Math. Ann. 333, 355–391 (2005) **Mathematische Annalen**

DOI: 10.1007/s00208-005-0680-0

# Harbater-Mumford subvarieties of moduli spaces of covers

**Anna Cadoret**

Received: 11 January 2005 / Revised version: 7 May 2005 /
Published online: 12 August 2005 – © Springer-Verlag 2005

**Abstract.** We define Harbater-Mumford subvarieties, which are special kinds of closed subvarieties of Hurwitz moduli spaces obtained by fixing some of the branch points. We show that, for many finite groups, finding geometrically irreducible HM-subvarieties defined over $\mathbb{Q}$ is always possible. This provides information on the arithmetic of Hurwitz spaces and applies in particular to the regular inverse Galois problem with (almost all) fixed branch points. Profinite versions of our results can also be stated, providing new tools to study the geometry of modular towers and the regular inverse Galois problem for profinite groups.

*Mathematics Subject Classification (2000):* 12F12, 14G32, 20E45, 14H30, 20E22

## Introduction

The regular inverse Galois problem over some field $k$, (RIGP/$k$), essentially reduces to finding $k$-rational points on Hurwitz moduli spaces of covers [FV91]. In this context, two main methods can be distinguished: on the one hand, genus 0 methods [M89] which may provide in special situations $\mathbb{Q}$ or $\mathbb{Q}^{ab}$-rational points on usually low-dimensional Hurwitz spaces and, on the other hand, large field methods [DF94], [D95], [Des95][1], which combine irreducibility Conway and Parker type results [FV91], realization results over local fields [H03], [DF94] and the local-global principle for varieties [Mo89], [P96] to provide $\mathbb{Q}^{\Sigma}$[2]-rational points. Our main theorem (theorem 2.3) conjoins these two aspects: it is, as Conway and Parker's theorem, a global structure result about high-dimensional Hurwitz spaces but, as genus 0 methods, it deals with low-dimensional closed subvarieties (of those high-dimensional Hurwitz spaces) obtained by specializing most of the branch points. In §2.1, we give a more precise account on the history behind our main theorem.

A. Cadoret
Université de Lille 1, Mathématiques, 59655 Villeneuve d'Ascq Cedex, France
e-mail: cadoret@math.jussieu.fr

[1] See also works of Pop et al who have developed a parallel approach based on common principles but not using Hurwitz spaces [P96], [H03], [V99].

[2] Given a global field $Q$ and a finite set $\Sigma$ of places of $Q$, we always denote by $Q^{\Sigma}$ the maximal algebraic extension of $Q$ (in a fixed separable closure of $Q$) which is totally split at each place $v \in \Sigma$. In the special case $Q = \mathbb{Q}$ and $\Sigma$ only consists of the prime at infinity, we use the notation $\mathbb{Q}^{tr}$ for $Q^{\Sigma}$; $\mathbb{Q}^{tr}$ is the field of totally real algebraic numbers.

The starting point are special components of Hurwitz moduli spaces of covers introduced by M. Fried [F95] - the Harbater-Mumford components (*cf.* §2.2). We consider the closed subvarieties - we call HM-subvarieties - of these HM-components obtained by specializing most of the branch points; our main result is a general criterion to ensure they are geometrically irreducible. If for instance the monodromy group $G$ of the studied covers is any group satisfying the assumptions of theorem 1 below, our criterion produces infinitely many Hurwitz spaces carrying geometrically irreducible HM-curves, defined over the same field as the whole Hurwitz space, and lying in the sublocus corresponding to covers with all their branch points but one fixed. In general, "all their branch points but one" should be replaced by "all their branch points but $r(G)$" for some integer $r(G)$ depending only on the finite group $G$ in question.

One motivation for this work was to gain more information about the branch point divisor of covers defined over large fields. Indeed, when applying the local-global principle to solve for instance (RIGP/$\mathbb{Q}^{tr}$), this information is entirely lost. Showing that any finite group $G$ can be regularly realized over $\mathbb{Q}^{tr}$ with a $\mathbb{Q}$-rational branch point divisor would be a significant step towards the (RIGP/$\mathbb{Q}$): as explained in [D92], the monodromy of such a cover and its conjugates obeys strong group-theoretical constraints. Also, showing all the groups $G_n$ of a projective system $(G_{n+1} \twoheadrightarrow G_n)_{n\geq 0}$ can be regularly realized over a large field $k$ with the same branch point divisor $\mathbf{t}$ is a missing step to investigate the (RIGP/$k$) for profinite groups; this is the underlying idea of works like [DDes04]. Our result enables us to handle the derived problem - we denote by (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) - where the subset $\mathbf{t}_2 \subset \mathbf{t}$ is fixed and its complement, $\mathbf{t}_1$ is allowed to vary (the cardinality $|\mathbf{t}_1|$ of $\mathbf{t}_1$ corresponding to the dimension of the HM-subvarieties we consider). We are particularly interested in the case when $\mathbf{t}_2$ is defined over $\mathbb{Q}$ and $|\mathbf{t}_1|$ is as small as possible. The first and most difficult step, which is to ensure the HM-subvarieties are geometrically irreducible, is given by our criterion. The second one consists in showing these HM-subvarieties can be built in such a way they carry real or $p$-adic points; this requires a careful use of recent results from [DE03] about the existence of $p$-adic points on HM-components. We can then apply the usual local-global machinery to obtain results like

**Theorem 1.** *Let $G$ be a finite group containing two conjugacy classes $A$, $B$ such that $G =< A >=< B >$ and $G =< a, b >$ for any $a \in A$, $b \in B$. Let $o(A)$ denote the order of the elements in $A$ and write $k_A := \mathbb{Q}(\mathrm{e}^{\frac{2\pi i}{o(A)}})$. Then, for any finite set $\Sigma$ of non archimedean places of $k_A$ of residue characteristic not dividing $|G|$ there exists a $\mathbb{Q}$-rational divisor $\mathbf{t}_\Sigma$ and $G$-covers $f$ defined over $k_A^\Sigma$ with group $G$ and branch point divisor $\mathbf{t}_f = \mathbf{t}_{f,1} + \mathbf{t}_\Sigma$ where $|\mathbf{t}_{f,1}| = 1$.*

As another application, we obtain new regular realizations of some prodihedral groups over $\mathbb{Q}^{tr}$ (*cf.* also [C04a]).

Moreover, our irreducibility criterion behaves well with Frattini extensions. This allows us to investigate the arithmetic of Fried's modular towers [F95] (section 4.1.2) and tackle the related (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) for profinite groups like the universal $p$-Frattini cover ${}_p\tilde{G}$ of a finite $p$-perfect group $G$ (for some prime $p$ dividing $|G|$). For instance, with the notation and hypotheses of theorem 1 but assuming in addition that $G$ is $p$-perfect and $A$, $B$ are $p'$-conjugacy classes, one obtains this structure result

**Theorem 2.** *There exist modular towers $(\mathcal{H}_{n+1} \to \mathcal{H}_n)_{n\geq 0}$ associated with $G$ such that for any finite set $\Sigma$ of non archimedean places of $k$ of residue characteristic not dividing $|G|$ there exists a $\mathbb{Q}$-rational divisor $\mathbf{t}_\Sigma$ and a projective system $(\mathcal{C}_{n+1,\Sigma} \to \mathcal{C}_{n,\Sigma})_{k\geq 0}$ of geometrically irreducible HM-curves defined over $k$ satisfying:*

*(i) $\mathcal{C}_{n,\Sigma} \subset \mathcal{H}_n$ parametrizes G-covers $f_n$ with group ${}^n_p\tilde{G}$ and branch point divisor $\mathbf{t}_{f_n} = \mathbf{t}_{f_n,1} + \mathbf{t}_\Sigma$ where $|\mathbf{t}_{f_n,1}| = 1$, $n \geq 0$.*
*(ii) $\varprojlim \mathcal{C}_{n,\Sigma}(k_P)^{noob} \neq \emptyset$, $P \in \Sigma$.*
*(iii) $\mathcal{C}_{n,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $n \geq 0$.*

Here ${}^n_p\tilde{G}$ denotes the $n$th characteristic quotient of ${}_p\tilde{G}$ (*cf.* §4.1.2) and the "noob" labelling (for no obstruction) means we consider the sets of $k$-rational points corresponding to G-covers defined over $k$ and not only with field of moduli $k$ (*cf.* §1.1).

This shows a strong arithmetical property is kept along some modular towers. It is a positive result which emphasizes the difficulty of Fried's conjectures about the disappearance of rational points over a number field on a modular tower beyond a certain level [D04], [F95].

The paper is organized as follows. In section 1 we recall necessary definitions and basic results, section 2 is devoted to the statements and examples, section 3 to the proofs. In section 4, we give applications of our results such as theorem 1 and theorem 2.

I wish to thank P. Dèbes for encouraging me to write this paper and the careful re-reading he made of it. I also want to thank the referee for his constructive suggestions.

## 1. Preliminaries

This section is devoted to recalling the necessary definitions and some basic facts about Hurwitz spaces.

Given a morphism $V \to W$ of algebraic varieties and $W_0 \hookrightarrow W$ a subvariety, we will often denote the fiber product $V \times_W W_0$ by $V_{W_0}$. Also, given a finite group $G$ and an integer $r \geq 1$ we will denote the set of all the $r$-tuples $\mathbf{C} = (C_1, ..., C_r)$ of non trivial conjugacy classes of $G$ by $\mathcal{C}_r(G)$; we will sometimes write $l(\mathbf{C}) := r$

for the length of such a tuple $\mathbf{C} \in \mathcal{C}_r(G)$. And for any conjugacy class $C$, we will write $o(C)$ for the order of any element in $C$. Finally, given a tuple $\mathbf{t}' = (t_1, ..., t_r)$ and two integers $1 \leq i < j \leq r$, we will write $\mathbf{t}'_{i,j} := (t_i, ..., t_j)$.

### *1.1. G-covers and Hurwitz spaces*

Recall a G-cover with group $G$ is a pair $(f, \alpha)$ where $f : X \to \mathbb{P}^1$ is a Galois cover with group $G$ and $\alpha : \mathrm{Aut}(f) \to G$ is a group isomorphism. In the following, we will always drop the notation $\alpha$ though it remains part of the data. One can attach to each G-cover of $\mathbb{P}^1_{\mathbb{C}}$ the three following invariants: the monodromy group $G$, the branch point set $\mathbf{t} = \{t_1, ..., t_r\} \subset \mathbb{P}^1(\mathbb{C})$ and for each $t \in \mathbf{t}$ the *associated inertia canonical conjugacy class* $C_t$ . To summarize this, we will sometimes say the considered G-cover has invariants $G$, $(C_t)_{t\in\mathbf{t}}$, $\mathbf{t}$. Adopting the topological point of view, let us recall what these invariants correspond to: given $\mathbf{t} = \{t_1, ..., t_r\}$, introduce a *topological bouquet* $\underline{\gamma}$ of $\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}$, that is an $r$-tuple of homotopy classes of loops $\gamma_1, ..., \gamma_r$ based at some point $t_0 \notin \mathbf{t}$ such that (1) $\gamma_1, ..., \gamma_r$ generate the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}, t_0)$ with the single relation $\gamma_1...\gamma_r = 1$ and (2) $\gamma_i$ is a loop revolving once, counterclockwise, about $t_i$, $i = 1, ..., r$. Now, considering a G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$, the monodromy action defines a permutation representation $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C})\backslash\mathbf{t}, t_0) \to \mathrm{Per}(f^{-1}(t_0))$. The image group $G$ of this representation is the monodromy group (we also say the Galois group) of $f$ and the conjugacy class $C_{t_i}$ of the image of $\gamma_i$ in $G$ is the inertia canonical class corresponding to $t_i$, $i = 1, ..., r$.

For any integer $r \geq 3$ let $\mathcal{U}^r \subset (\mathbb{P}^1_{\mathbb{C}})^r$ be the subset of $(\mathbb{P}^1_{\mathbb{C}})^r$ consisting of all $r$-tuples $\mathbf{t}' = (t_1, ..., t_r) \in (\mathbb{P}^1_{\mathbb{C}})^r$ such that $t_i \neq t_j$ for $1 \leq i \neq j \leq r$, let $\mathcal{U}_r = \mathcal{U}^r/S_r$ be the quotient space of $\mathcal{U}^r$ by the natural action of the symmetric group $S_r$ and $\sigma_r : \mathcal{U}_r \to \mathcal{U}^r/S_r$ the canonical projection. Given a finite group $G$ let $\psi_{r,G} : \mathcal{H}_{r,G} \to \mathcal{U}_r$ be the coarse moduli space (fine assuming $Z(G) = \{1\}$) for the category of G-covers of $\mathbb{P}^1_{\mathbb{C}}$ with group $G$ and $r$ branch points, where $\psi_{r,G}$ is the map which to a given isomorphism class of G-covers associates its branch point set. For any $r$-tuple $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$ let $\mathcal{H}_{r,G}(\mathbf{C})$ be the corresponding *Hurwitz space* [FV91], that is the union of irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with invariants $G$, $\mathbf{C}$, $\mathbf{t}$. A point $\mathbf{h} = (h, (t_1, ..., t_r))$ of the fiber product $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$ then corresponds to a G-cover given with an ordering of its branch points, which allows us to define a monodromy map:

$$\begin{aligned} M : \ & \mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r \to \{C_1, \ldots , C_r\}^r \\ & (h, (t_1, \ldots , t_r)) \to (C_{t_1}, \ldots , C_{t_r}) \end{aligned}$$

This map, being continuous, is constant on each connected component of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$. So, $M^{-1}(\mathbf{C})$ is a union of connected components of $\mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$; we will denote this variety by $\mathcal{H}'_{r,G}(\mathbf{C})$. We have a commutative diagram:

$$\begin{tikzcd}
\mathcal{H}'_{r,G}(\mathbf{C}) \arrow[r, hook] \arrow[dr, "\psi'_{r,G}"'] & \mathcal{H}_{r,G}(\mathbf{C}) \times_{\mathcal{U}_r} \mathcal{U}^r \arrow[r, "\Sigma_r"] \arrow[d] \arrow[dr, phantom, "\square"] & \mathcal{H}_{r,G}(\mathbf{C}) \arrow[d, "\psi_{r,G}"] \\
 & \mathcal{U}^r \arrow[r, "\sigma_r"] & \mathcal{U}_r
\end{tikzcd}$$

We will freely use the general theory of Hurwitz spaces (see for instance [FV91] and [V99]), and only recall here the description of the fibers of $\psi_{r,G}$ and $\psi'_{r,G}$ in terms of *Nielsen classes* $\mathrm{ni}(\mathbf{C})$ and *straight Nielsen classes* $\mathrm{sni}(\mathbf{C})$ respectively, where:

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

and $\mathrm{sni}(\mathbf{C})$ is the set defined as $\mathrm{ni}(\mathbf{C})$, but replacing (3) by

$$(3)' g_i \in C_i fori = 1, ..., r.$$

We use the notation $\overline{\mathrm{ni}}(\mathbf{C})$ and $\overline{\mathrm{sni}}(\mathbf{C})$ for the corresponding quotient sets modulo the componentwise action of the inner automorphism group, $\mathrm{Inn}(G)$.

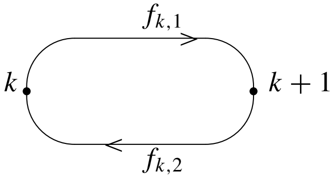
Given $\mathbf{t} \in \mathcal{U}_r$, it is classical that $(\psi_{r,G})^{-1}(\mathbf{t})$ is in bijection with $\overline{\mathrm{ni}}(\mathbf{C})$. Furthermore, if we choose an ordering of the branch points $\mathbf{t}' = (t_1, ..., t_r)$ in $\mathbf{t}$, then $\overline{\mathrm{sni}}(\mathbf{C})$ is in bijection with $(\psi'_{r,G})^{-1}(\mathbf{t}')$. The correspondence is given by the monodromy action and depends on the choice of a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C}) \backslash \mathbf{t}$; we denote it by $BCD_{\underline{\gamma}}$ (for B(ranch) (C)ycle (D)escription).

For later use, we also recall that two finite cyclotomic field extensions of $\mathbb{Q}$ - which we denote by $\mathbb{Q}_{\mathbf{C}}$ and $\mathbb{Q}'_{\mathbf{C}}$ - are associated to $\mathbf{C}$. Precisely, $\mathbb{Q}_{\mathbf{C}} = \overline{\mathbb{Q}}^{\Delta_{\mathbb{C}}}$ and $\mathbb{Q}'_{\mathbf{C}} = \overline{\mathbb{Q}}^{\Delta'_{\mathbb{C}}}$ where $\Delta_{\mathbf{C}}$ and $\Delta'_{\mathbf{C}}$ are the closed subgroups of finite index of the absolute Galois group $\Gamma_{\mathbb{Q}}$ defined by $\Delta_{\mathbf{C}} = \{\sigma \in \Gamma_{\mathbb{Q}} | \mathbf{C}^{\chi(\sigma)} = \mathbf{C} \text{ up to permutation}\}$ and $\Delta'_{\mathbf{C}} = \{\sigma \in \Gamma_{\mathbb{Q}} | \mathbf{C}^{\chi(\sigma)} = \mathbf{C}\}$ (here, $\chi : \Gamma_{\mathbb{Q}} \to \hat{\mathbb{Z}}$ is the cyclotomic character). Resulting from the branch cycle argument [V99, lemma 2.8], $\mathbb{Q}_{\mathbf{C}}$ is the field of definition of $\mathcal{H}_{r,G}(\mathbf{C})$ and $\mathbb{Q}'_{\mathbf{C}}$, the one of $\mathcal{H}'_{r,G}(\mathbf{C})$. When $\mathbb{Q}_{\mathbf{C}} = \mathbb{Q}$, we say that $\mathbf{C}$ is *a rational union of conjugacy classes* and, when $\mathbb{Q}'_{\mathbf{C}} = \mathbb{Q}$, that $\mathbf{C}$ is *a tuple of rational conjugacy classes.*

Finally, since Hurwitz spaces are only coarse moduli spaces in general, we will write $\mathcal{H}_{r,G}(\mathbf{C})(k)^{noob}$ for the set of all the $k$-rational points in the non obstruction locus that is, corresponding to G-covers defined over $k$.

### *1.2. The covers $\Psi_{r,G}$ and $\Psi'_{r,G}$*

From now on, we will always assume $r \geq 4$. We first recall useful results about Hurwitz braid groups and then give a description of the covers $\Psi_{r,G}$ and $\Psi'_{r,G}$ in terms of group actions. Fix $\mathbf{t} = \{1, ..., r\} \in \mathcal{U}_r(\mathbb{C})$ and $\mathbf{t}' = (1, ..., r) \in \mathcal{U}^r(\mathbb{C})$ and for $k = 1, ..., r-1$ define the simple arcs $f_{k,i} : [0,1] \to \mathbb{P}^1(\mathbb{C})$, $i = 1, 2$ by



and write $\begin{array}{cccl} q_k: & [0,1] & \to & \mathcal{U}^r(\mathbb{C}) \\ & t & \to & (1, ..., k-1, f_{k,1}(t), f_{k,2}(t), k+2, ..., r) \end{array}$ for the usual topological braid. Let $H_r$ be the abstract group given by the presentation with generators $Q_1, ..., Q_{r-1}$ and defining relations

(1) $Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}$ for $i = 1, \dots, r-2$
(2) $Q_i Q_j = Q_j Q_i$ for $i, j = 1, \dots, r-1$ with $|j-i| > 1$
(3) $Q_1 Q_2 \cdots Q_{r-1} Q_{r-1} \cdots Q_2 Q_1 = 1$

and $SH_r$ the kernel of the morphism $H_r \to \mathcal{S}_r$, $Q_i \to (i, i+1)$. Set

$$\left.\begin{array}{l} A_{i,j} = Q_{j-1}^{-1} \cdots Q_{i+1}^{-1} Q_i^{-2} Q_{i+1} \cdots Q_{j-1} \\ \quad\;\; = Q_i \cdots Q_{j-2} Q_{j-1}^{-2} Q_{j-2}^{-1} \cdots Q_i^{-1} \end{array}\right\}, 1 \leq i < j \leq r$$

(we will also often use the notation $a_{i,j} = A_{i,j}^{-1}$, $1 \leq i < j \leq r$) and denote by $\Pi_{k,r}$ the subgroup of $SH_r$ generated by $\{A_{i,j}\}_{1 \leq i \leq k, i < j \leq r}$, $k = 1, ..., r-1$. The following result will play an important part in the proof of theorem 2.3. It is a direct corollary of [Bi74, lemma 1.8.2], which gives a presentation of $SH_r$ with generators $A_{i,j}$, $1 \leq i < j \leq r$ and defining relations.

