NONRIGID CONSTRUCTIONS IN GALOIS THEORY
PIERRE DEBES AND MICHAEL D. FRIED

The context for this paper is the Inverse Galois Problem. First we give an if and only if condition that a finite group is the group of a Galois regular extension of $\mathbb{R}(X)$ with only real branch points. It is that the group is generated by elements of order 2 (Theorem 1.1 (a)). We use previous work on the action of the complex conjugation on covers of $\mathbb{P}^1$. We also show each finite group is the Galois group of a Galois regular extension of $\mathbb{Q}^r(X)$. Here $\mathbb{Q}^r$ is the field of all totally real algebraic numbers (Theorem 5.7). Sections 1, 2, and 3 discuss consequences, generalizations, and related questions.

The second part of the paper, §4 and §5, concerns descent of fields of definition from $\mathbb{R}$ to $\mathbb{Q}$. Use of Hurwitz families reduces the problem to finding $\mathbb{Q}$-rational point on a special algebraic variety. Our first application considers realizing the symmetric group $S_m$ as the group of a Galois extension of $\mathbb{Q}(X)$, regular over $\mathbb{Q}$, satisfying two further conditions. These are that the extension has four branch points, and it also has some totally real residue class field specializations. Such extensions exist for $m = 4, 5, 6, 7, 10$ (Theorem 4.11).

Suppose that $m$ is a prime larger than 7. Theorem 5.1 shows that the dihedral group $D_m$ of order $2m$ is not the group of a Galois regular extension of $\mathbb{Q}(X)$ with fewer than 6 branch points. The proof interprets realization of certain dihedral group covers as corresponding to rational points on modular curves. We then apply Mazur’s Theorem. New results of Kamienny and Mazur suggest that no bound on the number of branch points will allow realization of all $D_m$'s.

0.1. Description of Theorem 1.1. Throughout, $\mathbb{C}$ denotes the complex number field, $X$ an indeterminate, and $\overline{\mathbb{C}(X)}$ a fixed algebraic closure of $\mathbb{C}(X)$. Let $k$ be a subfield of $\mathbb{C}$. We say a finite extension $Y/k(X)$ with $\overline{\mathbb{C}(X)} \supset Y$ is regular over $k$ if $\overline{k} \cap Y = k$. Equivalently $[Y: k(X)] = [Y\mathbb{C}: \mathbb{C}(X)]$. Denote this degree by $n$. Regard the degree $n$ field extension $Y\mathbb{C}/\mathbb{C}(X)$ as the function field extension of a degree $n$ cover $\varphi: Y_C \to \mathbb{P}^1$. Here $\mathbb{P}^1$ is the complex projective line and $Y_C$ is an irreducible non-singular curve.

The map $\varphi$ is ramified over a finite number of points $x_1, \ldots, x_r$. We call these the branch points of the cover (or of the extension $Y/k(X)$). Our first result (Theorem 1.1(a)) shows exactly when a finite group $G$ is the group of a Galois regular extension of $\mathbb{R}(X)$ with only real branch points.
This happens if and only if $G$ is generated by involutions.

Theorem 1.1 uses formulas for the action of complex conjugation on the fundamental group of $\mathbb{P}^1 \setminus \{x_1, \ldots, x_r\}$ (cf. §2.3). Hurwitz [Hur] knew these. Krull and Neukirch investigated them further [KN]. Still, no one has exploited this simple statement about groups generated by involutions.

0.2. Relations with the inverse Galois problem. Here is a weak version of the Inverse Galois problem. Does each group occur as the Galois group of a field extension of $\mathbb{Q}$? As do others, we approach this through its geometric analog. That is, we consider it over $\mathbb{Q}(X)$ rather than $\mathbb{Q}$. This is a descent problem. Suppose we are given a group $G$, a suitably large integer $r$, and $r$ points $x_1, \ldots, x_r \in \mathbb{P}^1(\mathbb{C})$. Topology then constructs a Galois extension of $\mathbb{C}(X)$ with Galois group $G$ and branch points $x_1, \ldots, x_r$. One must then restrict the scalars from $\mathbb{C}$ to $\mathbb{Q}$. Theorem 1.1 gives a form of descent from $\mathbb{C}$ to $\mathbb{R}$. Proposition 2.3 and Comment 3 of §3.5 refine these for specific applications (see §0.4).

We stress the condition on the branch points. Theorem 1.1 (a) shows that Galois groups occur over $\mathbb{Q}$ (or even $\mathbb{R}$) using $r$ branch points in $\mathbb{P}^1(\mathbb{R})$ only if $r$ elements of order 2 generate $G$. Therefore, in practice, classical "rigidity" [Se3; Theorem 9.1] realizes only groups over $\mathbb{Q}(X)$ that are generated by 3 elements of order 2.

Corollary 1.2 is another consequence of Theorem 1.1 (a). Each finite group has a totally nonsplit cover (cf. §1.2) that is not the Galois group of a regular extension of $\mathbb{R}(X)$ with only real branch points. Nevertheless, every finite group is the Galois group of a regular extension of $\mathbb{R}(X)$, with branch points consisting of complex conjugate pairs ([Se3; Ex. p. 107] or Theorem 3.1). Theorem 5.7 notes that each finite group is the Galois group of a regular extension of $\mathbb{Q}^\text{tr}(X)$. Here $\mathbb{Q}^\text{tr}$ is the field of all totally real algebraic numbers.

0.3. Extension of Theorem 1.1. Theorem 1.1 (b) applies to not necessarily Galois extensions. Finite group $G$ is the monodromy group of a cover $\phi: Y_\mathbb{C} \to \mathbb{P}^1$ defined over $\mathbb{R}$ with only real branch points if and only if

\begin{equation*}
G \text{ has an automorphism } h \text{ and a system of generators } 
\alpha_1, \ldots, \alpha_s \text{ such that } h(\alpha_i) = \alpha_i^{-1} \text{ for } i = 1, \ldots, s.
\end{equation*}

Of course, (*) holds if $G$ is generated by elements of order 2. Sections 1.2–1.5 have a more complete discussion on (*) and related
conditions. In particular, we discuss the persistence of property (\(*\)). Given a group \(G\) satisfying (\(*\)), when does there exist a totally non-split cover of \(G\) that does not satisfy (\(*\)) (§1.5).

Notation and basic tools appear in §2. Classical identifications in the theory of covers appear in §2.1 and §2.2. Skip these on a first reading. Sections 3.1–§3.4 give the proof of Theorem 1.1. The final descent argument for the constructive part (\(\Leftarrow\)) uses Weil’s general criterion. This says that the field of moduli (§2.4) \(K\) of a cover is a field of definition if a certain cocycle condition holds. We add an observation to a result of Coombes and Harbater [CoH] for Galois covers (Theorem 2.4 (ii)). Thus, \(K\) is also a field of definition for the \(G\)-cover; the cover and its automorphisms can be defined over \(K\).

This method is natural, but perhaps intricate. Serre suggested simplifying this using the algebraic fundamental group rather than the classical topological fundamental group. Section 3.6 gives a second proof of Theorem 1.1 (a) following Serre’s viewpoint. This is constructive. Assume we have a group \(G\) and generators of \(G\) with property (\(*\)). We give an explicit description, in terms of “branch cycles,” of a cover \(\varphi: Y_C \rightarrow \mathbb{P}^1\) that has the properties stated in Theorem 1.1 (b). Furthermore, we can force this cover to have some fibers of only real points.

0.4. Enhanced applications. The topological action of complex conjugation \(c\) induces its arithmetic action. (Section 3.7 has a precise formulation.) We note that no naive \(p\)-adic analog of this representation of complex conjugation holds for the Frobenius \(F_p \in G(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)\) (§3.7).

Comment 3 in §3.5 answers a question of E. Dew in his thesis [D]. In so doing it refines the technique of descending from \(C\) to \(\mathbb{R}\). Consider the field of moduli \(K\) of a \(G\)-cover when \(K\) is a number field. How can we effectively decide if each completion of \(K\) is a field of definition of the \(G\)-cover? We give iff conditions for the field of moduli, on one hand, and the field of definition, on the other, of a \(G\)-cover to be (in) \(\mathbb{R}\). Dew has started an investigation of a local-global question for the field of moduli being a field of definition. Knowing the answer over each local place (including infinite places) does not answer the global question.

Descent to \(\mathbb{Q}\) appears in §4. We consider \(G = S_m\) and specific choices of 3 generators of order 2. Then, we investigate if certain 4 branch point covers \(\varphi: Y_C \rightarrow \mathbb{P}^1\) derived from Theorem 1.1 can be defined over \(\mathbb{Q}\). “Rigidity assumptions” from [Se3; Ch. 8, 9] do not
apply. They rarely do when there are 4 (or more) branch points.

In §4.1 and §4.2, we recall from [Frl] how to handle nonrigid cases.
When \( r = 4 \), Hurwitz family ideas reduce the problem to finding a rational point on a certain curve \( C(C) \). Section 4.3 gives a formula for the genus of \( C(C) \). We can answer our original question about \( S_m \) when the curve \( C(C) \) has genus 0. Our computation shows this happens exactly when \( m = 4, 5, 6, 7, 10 \). So, for these values of \( m \), we realize the symmetric group \( S_m \) as the Galois group of a regular extension of \( \mathbb{Q}(X) \) with 4 branch points and with some totally real residue class specializations (Theorem 4.11). Serre noted, with 3 branch points instead of 4, only one centerless group, \( G = S_3 \), had the same property [Se2].

We do not know how to improve on our sporadic 3 generator cases to draw the conclusion of Theorem 4.11 for an infinite number of groups. Descent from \( \mathbb{R} \) to \( \mathbb{Q} \) is the difficulty because we must find rational points on low dimensional Hurwitz spaces. Even with easy groups this is a difficult obstruction. For example, the dihedral group \( D_m \) of order \( 2m \) is generated by 2 elements of order 2.

Consider a prime \( m > 7 \). Theorem 5.1 shows that \( D_m \) requires covers with at least 6 branch points to be realized as the Galois group of a regular extension of \( \mathbb{Q}(X) \). Mazur has formulated conjectures that imply that realization of all \( D_m \)'s will require an unbounded number of branch points [KM]. We borrow some of his formulation from an e-mail discussion with him.

0.5. **Acknowledgments.** David Harbater made expositional simplifications in our proof on Comment 3—Dew's question—in §3. In addition, much of the proof of Theorem 2.4 (§2.4) is implicit in the result in [CH]. Our concern is with Property (ii) which was not stated there.

1. **First results and consequences.** Let \( Y/K(X) \) be a regular extension of degree \( n \) and \( \phi: Y_C \rightarrow \mathbb{P}^1 \) the associated cover. That is, \( Y_C \) is the set of places of the field \( Y_C \) and \( \phi \) is the natural restriction of places—points of \( \mathbb{P}^1 \)—to \( C(X) \). Branch points \( x_1, \ldots, x_r \) are the places ramified in the extension \( Y_C/C(X) \).

1.1. **Statement of Theorem 1.1.** Let \( x_0 \) be a point in \( \mathbb{P}^1(\mathbb{R}) \backslash \{x_1, \ldots, x_r\} \). Denote the fundamental group

\[
\pi - 1(\mathbb{P}^1 \backslash \{x_1, \ldots, x_r\}, x_0)
\]

for short by \( \pi_1 \). There is a natural action \( T \) of \( \pi_1 \) called the *monodromy action* on the points of the fiber \( \phi^{-1}(x_0) \). For its description,
start with $[\gamma]$, the homotopy class of a closed path based at $x_0$. Then $T([\gamma])$ permutes $\varphi^{-1}(x_0)$; it maps $y \in \varphi^{-1}(x_0)$ to $T([\gamma])(y)$, the terminal point of the unique lift of $\gamma$ through $\varphi$ with initial point $y$.

The permutation $T([\gamma])$ is independent of the representative of $[\gamma]$. Fix a labeling $y_1, \ldots, y_n$ of the points of the fiber $\varphi^{-1}(x_0)$. Regard $T$ as an action $T: \pi_1 \to S_n$ of $\pi_1$ on the integers $1, \ldots, n$. Up to conjugation by an element of $S_n$, this action does not depend on labeling the $y_i$'s or on the base point $x_0$. Call the group $T(\pi_1)$ the monodromy group of the cover. This defines a subgroup of $S_n$ up to conjugation by elements of $S_n$.

**Theorem 1.1.** (a) Consider a finite group $G$. It is the group of a regular Galois extension of $\mathbb{R}(X)$ with only real branch points exactly when

\[
G \text{ is generated involutions.}
\]

(b) Furthermore, $G$ is the monodromy group of a cover $\varphi: Y_C \to \mathbb{P}^1$ defined over $\mathbb{R}$ with only real branch points if and only if

\[
\exists h \in \text{Aut}(G), \exists \alpha_1, \ldots, \alpha_s \in G \mid 
\langle \alpha_1, \ldots, \alpha_s \rangle = G, \ h(\alpha_i) = \alpha_i^{-1}, \quad i = 1, \ldots, s.
\]

**Addition to Theorem 1.1 (a).** We can take the number of generating involutions of $G$ equal to the number of branch points of the regular Galois extension of $\mathbb{R}(X)$ in the statement.

**Addition to Theorem 1.1 (b).** The cover $\varphi: Y_C \to \mathbb{P}^1$ defined over $\mathbb{R}$ produced in §3.3 for the only if part of (b) has branch cycles

\[
(\alpha_1, \alpha_1^{-1}\alpha_2, \ldots, \alpha_{s-1}^{-1}\alpha_s, \alpha_s^{-1})
\]

(cf. §2.3). It is Galois over $\mathbb{C}$. Indeed, it is Galois over $\mathbb{R}$ if $h$ is induced by conjugation by $h' \in G$ with $h'$ of order 2.

