representative but, a priori, there is no reason why normalized representatives should have better lifting properties. So, to obtain

an if and only if condition, the "good" cohomological object is the **lifting cohomological obstruction of $f$ over $k$** defined by

$$I_k(f) := i(p^{-1}([\overline{c}]_f) \subset \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$$

where, $p$ and $i$ are the natural map induced by functoriality which appear in the diagram below.

$$\begin{array}{ccc} \mathrm{H}^1(k, N_f^0) & \xrightarrow{i} & \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k})) \\ \Big\downarrow{\scriptstyle p} & & \\ \mathrm{H}^1(k, Q_f^0) & & \end{array} \tag{4}$$

The definition of $I_k(f)$ depends only on the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of $f$ and commutes with base extension that is, for any field extension $k_0/k$ we have $I_{k_0}(f \times_k k_0) \supset \mathrm{Res}_k^{k_0}(I_k(f))$. In the following, we will write $I_{k_0}(f)$ instead of $I_{k_0}(f \times_k k_0)$.

Proposition 2.4 (Cohomological obstruction): *Let $k_0/k$ be a field extension. Then the G-cover $f$ is $G/PGL_2$-isomorphic to a G-cover with field of moduli $k_0$ as G-cover if and only if $I_{k_0}(f)$ contains the trivial cohomology class.*

*Proof.* As all the objects we consider commute with base extension, it is enough to make the proof with $k_0 = k$. Let $f_0 : X_0 \to \mathbb{P}^1_{\overline{k}} \in \mathcal{N}(f)$ be a normalized representative of $f$ and assume there exists $v \in \mathrm{PGL}_2(\overline{k})$ such that $v \circ f_0$ has field of moduli $k$ as G-cover that is, for any $\sigma \in \Gamma_k$ we have a commutative diagram

$$\begin{array}{ccccc} X_0 & \xrightarrow{f_0} & \mathbb{P}^1_{\overline{k}} & & \\ {\scriptstyle u_\sigma}\uparrow & & \uparrow{\scriptstyle {}^{v^{-1}\,\sigma}v} & \searrow^{v} & \\ {}^{\sigma}X_0 & \xrightarrow[{}^{\sigma}f_0]{} & \mathbb{P}^1_{\overline{k}} & \xrightarrow[{}^{\sigma}v]{} & \mathbb{P}^1_{\overline{k}} \end{array}$$

This implies that the map $c_v : \Gamma_k \to N_f^0$ sending $\sigma$ to ${}^{v^{-1}\,\sigma}v$ is a well-defined 1-cocycle satisfying furthermore (i) $p([c_v]) = [\overline{c}]_f$ and (ii) $i([c_v])$ is the trivial class in $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$.

Conversely, assume that $I_k(f)$ contains the trivial class, that is, there exists a well-defined 1-cocycle $c : \Gamma_k \to N_f^0$ such that (i) $p([c]) = [\overline{c}]_f$ and (ii) $i([c])$ is the trivial class in $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$. But condition (ii) means that $c_\sigma = {}^{v^{-1}\,\sigma}v$

for some $v \in \mathrm{PGL}_2(\overline{k})$ and condition (i) means that there exists $f_0 : X_0 \to \mathbb{P}^1_{\overline{k}} \in \mathcal{N}(f)$ with $p([c_{f_0}]) = p([c])$. In other words, for any $\sigma \in \Gamma_k$, we have a commutative diagram

$$\begin{array}{ccc} {}^{\sigma}X_0 & \xrightarrow{u_\sigma} & X_0 \\ {\scriptstyle {}^{\sigma}f_0}\downarrow & & \downarrow{\scriptstyle f_0} \\ \mathbb{P}^1_{\overline{k}} & \xrightarrow[e_\sigma \circ (v^{-1}\ {}^{\sigma}v)]{} & \mathbb{P}^1_{\overline{k}} \end{array}$$

with $e_\sigma \in E_f^0$. Up to replacing $u_\sigma$ by $\epsilon_\sigma^{-1} \circ u_\sigma$ where $\epsilon_\sigma$ is any automorphism of $X_0$ lifting $e_\sigma$, we obtain that $v \circ f_0$ has field of moduli $k$ as G-cover. ∎

Our invariant $I_k(f)$ can also be interpreted in terms of gerbes. For the theory of gerbes, which is a classical alternative to Galois cohomology for descent problems ([9], [10]) we refer to [18] and [11].

In general, given a G-cover $f$ with field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover, the natural prestack of models over $\mathrm{spec}(k)_{et}$ associated to $f$, $\mathcal{PS}_{G/PGL_2}(f)$, is not a stack and so, a fortiori not a gerbe. More precisely, to show $\mathcal{PS}_{G/PGL_2}(f)$ is a stack (and hence a gerbe), we would have to check

Condition (S): For any finite Galois extensions $E/k$ and $F/E$ and for any $f_F : X \to \mathbb{P}^1_F \in \mathcal{PS}_{G/PGL_2}(f)(F)$, if for any $\sigma \in \mathrm{Gal}(F|E)$ there exists a $\mathrm{G}/\mathrm{PGL}_2$-isomorphism $(u_\sigma, v_\sigma)$ from ${}^{\sigma}f$ to $f$ such that

$$(u_{\sigma\tau}, v_{\sigma\tau}) = (u_\sigma, v_\sigma)\ {}^{\sigma}(u_\tau, v_\tau), \quad \sigma, \tau \in \mathrm{Gal}(F|E),$$

then there exists a G-cover $f_E : X_E \to \mathbb{P}^1_E$ defined over $E$ and a $\mathrm{G}/\mathrm{PGL}_2$-isomorphism $(u_0, v_0)$ from $f_E \times_E F$ to $f$ such that $(u_\sigma, v_\sigma) = (u_0^{-1}\ {}^{\sigma}u_0, v_0^{-1}\ {}^{\sigma}v_0)$, $\sigma \in \mathrm{Gal}(F|E)$.

If we use Weil's cocycle criterion for algebraic varieties, $v_{\sigma\tau} = v_\sigma\ {}^{\sigma}v_\tau$, $\sigma, \tau \in \mathrm{Gal}(F|E)$ implies that there exists a $E$-curve $\mathcal{C}_E$ and a $F$-isomorphism $\mathbb{P}^1_F \xrightarrow{v} \mathcal{C}_E \times_E F$ such that $v_\sigma = v^{-1}\ {}^{\sigma}v$, $\sigma \in \mathrm{Gal}(F|E)$. Applying again Weil's cocycle criterion to the G-cover $v \circ f_F : X \to \mathcal{C}_E \times_E F$, $u_{\sigma\tau} = u_\sigma\ {}^{\sigma}u_\tau$, $\sigma, \tau \in \mathrm{Gal}(F|E)$ implies that there exists a G-cover $f_E : X_E \to \mathcal{C}_E$ and a $F$-isomorphism $u$ from $f$ to $f_E \times_E F$ such that $u_\sigma = u^{-1}\ {}^{\sigma}u$, $\sigma \in \mathrm{Gal}(F|E)$. The problem is that one cannot assert, in general, that $\mathcal{C}_E(E) \neq \emptyset$ and, so, $\mathcal{C}_E$ may not be isomorphic to $\mathbb{P}^1$ over $E$. This is exactly what our cohomological obstruction encodes.

PROPOSITION 2.5: *Assume that $Z(G)$ is trivial. Then the prestack of models $\mathcal{PS}_{G/PGL_2}(f)$ is a gerbe over $k$ if and only if for any finite extension $E/k$ the cohomological obstruction $I_E(f) \subset \mathrm{H}^1(E, \mathrm{PGL}_2(\overline{E}))$ is either empty or contains only the trivial class. The if condition remains true without the assumption that $Z(G)$ is trivial.*

*Proof.* Let $f : X \to \mathbb{P}^1_{\overline{k}}$ such that, for any finite extension $E/k$, either $I_E(f)$ is empty or contains only the trivial class. We may assume that $f$ is a normalized representative. Then, with the notation of condition (S) above, the map $v : \mathrm{Gal}(F|E) \to \mathrm{PGL}_2(F)$ sending $\sigma$ to $v_\sigma$ is a 1-cocycle the cohomology class of which $[v] \in \mathrm{H}^1(\mathrm{Gal}(F|E), \mathrm{PGL}_2(F))$ injects by inflation in $I_E(f)$. If $I_E(f) = \emptyset$, then condition (S) above is trivially satisfied and the proposition is straightforward. If $I_E(f)$ contains only the trivial class in $\mathrm{H}^1(E, \mathrm{PGL}_2(\overline{E}))$, then $[v]$ becomes trivial in $\mathrm{H}^1(E, \mathrm{PGL}_2(\overline{E}))$ but, as inflation is injective, $[v]$ is already trivial in $\mathrm{H}^1(\mathrm{Gal}(F|E), \mathrm{PGL}_2(F))$ that is, there exists $v_0 \in \mathrm{PGL}_2(F)$ such that $v_\sigma = v_0^{-1}\ {}^\sigma v_0$, $\sigma \in \mathrm{Gal}(F|E)$. Applying Weil's cocycle criterion to $v_0 \circ f$ then yields the conclusion of condition (S).

Conversely, suppose that $Z(G)$ is trivial and $\mathcal{PS}_{G/PGL_2}(f)$ is a stack over $k$. If $I_E(f) \neq \emptyset$, any $[v] \in I_E(f)$ can be represented by a 1-cocycle $v : \Gamma_k \to \mathrm{PGL}_2(\overline{k})$ such that for any $\sigma \in \Gamma_k$ there exists a G-cover isomorphism $u_\sigma$ between ${}^\sigma f$ and $v_\sigma^{-1} \circ f$. The assumption that $Z(G)$ is trivial ensures that $u$ also satisfies Weil's cocycle conditions. Now, choose a Galois extension $F/E$ over which $f$ is defined and $[v]$ becomes trivial (that is $[v]$ can be regarded as an element of $H^1(\mathrm{Gal}(F|E), \mathrm{PGL}_2(F))$, which, by inflation, injects in $\mathrm{H}^1(E, \mathrm{PGL}_2(\overline{E}))$). Then, the stack condition (S) implies that there exists a G-cover $f_E : X_E \to \mathbb{P}^1_E$ and a G/$\mathrm{PGL}_2$-isomorphism $(u_0, v_0)$ defined over $F$ between $f_E \times_E F$ and $f$ such that $(u_\sigma, v_\sigma) = (u_0^{-1}\ {}^\sigma u_0, v_0^{-1}\ {}^\sigma v_0)$, $\sigma \in \mathrm{Gal}(F|E)$. In particular, $[v]$ is trivial in $H^1(\mathrm{Gal}(F|E), \mathrm{PGL}_2(F))$ thus in $\mathrm{H}^1(E, \mathrm{PGL}_2(\overline{E}))$. ∎

The above discussion also provides a geometrical description of the cohomological obstruction $I_k(f)$. Indeed, recall that a twist of $\mathbb{P}^1_k$ over $k$ is a pair $(\mathcal{C}/k, \phi)$, where $\mathcal{C}/k$ is a smooth, geometrically irreducible projective curve over $k$ and $\phi : \mathcal{C} \times_k \overline{k} \tilde{\to} \mathbb{P}^1_{\overline{k}}$ is a $\overline{k}$-isomorphism. Then, classically, $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ classifies the isomorphism classes of twists of $\mathbb{P}^1_k$ over $k$ (the trivial class corresponding to the trivial twist $(\mathbb{P}^1_k, \mathrm{Id})$). The twists corresponding to $I_k(f) \subset \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ are precisely those twists $\theta = (\mathcal{C}/k, \phi)$ such that there exists a G-cover $f_\theta : X_\theta \to \mathcal{C}$ defined over $k$ with $f_\theta \times_k \overline{k}$ G-isomorphic to $f$ over $\overline{k}$.

2.3. A VARIANT FOR RAMIFICATION DIVISORS. The notions and construction of Sections 2.1 and 2.2 can be extended to ramification divisors. Indeed, given an integer $r \geq 3$ and $\mathbf{t} \in \mathcal{U}_r(\overline{k})$, the conjugacy class $\mathcal{S}_{\mathbf{t}}$ of the stabilizer $S_{\mathbf{t}}$ of $\mathbf{t}$ in $\mathrm{PGL}_2(\overline{k})$ is an invariant of the $\mathrm{PGL}_2(\overline{k})$-orbit $\mathbf{t}^{rd} \in \mathcal{J}_r(\overline{k})$ of $\mathbf{t}$. Let $S^0_{\mathbf{t}}$ be the representative of $\mathcal{S}_{\mathbf{t}}$ which appears in (1) of Lemma 2.1 and call it the **normalized stabilizer** of $\mathbf{t}$; we will denote by $N^0_{\mathbf{t}}$ and $Q^0_{\mathbf{t}}$ the corresponding normalizer and $\Gamma_k$-module quotient. A **normalized representative of $\mathbf{t}$** is a representative $\mathbf{t}_0$ of the $\mathrm{PGL}_2(\overline{k})$-orbit $\mathbf{t}^{rd}$ of $\mathbf{t}$ such that $S_{\mathbf{t}_0} = S^0_{\mathbf{t}}$. Now, assume that $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$. Then, following exactly the pattern of Section 2.2, the set of normalized representative $\mathbf{t}_0$ of $\mathbf{t}^{rd}$ defines a set of equivalent 1-cocycle $\overline{c}_{\mathbf{t}_0} : \Gamma_k \to Q^0_{\mathbf{t}}$. We write $[\overline{c}]_{\mathbf{t}^{rd}}$ for the corresponding cohomology class and we define the **lifting cohomological obstruction of $\mathbf{t}^{rd}$ over $k$** by $I_k(\mathbf{t}^{rd}) = i(p^{-1}([\overline{c}]_{\mathbf{t}^{rd}}))$. We have the analog of Proposition 2.4.

PROPOSITION 2.6 (Cohomological obstruction): *Let $k_0/k$ be a field extension. Then $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$ can be lifted to a ramification divisor $\mathbf{t} \in \mathcal{U}_r(k_0)$ if and only if $I_{k_0}(\mathbf{t}^{rd})$ contains the trivial cohomology class.*

## 3. Criteria for the lifting problem

We have now a cohomological tool to deal with the lifting problem.