**Theorem 1.1.** *The groups $\Pi_{k,r}$ are normal in $SH_r$, $k = 1, ..., r-1$.*

The next theorem gives the link between the abstract groups $H_r$, $SH_r$ and the topological fundamental groups $\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t})$, $\pi_1^{\mathrm{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}')$. More precisely, it states that

**Theorem 1.2. (Artin (1925), Fadell and Van Buskirk (1962))** *The group homomorphisms*

$$\begin{array}{rl} u_r : H_r \to & \pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \\ Q_i \to & [(\sigma_r)_*(q_i)] \end{array} \; \textit{and} \; \begin{array}{rl} v_r : SH_r \to & \pi_1^{\mathrm{top}}(\mathcal{U}^r(\mathbb{C}), \mathbf{t}') \\ A_{i,j} \to & [q_i \cdots q_{j-2} q_{j-1}^{-2} q_{j-2}^{-1} \cdots q_i^{-1}] \end{array}$$

*are isomorphisms.*

Let us use this result to show that $\Pi_{k,r} \simeq \pi_1^{\mathrm{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}(\mathbb{C}), \mathbf{t}'_{1,k})$, $k = 1, ..., r-1$. For this, consider the homotopy sequence of the fibration with connected fibers

$$\begin{array}{rccc} p_{k+1,r} : & \mathcal{U}^r(\mathbb{C}) & \to & \mathcal{U}^{r-k}(\mathbb{C}) \\ & (t_1, \dots, t_r) & \to & (t_{k+1}, \dots, t_r) \end{array}$$

which gives rise to the short exact sequence of topological fundamental groups

$$1 \to \pi_1^{\mathrm{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}, \mathbf{t}'_{1,k}) \to \pi_1^{\mathrm{top}}(\mathcal{U}^r, \mathbf{t}') \overset{(p_{k+1,r})_*}{\to} \pi_1^{\mathrm{top}}(\mathcal{U}^{r-k}, \mathbf{t}'_{k+1,r}) \to 1$$

It follows from the definition of the topological braids $(q_i)_{1\leq i\leq r-1}$ that $v_r(\Pi_{k,r}) < \ker((p_{k+1,r})_*)$. The group homomorphism $\eta_{k,r} : SH_r \to SH_{r-k}$ defined by $\eta_{k,r}(A_{i,j}) = A_{i-k,j-k}$ if $k < i < j \leq r$ and $\eta_{k,r}(A_{i,j}) = 1$ else is well defined and we get the commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & \Pi_{k,r} \arrow[r] \arrow[d, "v_r|_{\Pi_{k,r}}"'] & SH_r \arrow[r, "\eta_{k,r}"] \arrow[d, "v_r"'] & SH_{r-k} \arrow[r] \arrow[d, "v_{r-k}"'] & 1 \\
1 \arrow[r] & \pi_1^{\mathrm{top}}(\mathcal{U}^r_{\mathbf{t}'_{k+1,r}}, \mathbf{t}'_{1,k}) \arrow[r] & \pi_1^{\mathrm{top}}(\mathcal{U}^r, \mathbf{t}') \arrow[r, "(p_{k+1,r})_*"'] & \pi_1^{\mathrm{top}}(\mathcal{U}^{r-k}, \mathbf{t}'_{k+1,r}) \arrow[r] & 1
\end{tikzcd}$$

But, according to theorem 1.2, the two last vertical arrows $v_r$, $v_{r-k}$ are isomorphisms and, by the five lemma so is the first one, $v_r|_{\Pi_{k,r}}$.

For any $\mathbf{t} \in \mathcal{U}_r(\mathbb{C})$, for any $t_0 \in \mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$, any ordering $\mathbf{t}'$ of $\mathbf{t}$ defines generators $Q_1, ..., Q_{r-1}$ of $\pi_1^{\mathrm{top}}(\mathcal{U}_r(\mathbb{C}), \mathbf{t}) \simeq H_r$ [FV91] §1.3 as above. With these generators, the cover $\Psi_{r,G} : \mathcal{H}_{r,G}(\mathbf{C}) \to \mathcal{U}_r$ corresponds to the action of $H_r$ on the fiber $(\Psi_{r,G})^{-1}(\mathbf{t}) \simeq \overline{\mathrm{ni}}(\mathbf{C})$ given by

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

Likewise, the cover $\Psi'_{r,G} : \mathcal{H}'_{r,G}(\mathbf{C}) \to \mathcal{U}^r$ corresponds to the action of $SH_r$ on the fiber $(\psi'_{r,G})^{-1}(\mathbf{t}) \simeq \overline{\mathrm{sni}}(\mathbf{C})$ induced by the one of $H_r$ on $\overline{\mathrm{ni}}(\mathbf{C})$ [FV91] §1.4.

Fix now an $(r-k)$-tuple $\mathbf{t}'_{k+1,r} = (t_{k+1}, ..., t_r) \in \mathcal{U}^{r-k}(\mathbb{C})$ and consider the following cartesian square

$$\begin{tikzcd}
\mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}'_{k+1,r}} \arrow[r] \arrow[d, "(\Psi'_{r,G})_{\mathbf{t}'_{k+1,r}}"'] \arrow[dr, phantom, "\square"] & \mathcal{H}'_{r,G}(\mathbf{C}) \arrow[d, "\Psi'_{r,G}"] \\
\mathcal{U}^r_{\mathbf{t}'_{k+1,r}} \arrow[r] & \mathcal{U}^r
\end{tikzcd}$$

By Grauert-Remmert's Theorem (for $k = 1$, Riemann's Existence Theorem) the etale cover $(\Psi'_{r,G})_{\mathbf{t}'_{k+1,r}} : \mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}'_{k+1,r}} \to \mathcal{U}^r_{\mathbf{t}'_{k+1,r}}$ extends to a branched cover $(\overline{\Psi}'_{r,G})_{\mathbf{t}'_{k+1,r}} : \overline{\mathcal{H}}'_{r,G}(\mathbf{C})_{\mathbf{t}'_{k+1,r}} \to \mathcal{U}^k$ associated with the action of $\Pi_{k,r}$ induced by the one of $SH_r$ on $\overline{\mathrm{sni}}(\mathbf{C})$. When $k = 1$, we obtain a branched cover $(\overline{\Psi}'_{r,G})_{\mathbf{t}'_{2,r}} : \overline{\mathcal{H}}'_{r,G}(\mathbf{C})_{\mathbf{t}'_{2,r}} \to \mathbb{P}^1_{\mathbb{C}}$ with branch points $t_2, ..., t_r$ and branch cycle description the images of $(A_{1,i})_{2\leq i\leq r}$ under the permutation action of $SH_r$ on $\overline{\mathrm{sni}}(\mathbf{C})$.

Resulting from the branch cycle argument [V99, lemma 2.8], $(\mathcal{H}'_{r,G})_{\mathbf{t}'_{k+1,r}}$ is defined over the field $\mathbb{Q}'_{\mathbf{C}}(\mathbf{t}'_{k+1,r})$ and its image $\Sigma_r(\mathcal{H}'_{r,G}(\mathbf{C})_{\mathbf{t}'_{k+1,r}})$ in the symmetrised Hurwitz space $\mathcal{H}_{r,G}(\mathbf{C})$ is defined over a subfield $\mathbb{Q}(\mathbf{C},\mathbf{t}'_{k+1,r})$ of $\mathbb{Q}'_{\mathbf{C}}(\mathbf{t}'_{k+1,r})$ which can be explicitly computed taking into account the rationality property of $(\mathbf{C},\mathbf{t}'_{k+1,r})$ (for instance, if $\mathbf{C}$ is a tuple of rational conjugacy classes then $\mathbb{Q}(\mathbf{C},\mathbf{t}'_{k+1,r}) = \mathbb{Q}(\mathbf{t}_{k+1,r})$. Similar fields can be defined for any field $Q$ of characteristic 0.

## 2. HM-subvarieties

### *2.1. History behind the main theorem*

This paper originates in [FV91, Proposition 1] (usually referred to as Conway and Parker's theorem). For any centerless finite group $G$, there exists an infinite (so, in particular, non empty) family $\underline{\mathcal{H}}_G := (\mathcal{H}_{G,i})_{i\in I}$ of geometrically irreducible varieties defined over $\mathbb{Q}$ such that *there exists a regular realization of $G$ over $\mathbb{Q}$ if and only if $\mathcal{H}_{G,i}(\mathbb{Q}) \neq \emptyset$, for some $i \in I$.* The RIGP thus becomes a purely diophantine problem. The practical value of this statement starts with asking how explicit this family of varieties is and whether it points to where such $\mathbb{Q}$-rational points might be located. The branch cycle argument shows there exists a partition $I = \coprod_{\mathbf{C}} I_{\mathbf{C}}$ of the index set $I$ where $\mathbf{C}$ runs over all the finite rational unions of non trivial conjugacy classes of $G$. For such $\mathbf{C}$, the set $I_{\mathbf{C}}$ is finite - possibly empty - and the family $(\mathcal{H}_{G,i})_{i\in I_{\mathbf{C}}}$ consists of all the geometrically irreducible components of $\mathcal{H}_{r,G}(\mathbf{C})$ which are defined over $\mathbb{Q}$ (where $r$ is the length of $\mathbf{C}$).

What, more precisely, [FV91, Proposition 1] does is to exhibit an "almost" explicit infinite subfamily $\underline{\mathcal{H}}^1_G := (\mathcal{H}_{G,i})_{i\in I_1} \subset \underline{\mathcal{H}}_G$. The varieties lying in $\underline{\mathcal{H}}^1_G$ are full Hurwitz spaces $\mathcal{H}_G(\mathbf{C})$ for all the finite rational unions of conjugacy classes containing $\geq c(G)$ copies of each non trivial conjugacy class of $G$. The constant $c(G)$ only depends on $G$ but we have no explicit lower bound for it - whence the "almost". In [F95, Th. 3.21 and Cor. 3.23], another explicit infinite subfamily $\underline{\mathcal{H}}^2_G := (\mathcal{H}_{G,i})_{i\in I_2} \subset \underline{\mathcal{H}}_G$ is identified. The varieties lying in $\underline{\mathcal{H}}^2_G$ are the so-called Harbater-Mumford components which are geometrically irreducible. We give more details on this in §2.2 below.

The ultimate goal for regular realizations of $G$ over $\mathbb{Q}$ would be to ensure that some of the $\mathcal{H}_{G,i}$ carry $\mathbb{Q}$-rational points (that is, 0-dimensional geometrically irreducible subvarieties defined over $\mathbb{Q}$). From this point of view, the main result of our paper can be regarded as an intermediate step. We show that $\mathcal{H}_{G,i}$ carries low-dimensional geometrically irreducible subvarieties $\mathcal{H}_{G,i,\mathbf{t}}$ defined over $\mathbb{Q}$ for infinitely many $i \in I_2$. The subvarieties $\mathcal{H}_{G,i,\mathbf{t}}$ are those obtained by fixing all the branch points except the $r(G)$ first ones and so, they are of dimension $r(G)$. The constant $r(G)$ only depends on $G$ and is explicitly computable. In many cases we show that $r(G) = 1$, hence obtaining geometrically irreducible $\mathbb{Q}$-curves on $\mathcal{H}_{G,i}$ for infinitely many $i \in I_2$.

### 2.2. HM-components of Hurwitz spaces

We recall here the definition and main properties of H(arbater)-M(umford) components of Hurwitz spaces, which have been introduced by M. Fried [F95] and then studied by P. Dèbes and M. Emsalem [DE03]. To do this, we need the notion of H(arbater)-M(umford) type for covers of $\mathbb{P}^1$. Given a finite group $G$, an integer $s \geq 2$ and a *symmetric* $2s$-tuple $\mathbf{C}$ of non trivial conjugacy classes of $G$, that is consisting of $s$ pairs $(C_i, C_i^{-1})$, any $2s$-tuple in $\overline{\mathrm{ni}}(\mathbf{C})$ of the form $\mathbf{g} = [g_1, ..., g_s] := (g_1, g_1^{-1}, ..., g_s, g_s^{-1})$ is called a *Harbater-Mumford representative*; we denote the set of all these $2s$-tuples by $\overline{\mathrm{hm}}(\mathbf{C})$. A G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$ with invariants $G, \mathbf{C}, \mathbf{t}$ is said to be *of Harbater-Mumford type* (a HM-G-cover for short) if there exists a topological bouquet $\underline{\gamma}$ for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ and an $2s$-tuple $\mathbf{g} \in \overline{\mathrm{hm}}(\mathbf{C})$ such that $BCD_\gamma(f) = \mathbf{g}$. A *HM-component* of the Hurwitz space $\mathcal{H}_{2s,G}(\mathbf{C})$ is the component of some HM-cover. Equivalently, it is a component that corresponds to the orbit of some HM representative under the action of the Hurwitz braid group $H_{2s}$. The following theorem is proved in [F95], with the assumption $Z(G) = \{1\}$, and in [DE03] without this assumption; a main tool of these proofs is Wewer's compactification of Hurwitz spaces [W98].

**Theorem 2.1.** *The union* $\mathrm{HM}(\mathbf{C})$ *of all the HM-components of the Hurwitz space* $\mathcal{H}_{2s,G}(\mathbf{C})$ *is defined over* $\mathbb{Q}_{\mathbf{C}}$. *Likewise, the union* $\mathrm{HM}'(\mathbf{C})$ *of all the HM-components of the Hurwitz space* $\mathcal{H}'_{2s,G}(\mathbf{C})$ *is defined over* $\mathbb{Q}'_{\mathbf{C}}$.

Using Fried's terminology, say an $r$-tuple $\mathbf{C}$ of non trivial conjugacy classes of $G$ is g-*complete* if for any $g_i \in C_i, i = 1, ..., r$, we have $G =< g_1, ..., g_r >$ and an $2s$-tuple $\mathbf{C}$ consisting of $s$ pairs $(C_i, C_i^{-1})$ of non trivial conjugacy classes of $G$ is *HM*-g-*complete* if, when removing a pair $(C_i, C_i^{-1})$, the remaining $(2s-2)$-tuple is g-complete. Being HM-g-complete is a condition that ensures there is a single HM-component in $\mathcal{H}'_{2s,G}(\mathbf{C})$, as proved in [F95, Th. 3.21]. In particular, if $\mathbf{C}$ is both a rational union of non trivial conjugacy classes of $G$ and HM-g-complete, then the HM-component $\mathrm{HM}(\mathbf{C})$ of $\mathcal{H}_{2s,G}(\mathbf{C})$ is a geometrically irreducible variety defined over $\mathbb{Q}$. Likewise, if $\mathbf{C}$ is both a tuple of non trivial rational conjugacy classes of $G$ and HM-g-complete, then the HM-component $\mathrm{HM}'(\mathbf{C})$ of $\mathcal{H}'_{2s,G}(\mathbf{C})$ is a geometrically irreducible variety defined over $\mathbb{Q}$.

### 2.3. Definition

Given a finite group $G$ and an integer $R \geqslant 4$, the closed subvarieties of $\mathcal{H}_{r,G}$, $\mathcal{H}'_{r,G}$ obtained by specializing some of the branch points are of particularly interest when considering the regular inverse Galois problem. We will deal with special kinds of such subvarieties - we call HM-subvarieties. More precisely, given a symmetric $2s$-tuple $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1})$ of non trivial conjugacy classes of $G$, for any $\mathbf{t}'_{k+1,2s} \in \mathcal{U}^{2s-k}(\overline{\mathbb{Q}})$, with $1 \leq k \leq 2s-1$ we will say that

$\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$ is the *HM-subvariety associated with the data* $(G, \mathbf{C}, \mathbf{t}'_{k+1,2s})$ and that $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{k+1,2s}} := \Sigma_{2s}(\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{k+1,2s}})$ (which is a subset of the fiber of $\Psi_{2s,G}$ above the set of all $\tau \in \mathcal{U}_{2s}(\overline{\mathbb{Q}})$ such that $\mathbf{t}_{k+1,2s} \subset \tau$) is the *symmetrised HM-subvariety associated with the data* $(G, \mathbf{C}, \mathbf{t}'_{k+1,2s})$. Finding HM-subvarieties which are geometrically irreducible and defined over $\mathbb{Q}$ with $k$ small is the aim of this paper.

Starting from a symmetric $2s$-tuple $\mathbf{C} = (C_1, C_1^{-1}, ..., C_s, C_s^{-1})$ such that there is one single HM-component in $\mathcal{H}'_{2s,G}(\mathbf{C})$ - or, equivalently, such that all the HM representatives fall in one single $SH_{2s}$-orbit $O^{HM}(\mathbf{C})$ - and given $1 \leq k \leq 2s-1$, for any $\mathbf{t}'_{k+1,2s} \in \mathcal{U}^{2s-k}(\overline{\mathbb{Q}})$, the number of geometrically irreducible components of $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$ corresponds to the number of orbits of $O^{HM}(\mathbf{C})/\Pi_{k,2s}$. Consider the associated symmetrised HM-subvariety, $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$. An obvious necessary condition to get one of its geometrically irreducible component defined over $\mathbb{Q}$ is that $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{k+1,2s}}$ be itself defined over $\mathbb{Q}$. This is the rationality condition given by the branch cycle argument [V99, Lemma 2.8]:

$$\begin{cases} -\mathbf{C} \text{ is a rational union of conjugacy classes.} \\ -(\mathbf{C}_{k+1}, \ldots, \mathbf{C}_{2s}) \text{ is a rational union of conjugacy classes and} \\ \quad \mathbf{t}_{k+1,2s} \in \mathcal{U}_{2s-k}(\mathbb{Q}). \\ - \text{For any } \sigma \in \Gamma_{\mathbb{Q}}, \mathbf{C}^{\chi(\sigma)}_{\alpha(\sigma)(i)} = \mathbf{C}_i, \text{ with } k+1 \leq i \leq 2s \text{ where } \chi : \Gamma_{\mathbb{Q}} \to \hat{\mathbb{Z}} \\ \quad \text{is the cyclotomic character and } \alpha : \mathrm{G}_{\mathbb{Q}} \to \mathcal{S}_{2\mathrm{s}-\mathrm{k}} \text{ is the natural representation} \\ \quad \text{induced by the action of } \Gamma_{\mathbb{Q}} \text{ on } \mathbf{t}'_{k+1,2s}. \end{cases}$$

Consider the case $k = 1$ and assume the rationality condition above holds for $\mathbf{t}'_{2,2s} \in \mathcal{U}^{2s-1}(\mathbb{Q})$. Let $O_1^{HM}(\mathbf{C}) \in O^{HM}(\mathbf{C})/\Pi_{1,2s}$ be the orbit of some HM-representative under $\Pi_{1,2s}$. The starting point of our work was problem **B**.2 of [F95] which asks for a sufficient condition to ensure

$$(\mathbf{C}1) \quad \text{all the HM representatives fall in } O_1^{HM}(\mathbf{C})$$

Our main theorem (theorem 2.3) gives such a sufficient condition ((**H**1) for $m = 1$). There is, however, a subtlety. Indeed, the following can happen (*cf.* comment 1 after theorem 2.3)

(**S**) $O^{HM}(\mathbf{C})/\Pi_{1,2s}$ may consist of several orbits yet one contains all the HM-representatives.

or, equivalently, $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{2,2s}}$ may have several geometrically irreducible components yet one contains all the points corresponding to HM-representatives. It does not necessarily follow this geometrically irreducible component is defined over $\mathbb{Q}$ as in the proof of theorem 2.1. On the contrary, lemma 2.2 below states that, if (**S**) occurs, then for generic choices of $\mathbf{t}'_{2,2s} \in \mathcal{U}^{2s-1}(\mathbb{Q})$ none of the geometrically irreducible components of $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{2,2s}}$ is defined over $\mathbb{Q}$.

That is why we need a stronger condition than (**H**1). This is condition (**H**2) in theorem 2.1. For $m = 1$, it ensures that $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{2,2s}}$ remains geometrically irreducible. This is equivalent to the transitivity condition

$$(\mathbf{C}1) \quad \Pi_{1,2s} \text{ acts transitively on } O^{HM}(\mathbf{C}).$$

and automatically implies that $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{2,2s}}$ is defined over $\mathbb{Q}$ provided $\mathbf{t}'_{2,2s} \in \mathcal{U}^{2s-1}(\mathbb{Q})$.

**Lemma 2.2.** *Assume* (**S**) *occurs then, for generic choices of* $\mathbf{t}'_{2,2s} \in \mathcal{U}^{2s-1}(\mathbb{Q})$ *the group* $\Gamma_{\mathbb{Q}}$ *acts transitively on the geometrically irreducible components of* $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{2,2s}}$.