1.2. **Group theoretical conditions.** As noted, (1.1) $\Rightarrow$ (1.2). The converse is false: abelian groups distinct from $(\mathbb{Z}/2)^m$ satisfy (1.2) but not (1.1). For example, the cyclic group $\mathbb{Z}/m$ is the monodromy group of the Galois cover $\varphi: \mathbb{P}^1 \to \mathbb{P}^1$ given by $\varphi(y) = y^m$. For $m \neq 2$, it is defined over $\mathbb{R}$ with only real branch points. Yet, the corresponding function field extension $\mathbb{R}(y)/\mathbb{R}(y^m)$ is not Galois.

Consider two further conditions.

(1.3) $G$ is a subgroup of $G'$ with $[G': G] = 2$, and $G'$ is generated by involutions in $G' \setminus G$. 


Further: If \( h' \in G \) of order 2 induces \( h \), then \( G \) is generated by involutions.

\((1.4)\) \( G = \mathbb{Z}/2 \) or \( \text{Aut}(G) \) is of even order.

We now show \((1.1) \Rightarrow (1.2) \Leftrightarrow (1.3) \Rightarrow (1.4)\).

\((1.2) \Rightarrow (1.3)\). Define \( G' \) to be \( G' = G \times \langle h \rangle \) the semi-direct product of \( G \) and the group generated by the automorphism \( h \). The elements \( (\alpha_i, h), \ i = 1, \ldots, s \), and \( h \) generate \( G' \) and they are of order 2:

\[
(\alpha_i, h)(\alpha_i, h) = (\alpha_i h(\alpha_i), h^2) = (\alpha_i \alpha_i^{-1}, 1) = 1.
\]

Also, \( (\alpha_i, h) \in G' \setminus G \). Suppose \( h \) is represented by inner automorphism by an element \( h' \in G \) with \( h' \) of order 2. Then \( G \) is generated by involutions; include \( h' \) with \( \alpha_i h' \), \( i = 1, \ldots, s \).

\((1.2) \Leftrightarrow (1.3)\). Consider the situation where \( g_0, g_1, \ldots, g_r \) are involutions in \( G' \setminus G \) that generate \( G' \). Then, \( \beta_i = g_0 g_i, \ i = 1, \ldots, r \), are in \( G \). Clearly, \( g_0 \) conjugates them to their inverses: \( g_0(g_0 g_i)g_0 = g_0 g_i g_0 = (g_0 g_i)^{-1} \). We have only to check if they generate \( G \).

Take \( H \) to be the subgroup that the \( \beta_i \)s generate. We show \( G \) is the union of the cosets of \( H \) and \( g_0 H \) to conclude the proof. Do an induction on elements of \( G \) presented as words \( g_i \cdots g_i \) in the \( g_i \)\s. Assume words of length at most \( t - 1 \) are in one of the cosets \( H \) or \( g_0 H \). Now do cases for \( g_i \cdots g_i = \sigma \) in \( H \) or \( g_0 H \). If \( \sigma \in H \), then \( g_0 g_i \sigma \) is also in \( H \). Multiply by \( g_0 \) to see \( g_i \sigma \in g_0 H \). On the other hand, if \( \sigma \in g_0 H \), then multiply by \( (g_i g_0) g_0 \) to get \( g_i \sigma \) in \( H \). We’re done.

\((1.3) \Rightarrow (1.4)\) Suppose \( G' \) contains \( \tau \) of order 2 not in the centralizer \( \text{Cen}_{G'}(G) \) in \( G' \). Then, conjugation by \( \tau \) is an automorphism of \( G \) of order 2. Thus, \( |\text{Aut}(G)| \) is even. Assume all elements of \( G' \) of order 2 are in \( \text{Cen}_{G'}(G) \). Pick an element \( a \) of order 2 from \( G' \setminus G \). Then \( a \in \text{Cen}_{G'}(G) \). Therefore, \( G' \) is the direct product \( G \times \langle a \rangle \) and involutions—\( au \) with \( u \) running over involutions of \( G' \setminus G \)—generate \( G \). Since those generators of \( G \) are also in \( \text{Cen}_{G'}(G) \), the group \( G \) is abelian. Conclude: \( |\text{Aut}(G)| \) is even unless \( G = \mathbb{Z}/2 \).

So, groups distinct from \( \mathbb{Z}/2 \), with odd order automorphism group, are not monodromy groups of a cover over \( \mathbb{R} \) with only real branch points. Here is how to get such a group. Consider a \( p \)-group \( P \) with \( p \) odd. Then, \( \text{Aut}(P) \) acts on the frattini quotient module \( P/[P, P]P^p \) with kernel a \( p \)-group [Hu; Satz 3.17, p. 274]. There exists \( P \) with any desired nontrivial representation occurs in the frattini quotient [BK; Th. 1]. In particular, choose \( P \) so that its automorphism group is odd.
1.3. A corollary of Theorem 1.1. Recall that a cover of a group $G$ is a surjective homomorphism $\psi: F \to G$. The cover is finite if $F$ is a finite group. It is totally nonsplit if $F$ has no proper subgroup that maps surjectively to $G$. This is equivalent to the condition for a frattini cover as after Lemma 1.3 below. The frattini subgroup of a group $H$ is the intersection of all the maximal proper open subgroups of $H$.

**Corollary 1.2.** Let $G$ be any finite group. Then there is a totally nonsplit finite cover $\psi: F \to G$ of $G$ where $F$ is not the group of a regular Galois extension of $\mathbb{R}(X)$ with only real branch points.

Corollary 1.2 follows from Theorem 1.1 (a) and this lemma.

**Lemma 1.3.** Let $G$ be a finite group. There is a totally nonsplit finite cover $\psi: F \to G$ of $G$ where $F$ is not generated by elements of order 2.

Consider a homomorphism $\psi: H \to K$ of profinite groups: projective limits of finite groups. Call it a frattini cover if the equivalent conditions (i) or (ii) hold.

(i) $\psi$ is surjective and $\ker(\psi)$ is contained in the frattini group of $H$.

(ii) Subset $S$ of $H$ generates $H$ if and only if $\psi(S)$ generates $K$.

The main result for frattini covers is the existence of a universal frattini cover for any profinite group. This is the cover $\tilde{G}$ in the following statement.

**Proposition 1.4** ([FrJ; Proposition 20.33]). Each profinite group $G$ has a cover $\tilde{\psi}: \tilde{G} \to G$, unique up to isomorphism, satisfying this condition. If $\psi: H \to G$ is any frattini cover of $G$, there exists a cover $\gamma: \tilde{G} \to H$ such that $\psi \circ \gamma = \tilde{\psi}$. Furthermore, $\tilde{g}$ is a profinite projective group.

1.4. Proof of Lemma 1.3. We may assume $G \neq \{1\}$. Consider the universal frattini cover, $\tilde{\psi}: \tilde{G} \to G$, of $G$. Let $\mathcal{N} = \{N_i \mid i \in I\}$ be the collection of all normal subgroups of finite index of $\tilde{G}$. Let $F_i = \tilde{G}/N_i$, $i \in I$, and for 2 indices $i, j \in I$ such that $N_j \supseteq N_i$, let
\( \pi_{ij} : F_i \to F_j \) be the natural homomorphism. The system \( \langle F_i, \pi_{ij} \rangle \) is projective. From compactness of \( \tilde{G} \), \( \varprojlim F_i = \tilde{G} \). Take \( n = |G| \).

For each \( i \in I \), let \( \text{gen}_2(F_i) \) be the subset of \( F_i^n \) consisting of all \( n \)-tuples \( \alpha = (\alpha_1, \ldots, \alpha_n) \) such that \( \langle \alpha_1, \ldots, \alpha_n \rangle = F_i \) and \( \alpha_i^2 = 1 \), \( i = 1, \ldots, n \). For \( i, j \in I \) with \( N_j \supseteq N_i \), denote the restriction to \( \text{gen}_2(F_i) \) of the natural map induced by \( \pi_{ij} \) on \( F_i^n \) by \( \pi_{ij} : \text{gen}_2(F_i) \to \text{gen}_2(F_j) \).

The system \( \{\text{gen}_2(F_i), \pi_{ij}\} \) is projective and an element of \( \varprojlim \text{gen}_2(F_i) \) is an \( n \)-tuple \( \hat{\alpha} = (\hat{\alpha}_1, \ldots, \hat{\alpha}_n) \) such that \( \langle \hat{\alpha}_1, \ldots, \hat{\alpha}_n \rangle = \tilde{G} \) and \( \hat{\alpha}_i^2 = 1 \) for \( i = 1, \ldots, n \). Yet, such an \( n \)-tuple cannot exist. Indeed, from Proposition 1.4, \( \tilde{G} \) is projective. Therefore, it has no nontrivial element of finite order [FrJ; Cor. 20.14]. Conclude that \( \varprojlim \text{gen}_2(F_i) \) is empty. For all \( i \in I \), \( \text{gen}_2(F_i) \) is finite, hence compact. Thus, \( \text{gen}_2(F_i) \) is empty for some \( i \in I \). That is, elements of order 2 in \( F_i \) do not generate \( F_i \).

Next, set \( F = \tilde{G}/(\ker \psi \cap N_i) \). We easily see that the natural map \( \psi : F \to G \) is a frattini cover. From Axiom (ii) for frattini covers, the elements of order 2 in \( F \) do not generate \( F \). The finite cover \( \psi : F \to G \) is the required cover. \( \square \)

1.5. Persistence of condition (1.2) to frattini covers. The collection of finite groups has no practical topology on it. Therefore, a statement about a property being general for finite groups has traditionally been applied by restricting consideration to natural sequences of finite groups. For example, a statement that indexes the subscript \( n \) among the alternating groups \( A_n \) is typical.

On the other hand, suppose a property \( P \) can be interpreted for all finite groups. Assume that \( G \) has property \( P \). As above, consider those frattini covers of \( G \) that also have property \( P \). For one, Proposition 1.4 shows these groups—as a collection—intrinsically attach to \( G \). Therefore, persistence of property \( P \) to hold for frattini covers is intrinsic to the immediate seed group \( G \). In addition, the kernel of the universal frattini cover \( \tilde{G} \) of \( G \) is pro-nilpotent. Thus, there are measures of the persistence of property \( P \). The following question introduces an analog of Lemma 1.3 that fits the above discussion.

**Question 1.5.** Consider a group \( G \) that satisfies condition (1.2). Does its universal frattini cover satisfy (1.2)?

If "Yes" is the answer to Question 1.5, then a cofinal family of finite frattini covers of \( G \) satisfies (1.2).
If $G$ is a $p$-group, then the universal frattini cover $\tilde{G}$ of $G$ is a free pro-$p$-group. In addition, in all cases, $\tilde{G}$ has the same rank—minimal number of generators—as $G$ [FrJ; §20.8].

**Observation** 1.6. Question 1.5 has a positive answer when $G$ is a $p$-group satisfying (1.2).

**Proof.** A characteristic subgroup of $\tilde{G}$ gives the quotient $G$. Since $\tilde{G}$ is a free group, there is an automorphism of $\tilde{G}$ satisfying (1.2) that extends condition (1.2) for $G$. □

Let $\mathcal{C}$ be a nontrivial family of finite groups. We say $\mathcal{C}$ is *full* [FrJ; p. 189] if $\mathcal{C}$ is closed under taking subgroups, quotients, and middle terms of short exact sequences with end terms in $\mathcal{C}$. If $\mathcal{C}$ is full, there is a unique free pro-$\mathcal{C}$-group of any given rank [FrJ; Prop. 15.17]. For the case of rank $s$, denote this by $\hat{F}_s(\mathcal{C})$. In fact, the free pro-$\mathcal{C}$-group on $s$ generators clearly has an automorphism $h$ that satisfies (1.2).

If $G$ is not a $p$-group, then we do not know the answer to Question 1.5. We conclude this section by showing that the universal frattini cover $\tilde{G}$ of $G$ is not of the form $\hat{F}_s(\mathcal{C})$. Here $\mathcal{C}$ can be any full family of finite groups. In particular, this suggests a negative answer to Question 1.5 for such a $G$.

Suppose, on the contrary that $\hat{F}_s(\mathcal{C}) = \tilde{G}$. Let $p'$ and $p''$ be distinct primes that divide $|G|$. Then, the kernel of $\tilde{G} \to G$ is pro-nilpotent with at least two sylow subgroups, $P_{p'}$ and $P_{p''}$ corresponding to these primes. These are nontrivial free pro-$p$-groups of finite rank. Since $\ker(\tilde{G} \to G)$ is a subgroup of finite index of $\hat{F}_s(\mathcal{C})$, it is of the form $\hat{F}_{s'}(\mathcal{C})$ for some finite number $s' > s$ [FrJ; Prop. 15.27]. The next result gives a contradiction by showing that $\hat{F}_{s'}(\mathcal{C})$ has a non-nilpotent quotient. For this, denote the primes $p'$ and $p''$ as $p$ and $q$. Let $\mathbb{Z}/p$ act on $A = (\mathbb{Z}/q)^p$ as cyclic permutations of the coordinates. Consider the semi-direct product $B = A \times S\mathbb{Z}/p$ generated by this action.

**Proposition 1.7.** The group $B$ is a non-nilpotent group of rank 2. Assume that $pq$ divides $|G|$. Then, $\tilde{G}$ is not of the form $\hat{F}_{s'}(\mathcal{C})$ for some full family $\mathcal{C}$.

**Proof.** Assume we have shown $B$ to have the properties of the proposition. From above, we are done if the non-nilpotent group $B$
is a quotient of $\tilde{F}_s(\mathcal{C})$. We know that $\mathcal{C}$ is full family, containing groups whose orders are divisible by $p$ and $q$. Thus, $\mathcal{C}$ contains $B$. Since $s' \geq 2$, there is a surjection of $\tilde{F}_s(\mathcal{C})$ on $B$. It remains to show the properties of $B$.

Here are two generators of $B$: $\alpha = (1, 0, \ldots, 0) \in a$ and $\tau = 1 \in \mathbb{Z}/p$. Indeed, the $\mathbb{Z}/p$ orbit of $\alpha$ gives a basis for $A$. Finally, $\mathbb{Z}/p$ is a $p$-sylow for $B$. It is not, however, normal: $\alpha \tau \alpha^{-1}$ is $(1, -1, 0, \ldots, 0) \times \tau$. Thus, $B$ is not nilpotent.

