Pacific Journal of Mathematics

COUNTING REAL GALOIS COVERS OF THE PROJECTIVE LINE

ANNA CADORET

Volume 219 No. 1 March 2005

PACIFIC JOURNAL OF MATHEMATICS
Vol. 219, No. 1, 2005

COUNTING REAL GALOIS COVERS OF THE PROJECTIVE LINE

ANNA CADORET

For Galois covers of $\mathbb{P}^1$ of a given ramification type — essentially, a given monodromy group G and branch locus, assumed to be defined over $\mathbb{R}$ — we ask: How many covers are defined over $\mathbb{R}$ and how many are not? J.-P. Serre showed that the number of all Galois covers with given ramification type can be computed from the character table of G. We adapt Serre's method of calculation to the more refined situation of Galois covers defined over $\mathbb{R}$, for which there is a group-theoretic characterization due to P. Dèbes and M. Fried. We obtain explicit answers to our problem. As an application, we exhibit new families of covers not defined over their field of moduli, the monodromy group of which can be chosen arbitrarily large. We also give examples of Galois covers defined over the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real algebraic numbers with $\mathbb{Q}$-rational branch locus.

Introduction

By Riemann's Existence Theorem there is a bijective correspondence between isomorphism classes of Galois covers $f : X \to \mathbb{P}^1_{\mathbb{C}}$ of the projective line with Galois group G and branch points $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$ and r-tuples $(g_1, \ldots, g_r) \in G$ of generators of G satisfying the relation $g_1 \cdots g_r = 1$. Fixing an r-tuple $\boldsymbol{C} = (C_1, \ldots, C_r)$ of conjugacy classes of G, we say f is of type $\boldsymbol{C}$ if the corresponding r-tuple $(g_1, \ldots, g_r) \in G$ has the extra property that there exists a permutation σ such that $g_i \in C_{\sigma(i)}$ for $i = 1, \ldots, r$.

An important and well-known formula proved by Serre [1992, Chapter 7] computes the number of r-tuples $(g_1, \ldots, g_r) \in G$ with $g_i \in C_i$ for $i = 1, \ldots, r$ and such that $g_1 \cdots g_r = 1$. In many cases, this formula can be used to compute the number of isomorphism classes of G-covers of $\mathbb{P}^1$ of type $\boldsymbol{C}$, with branch points $t_1, \ldots, t_r \in \mathbb{P}^1(\mathbb{C})$. This formula has proved to be particularly powerful in the classical rigid situation and led, for instance, to the realization over $\mathbb{Q}$ of most

MSC2000: 12F12, 20C40, 14D22.

Keywords: inverse Galois theory, group representations, ramification type, fine and coarse moduli spaces.

of the sporadic groups (see [Malle and Matzat 1999, Chapter II] for a systematic investigation of this method).

Here we consider the refined problem of counting the number of those G-covers of $\mathbb{P}^1$ with fixed branch locus and for which the field of the real numbers $\mathbb{R}$ is a field of definition. We also consider the related problem of how many G-covers have their field of moduli contained in $\mathbb{R}$. For these two questions P. Dèbes and M. Fried [1994] showed that there is also a group theoretic characterization: the r-tuples $(g_1, \ldots, g_r) \in G$ should satisfy some additional conditions, involving the involutions of G (see Section 1).

We generalize Serre's formula and use Dèbes and Fried's results to give a general formula for the number of r-tuples $(g_1, \ldots, g_r) \in G$ corresponding to G-covers $f : X \to \mathbb{P}^1$ with given branch locus and which are defined over $\mathbb{R}$. In the general situation, this formula is more complicated than the one given by Serre. In order to simplify it and make it effective, we consider two special cases separately, where the branch locus consists either only of real points or only of pairs of complex conjugate points. We then give several applications.

Thus, we deal with the existence of G-covers which are not defined over their field of moduli. Some criteria are already known that guarantee that the field of moduli is a field of definition, for instance when $Z(G)$ is a direct summand of G [Coombes and Harbater 1985, Proposition 2.8]. Most of these results rely on a cohomological approach (see [Dèbes 1995], [Dèbes and Douai 1997] or [Wewers 2002], for instance); ours is different and leads to criteria — one of them being an easy-to-check group-theoretic condition — for G-covers not to be defined over their field of moduli. Applying these criteria, we exhibit infinite families of groups for which one can always find such G-covers.

We also explain how to use our computations to descend from $\mathbb{C}$ to the field $\mathbb{Q}^{\mathrm{tr}}$ of all totally real algebraic numbers. It is known, by [Dèbes and Fried 1994, Theorem 5.7], that each finite group is the Galois group of a regular extension of $\mathbb{Q}^{\mathrm{tr}}(X)$ but the proof does not show this can be done with a branch point divisor $\boldsymbol{t}$ defined over $\mathbb{Q}$. Our method — when it works — enables us to choose $\boldsymbol{t}$ this way. We conclude by considering the case of the Mathieu group M_{11}.

The paper is organized as follows. In Section 1 we introduce the main tools. In Section 2 we state the results and make some remarks. Section 3 is devoted to the proofs and Section 4 to examples and applications.

1. Preliminaries

Notations. For a finite group G, denote:

– the set of all inner automorphisms of G by $\mathrm{Int}(G)$.

– the set of all elements of order ≤ 2 in G by $\mathrm{Inv}(G)$.

– the set of all the irreducible complex characters of G by $\mathrm{Irr}(G)$ and the trivial character of G by χ_1.

– for all $g \in G$ the centralizer of g in G by $\mathrm{Cen}_G(g)$.

Recall that a G-cover with group G is a pair (f, α), 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. One can attach certain invariants to each G-cover of $\mathbb{P}^1_{\mathbb{C}}$: the monodromy group G, the branch point set $\boldsymbol{t} = \{t_1, \ldots, t_r\} \subset \mathbb{P}^1(\mathbb{C})$ (which we sometimes view as a divisor $(t_1) + \cdots + (t_r)$ on $\mathbb{P}^1$) and for each $t \in \boldsymbol{t}$ the *associated inertia canonical conjugacy class* C_t. To summarize this, we will sometimes say the G-cover being considered has *ramification type* $[G, \boldsymbol{C}, \boldsymbol{t}]$; see [Völklein 1996, Definition 2.12, p. 37]. Adopting the topological point of view, recall what these invariants correspond to: given $\boldsymbol{t} = \{t_1, \ldots, t_r\}$, introduce a *topological bouquet* $\boldsymbol{\gamma}$ of $\mathbb{P}^1_{\mathbb{C}} \setminus \boldsymbol{t}$, that is, an r-tuple of homotopy classes of loops $\gamma_1, \ldots, \gamma_r$ based at some point $t_0 \notin \boldsymbol{t}$ such that

– $\gamma_1, \ldots, \gamma_r$ generate the topological fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \boldsymbol{t}, t_0)$ with the single relation $\gamma_1 \cdots \gamma_r = 1$,

– γ_i is a loop revolving once counterclockwise about t_i, for $i = 1, \ldots, r$.

Now, considering a G-cover $f : X \to \mathbb{P}^1_{\mathbb{C}}$, the monodromy action defines a permutation representation $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \boldsymbol{t}, t_0) \to \mathrm{Per}(f^{-1}(t_0))$. The image group G of this representation is the monodromy group (equivalently, the Galois group) of f and the conjugacy class C_{t_i} of the image of γ_i in G is the inertia canonical class corresponding to t_i, $i = 1, \ldots, r$.

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 $\boldsymbol{t}' = (t_1, \ldots, t_r) \in (\mathbb{P}^1_{\mathbb{C}})^r$ 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 let $\pi_r : \mathcal{U}_r \to \mathcal{U}^r / S_r$ be 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 (or the fine moduli space if $Z(G) = \{1\}$) 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 application which to a given isomorphism class of G-covers associates its branch point set. For any r-tuple $\boldsymbol{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in G let $\mathcal{H}_{r,G}(\boldsymbol{C})$ be the corresponding *Hurwitz space* [Fried and Völklein 1991], that is the union of irreducible components of $\mathcal{H}_{r,G}$ parametrizing the isomorphism classes of G-covers with ramification type $[G, \boldsymbol{C}, \boldsymbol{t}]$. A point $\big(h, (t_1, \ldots, t_r)\big)$ of the fiber product $\mathcal{H}_{r,G}(\boldsymbol{C}) \times_{\mathcal{U}_r} \mathcal{U}^r$ then corresponds to a G-cover given with an ordering of its branch points, which allows us to define a monodromy application

$$\begin{array}{rccc} M\colon & \mathcal{H}_{r,G}(\boldsymbol{C}) \times_{\mathcal{U}_r} \mathcal{U}^r & \longrightarrow & \{C_1, \ldots, C_r\}^r, \\ & (h, (t_1, \ldots, t_r)) & \longmapsto & (C_{t_1}, \ldots, C_{t_r}). \end{array}$$

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

$$\begin{array}{ccc} \mathcal{H}'_{r,G}(\boldsymbol{C}) & \xrightarrow{\Pi_r} & \mathcal{H}_{r,G}(\boldsymbol{C}) \\ \downarrow{\scriptstyle \psi'_{r,G}} & & \downarrow{\scriptstyle \psi_{r,G}} \\ \mathcal{U}^r & \xrightarrow{\pi_r} & \mathcal{U}_r \end{array}$$

We will freely use the general theory of Hurwitz spaces (see [Fried and Völklein 1991] and [Völklein 1996], for instance), and only recall here the description of the fibers of $\psi_{r,G}$ and $\psi'_{r,G}$ in terms of *Nielsen classes* $\mathrm{Ni}(\boldsymbol{C}, G)$ and *straight Nielsen classes* $\mathrm{SN}(\boldsymbol{C}, G)$. Recall that

$$\mathrm{Ni}(\boldsymbol{C}, G)=\left\{(g_1,\dots,g_r)\in G^r \;\middle|\; \begin{array}{l} G=\langle g_1,\dots,g_r\rangle,\ g_1\cdots g_r=1,\ \text{and} \\ \exists\sigma\in S_r \text{ such that } g_i\in C_{\sigma(i)} \text{ for } i=1,\dots,r \end{array}\right\}$$

and $\mathrm{SN}(\boldsymbol{C}, G)$ is defined likewise but with the requirement that σ be the identity. We use the notations $\overline{\mathrm{ni}}(\boldsymbol{C}, G)$ and $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ for the corresponding quotient sets modulo the componentwise action of $\mathrm{Int}(G)$.

Given $\boldsymbol{t}\in\mathcal{U}_r$, it is a classical result that $(\psi_{r,G})^{-1}(\boldsymbol{t})$ is in bijection with $\overline{\mathrm{ni}}(\boldsymbol{C}, G)$. Furthermore, if we choose an ordering of the branch points $\boldsymbol{t}'=(t_1,\dots,t_r)$ in $\boldsymbol{t}$, $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ is in bijection with $(\psi'_{r,G})^{-1}(\boldsymbol{t}')$. The correspondence is given by the monodromy action. We will sometimes say abusively that *a G-cover with branch point set $\boldsymbol{t}\in\mathcal{U}_r(\mathbb{C})$ is in $\overline{\mathrm{ni}}(\boldsymbol{C}, G)$* when its isomorphism class has ramification type $[G, \boldsymbol{C}, \boldsymbol{t}]$ or that, *if an ordering $\boldsymbol{t}'=(t_1,\dots,t_r)\in\mathcal{U}^r(\mathbb{C})$ is given, a G-cover is in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$* when C_i is the inertia canonical class associated with t_i for $i=1,\dots,r$.

Convention. Since we are interested in G-covers defined over $\mathbb{R}$, we will always suppose the branch point divisor is real, that is, it consists of $r=r_1+2r_2$ branch points, of which

- r_1 real branch points $t_1,\dots,t_{r_1}$, assumed to be in the order $t_1<\cdots<t_{r_1}$, and
- r_2 complex conjugated pairs $\{z_i,\bar{z}_i\}\subset\mathbb{P}^1(\mathbb{C})\setminus\mathbb{P}^1(\mathbb{R})$. We will generally write $z_i=t_{r_1+i}$ and $\bar{z}_i=t_{r+1-i}$ for $i=1,\dots,r_2$. We may also, if needed, order these pairs according to their real and imaginary parts.

Two subsets of $\mathrm{SN}(\boldsymbol{C}, G)$ will play an important role later. $\mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ consists of those $(g_1,\dots,g_r)$ in $\mathrm{SN}(\boldsymbol{C}, G)$ satisfying the condition that there exists $g_0\in G$ such that

$$\text{(1–1)}\qquad \begin{array}{ll} g_0(g_1\cdots g_i)g_0^{-1}=(g_1\cdots g_i)^{-1} & \text{for } i=1,\dots,r_1-1, \\ g_0g_{r_1+i}g_0^{-1}=g_{r+1-i}^{-1} \text{ and } g_0g_{r+1-i}g_0^{-1}=g_{r_1+i}^{-1} & \text{for } i=1,\dots,r_2. \end{array}$$

$\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ consists of those $(g_1, \dots, g_r)$ in $\mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ for which g_0 can be chosen from $\mathrm{Inv}(G)$.