3.1. NON EMPTINESS OF $I_k(f)$. Let us start by studying when one can assert that, given a G-cover $f : X \to \mathbb{P}^1_k$ with field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover, the cohomological obstruction $I_k(f)$ of $f$ over $k$ is not empty. This problem is partially answered by the following proposition.

PROPOSITION 3.1: *Let $E$ be any of the groups listed in* (1) *of Lemma 2.1 and denote as usual by $N$ and $Q = N/E$ the corresponding normalizer and quotient $\Gamma_k$-module. Then, the canonical map of pointed sets $p : \mathrm{H}^1(k, N) \to \mathrm{H}^1(k, Q)$ is surjective (and so $I_k(f) \neq \emptyset$) except possibly when $E = C_n$, $n \geq 2$ or $E = V_4$.*

*Proof.* If $E = \mathcal{S}_4, \mathcal{A}_5$ then $Q$ is trivial and there is nothing to prove. If $E = \mathcal{A}_4$ then $N = \mathcal{S}_4$ and $N$ is isomorphic, as a $\Gamma_k$-module, to $\mathcal{A}_4 \rtimes \mathbb{Z}/2\mathbb{Z}$ (a $\Gamma_k$-invariant complement of $\mathcal{A}_4$ in $\mathcal{S}_4$ being, for instance, the group generated by $\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$). Thus, we have a split short exact sequence of $\Gamma_k$-modules

$$1 \longrightarrow E \longrightarrow N \longrightarrow Q \longrightarrow 1. \tag{5}$$

And, if we apply the functor $\mathrm{H}^1(k,\cdot)$ to (5), we get the split short exact sequence of pointed sets

$$1 \longrightarrow \mathrm{H}^1(k,E) \longrightarrow \mathrm{H}^1(k,N) \longrightarrow \mathrm{H}^1(k,Q) \longrightarrow 1.$$

and, in particular, the surjectivity of $p : \mathrm{H}^1(k,N) \to \mathrm{H}^1(k,Q)$.

If $E = D_{2n} \simeq \mu_n \rtimes \mathbb{Z}/2$, $n \geq 3$, then $p : \mathrm{H}^1(k,N) \to \mathrm{H}^1(k,Q)$ is the map induced by functoriality from the $\Gamma_k$-module epimorphism $p : \mu_{2n} \rtimes \mathbb{Z}/2 \to \mu_2$ sending $(x,1)$ to $x^n$. Consider the following commutative diagram of short exact sequences of $\Gamma_k$-modules (where the vertical arrows are the natural inclusions).

(6)
$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mu_n & \longrightarrow & \mu_{2n} & \xrightarrow{(\cdot)^n} & \mu_2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & E & \longrightarrow & N & \xrightarrow{p} & \mu_2 & \longrightarrow & 1 \end{array}$$

If we apply the functor $\mathrm{H}^1(k,\cdot)$ to (6), we get the following commutative diagram of pointed sets with exact rows.

$$\begin{array}{ccccccccc} \cdots & \longrightarrow & \mathrm{H}^1(k,\mu_n) & \longrightarrow & \mathrm{H}^1(k,\mu_{2n}) & \xrightarrow{(\cdot)^n} & \mathrm{H}^1(k,\mu_2) & \xrightarrow{\delta} & \mathrm{H}^2(k,\mu_n) \\ & & \downarrow & & \downarrow & & \| & & \\ \cdots & \longrightarrow & \mathrm{H}^1(k,E) & \longrightarrow & \mathrm{H}^1(k,N) & \xrightarrow{p} & \mathrm{H}^1(k,\mu_2) & & \end{array}$$

As the last vertical arrow is a group isomorphism, the map $p$ is surjective if and only if the group morphism $\mathrm{H}^1(k,\mu_{2n}) \stackrel{(\cdot)^n}{\to} \mathrm{H}^1(k,\mu_2)$ is. But via the canonical isomorphisms $\mathrm{H}^1(k,\mu_{2n}) \tilde{\to} k^\star/(k^\star)^{2n}$, $\mathrm{H}^1(k,\mu_2) \tilde{\to} k^\star/(k^\star)^2$, the group morphism $\mathrm{H}^1(k,\mu_{2n}) \stackrel{(\cdot)^n}{\to} \mathrm{H}^1(k,\mu_2)$ is $k^\star/(k^\star)^{2n} \stackrel{(\cdot)^n}{\to} k^\star/(k^\star)^2$, which is straightforwardly surjective. ∎

Remark 3.2: (1) If $E = V_4$ then $N = \mathcal{S}_4$ and $N$ is isomorphic, as a group, to $V_4 \rtimes (\mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z})$ but the short exact sequence

$$1 \to V_4 \to \mathcal{S}_4 \to \mathbb{Z}/3\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \to 1,$$

which splits in the category of groups does not in the category of $\Gamma_k$-modules when $i \notin k$.

(2) If $E = C_n$, $n \geq 2$, the proof of Corollary 3.3 shows that $p$ is surjective if and only if, for any quadratic extension $L/k$ the natural map $\mathrm{Br}(L|k) \xrightarrow{n} \mathrm{Br}(L|k)$ is surjective.

3.2. Fields of cohomological dimension $\leq 1$.

Corollary 3.3 (Fields of cohomological dimension $\leq 1$): *Let $k$ be a field of characteristic 0.*

(1) *If $k$ has 2-cohomological dimension $\mathrm{cd}_2(k) \leq 1$ then for any $G$-cover $f$ with field of moduli $k$ as $G/PGL_2$-cover the cohomological obstruction $I_k(f)$ only consists of the trivial class. In particular the prestack $\mathcal{PS}_{G/PGL_2}(f)$ is a stack and the natural map $\mathcal{H}(\mathbf{C})(k) \to \mathcal{H}^{rd}(\mathbf{C})(k)$ is surjective.*

(2) *If $k$ has cohomological dimension $\mathrm{cd}(k) \leq 1$ then the natural map $H(\mathbf{C})(k) \to \mathcal{H}^{rd}(\mathbf{C})(k)$ is surjective.*

*Proof.* (1)

Step 1: We first show that under the assumption $cd_2(k) \leq 1$ the map $p : \mathrm{H}^1(k, N) \to \mathrm{H}^1(k, Q)$ is always surjective. From Proposition 3.1, there are two remaining cases to consider: $E = V_4$ and $E = C_n$, $n \geq 2$.

If $E = V_4$ use that 2 is the only prime dividing $|V_4|$ and apply [28, I §5 Proposition 46] to the short exact sequence of $\Gamma_k$-modules

$$1 \to E \to N \to Q \to 1$$

with $I = \{2\}$.

If $E = C_n$, $n \geq 2$, we can even prove that $p$ is bijective. Indeed, $p : \mathrm{H}^1(k, N) \to \mathrm{H}^1(k, Q)$ is the map induced by functoriality from the $\Gamma_k$-module epimorphism $p : k^\star \rtimes \mathbb{Z}/2 \to k^\star \rtimes \mathbb{Z}/2$ sending $(x, 1)$ to $(x^n, 1)$. Consider the following commutative diagram of short exact sequences of $\Gamma_k$-modules, where $s : \mathbb{Z}/2 \to k^\star \rtimes \mathbb{Z}/2$ is the canonical section sending 1 to $(1, 1)$.

(7)

$$\begin{array}{ccccccccc} & & & & & \overset{s}{\curvearrowleft} & & & \\ 1 & \longrightarrow & k^\star & \longrightarrow & N & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle p} & \overset{s}{\curvearrowleft} & \| & & \\ 1 & \longrightarrow & k^\star & \longrightarrow & Q & \longrightarrow & \mathbb{Z}/2 & \longrightarrow & 1 \end{array}$$

If we apply the functor $\mathrm{H}^1(k,\cdot)$ to (7), we get the commutative diagram of pointed sets with exact rows below.

$$
\begin{array}{ccccccc}
\mathrm{H}^1(k,\overline{k}^\star) & \longrightarrow & \mathrm{H}^1(k,\overline{k}^\star \rtimes \mathbb{Z}/2) & \overset{\pi}{\underset{s}{\rightleftarrows}} & \mathrm{H}^1(k,\mathbb{Z}/2) & \longrightarrow & \star \\
\downarrow & & \downarrow p & & \| & & \\
\mathrm{H}^1(k,\overline{k}^\star) & \longrightarrow & \mathrm{H}^1(k,\overline{k}^\star \rtimes \mathbb{Z}/2) & \overset{\pi}{\underset{s}{\rightleftarrows}} & \mathrm{H}^1(k,\mathbb{Z}/2) & \longrightarrow & \star
\end{array}
\tag{8}
$$

To prove the bijectivity of $p$ in (8), we prove that the two last horizontal arrows $\pi$ are bijective. Given a quadratic character $\chi \in \mathrm{H}^1(k,\mathbb{Z}/2)$, denote by $L_\chi$ the fixed field of $\ker(\chi)$ in $\overline{k}$. The point is that the Brauer group $\mathrm{Br}(L_\chi|k)$ (which becomes trivial under our assumption) maps surjectively onto the fiber $\pi^{-1}(\chi)$. Indeed, let $s(\chi) : \Gamma_k \to k^\star \rtimes \mathbb{Z}/2$ be the canonical 1-cocycle lifting $\chi$. The $\Gamma_k$-module $k^\star$ twisted by $s(\chi)$ is the group $k^\star$ equipped with the $\Gamma_k$-module structure $\sigma \cdot x = \sigma(x)^{-1}$ if $\sigma \notin \ker(\chi)$ and $\sigma \cdot x = \sigma(x)$ if $\sigma \in \ker(\chi)$; we denote it by ${}_{s(\chi)}\overline{k}^\star$. Then, by [28, I §5, Corollary 2], there is a natural surjective map $\mathrm{H}^1(k,\ {}_{s(\chi)}\overline{k}^\star) \twoheadrightarrow \pi^{-1}(\chi)$.

Then, we prove that $\mathrm{H}^1(k,\ {}_{s(\chi)}\overline{k}^\star)$ is isomorphic to $\mathrm{Br}(L_\chi|k)$. Consider the inflation-restriction exact sequence

$$
0 \to \mathrm{H}^1(\Gamma_k/\Gamma_{L_\chi}, ({}_{s(\chi)}\overline{k}^\star)^{\Gamma_{L_\chi}}) \to \mathrm{H}^1(\Gamma_k, {}_{s(\chi)}\overline{k}^\star) \to \mathrm{H}^1(\Gamma_{L_\chi}, {}_{s(\chi)}\overline{k}^\star). \tag{9}
$$

As a $\Gamma_{L_\chi}$-module, ${}_{s(\chi)}\overline{k}^\star$ is just $\overline{L}_\chi^\star$, hence, by Hilbert 90, the last term of (9) is trivial. Thus, by exactness, $\mathrm{H}^1(\Gamma_k/\Gamma_{L_\chi}, ({}_{s(\chi)}\overline{k}^\star)^{\Gamma_{L_\chi}})$ is isomorphic to $\mathrm{H}^1(\Gamma_k, {}_{s(\chi)}\overline{k}^\star)$. But $\Gamma_k/\Gamma_{L_\chi} = \mathrm{Gal}(L_\chi|k)$ is just $\mathbb{Z}/2$ so, by the cohomology of cyclic groups [28, VIII, §4], $\mathrm{H}^1(\Gamma_k/\Gamma_{L_\chi}, ({}_{s(\chi)}\overline{k}^\star)^{\Gamma_{L_\chi}})$ is isomorphic to

$$
\ker({}_{s(\chi)}N)/\mathrm{im}({}_{s(\chi)}D),
$$

where ${}_{s(\chi)}N$ and ${}_{s(\chi)}D$ are the norm and derivation for the twisted action. If we denote by $N$ and $D$ the norm and derivation for the usual action, a direct computation shows that $\ker({}_{s(\chi)}N) = \ker(D)$ and $\mathrm{im}({}_{s(\chi)}D) = \mathrm{im}(N)$ thus $\mathrm{H}^1(\Gamma_k/\Gamma_{L_\chi}, ({}_{s(\chi)}\overline{k}^\star)^{\Gamma_{L_\chi}})$ is isomorphic to $\mathrm{H}^2(\Gamma_k/\Gamma_{L_\chi}, L_\chi^\star) = \mathrm{Br}(L_\chi|k)$.

Finally, as $L_\chi/k$ is a quadratic extension, $\mathrm{Br}(L_\chi|k)$ is contained in the 2-torsion subgroup of $\mathrm{Br}(k)$, which is trivial by assumption. So $\pi^{-1}(\chi)$ consists of one single element, which yields the injectivity. And the surjectivity is straightforward since $\pi : \mathrm{H}^1(k,\overline{k}^\star \rtimes \mathbb{Z}/2) \to \mathrm{H}^1(k,\mathbb{Z}/2)$ admits a section.

STEP 2: From the first step $I_k(f) \neq \emptyset$. We can show now that it consists only of the trivial cohomology class because, under our assumption, $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ is trivial. Indeed, consider the canonical short exact sequence of $\Gamma_k$-modules

$$1 \to \mu_2 \to \mathrm{SL}_2(\overline{k}) \to \mathrm{PGL}_2(\overline{k}) \to 1.$$

It gives rise to the exact sequence of pointed sets

$$\mathrm{H}^1(k, \mathrm{SL}_2(\overline{k})) \to \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k})) \xrightarrow{\delta} \mathrm{H}^2(k, \mu_2). \tag{10}$$

But, on the one hand, $\mathrm{H}^1(k, \mathrm{SL}_2(\overline{k}))$ is trivial by Hilbert 90 and, on the other hand, $cd_2(k) \leq 1$ implies that $\mathrm{H}^2(k, \mu_2)$ is trivial too.