2. Basic tools.

2.1. Identification of Galois and monodromy actions. Let $y_1$ be a primitive element of the regular extension $Y/K(X)$. Take $P \in K[X, Y]$ to be an irreducible polynomial such that $P(X, y_1) = 0$ and $\deg_Y P = n$. Identify the curve $Y_C$ with projective normalization of the affine plane curve $P(x, y) = 0$. Here $\varphi: Y_C \to \mathbb{P}^1$ is projection: $(x, y) \to x$. Take $x_0$ to be distinct from the branch points of the cover.

Let $\overline{Y_C}$ be the Galois closure of $Y_C/C(X)$. The Galois group $G(\overline{Y_C}/C(X))$ is the geometric Galois group of the extension $Y/K(X)$. Embed it in $S_n$ through its action on the $n$ conjugates $y_1, \ldots, y_n$ of $y_1$. Since we assume $Y/K(X)$ is regular, it is a transitive action.

Identify the points $p_1, \ldots, p_n$ in the fiber $\varphi^{-1}(x_0)$ and the conjugates $y_1, \ldots, y_n$ of $y_1$ as follows. Each embedding $Y_C \to C((X-x_0))$ in the Laurent series around $x_0$ determines a point $p_i \in Y$ above $x_0$. Since $x_0$ is not a branch point, there are $n$ such embeddings. Each corresponds to one of the $y_i$s.

From now on, fix an embedding $\overline{Y_C} \to C((X-x_0))$. That is, regard $\overline{Y_C}$ as a subfield of $C((X-x_0))$ and label the points $p_1, \ldots, p_n$ so that $p_i$ corresponds to the power series $y_i$ in $C((X-x_0))$, $i = 1, \ldots, n$. From classical analytic continuation theory, for this labeling, the images in $S_n$ of both $T(\pi_1)$ and the geometric Galois group $G(\overline{Y_C}/C(X))$ are the same. Denote this common group by $\Gamma_Y$ (or simply $\Gamma$). Furthermore, denote the image in $\Gamma$ of an element $s \in T(\pi_1)$ by $\overline{s}$, and the image in $\Gamma$ of an element $\sigma \in G(\overline{Y_C}/C(X))$ by $\overline{\sigma}$. Even in the case where $Y_C \to \mathbb{P}^1$ is Galois, automorphisms of this cover do not naturally identify with automorphisms of $\overline{Y_C}/C(X)$. In particular, restriction of the former automorphisms to the fiber over $x_0$ do not correspond to automorphisms of $\overline{Y_C}/C(X)$.

We make an assumption a little stronger than saying that $x_0$ is not a branch point. We ask that $\frac{\partial}{\partial Y}(P(x_0, Y))$ has no repeated zeros.
Then, the first term $y_i(x_0)$ determines each of the power series $y_i$. Thus, for the labeling above, identify $p_i$ with the geometric point $(x_0, y_i(x_0))$ on the affine plane curve $P(x, y) = 0$.

2.2. The arithmetic Galois group. From here on, assume the base point $x_0$ is in $\mathbb{P}^1(\mathbb{Q})$. Consider the automorphism group $\text{Aut}(\mathbb{C})$. An automorphism $\tau \in \text{Aut}(\mathbb{C})$ acts coordinatewise on the geometric points of any affine variety defined over $\mathbb{C}$. This action transforms the affine curve with equation $P(x, y) = 0$ into the affine curve of equation $P^\tau(x, y) = 0$. Denote the projective normalization of the curve $P^\tau(x, y) = 0$ by $Y^\tau_\mathbb{C}$ and the associated cover by $\varphi^\tau_\mathbb{C} : Y^\tau_\mathbb{C} \to \mathbb{P}^1$.

On the other hand, there is a natural extension of $\tau$ to $\mathbb{C}((X-x_0))$. Apply $\tau$ to the coefficients of a power series $y$ to get $y^\tau$. Indicate the transform of a subfield $F$ of $\mathbb{C}((X-x_0))$ by $F^\tau$. This action maps the power series $y_1, \ldots, y_n$ onto the $n$ roots $y_1^\tau, \ldots, y_n^\tau$ in $\mathbb{C}((X-x_0))$ of the polynomial $P^\tau$. Also, the field extension $(Y^\tau_{\mathbb{C}})/(F(X))$ is the function field extension of the cover $\varphi^\tau_\mathbb{C} : Y^\tau_\mathbb{C} \to \mathbb{P}^1$.

Points on $Y^\tau_\mathbb{C}$ above $x_0$ correspond to the power series $y_1^\tau, \ldots, y_n^\tau$. Label these, respectively, $p_1^\tau, \ldots, p_n^\tau$. As in §2.1, $p_i^\tau$ corresponds to the point $(x_0, y_i(x_0)^\tau)$ on the affine curve of equation $P^\tau(x, y) = 0$. Conclude that the effect of $\tau$ on $p_1, \ldots, p_n$ agrees with the action on the power series and with coordinatewise action on the geometric points.

Denote the subgroup of $\text{Aut}(\mathbb{C})$ consisting of all automorphisms that fix $K$ by $\text{Aut}_K(\mathbb{C})$. Assume, in addition, that $\tau \in \text{Aut}_K(\mathbb{C})$. Then $P = P^\tau$, $Y^\tau_\mathbb{C} = Y^\tau_\mathbb{C}$ and $\tau$ permutes the points $p_1, \ldots, p_n$ in the fiber $\varphi^{-1}(x_0)$. Thus, $\tau$ induces a permutation $\bar{\tau} \in S_n$. Now consider $\hat{\gamma}$, the Galois closure over $K(X)$ of the extension $Y(K(X))$. Call the Galois group $G(\hat{\gamma}/K(X))$ the arithmetic Galois group of the extension. Label the image of $y \in \hat{\gamma}$ under the automorphism $\sigma \in G(\hat{\gamma}/K(X))$ by $\sigma(y)$. Also, denote the permutation of $\{1, \ldots, n\}$ induced by $\sigma$ on $\{y_1, \ldots, y_n\}$ by $\sigma$. Use $\hat{\Gamma}$ for the group $\{\sigma|\sigma \in G(\hat{\gamma}/K(X))\}$. Note that $\bar{\tau} \in \hat{\Gamma}$, for all $\tau \in \text{Aut}_K(\mathbb{C})$.

**Proposition 2.1.** The group $\Gamma$ is normal in $\hat{\Gamma}$. The quotient group $\hat{\Gamma}/\Gamma$ consists of the cosets modulo $\Gamma$ of the elements $\bar{\tau}$, with $\tau \in \text{Aut}_K(\mathbb{C})$.

**Proof.** Let $\hat{K}$ be the constant field of the extension $\hat{\gamma}/K(X) : \hat{K} = \hat{\gamma} \cap K$. Clearly, $\hat{\gamma} \mathbb{C} = \hat{\gamma} \mathbb{C}$; restriction $G(\hat{\gamma} \mathbb{C}/C(X)) \to G(\hat{\gamma}/\hat{K}(X))$ is an isomorphism. In particular, $\Gamma$ is the image of $G(\hat{\gamma}/\hat{K}(X))$ in
$S_n$. It is a normal subgroup of $\hat{\Gamma}$ because $\hat{K}/K$ is Galois. The map $\text{Aut}_K(\mathbb{C})$ to $G(\hat{K}/K)$ is onto. Therefore, $\tau$, with $\tau \in \text{Aut}_K(\mathbb{C})$, form a full set of representatives (perhaps not distinct) for the quotient $\hat{\Gamma}/\Gamma$. The result follows. □

2.3. Complex conjugation and monodromy. Retain §2.1—§2.2 notation. We know generators for the fundamental group $\pi_1 = \pi_1(\mathbb{P}^1 \backslash \{x_1, \ldots, x_r\}, x_0)$. These are homotopy classes $[\gamma_i]$ of suitably chosen loops starting from $x_0$ around the branch points $x_i$, $i = 1, \ldots, r$. These freely generate except for one relation, $[\gamma_1][\gamma_2] \cdots [\gamma_r] = 1$. For $i = 1, \ldots, r$, set $s_i = T([\gamma_i])$; the $s_i$s generate the monodromy group of the cover and satisfy $s_1s_2 \cdots s_r = 1$.

Call the $\tau$-tuple $(s_1, \ldots, s_r)$ the branch cycle description of the cover associated with the data (or bouquet) $(\gamma_1, \ldots, \gamma_r)$. It is an element of $S_n'$ when we label the points $p_1, \ldots, p_n$ in the fiber $\varphi^{-1}(x_0)$. Another labeling of the fiber $\varphi^{-1}(x_0)$ defines an element of $S_n'$ that is coordinatewise conjugate by an element of $S_n$ to the first branch cycle description of the cover coming from the bouquet $(\gamma_1, \ldots, \gamma_r)$. This produces a one-one correspondence between the following sets:

- degree $n$ covers $\varphi: Y_C \to \mathbb{P}^1$ (up to equivalence of covers) ramified over the points $x_1, \ldots, x_r$; and
- $r$-tuples $(s_1, \ldots, s_r) \in S_n'$ (modulo coordinatewise conjugation by $S_n$) with $s_1s_2 \cdots s_r = 1$ and $(s_1, \ldots, s_r)$ transitive on $1, \ldots, n$.

Unless otherwise specified, assume from here the following.

(2.1) Branch points $x_1, \ldots, x_r$, $r \geq 3$,

are in $\mathbb{P}^1(\mathbb{R})$ and $x_1 < x_2 < \cdots < x_r \leq \infty$.

Fix the base point $x_0 \in \mathbb{P}^1(\mathbb{Q}) \backslash \{\infty\}$ on the arc between $x_1$ and $x_r$ not containing $x_2$ on the real projective line. Denote complex conjugation on $\mathbb{C}$ by $c$. It maps the homotopy class $[\gamma] \in \pi_1$ of a closed path $\gamma$ based at $x_0$ to the homotopy class $[\gamma^c]$ of the conjugate path $\gamma^c$. With suitable loops around the $x_i$s, we write this action explicitly.

For the rest of §2 and §3 use the specific bouquet $(\gamma_1, \ldots, \gamma_r)$ from [FrD; §2.1]. For this we have the following.

PROPOSITION 2.2. The paths $\gamma_1^c, \ldots, \gamma_r^c$ are respectively homotopic to

$$(\gamma_2 \cdots \gamma_r)^{-1}\gamma_1^{-1}(\gamma_2 \cdots \gamma_r), (\gamma_3 \cdots \gamma_r)^{-1}\gamma_2^{-1}(\gamma_3 \cdots \gamma_r),$$

$$\cdots, (\gamma_r)^{-1}\gamma_{r-1}^{-1}\gamma_r, \gamma_r^{-1}.$$
Hurwitz knew these formulas [Hur; p. 357]. Krull and Neukirch [KN] investigated them further. We consider them deriving from the action of a general operator. Suppose we have a group \( U \) and an integer \( r > 0 \). Define \( \mathcal{E}_r: U^r \to U^r \) to send \( u = (u_1, \ldots, u_r) \in U^r \) to \( \mathcal{E}_r(u) \overset{\text{def}}{=} (u_1^\varphi, \ldots, u_r^\varphi) \) with \( u_i^\varphi = u_i^{-1} \) and

\begin{equation}
(2.2) \quad u_i^\varphi = (u_{i+1} \cdots u_r)^{-1}u_i^{-1}(u_{i+1} \cdots u_r), \quad i = 1, \ldots, r - 1.
\end{equation}

We also have

\begin{equation}
(2.3) \quad u_1^\varphi \cdots u_r^\varphi = (u_1 \cdots u_r)^{-1}, \quad i = 1, \ldots, r - 1.
\end{equation}

Consider a cover \( \varphi: Y_C \to \mathbb{P}^1 \) and its conjugate \( \varphi^c: Y_C^c \to \mathbb{P}^1 \). The fiber \( (\varphi^c)^{-1}(x_0) \) consists of the points \( p_1^c, \ldots, p_n^c \). Let \( T^c \) denote the monodromy action on the fiber \( (\varphi^c)^{-1}(x_0) \). For any closed path \( \gamma \) based at \( x_0 \), we have \( T^c([\gamma]^c)(p_i^c) = [T([\gamma])(p_i)]^c \). Replace \( \gamma \) by \( \gamma^c \) and apply \( c \) to both sides. This gives the equivalent expression:

\begin{equation}
(2.4) \quad T^c([\gamma])(p_i^c) = T([\gamma^c])(p_i).
\end{equation}

From (2.4):

\begin{equation}
(2.5) \quad \text{the } r\text{-tuple } (T([\gamma_1^c]), \ldots, T([\gamma_r^c])) \text{ is the branch cycle description of the cover } \varphi^c: Y_C^c \to \mathbb{P}^1 \text{ associated with the bouquet } (\gamma_1, \ldots, \gamma_r).
\end{equation}

The (a) part of the next proposition rephrases (2.4) and (2.5). The (b) part follows because the assumptions imply \( Y_C^c = Y_C \).

**Proposition 2.3.** (a) Suppose \( s = (s_1, \ldots, s_r) \) is the branch cycle description of the cover \( \varphi: Y_C \to \mathbb{P}^1 \) associated with the bouquet \( (\gamma_1, \ldots, \gamma_r) \). Then, \( \mathcal{E}_r(s) = (s_1^\varphi, \ldots, s_r^\varphi) \) is the branch cycle description of the cover \( \varphi^c: Y_C^c \to \mathbb{P}^1 \) associated with the bouquet \( (\gamma_1, \ldots, \gamma_r) \).

(b) If \( R \supset K \) then \( \mathcal{E}_r(s) = \tilde{c} \bar{s} \tilde{c} \). That is \( \tilde{s}_i^\varphi = \tilde{c} \bar{s}_i \tilde{c}, \ i = 1, \ldots, r \).