As above we write $\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ and $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ for the corresponding quotient sets modulo the action of $\mathrm{Int}(G)$. We have

$$\left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| = \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| [G : Z(G)].$$

We will also need the sets $\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ and $\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$, which are defined like $\mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ and $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$, but dropping the generating condition $G = \langle g_1, \dots, g_r \rangle$. It follows readily from the definitions that

$$\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| = \frac{\left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|}{[G : Z(G)]} \le \frac{\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|}{[G : Z(G)]},$$

so computing the cardinality of the "Σ-versions", which is easier, gives an upper bound for $\left|\mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ and $\left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$. Moreover, in lots of situations $\mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2) = \Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ and $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2) = \Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$; see Remark 2.7.

One of the main results of [Dèbes and Fried 1994] is that, given $\boldsymbol{t}' \in \mathcal{U}^r$ ordered according to the Convention above, there exists an identification $(\Psi'_{r,G})^{-1}(\boldsymbol{t}') \simeq \overline{\mathrm{sn}}(\boldsymbol{C}, G)$, as recalled above, such that $\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ is exactly the set of those G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ whose field of moduli is contained in $\mathbb{R}$, and $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ is the set of those G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ that are defined over $\mathbb{R}$.

A complete proof of this can be found in [Dèbes and Fried 1994]. We only recall the main ideas. Let $\boldsymbol{t} \in \mathcal{U}_r(\mathbb{R})$ be a real branch point divisor ordered according to the convention. The first step consists in describing the action of complex conjugation c on the fundamental group $\pi_1^{\mathrm{top}}(\mathbb{P}^1(\mathbb{C}) \setminus \boldsymbol{t}, t_0)$ of $\mathbb{P}^1(\mathbb{C}) \setminus \boldsymbol{t}$, which we denote by π^{top}. One can find $\Gamma_1, \dots, \Gamma_r \in \pi^{\mathrm{top}}$ that generate π^{top} with the single relation $\Gamma_1 \cdots \Gamma_r = 1$ and complex conjugation c acts on π^{top} by Hurwitz's formulas (see [Malle and Matzat 1999], for instance):

$$\begin{aligned} &c\Gamma_i = \Gamma_1 \cdots \Gamma_{i-1} \Gamma_i^{-1} (\Gamma_1 \cdots \Gamma_{i-1})^{-1} && \text{for } i = 1, \dots, r_1, \\ &c\Gamma_{r_1+i} = \Gamma_{r+1-i}^{-1} && \text{for } i = 1, \dots, r_2. \end{aligned} \tag{1–2}$$

We will denote by $\mathscr{C}$ the formal operator that maps each component Γ_i of an r-tuple $(\Gamma_1, \dots, \Gamma_r)$ to the right-hand term of the formulas (1–2) (that is, $c\Gamma_i = \Gamma_i^{\mathscr{C}}$ for $i = 1, \dots, r$). Let $\Omega/\mathbb{C}(X)$ be the maximal algebraic extension of $\mathbb{C}(X)$ unramified outside $\boldsymbol{t}$; this is a Galois extension with group $\mathrm{Gal}(\Omega/\mathbb{C}(X)) =: \pi^{\mathrm{alg}}$. And by Riemann's Existence Theorem we get an isomorphism $\widehat{\pi^{\mathrm{top}}} \simeq \pi^{\mathrm{alg}}$, where $\widehat{\pi^{\mathrm{top}}}$ is the profinite completion of π^{top} [Serre 1992].

The second step is a necessary and sufficient condition for the "descent from $\mathbb{C}$ to $\mathbb{R}$": Since the branch point divisor is real, $\Omega/\mathbb{R}(X)$ is Galois with group

$\mathrm{Gal}(\Omega/\mathbb{R}(X)) =: \pi_{\mathbb{R}}$. Furthermore, since $\mathbb{P}^1$ has real points, the short exact sequence (1–3) below splits and $\pi_{\mathbb{R}} \simeq \pi^{\mathrm{alg}} \rtimes \mathbb{Z}/2\mathbb{Z}$. Now, if $K/\mathbb{C}(X)$ is the function field extension of an algebraic G-cover $f : X \to \mathbb{P}^1$ and $\psi : \pi^{\mathrm{alg}} \to G$ is the corresponding epimorphism, f can be defined over $\mathbb{R}$ (so f is in $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$) if and only if there exists a map $\tilde{\psi}$ such that the diagram

(1–3)
$$\begin{array}{ccccccccc} 1 & \longrightarrow & \pi^{\mathrm{alg}} & \longrightarrow & \pi_{\mathbb{R}} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \psi} & \swarrow{\scriptstyle \exists \tilde{\psi}} & & & & & \\ & & G & & & & & & \end{array}$$

commutes. For all $\psi \in \mathrm{Hom}(\pi^{\mathrm{alg}}, G)$, write $g_i = \psi(\Gamma_i)$ for $i = 1, \ldots, r$. Then ψ extends to $\tilde{\psi} \in \mathrm{Hom}(\pi^{\mathrm{alg}} \rtimes \mathbb{Z}/2\mathbb{Z}, G)$ if and only if there exists $g_0 \in \mathrm{Inv}(G)$ for which $g_0 g_i g_0 = g_i^{\mathscr{C}}$ for $i = 1, \ldots, r$; see [Dèbes and Fried 1994, Lemma 3.3]. This provides the condition in the definition of $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$.

Furthermore, if $f : X \to \mathbb{P}^1_{\mathbb{C}}$ corresponds to $(g_1, \ldots, g_r) \in \mathrm{SN}(\boldsymbol{C}, G)$, then $f^c : X^c \to \mathbb{P}^1_{\mathbb{C}}$ corresponds to $(g_1^{\mathscr{C}}, \ldots, g_r^{\mathscr{C}}) \in \mathrm{SN}(\boldsymbol{C}^{\mathscr{C}}, G)$. So the set of all isomorphism classes of G-covers with field of moduli contained in $\mathbb{R}$ and branch points $\boldsymbol{t}'$ in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ corresponds to $\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$. The extra condition $g_0^2 = 1$ that appears in $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ comes from Weil's cocycle condition [Weil 1956].

Remark. If we fix $\boldsymbol{t} \in \mathcal{U}_r(\mathbb{R})$, the real points in the fiber $(\psi_{r,G})^{-1}(\boldsymbol{t})$ correspond to G-covers whose field of moduli is contained in $\mathbb{R}$. So, when working with moduli spaces, it is no longer possible to distinguish between G-covers defined over $\mathbb{R}$ and those that only have their field of moduli contained in $\mathbb{R}$. Some information is lost.

2. Statements and remarks

Our main results are estimates of the cardinality of $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$. What we actually compute is not $\left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ but $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$, which is an upper bound for $\left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$. In the sequel, we will always assume $\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2) \neq \varnothing$.

We distinguish three situations, depending on the configuration of branch points:

(R) $r_2 = 0$ (real configuration).

(C) $r_1 = 0$ (complex pairs configuration).

(R-C) $r_1, r_2 \geq 0$ (general configuration).

Though (R) and (C) are just special cases of (R-C), they allow us to compute $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ more easily, and the formulas obtained are much simpler than in the general case.

To make the formulas more legible, we will write:

– Z_i for the order of the centralizer of any element in the conjugacy class C_i.

– $\boldsymbol{\chi} \in \mathrm{Irr}(G)^r$ for any r-tuple $(\chi_1, \ldots, \chi_r) \in \mathrm{Irr}(G)^r$.

– $\boldsymbol{u} \in \mathrm{Inv}(G)^r$ for any r-tuple $(u_0, \ldots, u_{r-1}) \in \mathrm{Inv}(G)^r$.

We also fix $g_1, \ldots, g_r \in G$ with $g_i \in C_i$ for $i = 1, \ldots, r$.

Theorem 2.1 (Configuration (R): Real branch points). *For all* $\boldsymbol{\chi} \in \mathrm{Irr}(G)^r$ *set*

$$I_{\boldsymbol{\chi}} = \sum_{\boldsymbol{u} \in \mathrm{Inv}(G)^r/\sim_G} \chi_1(u_0u_1)\,\chi_2(u_1u_2)\cdots\chi_r(u_{r-1}u_0),$$

where $\mathrm{Inv}(G)^r/\sim_G$ *is the quotient set of the equivalence relation on* $\mathrm{Inv}(G)^r$ *that identifies two* r*-tuples* $\boldsymbol{u}, \boldsymbol{u}' \in \mathrm{Inv}(G)^r$ *if* $(u_0, \ldots, u_{r-1}) = g.(u'_0, \ldots, u'_{r-1})$ *for some* $g \in G$. *Also set*

$$n^{\mathbb{R}}(\boldsymbol{C}; r, 0) = \frac{1}{Z_1 \cdots Z_r} \sum_{\boldsymbol{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1)\cdots\chi_r(g_r)\; I_{\boldsymbol{\chi}}.$$

Then

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r, 0)\right| = n^{\mathbb{R}}(\boldsymbol{C}; r, 0).$$

Remark 2.2. This formula can be improved to give

$$\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r, 0)\right| = \frac{|Z(G)|}{|G|Z_1 \cdots Z_r} \sum_{\boldsymbol{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1)\cdots\chi_r(g_r)\; I^*_{\boldsymbol{\chi}},$$

where $I^*_{\boldsymbol{\chi}}$ is defined as $I_{\boldsymbol{\chi}}$ with the only difference that the summation domain is the subset of $\mathrm{Inv}(G)^r/\sim_G$ consisting of those r-tuples of representatives $\boldsymbol{u} \in \mathrm{Inv}(G)^r/\sim_G$ such that $G = \langle u_0u_1, \ldots, u_{r-2}u_{r-1}\rangle$. This condition does not depend on the representative $\boldsymbol{u}$ since, if $g \cdot \boldsymbol{u} \in \mathrm{Inv}(G)^r$ for some $g \in G$ then $gu_igu_{i+1} = (gu_i)^{-1}gu_{i+1} = u_iu_{i+1}$ for $i = 0, \ldots, r-2$.

Theorem 2.3 (Configuration (C): Complex conjugate branch points). *For* $\chi \in \mathrm{Irr}(G)$ *and* $g_0 \in G$, *denote by*

$$\frac{\alpha_{\chi, g_0}}{|\,\mathrm{Cen}_G(g_0)|}$$

the number of occurrences of the trivial representation in the decomposition of $\chi|_{\mathrm{Cen}_G(g_0)}$ *into a direct sum of irreducible linear representations*; *thus*

$$\alpha_{\chi, g_0} = \sum_{u \in \mathrm{Cen}_G(g_0)} \chi(u)$$

(see [Serre 1978]). *Also set*

$$A_\chi = \sum_{g_0 \in \mathrm{Inv}(G)/\sim_{Z(G)}} \alpha_{\chi, g_0},$$

where $\mathrm{Inv}(G)/\sim_{Z(G)}$ *is defined like* $\mathrm{Inv}(G)^r/\sim_G$ *in Theorem 2.1 and*

$$n^{\mathbb{R}}(\boldsymbol{C};0,s)=\frac{|C_1|\cdots|C_s|}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\chi(g_1)\cdots\chi(g_s)}{\chi(1)^{s-1}}\,A_\chi.$$

Then

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\right|\le n^{\mathbb{R}}(\boldsymbol{C};0,s),$$

with equality if $\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)=\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C};0,s)$.

Theorem 2.4 (Configuration (R-C): Real and complex conjugate branch points). *For* $r_1,r_2>0$, *set*

$$n_0^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)=\sum_{\boldsymbol{\chi},\alpha,\beta,\boldsymbol{u}}\frac{\alpha(g_{r_1})\prod_{i=1}^{r_2}\beta(g_{r_1+i})}{\beta(1)^{r_2-1}}\prod_{i=1}^{r_1-1}(\chi_i(g_i)\chi_i(u_{i-1}u_i))\times\sum_{x\in G}\alpha(u_{r_1-1}x^{-1}u_0x)\beta(x),$$

where the first summation is taken over all $\boldsymbol{\chi}\in\mathrm{Irr}(G)^{r_1-1}$, *all* $\alpha,\beta\in\mathrm{Irr}(G)$ *and all* $\boldsymbol{u}$ *in the quotient of* $\mathrm{Inv}(G)^{r_1}$ *by an equivalence relation* $\sim$ *to be defined in Section 3.3. Also set*

$$n^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)=\frac{|C_{r_1+1}|\cdots|C_{r_1+r_2}|}{|G|\,Z_1\cdots Z_{r_1}}\,n_0^{\mathbb{R}}(\boldsymbol{C};r_1,r_2).$$

Then

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)\right|\le n^{\mathbb{R}}(\boldsymbol{C};r_1,r_2).$$

Note that for $r_2=0$ or $r_1=0$ the formulas in this theorem reduce to those in the preceding two theorems, so long as (for $r_1=0$) we replace $\boldsymbol{u}\in\mathrm{Inv}(G)^{r_1}/\sim$ by $u_0\in\mathrm{Inv}(G)/\sim_G$ and g_1,u_{r_1-1} by u_0.

Remark 2.5. For a fixed $\boldsymbol{t}\in\mathcal{U}_r(\mathbb{R})$, the invariants of G and $\boldsymbol{C}$ on which the number of real G-covers in $\mathrm{SN}(\boldsymbol{C},G)$ depends clearly appear in Theorems 2.1, 2.3 and 2.4. Compared with Serre's formula for the basic rigidity criterion, one can notice the important part played by the involutions of G.