(2) By the above, any G-cover $f : X \to \mathbb{P}^1_k$ with field of moduli $k$ as $\mathrm{G}/\mathrm{PGL}_2$-cover is $\mathrm{G}/\mathrm{PGL}_2$-isomorphic to a G-cover $f_0 : X_0 \to \mathbb{P}^1_k$ with field of moduli $k$ as G-cover. Now, since $cd(k) \leq 1$, the group $\mathrm{H}^2(k, Z(G))$ is trivial and thus, $f_0$ is defined over $k$ [9]. (Alternatively, using gerbes, by (1) the prestack $\mathcal{PS}_{G/PGL_2}(f)$ is a gerbe. But any gerbe over a field of cohomological dimension $\leq 1$ is neutral [12].) ∎

Using that any number field $k$ is an intersection of fields of cohomological dimension $\leq 1$ [7, Proposition 2.7], we obtain the following corollary.

COROLLARY 3.4: *For any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(\overline{\mathbb{Q}})$ the field $\kappa(\mathbf{p}^{rd})$ is the intersection of the fields $\kappa(\mathbf{p})$ for all $\mathbf{p} \in \Pi^{-1}(\mathbf{p}^{rd})$.*

3.3. *p*-ADIC FIELDS. For $p$-adic fields $k/\mathbb{Q}_p$ (which are of cohomological dimension 2), we obtain an upper bound which only depends on $k$ and not on $r \geq 3$.

COROLLARY 3.5: *Let $k/\mathbb{Q}_p$ be a $p$-adic field. Then there exists an integer $d(k) \geq 1$ depending only on $k$ such that, for any finite group $G$, any $r$-tuple $\mathbf{C}$ of nontrivial conjugacy classes of $G$ and any $k$-rational point $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$, we have*

$$\mathrm{m}_k(\mathbf{p}^{rd}) \leq d(k).$$

*Proof.* From [28, IV, Theorem 4] the set $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ is finite. In particular, there exists a finite extension $k_0/k$ such that the image of the restriction

$\mathrm{Res}_k^{k_0} : \mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k})) \to \mathrm{H}^1(k_0, \mathrm{PGL}_2(\overline{k}))$ is trivial. So, if $f : X \to \mathbb{P}^1_k$ is a representative of the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of G-covers corresponding to $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$, $I_{k_0}(f)$ is either empty or contains only the trivial class. The former can only occur if $f$ has normalized base group $V_4$ or $C_n$, $n \geq 2$. But, by Lemma 3.7, up to replacing $k_0$ by a degree $\leq 6$ extension $k_0'/k_0$, we can always assert that $I_{k_0'}(f)$ is not empty. So the bound $d(k) = 6[k_0 : k]$ works. ∎

Another classical problem in arithmetic geometry is the existence of local-global properties. Given a number field $k$ and a place $v$ of $k$, we write $k_v/k$ for the completion of $k$ at $v$. Then, we have the following partial result.

COROLLARY 3.6 (Partial local-global principle): *Fix a finite group $G$ and an $r$-tuple $\mathbf{C}$ of nontrivial conjugacy classes of $G$. Then, for any $k$-rational point $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a $G$-cover with trivial base invariant, $\mathrm{m}_k(\mathbf{p}^{rd}) = 1$ if and only if $\mathrm{m}_{k_v}(\mathbf{p}^{rd}) = 1$ for all places $v$ of $k$.*

*Proof.* Let $f : X \to \mathbb{P}^1_k$ be a representative of the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of G-covers corresponding to $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$. Then, as $f$ has trivial base group, $I_k(f)$ contains exactly one class $[c]_f$. Hence, the conclusion follows from the local-global principle for $\mathrm{H}^1(k, \mathrm{PGL}_2(\overline{k}))$ (or, equivalently, for quadratic forms [27, IV.3, Theorem 8]). ∎

3.4. THE GENERAL CASE. In this section $k$ is any field of characteristic 0.

3.4.1. *Nontrivial base invariant.* Let $E$ be one of the groups listed in Lemma (1) of 2.1, let $N$ be its normalizer and $Q := N/E$ the resulting $\Gamma_k$-module quotient. Assume that $E$ is not trivial. We define

$$\begin{aligned} d(E) = & 1 \quad \text{if } E = \mathcal{A}_5, \mathcal{S}_4,\ D_{2n},\ n \geq 3 \text{ odd}, \\ & 2 \quad \text{if } E = \mathcal{A}_4,\ D_{2n},\ n \geq 3 \text{ even}, C_n,\ n \geq 2, \\ & 6 \quad \text{if } E = V_4. \end{aligned}$$

Recall the notation $p$ and $i$ of diagram (4).

LEMMA 3.7: *For any $[\overline{c}] \in \mathrm{H}^1(k, Q)$ there exists a finite extension $k_{[\overline{c}]}/k$ such that $[k_{[c]} : k] \leq d(E)$ and $i(p^{-1}(\mathrm{Res}_k^{k_{[c]}}[\overline{c}])) \subset \mathrm{H}^1(k_{[c]}, \mathrm{PGL}_2(\overline{k}))$ contains the trivial class.*

*Proof.* If $E = \mathcal{A}_5$, $\mathcal{S}_4$ then $E = N$ and $Q$ is trivial so there is nothing to prove. If $E = D_{2n}$, $n \geq 3$ odd then $N = D_{4n}$ and we are in the situation of Lemma 2.2.

If $E = C_n$, $n \geq 2$, recall the notation of diagram (8). As above, to $\chi = \pi([\overline{c}]) \in \mathrm{H}^1(k, \mathbb{Z}/2)$ corresponds the quadratic extension $L_\chi/k$ and the restriction map $\mathrm{Res}_k^{L_\chi} : \mathrm{H}^1(k, \mathbb{Z}/2) \to \mathrm{H}^1(L_\chi, \mathbb{Z}/2)$ sends $\chi$ to the trivial class. So the restriction map $\mathrm{Res}_k^{L_\chi} : \mathrm{H}^1(k, N) \to \mathrm{H}^1(L_\chi, N)$ sends $s(\chi)$ to the trivial class. But, by definition, $\mathrm{Res}_k^{L_\chi}(s(\chi)) \in p^{-1}(\mathrm{Res}_k^{L_\chi}[\overline{c}])$. So we can take $k_{[\overline{c}]} = L_\chi$.

If $E = \mathcal{A}_4$, $D_{2n}$, $n \geq 3$ or $V_4$ then $Q$ is a trivial $\Gamma_k$-module thus $\mathrm{H}^1(k, Q)$ is the set of all group morphisms $\Gamma_k \to Q$ (modulo inner conjugation by elements of $Q$). So, if we write once again $k_{[\overline{c}]}$ for the fixed field of $\ker([\overline{c}])$ in $\overline{k}$ then we have $[k_{[\overline{c}]} : k] \leq |Q|$ and $\mathrm{Res}_k^{k_{[\overline{c}]}}([\overline{c}])$ is the trivial class in $\mathrm{H}^1(k_{[\overline{c}]}, Q)$. So, in particular, $p^{-1}(\mathrm{Res}_k^{k_{[\overline{c}]}}([\overline{c}]))$ contains the trivial class. ∎

Now, Lemma 3.7 combined with Proposition 2.6 and Proposition 2.4 yields respectively Corollary 3.8 and Corollary 3.9 below.

Corollary 3.8 (Lifting ramification divisors with nontrivial stabilizer): *For any $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$ with nontrivial normalized stabilizer $S$ we have $\mathrm{m}_k(\mathbf{t}^{rd}) \leq d(S)$.*

Corollary 3.9 (Lifting G-covers with nontrivial base invariant): *Let $G$ be a finite group and $\mathbf{C}$ be an $r$-tuple of nontrivial conjugacy classes of $G$. Then, for any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a $G$-cover with nontrivial normalized base group $E$ we have $\mathrm{m}_k(\mathbf{p}^{rd}) \leq d(E)$.*

3.4.2. *Trivial base invariant.*

Lemma 3.10: *For any $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$ we have $\mathrm{m}_k(\mathbf{t}^{rd}) \leq r!$*

*Proof.* For this, we consider the following commutative square, where $\Pi_r$ and $\Pi^r$ are the quotient map modulo $\mathrm{PGL}_2$ whereas $\Sigma_r$, $\Sigma_r^{rd}$ are the quotient map modulo the symmetric group $\mathcal{S}_r$.

$$\begin{array}{ccc} \mathcal{U}^r & \xrightarrow{\Pi^r} & \mathcal{U}^r/\mathrm{PGL}_2 \\ {\scriptstyle \Sigma_r}\downarrow & & \downarrow{\scriptstyle \Sigma_r^{rd}} \\ \mathcal{U}_r & \xrightarrow{\Pi_r} & \mathcal{J}_r \end{array} \tag{11}$$

All the morphisms in (11) are defined over $\mathbb{Q}$. Furthermore, the map $s^r : \mathcal{U}^r/\mathrm{PGL}_2 \to \mathcal{U}^r$ sending $\mathrm{PGL}_2\mathbf{t}' \in \mathcal{U}^r/\mathrm{PGL}_2$ to its unique representative of the

form $(0, 1, \infty, \lambda^r(\mathbf{t}')) \in \mathcal{U}^r$ is a section of $\Pi_r : \mathcal{U}^r \to \mathcal{U}^r/\mathrm{PGL}_2$ defined over $\mathbb{Q}$. So the conclusion follows from the fact $\Sigma_r^{rd}$ has degree $\leq r!$. ∎

Given an integer $r \geq 3$ there are only finitely many conjugacy classes of finite subgroups of $\mathrm{PGL}_2(\overline{k})$ of the form $\mathcal{S}_{\mathbf{t}}$ with $\mathbf{t} \in \mathcal{U}_r(\overline{k})$ so we can define $c(r) = \max\{|S^0_{\mathbf{t}}| : \mathbf{t} \in \mathcal{U}_r(\overline{k})\}$ (more precisely, $c(2s+1) = 4s+2$, $s \geq 1$ and $c(2s) = 4s$, $s \geq 2$ except in the following cases: $c(2s) = 60$ for $s = 6$, 10 and $c(2s) = 24$ for $s = 3$, 4, see the proof of Lemma 3.12 for a proof of this assertion).

Corollary 3.11 (Lifting G-covers): *Let $G$ be a finite group and $\mathbf{C}$ be an $r$-tuple of nontrivial conjugacy classes of $G$. Then, for any $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ we have $\mathrm{m}_k(\mathbf{p}^{rd}) \leq r!c(r)$.*

*Proof.* In the case of a nontrivial base invariant, Corollary 3.9 solves the problem. So, let $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a G-cover $f : X \to \mathbb{P}^1_{\overline{k}}$, with trivial base group and ramification divisor $\mathbf{t} \in \mathcal{U}_r(\overline{k})$. Then, according to Lemma 3.10, we may assume that there exists a finite extension $k_0/k$ with $[k_0 : k] \leq r!$ and such that $\mathbf{t} = \Sigma_r(\mathbf{t}')$ for some $\mathbf{t}' \in \mathcal{U}^r(k_0)$. Now, for any $\sigma \in \Gamma_{k_0}$ we have a commutative square.

$$\begin{array}{ccc} X & \xrightarrow{u_\sigma} & {}^\sigma X \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle {}^\sigma f} \\ \mathbb{P}^1_{\overline{k}} & \xrightarrow{v_\sigma} & \mathbb{P}^1_{\overline{k}} \end{array}$$

As $f$ has a trivial base group, the map $v : \Gamma_{k_0} \to S_{\mathbf{t}}$ sending $\sigma$ to $v_\sigma$ is a well-defined 1-cocycle. Furthermore, $S_{\mathbf{t}}$ is a trivial $\Gamma_{k_0}$-module so $\mathrm{H}^1(k_0, S_{\mathbf{t}})$ is just the set of all group morphisms $\Gamma_{k_0} \to S_{\mathbf{t}}$ modulo inner automorphism of $S_{\mathbf{t}}$. In particular, if $k_0'$ is the fixed field of $\ker([v])$ in $\overline{k}$, then $[k_0' : k_0] \leq |S_{\mathbf{t}}| \leq c(r)$ and $\mathrm{Res}^{k_0'}_{k_0}([v])$ is trivial in $\mathrm{H}^1(k_0', S_{\mathbf{t}})$, that is $v_\sigma = \mathrm{Id}$, $\sigma \in \Gamma_{k_0'}$ and $f$ has field of moduli $k_0'$ as G-cover. ∎

3.4.3. *Lifting ramification divisors and hyperelliptic curves.* For $g \geq 1$ and $r = 2(g+1)$, $\mathcal{J}_r$ is the coarse moduli space for genus $g$ hyperelliptic curves and for any $\mathbf{t}^{rd} \in \mathcal{J}_r(\overline{k})$ corresponding to the isomorphism class of an hyperelliptic curve $X_{\mathbf{t}^{rd}}$, the stabilizer $S_{\mathbf{t}}$ is isomorphic to the automorphism group $\mathrm{Aut}(X_{\mathbf{t}^{rd}})$ modulo the hyperelliptic involution $i$. An hyperelliptic curve $X_{\mathbf{t}^{rd}}/\overline{k}$ is said to be **hyperelliptically defined over** $k$ if it admits a $k$-model $X_k/k$ with equation

$y^2 = P(x)$, where $P \in k[x]$ and $\mathrm{disc}(P) \neq 0$ or, equivalently, if $\mathrm{m}_k(\mathbf{t}^{rd}) = 1$. This provides a reformulation of Corollary 3.8 in terms of hyperelliptic curves.

When $g = 1$ or $g \geq 2$ is even, a genus $g$ hyperelliptic curve $X/\overline{k}$ is defined over $k$ if and only if it is hyperelliptically defined over $k$ [24]. This is no longer true when $g \geq 3$ is odd [17].

In the case of divisors with nontrivial stabilizers Corollary 3.8 can be improved as follows.