*Proof.* Indeed, consider a birational equation $H(t_1, ..., t_{2s}, Y) = 0$ of $\mathrm{HM}'(\mathbf{C})$. Then $H(t_1, ..., t_{2s}, Y) \in \mathbb{Q}[t_1, ..., t_{2s}, Y]$ is absolutely irreducible. Let $H(t_1, ..., t_{2s}, Y) = \prod_{1\leq i\leq r} F_i(t_1, Y)$ be the factorization of $H(t_1, ..., t_{2s}, Y)$ into a product of irreducible factors in $\overline{\mathbb{Q}(t_2, ..., t_{2s})}[t_1, Y]$. Assume $r \geq 2$ that is, $H(t_1, ..., t_{2s}, Y)$ splits and let $z$ be a primitive element of the field generated over $\mathbb{Q}(t_2, ..., t_{2s})$ by the coefficients of the $(F_i)_{1\leq i\leq r}$. The finite Galois extension $\mathbb{Q}(t_2, ..., t_{2s}, z)/\mathbb{Q}(t_2, ..., t_{2s})$ is not trivial and we denote by $h(t_2, ..., t_{2s}, Z) \in \mathbb{Q}[t_2, ..., t_{2s}, Z]$ the irreducible polynomial of $z$ (up to multiplication by an element of $\mathbb{Q}[t_2, ..., t_{2s}]$) over $\mathbb{Q}(t_2, ..., t_{2s})$. By the Bertini-Noether theorem, there exists a Zariski closed subset $F$ of the hypersurface $V(h)$ defined by $h(t_2, ..., t_{2s}, Z) = 0$ such that for any $(t_2^0, ..., t_{2s}^0, z^0) \in V(h)(\overline{\mathbb{Q}}) \setminus F$, the polynomials $(F_i(t_2^0, ..., t_{2s}^0, z^0, t_1, Y))_{1\leq i\leq r}$ remain irreducible in $\overline{\mathbb{Q}}[t_1, Y]$. Setting $W := (V(h)(\overline{\mathbb{Q}}) \cap \mathbb{Q}^{2s-1} \times \overline{\mathbb{Q}}) \setminus F$, Hilbert irreducibility theorem states there exists a Zariski dense subset $U$ of $W$ such that for any $(t_2^0, ..., t_{2s}^0, z^0) \in U$, $\mathbb{Q}(z^0)/\mathbb{Q}$ is a Galois extension with group $\mathrm{Gal}(\mathbb{Q}(z^0)|\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(t_2, ..., t_{2s}, z)|\mathbb{Q}(t_2, ..., t_{2s}))$. In particular, $\Gamma_{\mathbb{Q}}$ acts transitively on the $(F_i(t_2^0, ..., t_{2s}^0, z^0, t_1, Y))_{1\leq i\leq r}$ the same way as $\Gamma_{\mathbb{Q}(t_2,...,t_{2s})}$ does on the $(F_i)_{1\leq i\leq r}$. □

### *2.4. Irreducible HM-subvarieties defined over $\mathbb{Q}$*

*2.4.1. Statements and comments* Given a group $G$, for any tuple $\mathbf{a} = (a_1, ..., a_m) \in G^m$ and any subgroup $H$ of $G$, we will write

$$< \mathbf{a}^H > := < \{a_1^{h_1}, ..., a_m^{h_m}\}_{h_1,...,h_m \in H} >$$

Given a tuple $\mathbf{A} = (A_1, ..., A_m)$ of subsets of $G$, the symbol $\mathbf{a} \in \mathbf{A}$ means we consider a tuple of elements $\mathbf{a} = (a_1, ..., a_m)$ with $a_i \in A_i$, $i = 1, ..., m$. Finally, given a tuple $\mathbf{A} = (A_1, ..., A_m)$ of conjugacy classes of $G$, we write $[\mathbf{A}] = (A_1, A_1^{-1}, ..., A_m, A_m^{-1})$ and $[\mathbf{A}]^r$ for the tuple obtained by repeating $r$ times $[\mathbf{A}]$.

**Theorem 2.3.** (**Main Theorem**) *Let $G$ be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$ of non trivial conjugacy classes and consider the following hypotheses:*

$$(\mathbf{H}1)\begin{cases} (\mathbf{H}1.0) & There\ exists\ \mathbf{a} \in \mathbf{A}\ such\ that G =< \mathbf{a}, \mathbf{B} > . \\ (\mathbf{H}1.1) & < \mathbf{a}^{<\mathbf{b}>} > \ acts\ transitively\ on B_i, \\ & for\ all\ \mathbf{a} \in \mathbf{A}, \mathbf{b} \in \mathbf{B}, i = 1, \dots , n. \\ (\mathbf{H}1.2) & < \mathbf{a}_i^{<\mathbf{B}>} > \ acts\ transitively\ on A_i, \\ & for\ all\ \mathbf{a}_i = (a_1, \dots , a_{i-1}) \in A_1 \times \cdots \times A_{i-1}, i = 2, \dots , m. \end{cases}$$

($\mathbf{H}2$) *There exists $b_i \in B_i, b_j \in B_j$ such that $b_ib_j = b_jb_i, 1 \leq i \neq j \leq n$.*

*For any integer $s \geq 1$ write $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$. Then we have the following*

→ ($\mathbf{C}1$) *If $\mathbf{A}, \mathbf{B}$ satisfy ($\mathbf{H}1$) then for $s$ large enough, ($\mathbf{C}1$) holds : all the HM-representatives fall in one single $\Pi_{2m-1,2(m+sn)}$-orbit $O^{HM}_{2m-1}(\mathbf{C}_s)$*

→ ($\mathbf{C}2$) *If, in addition $\mathbf{B}$ satisfy ($\mathbf{H}2$) then ($\mathbf{C}2$) holds : $\Pi_{2m-1,2(m+sn)}$ acts transitively on the $SH_{2(m+sn)}$-orbit $O^{HM}(\mathbf{C}_s)$.*

The arrows in →($\mathbf{C}1$) and →($\mathbf{C}2$) are meant to distinguish the full statements from their conclusion parts.

### Comments

1. Here is an example of ($\mathbf{S}$) (that is ($\mathbf{C}1$) holds but not ($\mathbf{C}2$)). Consider the direct product $G := \mathcal{S}_3 \times Q_8$ of the symmetric group of order 6 by the quaternion group $Q_8$. Denote by $C^{(\nu)}$ the conjugacy class of $\nu$-cycles in $\mathcal{S}_3$, $\nu = 2, 3$ and by $C_i$, $C_j$, $C_k$ the conjugacy classes of $i$, $j$, $k$ in $Q_8$. Also set $\mathbf{C}_1 := [C^{(2)} \times \{1\}, C^{(3)} \times \{1\}]$, $\mathbf{C}_2 := [\{1\} \times C_i, \{1\} \times C_j]$, $\mathbf{C} = (\mathbf{C}_1, \mathbf{C}_2)$. Then, one easily checks that $\overline{\mathrm{sni}}(\mathbf{C}_1)$ and $\overline{\mathrm{sni}}(\mathbf{C}_2)$ consists of two elements, say $\mathbf{g}_{1,1}$, $\mathbf{g}_{1,2}$ and $\mathbf{g}_{2,1}$, $\mathbf{g}_{2,2}$ respectively and so, $\overline{\mathrm{sni}}(\mathbf{C}) = \overline{\mathrm{sni}}(\mathbf{C}_1) \times \overline{\mathrm{sni}}(\mathbf{C}_2)$. Furthermore, $\overline{\mathrm{sni}}(\mathbf{C}_a)$ only contains one HM-representative - say $g_{a,1}, a = 1, 2$ so $\mathbf{g} := (\mathbf{g}_{1,1}, \mathbf{g}_{2,1})$ is the only HM-representative contained in $\overline{\mathrm{sni}}(\mathbf{C})$. As a result, showing ($\mathbf{S}$) amounts to showing that the $\Pi_{1,8}$-orbit of $\mathbf{g}$ is strictly contained in its $SH_8$-orbit. To show this, choose explicit representatives for the $g_{a,b}, a, b = 1, 2$. For instance: $\mathbf{g}_{1,1} = (\tau, \tau, c, c^{-1})$, $\mathbf{g}_{1,2} = (\tau, \tau c, c, c)$ where $\tau = (1, 2)$ and $c = (1, 2, 3)$ and $\mathbf{g}_{2,1} = (i, -i, j, -j)$, $\mathbf{g}_{2,2} = (i, i, j, j)$. On the one hand, one has $SH_8 \cdot \mathbf{g} = \overline{\mathrm{sni}}(\mathbf{C})$ ($A_{1,3} \cdot \mathbf{g}_{1,1} = \mathbf{g}_{1,2}$, $A_{6,7} \cdot \mathbf{g}_{2,1} = \mathbf{g}_{2,2}$) and, on the other hand, one has $SH_8 \cdot \mathbf{g} = \{\mathbf{g}, (\mathbf{g}_{1,2}, \mathbf{g}_{2,1})\}$ (any conjugate of $\tau$ in $G$ acts trivially on the elements of $Q_8$).

2. We can now give an explicit value for the constant $r(G)$ of the introduction. For $s \geq 1$ large enough and for any $\mathbf{t}' := \mathbf{t}'_{2m,2(m+sn)} \in \mathcal{U}^{2sn+1}(\overline{\mathbb{Q}})$, both $\mathrm{HM}'(\mathbf{C}_s)_{\mathbf{t}'}$ and $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'}$ are geometrically irreducible of dimension $2m-1$. In particular, when $m = 1$, we obtain HM-curves and condition (**H**1.2) is empty. The constant $r(G)$ mentioned in the introduction can be defined by as the smallest integer $r = 2m-1$ such that there exists **A**, **B** satisfying (**H**1), (**H**2) with $|\mathbf{A}| = m$.
   Compared with [F95, theorem 3.1], theorem 2.3 usually provides lower dimensional geometrically irreducible varieties. For instance, with $G = M_{11}$ and $\mathbf{A} = (8A)$, $\mathbf{B} = (11A)$ (*cf.* example (2) below), the former provides an 8-dimensional variety whereas the latter provides a curve.
   Also observe that the tuple $\mathbf{C}_s = ([\mathbf{A}], [\mathbf{B}]^s)$ built in theorem 2.3 is far from being unique. For instance, any tuple of the form $(\mathbf{C}_s, B_{i_1}, B_{i_1}^{-1}, ..., B_{i_t}, B_{i_t}^{-1})$, $1 \leq i_1, ..., i_t \leq n, t \geq 0$ also works.
3. Instead of (**H**1.1) and (**H**1.2) one can consider the stronger - but easier to check - conditions

$$\begin{cases} (\mathbf{H}1.1^+) < \mathbf{a}^{<\mathbf{b}>} >= G, \text{ for all } \mathbf{a} \in \mathbf{A}, \mathbf{b} \in \mathbf{B}. \\ (\mathbf{H}1.2^+) < \mathbf{a}_i^{<\mathbf{B}>} >= G, \text{ for all } \mathbf{a}_i = (a_1, \dots, a_{i-1}) \in A_1 \times \dots \times A_{i-1}, \\ \qquad\qquad i = 2, \dots, m. \end{cases}$$

These lead to the following practical corollary.

**Corollary 2.4.** *Let G be a finite group containing two tuples* $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$ *and* $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$ *such that*

$(i)$ $G =< A_1 >=< \mathbf{B} >$ .
$(ii)$ $(\mathbf{A}, \mathbf{B}) \in \mathcal{C}_{m+n}(G)$ *is g-complete.*
$(iii)$ *There exists* $b_i \in B_i$, $b_j \in B_j$ *such that* $b_i b_j = b_j b_i$, $1 \leq i \neq j \leq n$.

*Then, for s large enough, writing* $\mathbf{C}_s := ([\mathbf{A}], [\mathbf{B}]^s)$, *there is a unique* $SH_{2(m+sn)}$*-HM-orbit* $O^{HM}(\mathbf{C}_s)$ *and* $\Pi_{2m-1,2(m+sn)}$ *acts transitively on it.*

*Proof.* For any $\mathbf{a} \in \mathbf{A}$, $\mathbf{b} \in \mathbf{B}$, $< \mathbf{a}^{<\mathbf{b}>} >$ is normal in $< \mathbf{a}, \mathbf{b} >$. But by (ii) $< \mathbf{a}, \mathbf{b} >= G$ thus, $< \mathbf{a}^{<\mathbf{b}>} >$ is normal in $G$ and, in particular, contains $< A_1 >= G$ (by (i)), which implies (**H**1.1$^+$). As for (**H**1.2$^+$), since $< \mathbf{a}_i^{<\mathbf{B}>} >$ is normal in $< \mathbf{B} >= G$ (by (i)) it contains $< A_1 >= G$ (by (i)), which implies (**H**1.2$^+$). □

The hypotheses of corollary 2.4 are fulfilled automatically when $G$ is simple and (**A**, **B**) g-complete (*cf.* example (2)). They also are preserved by Frattini extensions (*cf.* proposition 2.7). However compared with theorem 2.3, corollary 2.4 is often too restrictive (*cf.* examples (1) and (3))

*2.4.2. Examples* The purpose of this section is to give examples of groups satisfying ($\mathbf{H}1.1$), ($\mathbf{H}1.2$) and ($\mathbf{H}2$) (condition ($\mathbf{H}1.0$) is here to ensure $\overline{\mathrm{hm}}(\mathbf{C})$ is not empty and it will always be fulfilled in our examples - where either the tuple $(\mathbf{A}, \mathbf{B})$ is g-complete or the stronger condition ($\mathbf{H}1.1^+$) holds). We are particularly interested in minimizing $m$ that is, obtaining HM-subvarieties of low dimension.

(1) Symmetric and alternating groups: Consider the symmetric group $\mathcal{S}_p$ where $p \geq 5$ is a prime number, $\mathbf{A} = (C^{(p)})$ and $\mathbf{B} = (C^{(2)})$ where $C^{(i)}$ denotes the conjugacy class of $i$-cycles in $G$, $i = 2, ..., p$. For any $a \in C^{(p)}, b \in C^{(2)}$, $< a^{<b>} > \lhd < a, b >$. But $< a, b >$ is a transitive group of prime degree $p$, so it is primitive [Wi84, Th.8.3] and, since it contains a 2-cycle, it is $\mathcal{S}_p$ [Wi84, Th.13.3]. As a consequence $< a^{<b>} >= \mathcal{A}_p$, which acts transitively on the 2-cycles class. Likewise, consider the alternating group $G := \mathcal{A}_p$ where $p \geq 5$ is a prime number, $\mathbf{A} = (C^{(p)})$ and $\mathbf{B} = (C^{(3)})$. For any $a \in C^{(p)}, b \in C^{(3)}$, $< a^{<b>} > \lhd < a, b >$. But $< a, b >$ is a transitive group of prime degree $p$, so it is primitive and, since it contains a 3-cycle, it is $\mathcal{A}_p$ [Wi84, Th. 13.3]. So conditions ($\mathbf{H}1$) and ($\mathbf{H}2$) hold.

(2) Non abelian finite simple groups: Suppose $G$ is a non abelian finite simple group. With the notation of corollary 2.4, observe that since $G$ is simple hypothesis (i) is automatically fulfilled since the groups $< A_1 >$, $< \mathbf{B} >$ are normal. So we are only left to check hypotheses (ii) and (iii). Taking $n = 1$, (iii) is automatically fulfilled too. So, for a simple group $G$ we always have $c(G) \leq 2l(G) - 3$ where $l(G)$ denotes the minimal length of a g-complete tuple $(A_1, ..., A_m, B)$ of non trivial conjugacy classes of $G$.

*Example 2.5.* Here are examples of simple groups containing g-complete 2-tuples of conjugacy classes.
- According to the Atlas, the Mathieu group $M_{11}$ has 10 conjugacy classes: 1A, 2A, 3A, 4A, 5A, 6A, 8A, B**, 11A, B** and its maximal subgroups have order 720, 660, 144, 120, 48. Since none of these orders is divisible by both 8 and 11, (8A, 11A) is a g-complete 2-tuple for $M_{11}$. So, $M_{11}$ satisfies ($\mathbf{H}1$) with $\mathbf{A} = (8A), \mathbf{B} = (11A)$.

- The argument above, using the maximal subgroups given by the Atlas, works for instance with $m = 1$ and
$M_{23}$ with $A = 7A$ and $B = 11A$, (443520, 40320, 20160, 7920, 5760, 253).
$Sz(8)$ with $A = 5A$ and $B = 7A$, (448, 52, 20, 14).
$J_2$ with $A = 5A$ and $B = 7A$, (6048, 2160, 1920, 1152, 720, 600, 336, 300, 60).
$J_3$ with $A = 5A$ and $B = 17A$, (8160, 3420, 2880, 2448, 2160, 1944, 1920, 1152).
$Ly$ with $A = 37A$ and $B = 67A$, ($5859.10^6$, $5388768.10^3$, $465.10^5$, $299168.10^2$, $9.10^6$, 3849120, 699840, 1474, 666).
*etc.*

- Consider the projective special linear groups $\mathrm{L}_2(p)$ where $p \equiv 3$ [mod4], $p \geq 7$ is a prime number. The following theorem of Dickson [Di]: *Let $p \geq 5$ a prime number, then the order of the maximal subgroups of the projective special linear group $L_2(p)$ belongs to $\{\frac{p(p-1)}{2}, p-1, p+1, 60\}$ if $p \equiv \pm 1$ [mod10] and to $\{\frac{p(p-1)}{2}, p-1, p+1, 24, 12\}$ else* shows the tuple $(2A, pA)$ is g-complete.

(3) Families of $p$-groups: All the assertions in the following can be found in [S86], Chap. 2 §2 or Chap. 4 §4.

(3-1) $p = 2$: Then $G$ is one of the following groups:
- Dihedral group of order $2^r$: $D_{2^r} = < x, y | x^{2^{r-1}} = y^2 = 1,\ yxy = x^{-1} >$.
- Special dihedral group of order $2^r$: $S_{2^r} =< x, y | x^{2^{r-1}} = y^2 = 1,\ yxy = x^{-1+2^{r-2}} >$.
- Generalized quaternion group of order $2^r$: $Q_{2^r} = < x, y | x^{2^{r-1}} = y^2,\ y^{-1}xy = x^{-1} >$.

and, taking $A = C_y^G$, $B = C_x^G$, using the relations, one immediately checks that for each $a \in A$ we have $B = \{x, axa^{-1}\}$, so condition (**H**1.1) is fulfilled and, since $m = n = 1$, conditions (**H**1.2) and (**H**2) are empty.

(3-2) $p > 2$: We use the following lemma.

**Lemma 2.6.** *Let $G$ be a finite group with Frattini subgroup $\Phi(G)$. Assume the quotient $G/\Phi(G)$ is abelian, then, for any $x_1, ..., x_d \in G$ such that $G/\Phi(G) = \bigoplus_{i=1}^d < \overline{x_i} >$, the tuple $\mathbf{C} := (C_{x_1}^G, ..., C_{x_d}^G)$ is g-complete.*

*Proof.* Indeed, for any $g_1, ..., g_d \in G$, since $G/\Phi(G)$ is abelian, one has $\overline{x_i^{g_i}} = \overline{x_i}$, $i = 1, ..., r$ so $G =< x_1^{g_1}, ..., x_d^{g_d}, \Phi(G) >$ which, by the characterization of the Frattini subgroup, implies $G =< x_1^{g_1}, ..., x_d^{g_d} >$. □

A finite $p$-group $G$ has the property that $G/\Phi(G)$ is an elementary abelian $p$-group. Assume furthermore that $\Phi(G) = Z(G)$ and $G/\Phi(G) =< \overline{x} > \oplus < \overline{y} >$. Then any $g \in G$ can be written in a unique way $g = x^{u_g} y^{v_g} \phi_g = y^{v_g} x^{u_g} \psi_g$ with $\phi_g, \psi_g \in Z(G)$ and all the elements in $A := C_y^G$ are of the form $y\phi$, $\phi \in Z(G)$. So, for any $a \in A$, we have $B = C_x^G = \{a^i x a^{-i}\}_{i \geq 0}$ and, consequently, $< a > \subset < a^{<b>} >$ for any $b \in B$. This shows (**H**1.1) is fulfilled and, once again, since $m = n = 1$, conditions (**H**1.2) and (**H**2) are empty. The following groups satisfy these hypotheses:
- $M(p^r) =< x, y | x^{p^{r-1}} = y^p = 1,\ y^{-1}xy = x^{1+p^{r-2}} >$.
- Any non abelian group of order $p^3$. Recall that such a group is isomorphic to $D_8$ or $Q_8$ if $p = 2$ or to $M(p^3)$ or $E(p^3)$ if $p > 2$, where

$$E(p^3) < x, y | x^p = y^p = [x, y]^p = 1,\ [x, y] \in Z(E(p^3)) >$$

(4) Frattini extensions: The next result is about Frattini extensions; it is related to modular towers §4.1.2 and will be proved in 3.2. It will give us information about regular realizations of finite unsplit extensions of a given finite group $G$, which is a difficult matter, even when the group $G$ is known to be regularly realized (this is the theory of embedding problems, [MMa99], Chap.V)

**Proposition 2.7.** (Frattini covers) *Let $G$ be a finite group satisfying* (**H**1.0)*,* (**H**1.1$^+$)*,*(**H**1.2$^+$) *with* $\mathbf{A} = (A_1, ..., A_m)$*,* $\mathbf{B} = (B_1, ..., B_n)$*. Then, for $s$ large enough,* $([\mathbf{A}], [\mathbf{B}]^s)$ *satisfies* (**C**1) *and*

→ (**C**3) *Given a finite Frattini cover* $\tilde{G} \to G$, (**C**3) *holds, that is : for any tuples* $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}$ *above* $\mathbf{A}$, $\mathbf{B}$, *the tuple* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *satisfies* (**C**1).