Remark 2.6. From a practical point of view, the terms depending on involutions make formulas in configurations (R) and (R-C) complicated for direct computations. On the contrary, $n^{\mathbb{R}}(\boldsymbol{C};0,s)$ is easy to compute once the character table of G and the centralizers of its involutions are known. When $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C};0,s)$ is properly contained in $\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)$, the number $n^{\mathbb{R}}(\boldsymbol{C};0,s)$ only gives an upper bound for $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\right|$, but we explain in the next remark how this difficulty can be handled.

Remark 2.7. One can proceed as in the classical rigidity context, generalizing the method given in [Serre 1992] to evaluate $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)\right|$ from $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)\right|$:

(1) Evaluate $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)\right|$ by $n^{\mathbb{R}}(\boldsymbol{C};r_1,r_2)$, using the character table of G.

(2) Compute $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| - \left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$, by finding r-tuples

$$(g_1, \ldots, g_r) = \boldsymbol{g} \in \Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$$

that do not generate G (to do this, try to find r-tuples the entries of which are contained in a maximal subgroup of G). But we have to be careful: when an r-tuple $\boldsymbol{g} \in \Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2) \setminus \mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ has been found, the following should be done.

- In situation (R): $\boldsymbol{g}$ has to be counted once as in the classical rigidity method.
- In situation (C): an extra difficulty arises from the computation of A_χ. One has to compute $\mathrm{Cen}_G(\langle g_1, \ldots, g_{2s}\rangle)$ and notice that $\boldsymbol{g}$ corresponds to one single class of $\mathrm{Inv}(G)/\sim_{\mathrm{Cen}_G(\langle g_1,\ldots,g_{2s}\rangle)}$. If this class can be written as the union of n classes of $\mathrm{Inv}(G)/\sim_{Z(G)}$, then $\boldsymbol{g}$ has to be counted n times.
- Situation (R-C) is dealt with like situation (C).

The best situation is obviously when $\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2) = \mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$. This occurs, for instance, when each nontrivial conjugacy class of G appears at least once in $\boldsymbol{C}$ or, more generally, when $\boldsymbol{C}$ is *g-complete* [Fried 1995], that is, when $G = \langle g_1, \ldots, g_r\rangle$ for all choices $g_i \in C_i$, $i = 1, \ldots, r$. Then Theorem 2.3 provides $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ directly. Moreover, if $\Sigma(\boldsymbol{C}, G) = \mathrm{SN}(\boldsymbol{C}, G)$, one can also compute $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|$ with Serre's formula [1992], and hence the proportion of G-covers defined over $\mathbb{R}$, namely

$$\frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|}.$$

Remark 2.8. As in the rigidity context, $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|$ and $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ provide information about the field of moduli of the associated G-covers. For instance, the condition $\left|\overline{\mathrm{sn}}(\boldsymbol{C}; r_1, r_2)\right| = \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ (under some technical assumptions) leads to G-covers defined over $\mathbb{Q}^{\mathrm{tr}}$; see Section 4.2.1 and Section 4.2.2 for applications of this. Similarly, when $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ contains a G-cover f defined over $\mathbb{Q}^{\mathrm{tr}}$ and satisfying some other technical conditions, $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ is an upper bound for the degree of a field extension $K/\mathbb{Q}$ over which f is defined; see [Dèbes 1995, Theorem 4.1].

Remark 2.9. As in Theorems 2.1, 2.3 and 2.4, one can give formulas for G-covers with field of moduli contained in $\mathbb{R}$. They can be proved just like the ones for G-covers defined over $\mathbb{R}$, using in the proof, instead of condition (1–1), the equivalent condition that there exist $g_0 \in G$ such that $g_0^2 \in Z(G)$ and

$$\text{(2–1)} \qquad \begin{aligned} &(g_0 g_1 \cdots g_i)^2 = g_0^2 \qquad \text{for } i = 1, \ldots, r_1 - 1,\\ &g_0 g_{r_1+i} g_0^{-1} = g_{r+1-i}^{-1} \quad \text{for } i = 1, \ldots, r_2. \end{aligned}$$

We write $Z(G)^{1/2} = \{g \in G \mid g^2 \in Z(G)\}$. We state the results for configurations (R) and (C) only:

(R) Set $E_{r,G} = \{\boldsymbol{u} \in G^r \mid \exists g_0 \in Z(G)^{1/2};\ u_i^2 = g_0^2 \text{ for } i = 0, \dots, r-1\}/\sim_G$ and

$$I_{\boldsymbol{\chi}}^{\mathrm{mod}} = \sum_{\boldsymbol{u} \in E_{r,G}} \chi_1(u_0 u_1^{-1}) \chi_2(u_1 u_2^{-1}) \cdots \chi_r(u_{r-1} u_0^{-1}) \quad \text{for any } \boldsymbol{\chi} \in \mathrm{Irr}(G)^r,$$

$$n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r, 0) = \frac{1}{Z_1 \cdots Z_r} \sum_{\boldsymbol{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1) \cdots \chi_r(g_r)\, I_{\boldsymbol{\chi}}^{\mathrm{mod}}.$$

Then $\left|\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r, 0)\right| = n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r, 0)$.

(C) Set $A_\chi^{\mathrm{mod}} = \sum_{g_0 \in Z(G)^{1/2}/\sim_{Z(G)}} \alpha_{\chi, g_0}$ for any $\chi \in \mathrm{Irr}(G)$ and

$$n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s) = \frac{|C_1| \cdots |C_s|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-1}} A_\chi^{\mathrm{mod}}.$$

Then $\left|\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)\right| \le n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)$, with equality if $\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s) = \mathrm{SN}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)$.

3. Proofs

We give the proofs of Theorems 2.1 and 2.3 in detail; for Theorem 2.4, we just explain the main changes, in particular we give the description of $\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ we use so as to explain the definition of $\sim$. For a detailed proof of Theorem 2.4, see [Cadoret 2004].

Following Serre's method, we will compute $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|$ using the function

$$\epsilon = \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi,$$

which is 1 on 1_G and 0 elsewhere.

Lemma 3.1. *Given a finite group G, an irreducible character $\chi \in \mathrm{Irr}(G)$ and $g_1, \dots, g_n, u, v \in G$, we have*

$$\sum_{(\gamma_1, \dots, \gamma_n) \in G} \chi(u g_1^{\gamma_1} \cdots g_n^{\gamma_n} v) = \frac{|G|^n \prod_{i=1}^n \chi(g_i)}{\chi(1)^n} \chi(uv).$$

Proof. Let $R : G \to \mathrm{GL}(V)$ be a linear irreducible representation of G with character χ. Then

$$\sum_{\boldsymbol{\gamma} \in G} R(u g_1^{\gamma_1} \cdots g_n^{\gamma_n} v) = R(u) \Big(\sum_{\gamma_1 \in G} R(g_1^{\gamma_1}) \cdots \sum_{\gamma_n \in G} R(g_n^{\gamma_n}) \Big) R(v).$$

But, for any $g, h \in G$,

$$\sum_{\gamma \in G} R(g^\gamma)R(h) = \sum_{\gamma \in G} R(g^\gamma h) = \sum_{\gamma \in G} R(hg^{h^{-1}\gamma})$$
$$= R(h) \sum_{\gamma \in G} R(g^{h^{-1}\gamma}) = R(h) \sum_{\gamma \in G} R(g^\gamma).$$

So, according to Schur's lemma (see [Serre 1978, Chapter 2, Proposition 4], for instance):

$$\sum_{\gamma \in G} R(g^\gamma) = \lambda \operatorname{Id}_V \quad \text{with } \lambda = \frac{1}{\dim V} \operatorname{Tr}\Big(\sum_{\gamma \in G} R(g^\gamma) \Big) = \frac{|G|}{\chi(1)} \chi(g).$$

Consequently,

$$\sum_{\gamma_1 \in G} R(g_1^{\gamma_1}) \cdots \sum_{\gamma_n \in G} R(g_n^{\gamma_n}) = \frac{|G|^n \prod_{i=1}^n \chi(g_i)}{\chi(1)^n} \operatorname{Id}_V,$$

so

$$\sum_{\gamma \in G} R(u g_1^{\gamma_1} \cdots g_n^{\gamma_n} v) = \frac{|G|^n \prod_{i=1}^n \chi(g_i)}{\chi(1)^n} R(uv).$$

Taking traces yields the formula in the statement of the lemma. □

3.1. ***Real branch points.*** In the case of $\Sigma^{\mathbb{R}}(\boldsymbol{C}; r, 0)$, the defining conditions that $g_1 \cdots g_r = 1$ and that there exist $g_0 \in \operatorname{Inv}(G)$ satisfying (1–1) are equivalent to the condition

$$g_1 \cdots g_r = 1 \quad \text{and} \quad \exists g_0 \in G \text{ such that } (g_0 g_1 \cdots g_i)^2 = 1 \text{ for } i = 1, \ldots, r-1,$$

which in turn is equivalent to

$$\text{(3–1)} \quad g_1 = u_0 u_1, \ldots, g_{r-1} = u_{r-2} u_{r-1} \text{ and } g_r = u_{r-1} u_0 \text{ for some } (u_0, \ldots, u_{r-1}) \in \operatorname{Inv}(G)^r$$

(just take $u_i = g_0 \cdots g_i$ for $i = 0, \ldots, r-1$). In the rest of this subsection we will use the r-cycle $c = (0, \ldots, r-1) \in S_r$ to shorten the formulas. For instance, (3–1) can be rewritten as $g_{i+1} = u_i u_{c(i)}$ for $i = 0, \ldots, r-1$.

Now fix $g_1, \ldots, g_r \in G$ with $g_i \in C_i$ for $i = 1, \ldots, r$, and consider the set $E_{\boldsymbol{g}}$ of those r-tuples $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_r) \in G^r$ for which there is an r-tuple $(u_0, \ldots, u_{r-1}) \in \operatorname{Inv}(G)^r$ such that $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$ for $i = 0, \ldots, r-1$. The correspondence $\boldsymbol{\gamma} \to (g_1^{\gamma_1}, \ldots, g_r^{\gamma_r})$ provides a surjective map $E_{\boldsymbol{g}} \to \Sigma^{\mathbb{R}}(\boldsymbol{C}; r, 0)$. Two r-tuples $\boldsymbol{\gamma}, \boldsymbol{\gamma}' \in G^r$ have the same image if and only if ${\gamma_i}^{-1}\gamma_i' \in \operatorname{Cen}_G(g_i)$ for $i = 1, \ldots, r$. Thus

$$\big|\Sigma^{\mathbb{R}}(\boldsymbol{C}; r, 0)\big| = \frac{|E_{\boldsymbol{g}}|}{Z_1 \cdots Z_r},$$

which reduces the problem to computing $|E_{\boldsymbol{g}}|$.

To do so, we check for each $(\gamma_1, \dots, \gamma_r) \in G^r$ and each r-tuple $(u_0, \dots, u_{r-1}) \in \mathrm{Inv}(G)^r$, whether $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$ for $i = 0, \dots, r-1$, that is, whether

$$\prod_{i=0}^{r-1} \epsilon\left(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}\right) = 1.$$

However, we must take into account that for a given $\boldsymbol{\gamma} \in G^r$, distinct r-tuples $\boldsymbol{u}, \boldsymbol{u}' \in \mathrm{Inv}(G)^r$ can satisfy $g_{i+1}^{\gamma_{i+1}} = u_i u_{c(i)}$ for $i = 0, \dots, r-1$; this is equivalent to the condition $u_0 u_0' = u_1 u_1' = \cdots = u_{r-1} u_{r-1}'$, which can also be written

$$G \cdot (u_0, \dots, u_{r-1}) = G \cdot (u_0', \dots, u_{r-1}'),$$

where G acts on G^r by left translation. This defines the equivalence relation $\sim_G$ on $\mathrm{Inv}(G)^r$ that appears in the statement of Theorem 2.1.

Putting these remarks together we get

$$\begin{aligned} |E_{\boldsymbol{g}}| = \sum_{\substack{\boldsymbol{\gamma} \in G^r \\ \boldsymbol{u} \in \mathrm{Inv}(G)^r/\sim_G}} \prod_{i=0}^{r-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}) &= \sum_{\boldsymbol{u} \in \mathrm{Inv}(G)^r/\sim_G} \left(\sum_{\boldsymbol{\gamma} \in G} \prod_{i=0}^{r-1} \epsilon(u_i g_{i+1}^{\gamma_{i+1}} u_{c(i)}) \right) \\ &= \sum_{\boldsymbol{u} \in \mathrm{Inv}(G)^r/\sim_G} \left(\prod_{i=0}^{r-1} \sum_{\gamma \in G} \epsilon(u_i g_{i+1}^{\gamma} u_{c(i)}) \right). \end{aligned}$$

Using the formula $\epsilon = |G|^{-1} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1)\chi$ and Lemma 3.1 we obtain, for $i = 0, \dots, r-1$ and $\boldsymbol{u} \in \mathrm{Inv}(G)^r$,

$$\begin{aligned} \sum_{\gamma \in G} \epsilon(u_i g_{i+1}^{\gamma} u_{c(i)}) &= \frac{1}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \chi(1) \sum_{\gamma \in G} \chi(u_i g_{i+1}^{\gamma} u_{c(i)}) \\ &= \sum_{\chi \in \mathrm{Irr}(G)} \chi(g_{i+1}) \chi(u_i u_{c(i)}). \end{aligned}$$

Substituting this back into the previous formula leads to the announced result. Note that the generating condition $G = \langle u_0 u_1, \dots, u_{r-2} u_{r-1} \rangle$ can be taken into account to get $\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; r, 0)$: the only change then is that, in the sums above, the r-tuples $\boldsymbol{u}$ run over the subset of $\mathrm{Inv}(G)^r/\sim_G$ of those r-tuples $\boldsymbol{u}$ of representatives satisfying this extra generating condition. This yields the formula in Remark 2.2. □

3.2. ***Complex conjugate branch points.*** This time the conditions $g_1 \cdots g_r = 1$ and (1–1) (for some $g_0 \in \mathrm{Inv}(G)$) are equivalent to

$$g_1 \cdots g_{2s} = 1 \quad \text{and} \quad \exists g_0 \in G \text{ such that } g_0 g_i g_0 g_{2s+1-i} = 1 \text{ for } i = 1, \dots, s,$$

which in turn is equivalent to

(3–2) there exists $g_0 \in \mathrm{Inv}(G)$ such that $g_0 g_i g_0 g_{2s+1-i} = 1$ for $i = 1, \dots, s$ and $[g_1 \cdots g_s,\ g_0] = 1$

(where $[\ ,\ ]$ denotes the commutator, $[u,\ v] := uvu^{-1}v^{-1}$ for $u, v \in G$).