LEMMA 3.12: *For any $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$ with normalized stabilizer $S$ we have the following.*

(1) *If $r = 3, 4$ then $\mathrm{m}_k(\mathbf{t}^{rd}) = 1$.*
(2) *If $r \geq 5$ and $r \equiv 1, 2, 3 \bmod 4$ then $\mathrm{m}_k(\mathbf{t}^{rd}) = 1$ if $S$ is non cyclic; and $\mathrm{m}_k(\mathbf{t}^{rd}) \leq 2$ if $S$ is cyclic nontrivial.*

*Proof.* (1) For $r = 3$, there is nothing to prove. For $r = 4$, we use that $\mathcal{J}_4$ is a coarse moduli space for elliptic curves. For any $\mathbf{t} \in \mathcal{U}_4(\overline{k})$ such that $\mathbf{t}^{rd} \in \mathcal{J}_4(k)$, denote by $E_{\mathbf{t}^{rd}}/\overline{k}$ the associated (isomorphism class of) elliptic curve(s). Then, $E_{\mathbf{t}^{rd}}/\overline{k}$ has field of moduli $k$. But, by [29, I §4, Proposition 4.5], the field of moduli of an elliptic curve is its minimal field of definition. So there exists an elliptic curve $E/k$ defined over $k$ such that $E_{\overline{k}}$ is isomorphic to $E_{\mathbf{t}^{rd}}$. And, if $Y^2 = X^3 + AX + B$ is a Weierstrass equation for $E$, with $A, B \in k$ then the roots $x_1$, $x_2$, $x_3$, of $X^3 + AX + B$ produce a $k$-rational lift $\{x_1, x_2, x_3, \infty\} \in \mathcal{U}_4(k)$ of $\mathbf{t}^{rd}$.

(2) We consider separately the case $r \equiv 2 \bmod 4$ and $r \equiv 1, 3 \bmod 4$. For the $r \equiv 2 \bmod 4$ case, we use that $\mathcal{J}_r$ is the coarse moduli space for genus $g$ hyperelliptic curves (with $r = 2(g-1)$). Then, by [19, Theorem 5.4] and [24], any genus $g$ hyperelliptic curve $X$ such that the automorphism group of $X$ modulo the hyperelliptic involution is non cyclic is hyperelliptically defined over its field of moduli. Now, the conclusion follows from Corollary 3.8 for nontrivial cyclic groups. For the $r = 2s + 1$ case, and, even for general $r$, one can determine precisely which finite subgroups of $\mathrm{PGL}_2(\overline{k})$ occur as stabilizers of order $r$ subsets of the projective line. For this, let $E$ be one of the groups listed in (1) of Lemma 2.1 and consider the Galois cover $\Pi_E : \mathbb{P}^1 \to \mathbb{P}^1/E$. Then any $\mathbf{t} \in \mathcal{U}_r(\overline{k})$ with stabilizer $E$ is a disjoint union of fibers of $\Pi_E$. Now, Riemann–Hurwitz gives the ramification indices of $\Pi_E$, which are listed below.

| $E$ | $\mathcal{A}_5$ | $\mathcal{S}_4$ | $\mathcal{A}_4$ | $D_{2n}$, $n \geq 2$ | $C_n$, $n \geq 2$ |
|---|---|---|---|---|---|
| Ramification indices of $\Pi_E$ | $(2,3,5)$ | $(2,3,4)$ | $(2,3,3)$ | $(2,2,n)$ | $(n,n)$ |

In particular, $E$ stabilizes order $r$ subsets of the projective line if and only if $r$ is of the form listed below.

| $E$ | $r$ |
|---|---|
| $\mathcal{A}_5$ | $r = \epsilon_1 30 + \epsilon_2 20 + \epsilon_3 12 + m60$ |
| $\mathcal{S}_4$ | $r = \epsilon_1 12 + \epsilon_2 8 + \epsilon_3 6 + m24$ |
| $\mathcal{A}_4$ | $r = \epsilon_1 6 + (\epsilon_2 + \epsilon_3)4 + m12$ |
| $D_{2n}$, $n \geq 2$ | $r \equiv 0, 2, n, n+2 [\mathrm{mod}\ 2n]$ |
| $C_n$, $n \geq 2$ | $r \equiv 0, 1, 2 [\mathrm{mod}\ n]$ |

with $\epsilon_i = 0, 1$, $i = 1, 2, 3$ and $m \geq 0$. In particular, for odd value of $r$, the only possible groups are the cyclic groups and the dihedral groups $D_{2n}$, $n \geq 2$ with $n$ odd. So we can conclude with Corollary 3.8. ∎

Combining Lemma 3.10, Lemma 3.12 and [19, Theorem 5.4] yields the following statement about hyperelliptic curves in characteristic 0.

COROLLARY 3.13: *For any integer $g \geq 2$, an hyperelliptic curve $X$ of genus $g$ can be hyperelliptically defined over a degree $\leq (2g+2)!$ extension of its field of moduli. Furthermore, if the automorphism group of $X$ modulo the hyperelliptic involution is noncyclic, then $X$ can be defined over its field of moduli and if it is cyclic nontrivial then $X$ can be defined over a quadratic extension of its field of moduli.*

REMARK 3.14 (Optimality of the bounds): It is not clear whether the bounds given in Corollary 3.9 are optimal. However, for $E = C_n$, $n \geq 6$ the bound 2 is optimal. Indeed, let $G$ be $\mathbb{Z}/2\mathbb{Z}$ and let $\mathbf{C}$ be $r := 2(3n-1)+2$ copies of the nontrivial conjugacy class of $G$. For each $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ there is only one isomorphism class of G-cover with invariants $G$, $\mathbf{C}$, $\mathbf{t}$; we denote this G-cover by $f_{\mathbf{t}}$. Furthermore, the base group $E_{f_{\mathbf{t}}}$ of $f_{\mathbf{t}}$ is precisely $S_{\mathbf{t}}$. Indeed, $E_{f_{\mathbf{t}}}$ is contained in $S_{\mathbf{t}}$ and for any $v \in S_{\mathbf{t}}$, both G-covers $f_{\mathbf{t}}$ and $v \circ f_{\mathbf{t}}$ have invariants $G$, $\mathbf{C}$, $\mathbf{t}$ so they are isomorphic as G-covers. The same argument, combined with the fact an involution class is always $\mathbb{Q}$-rational, shows that the field of moduli of $f_{\mathbf{t}}$ as G-cover is the field of definition $\mathbb{Q}(\mathbf{t})$ of $\mathbf{t}$ and the field of moduli of $f_{\mathbf{t}}$ as $\mathrm{G}/\mathrm{PGL}_2$-cover is the field of definition $\mathbb{Q}(\mathbf{t}^{rd})$ of $\mathbf{t}^{rd}$. Now, we are going to

choose a special value of $\mathbf{t}$. Consider a genus $3n-1$ hyperelliptic curve $X_n/\overline{\mathbb{Q}}$ as those studied in [19, Lemma 5.5 and Proposition 5.6]. The automorphism group of $X_n$ modulo the hyperelliptic involution is the cyclic group $C_n$ and the field of moduli of $X_n$ is contained in $k := \mathbb{R}\cap\overline{\mathbb{Q}}$ but $X_n$ is not defined over $k$. If $n \geq 6$ is odd then $3n-1$ is even and, hence, any $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ such that $X_{\mathbf{t}^{rd}}$ is isomorphic to $X_n$ has a stabilizer $\mathcal{S}_{\mathbf{t}}$ isomorphic to $C_n$ but $\mathbf{t} \notin \mathcal{U}_r(k)$. In terms of G-covers, $f_{\mathbf{t}}$ has base invariant $C_n$, its field of moduli as $\mathrm{G/PGL_2}$-cover is contained in $k$ but its field of moduli as G-cover is not, so, according to Corollary 3.9 the field of moduli of $f_{\mathbf{t}}$ as G-cover is a quadratic extension of the field of moduli of $f_{\mathbf{t}}$ as $\mathrm{G/PGL_2}$-cover.

3.5. The profinite case. For a few years, the profinite aspects of regular inverse Galois theory have been focussed on, in particular with the development of Fried's modular towers theory [15], [8], [4], [3] etc.

In this setting, most of the conjectures are stated for reduced Hurwitz towers but they are usually easier to tackle for nonreduced ones. For instance, the modular tower conjecture [3, Conjecture 2.1] predicts that for any integer $d \geq 1$ and any reduced modular tower $\underline{\mathcal{H}}^{rd} = (\mathcal{H}^{rd}_{n+1} \to \mathcal{H}^{rd}_n)_{n\geq 0}$ we have $(\mathcal{H}^{rd}_n)^{(d)}(\mathbb{Q}) = \emptyset$ for $n >> 0$, where, given a $k$-variety $X$ and an integer $d \geq 1$, we write $X^{(d)}$ for the image of the diagonal morphism from $X$ into the $d$th-symmetric product $X \times_k \cdots \times_k X/\mathcal{S}_d$ (in particular, $X^{(d)}(k) = \bigcup_{[K:k]\leq d} X(K)$).

Now, let $((G_{n+1}, \mathbf{C}_{n+1}) \twoheadrightarrow (G_n, \mathbf{C}_n))_{n\geq 0}$ be a complete projective system of finite groups and $r_n$-tuples of nontrivial conjugacy classes. We consider the corresponding Hurwitz tower $(\mathcal{H}(\mathbf{C}_{n+1}) \to \mathcal{H}(\mathbf{C}_n))_{n\geq 0}$ and reduced Hurwitz tower $(\mathcal{H}^{rd}(\mathbf{C}_{n+1}) \to \mathcal{H}^{rd}(\mathbf{C}_n))_{n\geq 0}$. Assume first that $r_n \leq r$, $n \geq 0$ for some $r \geq 3$. Then, Corollary 3.11 implies that, if for some $d \geq 1$, we have $\mathcal{H}(\mathbf{C}_n)^{(r!c(r)d)}(k) = \emptyset$, $n >> 0$ then $\mathcal{H}^{rd}(\mathbf{C}_n)^{(d)}(k) = \emptyset$, $n >> 0$. In particular, the modular tower conjecture (for all $d$) for reduced modular towers and nonreduced ones are equivalent.

Another consequence of Corollary 3.11 is that one can lift projective systems of $k$-rational points from reduced towers of Hurwitz spaces to nonreduced ones.

Corollary 3.15: *Let $\mathbf{p}^{rd} = (p^{rd}_n)_{n\geq 0} \in \varprojlim \mathcal{H}^{rd}(\mathbf{C}_n)(k)$ be a projective system of $k$-rational points on a reduced tower of Hurwitz spaces. Then there exists a finite field extension $k_0/k$ (depending on $\mathbf{p}^{rd}$) such that $\mathbf{p}^{rd}$ can be lifted to*

*a projective system* $\mathbf{p} = (p_n)_{n\geq 0} \in \varprojlim \mathcal{H}(\mathbf{C}_n)(k_0)$ *of* $k_0$*-rational points on the nonreduced tower up to a finite extension.*

*Proof.* Let $(f_n : X_n \to \mathbb{P}^1_k, \alpha_n)_{n\geq 0}$ be a projective system of G-covers corresponding to $\mathbf{p}^{rd}$. For each $n \geq 0$, $\sigma \in \Gamma_k$, write $\mathcal{H}_{\sigma,n}$ for the set of all $\mathrm{G}/\mathrm{PGL}_2$-isomorphisms from $f_n$ to ${}^\sigma f_n$. This defines a projective system of nonempty finite sets $(\mathcal{H}_{\sigma,n+1} \to \mathcal{H}_{\sigma,n})_{n\geq 0}$. To check this, for any $n \geq 0$ write $G_{n+1,n}$ for the automorphism group of the Galois cover $f_{n+1,n} : X_{n+1} \to X_n$. Fix $\sigma \in \Gamma_k$ and $(u, v)$ a $\mathrm{G}/\mathrm{PGL}_2$-isomorphism from $f_n$ to ${}^\sigma f_n$. Then, by definition of G-covers, for all $g \in \mathrm{Aut}(f_{n+1})$, we have ${}^\sigma\alpha_{n+1}(ugu^{-1}) = \alpha_{n+1}(g)$ and ${}^\sigma\alpha_{n+1}({}^\sigma g) = \alpha_{n+1}(g)$, so $ugu^{-1} = {}^\sigma g$. In particular, $uG_{n+1,n}u^{-1} = {}^\sigma G_{n+1,n}$ and, hence, $u(X_n) = {}^\sigma X_n$. So $(u, v) \in \mathcal{H}_{\sigma,n+1}$ induces the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism $(u|^{{}^\sigma X_n}_{X_n}, v) \in \mathcal{H}_{\sigma,n}$, whence the projectivity. The fact that $\mathcal{H}_{\sigma,n}$ is finite is straightforward and the fact it is nonempty results from the assumption that $p_n^{rd}$ is a $k$-rational point, $n \geq 0$.

Now, choose $((u_{\sigma,n}), v_\sigma)_{n\geq 0} \in \varprojlim \mathcal{H}_{n,\sigma}$. This defines the profinite commutative diagram below.