2.4. **Descending the base field—Weil’s method.** We now descend the base field in the second part of the proof of Theorem 1.1. Without condition (ii) below, it results from Prop. 2.5 of [CoH]. Here is the framework. Let \( \Psi: E \to \mathbb{P}^1 \) be a Galois cover, and let \( H \) be the subgroup of \( \text{Aut}(C) \) given as

\[ \{ \tau \in \text{Aut}(C/Q) | \Psi: E \to \mathbb{P}^1 \text{ and } \Psi^\tau: E^\tau \to \mathbb{P}^1 \text{ are equivalent covers} \}. \]

Take \( K = C^H \), the fixed field of \( H \) in \( C \). Then, \( K \) is the field of moduli of the cover. Choose \( x_0 \), a point in \( \mathbb{Q} \) distinct from the branch points of the cover.
Theorem 2.4. Assume the conditions of the paragraph above. There exists an extension $Y/K(X)$, regular over $K$, such that

(i) the cover $\varphi: Y_C \to \mathbb{P}^1$ is equivalent to the cover $\Psi: E \to \mathbb{P}^1$, and

(ii) $K((x - x_0))$ contains $Y$.

Condition (ii) is equivalent to the following.

(ii') Permutations $\bar{\tau}$ acting on the Galois closure of $Y/K(X)$ have a common fixed point for all $\bar{\tau} \in \bar{H}$ (notation as in §2.2).

Danger: $Y/K(X)$ need not be Galois. It is Galois if and only if $\bar{\tau} = 1$, for all $\bar{\tau} \in \bar{H}$. That is, one point of the cover over $x_0$ is defined over $K$. Thus, if the cover is Galois, all points over $x_0$ must be defined over $K$. In the other direction, let $\tilde{K}$ be the constants of the Galois closure of the extension $Y/K(X)$. Then $\tilde{K} = K$ if and only if $Y/K(X)$ is Galois. We know the field generated by coordinates of the collection of points above $x_0$ contains $\tilde{K}$. Therefore, if these points are defined over $K$, then $\tilde{K} = K$.

Proof. By definition, for each $\tau \in H$, there is an isomorphism $\delta_\tau: E \to E^\tau$ such that $\Psi^\tau \circ \delta_\tau = \Psi$. The automorphism $\delta_\tau$ sends the fiber $\Psi^{-1}(x_0) = \{e_1, \ldots, e_n\}$ to the fiber $(\Psi^\tau)^{-1}(x_0) = \{e_1^\tau, \ldots, e_n^\tau\}$. The cover $\Psi^\tau: E^\tau \to \mathbb{P}^1$ is Galois. Thus, there exists an automorphism $\chi_\tau: E^\tau \to E^\tau$ such that $\chi_\tau \circ \delta_\tau$ sends $e_1$ to $e_1^\tau$. Denote the isomorphism $\chi_\tau \circ \delta_\tau$ by $c_\tau$. The collection $\{c_\tau\}_{\tau \in H}$ satisfies the cocycle condition: $c_{\tau_2} \circ c_{\tau_1} = c_{\tau_1 \tau_2}$ for all $\tau_1, \tau_2 \in H$. Indeed:

$$c_{\tau_2} \circ c_{\tau_1} (e_1) = c_{\tau_2} (c_{\tau_1} (e_1)) = c_{\tau_2} (e_1^\tau_1) = e_1^{\tau_1 \tau_2} = c_{\tau_1 \tau_2} (e_1).$$

Weil's cocycle criterion now reduces the field of definition [We]. There exists a cover $\varphi_K: E_k \to \mathbb{P}^1$, defined over $K$ with the following properties. There is an isomorphism $\Theta: E_K \to E$ (defined over $\mathbb{C}$) such that

$$\begin{align*}
(2.6) & \quad (a) \quad \Psi \circ \Theta = \varphi_K, \quad \text{and} \\
& \quad (b) \quad \Theta^\tau \circ \Theta^{-1} = c_\tau, \quad \text{for all } \tau \in H.
\end{align*}$$

Define $Y$ to be the function field over $K$ of $E_K$. The extension $Y/K(X)$ is regular and satisfies condition (i). In fact, $\varphi: Y_C \to \mathbb{P}^1$ is the cover $\varphi_K: E_K \to \mathbb{P}^1$.

Finally, consider the point $p_1 = \Theta^{-1}(e_1)$ on $E_K$. From (2.6) (b), $p_1^\tau = p_1$, for all $\tau \in H$. That is, $p_1 \in E_K$ is $K$-rational. As before, let $y_1$ be the power series corresponding to $p_1$. Then $y_1 \in K((X - x_0))$. Since $Y = K(X, y_1)$, $K((X - x_0)) \supset Y$. □
3. Proof of Theorem 1.1.

3.1. Proof of Theorem 1.1 (b) \(\Rightarrow\). Let \(Y/R(X)\) be a degree \(n\) regular extension whose associated cover \(\varphi: Y_C \to \mathbb{P}^1\) has monodromy group \(\Gamma_Y = G\). Let \(s = (s_1, \ldots, s_r)\) be the branch cycle description of \(\varphi: Y_C \to \mathbb{P}^1\) associated to the bouquet \((\gamma_1, \ldots, \gamma_r)\) of Proposition 2.2. From Proposition 2.3 (b), we have \(s_i^{\varphi} = \bar{c}i\bar{c}, \ i = 1, \ldots, r\). Apply (2.3). Then, \((\bar{s}_i \cdots \bar{s}_r)^{-1} = \bar{c}(\bar{s}_i \cdots \bar{s}_r)\bar{c}, \ i = 1, \ldots, r\). Set \(\alpha_i = \bar{s}_{i+1} \cdots \bar{s}_r, \ i = 1, \ldots, r - 1\). Thus

(3.1) \[\bar{c}\alpha_i\bar{c} = \alpha_i^{-1}, \quad i = 1, \ldots, r - 1.\]

Conjugating \(G\) by \(\bar{c} \in S_n\) gives the \(h\) that Theorem 1.1 (b) requires. \(\square\)

3.2. Proof of Theorem 1.1 (a) \(\Rightarrow\). Here, \(Y/R(X)\) is a degree \(n\) Galois regular extension with group \(\Gamma_Y = G\). So (3.1) of §3.1 still holds. In addition, since \(\Gamma_Y = \Gamma_Y\), we have \(\bar{c} \in G\) (statement prior to Proposition 2.1). Thus, \(\bar{c}, \bar{c}\alpha_1, \ldots, \bar{c}\alpha_r\) are of order \(\leq 2\) and they generate \(G\). \(\square\)

3.3. Proof of Theorem 1.1 (b) \(\Leftarrow\). Let \(G\) be a group with property (1.2). Let \(r = s + 1\) and \(n = |G|\). Regard \(G\) as a subgroup of \(S_n\) through its regular representation. Consider the \(r\)-tuple \(s = (s_1, \ldots, s_r) \in S^r_n\) defined by

(3.2) \[s = (\alpha_1, \alpha_1^{-1}\alpha_2, \alpha_2^{-1}\alpha_3, \ldots, \alpha_{r-2}^{-1}\alpha_{r-1}, \alpha_{r-1}^{-1}).\]

The \(s_i\)s generate \(G\). They also satisfy \(s_1 \cdots s_r = 1\). Fix \(r + 1\) points \(x_0, x_1, \ldots, x_r\) in \(\mathbb{P}^1(\mathbb{R})\) and a bouquet \((\gamma_1, \ldots, \gamma_r)\) as in §2.3. From Riemann’s Existence Theorem (§2.3), there exists a cover \(\Psi: E \to \mathbb{P}^1\), unique up to equivalence of covers, with the following properties. Its branch points are \(x_1, \ldots, x_r\), and \(s = (s_1, \ldots, s_r)\) is the branch cycle description of the cover associated to the bouquet \((\gamma_1, \ldots, \gamma_r)\). Furthermore, since \(G \to S_n\) is the regular representation, \(\Psi: E \to \mathbb{P}^1\) is a Galois cover with automorphism group \(G\).

From Proposition 2.3 (a), \(\mathcal{C}_r(s) = (s_1^{\varphi}, \ldots, s_r^{\varphi})\) is the branch cycle description of the cover \(\Psi^c: E^c \to \mathbb{P}^1\) associated to the bouquet \((\gamma_1, \ldots, \gamma_r)\). From the definition of \(\mathcal{C}_r\) and (1.2) check easily that \(s_i^{\varphi} = h(s_i), \ i = 1, \ldots, r\). Suppose that conjugation by \(\kappa \in S_n\) coincides with the automorphism \(h\) on \(G\). Thus:

(3.3) \[s_i^{\varphi} = \kappa s_i \kappa^{-1} \quad \text{for } i = 1, \ldots, r.\]
From Riemann's Existence Theorem (§2.3), the covers $\Psi: E \to \mathbb{P}^1$ and $\Psi^c: E^c \to \mathbb{P}^1$ are equivalent covers. Apply Theorem 2.4 to conclude there exists a regular extension $Y/\mathbb{R}(X)$ with these properties.

(i) $\phi: Y_C \to \mathbb{P}^1$ is equivalent to the cover $\Psi^c: E^c \to \mathbb{P}^1$.

(ii) $\mathbb{R}((X-x_0))$ contains $Y$.

The cover $\phi: Y_C \to \mathbb{P}^1$ is defined over $\mathbb{R}$. It is the desired cover. $\square$

3.4. Proof of Theorem 1.1 (a) $\Leftarrow$. Let $G$ be a group generated by involutions $\alpha_1, \ldots, \alpha_s$. In particular, $G$ has property (1.2) with $\kappa = 1$. Thus, the construction around (3.3) holds, with $h = 1$, $\kappa = 1$. Consider the regular extension $Y/\mathbb{R}(X)$ produced in §3.3. It is Galois over $\mathbb{C}(x)$ with (geometric) Galois group $G$. Also, $\mathbb{R}((X-x_0))$ contains $Y$. The branch cycle description $s = (s_1, \ldots, s_r)$ of the cover $\phi: Y_C \to \mathbb{P}^1$ associated with the bouquet $(\gamma_1, \ldots, \gamma_r)$ has this property:

(3.4) $s_i^{\mathbb{C}} = s_i$ for $i = 1, \ldots, r$.

From Proposition 2.3 (b), we also have $s_i^{\mathbb{C}} = \bar{c}s_i\bar{c}$, $i = 1, \ldots, r$. Therefore, $\bar{c} \in \text{Cen}_{S^*}(G)$. Since $\mathbb{R}((X-x_0))$ contains $Y$, $\bar{c}$ has a fixed point. Conclude that $\bar{c} = 1$. Therefore, from Proposition 2.1, $\Gamma_Y = \Gamma_Y: Y/\mathbb{R}(X)$ is a Galois regular extension with Galois group $\Gamma_Y = G$. $\square$

REMARK. In the above argument, $\bar{c} = 1$. That is, $\varphi^{-1}(x_0)$ has only real points. Equivalently, $\mathbb{R}$ contains the residue class algebra $Y_{x_0}$. $\square$

3.5. Comments. This section consists of elaborate comments. Each uses the proof of Theorem 1.1 for further exploration. These are the topics.

- Branch points need not be real.
- The cover need not be Galois.
- You can decide when the field of moduli of a cover is $\mathbb{R}$.

Comment 1. Dropping the assumption "the branch points are real." The "real branch point situation" of Theorem 1.1 allowed special generators $[\gamma_1], \ldots, [\gamma_r]$ of the fundamental group $\pi_1$ from §2.3. Explicit formulas gave $[\gamma_1^c], \ldots, [\gamma_r^c]$ as words in $[\gamma_1], \ldots, [\gamma_r]$ (cf. Proposition 2.2). We can work with the general cover defined over $\mathbb{R}$ similarly.

Here, the branch points consist of $r_1$ real points and $r_2$ complex conjugate pairs, where $r = r_1 + 2r_2$. Use the paths of [FrD; §2.2]
for which we know the complex conjugation action explicitly. Slight adjustments to the proof above lead to this more general result.

**Theorem 3.1.** Finite group $G$ is the group of a regular extension $Y/\mathbb{R}(X)$ with $r$ branch points, $r_1$ of these real, exactly when $G$ has special generators. Specifically, $(r + r_1)/2$ elements generate $G$ with at least $r_1$ of them involutions.

More precisely, the following statements are equivalent.

(a) There exists a Galois regular extension $Y/\mathbb{R}(X)$ of group $G$, with $r$ branch points $t_1, \ldots, t_r, \overline{z}_1, \ldots, \overline{z}_r, z_1, \ldots, z_r$, where $t_i \in \mathbb{R}$, $i = 1, \ldots, r_1$, and $z_i \notin \mathbb{R}$, $i = 1, \ldots, r_2$.

(b) There exists $(g'_1, \ldots, g'_r) \in G^r$ which satisfy these conditions:

   (i) $g'_1 \cdots g'_r = 1$,
   (ii) $(g'_1, \ldots, g'_r) = G$,
   (iii) $\exists g'_0 \in G$ such that $(g'_0 \cdots g'_i)^2 = 1$, $i = 0, \ldots, r_1 - 1$.

The special case $r = r_1$ corresponds to Theorem 1.1 (a). For $r_1 = 0$, we get a result from the introduction. Namely, every finite group $G$ is the Galois group of a Galois regular extension of $\mathbb{R}(X)$.

**Comment 2.** Nonregular representations. Here, suppose $G$ has an embedding in $S_n$ (not necessarily the regular representation). Assume $\alpha_1, \ldots, \alpha_s$ are generators for which (1.2) holds. Denote the $s$-tuple of (3.2) by $\mathbf{s}(\alpha)$. Let $x_0, x_1, \ldots, x_r$ be $r + 1$ points in $\mathbb{P}^1(\mathbb{R})$. Take $(\gamma_1, \ldots, \gamma_r)$ to be a bouquet as in §2.3 with $\mathbf{s}(\alpha)$ the associated branch cycle description of the cover with $x_1, \ldots, x_r$ as branch points. Denote the degree $n$ (not necessarily Galois) cover from §3.3 by $\Psi_{\mathbf{s}(\alpha), x}: E \to \mathbb{P}^1$. We ask if we can define this cover over $\mathbb{R}$.