*We have the following additional conclusions:*

→ (**C**4) *If the $B_i, i = 1, \dots, n$ are $p'$-conjugacy classes for a given prime number $p$ and $G$,* $\mathbf{A}, \mathbf{B}$ *satisfy* (**H**2) *then, given a finite Frattini cover* $\tilde{G} \to G$ *with $p$-group kernel,* (**C**4) *holds, that is : there exists tuples* $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}$ *of conjugacy classes of* $\tilde{G}$ *above* $\mathbf{A}$ *and* $\mathbf{B}$ *such that the tuple* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *satisfies* (**C**1) *and* (**C**2).

→ (**C**5) *If $n = 1$ then, given a finite Frattini cover* $\tilde{G} \to G$*,(***C**5*) holds, that is : for any tuples* $\tilde{\mathbf{A}}, \tilde{\mathbf{B}}$ *above* $\mathbf{A}, \mathbf{B}$, *the tuple* $([\tilde{\mathbf{A}}], [\tilde{\mathbf{B}}]^s)$ *satisfies (***C**1*) and(***C**2*).*

## 3. Group theoretical proofs

This section is devoted to the proofs of theorems 2.3 and proposition 2.7. They rely on the following technical lemma, the proof of which is postponed to section 3.3:

**Lemma 3.1.** *Suppose given a finite group $G$ and a symmetric $2s$-tuple* $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$*.*

*(1) For any $1 \leq k \leq s$ there exists $u_k \in \Pi_{1,2s}$ such that for any HM representative* $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$

$$u_k \cdot \mathbf{g} = [g_1, ..., g_k^{g_1}, ..., g_s]$$

*(2) For any $2 \leq k \leq s$ and for any $\underline{i} = (i_1, ..., i_r)$ with $2 \leq i_1 < i_2 < ... < i_r \leq k - 1$ there exists $v_{\underline{i},k} \in \Pi_{1,2s}$ such that for any HM representative* $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$

$$v_{\underline{i},k} \cdot \mathbf{g} = [g_1, ..., {g_k^{g_1}}^{g_{i_r} \cdots g_{i_1}}, ..., g_s]$$

*(3) For any* $2 \leq k \leq s$, *for any* $\underline{i} = (i_1, ..., i_r)$ *with* $k + 1 \leq i_1 < i_2 < ... < i_r \leq s - 1$ *there exists* $w_{k,\underline{i}} \in \Pi_{1,2s}$ *such that for any HM representative* $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$

$$w_{k,\underline{i}} \cdot \mathbf{g} = [g_1, ..., g_k^{g_1^{g_{i_r} \cdots g_{i_1}}}, ..., g_s]$$

The underlying idea of lemma 3.1 (and of the whole proof) is that, the larger the tuple $[C_2, ..., C_s]$ is, the larger the groups generated by the $g_1^{g_{i_r} \cdots g_{i_1}}$ with $\underline{i} = (i_1, ..., i_r)$ as in (2) and (3) of lemma 3.1 are; our purpose is to show that under the assumptions of theorem 2.3 these groups are large enough to act transitively on the conjugacy classes $C_2, ..., C_s$.

### *3.1. Proof of theorem 2.3*

In the following, we say $\sigma = (\sigma(1), ..., \sigma(\nu))$ is an ordered $\nu$-tuple in a subset $\Sigma \subset \mathbb{N}$ if $\sigma(k) \in \Sigma$, $k = 1, ..., \nu$ and $\sigma(1) < \sigma(2) < ... < \sigma(\nu)$. Given such an ordered $\nu$-tuple $\sigma$, we write $\sigma + l$ for the translated ordered $\nu$-tuple $(\sigma(1) + l, ..., \sigma(\nu) + l)$.

*3.1.1. Case* $m = 1$ Let $G$ be a finite group and $A$, $\mathbf{B} = (B_1, ..., B_n)$ be $n + 1$ non trivial conjugacy classes of $G$.

(1) Given $\mathbf{b} = (b_1, ..., b_n) \in \mathbf{B}$, write $< \mathbf{b} >= \{\beta_1, ..., \beta_s\}$; each $\beta_j$ can be written as a product of say $s(j)$ terms of the form $\mathbf{b}_{\sigma_{k,j}} := b_{\sigma_{k,j}(1)} \cdots b_{\sigma_{k,j}(\nu_{k,j})}$ where $\sigma_{k,j} = (\sigma_{k,j}(1), ..., \sigma_{k,j}(\nu_{k,j}))$ is an ordered tuple in $\{1, ..., n\}$, $k = 1, ..., s(j)$, $j = 1, ..., s$. Setting $N(\mathbf{b}) = \max\{s(j)\}_{1 \leq j \leq s}$, the set

$$\{\mathbf{b}_{\sigma_1} \cdots \mathbf{b}_{\sigma_s}\}_{\substack{\sigma \text{ ordered tuple in } \{1,...,n\} \\ s \leq N(\mathbf{b})}}$$

contains $< \mathbf{b} >$, that is, is equal to $< \mathbf{b} >$. And, since by definition $< a^{<\mathbf{b}>} >$ is the subgroup generated by $\{a^b\}_{b \in <\mathbf{b}>}$, one deduces from the above that

$$< a^{<\mathbf{b}>} >=< \{a^{\mathbf{b}_{\sigma_1} \cdots \mathbf{b}_{\sigma_s}}\}_{\substack{\sigma \text{ ordered tuple in } \{1,...,n\} \\ s \leq N(\mathbf{b})}} >$$

(2) Write $N_i = |B_i|$, $i = 1, ..., n$ and $N^0 = \max\{\mathrm{N}(\mathbf{b})\}_{\mathbf{b} \in \mathbf{B}}$ and set $N = N_1 \cdots N_n N^0$. Then, for any $(b_{i,1}, ..., b_{i,n})_{1 \leq i \leq N} \in \mathbf{B}^N$ there is at least one $\mathbf{b} = (b_1, ..., b_n) \in \mathbf{B}$ which is repeated $N^0$ times among the $(b_{i,1}, ..., b_{i,n})$, $i = 1, ..., N$ and since $N(\mathbf{b}) \leq N^0$, step (1) yields:

**Lemma 3.2.** *There exists* $N := N(\mathbf{B}) \geq 1$ *depending only on* $\mathbf{B}$ *such that for any* $(u_i)_{1 \leq i \leq nN} := (b_{i,1}, ..., b_{i,n})_{1 \leq i \leq N} \in \mathbf{B}^N$ *there exists* $\mathbf{b} \in \mathbf{B}$ *satisfying*

$$< a^{<\mathbf{b}>} >=< \{a^{u_{\sigma(\nu)} \cdots u_{\sigma(1)}}\}_{\sigma \text{ ordered tuple in } \{1,...,nN\}} >, \text{ for each } a \in A$$

We now show that, for $x \geq N(\mathbf{B}) + 1$, the tuple $\mathbf{C}_x = ([A], [\mathbf{B}]^{2x})$ will satisfy ($\mathbf{C}1$) provided $A, \mathbf{B}$ satisfy ($\mathbf{H}1$) and ($\mathbf{C}2$) provided $\mathbf{B}$ also satisfies ($\mathbf{H}2$).

($\mathbf{H}1$) $\Rightarrow$ ($\mathbf{C}1$): For any $1 \leq k \leq 4nx$ one can always find in $[\mathbf{B}]^{2x}$ either $N(\mathbf{B}) + 1$ copies of $[\mathbf{B}]$ before $k$ (if $2nx \leq k \leq 4nx$) or $N(\mathbf{B}) + 1$ copies of $[\mathbf{B}]$ after $k$ ( if $0 \leq k \leq 2nx$). Let $\mathbf{g} = [a, h_1, ..., h_{2nx}] \in \overline{\mathrm{hm}}(\mathbf{C}_x)$ be a HM-representative and $g \in G$. We are to show that, for any $1 \leq k \leq 4nx$, $\mathbf{g}$ and $[a, h_1, ..., h_k^g, ..., h_{2nx}]$ fall in the same orbit under $\Pi_{1,4nx+2}$. Suppose for instance $2nx \leq k \leq 4nx$, that is there are at least $N(\mathbf{B}) + 1$ copies of $[\mathbf{B}]$ before $k$ and so, according to lemma 3.2, there is at least one $n$-tuple $\mathbf{b} = (b_1, ..., b_n) \in \mathbf{B}$ such that $< a^{<\mathbf{b}>} >$ is generated by the set $\{a^{h_{\sigma(\nu)} \cdots h_{\sigma(1)}}\}_{\sigma \text{ ordered tuple in } \{1,...,nx-1\}}$. But since $< a^{<\mathbf{b}>} >$ acts transitively on the conjugacy class of $h_k$, we can assume that $g \in < a^{<\mathbf{b}>} >$ and, consequently, that $g$ can be written as a product $x_1 \cdots x_s$ of $s$ terms of the form $x_k = a^{h_{\sigma_k(\nu_k)} \cdots h_{\sigma_k(1)}}$, where $\sigma_k = (\sigma_k(1), ..., \sigma_k(\nu_k))$ is an ordered tuple in $\{1, ..., nx - 1\}$, $k = 1, ..., s$. So, we are left to do the following $s$ operations

$$\begin{aligned}\mathbf{g} &\rightarrow [a, h_1, \ldots, h_k^{x_s}, \ldots, h_{2nx}]\\ &\rightarrow [a, h_1, \ldots, h_k^{x_{s-1}x_s}, \ldots, h_{2nx}]\\ &\ldots\\ &\rightarrow [a, h_1, \ldots, h_k^{x_1 \cdots x_{s-1}x_s}, \ldots, h_{2nx}]\end{aligned}$$

But, according to part (2) of lemma 3.1, these can be handled by applying successively $v_{\sigma_s+1,k+1}$, $v_{\sigma_{s-1}+1,k+1}$ *etc.*, $k = 1, ..., s$. If $1 \leq k \leq 2nx$, use part (3) of lemma 3.1 instead of part (2).

($\mathbf{H}1$) & ($\mathbf{H}2$) $\Rightarrow$ ($\mathbf{C}2$): From now on, we denote by $\mathbf{C}$ the tuple $\mathbf{C}_x$ built above and set $s = 2nx + 1$. We assume furthermore ($\mathbf{H}2$) is fulfilled that is, there exists $b_i \in B_i$, $b_j \in B_j$ such that $b_i b_j = b_j b_i$, $1 \leq i \neq j \leq n$. We have shown that all the HM-representatives fall in one single orbit $\mathrm{O}_1^{\mathrm{HM}}(\mathbf{C}) \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{1,2\mathrm{s}}$ so in one single orbit $\mathrm{O}_2^{\mathrm{HM}}(\mathbf{C}) \in \overline{\mathrm{sni}}(\mathbf{C})/\Pi_{2,2\mathrm{s}}$ as well. In the first place, we prove the $\Pi_{2,2s}$ HM-orbit $\mathrm{O}_2^{\mathrm{HM}}(\mathbf{C})$ has the same length as the $SH_{2s}$ HM-one $\mathrm{O}^{\mathrm{HM}}(\mathbf{C})$, that is, they coincide. In the second place we show that $\mathrm{O}_2^{\mathrm{HM}}(\mathbf{C}) = \mathrm{O}_1^{\mathrm{HM}}(\mathbf{C})$.

Condition ($\mathbf{H}2$) implies $SH_{2s}$ leaves $\mathrm{O}_2^{\mathrm{HM}}(\mathbf{C})$ globally invariant. Indeed, since $\Pi_{2,2s}$ is normal in $SH_{2s}$, $SH_{2s}$ permutes the orbits of $\overline{\mathrm{sni}}(\mathbf{C})/\Pi_{2,2s}$. But, for any HM-representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, straightforward computations give

$$\begin{cases} a_{2i,2j} \cdot \mathbf{g} = ([g_1, \ldots, g_{i-1}], g_i, (g_i^{-1})^{g_i^{-1} g_j}, [g_{i+1}, \ldots, g_{j-1}], \\ \quad g_j^{g_i^{-1}}, g_j^{-1}, [g_{j+1}, \ldots, g_{2nx+1}]), \quad 2 \leq i < j \leq s \\ a_{2i,2j+1} \cdot \mathbf{g} = ([g_1, \ldots, g_{i-1}], g_i, (g_i^{-1})^{g_i^{-1} g_j^{-1}}, [g_{i+1}, \ldots, g_{j-1}], g_j, \\ \quad (g_j^{-1})^{g_j^{-1} g_i^{-1}}, [g_{j+1}, \ldots, g_{2nx+1}]), \quad 2 \leq i \leq j \leq s - 1 \\ a_{2i-1,2j} \cdot \mathbf{g} = ([g_1, \ldots, g_{i-1}], g_i^{g_j}, g_i^{-1}, [g_{i+1}, \ldots, g_{j-1}], g_j^{g_i}, g_j^{-1}, \\ \quad [g_{j+1}, \ldots, g_{2nx+1}]), \quad 2 \leq i \leq j \leq s \\ a_{2i-1,2j+1} \cdot \mathbf{g} = ([g_1, \ldots, g_{i-1}], g_i^{g_j^{-1}}, g_i^{-1}, [g_{i+1}, \ldots, g_{j-1}], g_j, \\ \quad (g_j^{-1})^{g_j^{-1} g_i}, [g_{j+1}, \ldots, g_{2nx+1}]), \quad 2 \leq i < j - 1 \leq s - 2 \end{cases}$$

Consequently, any HM-representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$ with $g_i g_j = g_j g_i$ - such a HM representative always exists according to (**H**2) and the way **C** was built - is fixed by $a_{i,j}$ that is, $a_{i,j} \cdot O_2^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$, $3 \leq i < j \leq 2s$. And, since $O_2^{HM}(\mathbf{C})$ is a $\Pi_{2,2s}$ orbit, we obviously have $a_{i,j} \cdot O_2^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$, $i = 1, 2 < j \leq 2s$. Consequently

$$\begin{aligned} SH_{2s} \cdot O_2^{HM}(\mathbf{C}) &= O_2^{HM}(\mathbf{C}) \\ &\supset SH_{2s} \cdot \overline{\text{hm}}(\mathbf{C}) = O^{HM}(\mathbf{C}) \end{aligned}$$

We now show that $O_1^{HM}(\mathbf{C}) = O_2^{HM}(\mathbf{C})$. As above, $\Pi_{1,2s}$ being normal in $\Pi_{2,2s}$ entails that $\Pi_{2,2s}$ permutes the orbits of $\overline{\text{sni}}(\mathbf{C})/\Pi_{1,2s}$. Thus, it is enough to show that for any $i = 3, ..., 2s$ there exists $\mathbf{g} \in \overline{\text{hm}}(\mathbf{C})$ with $a_{2,i} \cdot \mathbf{g} \in O_1^{HM}(\mathbf{C})$. But, for any HM-representative $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$ straightforward computations give

$$\begin{cases} a_{2,2i+1}^{-1} \cdot \mathbf{g} = (g_1, (g_1^{-1})^{g_i}, [g_2, \dots, g_{i-1}], g_i, (g_i^{-1})^{g_1}, [g_{i+1}, \dots, g_s]) \\ \qquad\qquad = (g_1^{g_i^{-1}}, g_1^{-1}, [g_2^{g_i^{-1}}, \dots, g_{i-1}^{g_i^{-1}}], g_i, (g_i^{-1})^{g_i^{-1} g_1}, [g_{i+1}^{g_i^{-1}}, \dots, g_s^{g_i^{-1}}]) \\ a_{2,2i}^{-1} \cdot \mathbf{g} \quad = (g_1, (g_1^{-1})^{g_i^{-1}} [g_2, \dots, g_{i-1}], g_i^{g_i^{-1} g_1}, g_i^{-1}, [g_{i+1}, \dots, g_s]) \\ \qquad\qquad = (g_1^{g_i}, g_1^{-1} [g_2^{g_i}, \dots, g_{i-1}^{g_i}], g_i^{g_1}, g_i^{-1}, [g_{i+1}^{g_i}, \dots, g_s^{g_i}]) \end{cases}$$

and, by the proof of (**H**1) ⇒ (**C**2), there exists $u_{i,\mathbf{g}}, v_{i,\mathbf{g}} \in \Pi_{1,2s}$ such that

$$\begin{cases} u_{i,\mathbf{g}} \cdot \mathbf{g} = [g_1, g_2^{g_i^{-1}}, \dots, g_{i-1}^{g_i^{-1}}, g_i, g_{i+1}^{g_i^{-1}}, \dots, g_{2nx+1}^{g_i^{-1}}] \\ v_{i,\mathbf{g}} \cdot \mathbf{g} = [g_1, g_2^{g_i}, \dots, g_{i-1}^{g_i}, g_i, g_{i+1}^{g_i}, \dots, g_{2nx+1}^{g_i}] \end{cases}$$

One then checks that

$$\begin{cases} a_{1,2i} u_{i,\mathbf{g}} \cdot \mathbf{g} \quad = a_{2,2i+1}^{-1} \cdot \mathbf{g} \\ a_{1,2i-1} v_{i,\mathbf{g}} \cdot \mathbf{g} = a_{2,2i}^{-1} \cdot \mathbf{g} \end{cases}$$

which yields the expected result observing that $a_{1,2i} u_{i,\mathbf{g}}, a_{1,2i-1} v_{i,\mathbf{g}} \in \Pi_{1,2s}$.

□

*3.1.2. Case $m \geq 2$* Keeping the same notation as above the $2s$-tuple we are going to consider will be once again of the form $\mathbf{C}_x = ([\mathbf{A}], [\mathbf{B}]^{2x})$ with $x$ large enough. The following lemma is a straightforward generalization of lemma 3.2.

**Lemma 3.3.** *Let $G$ be a finite group and consider two tuples $\mathbf{A} = (A_1, ..., A_m) \in \mathcal{C}_m(G)$, $\mathbf{B} = (B_1, ..., B_n) \in \mathcal{C}_n(G)$. There exists $N := N(\mathbf{B}) \geq 1$ depending only on $\mathbf{B}$ such that for any $(u_i)_{1 \leq i \leq nN} := (b_{i,1}, ..., b_{i,n})_{1 \leq i \leq N} \in \mathbf{B}^N$ there exists $\mathbf{b} \in \mathbf{B}$ satisfying*

$$< \mathbf{a}^{<\mathbf{b}>} >=< \{a_i^{u_{\sigma(\nu)} \cdots u_{\sigma(1)}}\}_{\substack{1 \leq i \leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \textit{ for each } \mathbf{a} \in \mathbf{A}$$

(**H**1) ⇒ (**C**1): As in section 3.1.1, if $x \geq N+1$, condition (**H**1.1) ensures two HM-representatives of the form $[a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_m, h_1^{g_1}, ..., h_{2nx}^{g_{2nx}}]$ fall in the same orbit under $\Pi_{2m-1,4nx+2m}$. To prove it, just observe the method used to construct the elements $u_k$, $v_{\underline{i},k}$, $w_{k,\underline{i}}$ of $\Pi_{1,2s}$ in lemma 3.1 gives similarly elements $u_k^i$, $v_{\underline{i},k}^i$, $w_{k,\underline{i}}^i$ of $\Pi_{2i-1,2s}$ such that

$$\begin{cases} u_k^i \cdot \mathbf{g} = [g_1, \ldots, g_k^{g_i}, \ldots, g_s], \quad 1 \leq i < k \leq s \\ v_{i_1<\ldots<i_r,k}^i \cdot \mathbf{g} = [g_1, \ldots, g_k^{g_i^{g_{i_r}\cdots g_{i_1}}}, \ldots, g_s], \\ \quad \underline{i} = (i_1, \ldots, i_r) \quad \text{with}\, i < i_1 < i_2 < \ldots < i_r < k \\ w_{k,i_1<\ldots<i_r}^i \cdot \mathbf{g} = [g_1, \ldots, g_k^{g_i^{g_{i_r}\cdots g_{i_1}}}, \ldots, g_s], \\ \quad \underline{i} = (i_1, \ldots, i_r) \quad \text{with}\, i < k < i_1 < i_2 < \ldots < i_r \end{cases}$$

Now, let $2 \leq i \leq m$ and $g \in G$. We are left to show $\mathbf{g} = [a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_i^g, ..., a_m, h_1^{g_1}, ..., h_{2nx}^{g_{2nx}}]$ fall in the same orbit under $\Pi_{2m-1,4nx+2m}$. First note that there exists a constant $M \geq 1$ such that any element of $< \mathbf{B} >$ can be written as the product of at most $M$ elements of $\cup_{1\leq i\leq n} B_i$. Up to increasing the number $x$ of copies of $\mathbf{B}^0$, we assume $2x \geq M$. Since $< \mathbf{a}_i^{<\mathbf{B}>} >$ acts transitively on the conjugacy class of $a_i$, we can assume that $g \in < \mathbf{a}_i^{<\mathbf{B}>} >$ and consequently that $g$ can be written as the product $x_1 \cdots x_s$ of $s$ terms of the form $x_k = a_{i_k}^{b_{k,\nu_k} \cdots b_{k,1}}$, where $i_k \in \{1, ..., i-1\}$, $b_{k,j} \in \cup_{1\leq i\leq n} B_i$, $j = 1, ..., \nu_k$ and $\nu_k \leq M, k = 1, ..., s$. So, this time, we have to carry out the following $s$ operations

$$\begin{aligned} \mathbf{g} &\to [a_1, \ldots, a_i^{x_s}, \ldots, a_m, h_1, \ldots, h_{2nx}] \\ &\to [a_1, \ldots, a_i^{x_{s-1}x_s}, \ldots, a_m, h_1, \ldots, h_{2nx}] \\ &\ldots \\ &\to [a_1, \ldots, a_i^{x_1\cdots x_{s-1}x_s}, \ldots, a_m, h_1, \ldots, h_{2nx}] \end{aligned}$$

Since $2x \geq M$, one can always find $(h'_1, ..., h'_{2nx}) \in \mathbf{B}^{2x}$ and $s$ ordered tuples $\sigma_k = (\sigma_k(1), ..., \sigma_k(\nu_k))$ in $\{1, ..., 2nx\}$, $k = 1, ..., s$ such that $b_{k,i} = h'_{\sigma_k(i)}$, $i = 1, ..., \nu_k$, $k = 1, ..., s$. But, as already noticed, $[a_1, ..., a_m, h_1, ..., h_{2nx}]$ and $[a_1, ..., a_m, h'_1, ..., h'_{2nx}]$ fall in the same orbit of $\Pi_{2m-1,4nx+2m}$. Then apply successively the elements $w_{\sigma_s+m,i}^{i_s}, w_{\sigma_{s-1}+m,i}^{i_{s-1}}$ *etc.*, $k = 1, ..., r$ to $[a_1, ..., a_m, h'_1, ..., h'_{2nx}]$ in order to obtain $[a_1, ..., a_i^g, ..., a_m, h'_1, ..., h'_{2nx}]$. To conclude, use once again that $[a_1, ..., a_i^g, ..., a_m, h'_1, ..., h'_{2nx}]$ and $[a_1, ..., a_i^g, ..., a_m, h_1, ..., h_{2nx}]$ fall in the same orbit of $\Pi_{2m-1,4nx+2m}$.