As above, fix $g_1, \dots, g_{2s} \in G$ with $g_i \in C_i$ for $i = 1, \dots, 2s$ and consider the set $E_{\boldsymbol{g}}$ of $2s$-tuples $\boldsymbol{\gamma} = (\gamma_1, \dots, \gamma_{2s}) \in G^r$ such that $g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma_{2s+1-i}} = 1$ for $i = 1, \dots, s$ and $[g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0] = 1$ for some $g_0 \in \mathrm{Inv}(G)$. Again, the correspondence $\boldsymbol{\gamma} \to (g_1^{\gamma_1}, \dots, g_{2s}^{\gamma_{2s}})$ provides a surjective map $E_{\boldsymbol{g}} \to \Sigma^{\mathbb{R}}(\boldsymbol{C}; 0, s)$, and two $2s$-tuples $\boldsymbol{\gamma}, \boldsymbol{\gamma}' \in G^r$ have the same image if and only if $\gamma_i^{-1}\gamma_i' \in \mathrm{Cen}_G(g_i)$ for $i = 1, \dots, 2s$. Consequently,

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = \frac{|E_{\boldsymbol{g}}|}{Z_1 \cdots Z_{2s}},$$

which reduces the problem to computing $|E_{\boldsymbol{g}}|$.

To do so, we check for each $(\gamma_1, \dots, \gamma_{2s}) \in G^{2s}$ and each $g_0 \in \mathrm{Inv}(G)$ whether $g_0\ g_i^{\gamma_i}\ g_0\ g_{2s+1-i}^{\gamma_{2s+1-i}} = 1$ for $i = 1, \dots, 2s$ and $[g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0] = 1$; in other words, whether

$$\epsilon\left([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]\right) \prod_{i=1}^{s} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma_{2s+1-i}}) = 1.$$

As in Section 3.1, note that for a given $\boldsymbol{\gamma} \in G^r$, distinct involutions $g_0, g_0' \in \mathrm{Inv}(G)$ can satisfy condition (3–2). This is equivalent to the condition $g_0 g_0' \in \mathrm{Cen}_G\left(g_1^{\gamma_1}, \dots, g_s^{\gamma_s}\right)$ or $\mathrm{Cen}_G\left(g_1^{\gamma_1}, \dots, g_s^{\gamma_s}\right).g_0 = \mathrm{Cen}_G\left(g_1^{\gamma_1}, \dots, g_s^{\gamma_s}\right).g_0'$. And since $Z(G) < \mathrm{Cen}_G\left(g_1^{\gamma_1}, \dots, g_s^{\gamma_s}\right)$, the preceding equivalent conditions are implied by $Z(G) \cdot g_0 = Z(G) \cdot g_0'$ (see Remark 3.2), where $\mathrm{Cen}_G\left(g_1^{\gamma_1}, \dots, g_s^{\gamma_s}\right)$ and $Z(G)$ act on G by left translation. Here again this gives the equivalence relation $\sim_{Z(G)}$ on $\mathrm{Inv}(G)$ appearing in the statement of Theorem 2.3.

Putting these remarks together we get

$$\begin{aligned}
|E_{\boldsymbol{g}}| &\le \sum_{\substack{\boldsymbol{\gamma} \in G^{2s} \\ g_0 \in \mathrm{Inv}(G)/\sim_{Z(G)}}} \epsilon\left([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]\right) \prod_{i=1}^{s} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma_{2s+1-i}}) \\
&\le \sum_{\substack{(\gamma_1, \dots, \gamma_s) \in G \\ g_0 \in \mathrm{Inv}(G)/\sim_{Z(G)}}} \epsilon\left([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]\right) \sum_{(\gamma_{s+1}, \dots, \gamma_{2s}) \in G} \prod_{i=1}^{s} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma_{2s+1-i}}) \\
&\le \sum_{\substack{(\gamma_1, \dots, \gamma_s) \in G \\ g_0 \in \mathrm{Inv}(G)/\sim_{Z(G)}}} \epsilon\left([g_1^{\gamma_1} \cdots g_s^{\gamma_s}, g_0]\right) \prod_{i=1}^{s} \sum_{\gamma \in G} \epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma}).
\end{aligned}$$

As before, Lemma 3.1 combined with the formula defining ϵ gives

$$\prod_{i=1}^{s}\sum_{\gamma\in G}\epsilon(g_0 g_i^{\gamma_i} g_0 g_{2s+1-i}^{\gamma}) = \prod_{i=1}^{s}\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_0 g_i^{\gamma_i} g_0)\chi(g_{2s+1-i}) = \prod_{i=1}^{s}\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_i)\chi(g_{2s+1-i}).$$

Hence we now have

$$|E_{\boldsymbol{g}}| \leq \Big(\sum_{\substack{(\gamma_1,\dots,\gamma_s)\in G\\ g_0\in \mathrm{Inv}(G)/\sim_{Z(G)}}}\epsilon\big([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]\big)\Big)\Big(\prod_{i=1}^{s}\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_i)\chi(g_{2s+1-i})\Big).$$

By definition, $[u,v]=1$ if and only if $u\in \mathrm{Cen}_G(v)$. Thus

$$\sum_{(\gamma_1,\dots,\gamma_s)\in G}\epsilon\big([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]\big) = \sum_{u\in\mathrm{Cen}_G(g_0)}\sum_{(\gamma_1,\dots,\gamma_s)\in G}\epsilon(g_1^{\gamma_1}\cdots g_s^{\gamma_s}u) = \sum_{u\in\mathrm{Cen}_G(g_0)}\frac{1}{|G|}\sum_{\chi\in\mathrm{Irr}(G)}\chi(1)\sum_{(\gamma_1,\dots,\gamma_s)\in G}\chi(g_1^{\gamma_1}\cdots g_s^{\gamma_s}u).$$

So, using Lemma 3.1 again,

$$\sum_{(\gamma_1,\dots,\gamma_s)\in G}\epsilon([g_1^{\gamma_1}\cdots g_s^{\gamma_s}, g_0]) = |G|^{s-1}\sum_{u\in\mathrm{Cen}_G(g_0)}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}}\chi(u) = |G|^{s-1}\sum_{\chi\in\mathrm{Irr}(G)}\frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}}\sum_{u\in\mathrm{Cen}_G(g_0)}\chi(u).$$

We recognize here $\alpha_{\chi,g_0} = \sum_{u\in\mathrm{Cen}_G(g_0)}\chi(u)$. Finally, we get

$$|E_{\boldsymbol{g}}| \leq |G|^{s-1}\Big(\prod_{i=1}^{s}\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_i)\chi(g_{2s+1-i})\Big)\Big(\sum_{\chi\in\mathrm{Irr}(G)}\frac{\prod_{i=1}^{s}\chi(g_i)}{\chi(1)^{s-1}}A_\chi\Big).$$

To end the proof, just recall that we have assumed $\big|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\big|\neq\varnothing$; this implies in particular that $C_i = C_{2s+i-1}^{-1}$ for $i=1,\dots,s$, so $Z_i = Z_{2s+1-i}$ and

$$\chi(g_i)\chi(g_{2s+1-i}) = |\chi(g_i)|^2,$$

whence

$$\sum_{\chi\in\mathrm{Irr}(G)}\chi(g_i)\chi(g_{2s+1-i}) = \sum_{\chi\in\mathrm{Irr}(G)}|\chi(g_i)|^2 = Z_i$$

for $i=1,\dots,s$, which leads to the announced result.

Remark 3.2. We only get an upper bound for $\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\right|$ because of the inclusions $Z(G) < \mathrm{Cen}_G\left(g_1^{\gamma_1},\dots,g_r^{\gamma_r}\right)$, which may be proper. But if $\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s) = \mathrm{SN}^{\mathbb{R}}(\boldsymbol{C};0,s)$, these inclusions become equalities and

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\right| = \left|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C};0,s)\right|.$$

3.3. ***Real and complex conjugate branch points.*** The method consists in rewriting the defining conditions $g_1\cdots g_r = 1$ and (1–1) as in the last two sections, but replacing $g_1\cdots g_{r_1} = 1$ and $g_{r_1+1}\cdots g_{r_1+2r_2} = 1$ by the weaker condition

$$g_1\cdots g_{r_1}g_{r_1+1}\cdots g_{r_1+2r_2} = 1.$$

So, in the general situation the defining conditions are equivalent to the existence of $g_0 \in \mathrm{Inv}(G)$ such that $g_1\cdots g_r = 1$, $(g_0g_1\cdots g_i)^2 = 1$ for $i = 1,\dots,r_1-1$, and $g_0g_{r_1+i}g_0g_{r+1-i} = 1$ for $i = 1,\dots,r_2$; this in turn is equivalent to

(3–3) there exists $(u_0,\dots,u_{r_1-1}) \in \mathrm{Inv}(G)^{r_1}$ such that

$$\begin{cases} u_0u_{r_1-1}g_{r_1}[g_{r_1+1}\cdots g_{r_1+r_2},u_0] = 1,\\ g_{i+1} = u_iu_{i+1} \text{ for } i = 0,\dots,r_1-2,\\ u_0\, g_{r_1+i}\, u_0\, g_{r+1-i} = 1 \text{ for } i = 1,\dots,r_2. \end{cases}$$

We still fix $g_1,\dots,g_r \in G$ with $g_i \in C_i$ for $i = 1,\dots,r$ and consider the set $E_{\boldsymbol{g},r_1,r_2}$ of those r-tuples $\boldsymbol{\gamma} = (\gamma_1,\dots,\gamma_{2s}) \in G^r$ such that $(g_1^{\gamma_1},\dots,g_r^{\gamma_r})$ satisfies condition (3–3). As above,

$$\left|\Sigma^{\mathbb{R}}(\boldsymbol{C};0,s)\right| = \frac{|E_{\boldsymbol{g},r_1,r_2}|}{Z_1\cdots Z_{2s}},$$

which once again reduces the problem to computing $|E_{\boldsymbol{g},r_1,r_2}|$. Then, for each $\boldsymbol{\gamma} = (\gamma_1,\dots,\gamma_r) \in G^r$, to decide whether $\boldsymbol{\gamma} \in E_{\boldsymbol{g},r_1,r_2}$, we check for every $\boldsymbol{u} = (u_0,\dots,u_{r_1-1}) \in \mathrm{Inv}(G)^{r_1}$ whether

$$\prod_{i=0}^{r_1-1}\epsilon(u_ig_{i+1}^{\gamma_{i+1}}u_{i+1})\prod_{i=1}^{r_2}\epsilon(u_0g_{r_1+i}^{\gamma_{r_1+i}}u_0g_{r+1-i}^{\gamma_{r+1-i}})\,\epsilon\left(u_0u_{r_1-1}g_{r_1}^{\gamma_{r_1}}[g_{r_1+1}^{\gamma_{r_1+1}}\cdots g_{r_1+r_2}^{\gamma_{r_1+r_2}},u_0]\right) = 1.$$

Now, the introduction of $\sim$ derives from the usual remarks about counting exactly once each element $\boldsymbol{\gamma} \in E_{\boldsymbol{g},r_1,r_2}$. Specifically, for all $(\gamma_1,\dots,\gamma_{r_1-1}) \in G^{r_1-1}$ and $\boldsymbol{u},\boldsymbol{u}' \in \mathrm{Inv}(G)^{r_1}$, the condition

$$u_ig_{i+1}^{\gamma_{i+1}}u_{i+1} = 1 = u_i'g_{i+1}^{\gamma_{i+1}}u_{i+1}',\ i = 0,\dots,r_1-1$$

is equivalent to $u_0u_0' = u_1u_1' = \cdots = u_{r_1-1}u_{r_1-1}'$, which can also be written $G.(u_0,\dots,u_{r_1-1}) = G.(u_0',\dots,u_{r_1-1}')$, where G acts on G^{r_1} by left translation. Likewise, for all $(\gamma_{r_1+1},\dots,\gamma_r) \in G^{2r_2}$ and $u_0,u_0' \in \mathrm{Inv}(G)$, the condition

$$u_0g_{r_1+i}^{\gamma_{r_1+i}}u_0 = (g_{r+1-i}^{\gamma_{r+1-i}})^{-1} = u_0'g_{r_1+i}^{\gamma_{r_1+i}}u_0',\ i = 1,\dots,r_2$$

is equivalent to

$$u_0 u_0' \in \mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big),$$

that is, $\mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big) \cdot u_0 = \mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big) \cdot u_0'$, which is implied by

$$N \cdot u_0 = N \cdot u_0',$$

where $N = \mathrm{Cen}_G\big(C_{r_1+1}, \ldots, C_{r_1+r_2}\big)$ is the centralizer of the subgroup generated by the conjugacy classes of $g_{r_1+1}, \ldots, g_{r_1+r_2}$ and both $\mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big)$ and N act on G by left translation.