We showed the answer to be positive in the Galois case, thanks to Theorem 2.4. In greater generality, the answer is yes whenever you can construct a collection $\{c_{\tau}\}_{\tau \in G(\mathbb{C}/\mathbb{R})}$ as in Theorem 2.4. It must satisfy the cocycle condition $c_{\tau_1} \circ c_{\tau_2} = c_{\tau_1 \tau_2}$, for all $\tau_1, \tau_2 \in G(\mathbb{C}/\mathbb{R})$. For example, you can do this when the cover $\Psi: E \to \mathbb{P}^1$ has no nontrivial automorphism. This is the same as the condition $\text{Cen}_{S_n}(G) = \{1\}$.

**Comment 3—from E. Dew [D].** When the field of moduli is $\mathbb{R}$. Suppose $\varphi: E \to \mathbb{P}^1$ is a Galois cover and complex conjugation gives an equivalent cover $\varphi^e: E^e \to \mathbb{P}^1$. We say $\mathbb{R}$ contains the field of moduli. Suppose also that the covers have real branch points. Let
Let \( \gamma = (\gamma_1, \ldots, \gamma_r) \) be a bouquet as in §2.3 and let \((s_1, \ldots, s_r)\) be the branch cycle description associated to the bouquet \(\gamma\). With \(\alpha_i = s_1 \cdots s_i, \; i = 1, \ldots, r - 1\), Proposition 2.3 gives this:

\[ (*) \quad \text{The set } N_\alpha = \{ \kappa \in S_n : \kappa \alpha_i \kappa^{-1} = \alpha_i^{-1}, \; i = 1, \ldots, r - 1 \} \]

is nonempty.

Thus, (*) is a necessary condition. We want to know what to add to this for an if and only if condition for the following:

\[ (**) \quad \text{There is a cover equivalent to } \psi : E \to \mathbb{P}^1 \text{ defined and Galois over } \mathbb{R}. \]

It is tempting to answer: \( N_\alpha \cap G \) is nonempty. Here \( G \) denotes the monodromy group of the cover. Yet, this condition may not be sufficient in general. The correct answer is this:

\[ (***) \quad \exists \kappa \in N_\alpha \cap G \text{ with } \kappa^2 = 1. \]

**Note.** In the addition following Theorem 1.1 (b) we selected the \( s_1 \)s so \( \kappa = 1 \) lies in \( N_\alpha \). Also, (***) is equivalent to asking that \( \kappa^2 \) be the square of an element of the center \( Z(G) \); divide \( \kappa \) by this element.

**Proof of the equivalence of (**) and (***)**. Assume that the cover \( \psi : E \to \mathbb{P}^1 \) is defined and Galois over \( \mathbb{R} \). Then the element \( \overline{c} \) (see §2.2 for the definition of \( \overline{c} \)) is in \( N_\alpha \cap G \) and it satisfies \( \overline{c}^2 = 1 \).

In the other direction, assume (***) . Following the proof of Theorem 2.4 we use Weil’s criterion. Here, however, we choose a different cocycle. Let \( H = \{ 1, c \} \) denote the Galois group of \( \mathbb{C}/\mathbb{R} \). Recall the dictionary between covers and branch cycle descriptions (for the bouquet \( \gamma \)). An isomorphism \( \delta : E \to E^c \) such that \( \psi^c \circ \delta = \psi \) comes from an element \( \kappa \) in \( N_\alpha \).

To use (***) , label points \( p \) on \( E \) above the base point \( x_0 \). Apply \( c \) to \( p \); then permute the naming of the image points \( p^c \) by \( \kappa \). The new points \( \kappa(p^c) \) give us points above \( x_0 \) in \( E^c \). These produce exactly the same branch cycle description (relative to \( \gamma \)) for \( E^c \) as do the points \( p \) for \( E \). Thus, these respective namings of the points give a unique isomorphism \( \delta_c : E \to E^c \) that sends points \( p \) to the respective points \( \kappa(p^c) \). In addition to \( \psi^c \circ \delta = \psi \), \( \delta_c \) satisfies these two conditions:

\[ (\dagger) \quad \delta_c^2 \circ \delta_c = 1; \quad \text{and} \]

\[ (\ddagger) \quad \delta_c \text{ commutes with the action of } c \text{ that takes automorphisms of } E \to \mathbb{P}^1 \text{ to automorphisms of } E^c \to \mathbb{P}^1. \]
Indeed, \((†)\) follows because the effect of the left side of \((†)\) on \(p\) is given by \(κ^2\). As for \((††)\), automorphisms of the covers commute with a renaming of the points of \(p\).

For convenience take \(δ_1\) to be the identity. Condition \((†)\) guarantees that the collection \(\{δ_τ\}\) satisfies the cocycle condition
\[
δ_{τ_1}^2 \circ δ_{τ_2} = δ_{τ_1τ_2}.
\]
Therefore, one can descend the field of definition of the cover to \(ℝ\). Condition \((††)\) assures the automorphisms are also defined over \(ℝ\).

Section 3.6 gives a more algebraic approach to the above. In particular, the equivalence of \((**)\) and \((***)\) follows immediately from Lemma 3.3.

3.6. Serre's approach. Serre suggested that the algebraic fundamental group, rather than the topological fundamental group, would be more convenient for proving Theorem 1.1 (a). We follow Serre's exposition [Se3; cf. Ch. 7, 8, 9].

Assume \(K\) has characteristic 0. Let \(x_1, \ldots, x_r\) be \(r\) distinct points in \(ℙ^1(ℙ)\). Denote the maximal algebraic extension of \(K(X)\) unramified outside \(x_1, \ldots, x_r\) by \(Ω\). The extension \(Ω/K(X)\) is Galois. Its group is the algebraic fundamental group of \(ℙ^1(ℙ)\)\(\{x_1, \ldots, x_r\}\). Denote this profinite group by \(π_{alg}\).

When \(ℙ = ℂ\), \(π_{alg}\) is the profinite completion \(\hat{π}\) of the topological fundamental group \(π\) [Se3; Theorem 7.5, p. 69]. By analogy with the complex case, denote the free group on \(r\) generators \(Γ_1, \ldots, Γ_r\) with the single relation \(Γ_1 \cdots Γ_r = 1\) by \(π\). There is a map \(i: π \to π_{alg}\) with the following properties.

(i) \(i(Γ_i) = Γ_i\) is a generator of an inertia group of the extension \(Ω/K(X)\) above \(x_i\), \(i = 1, \ldots, r\).

(ii) The map \(i\) extends to an isomorphism \(\hat{i}: \hat{π} \to π_{alg}\).

If the divisor \((x_1) + (x_2) + \cdots + (x_r)\) of \(ℙ^1\) is \(K\)-rational, the extension \(Ω/K(X)\) is Galois. Let \(π_K\) denote the Galois group of this extension. We have this exact sequence:

\[
1 \to π_{alg} \to π_K \to Λ_K \to 1.
\]

Here \(Λ_K\) denotes the Galois group of the extension \(Ω/K\). Note: the map \(π_K \to Λ_K\) has many sections. Indeed, for each \(x_0 \in ℙ^1(K)\)\(\{x_1, \ldots, x_r\}\), we can embed \(Ω\) in \(ℙ((X - x_0))\) where the elements of \(Λ_K\) act naturally (cf. §2.2).

Given a finite group \(G\), a surjective homomorphism \(ψ ∈ \text{Hom}(π_{alg}, G)\) produces a Galois extension \(E/Ω(K)\) with group \(G\).
We say $E$ descends to $K$ if there exists a Galois regular extension $E_K/K(X)$ with $CE_K = E$. This happens if and only if the homomorphism $\psi$ extends to $\pi_K$.

In our context, $K = \mathbb{R}$ and the branch points $x_1, \ldots, x_r$ are real. Section 2.3 gives generators $\Gamma_1, \ldots, \Gamma_r$ of $\pi_{\text{alg}}$ so that complex conjugation $c \in \Lambda_{\mathbb{R}}$ acts on them by the formulas (2.2). Recall from §2.3 the operator $E$ in our next result.

**Proposition 3.2.** Assume the branch points $x_1, \ldots, x_r$ are real. Then, $\pi_K$ is isomorphic to the semi-direct product $\pi_{\text{alg}} \rtimes s\mathbb{Z}/2$ where $c = 1 \in \mathbb{Z}/2$ maps $\Gamma \in \pi_{\text{alg}}$ to $\Gamma^c$ as follows:

(3.6) \[ \Gamma_i^c = \Gamma_i^\varepsilon, \quad i = 1, \ldots, r. \]

The group theoretical observation that supports Theorem 1.1 (a) now appears clearly.

**Lemma 3.3.** Let $\psi \in \text{Hom}(\pi_{\text{alg}}, G)$ and $g_i = \psi(\Gamma_1) \cdots \psi(\Gamma_i), \ i = 1, \ldots, r$. Then, $\psi$ extends to $\tilde{\psi} \in \text{Hom}(\pi_{\text{alg}} \rtimes s\mathbb{Z}/2, G)$ if and only if there exists an involution $\kappa \in G$ with all of $\kappa g_1, \ldots, \kappa g_r$ involutions.

**Proof.** Assume $\tilde{\psi} \in \text{Hom}(\pi_{\text{alg}} \rtimes s\mathbb{Z}/2, G)$ extends $\psi$. Set $\kappa = \tilde{\psi}(c), \ |\kappa| = 2$ and

(3.7) \[ \psi(\Gamma^c) = \kappa \psi(\Gamma) \kappa \]

for each $\Gamma \in \pi_{\text{alg}}$. Substitute $\Gamma_i$ for $\Gamma$ and use (2.3) to get $g_i^{-1} = \kappa g_i \kappa, \ i = 1, \ldots, r$.

For the converse, define $\tilde{\psi} \in \text{Hom}(\pi_{\text{alg}} \rtimes s\mathbb{Z}/2, G)$ by $\tilde{\psi}(\Gamma, e) = \psi(\Gamma) \kappa^e$ for each $\Gamma \in \pi_{\text{alg}}$ and $e = 0, 1$. Use (3.6) to check that (3.7) holds for $\Gamma = \Gamma_i, \ i = 1, \ldots, r$, and so for all $\Gamma \in \pi_{\text{alg}}$. This guarantees that $\tilde{\psi}$ is a homomorphism of groups. \(\Box\)

3.7. **$p$-adic analogs.** Proposition 3.2 gives the effect of complex conjugation $c$:

(3.8) $\Gamma_i^c$ is conjugate in $\pi$ to $\Gamma_i^{-1}, \ i = 1, \ldots, r$.

The exponent $-1$ comes from the "branch cycle argument" ([Fr1; p. 62] or [DFr; §1.4 Proposition 1.9]). We explain. Consider the cyclotomic character $\chi: \Lambda_K \rightarrow \prod_N G(K(\mu_N)/K), \ i = 1, \ldots, r$. Here $\mu_N$ denotes the group of $N$th roots of 1. The action of each $\tau \in \Lambda_K$ on the group $\pi_{\text{alg}}$ looks like this:

(3.9) $\Gamma_i^\tau$ is conjugate in $\pi_{\text{alg}}$ to $\Gamma_j^{\chi(\tau)}$ where $x_j = x_i^\tau$.  

Now take $K = \mathbb{Q}_p$. It is natural to ask if the Frobenius $F_p \in \Lambda_{\mathbb{Q}_p}$ satisfies an analog of (3.8). One cannot just replace the exponent $-1$ in (3.8) by the exponent $p$. Indeed, if this were true, conjugates of $\Gamma^p_i$, $i = 1, \ldots, r$ would generate $\pi$. This, however, would imply that a group generated by elements of order $p$ would be trivial, a contradiction.

We are not tempted to use the exponent $p$ when we recognize a simple property of the Frobenius $F_p$. It acts on $\mu_N$ as $p$th powers only when $p$ does not divide $N$. Question 3.4 below is subtler. Say that a finite extension $L/\mathbb{Q}_p(X)$ is $p'$-ramified if $p$ does not divide any of the orders $e_i$ of the inertia groups above $x_i$, $i = 1, \ldots, r$. For such extensions, $p$ is relatively prime to $N = \text{lcm}(e_1, \ldots, e_r)$. In this case, the value in $G(K(\mu_N)/K)$ of the cyclotomic character at $F_p$ is $p$. Define $\pi_p^{\text{alg}}$ to be the projective limit $\lim \pi^{\text{alg}}/D$. Here $D$ ranges over normal subgroups of $\pi$ of finite index where the field extension corresponding to $D$ is $p'$-ramified.

**Question 3.4.** Is the action of the Frobenius $F_p$ on $\pi \equiv \pi_p^{\text{alg}}$ induced by an action on $\pi$ such that $\Gamma^F_i$ is conjugate in $\pi$ to $\Gamma^p_i$ where $x_j = x^F_i$, $i = 1, \ldots, r$?

We believe the answer is still "No!" Here is an outline in this direction in the case of covers with branch points in $\mathbb{Q}_p$. Such a "frobenius" action would give a formula like this:

\[(3.10) \quad F_p\sigma_iF_p^{-1} = \omega_i(\sigma)\sigma^p_i\omega_i^{-1}(\sigma), \quad i = 1, \ldots, r.\]

Here $\omega_i(\sigma)$ is a word in the entries of $\sigma$. To regard the formula as similar to that over $\mathbb{R}$ requires some conditions on the words $\omega(\sigma)$. At the minimum, they should be independent of considerable data describing the cover.

Suppose we ask that $\omega(\sigma)$ be independent of the branch points and the choice of elements in the conjugacy classes given by the entries of $\sigma$. Then, such a formula implies the existence of a correspondence—much like a Hecke correspondence—on the naturally attached Hurwitz space. We conclude by showing how this gives a contradiction.

When $r = 4$, consider the observation of [Fr, 2; §4.2]. This relates all Hurwitz spaces to curves defined by the action of a subgroup of finite index in $\text{SL}_2(\mathbb{Z})$ on the upper half plane. Our assumptions on $\omega(\sigma)$ would imply the existence of an actual nontrivial Hecke theory on these curves. Some of these curves are modular curves, and they
have a well known Hecke theory. Still, most are not. For these, this
contradicts a result of Atkin [A]: noncongruence subgroup curves have
only trivial Hecke correspondences.