(**H**1) & (**H**2) ⇒ (**C**2): This part of the proof remains unchanged since (**H**2) ensures $SH_{4nx+2m}$ leaves $O_{2m-1}^{HM}(\mathbf{C}_x)$ globally invariant.

### *3.2. Proof of proposition 2.7*

We retain the notation of 3.1.1, 3.1.2 and of proposition 2.7. Consider the integer $N := N(\mathbf{B}) \geq 1$ defined in lemma 3.3. Then, according to ($\mathbf{H}11.^{+}$), for any $(\tilde{u}_i)_{1\leq i\leq nN} := (\tilde{b}_{i,1}, ..., \tilde{b}_{i,n})_{1\leq i\leq N} \in \tilde{\mathbf{B}}^N$ there exists $\tilde{\mathbf{b}} \in \tilde{\mathbf{B}}$ satisfying

$$G =< \{s(\tilde{a}_i^{\tilde{u}_{\sigma(\nu)}\cdots\tilde{u}_{\sigma(1)}})\}_{\substack{1\leq i\leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \text{ for each } \tilde{\mathbf{a}} \in \tilde{\mathbf{A}}$$

But, $s : \tilde{G} \to G$ being a Frattini cover, this entails

$$\tilde{G} =< \{\tilde{a}_i^{\tilde{u}_{\sigma(\nu)}\cdots\tilde{u}_{\sigma(1)}}\}_{\substack{1\leq i\leq m \\ \sigma \text{ ordered tuple in } \{1,...,nN\}}} >, \text{ for each } \tilde{\mathbf{a}} \in \tilde{\mathbf{A}}$$

So we can always take $N = N(\mathbf{B}) = N(\tilde{\mathbf{B}})$. Now, recall that in ($\mathbf{H}1$) $\Rightarrow$ ($\mathbf{C}1$) & ($\mathbf{C}2$) we have also imposed that $2x \geq M$. The Frattini property shows $M$ does not have to be increased when passing from $G$ to $\tilde{G}$. Indeed, ($\mathbf{H}1.2^{+}$) means that

$$G =< \{s(\tilde{a}_k^{\tilde{\beta}_1\cdots\tilde{\beta}_l})\}_{\substack{1\leq k\leq i-1 \\ \tilde{\beta}_j\in\cup_{1\leq i\leq n}\tilde{B}_i,\, l\leq M}} > \text{ for each } \tilde{\mathbf{a}}_i \in \tilde{\mathbf{A}}_1 \times \cdots \times \tilde{\mathbf{A}}_1,\ i = 2, ..., m.$$

which entails that

$$\tilde{G} =< \{\tilde{a}_k^{\tilde{\beta}_1\cdots\tilde{\beta}_l})\}_{\substack{1\leq k\leq i-1 \\ \tilde{\beta}_j\in\cup_{1\leq i\leq n}\tilde{B}_i,\, l\leq M}} > \text{ for each } \tilde{\mathbf{a}}_i \in \tilde{\mathbf{A}}_1 \times \cdots \times \tilde{\mathbf{A}}_1,\ i = 2, ..., m.$$

This and section 3.1.2 show the $4nx + 2m$-tuple $\tilde{\mathbf{C}}$ one gets replacing $A_i$ by $\tilde{A}_i$, $i = 1, ..., n$ and $B_i$ by $\tilde{B}_i$, $i = 1, ..., m$ satisfies ($\mathbf{C}1$). As for the second part of proposition 2.7, we are left to show $\tilde{\mathbf{B}}$ can be chosen in such a way that the commutativity conditions ($\mathbf{H}2$) are still fulfilled. For this, choose $b_i \in B_i$ and apply Schur-Zassenhauss lemma to the short exact sequence

$$1 \to \ker(s) \to s^{-1}(< b_i >) \overset{s}{\to} < b_i > \to 1$$

which splits uniquely up to conjugation, defining thus a single conjugacy class $\tilde{B}_i$ above $B_i$ the elements of which have the same order as those of $B_i, i = 1, ..., n$. Let us show the $n$-tuple $\tilde{\mathbf{B}} = (\tilde{B}_1, ..., \tilde{B}_n)$ works. For any $1 \leq i \neq j \leq n$ let $b_i \in B_i$, $b_j \in B_j$ such that $b_ib_j = b_jb_i$ so, in particular $< b_i, b_j > \simeq < b_i > \times < b_j >$. Once again Schur-Zassenhauss lemma implies the short exact sequence

$$1 \to \ker(s) \to s^{-1}(< b_i, b_j >) \overset{s}{\to} < b_i, b_j > \to 1$$

splits uniquely up to conjugation and, in particular that, for any section $\sigma$ of $s$ we have $\sigma(b_i)\sigma(b_j) = \sigma(b_j)\sigma(b_i)$ with $\sigma(b_i) \in \tilde{B}_i$, $\sigma(b_j) \in \tilde{B}_j$. This proves (1) and (2) is straightforward since $n = 1$.

### *3.3. Proof of lemma 3.1*

We proceed in two steps:

*3.3.1. First step* For $i = 1, ..., 2s$, set

$$\mathcal{B}^i_{1,2s} = \left\{ Q_1^{2\alpha_1+1} Q_2^{2\alpha_2+1} ... Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} ... Q_2^{2\beta_2+1} Q_1^{2\beta_1+1} \right\}_{\substack{\alpha_1,...,\alpha_{i-1} \in \mathbb{Z} \\ \beta_1,...,\beta_{i-1} \in \mathbb{Z} \\ \gamma_i \in \mathbb{Z} - \{0\}}}$$

and $\mathcal{B}_{1,2s} := \bigcup_{i=1}^{2s} \mathcal{B}^i_{1,2s}$. Then $\mathcal{B}_{1,2s}$ is contained in $\Pi_{1,2s}$. Indeed, each of the $\mathcal{B}^i_{1,2s}$, $i = 1, ..., 2s$ is. For $i = 1$, this is obvious. For $2 \leq i \leq 2s$, this results from the following equality: for any $\alpha_1, ..., \alpha_{i-1} \in \mathbb{Z}$, $\beta_1, ..., \beta_{i-1} \in \mathbb{Z}$, $\gamma_i \in \mathbb{Z} - \{0\}$

$$a_{1,2}^{\alpha_2} a_{1,3}^{\alpha_3} ... a_{1,i-1}^{\alpha_{i-1}} a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1} ... a_{1,3}^{\beta_3+1} a_{1,2}^{\beta_2+1} = Q_1^{2\alpha_1+1} Q_2^{2\alpha_2+1} ... Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} \\ ... Q_2^{2\beta_2+1} Q_1^{2\beta_1+1}$$

one can check computing “from the center”, *i.e.*:

$$\begin{aligned}
a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1} &= Q_1 \ldots Q_{i-1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+2-1} Q_{i-2}^{-1} \cdots Q_1^{-1} \\
a_{1,i-1}^{\alpha_{i-1}} (a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1}) &= a_{1,i-1}^{\alpha_{i-1}} Q_1 \ldots Q_{i-1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{-1} \cdots Q_1^{-1} \\
&= Q_1 \ldots Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} \\
&\quad Q_{i-2}^{-1} \cdots Q_1^{-1} \\
(a_{1,i-1}^{\alpha_{i-1}} (a_{1,i}^{\gamma_i} a_{1,i-1}^{\beta_{i-1}+1})) a_{1,i-2}^{\beta_{i-2}+1} &= Q_1 \ldots Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} \\
&\quad Q_{i-2}^{-1} \cdots Q_1^{-1} a_{1,i-2}^{\beta_{i-2}+1} \\
&= Q_1 \ldots Q_{i-2} Q_{i-1}^{2\alpha_{i-1}+1} Q_i^{2\gamma_i} Q_{i-1}^{2\beta_{i-1}+1} Q_{i-2}^{2\beta_{i-2}+2-1} \\
&\quad Q_{i-3}^{-1} \cdots Q_1^{-1} \\
etc. &\quad \ldots
\end{aligned}$$

*3.3.2. Second step* We use now elements of $\mathcal{B}_{1,2s}$ to build $u_k$, $v_{\underline{i},k}$ et $w_{k,\underline{i}}$. Set $\alpha_k := Q_{2k-2} Q_{2k-1}^2 Q_{2k-2}$, $k = 2, ..., s$ and note that

$$\begin{aligned}
&\alpha_k.(h_1, ..., h_{2k-3}, g, g_k, g_k^{-1}, h_{2k+1}, ..., h_{2s}) \\
&\quad = (h_1, ..., h_{2k-3}, g, g_k^g, (g_k^g)^{-1}, h_{2k+1}, ..., h_{2s})
\end{aligned}$$

(1) Construction of $\mathbf{u_k}$:

Set $\beta_k := Q_{2k-3} ... Q_1$, $k = 2, ..., s$, then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$,

-$\beta_2 \cdot \mathbf{g} = (g_1^{-1}, g_1, [g_2, ..., g_s])$.

-$\beta_3 \cdot \mathbf{g} = (g_1^{-1}, g_2^{g_1}, (g_2^{g_1})^{-1}, g_1, [g_3, ..., g_s])$.

-By induction, observing that $\beta_{k+1} = Q_{2k-1} Q_{2k-2} \beta_k$, $k \geq 1$, conclude that

$$\beta_k \cdot \mathbf{g} = (g_1^{-1}, [g_2^{g_1}, ..., g_{k-1}^{g_1}], g_1, [g_k, ..., g_s])$$

So, setting $u_k = \beta_k^{-1} \alpha_k \beta_k \in \mathcal{B}_{1,2s}$, one gets :

$$\begin{aligned}
u_k \cdot \mathbf{g} &= \beta_k^{-1} \cdot (\alpha_k \cdot (g_1^{-1}, [g_2^{g_1}, \ldots, g_{k-1}^{g_1}], g_1, [g_k, \ldots, g_s]) \\
&= \beta_k^{-1} \cdot (g_1^{-1}, [g_2^{g_1}, \ldots, g_{k-1}^{g_1}], g_1, [g_k^{g_1}, \ldots, g_s]) \\
&= \beta_k^{-1} \cdot (\beta_k \cdot [g_1, g_2, \ldots, g_{k-1}, g_k^{g_1}, g_{k+1}, \ldots, g_{2s}]) \\
&= [g_1, g_2, \ldots, g_{k-1}, g_k^{g_1}, g_{k+1}, \ldots, g_{2s}]
\end{aligned}$$

In the following, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\gamma(\underline{i}, j) = g_1^{g_{i_j} \cdots g_{i_1}}$, $j = 1, ..., r$.

(2) Construction of $\mathbf{v}_{\underline{\mathbf{i}},\mathbf{k}}$:

In this section, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\mathbf{g}_{\underline{i},0} = [g_2^{g_1}, ..., g_{i_1-1}^{g_1}]$ and $\mathbf{g}_{\underline{i},j} = [g_{i_j+1}^{\gamma(\underline{i},j)}, ..., g_{i_{j+1}-1}^{\gamma(\underline{i},j)}]$, $j = 1, ..., r$.

For any $1 \leq i < j \leq s$, write $\gamma_{i<j} := Q_{2j-1}^{-1} Q_{2j-2} \cdots Q_{2i}$, which acts this way:

$$\begin{aligned}&\gamma_{i<j}.(h_1, \ldots, h_{2i-1}, g, [g_{i+1}, \ldots, g_j], h_{2j+1}, \ldots, h_{2s})\\ &\quad = (h_1, \ldots, h_{2i-1}, [g_{i+1}^g, \ldots, g_{j-1}^g], g_j^g, g_j^{-1}, g^{g_j}, h_{2j+1}, \ldots, h_{2s})\end{aligned}$$

and for any $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ set $\gamma_{\underline{i}}^{(1)} := \gamma_{i_{r-1}<i_r} \circ \cdots \circ \gamma_{i_1<i_2} \circ \gamma_{1<i_1} \circ Q_1$. Then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$:

- For any $1 < i_1 \leq s$, $\gamma_{(i_1)}^{(1)} \cdot \mathbf{g} = \gamma_{1<i_1} \cdot \mathbf{g} = (g_1^{-1}, [g_2^{g_1}, ..., g_{i_1-1}^{g_1}], g_{i_1}^{g_1}, g_{i_1}^{-1}, g_1^{g_{i_1}}, [g_{i_1+1}, ..., g_s])$.
- By induction, observing that $\gamma_{(\underline{i},i_{r+1})}^{(1)} = \gamma_{i_r<i_{r+1}} \gamma_{\underline{i}}^{(1)}$, $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r < s$, $i_r < i_{r+1} < s$, $r \geq 1$, conclude that

$$\begin{aligned}\gamma_{\underline{i}}^{(1)} \cdot \mathbf{g} = (&g_1^{-1}, \mathbf{g}_{\underline{i},0}, g_{i_1}^{g_1}, g_{i_1}^{-1}, \mathbf{g}_{\underline{i},1}, ..., g_{i_{r-1}}^{\gamma(\underline{i},r-2)}, g_{i_{r-1}}^{-1}, \mathbf{g}_{\underline{i},r-1}, g_{i_r}^{\gamma(\underline{i},r-1)}, g_{i_r}^{-1},\\ &\gamma(\underline{i}, r), [g_{i_r+1}, ..., g_s])\end{aligned}$$

Finally, given $\underline{i} = (i_1, ..., i_r)$, $k$ with $1 < i_1 < ... < i_r < k \leq s$ write $\gamma_{\underline{i},k}^{(2)} := Q_{2k-3} \ldots Q_{2i_r}.\gamma_{\underline{i}}^{(1)}$ and compute

$$\begin{aligned}\gamma_{\underline{i},k}^{(2)} \cdot \mathbf{g} = (&g_1^{-1}, \mathbf{g}_{\underline{i},0}, g_{i_1}^{g_1}, g_{i_1}^{-1}, \mathbf{g}_{\underline{i},1}, ..., \mathbf{g}_{\underline{i},r-1}, g_{i_r}^{\mathbf{g}(\underline{i},r-1)}, g_{i_r}^{-1}, [g_{i_r+1}^{\mathbf{g}(\underline{i},r)}, ..., g_{k-1}^{\mathbf{g}(\underline{i},r)}], \mathbf{g}\\ &(\underline{i}, r), [g_k, ..., g_s])\end{aligned}$$

So, setting

$$v_{\underline{i},k} = (\gamma_{\underline{i},k}^{(2)})^{-1} \alpha_k \gamma_{\underline{i},k}^{(2)} \in \mathcal{B}_{1,2s}$$

for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$ one gets:

$$\begin{aligned}v_{\underline{i},k} \cdot \mathbf{g} &= (\gamma_{\underline{i},k}^{(2)})^{-1} \gamma_{\underline{i},k}^{(2)} \cdot [g_1, \ldots, g_{k-1}, g_k^{g_1^{g_{i_r} \cdots g_{i_1}}}, g_{k+1}, \ldots, g_s]\\ &= [g_1, \ldots, g_{k-1}, g_k^{g_1^{g_{i_r} \cdots g_{i_1}}}, g_{k+1}, \ldots, g_s]\end{aligned}$$

(3) Construction of $\mathbf{w}_{\mathbf{k},\underline{\mathbf{i}}}$:

In this section, given $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ and $\mathbf{g} = [g_1, ..., g_s] \in \overline{\mathrm{hm}}(\mathbf{C})$, we will write $\mathbf{g}_{\underline{i},0} == [g_2^{\gamma(\underline{i},r)^{-1}}, ..., g_{i_1-1}^{\gamma(\underline{i},r)^{-1}}]$ and $\mathbf{g}_{\underline{i},j} = [g_{i_j+1}^{\gamma(\underline{i},r)^{-1}}, ..., g_{i_{j+1}-1}^{\gamma(\underline{i},r)^{-1}}]$, $j = 1, ..., r$.

For any $2 \leq i < j \leq s$, write $\delta_{i<j} := Q_{2j-3}^{-1} \cdots Q_{2i-1}^{-1} Q_{2i-2}$, which acts this way:

$$\begin{aligned} &S_{i<j} \cdot (h_i, \dots, h_{zi-3}, g, [g_i, \dots, g_{j-1}], h_{2j+1}, \dots, h_{2s}) \\ &= (h_i, \dots, h_{2i-3}, gi^g, gi^{-1}, [g_{i+1}, \dots, g_{j-1}], g^{gi}, h_{2j+1}, \dots, h_{2s}) \end{aligned}$$

and for any $\underline{i} = (i_1, ..., i_r)$ with $1 < i_1 < ... < i_r \leq s$ set $\delta_{\underline{i}}^{(1)} := \delta_{i_r < i_r+1} \circ \delta_{i_{r-1}<i_r} \circ \cdots \circ \delta_{i_1<i_2} \circ \delta_{1<i_1} \circ Q_1$. Then, for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$:

$$\begin{aligned} \delta_{\underline{i}}^{(1)} \cdot \mathbf{g} = (&g_1^{-1}, [g_2, \dots, g_{i_1-1}], g_{i_1}^{g_1}, g_{i_1}^{-1}, [g_{i_1+1}, \dots, g_{i_2-1}], \dots, \\ &g_{i_{r-1}}^{\gamma(\underline{i},r-2)}, g_{i_{r-1}}^{-1}, [g_{i_{r-1}+1}, \dots, g_{i_r-1}], \\ &g_{i_r}^{\gamma(\underline{i},r-1)}, g_{i_r}^{-1}, \gamma(\underline{i}, r-1), [g_{i_r+1}, \dots, g_s]) \end{aligned}$$

Next, set $\delta_{\underline{i}}^{(2)} := Q_1^{-1} \cdots Q_{2i_r-1}^{-1} \cdot \delta_{\underline{i}}^{(1)} \in \mathcal{B}_{2s}$ and compute

$$\begin{aligned} \delta_{\underline{i}}^{(2)} \cdot \mathbf{g} = (&\gamma(\underline{i}, r), (g_1^{-1})^{\gamma(\underline{i},r)^{-1}}, \mathbf{g}_{\underline{i},0}, (g_{i_1}^{g_1})^{\gamma(\underline{i},r)^{-1}}, (g_{i_1}^{-1})^{\gamma(\underline{i},r)^{-1}}, \mathbf{g}_{\underline{i},1}, \dots, \\ &(g_{i_{r-1}}^{\gamma(\underline{i},r-2)})^{\gamma(\underline{i},r)^{-1}}, (g_{i_{r-1}}^{-1})^{\gamma(\underline{i},r)^{-1}}, \\ &\mathbf{g}_{\underline{i},r-1}, (g_{i_r}^{\gamma(\underline{i},r-1)})^{\gamma(\underline{i},r)^{-1}}, (g_{i_r}^{-1})^{\gamma(\underline{i},r)^{-1}}, [g_{i_r+1}, \dots, g_s]) \end{aligned}$$

Finally, given $\underline{i} = (i_1, ..., i_r)$, $k$ with $1 < k < i_1 < ... < i_r \leq s$ write $\delta_{k,\underline{i}}^{(3)} := e_{\underline{i}} \alpha_{i_r} e_{k,i_r}$ where

$$\begin{cases} e_{\underline{i}} &= Q_1 \cdots Q_{2i_1-3} Q_{2i_1-2}^{-1} Q_{2i_1-1} \cdots Q_{2i_{r-1}-3} \\ &\quad Q_{2i_{r-1}-2}^{-1} Q_{2i_{r-1}-1} \cdots Q_{2i_r-3} \\ e_{k,i_r} &= Q_{2i_r-3} \cdots Q_{2k} Q_{2k-1}^{-1} Q_{2k-2}^{-1} Q_{2k-3} \cdots Q_1 \end{cases}$$

then, $\delta_{k,\underline{i}}^{(3)} \in \mathcal{B}_{2s}$, which entails $w_{k,\underline{i}}^0 := \delta_{k,\underline{i}}^{(3)} \cdot \delta_{\underline{i}}^{(2)} \in \Pi_{1,2s}$ and for any $\mathbf{g} = [g_1, ..., g_s] \in \overline{\text{hm}}(\mathbf{C})$ one gets

$$w_{k,\underline{i}}^0 \cdot \mathbf{g} = [g_1, ..., g_{k-1}, g_k^{(g_1^{-1})^{g_{i_r} \cdots g_{i_1}}}, g_{k+1}, ..., g_s]$$

As a result, $w_{k,\underline{i}} = (w_{k,\underline{i}}^0)^{|<g_1>|-1} \in \Pi_{1,2s}$ works. Note that, this is the only step in the proof of lemma 3.1 where we use the assumption $G$ is finite. Actually, parts (1) and (2) of lemma 3.1 remain true without this assumption and part (3) only requires $g_1$ to be of finite order.