Hence, for $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{r_1-1}) \in G^{r_1-1}$, let $\sim_{\boldsymbol{\gamma}}$ be the relation defined on $\mathrm{Inv}(G)^{r_1}$ as follows: for all $\boldsymbol{u}, \boldsymbol{u}' \in \mathrm{Inv}(G)^{r_1}$,

$$\boldsymbol{u} \sim_{\boldsymbol{\gamma}} \boldsymbol{u}' \Longleftrightarrow \mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big) \cdot u_0 = \mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big) \cdot u_0'$$
$$\text{and } G \cdot (u_0, \ldots, u_{r_1-1}) = G \cdot (u_0', \ldots, u_{r_1-1}'),$$

and write $\sim$ for the relation one gets by replacing $\mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big)$ with $\mathrm{Cen}_G(N)$ in the definition above. These relations are equivalence relations on $\mathrm{Inv}(G)^{r_1}$ and we obtain formula $n^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)$ in Theorem 2.4 by summing on the equivalence classes $\mathrm{Inv}(G)^{r_1}/\sim$.

Remark 3.3. When $N = \mathrm{Cen}_G\big(g_{r_1+1}^{\gamma_{r_1+1}}, \ldots, g_{r_1+r_2}^{\gamma_{r_1+r_2}}\big)$ for all $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_{r_1-1}) \in G$, the inequality in Theorem 2.4 becomes an equality.

4. Applications

Except in Section 4.2.2, we will always assume we are in the complex pair configuration (C). We keep the notations from Section 2, particularly concerning A_χ, A_χ^{mod}, and α_{χ,g_0}. In addition, say $\boldsymbol{C}$ is $\mathbb{C}g$*-complete symmetric* if

(1) $\Sigma(\boldsymbol{C}, G) = \mathrm{SN}(\boldsymbol{C}, G)$ and

(2) $\boldsymbol{C} = (C_1, \ldots, C_s, C_s^{-1}, \ldots, C_1^{-1})$ (and so $\Sigma^{\mathbb{R}}(\boldsymbol{C}; 0, s) \neq \varnothing$).

If (1) is replaced by

$(1)^{\mathbb{R}}$ $\Sigma^{\mathbb{R}}(\boldsymbol{C}; 0, s) = \mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; 0, s)$,

we say that $\boldsymbol{C}$ is $\mathbb{R}g$*-complete symmetric*. In the following computations we will always make the hypothesis $\boldsymbol{C}$ is $\mathbb{C}g$*-complete symmetric*. Clearly g-completeness implies (1), which implies $(1)^{\mathbb{R}}$. Under condition (1) one can use Serre's formula directly to compute $\big|\mathrm{SN}(\boldsymbol{C}, G)\big|$, and under condition $(1)^{\mathbb{R}}$ one can use the formula for $n^{\mathbb{R}}(\boldsymbol{C}; 0, s)$ to compute $\big|\mathrm{SN}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\big|$.

In the examples, we describe the $2s$-tuples $\boldsymbol{C}$ satisfying (2) using the notation $\boldsymbol{C} = \big[A_1^{(a_1)}, \ldots, A_n^{(a_n)}\big]$ to indicate that the $2s$-tuple $\boldsymbol{C}$ consists of

– s first entries, where A_i occurs a_i times for $i = n, \ldots, n$, (so $s = a_1 + \cdots + a_n$),

– s last entries which are the inverses of the first s ones, in reverse order.

When $\boldsymbol{C}$ is $\mathbb{C}$g-complete symmetric, Serre's formula becomes

$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right| = |Z(G)| \left(\frac{|C_1| \cdots |C_s|}{|G|}\right)^2 \sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|\chi(g_1)| \cdots \chi(g_s)|}{\chi(1)^{s-1}}\right)^2.$$

Hence

$$\frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|} = |C_1| \cdots |C_s| \frac{\displaystyle\sum_{\chi \in \mathrm{Irr}(G)} \left(\frac{|\chi(g_1)| \cdots |\chi(g_s)|}{\chi(1)^{s-1}}\right)^2}{\displaystyle\sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-1}} A_\chi}.$$

Remark. Note that $Z(G) = \bigcap_{\chi \in \mathrm{Irr}(G)} Z_\chi$, where $Z_\chi = \left\{g \in G \;\middle|\; |\chi(g)| = \chi(1)\right\}$, for $\chi \in \mathrm{Irr}\,(G)$, so, if $\boldsymbol{C}$ is g-complete symmetric, $\left|\Sigma(\boldsymbol{C}, G)\right|$ remains unchanged when adding central classes, whereas $\left|\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)\right|$ and $\left|\Sigma^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)\right|$ do not. So adding central classes in $\boldsymbol{C}$ can change the proportion

$$\frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|}$$

of G-covers defined over $\mathbb{R}$ (and with field of moduli contained in $\mathbb{R}$ as well).

4.1. ***G-covers that are not defined over their field of moduli.*** First we deal with the quaternion group $\mathbb{H}_8$, for which we exhibit G-covers not defined over their field of moduli. Then we generalize to obtain in particular a simple group-theoretic criterion for a finite group to be the Galois group of some G-cover not defined over its field of moduli. Lots of infinite families of groups satisfy this criterion.

4.1.1. *The quaternion group* $\mathbb{H}_8$. In the quaternion group $\mathbb{H}_8$ we have four non-trivial conjugacy classes: $A = \{-1\}$, $A_i = \{\pm i\}$, $A_j = \{\pm j\}$, $A_k = \{\pm k\}$. Take

$$\boldsymbol{C} = \left[A^{(x)}, A_i^{(a)}, A_j^{(b)}, A_k^{(c)}\right] \quad (\text{so } s = x + a + b + c.)$$

To compute $n^{\mathbb{R}}(\boldsymbol{C}; 0, s)$, note that $\mathrm{Inv}(\mathbb{H}_8)/\sim_{Z(\mathbb{H}_8)} = \{1\}$. Thus $A_\chi = \alpha_{\chi,1} = 8$ if $\chi = \chi_1$ and $A_\chi = 0$ otherwise, which leads to

$$n^{\mathbb{R}}(\boldsymbol{C}; 0, s) = 2^{a+b+c}, \quad \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^{a+b+c-2}, \quad \left|\overline{\mathrm{sn}}(\boldsymbol{C}, \mathbb{H}_8)\right| = 2^{2(a+b+c)-3},$$

$$\frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, \mathbb{H}_8)\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|} = 2^{a+b+c-1},$$

$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}, \mathbb{H}_8)\right| - \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^{a+b+c-2}(2^{a+b+c-1} - 1).$$

If $a = b = 1$ and $x = c = 0$, so that $r = 2s = 4$, we get $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, \mathbb{H}_8)\right| = 2$ and $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, 2)\right| = 1$.[1] This gives rise to a new example of a G-cover with group $\mathbb{H}_8$ not defined over its field of moduli (recall that such an example was already given by K. Coombes and D. Harbater [1985, p. 831], but with three rational branch points $(1, 2, 3)$ and canonical inertia invariant $\boldsymbol{C} = (\{\pm i\}, \{\pm j\}, \{\pm k\})$.) We give a precise argument in Section 4.1.2, but the general idea is that, given the branch points $(z_1, z_2, \bar{z}_2, \bar{z}_1) \in \mathcal{U}^r$ with z_1, z_2 not real, the fiber $(\psi'_{4,\mathbb{H}_8})^{-1}((z_1, z_2, \bar{z}_2, \bar{z}_1))$ consists of two points P'_1, P'_2 corresponding to two G-covers f_1, f_2, one of which, say f_1, is defined over $\mathbb{R}$ and the other one, f_2, is not. If $P_1 = \Pi_4(P'_1)$ and $P_2 = \Pi_4(P'_2)$ are the corresponding points on $\mathcal{H}_{4,\mathbb{H}_8}(\boldsymbol{C})$ then, $P_1^c = P_1$ forces $P_2^c = P_2$ so P_2 is a real point; thus f_2 has its field of moduli contained in $\mathbb{R}$.

We can also use formula $n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)$, which is more precise. For this, note that $Z(\mathbb{H}_8)^{1/2}/\sim_{Z(\mathbb{H}_8)} = \mathbb{H}_8/\sim_{Z(\mathbb{H}_8)} = \{1, i, j, k\}$, so $A_\chi^{\mathrm{mod}} = \alpha_{\chi,1} + \alpha_{\chi,i} + \alpha_{\chi,j} + \alpha_{\chi,1} = 20$ if $\chi = \chi_1$ and $A_\chi^{\mathrm{mod}} = 4$ otherwise, which leads to

$$n^{\mathrm{mod}\,\mathbb{R}}(\boldsymbol{C}; 0, s) = 2^{a+b+c-1} \times (5 + (-1)^{b+c} + (-1)^{a+c} + (-1)^{a+b}),$$
$$\left|\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^{a+b+c-3} \times (5 + (-1)^{b+c} + (-1)^{a+c} + (-1)^{a+b}).$$

Taking $a = b = 1$ and $x = c = 0$ gives $\left|\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, 2)\right| = 2$, as expected. But we get more, since

$$\begin{aligned}\Delta^{\mathrm{mod}}(\boldsymbol{C}; 0, s) &:= \left|\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s)\right| - \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| \\ &= 2^{a+b+c-3}(3 + (-1)^{b+c} + (-1)^{a+c} + (-1)^{a+b}) > 0,\end{aligned}$$

so there are exactly $\Delta^{\mathrm{mod}}(\boldsymbol{C}; 0, s)$ G-covers in $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)$ that are not defined over $\mathbb{R}$ but have field of moduli contained in $\mathbb{R}$.

4.1.2. *General criteria.* With the usual notations, write

$$\Delta^{\mathrm{mod}}(\boldsymbol{C}; r_1, r_2) = \left|\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| - \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right|.$$

When $\boldsymbol{C}$ is $\mathbb{R}$g-complete symmetric and $(r_1, r_2) = (r, 0)$ or $(0, s)$, we have

$$\Delta^{\mathrm{mod}}(\boldsymbol{C}; r_1, r_2) = n^{\mathrm{mod}\,\mathbb{R}}(\boldsymbol{C}; r_1, r_2) - n^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2).$$

Thus we obtain the following simple criterion:

Proposition 4.1.3. *Let G be a finite group. For any $\mathbb{R}$g-complete r-tuple $\boldsymbol{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in G and for any r-tuple*

$$\boldsymbol{t}' = (t_1, \ldots, t_r) \in \mathcal{U}^r(\mathbb{R})$$

[1] Explicit representatives: $\mathrm{sni}(\boldsymbol{C}, \mathbb{H}_8) = \{(i, j, -j, -i), (i, j, j, i)\}$, $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, 2) = \{(i, j, -j, -i)\}$.

with $t_1 < \cdots < t_r$, of all the isomorphism classes of G-covers in the straight Nielsen class $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ with ordered branch point set $\boldsymbol{t}'$, exactly

$$\Delta^{\mathrm{mod}}(\boldsymbol{C}; r, 0) = \frac{|Z(G)|}{|G|Z_1 \cdots Z_r} \sum_{\boldsymbol{\chi} \in \mathrm{Irr}(G)^r} \chi_1(g_1) \cdots \chi_r(g_r)(I_{\boldsymbol{\chi}}^{\mathrm{mod}} - I_{\boldsymbol{\chi}})$$

have field of moduli contained in $\mathbb{R}$ but are not defined over $\mathbb{R}$.

Similarly, for any $\mathbb{R}$g-complete symmetric r-tuple $\boldsymbol{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in G and for any r-tuple $\boldsymbol{t}' = (z_1, \ldots, z_s, \bar{z}_s, \ldots, \bar{z}_1) \in \mathcal{U}^r(\mathbb{C})$ with z_i not real, $i = 1, \ldots, s$, of all the isomorphism classes of G-covers in the straight Nielsen class $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ with ordered branch point set $\boldsymbol{t}'$, exactly

$$\Delta^{\mathrm{mod}}(\boldsymbol{C}; 0, s) = \frac{|C_1| \cdots |C_s|}{[G : Z(G)]|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\chi(g_1) \cdots \chi(g_s)}{\chi(1)^{s-1}} (A_\chi^{\mathrm{mod}} - A_\chi)$$

have field of moduli contained in $\mathbb{R}$ but are not defined over $\mathbb{R}$.

This proposition shows in particular that, once a $\mathbb{R}$g-complete symmetric canonical inertia invariant $\boldsymbol{C}$ and a branch point configuration — (R) or (C) — are given, the number of G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$ can be computed explicitly and is independent of the branch points.