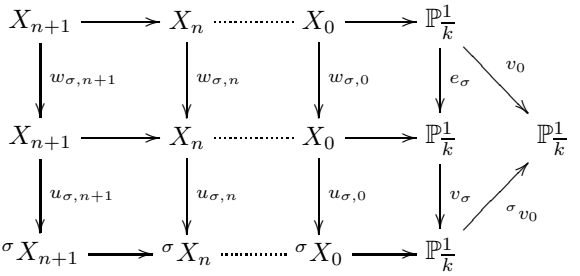
$$\begin{array}{ccccccc}
X_{n+1} & \longrightarrow & X_n & \cdots\cdots & X_0 & \longrightarrow & \mathbb{P}^1_{\overline{k}} \\
\downarrow{\scriptstyle u_{\sigma,n+1}} & & \downarrow{\scriptstyle u_{\sigma,n}} & & \downarrow{\scriptstyle u_{\sigma,0}} & & \downarrow{\scriptstyle v_\sigma} \\
{}^\sigma X_{n+1} & \longrightarrow & {}^\sigma X_n & \cdots\cdots & {}^\sigma X_0 & \longrightarrow & \mathbb{P}^1_{\overline{k}}
\end{array}$$

In particular, we have a decreasing sequence of finite subgroups

$$\cdots < E_{f_{n+1}} < E_{f_n} < \cdots < E_{f_0} < \mathrm{PGL}_2(\overline{k})$$

which is stationary for $n \geq n_0$. Without loss of generality, we may assume $n_0 = 0$. Up to replacing the projective system $(f_n)_{n\geq 0}$ by a projective system $(vf_n)_{n\geq 0}$ for some $v \in \mathrm{PGL}_2(\overline{k})$, we can assume $E_{f_0} = E$ is one of the groups listed in Lemma 2.1. Then the map $c : \Gamma_k \to Q$ sending $\sigma$ to $v_\sigma E$ is a well-defined 1-cocycle and it defines a cohomology class $[c] \in \mathrm{H}^1(k, Q)$. Let $k_0/k$ be a finite extension such that $[c]$ becomes trivial in $\mathrm{H}^1(k_0, Q)$. Then the trivial class in $\mathrm{H}^1(k_0, N)$ trivially lifts $[c]$. That is, there exists $v_0 \in \mathrm{PGL}_2(\overline{k})$ such that for any $\sigma \in \Gamma_{k_0}$ we have $v_\sigma e_\sigma = v_0^{-1}\, {}^\sigma v_0$ for some $e_\sigma \in E$. The same argument as above ensures that this does not affect the fact we have a profinite commutative diagram. Indeed, for each $n \geq 0$ denote by $\mathcal{U}_{\sigma,n}$ the set of all the $\mathrm{G}/\mathrm{PGL}_2$ automorphisms of $f_n$ restricting to $e_\sigma$. This, once again, yields

a projective system of nonempty finite sets $(\mathcal{U}_{\sigma,n+1} \to \mathcal{U}_{\sigma,n})_{n\geq 0}$. Then, any $(w_{\sigma,n})_{n\geq 0} \in \varprojlim \mathcal{U}_{n,\sigma}$ yields a profinite commutative diagram




showing that $(v_0 f_n)_{n\geq 0}$ is a projective system of G-covers with field of moduli $k_0$ thus corresponding to a projective system of $k_0$-rational points $\mathbf{p} = (p_n)_{n\geq 0} \in \varprojlim \mathcal{H}(\mathbf{C}_n)(k_0)$ lifting $\mathbf{p}^{rd}$. ∎

Let $k$ be either a number field or a finite field of characteristic $\neq p$ and let $\tilde{G}$ be a profinite extension of a finite group $G$ by a pro-$p$ group $P$ admitting a quotient isomorphic to $\mathbb{Z}_p$. Then [3, Theorem 2.5] states that there is no Galois extension $K/\overline{k}(T)$ with group $\tilde{G}$ and field of moduli $k$. Combining this and Corollary 3.15, we obtain the following results for reduced towers of Hurwitz spaces[2].

COROLLARY 3.16: *Assume that in Corollary 3.15 $G := \varprojlim G_n$ is an extension of a finite group $G$ by a pro-$p$ group $P$ such that $P \twoheadrightarrow \mathbb{Z}_p$. Then, for any number field $k$ we have $\varprojlim \mathcal{H}^{rd}(\mathbf{C}_n)(k) = \emptyset$.*

## 4. Topological characterization of the base invariant

The aim of this section is to explain how the base invariant can be read out off the Nielsen class. In Section 4.1, we recall how to compute explicitly the monodromy of the cover $\Psi : \mathcal{H}(\mathbf{C}) \to \mathcal{U}_r$. We apply this to give a partition of the Nielsen class encoding the base invariant. Finally, Section 4.2 describes entirely the cases $r = 3$, 4, which play an important part in our applications.

[2] In [20], K. Kimura gives a different proof of Corollary 3.15 (cf. [20, Lemma 5.2]) as well as a proof of the special case of Corollary 3.16 for Fried's modular towers (cf. [20, Theorem 5.4]).

4.1. The braid action. Let $\mathbf{t} = \{t_1, \dots, t_r\} \in \mathcal{U}_r(\overline{\mathbb{Q}})$ and choose $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \mathbf{t}$. Denote by $\mathcal{B}_0$ the set of all orientation preserving diffeomorphisms of $\mathbb{P}^1(\mathbb{C})$ with the compact-open topology.

With this topology, the evaluation map $\epsilon_{\mathbf{t}} : \mathcal{B}_0 \to \mathcal{U}_r(\mathbb{C})$ sending $h$ to $\{h(t_1), \dots, h(t_r)\}$ becomes a locally trivial fibration. So, we can consider the cobord morphism of its associated long exact homotopy sequence

$$\delta_{\mathbf{t}} : \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \to \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t}))$$

which sends a homotopy class $[\gamma]$ to the connected component of the unique continuous map $\tilde{\gamma} : [0,1] \to \mathcal{B}_0$ such that $\tilde{\gamma}(0) = \mathrm{Id}$ and $\epsilon_{\mathbf{t}} \circ \tilde{\gamma} = \gamma$. Then, $\delta_{\mathbf{t}}$ is an epimorphism ($\pi_0(\mathcal{B}_0) = 1$) and its kernel is the center $Z(\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}))$ of $\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$.

On the other hand, we have a natural representation

$$a_{\mathbf{t}} : \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) \to \mathrm{Out}(\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t})),$$

sending the connected component of $h \in \mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})$ to the outer automorphism of $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$ induced by composition by $h$.

The resulting morphism $\Lambda_{\mathbf{t}} = a_{\mathbf{t}} \circ \delta_{\mathbf{t}} : \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \to \mathrm{Out}(\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}))$ is called the **braid action**. It can be explicitly described by choosing specific generators of $\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$, $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}, t_0)$. Proceed as follows. Let $c : [0,1] \to \mathbb{P}^1(\mathbb{C})$ be a continuous injective closed path such that there exists $0 < s_1 < \cdots < s_r < 1$ with $c(s_i) = t_i$, $i = 1, \dots, r$. Then $c$ divides $\mathbb{P}^1(\mathbb{C})$ into two connected components $\mathcal{C}_1$, "on the left" and $\mathcal{C}_2$, "on the right". Next, choose two tuples $\mathbf{c} = (c_1, \dots, c_r)$, $\mathbf{d} = (d_1, \dots, d_{r-1})$ of continuous injective closed paths with

- $d_i = d_{i,1} \cdot d_{i,2}$ where $d_{i,1}$ is a continuous injective arc joining $t_i$ to $t_{i+1}$ in $\mathcal{C}_1$ and $d_{i,2}$ is a continuous injective arc joining $t_{i+1}$ to $t_i$ in $\mathcal{C}_2$, $i = 1, \dots, r-1$.

- $c_i = \alpha_i \beta_i \alpha_i^{-1}$ where $\beta_i$ is a small circle around $t_i$ and $\alpha_i$ is a continuous injective arc joining $t_0 \in \mathcal{C}_2$ to a point of $\mathcal{C}_2 \cap \beta_i$, $i = 1, \dots, r$. We require furthermore that $c_i \cap c_j = \{t_0\}$, $1 \leq i \neq j \leq r$ and that the group morphism $F_r / \langle \Gamma_1 \cdots \Gamma_r \rangle \to \pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}))$ sending $\Gamma_i$ to $[c_i]$, $i = 1, \dots, r$ be an isomorphism.

With this notation, let $[\delta_i] \in \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t}))$ be the Dehn twist around $d_i$ (see [2]) and $[q_i] \in \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$ be the braid induced by the path

$$q_i : [0,1] \to \mathcal{U}_r(\mathbb{C}), \quad t \to (t_1, \dots, t_{i-1}, d_{i,1}(t), d_{i,2}(t), t_{i+2}, \dots, t_r).$$

One then checks that $\delta_{\mathbf{t}}([q_i]) = [\delta_i]$ and that $a_{\mathbf{t}}([\delta_i])$ sends the $r$-tuple $\mathbf{c}$ to

$$(c_1, \ldots, c_{i-1}, c_{i+1}, c_i^{c_{i+1}^{-1}}, c_{i+2}, \ldots, c_r), \quad i = 1, \ldots, r-1.$$

Finally, we introduce the Hurwitz braid group $H_r$ given by the generators $Q_1, \ldots, Q_{r-1}$ and the relations

(1) $Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}$, $i = 1, \ldots, r-1$;
(2) $Q_iQ_j = Q_jQ_i$, $|j-i| > 2$;
(3) $Q_1 \cdots Q_{r-1}Q_{r-1} \cdots Q_1 = 1$.

The center $Z(H_r)$ of $H_r$ is generated by the involution $(Q_1 \cdots Q_{r-1})^r$; the quotient $M_r := H_r/Z(H_r)$ is the **mapping class group**. From [2], we have the following presentation result.

PROPOSITION 4.1: *The map $\mu$ sending $[q_i] \in \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$ to $Q_i \in H_r$ is a well-defined group isomorphism and we have the following commutative diagram with exact rows*

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z(H_r) & \longrightarrow & H_r & \longrightarrow & M_r & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \mu} & & \uparrow{\scriptstyle \mu} & & \uparrow{\scriptstyle \overline{\mu}} & & \\
1 & \longrightarrow & Z(\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})) & \longrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) & \xrightarrow{\delta_{\mathbf{t}}} & \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) & \longrightarrow & 1.
\end{array}$$

The next proposition gives an explicit description of the monodromy of the ramification divisor cover $\Psi : H(\mathbf{C}) \to \mathcal{U}^r(\mathbf{C})$ in terms of G-covers.

PROPOSITION 4.2: *For any $[f] \in \Psi^{-1}(\mathbf{t})$, and any continuous map $q : [0,1] \to \mathcal{U}_r(\mathbb{C})$ such that $q(0) = \mathbf{t}$, let $\overline{q} : [0,1] \to \mathcal{B}_0$ be the unique continuous map such that $\overline{q}(0) = \mathrm{Id}$ and $\epsilon_{\mathbf{t}} \circ \overline{q} = q$. Then the map $\tilde{q} : [0,1] \to \mathcal{H}(\mathbb{C})$ sending $t$ to $[\overline{q}(t) \circ f]$ is a well-defined continuous map such that $\Psi \circ \tilde{q} = q$ and $\tilde{q}(0) = [f]$.*

Let $M_{\mathbf{C}} : \Psi^{-1}(\mathbf{t}) \tilde{\to} \overline{\mathrm{ni}}(\mathbf{C})$ be the **monodromy bijection defined by c**, that is, the map sending the G-isomorphism class of a G-cover $(f, \alpha)$ to the $r$-tuple $(\alpha \circ M_{c_1}(f), \ldots, \alpha \circ M_{c_r}(f)) \in \overline{\mathrm{ni}}(\mathbf{C})$, where $M_{c_i}(f)$ denotes the monodromy action of $c_i$, $i = 1, \ldots, r$. Propositions 4.1 and 4.2 gives a group theoretic description of the monodromy of $\Psi$.

THEOREM 4.3: *Via the monodromy bijection $M_{\mathbf{c}} : \Psi^{-1}(\mathbf{t}) \to \overline{\mathrm{ni}}(\mathbf{C})$ and the group isomorphism $\mu : \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \to H_r$, the monodromy action for the*

*cover* $\Psi : \mathcal{H}(\mathbb{C}) \to \mathcal{U}_r(\mathbb{C})$ *becomes*

$$Q_i \cdot \mathbf{g} = (g_1, \dots, g_{i-1}, g_{i+1}^{g_i}, g_i, g_{i+2}, \dots, g_r), \quad i = 1, \dots, r-1.$$

Actually, given a braid $Q \in H_r$ and a $r$-tuple $\mathbf{g} \in \overline{\mathrm{ni}}(\mathbf{C})$, the element $Q \cdot \mathbf{g}$ only depends on $\delta_{\mathbf{t}}(Q)$ so the action $H_r \times \overline{\mathrm{ni}}_r(G) \to \overline{\mathrm{ni}}_r(G)$ induces a well-defined action $M_r \times \overline{\mathrm{ni}}_r(G) \to \overline{\mathrm{ni}}_r(G)$. In the following, we will not always distinguish these two actions. Given $[h] \in \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t}))$ we will write $Q_h$ for $\overline{\mu}([h]) \in M_r$ and call it, by abuse of language, **the braid associated to** $[h]$.

Given $\mathbf{t} \in \mathcal{U}_r(\overline{\mathbb{Q}})$, denote by $\mathcal{S}_{\mathbf{t}}$ the set of all the subgroups of $S_{\mathbf{t}}$. Also choose $\mathbf{c} = (c_1, \dots, c_r)$, $\mathbf{d} = (d_1, \dots, d_{r-1})$, $\mathbf{q} = (q_1, \dots, q_{r-1})$ as in Section 4.1. For any $E \in \mathcal{S}_{\mathbf{t}}$ we define the **E-Nielsen class associated with C and t** as the subset of all $\mathbf{g} \in \overline{\mathrm{ni}}(\mathbf{C})$ such that $\mathbf{g} \sim Q_v \mathbf{g}$, $v \in E$ and $\mathbf{g} \not\sim Q_v \mathbf{g}$, $v \notin E$.

By the monodromy bijection $M_{\mathbf{c}} : \Psi^{-1}(\mathbf{t}) \to \overline{\mathrm{ni}}(\mathbf{C})$ the $E$-Nielsen class $\overline{\mathrm{ni}}_E(\mathbf{C})$ corresponds to those G-covers $f$ with invariants $G$, $\mathbf{t}$, $\mathbf{C}$ and $E_f = E$. These sets define a partition of the Nielsen class when $E$ describes $\mathcal{S}_{\mathbf{t}}$ .

The next section provides a complete description for the cases $r = 3, 4$.

4.2. The cases $r = 3, 4$. Recall the notation of Proposition 4.1 and consider the following commutative diagram with exact rows, where $\nu$, $\overline{\nu}$ are the canonical inclusions.