## 4. The regular inverse Galois problem with fixed branch points

### *4.1. General strategy*

*4.1.1. For a finite group* We would like now to apply theorem 2.3 to the regular inverse Galois problem with fixed branch points. Consider a field $Q$ of characteristic 0, a finite group $G$, a symmetric $2s$-tuple $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$ and suppose that (**C**1) and (**C**2) from theorem 2.3 are satisfied that is, there exists $1 \leq l \leq 2s$ such that all the HM representatives of $\overline{\mathrm{sni}}(\mathbf{C})$ fall in one single $SH_{2s}$-orbit $O^{HM}(\mathbf{C})$ and $\Pi_{l,2s}$ acts transitively on this orbit. Then, $\mathrm{HM}'(\mathbf{C})$ (resp. $\mathrm{HM}(\mathbf{C})$) is a geometrically irreducible variety defined over $Q'_{\mathbf{C}}$ (resp. over $Q_{\mathbf{C}}$) and for any $\mathbf{t}'_{l+1,2s} \in \mathcal{U}^{2s-l+1}(\overline{Q})$, the HM-subvariety $\mathrm{HM}'(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$ (resp. the symmetrised HM-subvariety $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$) is a smooth geometrically irreducible variety of dimension $l$ defined over the finite extension $Q'_{\mathbf{C}}(\mathbf{t}'_{l+1,2s})/Q$ (resp. the finite extension $Q(\mathbf{C}, \mathbf{t}'_{l+1,2s})/Q$). So the problem is reduced to studying the rational points of a smooth geometrically irreducible variety $V$ of dimension $l$ defined over a finite extension $k_0/Q$.

This situation is particularly adapted to the *Local-global principle* [Mo89], [GPR97]. Let $Q$ be a global field and $\Sigma$ a nonempty finite set of places. Denote by $Q^{\Sigma}/Q$ the maximal extension of $Q$ in a separable closure $Q^s/Q$ which is totally split at each $v \in \Sigma$. The local-global principle for varieties states that, for any smooth geometrically irreducible $Q^{\Sigma}$-variety $V$, if $V(Q_v) \neq \emptyset$ for each embedding $Q^{\Sigma} \hookrightarrow Q_v$ and each $v \in \Sigma$ then $V(Q^{\Sigma}) \neq \emptyset$. This applies in particular to $Q = \mathbb{Q}$ and $\Sigma = \{p\}$, where $p$ is a prime number (resp. $\infty$) that is, $Q_p = \mathbb{Q}_p$, $Q^{\Sigma} = \mathbb{Q}^{tp}$ (resp. $Q_{\infty} = \mathbb{R}$, $Q^{\Sigma} = \mathbb{Q}^{tr}$).

So, using the modular interpretation of Hurwitz spaces we can state, for instance:

**Proposition 4.1.** *Fix a finite group $G$, a symmetric $2s$-tuple $\mathbf{C} = [C_1, ..., C_s] \in \mathcal{C}_{2s}(G)$ and an integer $1 \leq l \leq 2s$. Let $Q$ be a global field and $\Sigma$ a nonempty finite set of places. Assume*

**(Trans)** *All the HM representatives fall in one single $SH_{2s}$ -orbit$O^{HM}(\mathbf{C})$ and $\Pi_{l,2s}$ acts transitively on this orbit.*

**(LocReal)** *There exists a tuple $\mathbf{t}'_{\Sigma,l+1,2s} \in \mathcal{U}^{2s-l}(\overline{Q})$ such that $Q(\mathbf{C}, \mathbf{t}'_{\Sigma,l+1,2s}) \subset Q$ and, for each $v \in \Sigma$, there exists a HM G-cover $f$ defined over $Q_v$ with invariants $G$, $\mathbf{C}(\mathbf{t}'_f, \mathbf{t}'_{\Sigma,l+1,2s})$ (where $\mathbf{t}_f \in \mathcal{U}_l(Q_v)$ depends on $f$).*

*Then there exists a HM G-cover $f$ defined over $Q^{\Sigma}$ with invariants $G, \mathbf{C}$ and branch points $(\mathbf{t}'_f, \mathbf{t}'_{\Sigma,l+1,2s})$ (where $\mathbf{t}_f \in \mathcal{U}_l(Q^{\Sigma})$ depends on $f$).*

*Proof.* In terms of Hurwitz spaces, condition **(Trans)** implies that $\mathrm{HM}(\mathbf{C})$ is a geometrically irreducible variety defined over $Q$ and that for any $\mathbf{t}'_{l+1,2s} \in \mathcal{U}^{2s-l}(\overline{Q})$,

$\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{l+1,2s}}$ remains geometrically irreducible. Furthermore, according to condition **(LocReal)**, there exists $\mathbf{t}'_{\Sigma,l+1,2s} \in \mathcal{U}^{2s-l}(\overline{Q})$ such that $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(Q_v)^{noob} \neq \emptyset$, $v \in \Sigma$ with $Q(\mathbf{C}, \mathbf{t}'_{\Sigma,l+1,2s}) \subset Q$. So, since $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ is smooth, geometrically irreducible and defined over $Q$, the local-global principle entails that $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(Q^{\Sigma}) \neq \emptyset$, which is the expected conclusion when, for instance, $Z(G) = \{1\}$. Else, the local-global principle should be applied to the global descent variety $D^{HM}_{\mathbf{t}'_{\Sigma,l+1,2s}}$ [DDoMo04] associated with $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ instead of $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}$ itself. Indeed, one has $D^{HM}_{\mathbf{t}'_{\Sigma,l+1,2s}}(Q_v) \neq \emptyset$, $v \in \Sigma$. Since $D^{HM}_{\mathbf{t}'_{\Sigma,l+1,2s}}$ is smooth geometrically irreducible and defined over $Q$, the local-global principle yields $D^{HM}_{\mathbf{t}'_{\Sigma,l+1,2s}}(Q^{\Sigma}) \neq \emptyset$ or, equivalently, $\mathrm{HM}(\mathbf{C})_{\mathbf{t}'_{\Sigma,l+1,2s}}(Q^{\Sigma})^{noob} \neq \emptyset$. □

*Remark 4.2.* Existentially closed extension analog. Recall a field $Q$ is said to be existentially closed in a regular extension $\Omega/Q$ if for any smooth geometrically irreducible $Q$-variety $V$, $V(\Omega) \neq \emptyset$ entails $V(Q) \neq \emptyset$. For instance a large field $Q$ is existentially closed in $Q((X))/Q$ [P96]. Thus, an analog of proposition 4.1 can be stated for this situation, more precisely: *Let $Q$ be a field existentially closed in a regular extension $\Omega/Q$. Fix a finite group $G$, a symmetric $2s$-tuple $\mathbf{C} = [C_1, \dots, C_s] \in \mathcal{C}_{2s}(G)$ and an integer $1 \leq l \leq 2s$. Assume* **(Trans)** *and*

**(LocReal)** *There exists aHM G-cover defined over k with invariants $G$, $\mathbf{C}$ and branch points $\mathbf{t}' \in \mathcal{U}^{2s}(\overline{Q})$ such that $Q(\mathbf{C}, \mathbf{t}'_{l+1,2s}) \subset Q$.*

*Then there exists a HM G-cover $f$ defined over $k_0$ with invariants $G$, $\mathbf{C}$ and branch points $(\mathbf{t}'_f, \mathbf{t}'_{l+1,2s})$ (where $\mathbf{t}_f \in \mathcal{U}_l(Q)$ depends on $f$).*

*4.1.2. For a projective system of finite groups* The above strategy can also be developed for a complete projective system of finite groups $(G_{k+1} \twoheadrightarrow G_k)_{k\geq 0}$. Indeed, assume there exists a projective system $(\mathbf{C}_k = [C_{k,1}, ..., C_{k,s}])_{k\geq 0}$ of symmetric tuples $\mathbf{C}_k \in \mathcal{C}_{2s_k}(G_k)$ and an integer $1 \leq l \leq 2s_0$ such that (**C1**) and (**C2**) from theorem 2.3 are satisfied at each level $k \geq 0$. Then $(\mathrm{HM}'(\mathbf{C}_{k+1}) \to \mathrm{HM}'(\mathbf{C}_k))_{k\geq 0}$ (resp. $(\mathrm{HM}(\mathbf{C}_{k+1}) \to \mathrm{HM}(\mathbf{C}_k))_{k\geq 0}$) is a tower of geometrically irreducible varieties defined over $\cup_{k\geq 0} Q'_{\mathbf{C_k}}$ (resp. over $Q$) such that for any projective system of branch points $(\mathbf{t}'_k)_{k\geq 0} \in \varprojlim \mathcal{U}^{2s_k-l}(\overline{Q})$ the corresponding tower $(\mathrm{HM}'(\mathbf{C}_{k+1})_{\mathbf{t}'_{k+1}} \to \mathrm{HM}'(\mathbf{C}_k)_{\mathbf{t}'_k})_{k\geq 0}$ (resp. symmetrised tower $(\mathrm{HM}(\mathbf{C}_{k+1})_{\mathbf{t}'_{k+1}} \to \mathrm{HM}(\mathbf{C}_k)_{\mathbf{t}'_k})_{k\geq 0}$) is a tower of geometrically irreducible $l$-dimensional varieties defined over $\cup_{k\geq 0} Q'_{\mathbf{C_k}}(\mathbf{t}'_k)$ (resp. $\cup_{k\geq 0} Q(\mathbf{C_k}, \mathbf{t}'_k)$). Theorem 4.1 of [DE03] states that, given a complete projective system of finite groups $(G_{k+1} \twoheadrightarrow G_k)_{k\geq 0}$, $(\mathbf{C}_k)_{k\geq 0}$ can always be built in such a way that (**C1**) is fulfilled for any $k \geq 0$ and that, for any henselian field $H$ of characteristic 0 with residue characteristic either $p = 0$ or $p > 0$ not dividing any of the $|G_k|$, $k \geq 0$ and containing all the prime-to-$p$ roots of 1, $\varprojlim \mathrm{HM}(\mathbf{C}_k)(H)^{noob} \neq \emptyset$. We would like to obtain the same kind of results replacing the towers of HM-components by towers of HM-subvarieties in order to apply the profinite version of proposition 4.1.

We will deal with modular towers [F95] and some towers of Hurwitz spaces associated with modular towers we call associated central towers. The end of this section is devoted to describing the construction of these objects which are the main motivation for proposition 2.7.

**a/ Modular towers:** Fix a finite group $G$ and a prime number $p$ dividing $|G|$. Consider then the universal $p$-Frattini cover of $G$, ${}_p\tilde{\phi} : {}_p\tilde{G} \to G$ (*cf.* [F95], part II). Since $\ker({}_p\tilde{\phi})$ is a free pro-$p$ group, its Frattini series, defined inductively by $\mathrm{ker_0} = \mathrm{ker}({}_\mathrm{p}\tilde{\phi})$, $\mathrm{ker_1} = \mathrm{ker}_0^\mathrm{p}[\mathrm{ker_0}, \mathrm{ker_0}], \dots , \mathrm{ker_i} = \mathrm{ker}_{\mathrm{i}-1}^\mathrm{p}[\mathrm{ker_n}, \mathrm{ker_n}], \dots$, is a fundamental system of neighbourhoods of 1. This provides a complete projective system of finite groups $({}_p^{k+1}\tilde{G} \twoheadrightarrow {}_p^k \tilde{G})_{k\geq 0}$ with ${}_p^k\tilde{G} := {}_p\tilde{G}/\mathrm{ker}_k$, $k \geq 0$ such that ${}_p\tilde{G} = \varprojlim {}_p^k\tilde{G}$. Furthermore, for any $k \geq 0$ and any $p$'-conjugacy class $C_k$ of ${}_p^k\tilde{G}$, there exists a unique conjugacy class $C_{k+1}$ of ${}_p^{k+1}\tilde{G}$ above $C_k$ with $o(C_{k+1}) = o(C_k)$ [F95, lemma 3.7]. As a result, if $G$ is $p$-perfect (that is generated by elements of prime-to-$p$ order), any tuple of $p$'-conjugacy classes $\mathbf{C}_0 = (C_{0,1}, \dots , C_{0,r}) \in \mathcal{C}_r(G)$ with $\overline{\mathrm{hm}}([\mathbf{C}_0]) \neq \emptyset$ defines a unique projective system $(\mathbf{C}_k = (C_{k,1}, \dots , C_{k,r}))_{k\geq 0}$ such that for all $k \geq 0$, $o(C_{k,i}) = o(C_{k,0})$, $i = 1, \dots , r$, $\overline{\mathrm{hm}}([\mathbf{C}_k]) \neq \emptyset$ (Frattini property) and $\mathbf{C}_k$ has the same rationality properties as $\mathbf{C}_0$[3]. The corresponding projective system of HM-varieties

$$(\mathrm{HM}'([\mathbf{C}_{k+1}]) \to \mathrm{HM}'([\mathbf{C}_k]))_{k\geq 0}$$

is called the HM-modular tower associated with the data $(G, [\mathbf{C}_0], p)$. As usual, $(\mathrm{HM}([\mathbf{C}_{k+1}]) \to \mathrm{HM}([\mathbf{C}_k]))_{k\geq 0}$ will be called the symmetrised HM-modular tower associated with the data $(G, [\mathbf{C}_0], p)$.

**b/ Associated central towers:** To a given HM-modular tower, one can associate a family of Hurwitz towers we call associated central towers. For this, recall the classical following results about universal central extensions:

- If $G$ is perfect (that is, $G = [G, G]$) then, by Schur's theorem, the universal central extension $\hat{G} \twoheadrightarrow G$ of $G$ exists; furthermore, it is finite, Frattini and its kernel is the Schur Multiplier $M(G)$ of $G$.

[3] Indeed, for any $k \geq 1$, $[{}_p^k\tilde{G} : G] = p^{r_k}$ so, for any $q \geq 1$, $q$ is prime to $|{}_p^k\tilde{G}|$ if and only if $q$ is prime to $|G|$. As a result, for any $q \geq 1$ prime to $|{}_p^k\tilde{G}|$ and for any $1 \leq j \leq r$, $C_{k,j}^q$ is the only conjugacy class above $C_j^q$ with elements of the same order as those of $C_j^q$. In particular, for any $q \geq 1$ prime to $|G|$, if $\sigma_q \in \mathcal{S}_r$ satisfies $\mathbf{C}^q = (C_{\sigma_q(1)}, \dots , C_{\sigma_q(r)})$ then $\mathbf{C}_k^q = (C_{k,\sigma_q(1)}, \dots , C_{k,\sigma_q(s)})$.

- If $G$ is $q$-perfect for some prime $q$ dividing $|G|$ then the universal central $q$-extension $\widehat{{}^qG} \twoheadrightarrow G$ of $G$ exists; furthermore, it is finite, Frattini and its kernel is the $q$-part $M(G)_q$ of the Schur Multiplier $M(G)$ of $G$ (*cf.* [BF02], §3.6).

We keep the above notation, assuming furthermore that $G$ is $q$-perfect for some prime $q \neq p$ dividing $|G|$. Denote by $\widehat{{}^q\quad}$ the functor "universal $q$-central extension" and consider the projective system $(\widehat{{}^q({}^{k+1}_{\ p}\tilde{G})} \twoheadrightarrow \widehat{{}^q({}^k_p\tilde{G})})_{k\geq 0}$. For each $k \geq 0$ let $\mathcal{A}_k$ be the set of all symmetric $2r$-tuples of conjugacy classes of $\widehat{{}^q({}^k_p\tilde{G})}$ above $[\mathbf{C}_k]$. Then $(\mathcal{A}_{k+1} \to \mathcal{A}_k)_{k\geq 0}$ is a projective system of non empty finite sets, so its projective limit is non empty. In other words, there exists a projective system $(\widehat{{}^q[\mathbf{C}_k]})_{k\geq 0}$ of symmetric g-complete $2r$-tuples of conjugacy classes above $([\mathbf{C}_k])_{k\geq 0}$. Such a system defines a tower of Hurwitz spaces covering the HM-modular tower associated with the data $(G, [\mathbf{C}], p)$ we call an associated $q$-central tower. It cannot be defined uniquely in general except if $C_{0,1}, \dots, C_{0,r}$ (and thus, $C_{k,1}, \dots, C_{k,r}$, $k \geq 0$) are also $q$'-conjugacy classes, in which case, by Schur-Zassenhauss, the associated $q$-central tower can be defined uniquely with, furthermore, the property that $\widehat{{}^q[\mathbf{C}_k]}$ has the same rationality property as $[\mathbf{C}_k]$, $k \geq 0$ and, consequently that the associated $q$-central tower is defined over the same field as the original modular tower. In general, if the original modular tower is defined over $k \subset \overline{\mathbb{Q}}$, an associated $q$-central tower is defined over a subfield of $k(\mathrm{e}^{\frac{2\pi i}{e(M(G))_q}})$ where $e(M(G))_q$ denotes the $q$-part of the exponent of the Schur multiplier $M(G)$ of $G$. Indeed, one has $e(M({}^k_p\tilde{G})|\ e({}^k_p\tilde{G})$ with $e({}^k_p\tilde{G}) = p^{r_k}e(G)$ thus $e(M({}^k_p\tilde{G}))_q = e(M(G))_q$.

If $G$ is perfect, one can carry out the same construction with the functor "universal central extension", $\widehat{\quad}$, but the resulting associated central towers are not necessarily defined over a finite extension of $k$ since $\{e(M({}^k_p\tilde{G}))\}_{k\geq 0}$ is not necessarily bounded.

Theorem 2.3 and proposition 2.3 give group-theoretical conditions to ensure the transitivity condition **(Trans)** holds. Sections 4.2 and 4.3 are devoted to prove the local realization condition **(LocReal)** for fields like $\mathbb{R}$, $\mathbb{Q}_p$. As a result we can give explicit forms of proposition 4.1 and its profinite analog: theorems 4.4 and 4.5. Theorems 1 and 2 from the introduction are special cases of these results.

## *4.2. (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) over $\mathbb{Q}^\Sigma$*

*4.2.1. G-covers over a complete field of characteristic* 0 We start with a preliminary paragraph about the regular realization of finite groups over complete fields satisfying some additional technical conditions that we will need for our construction.

Let $k$ be a complete discrete valued field of characteristic 0 and of residue characteristic $p$. The main tools to deal with G-covers over $k$ are formal geometry [H87] or rigid geometry [L95], [P94]. Given a symmetric $2s$-tuple $\mathbf{C} = [C_1, , ..., C_s] \in \mathcal{C}_{2s}(G)$, these methods provide a construction of G-covers defined over $\mathbb{Q}_p$ with invariants $G$, $\mathbf{C}$, $\mathbf{t} \in \mathcal{U}_{2s}(\mathbb{Q})$. However, it is not obvious these G-covers are HM G-covers - and, in general, they are not. For a prime $p$ not dividing $|G|$, some technical assumptions on the branch points - conditions (*) and (**) below - are necessary to ensure they are [DE03] and for primes $p$ dividing $|G|$, the problem remains open (because of the possible bad reduction of Hurwitz spaces for these primes). Suppose given $\mathbf{t} = \{x_1, y_1, ..., x_s, y_s\} \in \mathcal{U}_{2s}(k)$ and consider the conditions

$(*)$ $x_i, y_i$ lie in the same coset, $i = 1, \dots, s$ and $x_1, \dots, x_s$ lie in pairwise distinct cosets.
$(**)$ $|x_i - y_i| < |x_i - x_j||p|^{\frac{1}{p-1}}, 1 \leq i \neq j \leq s$
(with the convention $|p|^{\frac{1}{p-1}} = 1 if p = 0$).

where $a, b \in k$ lie in the same coset means that either $|a|, |b| \leq 1$ and $|a-b| < 1$ or $|a|, |b| > 1$. We will sometimes write $\zeta_n := \mathrm{e}^{\frac{2\pi i}{n}}$, $n \geq 2$ in the following.