 Remark. The existence of a Galois regular extension of \( \mathbb{Q}_p(X) \)
with group any given group \( G \) was proved by Harbater [H]. In this
subsection we wanted more. An analog of Lemma 3.3 would be a
practical criterion for defining a given cover over \( \mathbb{Q}_p \).

4. Hurwitz spaces and rationality over \( \mathbb{Q} \).

4.1. Reduction of the problem. Suppose \( G \) is a group with an em-
bedding \( G \rightarrow S_n \). This need not be the regular representation. Let
\( \alpha_1, \ldots, \alpha_s \) be generators for which condition (1.2) holds. Denote a
specific cover produced by Comment 2 of §3.5 by \( \Psi_{s(\alpha)}, x : E \rightarrow \mathbb{P}^1 \).
Finally, we assume either

\( (4.1) \) \( G \rightarrow S_n \) is the regular representation or \( \text{Cen}_{S_n}^G(G) = \{1\} \).

From Comment 2 of §3.5, we can define \( \Psi_{s(\alpha)}, x : E \rightarrow \mathbb{P}^1 \) over \( \mathbb{R} \). In
this section, we try to descend to \( \mathbb{Q} \).

Question 4.1. Is there some choice of branch points \( x_1, \ldots, x_4 \) in
\( \mathbb{P}^1(\mathbb{R}) \) that gives a cover \( \Psi_{s(\alpha)}, x : E \rightarrow \mathbb{P}^1 \) produced by Comment 2
of §3.5 and defined over the rational number field \( \mathbb{Q} \).

We use Nielsen classes and Hurwitz families to investigate this.

Branch cycle descriptions provide much information (cf. §2.3 and
[DFr] §1.1). Still, they depend on many choices: a base point \( x_0 \), a
labeling of the points in the fiber \( \Phi^{-1}(x_0) \), an ordering of the branch
points \( x_1, \ldots, x_r \), and a sample bouquet \( \gamma_1, \ldots, \gamma_r \). There is an
intrinsic notion.

Consider the data attached to any branch cycle description \( (s_1, \ldots,
, s_r) \) of a cover. Most importantly, there is the group \( \langle s \rangle \) generated by
the \( s_i s \). Up to conjugation by \( S_n \), this is the monodromy group of
the cover. Secondly, there is the collection \( \{C_1, \ldots, C_r\} \) of conjugacy
classes of \( s_1, \ldots, s_r \) in the group \( \langle s \rangle \). From Lemma 1 of [Fr1], up
to conjugation by \( S_n \), this data is an invariant of the cover. This
observation gives the definition of the Nielsen class of a cover.

Let \( G \) be a subgroup of \( S_n \) and let \( C = (C_1, \ldots, C_r) \) be an \( r \)-tuple
of nontrivial (not necessarily distinct) conjugacy classes of \( G \).

Definition 4.2. To the data \( (G, C) \) we associate its Nielsen class:

\[
\text{ni}(C) = \{ s \in G^r | \langle s \rangle = G, s_1 \cdots s_r = 1 \}
\]

and there exists \( \omega \in S_r \), \( s(i)\omega \in C_i \), \( i = 1, \ldots, r \).
Suppose a cover $\Psi: E \to \mathbb{P}^1$ has any branch cycle description $s$, up to conjugation by elements of $S_n$, in $\text{ni}(C)$. We say the cover is in $\text{ni}(C)$. Alternatively, $\text{ni}(C)$ is the Nielsen class of the cover. The order in which we list the conjugacy classes does not matter. The \textit{straight Nielsen class} of $(C, G)$ is

$$\text{sni}(C) = \{s \in \text{ni}(C) | s_i \in C_i, \ i = 1, \ldots, r\}.$$  

We speak of a cover $\Psi: E \to \mathbb{P}^1$ with an ordering of its branch points being in $\text{sni}(C)$. This means, up to conjugation by elements of $S_n$, that any branch cycle description of the cover with this ordering is in $\text{sni}(C)$. The normalizer (resp., the straight normalizer) of the Nielsen class is

$$N(C) = \{\kappa \in S_n | \text{conjugation by } \kappa \text{ permutes } C_1, \ldots, C_r\},$$  

$$SN(C) = \{\kappa \in S_n | \text{conjugation by } \kappa \text{ fixes } C_1, \ldots, C_r\}.$$  

Note that $N(C)$ acts on the Nielsen class $\text{ni}(C)$ by conjugation: $\kappa \in N(C)$ maps $s \in \text{ni}(C)$ to $\kappa s \kappa^{-1} \in \text{ni}(C)$. Similarly, $SN(C)$ acts on the straight Nielsen class $\text{sni}(C)$. Denote the quotients of these actions by $\text{ni}(C)^{ab}$, $\text{sni}(C)^{ab}$, the \textit{absolute Nielsen classes}.

Under certain assumptions, there is a space representing a solution to a natural \textit{moduli problem}. This is the problem of parametrizing equivalence classes of covers in a given Nielsen class. \textit{Hurwitz monodromy action} interprets properties of this moduli space. We explain the monodromy action.

Consider the free group on $r$ generators, $Q_i$, $i = 1, \ldots, r - 1$, with these relations:

\begin{align*}
(4.2) & \quad (a) \quad Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}, \ i = 1, \ldots, r - 2; \\
& \quad (b) \quad Q_i Q_j = Q_j Q_i, \ |i - j| > 1; \ \text{and} \\
& \quad (c) \quad Q_1 Q_2 \cdots Q_{r-1} Q_{r-1} \cdots Q_1 = 1.
\end{align*}

This group, a quotient of the Artin braid group $[Bo]$, is called the \textit{Hurwitz monodromy group} of degree $r$. We denote it by $H_r$. The $Q_i$s act on $\text{ni}(C)^{ab}$ by this formula: for $s \in \text{ni}(C)^{ab}$

\begin{align*}
(4.3) & \quad (s)Q_i = (s_1, \ldots, s_{i-1}, s_i s_{i+1} s_i^{-1}, s_i, s_{i+2}, \ldots, s_r), \\
& \quad i = 1, \ldots, r - 1.
\end{align*}

Thus they induce a permutation representation of $H_r$ on $\text{ni}(C)^{ab}$: the Hurwitz monodromy action on the Nielsen class $\text{ni}(C)^{ab}$.
Denote the kernel of the natural permutation representation $H_r \rightarrow S_r$ sending $Q_i$ to the 2-cycle $(i i+1)$ by $SH_r$. This is the straight Hurwitz monodromy group. The group $SH_r$ acts on the straight Nielsen class $\text{sn}(C)^{ab}$. The next statement summarizes the basic moduli space properties in the special case that all of the conjugacy classes are rational ([Fr1; §4 and 5] or [DFr; §1]). (A conjugacy class is rational if it is closed under putting elements to powers relatively prime to the order of elements in the class.)

**Theorem 4.3.** Assume that (4.1) holds, that $G$ has no center, that $SH_r$ acts transitively on $\text{sn}(C)^{ab}$, and that $C_1, \ldots, C_r$ are rational conjugacy classes. Then there is an algebraic family $\mathcal{F}(C)$ of covers of $\mathbb{P}^1$ (a priori over $\mathbb{C}$)

$$\mathcal{F}(C): \mathcal{F}(C) \rightarrow \mathcal{H}(C) \times \mathbb{P}^1.$$

This universal Hurwitz family associated to $\text{ni}(C)$ satisfies (4.4)–(4.7).

1. **(4.4)** $\mathcal{F}(C)$ is a finite morphism of quasiprojective varieties, $\mathcal{H}(C)$ is irreducible and the generic fiber of $\text{pr}_1 \circ \mathcal{F}(C): \mathcal{F}(C) \rightarrow \mathcal{H}(C)$ is irreducible.

2. **(4.5)** The family $\mathcal{F}(C)$ is defined over $\mathbb{Q}$.

3. **(4.6)** Each cover $\Psi: E \rightarrow \mathbb{P}^1$ in the Nielsen class $\text{ni}(C)^{ab}$ is equivalent to a unique fiber cover $\mathcal{F}(C)_h: \mathcal{F}(C)_h \rightarrow \mathbb{P}^1$ (with $h \in \mathcal{H}(C)$) of the family $\mathcal{F}(C)$. Also, $\mathcal{F}(C)_h: \mathcal{F}(C)_h \rightarrow \mathbb{P}^1$ is defined over $\mathbb{Q}(h)$, the field of definition of the point $h$ on the algebraic variety $\mathcal{H}(C)$; $\mathbb{Q}(h)$ is the smallest field of definition for a cover that is equivalent to the cover $\Psi: E \rightarrow \mathbb{P}^1$.

4. **(4.7)** Denote the subvariety of $(\mathbb{P}^1)^r$ consisting of $r$-tuples with distinct coordinates by $U^r$. Then, consider the algebraic variety $U^r/S_r = U_r$ given by the quotient action of $S_r$. The “branch point reference map” $\Psi(C): \mathcal{H}(C) \rightarrow U_r$ sends each $h \in \mathcal{H}(C)$ to the branch point set of the fiber cover $\mathcal{F}(C)_h: \mathcal{F}(C)_h \rightarrow \mathbb{P}^1$. This is an étale morphism of degree $|\text{ni}(C)^{ab}|$ defined over $\mathbb{Q}$.

The original conjugacy classes, $C_1, \ldots, C_r$, are the conjugacy classes in $G$ of the entries of the $r$-tuple $s(\alpha)$. Theorem 4.3 has this consequence.
Proposition 4.4. Assume the hypotheses of Theorem 4.3. The answer to Question 4.1 is yes if and only if there are branch points, \(x_1, \ldots, x_r \in \mathbb{P}^1(\mathbb{Q})\), so that the point \(h \in \mathcal{H}(C)\) that corresponds to the cover \(\Psi_{s(a), x} : E \to \mathbb{P}^1\) is a \(\mathbb{Q}\)-rational point on \(\mathcal{H}(C)\).

4.2. Description of \(\mathcal{H}(C)\) for \(r = 4\). See [BFr; §1, Lemma 1.6], [Fr2; §4.1]. Both our examples will be 4 branch point situations. In this case, \(\mathcal{H}(C)\) has a more explicit description. Consider natural map \(U^r \to U_r\). Let \(\mathcal{H}(C)'\) be an irreducible component of the fiber product \(\mathcal{H}(C) \times_{U_r} U^r\) and \(p : \mathcal{H}(C)' \to U^r\) the natural projection. Theorem 4.5 uses the permutations of \(\text{sni}(C)^{ab}\) induced by these elements of \(SH_r : Q_1^2 ; Q_1^{-1}Q_2^2Q_1 ; Q_1^{-1}Q_2^{-1}Q_3^2Q_2Q_1\). Denote these by \(a_{12}, a_{13}, a_{14}\), respectively. These act on \(\text{sni}(C)^{ab}\). The transitivity hypothesis of Theorem 4.3 implies that the \(a_{ij}\)'s are transitive on \(\text{sni}(C)^{ab}\).

Theorem 4.5. For each \((x_2, x_3, x_4) \in U^3\), denote the inverse image \(p^{-1}(\mathbb{P}^1 \times (x_2, x_3, x_4))\) by \(\mathcal{H}(C)'(x_2, x_3, x_4)\). Composition of \(p\) with projection \(U^r \to \mathbb{P}^1\) on the first factor gives an unramified cover

\[\mathcal{H}(C)'(x_2, x_3, x_4) \to \mathbb{P}^1 \setminus \{x_2, x_3, x_4\}.\]

Complete this to a (ramified) cover \(C(C) \to \mathbb{P}^1\) of projective nonsingular curves. This will have the following properties.

(4.8) \(x_2, x_3, x_4\) are the 3 branch points of the cover.

(4.9) \((a_{12}, a_{13}, a_{14})\) (acting on \(\text{sni}(C)^{ab}\)) is a branch cycle description of the cover.

(4.10) The cover is defined over \(\mathbb{Q}\).

Corollary 4.6. The variety \(\mathcal{H}(C)\)' is birational to \(C(C) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1\).

Proof. For \((x_2, x_3, x_4)\) take the generic point of \(U^3\) in the above. The birational equivalence \(\mathcal{H}(C)'(x_2, x_3, x_4) \cong C(C)\) induces a birational map \(\mathcal{H}(C)' \to C(C) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1\). □

Section 4.3 has examples where \(C(C)\) is \(\mathbb{P}^1\) (over \(\mathbb{Q}\)). Consequently, the space \(\mathcal{H}(C)'\) is a \(\mathbb{Q}\)-rational variety. In particular, the \(\mathbb{Q}\)-rational points on \(\mathcal{H}(C)'\) form a dense subset of \(\mathcal{H}(C)'(\mathbb{R})\) (for the complex topology) and Question 4.1 has an affirmative answer.
4.3. *A formula for the genus of the curve* \( C(C) \). The Riemann-Hurwitz formula gives the genus \( g(C) \) of the curve \( C(C) \) (cf. Theorem 4.5):

\[
\text{(4.11) } \text{ind}(a_{12}) + \text{ind}(a_{13}) + \text{ind}(a_{14}) = 2(N + g(C) - 1)
\]

with \( N = |\text{sni}(C)^{ab}| \).

Here is how we compute \( \text{ind}(a_{1j}) \). Denote the length of the orbit of \( s \in \text{sni}(C)^{ab} \) under \( a_{1j} \) by \( i_{1j}(s) \), \( j = 1, 2, 3 \). Then

\[
\text{(4.12) } \text{ind}(a_{1j}) = \sum_{s \in \text{sni}(C)^{ab}} \frac{i_{1j}(s) - 1}{i_{1j}(s)}.
\]

Check easily that

\[
\text{(4.13) } (s)a_{12} = ((s_1 s_2) s_1 (s_1 s_2)^{-1}, s_1 s_2 s_1^{-1}, s_3, s_4)
\]

\[
= (s_1, s_2, (s_1 s_2)^{-1} s_3 (s_1 s_2), (s_1 s_2)^{-1} s_4 (s_1 s_2))
\]

(in \( \text{sni}(C)^{ab} \)).