Corollary 4.1.4. *Given a finite group G, there are G-covers with group G and branch point configuration (C) with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$ if and only if $Z(G)$ has an element which is a square in G but not in $Z(G)$.*

Proof. We compute $A_\chi^{\mathrm{mod}} - A_\chi = \sum_{g_0} \alpha_{\chi, g_0}$ for any $\chi \in \mathrm{Irr}(G)$, where g_0 ranges over a system of representatives of the set $Z(G)^{1/2}/\!\sim_{Z(G)} \backslash \mathrm{Inv}(G)/\!\sim_{Z(G)}$. For this, just note that for all $g_0 \in Z(G)^{1/2}$ there exists $z \in Z(G)$ such that $(zg_0)^2 = 1$ (that is, $Z(G)g_0 \in \mathrm{Inv}(G)/\!\sim_{Z(G)}$) if and only if g_0^2 is a square in $Z(G)$. Consequently, setting

$$E_G = \left\{ g_0 \in Z(G)^{1/2} \mid g_0^2 \notin \{z^2\}_{z \in Z(G)} \right\},$$

we get

$$A_\chi^{\mathrm{mod}} - A_\chi = \sum_{g_0 \in E_G/\sim_{Z(G)}} \alpha_{\chi, g_0}.$$

Also, it follows from their definition that the α_{χ, g_0} are nonnegative integers, and for $\chi = \chi_1$ they also are nonzero ($\alpha_{\chi_1, g_0} = |\mathrm{Cen}_{g_0}(G)|$), so the $A_\chi^{\mathrm{mod}} - A_\chi$ are nonnegative integers. Now, suppose there is a $\mathbb{R}$g-complete symmetric $2s$-tuple $\boldsymbol{C}$ of nontrivial conjugacy classes of G such that $\Delta^{\mathrm{mod}}(\boldsymbol{C}; 0, s) > 0$. Then there is $\chi \in \mathrm{Irr}(G)$ such that $A_\chi^{\mathrm{mod}} - A_\chi > 0$, which obviously implies $E_G \neq \varnothing$.

Conversely, let $C_1, \ldots, C_s$ be a listing of all the nontrivial conjugacy classes in G and set $\boldsymbol{C} = (C_1, C_1^{-1}, \ldots, C_s, C_s^{-1}, C_s, C_s^{-1}, \ldots, C_1, C_1^{-1})$. This $2s$-tuple is

$\mathbb{C}$g-complete symmetric. Thus one gets

$$\begin{aligned}\Delta^{\mathrm{mod}}(\boldsymbol{C};0,s) &= \frac{\big(|C_1|\cdots|C_s|\big)^2}{[G:Z(G)]\,|G|}\sum_{\chi\in\mathrm{Irr}(G)}\frac{|\chi(g_1)|^2\cdots|\chi(g_s)|^2}{\chi(1)^{2s-1}}(A_\chi^{\mathrm{mod}}-A_\chi)\\ &= \frac{\big(|C_1|\cdots|C_s|\big)^2}{[G:Z(G)]\,|G|}\Bigg(\sum_{\substack{\chi\in\mathrm{Irr}(G)\\ \deg(\chi)=1}}(A_\chi^{\mathrm{mod}}-A_\chi)\\ &\qquad + \sum_{\substack{\chi\in\mathrm{Irr}(G)\\ deg(\chi)>1}}\frac{|\chi(g_1)|^2\cdots|\chi(g_s)|^2}{\chi(1)^{2s-1}}(A_\chi^{\mathrm{mod}}-A_\chi)\Bigg),\end{aligned}$$

and, since $E_G\neq\varnothing$, $A_{\chi_1}^{\mathrm{mod}}-A_{\chi_1}=\sum_{g_0\in E_G/\sim_{Z(G)}}|\operatorname{Cen}_{g_0}(G)|>0$. □

Remarks. (a) Corollary 4.1.4 can be proved directly, only using the definitions of $\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C};0,s)$ and $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C};0,s)$; see [Cadoret 2004]. This alternate proof uses the same $4s$-tuple $\boldsymbol{C}$, which appears naturally in the proof above, to construct a G-cover in $\overline{\mathrm{sn}}^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C};0,s)\setminus\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C};0,s)$.

(b) Lots of groups satisfy the condition of Corollary 4.1.4, and therefore are groups of G-covers not defined over their field of moduli. For instance:

- $\mathrm{Gl}_n(p^m)$ with $n\geq 2$, $m\geq 1$, $p\geq 3$ prime,
- D_{2n} with $n\geq 4$ such that $4\,|\,n$,
- $\mathrm{O}_2(p^m,\mathrm{q}^h)$ with $m\geq 1$, $p\geq 3$ prime and q^h the hyperbolic form on $\mathbb{F}_{p^m}^2$,
- any group G such that $\mathrm{Inv}(G)\subset Z(G)$ and $[G:Z(G)]$ is even; for instance, $\mathrm{Sl}_2(p^m)$ with $m\geq 1$, $p\geq 3$ irreducible, T_{4n} with $n\geq 2$, etc.

To my knowledge, the only example of families of G-covers not defined over their field of moduli and in which the group G can be taken arbitrarily large was given by S. Wewers [2002]. The group is $\mathrm{Sl}_2(p)$ for $p\not\equiv\pm1$ modulo 8 an odd prime, the canonical inertia invariant is $(4A, pA, pB)$ and the branch points are (t_1,t_2,t_3), where $t_1\in\mathbb{Q}$ and $\{t_2,t_3\}$ is $\mathbb{Q}$-rational.

Computing $\Delta^{\mathrm{mod}}(\boldsymbol{C};r_1,r_2)$ can be difficult. The following proposition gives a weaker but more practical criterion for the existence of G-covers not defined over their field of moduli. We give here the statement and proof for situation (C) but it can immediately be generalized to situations (R) and (R-C).

Proposition 4.1.5. *Suppose given a finite group G and a symmetric $2s$-tuple $\boldsymbol{C}$ of nontrivial conjugacy classes in G. If $\big|\overline{\mathrm{sn}}(\boldsymbol{C},G)\big|-\big|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C};0,s)\big|$ is odd then for any $2s$-tuple of branch points $\boldsymbol{t}'=(z_1,\ldots,z_s,\bar z_s,\ldots,\bar z_1)\in\mathcal{U}^{2s}(\mathbb{C})$ with z_i not real for $i=1,\ldots,s$, there is in $\overline{\mathrm{sn}}(\boldsymbol{C},G)$ at least one isomorphism class of G-covers with field of moduli contained in $\mathbb{R}$ but not defined over $\mathbb{R}$.*

Proof. Write $m = \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|$ and $n = \left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|$. Let $P'_1, \ldots, P'_m$ be the points in $(\psi'_{2s,G})^{-1}(\boldsymbol{t}')$ corresponding to the G-covers that are defined over $\mathbb{R}$, and $P'_{m+1}, \ldots, P'_n$ the points corresponding to the G-covers that are not. Set $P_i = \Pi_{2s}(P'_i)$ for $i = 1, \ldots, n$, and also $E = \{P_1, \ldots, P_m\}$, $F = \{P_{m+1}, \ldots, P_n\}$. So, with $\boldsymbol{t} = \pi_{2s}(\boldsymbol{t}')$ we have $E \cup F \subset (\psi_{2s,G})^{-1}(\boldsymbol{t})$. Then observe that $E \cup F = \Pi_{2s}((\psi'_{2s,G})^{-1}(\boldsymbol{t}'))$ is left invariant by complex conjugation c. Indeed $(\psi'_{2s,G})^{-1}(\boldsymbol{t}')$ is the set of all G-covers f for which C_i is the inertia canonical class associated with z_i and C_i^{-1} is the inertia canonical class associated with $\bar{z}_i = z_{2s+1-i}$ for $i = 1, \ldots, s$, whereas $(\psi'_{2s,G})^{-1}(\boldsymbol{t}')^c$ is the set of all G-covers f^c for which, by Fried's branch cycle argument, C_i^{-1} is the inertia canonical class associated with $\bar{z}_i = z_{2s+1-i}$ and $(C_i^{-1})^{-1} = C_i$ is the inertia canonical class associated with $\bar{\bar{z}}_i = z_i$ for $i = 1, \ldots, s$. Now, since $P_1, \ldots, P_m$ are real points on $(\psi_{2s,G})^{-1}(\boldsymbol{t})$, we have $E^c = E$, which forces $F^c = F$. Hence, $|F|$ being odd, F has at least one point P invariant under c. This point P is real, which means it corresponds to an isomorphism class of G-covers with field of moduli contained in $\mathbb{R}$ but, by the definition of F, not defined over $\mathbb{R}$. □

4.1.6. *Dicyclic groups T_{4n} of order $4n$.* We turn to an application of the preceding proposition. The quaternion group $\mathbb{H}_8$ is the first term of the family of dicyclic groups $(T_{4n})_{n\geq 2}$. The group T_{4n} has the presentation

$$T_{4n} = \langle a, b \mid a^{2n} = 1,\ a^n = b^2,\ b^{-1}ab = a^{-1}\rangle,$$

and contains $n + 2$ nontrivial conjugacy classes:

- n classes $A_1, \ldots, A_n$ with $A_i = \{a^i, a^{-i}\}$ for $i = 1, \ldots, n$ (and $A_n = \{a^n\}$);
- $B_1 = \{a^{2j}b\}_{0\leq j\leq n-1}$ and $B_2 = \{a^{2j+1}b\}_{0\leq j\leq n-1}$.

Take

$$\boldsymbol{C} = \left[A_n^{(\alpha_n)}, A_1^{(\alpha_1)}, \ldots, A_{n-1}^{(\alpha_{n-1})}, B_1^{(\beta_1)}, B_2^{(\beta_2)}\right]$$

and write $\alpha = \alpha_1 + \cdots + \alpha_n$, so $s = \alpha + \beta_1 + \beta_2$. Then $\mathrm{Inv}(T_{4n})/\sim_{Z(T_{4n})} = \{1\}$; consequently $A_\chi = \alpha_{\chi,1} = 4n$ if $\chi = \chi_1$ and $A_\chi = 0$ otherwise. Using the character tables of these groups, which can be found in [James and Liebeck 1993, p. 385], and taking into account that we need $\beta_1 + \beta_2 \geq 1$ for $\boldsymbol{C}$ to be g-complete, we obtain

$$n^{\mathrm{mod},\mathbb{R}}(\boldsymbol{C}; 0, s) = 2^\alpha n^{\beta_1+\beta_2}, \quad \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^{\alpha-1}n^{\beta_1+\beta_2-1},$$

$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}, T_{4n})\right| = 2^{2\alpha-1}n^{2(\beta_1+\beta_2)-2}, \quad \frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, T_{4n})\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|} = 2^\alpha n^{\beta_1+\beta_2-1},$$

$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}, T_{4n})\right| - \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^{\alpha-1}n^{\beta_1+\beta_2-1}(2^\alpha n^{\beta_1+\beta_2-1} - 1).$$

Suppose $\alpha_1 = 1$, $\beta_1 \geq 1$, $\beta_2 \geq 0$, and $\alpha_1 = \cdots = \alpha_n = 0$. Then $\boldsymbol{C}$ is g-complete symmetric and $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, T_{4n})\right| - \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}, T_{4n})\right| = n^{\beta_1+\beta_2-1}(2n^{\beta_1+\beta_2-1} - 1)$ is odd

when n is (and, if $\beta_1 + \beta_2 = 1$, it is always odd). So, for each $n \geq 2$, for each $\boldsymbol{t} = \{z_1, \bar{z}_1, \ldots, z_s, \bar{z}_s\} \in \mathcal{U}_r(\mathbb{R})$ with z_i not real for $i = 1, \ldots, s$, there is at least one isomorphism class of G-cover f_n with ramification type $[T_{4n}, \boldsymbol{C}, \boldsymbol{t}]$ that is not defined over $\mathbb{R}$ but has its field of moduli contained in $\mathbb{R}$.

4.2. ***Descent from*** $\mathbb{C}$ ***to*** $\mathbb{Q}^{\mathrm{tr}}$**.** We give here a combinatorial method to determine if a finite group G admits G-covers defined over $\mathbb{Q}^{\mathrm{tr}}$ with a prescribed ramification type $[G, \boldsymbol{C}, \boldsymbol{t}]$. For this, we look for r-tuples $\boldsymbol{C}$ of nontrivial conjugacy classes in G such that $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r_1, r_2)\right| = \left|\overline{\mathrm{sn}}(\boldsymbol{C}, G)\right|$. If there is such a $\boldsymbol{C}$ and if $\boldsymbol{t} \in \mathcal{U}_r(\mathbb{R})$, the image on $\mathcal{H}_{r,G}(\boldsymbol{C})$ of the fiber $(\psi'_{r,G})^{-1}(\boldsymbol{t}') \cap \mathcal{H}'_{r,G}(\boldsymbol{C})$ above an ordering $\boldsymbol{t}'$ of $\boldsymbol{t}$ (conforming to the Convention on page 56) consists of real points; we denote it by

$$E^0_{r,G,\boldsymbol{t}}(\boldsymbol{C}) := \Pi_r\left((\psi'_{r,G})^{-1}(\boldsymbol{t}') \cap \mathcal{H}'_{r,G}(\boldsymbol{C})\right) \subset (\psi_{r,G})^{-1}(\boldsymbol{t}).$$

Now write

$$E_{r,G,\boldsymbol{t}}(\boldsymbol{C}) := \bigcup_{\substack{m \geq 1 \\ (|G|,m)=1}} E^0_{r,G,\boldsymbol{t}}(\boldsymbol{C}^m).$$

If $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}^m; r_1, r_2)\right| = \left|\overline{\mathrm{sn}}(\boldsymbol{C}^m, G)\right|$ for any $m \geq 1$ such that $(|G|, m) = 1$, then $E_{r,G,\boldsymbol{t}}(\boldsymbol{C})$ consists of real points. But, if we also assume $\boldsymbol{t} \in \mathcal{U}_r(\mathbb{Q})$, Fried's branch cycle argument asserts that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ stabilizes $E_{r,G,\boldsymbol{t}}(\boldsymbol{C})$. So any point in this set is $\mathbb{Q}^{\mathrm{tr}}$-rational.