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Z(H_r) & \longrightarrow & H_r & \longrightarrow & M_r & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \mu} & & \uparrow{\scriptstyle \mu} & & \uparrow{\scriptstyle \overline{\mu}} & & \\
1 & \longrightarrow & Z(\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})) & \longrightarrow & \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) & \xrightarrow{\delta_{\mathbf{t}}} & \pi_0(\mathrm{Stab}_{\mathcal{B}_0}(\mathbf{t})) & \longrightarrow & 1 \\
 & & \uparrow{\scriptstyle \nu} & & \uparrow{\scriptstyle \nu} & & \uparrow{\scriptstyle \overline{\nu}} & & \\
1 & \longrightarrow & Z(\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})) & \longrightarrow & \delta_{\mathbf{t}}^{-1}(\mathrm{Stab}_{\mathrm{PGL}_2(\overline{\mathbb{Q}})}(\mathbf{t})) & \xrightarrow{\delta_{\mathbf{t}}} & \mathrm{Stab}_{\mathrm{PGL}_2(\overline{\mathbb{Q}})}(\mathbf{t}) & \longrightarrow & 1
\end{array}$$

The aim of this section is to describe the images of $\overline{\mu} \circ \overline{\nu}$ in terms of $Q_1, \dots, Q_r$. The general method is (1) to compute explicitly $S_{\mathbf{t}}$, (2) to compute the action of each $e \in S_{\mathbf{t}}$ on a topological bouquet $\mathbf{c} = (c_1, \dots, c_r)$ and (3) identify this action with a braid (modulo $Z(H_r)$) $Q_e$. It can be carried out for all $r \geq 3$ but, for effective applications, we will need only the cases $r = 3, 4$.

4.2.1. *The case* $r = 3$. When $r = 3$, the Hurwitz braid group

$$H_3 = \langle Q_1, (Q_1 Q_2)^2 \mid Q_1^2 = (Q_1 Q_2 Q_1)^2 = (Q_1 Q_2)^3 = 1 \rangle$$

is finite and isomorphic to $\mathbb{Z}/3 \rtimes \mathbb{Z}/4$. So, $M_3 = \langle Q_1Q_2 \rangle \rtimes \langle Q_1 \rangle$ is isomorphic to $D_6$. Furthermore, any $\mathbf{t} \in \mathcal{U}_3(\overline{\mathbb{Q}})$ is conjugate to $\{1, \zeta_3, \overline{\zeta}_3\}$, which has stabilizer $D_6$. So, when $r = 3$ the canonical inclusions $\nu$ and $\overline{\nu}$ are isomorphisms.

4.2.2. *The case $r = 4$.* When $r = 4$, recall the $j$-morphism $j : \mathcal{U}_4 \to \mathbb{P}^1$ is defined by the following commutative diagram

$$\begin{array}{ccc} \mathcal{U}^4 & \xrightarrow{f_{(1,2,3)}} & \mathbb{P}^1 \\ {\scriptstyle \pi_4}\downarrow & & \downarrow{\scriptstyle j_0} \\ \mathcal{U}_4 & \overset{j}{\dashrightarrow} & \mathbb{P}^1, \end{array}$$

where $f_{(1,2,3)}$ is the map sending $\underline{\lambda} = (\lambda_1, \lambda_2, \lambda_3, \lambda_4) \in \mathbb{P}^1$ to $\frac{(\lambda_4-\lambda_1)(\lambda_2-\lambda_3)}{(\lambda_4-\lambda_3)(\lambda_2-\lambda_1)} \in \mathcal{U}^4$ and $j_0$ the map sending $\lambda \in \mathbb{P}^1$ to $\frac{2^8}{1728}\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$. Furthermore, $j$ is $\mathrm{PGL}_2$-invariant and factorizes through

$$\begin{array}{ccc} \mathcal{U}_4 & \xrightarrow{\quad j \quad} & \mathbb{P}^1 \\ {\scriptstyle \Pi_4}\downarrow & \nearrow_{\overline{j}} & \\ \mathcal{U}_4/\mathrm{PGL}_2 & & \end{array},$$

where $\overline{j}$ is an isomorphism. So, $j$ classifies the $\mathrm{PGL}_2$-orbits of $\mathcal{U}_4$ and, in particular, the conjugacy class of $S_{\mathbf{t}}$ in $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ depends only on $j(\mathbf{t})$.

THEOREM 4.4: *Let $\mathbf{t} \in \mathcal{U}_4(\overline{\mathbb{Q}})$ then the group $S_{\mathbf{t}}$ is conjugate in $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ to $V_4$ if $j(\mathbf{t}) \neq 0, 1$, $D_8$ if $j(\mathbf{t}) = 1$ and $\mathcal{A}_4$ if $j(\mathbf{t}) = 0$. Furthermore,*

*if $j(\mathbf{t}) \neq 0, 1$ then $S_{\mathbf{t}}$ can be identified with* $\langle (Q_1Q_2Q_3)^2, Q_1Q_3^{-1} \rangle \simeq V_4 \subset M_4$;

$j(\mathbf{t}) = 1$ $\quad \langle Q_1Q_2Q_3, Q_1Q_3^{-1} \rangle \simeq D_8 \subset M_4$;

$j(\mathbf{t}) = 0$ $\quad \langle (Q_1Q_2Q_3)^2, Q_2Q_3 \rangle \simeq \mathcal{A}_4 \subset M_4$.

*Proof.* The conjugacy class of the stabilizer $S_{\mathbf{t}}$ of $\mathbf{t} \in \mathcal{U}_4$ depends only on its j-invariant $j(\mathbf{t})$. We now compute effectively this stabilizer and use the results of Subsection 4.1 to compute the preimage of $S_{\mathbf{t}}$ via $\delta_{\mathbf{t}}$. Let $\lambda \in j_0^{-1}(j(\mathbf{t}))$ and set $\mathbf{t}_\lambda := \{0, 1, \infty, \lambda\} \in \mathcal{U}_4(\overline{\mathbb{Q}})$. Then any $v \in S_{\mathbf{t}_\lambda}$ sends $\{0, 1, \infty\}$ to one of the four following sets

(12) (a) $\{0, 1, \infty\}$ (b) $\{0, 1, \lambda\}$ (c) $\{0, \lambda, \infty\}$ (d) $\{\lambda, 1, \infty\}$,

with the additional conditions

$$\text{(13)} \qquad \text{(a) } v(\lambda)=\lambda \quad \text{(b) } v(\lambda)=\infty \quad \text{(c) } v(\lambda)=1 \quad \text{(d) } v(\lambda)=0.$$

From (12), there are 4 possibilities for $v$.

(1) If $v \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ sends $\{0,1,\infty\}$ to $\{0,1,\infty\}$ then it must be one of the following homographies: $z \to z$, $z \to \frac{1}{z}$, $z \to 1-z$, $z \to \frac{1}{1-z}$, $z \to \frac{z}{z-1}$, $z \to \frac{z-1}{z}$.
(2) If $v \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ sends $\{0,1,\lambda\}$ to $\{0,1,\infty\}$ then it must be one of the following homographies: $z \to \frac{1}{1-\lambda}\frac{z-\lambda}{z}$, $z \to (1-\lambda)\frac{z}{z-\lambda}$, $z \to \lambda\frac{z-1}{z-\lambda}$, $z \to \frac{\lambda-1}{\lambda}\frac{z}{z-1}$, $z \to \frac{\lambda}{\lambda-1}\frac{z-1}{z}$, $z \to \frac{1}{\lambda}\frac{z-\lambda}{z-1}$.
(3) If $v \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ sends $\{0,\lambda,\infty\}$ to $\{0,1,\infty\}$ then it must be one of the following homographies: $z \to \frac{z}{\lambda}$, $z \to \frac{\lambda-z}{\lambda}$, $z \to \frac{z-\lambda}{z}$, $z \to \frac{z}{z-\lambda}$, $z \to \frac{\lambda}{\lambda-z}$, $z \to \frac{\lambda}{z}$.
(4) If $v \in \mathrm{PGL}_2(\overline{\mathbb{Q}})$ sends $\{\lambda,1,\infty\}$ to $\{0,1,\infty\}$ then it must be one of the following homographies: $z \to \frac{z-\lambda}{z-1}$, $z \to \frac{z-1}{\lambda-1}$, $z \to \frac{\lambda-1}{z-1}$, $z \to \frac{z-1}{z-\lambda}$, $z \to \frac{1-\lambda}{z-\lambda}$.

The additional conditions (13) yield three different situations depending on the value of $\lambda$:

(1) If $\lambda \neq -1,\ \frac{1}{2},\ 2,\ \frac{1\pm i\sqrt{3}}{2}$ then the elements stabilizing $\{0,1,\infty,\lambda\}$ in $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ are the homographies: $z \to z$, $z \to \frac{\lambda}{z}$, $z \to \frac{z-\lambda}{z-1}$, $z \to \lambda\frac{z-1}{z-\lambda}$.
(2) If $\lambda = -1$ then the elements stabilizing $\{0,1,\infty,\lambda\}$ in $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ are the homographies: $z \to z$, $z \to \frac{1}{z}$, $z \to \frac{1+z}{1-z}$, $z \to -z$, $z \to \frac{z-1}{z+1}$, $z \to -\frac{1}{z}$, $z \to \frac{z+1}{z-1}$, $z \to \frac{1-z}{1+z}$.
(3) If $\lambda = \frac{1\pm i\sqrt{3}}{2}$ then the elements stabilizing $\{0,1,\infty,\lambda\}$ in $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ are the homographies: $z \to z$, $z \to \frac{z-1}{z}$, $z \to \frac{1}{1-z}$, $z \to \frac{\lambda-1}{\lambda}\frac{z}{z-1}$, $z \to \frac{1}{1-\lambda}\frac{z-\lambda}{z}$, $z \to \frac{\lambda-z}{\lambda}$, $z \to \frac{z}{z-\lambda}$, $z \to \frac{z-1}{\lambda-1}$, $z \to \frac{1-\lambda}{z-\lambda}$, $z \to \frac{\lambda}{z}$, $z \to \frac{z-\lambda}{z-1}$, $z \to \lambda\frac{z-1}{z-\lambda}$.

Finally, to determine the conjugacy class of $S_{\mathbf{t}_\lambda}$, compute the order of the elements and use Lemma 2.1.

We are now reduced to studying only three cases, that is, $j(\mathbf{t}) \neq 0,\ 1$, $j(\mathbf{t})=1$ ($\lambda = -1,\ 1/2,\ 2$) and $j(\mathbf{t})=0$ ($\lambda = \frac{1\pm i\sqrt{3}}{2}$). In each of these three cases, choose a topological bouquet $\mathbf{c}=(c_0,c_1,c_\infty,c_\lambda)$ as explained in §4.1 and compute the action of $S_{\mathbf{t}_\lambda}$ on it. One obtains the following description for $r=4$.

| $\lambda$ | generators of $S_{\mathbf{t}_\lambda}$ | order | corresponding braid (modulo $Z(H_4)$) |
|---|---|---|---|
| $\lambda \neq -1,\ \frac{1}{2},\ 2,\ \frac{1\pm i\sqrt{3}}{2}$ | $z \to \frac{\lambda}{z}$ | 2 | $(Q_1Q_2Q_3)^2$ |
| | $z \to \lambda\frac{z-1}{z-\lambda}$ | 2 | $Q_1^{-1}Q_3$ |
| $\lambda = -1$ | $z \to \frac{1+z}{1-z}$ | 4 | $Q_1Q_2Q_3$ |
| | $z \to \frac{1-z}{1+z}$ | 2 | $Q_1^{-1}Q_3$ |
| $\lambda = \frac{1+i\sqrt{3}}{2}$ | $z \to \frac{1+i\sqrt{3}}{2z}$ | 2 | $(Q_1Q_2Q_3)^2$ |
| | $z \to \frac{z-1}{\frac{(1-i\sqrt{3})}{2}z-1}$ | 2 | $Q_1^{-1}Q_3$ |
| | $z \to \frac{1}{1-z}$ | 3 | $Q_2Q_3$ |

From the generators given in Theorem 4.4, one can recover any $E$-Nielsen class for any subgroup $E$ of $V_4$ ($j(\mathbf{t}) \neq 0, 1$), $D_8$ ($j(\mathbf{t}) = 1$) or $\mathcal{A}_4$ ($j(\mathbf{t}) = 0$).

EXAMPLE 4.5 ($j(\mathbf{t}) \neq 0, 1$): Then $V_4 = \langle (Q_1Q_2Q_3)^2, Q_1^{-1}Q_3\rangle$ has five subgroups:

$$\{1\}, \quad C_1 := \langle (Q_1Q_2Q_3)^2\rangle, \quad C_2 := \langle Q_1^{-1}Q_3\rangle,$$
$$C_3 := \langle (Q_1Q_2Q_3)^2Q_1^{-1}Q_3\rangle \quad \text{and} \quad V_4.$$

Consider now the three relations

$$\text{(4-1)} \quad \mathbf{g} \sim (Q_1Q_2Q_3)^2 \cdot \mathbf{g} = (g_3, g_4, g_2, g_1)$$
$$\text{(4-2)} \quad \mathbf{g} \sim Q_1^{-1}Q_3 \cdot \mathbf{g} = (g_4^{g_3}, g_3, g_2, g_1^{g_2^{-1}})$$
$$\text{(4-3)} \quad \mathbf{g} \sim (Q_1Q_2Q_3)^2Q_1^{-1}Q_3 \cdot \mathbf{g} = (g_2^{g_1}, g_1, g_4, g_3^{g_4^{-1}})$$

and denote by $\overline{(4-1)}$, $\overline{(4-2)}$, $\overline{(4-3)}$ their negation. Then,

$$\overline{\mathrm{ni}}^{rd}_{C_i}(\mathbf{C}) = \{\mathbf{g} \in G^4 : (1),\ (2),\ (3),\ (4-i),\ \overline{(4-j)},\ 1 \leq j \neq i \leq 3\}/\mathrm{Inn}(G), \quad i = 1, 2, 3.$$

$$\overline{\mathrm{ni}}^{rd}_{\{1\}}(\mathbf{C}) = \{\mathbf{g} \in G^4 : (1),\ (2),\ (3),\ \overline{(4-i)},\ 1 \leq i \leq 3\}/\mathrm{Inn}(G).$$

$$\overline{\mathrm{ni}}^{rd}_{V_4}(\mathbf{C}) = \{\mathbf{g} \in G^4 : (1),\ (2),\ (3),\ (4-i),\ 1 \leq i \leq 3\}/\mathrm{Inn}(G).$$

## 5. Finding rational points on Hurwitz spaces

5.1. THE CASES $r = 3,\ 4$. We restrict here to the cases $r = 3,\ 4$, which are the most important ones for effective applications since, when $r = 3$, reduced Hurwitz spaces are finite sets of points and, when $r = 4$, reduced Hurwitz spaces are curves for which we can compute the ramification of the cover

$\Psi^{rd} : \mathcal{H}^{rd}(\mathbf{C}) \to \mathbb{P}^1$ above 0, 1, $\infty$ (Theorem 1.2). But, as we explained in Section 1.2, given a $\mathbb{Q}$-rational point on $\mathcal{H}^{rd}(\mathbf{C})$ it is not obvious at all whether it can be lifted to a $\mathbb{Q}$-rational point on $\mathcal{H}(\mathbf{C})$ or not. However, one can use the lifting property of the ramification divisor $\mathbf{t}$ (Lemma 3.12) to improve Corollary 3.9 in some special cases.