Thus, \( a_{12} \) acts by conjugation by \( s_1 s_2 \) on the third and fourth components and leaves the others unchanged. It follows that \( (s)(a_{12})^q = s \) in \( \text{sni}(C)^{ab} \) if and only if

\[
\text{(4.14) } (s_1, s_2, (s_1 s_2)^{-q} s_3 (s_1 s_2)^q, (s_1 s_2)^{-q} s_4 (s_1 s_2)^q)
\]

\[
= \kappa(s_1, s_2, s_3, s_4) \kappa^{-1}
\]

for some \( \kappa \in SN(C) \). For any subset \( A \) of \( G = (s) \), denote the centralizer of \( A \) in \( SN(C) \) by \( Z(A) \). Then, condition (4.14) is equivalent to this:

\[
\text{(4.15) There exists } \gamma \in Z(s_1, s_2) \text{ such that } \gamma (s_1 s_2)^{-q} \in Z(s_3).
\]

Hence, \( i_{12}(s) \) is the smallest integer \( q > 0 \) with \( (s_1 s_2)^{-q} \in Z(s_1, s_2) Z(s_3) \). Therefore, the factor group \( (s_1 s_2)/(s_1 s_2) \cap Z(s_1, s_2) Z(s_3) \) has order \( i_{12}(s) \). Similarly, check that

\[
(s)a_{12} = ((s_2 s_4)^{-1} s_1 (s_2 s_4), s_2, (s_4 s_2)^{-1} s_3 (s_4 s_2), s_4), \quad \text{and}
\]

\[
(s)a_{14} = (s_1, (s_4 s_1)^{-1} s_2 (s_4 s_1), (s_4 s_1)^{-1} s_3 (s_4 s_1), s_4) \quad \text{(in } \text{sni}(C)^{ab}).
\]

Thus, the integer \( i_{13}(s) \) (resp. \( i_{14}(s) \)) is the smallest integer \( q > 0 \) such that \( (s_4 s_2)^{-q} \in Z(s_2, s_4) Z(s_3) \) (resp., \( (s_4 s_1)^{-q} \in Z(s_1, s_4) Z(s_3) \)). Finally, we get

\[
\text{(4.16) } i_{12}(s) = |(s_1 s_2)/(s_1 s_2) \cap Z(s_1, s_2) Z(s_3)|,
\]

\[
i_{13}(s) = |(s_4 s_2)/(s_4 s_2) \cap Z(s_4, s_2) Z(s_3)|,
\]

\[
i_{14}(s) = |(s_4 s_1)/(s_4 s_1) \cap Z(s_4, s_1) Z(s_3)|.
\]
THEOREM 4.7. Assume the hypotheses of Theorem 4.3 and Theorem 4.5. Then, (4.11) gives the genus \( g(C) \), where (4.12) and (4.16) give \( \text{ind}(a_{12}), \text{ind}(a_{13}) \) and \( \text{ind}(a_{14}) \).

4.4. Symmetric groups. In this section, \( n = 2p+1 \) is an odd prime and the group \( G \) is the symmetric group \( S_n \) embedded in itself. Condition (4.1) holds. Consider the following involutions of \( S_n \):

\[
\begin{align*}
\alpha_1 &= (2n - 1)(3n - 2) \cdots (p - 1) p + 3)(p + 2) ; \\
\alpha_2 &= (n)(2n - 1)(3n - 2) \cdots (p - 1)(p + 3)(p + 2) ; \\
\alpha_3 &= (1n - 1)(2n - 2)(3n - 3) \cdots (p - 1)(p + 2)(p + 1).
\end{align*}
\]

Since these generate a transitive subgroup of \( S_n \), it is easy to see that they generate all of \( S_n \). Indeed, as \( n \) is a prime, the representation is primitive. It is well known that a primitive subgroup of \( S_n \) containing a 2-cycle is all of \( S_n \). As \( \alpha_1 \alpha_2 \) is a 2-cycle, we are done. Therefore, condition (1.2) is satisfied.

Here is the 4-tuple \( s(\alpha) = (s_1, s_2, s_3, s_4) \) of (3.2):

\[
\begin{align*}
s_1 &= \alpha_1 = (2n - 1)(3n - 2) \cdots (p - 1)(p + 3)(p + 2) ; \\
s_2 &= \alpha_1 \alpha_2 = (1n) ; \\
s_3 &= \alpha_2 \alpha_3 = (n - 1 \cdots 2 1) ; \\
s_4 &= \alpha_3 = (1n - 1)(2n - 2)(3n - 3) \cdots (p - 1)(p + 2)(p + 1).
\end{align*}
\]

Order \( C_1, C_2, C_3, C_4 \) so they respectively denote the conjugacy classes of \( s_4, s_1, s_2, s_3 \). Thus \( (s_1, s_2, s_3, s_4) \in \text{ni}(C)^{ab} \) and \( (s_4, s_1, s_2, s_3) \in \text{ni}(C)^{ab} \). Specifically, we have: \( C_1 = \{ \text{products of } p \text{ disjoint 2-cycles} \} \); \( C_2 = \{ \text{products of } p - 1 \text{ disjoint 2-cycles} \} \); \( C_3 = \{2\text{-cycles}\} \); \( C_4 = \{n\text{-cycles}\} \). Any conjugacy class in \( S_n \) is rational. In particular, these are.

We now investigate the Hurwitz monodromy action on \( \text{ni}(C)^{ab} \).

First, a lemma helps us list the elements in \( \text{ni}(C)^{ab} \). In the following, for \( s, \omega \in S_n \), we let \( s^\omega \) denote the conjugate of \( s \) under \( \omega \) (i.e., \( s^{\omega} = \omega^{-1} s \omega \)). For \( i \in \{1, \ldots, n\} \), \( i^\omega \) is the integer \( (i)\omega \).

**Lemma 4.8.** Let \( a, b \in S_n \) be involutions. Let \( O \) be a disjoint cycle in \( ab \) that contains an integer \( \rho_0 \) fixed by \( b \). There are two possibilities.

(i) \( O = (\rho_0 \rho_1 \cdots \rho_t \rho_1^t \cdots \rho_t^t) \) with \( t \geq 0 \) and none of the integers \( \rho_i, \ i > 0, \) fixed by \( b \); \( \rho_1 \) is then fixed by \( a \) and \( O \) is a cycle of odd length.
(ii) $O = (\rho_0\rho_1 \cdots \rho_t\rho^b_0\rho^b_1 \cdots \rho^b_t)$ with $t \geq 0$ and none of the integers $\rho_i$, $i > 0$, fixed by $b$; $\rho^b_0$ is then fixed by $b$ and $O$ is a cycle of even length.

Conversely, we have these partial products from $Ob$.

(i') $(\rho_0\rho_1 \cdots \rho_t\rho^b_0\rho^b_1 \cdots \rho^b_t)(\rho_1\rho^b_1) \cdots (\rho_t\rho^b_t)$ is a product of $t$ disjoint 2-cycles.

(ii'') $(\rho_0\rho_1 \cdots \rho_t\rho^b_0\rho^b_1 \cdots \rho^b_t)(\rho_1\rho^b_1) \cdots (\rho_t\rho^b_t)$ is a product of $t+1$ disjoint 2-cycles.

**Proof.** Conjugation by $b$ turns $ab$ into $(ab)^{-1}$. Therefore, $(O^b)^{-1}$ is a disjoint cycle in $ab$. Since $O$ and $(O^b)^{-1}$ have an integer in common, namely $\rho_0$, we obtain $O = (O^b)^{-1}$. The only cycles with that property are those described in statement (i) and (ii) of Lemma 4.8. The converse statements (i') and (ii') are immediate. \(\square\)

We now show there is a one-to-one correspondence between the elements of $\text{sni}(\mathbb{C})^{ab}$ and the subset $S$ of $\mathbb{N}^3$ of triples $[\mu, \beta, \gamma]$ satisfying

$$1 \leq \mu \leq p; \quad 1 \leq \beta \leq 2\mu - 1; \quad p + \mu + 1 \leq \gamma \leq n.$$ 

Start with this observation. Every element of the absolute straight Nielsen class $\text{sni}(\mathbb{C})^{ab}$ has a unique representative $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ with $\sigma_4 = (n\, n - 1 \cdots 1)$ and $\sigma_3 = (1\, 2\mu), \; \mu \in \{1, \ldots, p\}$. Existence is easy. Lemma 4.9 below (and $\text{Cen}(S_n) = \{1\}$) gives uniqueness.

**Lemma 4.9.** The group $S_n$ is generated by $\sigma_3$ and $\sigma_4$.

**Proof.** Consider a partition $I$ of $\{1, \ldots, n\}$. We say that $I$ is a set of imprimitivity for a subgroup $H$ of $S_n$, if $H$ permutes the elements of $I$. Sets of imprimitivity of the $n$-cycle $(n\, n - 1 \cdots 1)$ are the cosets modulo a nontrivial divisor of $n$. Since $n$ is prime, $\langle \sigma_3, \sigma_4 \rangle$ is a primitive subgroup of $S_n$, which contains a 2-cycle. Therefore, it is all of $S_n$. \(\square\)

For the representative $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ above, we obtain

$$\sigma_1\sigma_2 = (\sigma_3\sigma_4)^{-1} = (1\, 2\cdots 2\mu - 1)(2\mu\, 2\mu + 1 \cdots n).$$

Both $\sigma_1$ and $\sigma_2$ are of order 2 and $\sigma_2$ fixes 3 integers. Lemma 4.8 shows that only one of these integers, say $\beta$, occurs in the odd length cycle $(1\, 2\cdots 2\mu - 1)$ of $\sigma_1\sigma_2$. The two other integers fixed by $\sigma_2$ appear in the even length cycle $(2\mu\, 2\mu + 1 \cdots n)$. Denote the integer fixed by $\sigma_2$ that is in the second half of $\{2\mu, 2\mu + 1, \ldots, n\}$ by $\gamma$. 
That is, \( \gamma \) is in the set \( \{p + \mu + 1, \ldots, n\} \). This defines a triple \([\mu, \beta, \gamma]\) which lies in the set \( S \). The next proposition gives us the genus of covers with branch cycles coming from our previous lemmas. In §4.5 we draw conclusions from this about Question 4.1. Since the result is not terribly positive, §4.6 makes further comment on what we can expect from variations of this technique.

**Proposition 4.10.** The map \( \text{sni}(C)^{ab} \rightarrow S \) that assigns to each element of \( \text{sni}(C)^{ab} \) the triple \([\mu, \beta, \gamma]\) defined above is one-one and onto. In particular,

\[
|\text{sni}(C)^{ab}| = \sum_{1 \leq \mu \leq p} (2\mu - 1)(p - \mu + 1) = \frac{p(p + 1)(2p + 1)}{6}.
\]

**Proof.** Let \([\mu, \beta, \gamma]\) be a triple in \( S \). Set \( \sigma_{4} = (n \ n - 1 \ 1) \) and \( \sigma_{3} = (1 \ 2\mu) \). We need to show that there is a unique pair \((\sigma_{1}, \sigma_{2})\) with these properties:

(4.16) \( \sigma = (\sigma_{1}, \sigma_{2}, \sigma_{3}, \sigma_{4}) \in \text{sni}(C) \) and \( \sigma_{2} \) fixes \( \beta \) and \( \gamma \).

**Existence.** One has \((\sigma_{3}\sigma_{4})^{-1} = (1 \ 2 \ 2\mu - 1)(2\mu \ 2\mu + 1 \ \cdots n)\). Using Lemma 4.8 (i') and (ii'), write \((1 \ 2 \ 2\mu - 1) = a'b'\) with \( a' \) and \( b' \) products of \((\mu - 1)\) 2-cycles with support in \( \{1, 2, \ldots, 2\mu - 1\} \) and \( \beta \) fixed by \( b' \). Also, \((2\mu \ 2\mu + 1 \ \cdots n) = a''b''\) with \( a'' \) and \( b'' \) products of respectively \((n-2\mu+1)/2\) and \((n-2\mu-1)/2\) 2-cycles with support in \( \{2\mu, 2\mu + 1, \ldots, n\} \) and \( \gamma \) fixed by \( b'' \). Take \( \sigma_{1} = a'a'' \) and \( \sigma_{2} = b'b'' \). The 4-tuple \( \sigma = (\sigma_{1}, \sigma_{2}, \sigma_{3}, \sigma_{4}) \) has the required properties (4.16).

**Uniqueness.** \( \sigma_{1} \) and \( \sigma_{2} \) satisfy

\[
\sigma_{1}\sigma_{2} = (1 \ 2 \cdots 2\mu - 1)(2\mu \ 2\mu + 1 \ \cdots n).
\]

From Lemma 4.8 (i) and (ii), \((1 \ 2 \cdots 2\mu - 1)\) is of the form \((\rho_{0}\rho_{1}\cdots\rho_{t_{1}}\rho_{t_{1}'}\cdots\rho_{1}^{2})\) with \( \rho_{0} = \beta \), and \((2\mu \ 2\mu + 1 \ \cdots n)\) is of the form \((\tau_{0}\tau_{1}\cdots\tau_{t_{2}}\tau_{t_{2}'}\cdots\tau_{1}^{2})\) with \( \tau_{0} = \gamma \). This determines \( \sigma_{2} \) on \( \{1, 2, \ldots, 2\mu - 1\} \) and on \( \{2\mu, 2\mu + 1, \ldots, n\} \) (i.e., on all of \( \{1, \ldots, n\} \)).

In the rest of this section identify each element of \( \text{sni}(C)^{ab} \) with its image in \( S \). The next step consists in computing indices of \( a_{12}, a_{13}, a_{14} \) acting on \( \text{sni}(C)^{ab} \).