Here we will only deal with dihedral groups D_{2n} with n odd, in configurations (R) and (C). We show for instance that for any odd integer $n \geq 3$ and for any $r \geq 3$, D_{2n} is the Galois group of a regular extension of $\mathbb{Q}^{\mathrm{tr}}(X)$ with exactly r rational branch points (compare [Dèbes and Fried 1994, Conjecture 5.2], for instance). In configuration (C), we can only assert that this occurs with 4 branch points.

4.2.1. *Configuration (C).* Recall that D_{2n} has the presentation

$$D_{2n} = \langle u, v \mid u^n = v^2 = 1, vuv = v^{-1} \rangle$$

and has $\frac{1}{2}(n+1)$ nontrivial conjugacy classes:

- $\frac{1}{2}(n-1)$ classes $A_1, \ldots, A_{(n-1)/2}$ with $A_i = \{u^i, u^{-i}\}$ for $i = 1, \ldots, \frac{1}{2}(n-1)$, and
- $B = \{vu^i\}_{0 \leq i \leq n-1}$.

Now, take

$$\boldsymbol{C} = \left[A_1^{(a_1)}, \ldots, A_{(n-1)/2}^{(a_{(n-1)/2})}, B^{(b)}\right] \quad (\text{so } s = a_1 + \cdots + a_{(n-1)/2} + b),$$

and write $a = a_1 + \cdots + a_{(n-1)/2}$. Here $\mathrm{Inv}(D_{2n})/\sim_{Z(D_{2n})} = \{1, \{vu^i\}_{0\le i\le n-1}\}$, so

$$\alpha_{\chi,1} = \begin{cases} 2n & \text{if } \chi = \chi_1, \\ 0 & \text{otherwise,} \end{cases} \qquad \alpha_{\chi,v} = \begin{cases} 0 & \text{if } \chi = \chi_2, \\ 2 & \text{otherwise,} \end{cases}$$

where χ_2 is the irreducible character of D_{2n} defined by $\chi_2(u^k) = 1$ for $k = 1, \ldots, n$ and $\chi_2(v) = -1$. So we get $A_{\chi_1} = 4n$, $A_{\chi_2} = 0$ and $A_\chi = 2n$ if $\chi \neq \chi_1, \chi_2$, which, noticing that for $\boldsymbol{C}$ to be g-complete symmetric we need $b \ge 1$, leads to

$$n^{\mathbb{R}}(\boldsymbol{C}; 0, s) = 2^{a+1}n^b, \quad \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right| = 2^a n^{b-1},$$
$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})\right| = 2^{2a-1}n^{2b-2}, \quad \frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, s)\right|} = 2^{a-1}n^{b-1}.$$

For instance, if $a_1 = b = 1$ and $a_2 = \cdots = a_{n-1/2} = 0$, we get

$$\left|\overline{\mathrm{sn}}(\boldsymbol{C}^m, D_{2n})\right| = 2 = \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}^m; 0, s)\right|$$

for all $m \ge 1$ such that $(2n, m) = 1$. As a result, if we choose a $2s$-tuple of branch points $\boldsymbol{t} = (z_1, \ldots, z_s, \bar{z}_s, \ldots, \bar{z}_1) \in \mathcal{U}^r(\mathbb{C})$ whose associated divisor is rational, the discussion above shows that any point in $E_{4,D_{2n},\boldsymbol{t}}(\boldsymbol{C})$ is a $\mathbb{Q}^{\mathrm{tr}}$-point and, since $Z(D_{2n}) = \langle 1\rangle$, we conclude all the G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})$ are defined over $\mathbb{Q}^{\mathrm{tr}}$. Notice that $\boldsymbol{C} = (C_1, C_v, C_v, C_1)$ is not rational, so all the G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})$ are defined over $\mathbb{Q}^{\mathrm{tr}}$ but none of them is over $\mathbb{Q}$.

Remark. Generalizing the situation above, one gets the following descent criterion: *For any finite group G, for any r-tuple $\boldsymbol{C} = (C_1, \ldots, C_r)$ of nontrivial conjugacy classes in G, for any $\boldsymbol{t}^0 \in \mathcal{U}^r$ whose associated branch point divisor is rational, the conditions*

(1) $Z(G) = 1$ *and*

(2) $\left|\overline{\mathrm{sn}}(\boldsymbol{C}^n, G)\right| = \left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}^n; r_1, r_2)\right|$ *for any $n \ge 1$ such that $(|G|, n) = 1$*

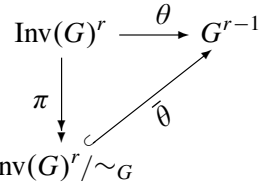
imply that all the G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, G)$ are defined over $\mathbb{Q}^{\mathrm{tr}}$.

Condition (2) can even be replaced by one that is easier to check when $\boldsymbol{C}$ is not g-complete:

(2)′ $\left|\Sigma(\boldsymbol{C}^n, G)\right| = \left|\Sigma^{\mathbb{R}}(\boldsymbol{C}^n; r_1, r_2)\right|$ and $\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}^n; r_1, r_2) \neq \varnothing$ for any $n \ge 1$ such that $(|G|, n) = 1$.

4.2.2. *Configuration (R).* The example we give here corresponds to situation (R). For any $r \ge 3$ we exhibit G-covers with group D_{2n} defined over $\mathbb{Q}^{\mathrm{tr}}$ (but not over $\mathbb{Q}$) and with r rational branch points. The example illustrates the difficulties one

can encounter when trying to compute $n^{\mathbb{R}}(\boldsymbol{C}; r, 0)$ directly. We will use the commutative diagram



where π is the canonical surjection and θ is the map given by the correspondence $(u_0, \dots, u_{r-1}) \to (u_0u_1, u_1u_2, \dots, u_{r-2}u_{r-1})$. Rewrite $n^{\mathbb{R}}(\boldsymbol{C}; r, 0)$ as

$$\begin{aligned} n^{\mathbb{R}}(\boldsymbol{C}; r, 0) &= \frac{1}{Z_1 \cdots Z_r} \sum_{\substack{\chi_1, \dots, \chi_r \in \mathrm{Irr}(G) \\ (u_0, \dots, u_{r-1}) \in \mathrm{Inv}(G)^r/\sim_G}} \prod_{1 \le i \le r} (\chi_i(g_i)\chi_i(u_{i-1}u_{c(i-1)})) \\ &= \frac{1}{Z_1 \cdots Z_r} \sum_{(u_0, \dots, u_{r-1}) \in \mathrm{Inv}(G)^r/\sim_G} \prod_{1 \le i \le r} \Big(\sum_{\chi \in \mathrm{Irr}(G)} \chi(g_i)\chi(u_{i-1}u_{c(i-1)}) \Big), \end{aligned}$$

where c denotes the r-cycle $(0, 1, \dots, r-1)$, as in Section 3.1. Also recall the general form of Serre's formula:

$$\big|\Sigma(\boldsymbol{C}, G)\big| = \frac{|C_1| \cdots |C_r|}{|G|} \sum_{\chi \in \mathrm{Irr}(G)} \frac{\prod_{1 \le i \le r} \chi(g_i)}{\chi(1)^{r-2}}.$$

When $G = D_{2n}$ we have $\overline{\chi} = \chi$ for any irreducible character $\chi \in \mathrm{Irr}(D_{2n})$, so

$$\sum_{\chi \in \mathrm{Irr}(G)} \chi(g_i)\chi(u_{i-1}u_{c(i-1)}) = \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(g_i)}\chi(u_{i-1}u_{c(i-1)})$$

is equal to Z_i if g_i and $u_{i-1}u_{c(i-1)}$ are conjugate and is equal to 0 otherwise, for $i = 1, \dots, r$. Consequently, the only tuples $\boldsymbol{u} = (u_0, \dots, u_{r-1}) \in \mathrm{Inv}(G)/\sim_G$ we will need in our computation are $\big(\bar{\theta}^{-1}(g_1^{\gamma_1}, \dots, g_{r-1}^{\gamma_{r-1}})\big)_{\gamma_1, \dots, \gamma_{r-1} \in G}$, when they exist. So,

$$n^{\mathbb{R}}(\boldsymbol{C}; r, 0) = \frac{1}{Z_r} \sum_{\boldsymbol{u} \in \bar{\theta}^{-1}(C_1 \times \cdots \times C_{r-1})} \sum_{\chi \in \mathrm{Irr}(G)} \overline{\chi(g_r)}\chi(u_{r-1}u_0).$$

With the notations of Section 4.2.1, we now apply these remarks to the specific r-tuple

$$\boldsymbol{C} = (B, A_{i_1}, \dots, A_{i_t}, B) \text{ (so } r = t + 2),$$

where we choose $1 \le i_1, \dots, i_t \le \frac{1}{2}(n-1)$, so that $\boldsymbol{C}$ is g-complete. A representative of $\bar{\theta}^{-1}(vu^k, u^{\epsilon_1 i_1}, \dots, u^{\epsilon_t i_t})$ is $(1, vu^k, vu^{k+\epsilon_1 i_1}, \dots, vu^{k+\epsilon_1 i_1 + \cdots + \epsilon_t i_t})$, with $k = 0, \dots, n-1$ and $\epsilon_1, \dots, \epsilon_t \in \{\pm 1\}$. Since $u_{r-1}u_0 = vu^{k+\epsilon_1 i_1 + \cdots + \epsilon_t i_t} \in B$, we

obtain

$$n^{\mathbb{R}}(\boldsymbol{C}; r, 0) = \frac{1}{2^2 n^t} \sum_{\epsilon_1,\dots,\epsilon_t \in \{\pm 1\}} \sum_{k=0}^{n-1} 2 \times n^t \times 2 = 2^t n.$$

Hence $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}^m; r, 0)\right| = 2^{t-1}$ for all $m \geq 1$ such that $(2n, m) = 1$, and at the same time, by Serre's formula, $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})\right| = 2^{t-1}$. So if we fix a r-tuple of rational branch points $\boldsymbol{t} = (t_1, \dots, t_r) \in \mathcal{U}^r(\mathbb{Q})$, using the same argument as above we conclude that all the G-covers in $\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})$ are defined over $\mathbb{Q}^{\mathrm{tr}}$. Moreover choosing for instance $i_1 = \cdots = i_t = 1$, we can assert those G-covers are not defined over $\mathbb{Q}$.

Remark. The computation we made above can be generalized to any tuple

$$\boldsymbol{C} = \left(B, A_{i_{1,1}}, \dots, A_{i_{1,u_1}}, B, B, A_{i_{2,1}}, \dots, A_{i_{2,u_2}}, B, B, \dots, B, A_{i_{t,1}}, \dots, A_{i_{t,u_t}}, B\right)$$

with $r = 2t + u_1 + \cdots + u_t$; we obtain $\left|\mathrm{sn}^{\mathbb{R}}(\boldsymbol{C}; r, 0)\right| = 2^{u_1+\cdots+u_t-1} n^{t-1}$ and $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})\right| = 2^{u_1+\cdots+u_t-1} n^{2t-2}$, so

$$\frac{\left|\overline{\mathrm{sn}}(\boldsymbol{C}, D_{2n})\right|}{\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; r, 0)\right|} = n^{t-1},$$

which only depends on t.