Let $G$ be a finite group and $\mathbf{C}$ be an $r$-tuple of nontrivial conjugacy classes of $G$. Assume that $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponds to a G-cover $f$ with nontrivial normalized base group and such that one of its representative $f_0$ has a ramification divisor $\mathbf{t} \in \mathcal{U}_r(\overline{k})$ with a $\Gamma_k$-invariant stabilizer $S_{\mathbf{t}}$ and a $\Gamma_k$-invariant base group $E_{f_0}$. Then $N_{f_0} \cap S_{\mathbf{t}}$ is globally $\Gamma_k$-invariant and $E_{f_0}$ is normal in $N_{f_0} \cap S_{\mathbf{t}}$. As a result, one can carry out the construction of Section 2.2 with $N_{f_0,\mathbf{t}} := N_{f_0} \cap S_{\mathbf{t}}$ and $Q_{f_0,\mathbf{t}} := N_{f_0,\mathbf{t}}/E_{f_0}$ replacing $N_f^0$ and $Q_f^0$ respectively. For each representative $f_0$ as above, we obtain a cohomology class $[\overline{c}_{f_0}] \in \mathrm{H}^1(k, Q_{f_0,\mathbf{t}})$ (which, this time, may depend on the choice of the representative $f_0$). Then, a sufficient condition for $f$ to be $\mathrm{G}/\mathrm{PGL}_2$-isomorphic to a G-cover with field of moduli $k_0$ as G-cover is that one of the sets $I_{k_0}(f_0) := i(p^{-1}([\overline{c}_{f_0}]))$, for $f_0$ a representative with $\Gamma_k$-invariant ramification divisor and $\Gamma_k$-invariant base group $E_{f_0}$, contains the trivial class.

In the sequel, the groups $C_n$, $n \geq 2$, $D_{2n}$, $n \geq 3$ etc. refer to the particular groups of (1) of Lemma2.1.

Corollary 5.1: *Let $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ corresponding to a G-cover $f$ with nontrivial base group $E$ and reduced ramification divisor $\mathbf{t}^{rd} \in \mathcal{J}_r(k)$. Assume that $\mathrm{m}_k(\mathbf{t}^{rd}) = 1$.*

(1) *If one of the following situation occurs:*

(i) *$E$ is non cyclic and $E = S_{\mathbf{t}}$;*
(ii) *$E \simeq C_n$ and $S_{\mathbf{t}} \simeq D_{2n}$, $n \geq 3$;*
(iii) *$E \simeq C_2$ and $S_{\mathbf{t}} \simeq D_{2n}$, $n \geq 3$ odd.*

*Then $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ can be lifted to a $k$-rational point $\mathbf{p} \in \mathcal{H}(\mathbf{C})(k)$.*

(2) *In particular,*

- *If $r = 3$ then $\mathbf{p}^{rd} \in \mathcal{H}^{rd}(\mathbf{C})(k)$ can be lifted to a $k$-rational point $\mathbf{p} \in \mathcal{H}(\mathbf{C})(k)$.*
- *If $r = 4$ then $\mathrm{m}_k(\mathbf{p}^{rd}) \leq 2$. Furthermore, if $j(\mathbf{t}) = 1$ and $E = C_4$, $D_8$, or if $j(\mathbf{t}) = 0$ and $E = \mathcal{A}_4$, or if $j(\mathbf{t}) \neq 0, 1$ and $E = V_4$ then $\mathbf{p}^{rd}$ can be lifted to a $k$-rational point $\mathbf{p} \in \mathcal{H}(\mathbf{C})(k)$.*

*Proof.* We apply the method described above. (1) By assumption, $\mathrm{m}_k(\mathbf{t}^{rd}) = 1$. So, one can assume that $f$ has a $\Gamma_k$-invariant ramification divisor $\mathbf{t} \in \mathcal{U}_r(k)$. (i) As $E_f = S_{\mathbf{t}}$ we also have $N_{f,\mathbf{t}} = E_f$ and, hence, $Q_{f,\mathbf{t}} = \{1\}$. (ii) By assumption, $E_f$ is the unique order $n$ cyclic subgroup of $S_{\mathbf{t}}$. So $E_f$ is necessarily $\Gamma_k$-invariant since $S_{\mathbf{t}}$ is. As a result, $N_{f,\mathbf{t}} = S_{\mathbf{t}}$ and the conclusion follows from Lemma 2.2. (iii) By Lemma 2.1 there exists $v \in \mathrm{PGL}_2(\overline{k})$ such that $S_{v\mathbf{t}} = D_{2n}$. By assumption, $E_{v\circ f}$ is one of the order 2 subgroups of $S_{v\mathbf{t}}$, which are all conjugate in $S_{v\mathbf{t}}$ since $n \geq 3$ is odd. So, up to replacing $v \circ f$ by $a^k \circ v \circ f$, with $a : z \to \zeta_n z$ for some $k = 0, \ldots, n-1$, we may assume that $E_{v\circ f}$ is the subgroup $C$ of $D_{2n}$ generated by $z \to 1/z$ and, in particular, that it is $\Gamma_k$-invariant. But, then, $N_{v\circ f, v\mathbf{t}} = \mathrm{Nor}_{D_{2n}}(C) = C = E_{v\circ f, v\mathbf{t}}$, whence the conclusion. According to Lemma 3.12, Subsection 4.2.1 and Theorem 4.4, the assertions of (2) are just special cases of (1). ∎

5.2. Effective criteria and examples. Now we can apply the remarks of Section 5.1 to give effective results.

We first recall the group-theoretical description of the projective normalization of the ramification divisor cover $\Psi^{rd} : \mathcal{H}^{rd}(\mathbf{C}) \to \mathcal{J}_4 \simeq \mathbb{P}^1 \setminus \{0, 1, \infty\}$. When $r = 4$, the center of $H_4$ is generated by the involution $(Q_1Q_2Q_3)^4 = (Q_1Q_3^{-1})^2$ and the minimal normal subgroup of $H_4$ containing either $(Q_1Q_2Q_3)^2$ or $Q_1Q_3^{-1}$ is the quaternion group $\mathbb{H}_8 = \langle (Q_1Q_2Q_3)^2, Q_1Q_3^{-1} \rangle$. The resulting quotient $H_4/\mathbb{H}_8$ is given by the generators $\gamma_1 = Q_1Q_2Q_1 (= Q_1Q_2Q_3) \mathrm{mod} \mathbb{H}_8$, $\gamma_\infty = Q_2 \mathrm{mod} \mathbb{H}_8$ and the relations

(1) $\gamma_1^2 = 1$
(2) $\gamma_1\gamma_\infty\gamma_1 = \gamma_\infty^{-1}\gamma_1\gamma_\infty^{-1}$.

So, it is isomorphic to $\mathrm{PSL}_2(\mathbb{Z})$. Hence, we obtain the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathbb{H}_8 & \longrightarrow & H_4 & \longrightarrow & \mathrm{PSL}_2(\mathbb{Z}) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{V}_4 & \longrightarrow & M_4 & \longrightarrow & \mathrm{PSL}_2(\mathbb{Z}) & \longrightarrow & 1 \end{array}$$

Finally, define the reduced Nielsen class $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$ to be the set of $\mathbb{H}_8$-orbits of $\overline{\mathrm{ni}}(\mathbf{C})$ (as $Z(H_4)$ acts trivially on $\overline{\mathrm{ni}}(\mathbf{C})$, $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$ is also the set of $V_4 = \mathbb{H}_8/Z(H_4)$-orbits of $\overline{\mathrm{ni}}(\mathbf{C})$).

THEOREM 5.2 ([1, Propositions 3.4 and 3.28]): *When $r = 4$, the projective normalization $\overline{\Psi}^{rd} : \overline{\mathcal{H}}^{rd}(\mathbf{C}) \to \mathbb{P}^1$ of $\Psi^{rd}$ is a cover ramified above 0, 1, $\infty$ and the ramification is given by the action of $\gamma_0 = Q_1Q_2 \bmod \mathbb{H}_8$, $\gamma_1 = Q_1Q_2Q_1 \bmod \mathbb{H}_8$, $\gamma_\infty = Q_2 \bmod \mathbb{H}_8$ over $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$.*

Given an orbit $O$ of the Nielsen class $\overline{\mathrm{ni}}(\mathbf{C})$ under the Hurwitz group $H_r$ we denote by $O^{rd}$ its associated reduced orbit $\mathbb{H}_8\backslash O$. We will say that $O^{rd}$ is **isolated** if there is no other orbit of $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$ under $H_r$ with length $|O^{rd}|$. This is a sufficient condition to ensure that the corresponding geometrically irreducible component $\mathcal{H}_{O^{rd}}$ of $\mathcal{H}^{rd}(\mathbf{C})$ is defined over $\mathbb{Q}_{\mathbf{C}}$. Considering $\gamma_i$ acting on $O^{rd}$, we will denote its cycle decomposition by $[(1)^{a_{i,1}}, (2)^{a_{i,2}}, \dots, (|O|)^{a_{i,|O^{rd}|}}]$.

We begin with a rigidity criterion.

COROLLARY 5.3 (Rigidity Criterion): *Fix a finite group $G$ and an $r$-tuple $\mathbf{C} = (C_1, \dots, C_r)$ of nontrivial conjugacy classes of $G$. Assume that there exists an isolated orbit $O^{rd}$ of $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$ under $H_4$ such that $a_{1,1} > 0$. Then there exists regular realizations of $G$ over $\overline{\mathbb{Q}}$ with field of moduli a degree $\leq a_{1,1}$ extension of $\mathbb{Q}_{\mathbf{C}}$, inertia canonical invariant $\mathbf{C}$ and ramification divisor with $j$-invariant 1.*

*Proof.* The fact that $O^{rd}$ is isolated ensures that $\mathcal{H}_{O^{rd}}$ is defined over $\mathbb{Q}_{\mathbf{C}}$. Above 1, the $a_{1,1}$ fixed points of $\gamma_1$ corresponds to $a_{1,1}$ $\mathrm{G/PGL}_2$-isomorphism classes of G-covers with ramification divisor having $j$-invariant 1 and normalized base group $C_4$ or $D_8$ (Theorem 4.4). As the set of fixed points of $\gamma_1$ is $\Gamma_{\mathbb{Q}_{\mathbf{C}}}$-invariant, each of these points is defined over a degree $\leq a_{1,1}$ extension of $\mathbb{Q}_{\mathbf{C}}$. The conclusion then follows from (2) of Corollary 5.1. ∎

EXAMPLE 5.4: All the computations were carried out using BRAID for GAP [21], [30]. Also, the notation used for groups and conjugacy classes are those of the ATLAS [6].

Consider $G = \mathcal{A}_7$, $\mathbf{C} = (5A, 5A, 5A, 5A)$. We obtain the following list for the lengths of the reduced orbits

$$(78, 90, 90, 105, 150, 195, 270, 270, 270, 270).$$

The unique reduced orbit $O^{rd}$ of length 195 (and reduced genus 4) has the monodromy data for $\gamma_0$, $\gamma_1$:

$$\text{Type of } \gamma_0 : [(3)^{65}]$$
$$\text{Type of } \gamma_1 : [(1), (2)^{97}]$$

So, the hypotheses of Corollary 5.3 are fulfilled with $a_{1,1} = 1$ and $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}$ (the conjugacy class $5A$ is rational).

Let us now use the genus 0 argument. Let $O^{rd}$ be an orbit of the reduced Nielsen class $\overline{\mathrm{ni}}^{rd}(\mathbf{C})$ under the Hurwitz braid group $H_4$ and denote by $g_{O^{rd}}$ the genus of the corresponding geometrically irreducible component $\mathcal{H}_{O^{rd}}$ of $\mathcal{H}^{rd}(\mathbf{C})$. Riemann-Hurwitz genus formula yields

$$g_{O^{rd}} := 1 - |O^{rd}| + \frac{1}{2} \sum_{i \in \{0,1,\infty\}} \sum_{1 \le j \le |O^{rd}|} a_{i,j}(j-1).$$

COROLLARY 5.5 (Genus 0): *Fix a finite group $G$ and an $r$-tuple $\mathbf{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes of $G$. Assume that there exists an isolated orbit $O$ of $\overline{\mathrm{ni}}(\mathbf{C})$ under $H_4$ such that (i) $g_{O^{rd}} = 0$, (ii) one of the $a_{i,1}, \ldots, a_{i,|O^{rd}|}$ is odd for some $i = 0, 1, \infty$ and (iii)$|O| = |O^{rd}|$. Then there exists regular realizations of $G$ over $\overline{\mathbb{Q}}$ with field of moduli $\mathbb{Q}_{\mathbf{C}}$ and inertia canonical invariant $\mathbf{C}$.*

*Proof.* The fact that $O^{rd}$ is isolated together with conditions (i)–(ii) classically ensures that the geometrically irreducible component $\mathcal{H}_{O^{rd}}$ of $\mathcal{H}^{rd}(\mathbf{C})$ corresponding to $O^{rd}$ is geometrically irreducible, defined over $\mathbb{Q}_{\mathbf{C}}$, has genus 0 and carries an odd degree $\mathbb{Q}_{\mathbf{C}}$-rational divisor. Thus, by Riemann–Roch theorem, it has a dense subset of $\mathbb{Q}_{\mathbf{C}}$-rational points. Let $f$ be a G-cover corresponding to an unramified $\mathbb{Q}_{\mathbf{C}}$-rational point on $\mathcal{H}_{O^{rd}}$. Then $f$ has field of moduli $\mathbb{Q}_{\mathbf{C}}$ as $\mathrm{G}/\mathrm{PGL}_2$-cover and the assumption (iii) $|O| = |O^{rd}|$ ensures that it has normalized base group $V_4$ (Theorem 4.4). The conclusion then follows again from (2) of Corollary 5.1. ∎

EXAMPLE 5.6: Consider $G = L_2(19)$, $\mathbf{C} = (3A, 3A, 3A, 3A)$. We obtain the following list for the lengths of the usual/ reduced orbits and the corresponding reduced genera

$$((126/126, 0), (576/288, 8), (864/216, 1)).$$

The unique reduced orbit $O^{rd}$ of length 126 and reduced genus 0 has the monodromy data:

$$\begin{aligned} \text{Type of } \gamma_0 &: [(1)^6, (3)^{40}] \\ \text{Type of } \gamma_1 &: [(2)^{63}] \\ \text{Type of } \gamma_\infty &: [(2)^3, (3)^2, (5)^4, (9)^6, (10)^4] \end{aligned}$$

So, the hypotheses of Corollary 5.5 are fulfilled with $d = 1$ and $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}$ (the conjugacy class $3A$ is rational). See Shih's theorem [22, I, Theorem 7.9] for a rigid realization of $L_2(19)$ with inertia canonical invariant $(3A, 19A, 19B)$.