Our purpose here is to build HM G-covers defined over $k$, with a totally $k$-rational fiber above some unramified $k$-rational point and with a $\mathbb{Q}$-rational branch point divisor or - at least - a $k_0$-rational branch point divisor where $k_0/\mathbb{Q}$ is an explicitly computable cyclotomic finite extension. If we impose for instance that $(x_1, ..., x_t) \in \mathcal{U}^t(\mathbb{Q})$ then the second part of condition (*) can't be satisfied if $t > p+1$. This difficulty can be overcome by adjoining roots of 1 to $k$; we explain precisely how below (Lemma 4.3).

The statement and proof of lemma 4.3 being rather technical, we first explain how we are going to proceed. As usual, the method consists in glueing cyclic G-covers in an appropriate way. We are going to use the rigid glueing procedure. Given four integers $n_1, n_2 \geq 2$ and $m_1, m_2 \geq 1$, for $i = 1, 2$ list the elements of $(\mathbb{Z}/n_i^{m_i}\mathbb{Z})^\star$ as $\epsilon u_{i,j}$, where $\epsilon = \pm 1$, $j = 1, \dots, \phi(n_i^{m_i})/2$ and $\phi$ is the Euler function. Consider then the two cyclic G-covers $f_i : X_i \to \mathbb{P}^1_{\mathbb{Q}}$ with group $< g_i >= \mathbb{Z}/n_i\mathbb{Z}$, inertia canonical invariant $(\{g_i^{\epsilon u_{i,j}}\}, \{g_i^{-\epsilon u_{i,j}}\})_{j=1,\dots,\phi(n_i^{m_i})/2,\ \epsilon=\pm 1}$ and branch points $\mathbf{t}^{i'} = (x^{\epsilon}_{i,j} := a_i + \zeta_{n_i^{m_i}}^{\epsilon u_{i,j}}, y^{\epsilon}_{i,j} := a_i + a + \zeta_{n_i^{m_i}}^{-\epsilon u_{i,j}})_{j=1,\dots,\phi(n_i^{m_i})/2,\ \epsilon=\pm 1}$, $i = 1, 2$ where $a \in \mathbb{Q}$ is chosen in such a way that $|a| < \min\{1, |p|^{\frac{1}{p-1}}\}$ and $a_1, a_2 \in \mathbb{Q}$ are translation terms we will specify below. Each of these two G-covers is defined over $\mathbb{Q}$ with a $\mathbb{Q}$-rational unramified point the fiber of which is totally $\mathbb{Q}$-rational [Des95] and is a HM G-cover. But to assert the G-cover obtained by glueing $f_1 \times_{\mathbb{Q}} k$ and $f_2 \times_{\mathbb{Q}} k$ will still be a HM G-cover, we have to check that $(\mathbf{t}^{1'}, \mathbf{t}^{2'})$ satisfy conditions (*) and (**) as well. This will occur for instance if $|a_1|, |a_2|, |a_1 - a_2| < 1$ provided $n_1^{m_1} \neq n_2^{m_2}$. So we just have to choose

$m_1, m_2 \geq 1$, $a_1, a_2 \in \mathbb{Q}$ this way. Given any integer $m \geq 1$, we will denote by $\mathrm{Rat}_m$ the *rationalization operator* which to each conjugacy class $C$ of a finite group $G$ associates the rational union of conjugacy classes

$$\mathrm{Rat}_m(C) := (C^{\epsilon u_i}, C^{-\epsilon u_i})_{i=1,\dots,\phi(o(C)^m)/2,\ \epsilon=\pm 1}$$

where $\{\pm u_i\}_{1\leq i\leq \phi(o(C)^m)/2} = (\mathbb{Z}/o(C)^m\mathbb{Z})^\star$. Likewise, given any tuple $\underline{m} = (m_1, \dots, m_t) \in \mathbb{N} \setminus \{0\}$, let $\mathrm{Rat}_{\underline{m}}$ be the rationalization operator which to any tuple $\mathbf{C} = (C_1, \dots, C_t) \in \mathcal{C}_t(G)$ associates the tuple

$$\mathrm{Rat}_{\underline{m}}(\mathbf{C}) := (\mathrm{Rat}_{m_1}(C_1), \dots, \mathrm{Rat}_{m_t}(C_t)).$$

We now state lemma 4.3 and give its proof, which is just a slight adjustement of the method described above.

**Lemma 4.3.** *Let $G$ be a finite group and $\mathbf{C} = (C_1, ..., C_t) \in \mathcal{C}_t(G)$ such that there exists $g_i \in C_i$, $i = 1, ..., t$ with $G =< g_1, ..., g_t >$. Assume that $p \not| \, |G|$, $k$ contains all the $o(C_1)$th roots of* 1. *Choose $\underline{m} = (m_2, ..., m_t) \in \mathbb{N} \setminus \{0\}$ such that $o(C_i)^{m_i} \neq o(C_j)^{m_j}$, $2 \leq i \neq j \leq t$ and write $r := l(\mathrm{Rat}_{\underline{m}}(C_2, ..., C_t))$. Then there exists a branch point tuple $\mathbf{t}' \in \mathcal{U}^{r+2}(\overline{\mathbb{Q}})$ satisfying conditions (*), (**) and $\mathbf{t}'_{1,2} \in \mathcal{U}^2(\mathbb{Q})$, $\mathbf{t}_{3,r+2} \in \mathcal{U}_r(\mathbb{Q})$. And, for any such branch point tuple, there exist HM G-covers defined over $k$ with invariants $G$, $([C_1], \mathrm{Rat}_{\underline{m}}(C_2, ..., C_t))$, $\mathbf{t}'$.*

*Proof.* Write $o_i := o(C_i)$ and choose $g_i \in C_i$, $i = 1, \dots, t$ such that $G =< g_1, \dots, g_t >$. Then for any $a_1, b_1 \in \mathbb{Q}$, the G-cover $f_1 : X_1 \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ with group $< g_1 >$, inertia canonical invariant $(\{g_1\}, \{g_1^{-1}\})$ and associated branch points $(x_1 := a_1, y_1 := b_1)$ is defined over $\mathbb{Q}(\zeta_{o_1})$ and has a $\mathbb{Q}(\zeta_{o_1})$-rational unramified point the fiber of which is totally $\mathbb{Q}(\zeta_{o_1})$-rational. For each $2 \leq i \leq t$, write

$$\mathrm{Rat}_{m_i}(C_i) = ((C_i^{u_{i,j}}, C_i^{-u_{i,j}})_{\epsilon=\pm 1})_{j=1,\dots,\phi(o_i^{m_i})/2}$$

Then, for any $a_i, b_i \in \mathbb{Q}$, any G-cover $f_i : X_i \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$ with group $< g_i >$, inertia canonical invariant $(\{g_i^{u_{i,j}}\}, \{g_i^{-u_{i,j}}\})_{\epsilon=\pm 1})_{1\leq j\leq \phi(o_i^{m_i})/2}$ and associated branch points $((x_{i,j}^\epsilon = a_i + \zeta_{o_i^{m_i}}^{\epsilon u_{i,j}}, y_{i,j}^\epsilon = b_i + \zeta_{o_i^{m_i}}^{-\epsilon u_{i,j}})_{\epsilon=\pm 1})_{1\leq j\leq \phi(o_i^{m_i})/2}$ is defined over $\mathbb{Q}$ and has a $\mathbb{Q}$-rational unramified point the fiber of which is totally $\mathbb{Q}$-rational. Choose furthermore $(a_i)_{1\leq i\leq t} \in \mathbb{Q}^t$ in such a way that $|a_i| < 1$ and $|a_i - a_j| < 1$, $1 \leq i \neq j \leq t$ and, given $a \in \mathbb{Q}$ such that $|a| <\min\{1, |p|^{\frac{1}{p-1}}\}$ set $b_i := a_i + a$, $i = 1, ..., t$. With $N := \prod_{2\leq i\leq t} o_i^{m_i}$, by assumption $p \not| N$ and, from this, one easily checks condition (*) and (**) are both fulfilled by $\mathbf{t}' := ((x_1, y_1), ((x_{i,j}^\epsilon, y_{i,j}^\epsilon)_{j=1,\dots,\phi(o_i^{m_i})/2})_{t_0+1\leq i\leq t,\ \epsilon=\pm 1})$. Condition (**) allows us to glue together - via rigid geometry - the G-covers $f_1 \times_{\mathbb{Q}(\zeta_{o_1})} k$ and $(f_i \times_{\mathbb{Q}} k)_{2\leq i\leq t}$ to get a G-cover $f : X \to \mathbb{P}^1_k$ defined over $k$ with group $G$, inertia canonical invariant $([C_1], \mathrm{Rat}_{\underline{m}}(C_2, ..., C_t))$ and branch points $\mathbf{t}'$. Condition (*) combined with [DE03, proposition 2.3, theorem 1.4], shows that the G-cover $f : X \to \mathbb{P}^1_k$ is actually a HM-cover. □

*4.2.2. Results* To avoid rationality problems, we only deal, in this section, with fields containing enough roots of 1 and HM-curves. The following statements and proofs can be adjusted for fields without roots of 1 and to HM-subvarieties of arbitrary dimensions. We refer to §4.4.2.3. of [C04b] for details about this matter.

**Theorem 4.4.** *Let $G$ be a finite group containing $n+1$ conjugacy classes $A$, $\mathbf{B} = (B_1, \dots, B_n)$ such that $\mathbf{A} = (A)$, $\mathbf{B}$ satisfy* (**H**1) *and* (**H**2) *from theorem 2.3. Set $k_A := \mathbb{Q}(\zeta_{o(A)})$ and write*

$$\mathbf{C}_s := ([A], \mathrm{Rat}_{\underline{m}}(\mathbf{B}^s)) \quad r_s := l(\mathbf{C}_s)$$

*where $\underline{m} = (m_1, \dots, m_{ns}) \in \mathbb{N} \setminus \{0\}^{ns}$ is any tuple such that $o(B_i)^{m_{i+kn}} \neq o(B_j)^{m_{j+ln}}$, $(i,k) \neq (j,l)$, $0 \leq i, j \leq n$, $1 \leq k, l \leq s-1$. Then, for $s$ large enough, $\mathrm{HM}'(\mathbf{C}_s)$ is a geometrically irreducible variety and, for any $\mathbf{t}' \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$ the HM-curve $\mathrm{HM}'(\mathbf{C}_s)_{\mathbf{t}'}$ remains geometrically irreducible. Furthermore, for any finite set $\Sigma$ of (non archimedean) places of $k_A$ of residue characteristic not dividing $|G|$, there exists $\mathbf{t}'_\Sigma \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$ with $\mathbf{t}_\Sigma \in \mathcal{U}_{r_s-1}(\mathbb{Q})$ and such that the corresponding symmetrised HM-curve $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ is defined over $k_A$ with the property that*

$$\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}(k_A^\Sigma)^{noob} \neq \emptyset$$

*Proof.* According to theorem 2.3, for $s$ large enough $\mathbf{C}_s$ satisfies condition (**Trans**) of proposition 4.1 (since $([\mathbf{A}], [\mathbf{B}]^s)$ already does) so we are only left to check condition (**LocReal**). Writing $\Sigma \cap \mathbb{Q} = \{p_1, \dots, p_r\}$, re-use the notation of lemma 4.3 and take for instance $a_i = (p_1 \cdots p_r)^i$, $i = 1, \dots, ns+1$, $a := (p_1 \cdots p_r)^n$ with $n >\max\{\frac{1}{p_i - 1}\}_{1 \leq i \leq r}$. These satisfy the conditions $|a_i|_p < 1$, $|a_i - a_j|_p < 1$ and $|a|_p < |p|^{\frac{1}{p-1}}$ for all $p \in \Sigma$, $1 \leq i \neq j \leq ns+1$. Set

$$\begin{cases} x_1 := a_1 \\ y_1 := a_1 + a \end{cases} \quad \text{and } \mathbf{t}'_1 := (x_1, y_1)$$

$$\begin{cases} x^\epsilon_{i+kn,j} := & a_{i+kn,j} + \zeta_{o(B_i)^{m_i}}^{\epsilon u_{i+kn,j}} \\ y^\epsilon_{i+kn,j} := & a_{i+kn,j} + a + \zeta_{o(B_i)^{m_i}}^{-\epsilon u_{i+kn,j}} \end{cases}$$

for $\epsilon = \pm 1$, $j = 1, \dots, \phi(o(B_i)^{m_i + kn})/2$, $1 \leq i \leq n$, $1 \leq k \leq s-1$ and

$$\mathbf{t}'_{k+1} := ((x^\epsilon_{i+kn,j}, y^\epsilon_{i+kn,j})_{\epsilon = \pm 1})_{\substack{j=1,\dots,\phi(o(B_i)^{m_i+kn})/2 \\ i=1,\dots,n}}, \qquad \text{for } 1 \leq k \leq s-1.$$

Then, writing $\mathbf{t}'_\Sigma := (\mathbf{t}'_1, (\mathbf{t}'_{k+1})_{1 \leq k \leq s-1})$ conclude thanks to lemma 4.3 that for each $v \in \Sigma$, there exists a HM-G-cover defined over $(k_A)_v$ with invariants $G$, $\mathbf{C}_s$, $\mathbf{t}'$ with $\mathbf{t}'_{2,r_s} = \mathbf{t}'_\Sigma$ that is, $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}((k_A)_v)^{noob} \neq \emptyset$. By the branch cycle argument, $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_\Sigma}$ is defined over $k_A$. Thus, as in the proof of proposition 4.1 applying the local-global principle to the global descent variety yields the announced result. □

In terms of G-covers, theorem 4.4 means that for $s$ large enough there exist HM-G-covers $f$ defined over $k_A^{\Sigma}$, with invariants $G$, $\mathbf{C}_s$, $\mathbf{t}_f$ where $\mathbf{t}_f$ can be written $\mathbf{t}_f = \{t_{1,f}\} + \mathbf{t}_{\Sigma}$ with $\mathbf{t}_{\Sigma} \in \mathcal{U}_{r_s-1}(\mathbb{Q})$. For instance, take for $G$ any group of section 2.4.2 (1), (2), (3).

Combining proposition 2.7 and the constructions of section 4.1.2 yields the following profinite version of theorem 4.4

**Theorem 4.5.** *Let $G$ be a finite group and $p$ a prime number dividing $|G|$. Assume $G$ contains $n+1$ $p$'-conjugacy classes $A$, $\mathbf{B} = (B_1, \dots, B_n)$ such that $\mathbf{A} = (A)$, $\mathbf{B}$ satisfy $(\mathbf{H}1.1^+)$, $(\mathbf{H}1.2^+)$ and $(\mathbf{H}2)$ from proposition 2.7 (for instance, assume $G$, $A$, $\mathbf{B}$ satisfy conditions (i), (ii) and (iii) of corollary 2.4). Set $k_A := \mathbb{Q}(\zeta_{o(A)})$ and write*

$$\mathbf{C}_s := ([A], \mathrm{Rat}_{\underline{m}}(\mathbf{B}^s)) \quad r_s := l(\mathbf{C}_s)$$

*where $\underline{m} = (m_1, \dots, m_{ns}) \in \mathbb{N} \setminus \{0\}^{ns}$ is such that $o(B_i)^{m_{i+kn}} \neq o(B_j)^{m_{j+ln}}$, $(i,k) \neq (j,l)$, $0 \leq i, j \leq n$, $1 \leq k, l \leq s-1$. Then, for $s$ large enough, the HM-modular tower $(\mathrm{HM}'(\mathbf{C}_{k+1,s}) \to \mathrm{HM}'(\mathbf{C}_{\underline{k,s}}))_{k \geq 0}$ is a tower of geometrically irreducible varieties and, for any $\mathbf{t}' \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$, $(\mathrm{HM}'(\mathbf{C}_{k+1,s})_{\mathbf{t}'} \to \mathrm{HM}'(\mathbf{C}_{k,s})_{\mathbf{t}'})_{k \geq 0}$ is a tower of HM-curves which are still geometrically irreducible. Furthermore, for any finite set $\Sigma$ of (non archimedean) places of $k_A$ of residue characteristic not dividing $|G|$, there exists $\mathbf{t}'_{\Sigma} \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$ with $\mathbf{t}_{\Sigma} \in \mathcal{U}_{r_s-1}(\mathbb{Q})$ and such that the corresponding tower of symmetrised HM-curves $(\mathrm{HM}'(\mathbf{C}_{k+1,s})_{\mathbf{t}'_{\Sigma}} \to \mathrm{HM}'(\mathbf{C}_{k,s})_{\mathbf{t}'_{\Sigma}})_{k \geq 0}$ is defined over $k_A$ with the property that*

$$\varprojlim HM'(\mathbf{C}_{k,s})_{\mathbf{t}'_{\Sigma}}((k_A)_v)^{noob} \neq \emptyset, \;\; v \in \Sigma$$

*and*

$$HM'(\mathbf{C}_{k,s})_{\mathbf{t}'_{\Sigma}}(k_A^{\Sigma})^{noob} \neq \emptyset, \qquad k \geq 0.$$

*This conclusion still holds (with the same $s$ and $\mathbf{t}'_{\Sigma}$) for any associated $q$-central tower (for primes $q \neq p$ dividing $|G|$ and such that $G$ is $q$ perfect) replacing $e(G)$ by $e(G)e(G)_q$.*

*Proof.* According to proposition 2.7, for $s$ large enough and for all $k \geq 0$, $\mathbf{C}_{k,s}$ (resp. $\widehat{{}^q\mathbf{C}_{k,s}}$) satisfies $(\mathbf{C}1)$, $(\mathbf{C}2)$ that is, $\mathrm{HM}(\mathbf{C}_{k,s})_{\mathbf{t}'_{\Sigma}}$ (resp. $\mathrm{HM}(\widehat{{}^q\mathbf{C}_{k,s}})_{\mathbf{t}'_{\Sigma}}$) is a geometrically irreducible HM-curve. Consider the $\mathbf{t}' \in \mathcal{U}^{r_s}(\mathbb{Q})$, $\mathbf{t}'_{\Sigma} \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$ built in the proof of theorem 4.4. Then, for any $v \in \Sigma$, $\mathrm{HM}(\mathbf{C}_{k,s})_{\mathbf{t}'}\ ((k_A)_v)^{noob} \neq \emptyset$ (resp. $\mathrm{HM}(\widehat{{}^q\mathbf{C}_{k,s}})_{\mathbf{t}'}((k_A)_v)^{noob} \neq \emptyset$) and, these sets being finite, their inverse limit is non-empty. The second part of the conclusion is obtained, once again, using the local-global principle and the global descent varieties. □

In terms of G-covers, theorem 4.5 means that for $s$ large enough and for all $k \geq 0$ there exist HM-G-covers $f_k$ defined over $k_A^{\Sigma}$, with invariants ${}_p^k\tilde{G}$, $\mathbf{C}_{k,s}$, $\mathbf{t}_{f_k}$ where $\mathbf{t}_{f_k}$ can be written $\mathbf{t}_{f_k} = \{t_{1,f_k}\} + \mathbf{t}_{\Sigma}$ with $\mathbf{t}_{\Sigma} \in \mathcal{U}_{r_s-1}(\mathbb{Q})$.

*Example 4.6.* Let us consider for instance $M_{11}$ (*cf.* section 2.4.2 (2)). Take $\mathbf{A} = (8A), \mathbf{B} = (11A)$ and, with the notation of theorem 4.5, let $(\mathcal{H}_{k+1,s} \rightarrow \mathcal{H}_{k,s})_{k \geq 0}$ be the HM-modular tower associated with the data $(M_{11}, \mathbf{C}_s, 3)$ and write $\mathcal{C}_{k,s,\Sigma} := (\mathcal{H}_{k,s})_{\mathbf{t}'_\Sigma}$, $k \geq 0$ for the resulting symmetrised HM-curves. Since 5 does not divide 8, 11, by Schur-Zassenhauss, there exists a unique conjugacy class $\widehat{{}^5(8A)_k}$ (resp. $\widehat{{}^5(11A)_k}$) lifting $(8A)_k$ (resp. $(11A)_k$) in $\widehat{{}^5\,{}^k_p\tilde{G}}$ with $o(\widehat{{}^5(8A)_k}) = 8$ (resp. $o(\widehat{{}^5(11A)_k}) = 11$). This defines uniquely an associated 5-central tower $(\widehat{{}^5\mathcal{H}}_{k+1,s} \rightarrow \widehat{{}^5\mathcal{H}}_{k,s})_{k \geq 0}$ defined over the same field $k := \mathbb{Q}(i\sqrt{2})$ as $(\mathcal{H}_{k+1,s} \rightarrow \mathcal{H}_{k,s})_{k \geq 0}$; write $\widehat{{}^5\mathcal{C}}_{k,s,\Sigma} := (\widehat{{}^5\mathcal{H}}_{k,s})_{\mathbf{t}'_\Sigma}$, $k \geq 0$ for the resulting curves. The following commutative diagram defined over $k$ summarizes the situation

$$\begin{tikzcd}
& \widehat{{}^5\mathcal{C}}_{k,s,\Sigma} \arrow[r, hook] \arrow[dl] \arrow[dd] & \widehat{{}^5\mathcal{H}}_{k+1,s} \arrow[dl] \arrow[dd] \\
\mathcal{C}_{k+1,s,\Sigma} \arrow[r, hook] \arrow[dd] & \mathcal{H}_{k+1,s} \arrow[dd] & \\
& \widehat{{}^5\mathcal{C}}_{k,s,\Sigma} \arrow[r, hook] \arrow[dl] & \widehat{{}^5\mathcal{H}}_{k,s} \arrow[dl] \\
\mathcal{C}_{k,s,\Sigma} \arrow[r, hook] & \mathcal{H}_{k,s} &
\end{tikzcd}$$

Theorem 4.5 then means that the non obstruction locus of the left side of this diagram carries (double) projective systems of $k_P$-points for each $P \in \Sigma$ and that $\mathcal{C}_{k,s,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $\widehat{{}^5\mathcal{C}}_{k,s,\Sigma}(k^\Sigma)^{noob} \neq \emptyset$, $k \geq 0$.