4.2.3. *$\mathbb{Q}^{\mathrm{tr}}$-realizations of D_{2a^∞} with $a \geq 3$ odd.* The results obtained in Sections 4.2.1 and 4.2.2 do not depend on $n \geq 3$ odd, which yields regular realizations of the profinite groups

$$D_{2a^\infty} := \limproj_{n \to +\infty} D_{2a^n} \simeq \mathbb{Z}_a \times_s \mathbb{Z}/2\mathbb{Z},$$

for $a \geq 3$ odd, over $\mathbb{Q}^{\mathrm{tr}}(X)$. Indeed, for any $a \geq 3$ odd and any $n \geq 1$, write

- $A_{1,a,n}, \dots, A_{a^n-1/2,a,n}$ with $A_i = \{u^i, u^{-i}\}$, $i = 1, \dots, \frac{1}{2}(a^n - 1)$,
- $B_{a,n} = \{v u^i\}_{0 \leq i \leq a^n - 1}$,

for the $\frac{1}{2}(a^n + 1)$ nontrivial conjugacy classes of D_{2a^n}. Also set

$$\boldsymbol{C}_{a,n} = (A_{1,a,n}, B_{a,n}, B_{a,n}, A_{1,a,n}).$$

This gives rise to a tower of Hurwitz spaces

$$\cdots \longrightarrow \mathcal{H}'_{4, D_{2a^{n+1}}}(\boldsymbol{C}_{a,n+1}) \xrightarrow{\psi'_{4, D_{2a^{n+1}}}} \mathcal{H}'_{4, D_{2a^n}}(\boldsymbol{C}_{a,n}) \xrightarrow{\psi'_{4, D_{2a^n}}} \cdots$$

$$\cdots \xrightarrow{\psi'_{4, D_{2a^2}}} \mathcal{H}'_{4, D_{2a}}(\boldsymbol{C}_{a,1}).$$

Fix $\boldsymbol{t}' = (z_1, \bar{z}_1, z_2, \bar{z}_2) \in \mathcal{U}^4(\mathbb{C})$ with $z_i \in \mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$ and $\{z_i, \bar{z}_i\} \in \mathcal{U}_2(\mathbb{Q})$, for $i = 1, 2$, and consider the projective system of finite sets of $\mathbb{Q}^{\mathrm{tr}}$-points (see Section

4.2.1)

$$\cdots \longrightarrow \Pi_4(\mathscr{H}'_{4,D_{2a^{n+1}}}(\boldsymbol{C}_{a,n+1})_{\boldsymbol{t}'}) \xrightarrow{\psi_{4,D_{2a^{n+1}}}} \Pi_4(\mathscr{H}'_{4,D_{2a^n}}(\boldsymbol{C}_{a,n})_{\boldsymbol{t}'}) \xrightarrow{\psi_{4,D_{2a^n}}} \cdots$$
$$\cdots \xrightarrow{\psi_{4,D_{2a^2}}} \Pi_4(\mathscr{H}'_{4,D_{2a^1}}(\boldsymbol{C}_{a,1})_{\boldsymbol{t}'}).$$

Then $\lim\text{proj}_{n\to+\infty} \Pi_4\big(\mathscr{H}'_{4,D_{2a^n}}(\boldsymbol{C}_{a,n})_{\boldsymbol{t}'}\big)$ is nonempty, and any element of this projective limit corresponds to a regular Galois realization of D_{2a^∞} over $\mathbb{Q}^{\mathrm{tr}}(X)$ (see [Cadoret 2004, § 5.3.1]) with branch points $\boldsymbol{t}'$ and inertia canonical invariant

$$(A_{1,a,\infty}, B_{a,\infty}, B_{a,\infty}, A_{1,a,\infty}),$$

where $B_{a,\infty} = \{vu^i\}_{i\geq 0}$ and $A_{i,a,\infty} = \{u^i, u^{-i}\}$ for $i \geq 1$.

Likewise, using the results of Section 4.2.2, one gets regular Galois realizations of D_{2a^∞} over $\mathbb{Q}^{\mathrm{tr}}(X)$ with rational branch points $\boldsymbol{t}' = (t_1, \ldots, t_{t+2}) \in \mathscr{U}^{t+2}(\mathbb{Q})$ and inertia canonical invariant $(B_{a,\infty}, A_{i_1,a,\infty}, \ldots, A_{i_t,a,\infty}, B_{a,\infty})$, where $i_1, \ldots, i_t \geq 1$ such that, for instance, $(i_j, a) = 1$ for $j = 1, \ldots, t$.

4.3. ***The Mathieu group M_{11}.*** Our formulas are manageable even for more complicated groups, particularly in the branch point configuration (C). Our last example concerns the Mathieu group M_{11}.

According to the Atlas [Conway et al. 1985], $|M_{11}| = 11.5.3^2.2^4$ and M_{11} has 10 conjugacy classes: $1A$, $2A$, $3A$, $4A$, $5A$, $6A$, $8A$, B^*, $11A$, B^{**}. The difficulty here is to compute $\mathrm{Cen}_{M_{11}}(2A)$. We apply Theorem 2.3 to the specific 4-tuple (8A,B*,11A,B**) to do this. We will use that $\big|\mathrm{Cen}_{M_{11}}(2A)\big| = 3.2^4$ and that any 2-Sylow S_2 of $\mathrm{Cen}_{M_{11}}(2A)$ is semidihedral of order 16, in symbols

$$S_2 = \langle x, a \mid x^2 = 1 = a^8, xax = a^3\rangle = \mathrm{SD}_{16}$$

(see [Robinson 1982, Ex. 7.4.4, p. 205]) to prove the following lemma, needed to carry out computations of $n^{\mathbb{R}}(\boldsymbol{C}; 0, s)$.

Lemma. $\mathrm{Cen}_{M_{11}}(2A)$ *contains* 1 *element of order* 1, 13 *elements of order* 2, 8 *elements of order* 3, 6 *elements of order* 4, 8 *elements of order* 6, *and* 12 *elements of order* 8 (6 *in each conjugacy class*).

First, note that SD_{16} contains:

- 4 elements of order 8: a, a^3, a^5, a^7;
- 6 elements of order 4: a^2, a^6, xa, xa^3, xa^5, xa^7;
- 5 elements of order 2: a^4, xa^2, xa^4, xa^6, x;
- 1 element of order 1.

Moreover, $Z(\mathrm{SD}_{16}) = \langle a^4\rangle$ and SD_{16} has 3 kinds of subgroups of index 2: $\mathbb{Z}/8\mathbb{Z} = \langle a\rangle$, $D_8 = \langle a^2, x\rangle$, $\mathbb{H}_8 = \langle a^2, xa\rangle$.

We are now able to describe $\mathrm{Cen}_{M_{11}}(2A)$ more precisely. According to the Atlas, there is an unsplit short exact sequence

$$1 \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow \mathrm{Cen}_{M_{11}}(2A) \xrightarrow{\theta} S_4 \longrightarrow 1.$$

So, since the center of S_4 is trivial, we get the inclusions $\langle 2A\rangle \subset Z(\mathrm{Cen}_{M_{11}}(2A)) \subset \mathbb{Z}/2\mathbb{Z}$, which obviously are equalities. Consequently, for all $\sigma \in S_4$:

- If σ has order 1 or 3 then $\theta^{-1}(\sigma)$ contains an element of same order and an element of twice this order.
- If σ has order 2 then $\theta^{-1}(\sigma)$ contains either two elements of order 2 or two elements of order 4 or two elements of order 6. Let n denote the number of elements of order 6 we obtain this way ($0 \leq n \leq 6$).
- If σ has order 4 then $\theta^{-1}(\sigma)$ contains either two elements of order 4 or two elements of order 8.

In particular, we have exactly 8 elements of order 3 and $8+n$ elements of order 6 in $\mathrm{Cen}_{M_{11}}(2A)$. All the other ones have order 1, 2, 4 or 8, so are contained in the 2-Sylow subgroups of $\mathrm{Cen}_{M_{11}}(2A)$. Write n_p for the number of p-Sylows in $\mathrm{Cen}_{M_{11}}(2A)$. From the above we deduce $n_3 = 4$. Furthermore, since $n_2 \,|\, 3$ and n_2 is odd we have $n_2 = 1, 3$. But if $n_2 = 1$, $\left|\mathrm{Cen}_{M_{11}}(2A)\right| = 32+n$, a contradiction; hence $n_2 = 3$. Still according to the Atlas, $\mathrm{Cen}_{M_{11}}(2A)$ contains a normal subgroup V of order 8, and as the 2-Sylows of $\mathrm{Cen}_{M_{11}}(2A)$ are conjugate, we get $S \cap T = V$ for all $S, T \in \mathcal{S}_2(\mathrm{Cen}_{M_{11}}(2A))$. Consequently, computing the order of $\mathrm{Cen}_{M_{11}}(2A)$ we now get $\left|\mathrm{Cen}_{M_{11}}(2A)\right| = 48+n$, which leads to $n = 0$. There are three possibilities for V:

$\underline{V = \mathbb{Z}/8\mathbb{Z}}$ and $\mathrm{Cen}_{M_{11}}(2A)$ has 1 element of order 1, 13 of order 2, 8 of order 3, 14 of order 4, 8 of order 6, 4 of order 8 (2 in each conjugacy class).

$\underline{V = D_8}$ and we have in $\mathrm{Cen}_{M_{11}}(2A)$: 1 element of order 1, 5 of order 2, 8 of order 3, 14 of order 4, 8 of order 6, 12 of order 8 (6 in each conjugacy class).

$\underline{V = \mathbb{H}_8}$ and we have in $\mathrm{Cen}_{M_{11}}(2A)$: 1 element of order 1, 13 of order 2, 8 of order 3, 6 of order 4, 8 of order 6, 12 of order 8 (6 in each conjugacy class).

Here are the computations corresponding to these three possibilities:

	A_{χ_1}	A_{χ_2}	A_{χ_3}	A_{χ_4}	A_{χ_5}	A_{χ_6}	A_{χ_7}	A_{χ_8}	A_{χ_9}	$A_{\chi_{10}}$
$V = \mathbb{Z}/8\mathbb{Z}$	15840	10560	0	0	7920	0	0	15840	2640	5280
$V = D_8$	15840	7920	2640	2640	2640	0	0	10560	5280	7920
$V = \mathbb{H}_8$	15840	7920	0	0	7920	0	0	15840	0	7920

Finally, since the maximal subgroups of M_{11} have order 720, 660, 144, 120, 48 and none of these orders can be divided by both 8 and 11, we conclude that (8A, B*, 11A, B**) is g-complete symmetric. Now, the first two configurations give $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, 2)\right| = \frac{538}{3}$ and $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, 2)\right| = \frac{536}{3}$, respectively, whereas the third one gives $\left|\overline{\mathrm{sn}}^{\mathbb{R}}(\boldsymbol{C}; 0, 2)\right| = 180$. So $V = \mathbb{H}_8$, which gives a description of the centralizer of the involution class in M_{11}. For this 4-uple Serre's formula gives $\left|\overline{\mathrm{sn}}(\boldsymbol{C}, M_{11})\right| = 8752$.

Acknowledgment

I thank P. Dèbes for encouraging me to write this paper and making many helpful suggestions.

References

[Cadoret 2004] A. Cadoret, *ThÃ©orie de Galois inverse et arithmÃ©tique des espaces de Hurwitz*, Thèse de doctorat, Université Lille I, 2004.

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Oxford, 1985. MR 88g:20025 Zbl 0568.20001

[Coombes and Harbater 1985] K. Coombes and D. Harbater, "Hurwitz families and arithmetic Galois groups", *Duke Math. J.* **52**:4 (1985), 821–839. MR 87g:14012 Zbl 0601.14023

[Dèbes 1995] P. Dèbes, "Covers of $\mathbf{P}^1$ over the p-adics", pp. 217–238 in *Recent developments in the inverse Galois problem* (Seattle, 1993), edited by M. D. Fried et al., Contemp. Math. **186**, Amer. Math. Soc., Providence, 1995. MR 96g:12005 Zbl 0856.12004

[Dèbes and Douai 1997] P. Dèbes and J.-C. Douai, "Algebraic covers: field of moduli versus field of definition", *Ann. Sci. École Norm. Sup.* (4) **30**:3 (1997), 303–338. MR 98k:11081 Zbl 0906.12001

[Dèbes and Fried 1994] P. Dèbes and M. D. Fried, "Nonrigid constructions in Galois theory", *Pacific J. Math.* **163**:1 (1994), 81–122. MR 95c:12008 Zbl 0788.12001

[Fried 1995] M. D. Fried, "Introduction to modular towers: generalizing dihedral group–modular curve connections", pp. 111–171 in *Recent developments in the inverse Galois problem* (Seattle, 1993), edited by M. D. Fried et al., Contemp. Math. **186**, Amer. Math. Soc., Providence, RI, 1995. MR 97a:11070 Zbl 0957.11047

[Fried and Völklein 1991] M. D. Fried and H. Völklein, "The inverse Galois problem and rational points on moduli spaces", *Math. Ann.* **290**:4 (1991), 771–800. MR 93a:12004 Zbl 0763.12004

[James and Liebeck 1993] G. James and M. Liebeck, *Representations and characters of groups*, Cambridge University Press, Cambridge, 1993. MR 94h:20007 Zbl 0792.20006

[Malle and Matzat 1999] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer, Berlin, 1999. MR 2000k:12004 Zbl 0940.12001

[Robinson 1982] D. J. S. Robinson, *A course in the theory of groups*, Graduate Texts in Mathematics **80**, Springer, New York, 1982. MR 84k:20001 Zbl 0483.20001

[Serre 1978] J.-P. Serre, *Représentations linéaires des groupes finis*, Third ed., Hermann, Paris, 1978. Fifth edition, 1998. MR 80f:20001 Zbl 0926.20003

[Serre 1992] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics **1**, Jones and Bartlett, Boston, 1992. MR 94d:12006 Zbl 0746.12001

[Völklein 1996] H. Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics **53**, Cambridge University Press, Cambridge, 1996. MR 98b:12003 Zbl 0868.12003

[Weil 1956] A. Weil, "The field of definition of a variety", *Amer. J. Math.* **78** (1956), 509–524. Reprinted as pp. 291–306 in *Oeuvres scientifiques*, vol. II, Springer, Berlin, 1979. MR 18,601a Zbl 0072.16001

[Wewers 2002] S. Wewers, "Field of moduli and field of definition of Galois covers", pp. 221–245 in *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, 1999), edited by M. D. Fried and Y. Ihara, Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, RI, 2002. MR 2004a:14016 Zbl 1024.12006

Received July 25, 2003. Revised January 13, 2004.

ANNA CADORET
UNIV. LILLE 1, MATHÉMATIQUES
59655 VILLENEUVE D'ASCQ CEDEX
FRANCE
cadoret@math.jussieu.fr