5.3. The expansion method. The method described here derives from the geometric description of the stratification of reduced Hurwitz spaces carried out in [5]; we refer to this paper for a structured approach of the method and only focus here on a resulting effective criterion.

Fix a finite group $G$ and a $r$-tuple $\mathbf{C} = (C_1, \dots, C_r)$ of nontrivial conjugacy classes of $G$. Assume that $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$. The expansion method explains how to obtain a regular realization of $G$ over $\mathbb{Q}$ from $\mathbf{p}^{rd}$ provided three of the conjugacy classes in $\mathbf{C}$ are rational.

Given a conjugacy class $C$ in $G$ and an integer $n \geq 1$ we write $C^n$ for the conjugacy class of the $g^n$, $g \in G$ and $[C]^n$ for the $n$-tuple $(C, \dots, C)$. With this notation, the **expanded tuple of C** is

$$\mathrm{Ex}(\mathbf{C}) := ([C_1^2]^{12}, [C_2^3]^8, [C_3^4]^6, [C_4]^{24}, \dots, [C_r]^{24})$$

Proposition 5.7 (Expansion): *Assume that $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$ and that $C_i$ is rational, $i = 1, 2, 3$ then $\mathcal{H}(\mathrm{Ex}(\mathbf{C}))(\mathbb{Q}) \neq \emptyset$.*

*Proof.* The idea is to consider the direct product $G \times \mathcal{S}_4$. Let $nA$ be the conjugacy class of $n$-cycles in the symmetric group $\mathcal{S}_4$. Then the triple $(2A, 3A, 4A)$ is $\mathbb{Q}$-rational and rigid. Also, by assumption, the conjugacy classes $C_i$, $i = 1, 2, 3$ are $\mathbb{Q}$-rational and $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$, which implies that the $r$-tuple $\mathbf{C}$ is $\mathbb{Q}$-rational. As a result, the $r$-tuple

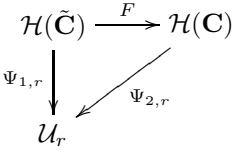
$$\tilde{\mathbf{C}} = ((C_1, 2A), (C_2, 3A), (C_3, 4A), (C_4, 0), \dots, (C_r, 0))$$

is $\mathbb{Q}$-rational. Hence, the natural morphism $\Phi : \mathcal{H}^{rd}(\tilde{\mathbf{C}}) \to \mathcal{H}^{rd}(\mathrm{Ex}(\mathbf{C}))$, which sends the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of a G-cover $f : X \to \mathbb{P}^1$ to the $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of the G-cover $f : X \to X/G \simeq \mathbb{P}^1$ is defined over $\mathbb{Q}$ [3]. But, by construction, any point in the image of $\Phi$ corresponds to a $\mathrm{G}/\mathrm{PGL}_2$-isomorphism class of G-covers with normalized base group $\mathcal{S}_4$. So, in particular,

[3] Note that, by elementary Galois theory, $\mathrm{Ex}(\mathbf{C})$ is the inertia canonical invariant of the factor G-cover $f : X \to X/G$. Note also that, as we work with reduced Hurwitz spaces, the morphism $\Phi$ is well-defined but, a priori, $\Phi$ cannot be lifted to a morphism between nonreduced Hurwitz space because the isomorphism $X/G \simeq \mathbb{P}^1$ is noncanonical. For more details about this morphism $\Phi$ — which, in particular, is a closed immersion, we refer to [5, Section 3 and Section 4].

by Corollary 3.9, any $\mathbb{Q}$-rational point in the image of $\Phi$ can be lifted to a $\mathbb{Q}$-rational point on $\mathcal{H}(\mathrm{Ex}(\mathbf{C}))$.

To conclude, it is enough to prove that $\mathcal{H}(\tilde{\mathbf{C}})(\mathbb{Q}) \neq \emptyset$. Consider the following commutative diagram, where $F : \mathcal{H}(\tilde{\mathbf{C}}) \to \mathcal{H}(\mathbf{C})$ is the natural cover, defined over $\mathbb{Q}$, which corresponds to sending the G-isomorphism class of a G-cover $f : X \to \mathbb{P}^1$ to the G-isomorphism class of the G-cover $f : X/G \to \mathbb{P}^1$.




The rigidity of $(2A, 3A, 4A)$ implies that the ramification divisors morphisms $\Psi_{1,r}$, $\Psi_{2,r}$ have the same degree and, hence, that $F$ is an isomorphism defined over $\mathbb{Q}$. Furthermore, $F$ commute with the action of $\mathrm{PGL}_2$ so, it induces a reduced isomorphism $F^{rd} : \mathcal{H}^{rd}(\tilde{\mathbf{C}}) \tilde{\to} \mathcal{H}^{rd}(\mathbf{C})$ defined over $\mathbb{Q}$. Now, the conclusion follows from $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$. The following diagram sums up the situation.

$$\mathcal{H}^{rd}(\mathbf{C}) \xrightarrow{(F^{rd})^{-1}} \mathcal{H}^{rd}(\tilde{\mathbf{C}}) \xrightarrow{\Phi} \mathcal{H}^{rd}(\mathrm{Ex}(\mathbf{C})) \xleftarrow{\Pi} \mathcal{H}(\mathrm{Ex}(\mathbf{C})). \qquad \blacksquare$$

EXAMPLE 5.8: In particular, starting from a regular realization of a finite group $G$ over $\mathbb{Q}$ with an inertia canonical invariant $\mathbf{C}$ satisfying the hypothesis of Proposition 5.7, one can construct new regular realizations of $G$ over $\mathbb{Q}$ with inertia canonical invariant $\mathrm{Ex}(\mathbf{C})$. Consider, for instance, the Monster M which has been regularly realized over $\mathbb{Q}$ with inertia canonical invariant the triple of $\mathbb{Q}$-rational classes $(2A, 3A, 29A)$. Proposition 5.7 shows that M can also be regularly realized over $\mathbb{Q}$ with inertia canonical invariant $[29A]^6$.

But, the cases when we know that $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$ without knowing that $\mathcal{H}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$ are more significant. So, consider

$$G = L_2(25), \quad \mathbf{C} = (3A, 3A, 3A, 3A).$$

We obtain the following list for the lengths of the usual/reduced orbits and the corresponding reduced genera

$$((1200/300, 7), (936/468, 17), (304/304, 5), (120/30, 0).$$

The unique reduced orbit $O^{rd}$ of length 30 and reduced genus 0 has the monodromy data:

$$\text{Type of } \gamma_0 : [(3)^{10}]$$
$$\text{Type of } \gamma_1 : [(2)^{15}]$$
$$\text{Type of } \gamma_\infty : [(2)^2, (3)^2, (6)^2, (8)^1]$$

So, by the genus 0 argument $\mathcal{H}^{rd}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$ (the conjugacy class $3A$ is rational). We cannot apply Corollary 5.5 and deduce that $\mathcal{H}(\mathbf{C})(\mathbb{Q}) \neq \emptyset$ since hypothesis (iii) is not fulfilled. But the hypotheses of Proposition 5.7 are, which yields a regular realization of $L_2(25)$ over $\mathbb{Q}$ with inertia canonical invariant $[3A]^{42}$. See [26] for a realization of $L_2(25)$ with a different inertia canonical invariant.

## References


[1] P. Bailey and M. D. Fried, *Hurwitz monodromy, spin separation and higher levels of a modular tower*, in *Arithmetic Fundamental Groups and Noncommutative Algebra (Berkeley, CA, 1999)*, Proceedings of Symposia in Pure Mathematics (M. Fried and Y. Ihara, eds.), vol. 70, American Mathematical Soceity, Providence, RI, 2002, pp. 79–220.

[2] J. S. Birman, *Braids, Links and Mapping Class Groups*, Princeton University Press, Princeton, N.J., 1974.

[3] A. Cadoret, *On the profinite regular inverse galois problem*, Publications of the Research Institute for Mathematical Sciences, to appear.

[4] A. Cadoret, *Harbater-Mumford subvarieties of moduli spaces of covers*, Mathematische Annalen **333** (2005), 355–391.

[5] A. Cadoret and A. Tamagawa, *Stratification of Hurwitz spaces by closed modular subvarieties*, Pure and Applied Mathematics Quatterly-Serre issue, to appear.

[6] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of Finite Groups*, Oxford University Press, Eynsham, 1985.

[7] K. Coombes and D. Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Mathematical Journal **52** (1985), 821–839.

[8] P. Dèbes and B. Deschamps, *Corps $\psi$-libres et théorie inverse de Galois infinie*, Journal für die Reine und Angewandte Mathematik **574** (2004), 197–218.

[9] P. Dèbes and J.-C. Douai, *Algebraic covers: field of moduli versus field of definition*, Annales Scientifiques de l'École Normale Superiére **30** (1997), 303–338.

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

[11] P. Dèbes and J.-C. Douai, *Gerbes and covers*, Communications in Algebra **27** (1999), 106–137.

[12] P. Dèbes, J.-C. Douai and M. Emsalem, *Familles de Hurwitz et cohomologie non abélienne*, Annales de l'Institut Fourier **50** (2000), 113–149.

[13] M. Dettweiler, *Plane curve complements and curves on Hurwitz spaces*, Journal für die Reine und Angewandte Mathematik **573** (2004), 19–43.

[14] M. Emsalem, *Espaces de Hurwitz*, in *Arithmétique des Revêtements Algébriques* (B. Deschamps, ed.), Séminaires et Congrès, vol. 5, Soc. Math. France, Paris, 2001, pp. 63–99.

[15] M. Fried, *Introduction to modular towers : generalizing the relation between dihedral groups and modular curves*, in *Proceedings of Summer Conference on recent developments in the inverse Galois problem*, Cont. Math. series, vol. 186, American Mathematical Society - Natural Science Foundation, Providence, RI, 1995, pp. 111–171.

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

[17] Y. Fuertes and G. Gonzalez-Diez, *Fields of moduli and definition of hyperelliptic covers*, Archiv der Mathematik **86** (2006), 398–408.

[18] J. Giraud, *Cohomologie Non Abélienne*, Springer-Verlag, Berlin, 1971.

[19] B. Huggins, *Fiels of moduli of hyperelliptic curves*, Mathematical Research Letter **14** (2007), 249–262.

[20] K. Kimura, *Modular Towers for Finite Groups that may not be Centerfree*, Master's thesis, R.I.M.S. - Kyoto, 2004.

[21] K. Magaard, S. Shpectorov and H. Völklein, *A gap package for braid orbit computations and applications*, Experimental Mathematics **12** (2003), 385–393.

[22] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999.

[23] B. H. Matzat, *Rationality criteria for Galois extensions*, in *Proceedings of Berkeley workshop Galois groups over* $\mathbb{Q}$, Math. Sci. Res. Inst. Publ., vol. 16, Springer-Verlag, New York, 1989, pp. 361–383.

[24] J.-F. Mestre, *Construction de courbes de genre* 2 *à partir de leurs modules*, in *Effective methods in algebraic geometry, Proceedings of the 1990 Castigliano conference*, Prog. Math., vol. 94, Birkh 1991.

[25] D. Mumford and J. Fogarty, *Geometric Invariant Theory, 2nd enlarged ed*, Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 34, Springer-Verlag, Berlin, 1982.

[26] B. Pryzwara, *Die Operation der Hurwitzschen Zopfgruppe auf den Erzengenden Systemklassen Endlicher Gruppen*, Ph.D. thesis, Karlsruhe, 1988.

[27] J.-P. Serre, *Cours d'Arithmétique*, Presses Universitaires de France, Paris, 1970.

[28] J.-P. Serre, *Cohomologie Galoisienne*, Springer-Verlag, Berlin, 1973.

[29] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 951, Springer-Verlag, New York, 1994.

[30] R. Staszewski, H. Völklein and G. Wiesend, *Counting generating systems of a finite group from given conjugacy classes,* in *Computational aspects of algebraic curves*, Lecture Notes Series on Computing, vol. 13, World. Sci. Publ. Hackensack, N.J., 2005, pp. 256–263.

[31] M. Suzuki, *Group Theory*, Grundlehren der Mathematischen Wissenschaften , vol. 247, Springer-Verlag, Berlin, 1982.

[32] H. Völklein, *Groups as Galois Groups - an Introduction*, Cambridge Studies in Advanced Mathematics vol. 53, Cambridge University Press, 1999.

[33] S. Wewers, *Construction of Hurwitz Spaces*, Ph.D. thesis, I.E.M. - Essen, 1998.