### *4.3. (RIGP/$\mathbf{t}_2 \subset \mathbf{t}$) over $\mathbb{Q}^{tr}$*

*4.3.1. G-covers defined over* $\mathbb{R}$ We first recall succinctly the description of G-covers defined over $\mathbb{R}$ with prescribed invariants given in [DF94]. We will use it in the next paragraph.

Let $\mathbf{t}' \in \mathcal{U}^r(\overline{\mathbb{Q}})$ be an $r$-tuple consisting of $r = r_1 + 2r_2$ branch points in configuration $(r_1, r_2)$, that is with

- $r_1$ real branch points $t_1, \ldots, t_{r_1}$.
- $r_2$ complex conjugate pairs $\{z_i, \overline{z}_i\} \subset \mathbb{P}^1(\mathbb{C}) \backslash \mathbb{P}^1(\mathbb{R})$ with $z_i = t_{r_1+i-1}$, $\overline{z}_i = t_{r_1+i}$, $i = 1, \ldots, r_2$.

Assume furthermore that $t_1 < \ldots < t_{r_1}$ and $\mathrm{Re}(z_1) < \ldots < \mathrm{Re}(z_{r_2})$. Then there exists a standard ordered topological bouquet $\underline{\gamma} = (\gamma_1, \ldots, \gamma_r)$ for $\mathbb{P}^1(\mathbb{C}) \setminus \mathbf{t}$ such that complex conjugation $c \in \Gamma_{\mathbb{R}}$ acts by

- ${}^c\gamma_i = (\gamma_i^{-1})^{(\gamma_1 \cdots \gamma_{i-1})}$, $i = 1, \ldots, r_1$
- ${}^c\gamma_{r_1+2i-1} = (\gamma_{r_1+2i}^{-1})^{(\gamma_1 \cdots \gamma_{r_1})}$, $i = 1, \ldots, r_2$

Let $G$ be a finite group and $\mathbf{C} = (C_1, ..., C_r) \in \mathcal{C}_r(G)$. Define the subset $\mathrm{sni}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ of $\mathrm{sni}(\mathbf{C})$ consisting of those $(g_1, ..., g_r)$ in $\mathrm{sni}(\mathbf{C})$ satisfying the additional condition:

(4) there exists an involution $g_0 \in G$ such that

- $g_i^{g_0} = (g_i^{-1})^{(g_1 \cdots g_{i-1})}, i = 1, \dots, r_1$
- $g_{r_1+2i-1}^{g_0} = (g_{r_1+2i}^{-1})^{(g_1 \cdots g_{r_1})}, i = 1, \dots, r_2$

Write $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ for the corresponding quotient set modulo the componentwise action of Inn(G). Similarly, define $\mathrm{sni}^{\mathrm{mod},\mathbb{R}}(\mathbf{C}; \mathrm{r}_1, \mathrm{r}_2)$ and $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ without requiring $g_0$ to be an involution. Then, $BCD_{\underline{\gamma}}$ defines an identification $(\Psi'_{r,G})^{-1}(\mathbf{t}') \simeq \overline{\mathrm{sni}}(\mathbf{C})$ such that $\overline{\mathrm{sni}}^{\mathbb{R}}(\mathbf{C}; r_1, r_2)$ corresponds to those G-covers in $\overline{\mathrm{sni}}(\mathbf{C})$ which are defined over $\mathbb{R}$ and $\overline{\mathrm{sni}}^{mod,\mathbb{R}}(\mathbf{C}; r_1, r_2)$ to those with field of moduli contained in $\mathbb{R}$.

*4.3.2. Statements and applications* We will use here a variant Rat of the rationalization operator $\mathrm{Rat}_1$ introduced in paragraph 4.2.1. Namely, $\mathrm{Rat}(C) := (C^{u_1}, C^{-u_1}, ..., C^{u_r}, C^{-u_r})$ if $\{C^u\}_{u \in (\mathbb{Z}/o(C)\mathbb{Z})^\star} = \{C^{\pm u_i}\}_{i=1,...,r}$

**Theorem 4.7.** *Let $G$ be a finite group containing two tuples $\mathbf{A} = (A_1, ..., A_m)$, $\mathbf{B} = (B_1, ..., B_n)$ satisfying* (**H**1) *and* (**H**2)*. Write $\mathbf{C}_s := (\mathrm{Rat}(\mathbf{A}), \mathrm{Rat}(\mathbf{B})^s)$ and $r := \sum_{k=1}^m |\mathrm{Rat}(A_k)|$, $r_s := s \sum_{k=1}^n |\mathrm{Rat}(B_k)|$. Then, for $s$ large enough, $\mathrm{HM}(\mathbf{C}_s)$ is a geometrically irreducible $\mathbb{Q}$-variety and there exists $\mathbf{t}'_{\mathbb{R}} \in \mathcal{U}^{r_s - r}(\overline{\mathbb{Q}})$ with a $\mathbb{Q}$-rational associated divisor $\mathbf{t}_{\mathbb{R}} \in \mathcal{U}_{r_s - r}(\mathbb{Q})$ and such that the symmetrised HM-subvariety $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}$ is a geometrically irreducible $r$-dimensional $\mathbb{Q}$-variety with,*

$$\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}(\mathbb{Q}^{tr})^{noob} \neq \emptyset$$

*Proof.* As in the proof of theorem 4.4, we are only to show $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}(\mathbb{R})^{noob} \neq \emptyset$. For this, apply the following procedure (with the notation of section 4.2.1): given a non trivial conjugacy class $C$

(1) – If $o(C) = 2$, associate to $C$ the tuple $\mathbf{t}'_C := (\sqrt{-1}, -\sqrt{-1})$.
– If $o(C) > 2$, associate to $C$ the tuple $\mathbf{t}'_C := (\zeta_{o(C)}^{u_1}, \zeta_{o(C)}^{-u_1}, \dots, \zeta_{o(C)}^{u_{\phi(o(C))/2}}, \zeta_{o(C)}^{-u_{\phi(o(C))/2}})$.

(2) Set $\mathbf{t}' := (\mathbf{t}'_{1,r}, \mathbf{t}'_{r+1,r_s})$ with

$$\begin{cases} \mathbf{t}'_{1,r} = (\mathbf{t}'_{A_i} + 4(i-1))_{i=1,\dots,m}, \\ \mathbf{t}'_{r+1,r_s} = ((\mathbf{t}'_{B_i} + 4(i-1))_{i=1,\dots,n} + 4(m + jn))_{j=0,\dots,s-1}. \end{cases}$$

Then, $\mathbf{t}' \in \mathcal{U}^{r_s}(\overline{\mathbb{Q}})$ is in configuration $(0, r_s/2)$ and since $\emptyset \neq \overline{\mathrm{hm}}(\mathbf{C}_s) \subset \mathrm{sni}^{\mathbb{R}}(\mathbf{C}_\mathrm{s}; 0, \mathrm{r}_\mathrm{s}/2)$, we obtain $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'}(\mathbb{R})^{noob} \neq \emptyset$. Set $\mathbf{t}'_{\mathbb{R}} := \mathbf{t}'_{r+1,r_s}$, which satisfies $\mathbf{t}'_{\mathbb{R}} \in \mathcal{U}_{r_s - r}(\mathbb{Q})$. Then, by the branch cycle argument, $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_{\mathbb{R}}}$ is defined over $\mathbb{Q}$ and conclude applying the local-global principle to the associated global descent variety as in the proof of proposition 4.1. □

As in section 4.2.2, one can state a profinite version of theorem 4.7 for modular towers and associated $q$-central towers; we leave this to the reader and give another application of our method to the profinite regular inverse Galois problem over $\mathbb{Q}^{tr}$ (see also [C04a]).

Let $(s_{k+1} : G_{k+1} \twoheadrightarrow G_k)$ be a complete projective system of finite groups and $(\mathbf{D}_k = (D_{k,1}, \dots , D_{k,r}))_{k\geq 0}$ a projective system of tuples $\mathbf{D}_k \in \mathcal{C}_r(G_k)$. Write $G := \underset{\longleftarrow}{\lim}\ G_k$ and $\mathbf{D} := \underset{\longleftarrow}{\lim}\mathbf{D}_k$. Also assume there exist $r_1, r_2 \geq 0$ with $r = r_1 + 2r_2$ such that the following holds

$$(*)\ \ \text{For all } m \geq 1 \text{ such that } (m, e(G)) = 1, \text{ we have}$$
$$s_{k+1}^{-1}(\overline{\text{sni}}^{\mathbb{R}}(\mathbf{D}_k; r_1, r_2)) \subset \overline{\text{sni}}^{\mathbb{R}}(\mathbf{D}_{k+1}; r_1, r_2)$$

**Lemma 4.8.** *Assume there exists a G-cover $f_0$ defined over $\mathbb{Q}^{tr}$ with invariants $G_0$, $\mathbf{D}_0$, $\mathbf{t}'$ such that ${}^\sigma\mathbf{t}'$ is in configuration $(r_1, r_2)$, for all $\sigma \in \Gamma_{\mathbb{Q}}$. Also assume that $Z(G)$ is a direct factor of $G$[4]. Then there exists a regular realization of $G$ defined over $\mathbb{Q}^{tr}$ with invariants $\mathbf{D}$, $\mathbf{t}'$.*

*Proof.* Let $\mathbf{p}_0 \in \mathcal{H}_{r,\underline{G_0}}(\mathbf{D}_0)_{\mathbf{t}}(\mathbb{Q}^{tr})^{noob}$ and $(f_k)_{k\geq 0}$ be a projective system of G-covers defined over $\overline{\mathbb{Q}}$ corresponding to a projective system of points $(\mathbf{p}_k)_{k\geq 0} \in \underset{\longleftarrow}{\lim}\ \mathcal{H}_{r,G_k}(\mathbf{D}_k)_{\mathbf{t}}$ above $\mathbf{p}_0$. For any $\sigma \in \Gamma_{\mathbb{Q}}$, by the branch cycle argument, ${}^\sigma(\mathbf{p}_k)_{k\geq 0} \in \underset{\longleftarrow}{\lim}\ \mathcal{H}_{r,G_k}(\mathbf{D}_k^{\chi(\sigma)})_{\mathbf{t}}$. Furthermore, since $f_0$ is defined over $\mathbb{Q}^{tr}$, ${}^\sigma f_0$ is defined over $\mathbb{R}$ with branch points ${}^\sigma\mathbf{t}'$ in configuration $(r_1, r_2)$ so, its branch cycle description lies in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{D}_0; r_1, r_2)$. The branch cycle description of ${}^\sigma f_k$ lies in $\overline{\text{sni}}(\mathbf{D}_k)$ above the one of ${}^\sigma f_0$ so, according to (*), in $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{D}_k; r_1, r_2)$. As a result, ${}^\sigma f_k$ is defined over $\mathbb{R}$. Now, let $D(f_k)$ be the descent variety of $f_k$ [DDoMo04]; it is a smooth geometrically irreducible $\mathbb{R}$-variety such that for any $\sigma \in \Gamma_{\mathbb{Q}}^{\sigma} D(f_k)(\mathbb{R}) = D({}^\sigma(f_k)(\mathbb{R}) \neq \emptyset$. Apply then the local-global principle to show $D(f_k)(\mathbb{Q}^{tr}) \neq \emptyset$; that is, $f_k$ is defined over $\mathbb{Q}^{tr}$. Finally, the hypothesis about $Z(G)$ assures the $\mathbb{Q}^{tr}$-model of the $(f_k)_{k\geq 0}$ can be chosen in a compatible way *cf.* §5.3.1 of [C04b]. □

*Example 4.9.* Let $D_{2a^\infty} := \underset{\longleftarrow}{\lim}\ D_{2a^k}$ be the prodihedral group of order $2a^\infty$ where

$$D_{2a^k} :=< u, v|\ u^{a^k} = v^2 = 1, \quad vuv = u^{-1} >$$

For any $k \geq 1$, let $A_{k,i}$ be the conjugacy class of $u^i$ in $D_{2a^k}$, $i = 1, ..., [(a^k + 1)/2]$ and $B_k$ be the conjugacy class of $v$ in $D_{2a^k}$. Then check that for any $1 \leq i_1, ..., i_t \leq$

[4] This hypothesis can be relaxed *cf.* §5.3.1 of [C04b]. If it is removed and if $\overline{\text{sni}}^{\mathbb{R}}(\mathbf{D}_k; r_1, r_2)$ is replaced by $\overline{\text{sni}}^{mod,\mathbb{R}}(\mathbf{D}_k; r_1, r_2)$, $k \geq 0$ then one obtains profinite Galois extensions of $\overline{\mathbb{Q}}(T)$ with invariants $G$, $\mathbf{D}$, $\mathbf{t}'$ and field of moduli contained in $\mathbb{Q}^{tr}$.

$[a^k + 1)/2]$ condition (*) is fulfilled with $\mathbf{D}_k := ([B_k], [A_{k,i_1}, ..., A_{k,i_t}])$, $k \geq 1$ (*cf* [C04b]). To prove the existence of $f_1$ as in the lemma, we re-use the idea (and the notation!) of the proof of theorem 4.7 as follows: observe that $\mathbf{A} := (B_1)$, $\mathbf{B} := (A_{1,1})$ satisfy (**H**1) and (**H**2) so, noticing that the tuple $\mathbf{C}_s$ of theorem 4.7 is of the form $\mathbf{D}_0 = ([B_0], [A_{0,i_1}, ..., A_{0,i_t}])$ above, for $s$ large enough and for any $\mathbf{t}'_{3,r_s} \in \mathcal{U}^{r_s-1}(\overline{\mathbb{Q}})$, $\mathrm{HM}(\mathbf{C}_s)_{\mathbf{t}'_{3,r_s}}$ is a geometrically irreducible curve. Let $\mathbf{t}'_{3,r_s} \in \mathcal{U}^{r_s-2}(\overline{\mathbb{Q}})$ built as in the proof of theorem 4.7 then, since $B$ is rational ($o(B) = 2$), $\mathrm{HM}(\mathbf{C}_s)_{(0,\mathbf{t}'_{3,r_s})}$ is defined over $\mathbb{Q}$. According to section 4.3.1, we obtain $\mathrm{HM}(\mathbf{C}_s)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{R})^{noob} \neq \emptyset$ so, applying once again the local-global principle to the global descent variety, $\mathrm{HM}(\mathbf{C}_s)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{Q}^{tr})^{noob} \neq \emptyset$ and, if $f_0$ is a G-cover corresponding to a point $\mathbf{p}_1 \in \mathrm{HM}(\mathbf{C}_s)_{(0,\mathbf{t}'_{3,r_s})}(\mathbb{Q}^{tr})^{noob}$, its branch point divisor is of the form $(t_1, 0, \mathbf{t}'_{2,r_s})$ that is in configuration $(2, r_s/2-1)$ and satisfying the hypothesis of lemma 4.8. Conclude, by applying this lemma, that there exists regular realization of $D_{2a^\infty}$ over $\mathbb{Q}^{tr}$ with invariants $\varprojlim ([B_k], [A_{k,1}^{u_1}, ..., A_{k,1}^{u_{\phi(a)/2}}])$, $(t_1, 0, \mathbf{t}'_{3,r_s})$.

## References

[BF02] Bailey, P., Fried, M.: Hurwitz monodromy, spin separation and higher levels of Modular Towers. Proceedings of symposia in pure mathematics, A.M.S., M. Fried and Y. Ihara ed., 2002

[Bi74] Birman, J. S.: Braids, links and mapping class groups. Princeton University Press, 1974

[C04a] Cadoret, A.: Counting Galois real covers of the projective line. Pacific J. Math. **219**, 101–129 (2005)

[C04b] Cadoret, A.: Théorie de Galois inverse et arithmétique des espaces de Hurwitz. thèse de doctorat de l'U.S.T.L., 2004

[D92] Dèbes, P.: Critère de descente pour le corps de définition des G-revêtements de $\mathbb{P}^1$. C.R. Acad. Sci. Paris, t.315, série I, 863–868 (1992)

[D95] Dèbes, P.: Covers of $\mathbb{P}^1$ over the $p$-adics. in Recent Developments in the Inverse Galois Problem, Contemporary Math. **186**, 217–238 (1995)

[D04] Dèbes, P.: Modular Towers. construction and diophantine questions, preprint 2004.

[DDes04] Dèbes, P., Deschamps, B.: Corps $\psi$-libres et théorie inverse de Galois infinie. J. fur die reine und angew. Math. **574**, 197–218 (2004)

[DDoMo04] Dèbes, P., Douai, J.-C., Moret-Bailly, L.: Descent varieties for algebraic covers. J. fur die reine und angew. Math. **574**, 51–78 (2004)

[DE03] Dèbes, P., Emsalem, M.: Harbater-Mumford Components and Towers of Moduli Spaces. J. Inst. Math. Jussieu, to appear.

[DF94] Dèbes, P., Fried, M.: Nonrigid Constructions in Galois Theory. Pacific J. Math. **163**, 81–122 (1994)

[Des95] Deschamps, B.: Existence de points $p$-adiques pour tout $p$ sur un espace de Hurwitz. Proceedings AMS-NSF Summer Conference, **186**, Cont. Math. series, Recent Developments in the Inverse Galois Problem, 111–171 (1995)

[Di] Dickson, L. E.: Linear groups with an exposition of the Galois field theory. Dover, 1958

[F95] Fried, M.: Introduction to Modular Towers:Generalizing the relation between dihedral groups and modular curves. Proceedings AMS-NSF Summer Conference. Cont. Math. series, Recent Developments in the Inverse Galois Problem **186**, 111–171 (1995)

[FV91] Fried, M., Volklein, H.: The Inverse Galois Problem and Rational Points on Moduli Spaces. Math. Ann. **290**, 771–800 (1991)

[GPR97] Green, B. W., Pop, F., Roquette, P.: On Rumely's Local-Global principle. Jber.d.Dt.Math.-Verein **97**, 43–74 (1997)

[H87] Harbater, D.: Galois coverings of the arithmetic line. Lecture Notes in Math. **1240**, 165–195 (1987)

[H03] Harbater, D.: Patching and Galois theory. MSRI Publications series, Cambridge University Press, **41**, 313–424 (2003)

[L95] Liu, Q.: Tout groupe fini est groupe de Galois sur $\mathbb{Q}_p(T)$. Contemporary Mathematics. **186**, 261–265 (1995)

[M89] Matzat, H. B.: Rationality criteria for Galois extensions. in Ihara et al., Galois groups over $\mathbb{Q}$, Proc. Workshop Berkeley 1987, Publ. Math. Sci. Res. Inst. **16**, 361–383, Springer, Berlin, Heidelberg, 1989

[MMa99] Malle, G., Matzat, H. B.: Inverse Galois Theory. S.M.M., Springer, Berlin, Heidelberg, 1999

[Mo89] Moret-Bailly, L.: Groupes de Picard et problèmes de Skolem II. Annales Sci. E.N.S., **22**, 181–194 (1989)

[P94] Pop, F.: Half Riemann's existence theorem. Algebra and Number Theory (G.Frey and J.Ritters, eds.), De Gruyter Proceedings in Mathematics, 1–26 (1994)

[P96] Pop, F.: Embedding problems over large fields. Annals of Math. **144**, p. 1–35, 1996. Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, 1999

[S86] Suzuki, M.: Group Theory I, II. G.M.W., **247**, **248** Springer, Berlin, Heidelberg, 1986

[V99] Volklein, H.: Groups as Galois groups - an introduction. Cambridge Studies in Advanced Mathematics, **53**, Cambridge University Press, 1999

[W98] Wewers, S.: Construction of Hurwitz Spaces. Thesis, Preprint **21** of the IEM, Essen, 1998

[Wi84] Wielandt, H.: Finite Permutation Groups. Academic Press, 1984