**Index of \( a_{12}.** Let \( s = [\mu, \beta, \gamma] \in \text{sni}(C)^{ab} \); the centralizer \( Z(s_{1}, s_{2}) \) is the subgroup of \( S_n \) generated by \((2\mu \ 2\mu + 1 \ \cdots n)^{p-\mu+1}\). Indeed, let
$t \in Z(s_1, s_2)$. Then $t$ commutes with
$$s_1s_2 = (1 2 \cdots 2\mu - 1)(2\mu 2\mu + 1 \cdots n).$$

Therefore, $t$ is of the form $(1 2 \cdots 2\mu - 1)^h(2\mu 2\mu + 1 \cdots n)^k$. Since $t$ fixes $\beta$ and permutes the 2 other fixed points of $s_2$, $h = 0$ and $k = \lambda(p - \mu + 1)$, for some integer $\lambda$. Recall from §4.3, the integer $i_{12}(s)$ is the smallest integer $q > 0$ such that, for some integer $\lambda$,
$$(1 2 \cdots 2\mu - 1)^q(2\mu 2\mu + 1 \cdots n)^q = (1^{\lambda(p+\mu-1)})$$
commutes with $s_3 = (1 2\mu)$ (i.e., fixes the pair $\{1, 2\mu\}$).

The two disjoint cycles $(1 2 \cdots 2\mu - 1)$ and $(2\mu 2\mu + 1 \cdots n)$ of $s_1s_2$ are of relatively prime order. Thus, $i_{12}(s) = (2\mu - 1)(p - \mu + 1)$.

Formulas (4.16) gives this:
$$\operatorname{ind}(a_{12}) = \sum_{1 \leq \mu \leq p} (2\mu - 1)(p - \mu + 1)
\left(1 - \frac{1}{(2\mu - 1)(p - 2\mu + 1)}\right)
= N - p = \frac{p(p - 1)(2p + 5)}{6}.$$
• If \(2\mu - 1 = p_1\), we obtain \((2\mu)(s_4s_2)^3 = 2\mu\) and \((1)(s_4s_2)^3 = 1\).

Hence \(i_{13}(s) = 3\).

The number of occurrences of \(\bullet\) is

\[
\sum_{1 \leq \mu \leq p} (p - \mu + 1) = \frac{p(p + 1)}{2},
\]

\(p - \mu + 1\) for each value of \(\mu\). Therefore, \(\text{ind}(a_{13}) = p(p + 1)^2/6\).

**Index of \(a_{14}\).** Let \(s = [\mu, \beta, \gamma] \in \text{sni}(C)_{ab}\). Again, the centralizer \(Z(s_1, s_4)\) is trivial. The integer \(i_{14}(s)\) is the smallest integer \(q > 0\) such that \((s_4s_1)^q = (s_2s_3)^{-q}\) fixes the pair \(\{1, 2\mu\}\). The calculation depends on the intersection set \(\{1, 2\mu\} \cap \{1^{s_2}, (2\mu)^{s_2}\}\). Note: By construction of \([\mu, \beta, \gamma]\), \(1 \leq 1^{s_2} \leq 2\mu - 1\) and \(2\mu \leq (2\mu)^{s_2} \leq n\). So we only have 4 cases to consider.

1st case. \(1^{s_2} = 1\) and \((2\mu)^{s_2} = 2\mu\). That is, \(s = [\mu, 1, \mu + p + 1]\).

Here, \(i_{14}(s) = 1\).

2nd case. \(1^{s_2} \neq 1\) and \((2\mu)^{s_2} = 2\mu\). That is, \(s = [\mu, \beta, \mu + p + 1]\)

with \(\beta \neq 1\). Here, \((2\mu)(s_2s_3)^3 = 2\mu\) and therefore, \((1)(s_2s_3)^3 = 1\).

Thus \(i_{14}(s) = 3\). (Note that \(i_{14}(s) \neq 1\) since \(1^{s_2} \neq 1, 2\mu\).)

3rd case. \(1^{s_2} = 1\) and \((2\mu)^{s_2} \neq 2\mu\). That is, \(s = [\mu, 1, \gamma]\) with \(\gamma \neq \mu + p + 1\). This is exactly as in the 2nd case.

4th case. \(1^{s_2} \neq 1\) and \((2\mu)^{s_2} \neq 2\mu\). Here, \((1)(s_2s_3)^2 = 2\mu\) and thus, \((2\mu)(s_2s_3)^2 = 1\).

Therefore, \(i_{14}(s) = 2\).

We have only to count the possibilities for \(s\) in each case: \(p\) for the first case, \((2\mu - 2)\) for each \(\mu\) of the second case, \((p - \mu)\) for each \(\mu\) for the third case, and the rest for the fourth case. The result:

\[
\text{ind}(a_{14}) = \sum_{1 \leq \mu \leq p} \frac{2}{3}(\mu + p - 2) + \frac{1}{2} \left[ N - p - \sum_{1 \leq \mu \leq p} (\mu + p - 2) \right].
\]

Finally, \(\text{ind}(a_{14}) = \frac{p(p-1)(p+3)}{6}\).

Now (4.11) gives the genus \(g(C)\) of \(C(C)\) (cf. Theorem 4.5):

\[
g(C) = \frac{(p - 2)(p - 3)}{6}.
\]

Thus, Question 4.1 has a positive answer for \(p = 2, 3\) (i.e., \(n = 5, 7\)). There is one condition, however, in Theorem 4.3 we have not checked yet: transitivity of \(SH_r\) on \(\text{sni}(C)_{ab}\). We use two steps.

From (4.13), \(a_{12} = Q^2_1\) conjugates by \(s_1s_2\) on the first two components of the 4-tuple \(s\) and leaves the others unchanged. So for
s = [μ, β, γ], we obtain:

\[ [μ, β, γ]_{a_{12}} = [μ, (β)(s_1s_2)^{-1}, (γ)(s_1s_2)^{-1}] \]

Still, the two disjoint cycles \((1 2 \cdots 2μ - 1)\) and \((2μ 2μ + 1 \cdots n)\) of \(s_1s_2\) are of relatively prime order. Therefore, the group generated by \(s_1s_2\) acts transitively on the ordered pairs \((β, γ)\) with \(1 ≤ β ≤ 2μ - 1\) and \(p + μ + 1 ≤ γ ≤ n\). Conclude that the orbits of \(a_{12}\) are the \(p\) subsets of \(\text{sni}(C)^{ab}\) corresponding to each value of \(μ\).

Now consider \(a_{13}\). We are done if we show that for any \(μ = 1, \ldots , p\), \(a_{13}\) sends some element \([1, 1, γ]\) to some element \([μ, β', γ']\). For \(s = [1, 1, γ]\), \(a_{13}\) leaves \(s_2\) and \(s_4\) unchanged and turns \(s_3 = (1 2)\) into

\[ (s_4s_2)^{-1}s_3(s_4s_2) = (1^5s_2; 2^5s_2) = (n^5; 1). \]

That is, \(a_{13}\) sends some element \([1, 1, γ]\) on some element \([μ, β', γ']\) with \((1 2μ) = (1 n^5)\), up to conjugation by a power of \(s_4\).

We have \(s_1s_2 = (1)(2 3 \cdots n)\). Lemma 4.8 (ii) implies the cycle \((2 3 \cdots n)\) has form \((ρ_0ρ_1 \cdots ρ_tρ_0^{β}ρ_t^{β'} \cdots ρ_t^{β})\) with \(ρ_0 = γ\). Check: when \(γ\) ranges over \(\{p + 2, \ldots , n\}\), \(n^5;\) takes on all values in \(\{3, 5, \ldots , n\}\). That is, \(2μ\) takes on all values in \(\{2, 4, \ldots , n - 1\}\).

### 4.5. Conclusions from §4.4 Example.

**Theorem 4.11.** For \(n = 5, 7\), \(S_n\) is the Galois group of a regular extension \(E/\mathbb{Q}(T)\) with these properties:

- (i) \(E/\mathbb{Q}(T)\) is ramified over 4 rational points; and
- (ii) for all \(t\) in a nonempty interval of the real line, the residue class extension \(E_t/\mathbb{Q}\) is a totally real extension.

*End of proof.* For \(n = 5, 7\), (4.18) yields \(g(C) = 0\). Hence, the curve \(C(C)\) is \(\mathbb{P}^1\) if it has a \(\mathbb{Q}\)-rational point. The disjoint cycles in the permutation \(a_{12}\) of \(\text{sni}(C)^{ab}\) are in 1-1 correspondence with the points over the branch point \(x_2 \in \mathbb{P}^1\) in the cover \(C(C) \to \mathbb{P}^1\) of Theorem 4.5. The previous study of \(a_{12}\) shows, for \(n = 5\) (resp., \(n = 7\)), there are 2 ramified points (resp., 3 ramified points) over \(x_2\) of ramification indices 1, 3 (resp., 3, 5, 6). Each of these points has a unique ramification index. Thus, these points are rational over \(\mathbb{Q}(x_2, x_3, x_4)\).

Consider \((γ, x_2, x_3, x_4)\) on \(C(C) \times \mathbb{P}^1 \times \mathbb{P}^1 \times \mathbb{P}^1\) with \(γ\) not lying over one of \(x_2, x_3, x_4\). From Proposition 4.4 and Corollary 4.6, each such \(\mathbb{Q}\)-rational point corresponds to a cover \(ψ: Y_C \to \mathbb{P}^1\) defined...
over \( \mathbb{Q} \). Equivalently, such a point corresponds to a regular extension \( Y/\mathbb{Q}(T) \), with 4 rational branch points and monodromy group \( S_5 \) (resp., \( S_7 \)).

Pick a \( \mathbb{Q} \)-rational point \((y, x_2, x_3, x_4)\) that corresponds to a cover having the 4-tuple \((\alpha_1, \alpha_1\alpha_2, \alpha_2\alpha_3, \alpha_3)\) as a branch cycle description. (This is with respect to a bouquet as in §2.3.) The \( \mathbb{Q} \)-points are dense in the space \( \mathscr{M}(\mathbb{C})'(\mathbb{R}) \). Thus, such a choice of point is possible. Choose \( x_0 \) between \( x_1 \) and \( x_4 \) on the real projective line. The remark in §3.4 shows that the action of complex conjugation is trivial on the fiber \( \psi^{-1}(x_0) \). That is, in the notation of §3.4, \( \overline{c} = 1 \). Let \( E/\mathbb{Q}(T) \) be the Galois closure of the extension \( Y/\mathbb{Q}(T) \). It is a regular extension with properties (i) and (ii).

\[ \square \]

4.6. \textit{Additions to Theorem 4.11.}

\textit{Comment (1).} The §4.4 method applies to any 3-tuple \((\alpha_1, \alpha_2, \alpha_3)\) of generators of \( S_n \) of order 2. For example, we have computed with \( n = 2p \) where \( p \) is an odd prime and

\[
\begin{align*}
\alpha_1 &= (1 \, n), \\
\alpha_2 &= (2 \, n)(3 \, n - 1)(4 \, n - 2) \cdots (p - 1 \, p + 3)(p \, p + 2), \\
\alpha_3 &= (1 \, n)(2 \, n - 1)(3 \, n - 2) \cdots (p - 1 \, p + 2)(p \, p + 1).
\end{align*}
\]

The associated curve \( C(\mathbb{C}) \) has genus \( g(\mathbb{C}) = \frac{1}{8}(p - 3)(p - 5) \). That is, the conclusion of Theorem 4.11 holds for \( n = 6 \) and \( n = 10 \). It also holds for the special case \( n = 4 \). Here, take \( \alpha_1 = (2 \, 3) \), \( \alpha_2 = (1 \, 4)(2 \, 3) \), and \( \alpha_3 = (1 \, 3) \).

\textit{Comment (2).} There is only one centerless group \( G \) for which Theorem 4.11 is true with 3 branch points instead of 4 branch points: \( G = S_3 \) ([Se2], [FrD]). If we allow a center, there are other candidates: the groups \( \mathbb{Z}/m \times \mathbb{Z}/2 \), for \( m = 2, 4, 6 \). Moreover, the group \( \mathbb{Z}/2 \times \mathbb{Z}/2 \) does satisfy the conclusions of Theorem 4.11 for 3 branch points.

5. \textbf{Two further applications.} The dihedral group \( D_m \) is the easiest non-abelian finite group. The reader must be surprised to hear that there are serious questions about realizing it as a Galois group of a regular extension \( L/\mathbb{Q}(x) \). The problem is not realizing the group, it is realizing it with extensions having few branch points. The problem is similar to that of §4: finding rational points on variants of Hurwitz spaces defined over \( \mathbb{Q} \) as in §4.5. There we could only proceed when we knew that a certain curve \( C(\mathbb{C}) \) was of genus 0.
Suppose, however, that the curve is of genus greater than 0. It could still have rational points on it. One rational point was all we needed to conclude realization of the groups with the properties of §4.5. With dihedral groups we can interpret existence of rational points even when the number of branch points is large. We owe this to identifications of the particular Hurwitz spaces with variants on classical modular curves. Section 5.1 gives a definitive result when the number of branch points is less than 6. Section 5.2 considers larger values of $r$ based on generalizations of Mazur's theorem.

Finally, we illustrate a new large field over which we know that all groups are Galois groups of regular extensions. For each prime $p$, there is a field $\mathbb{Q}_p^t$, the *totally $p$-adic* algebraic numbers. An algebraic number $\alpha$ is in $\mathbb{Q}_p^t$ if each conjugate of $\alpha$ is in $\mathbb{Q}_p$, the $p$-adic numbers. Section 5.3 considers the case of the real valuation.

5.1. Dihedral groups with $r$ small. In this section, $m$ is an odd prime. Consider the dihedral group $D_m = \mathbb{Z}/m \rtimes \mathbb{Z}/2$ in its regular representation. The order of $D_m$ is $n = 2m$. Two involutions generate it.

**Theorem 5.1.** For $m > 7$ a prime, $D_m$ is not the Galois group of a regular extension of $\mathbb{Q}(X)$ with 5 or fewer branch points.

**Proof.** Assume that $G = D_m$ is the Galois group of a regular extension $Y/\mathbb{Q}(X)$. Let $\Phi : Y_C \to \mathbb{P}^1$ be the associated cover. Take $x_1, \ldots, x_r$ to be an ordering of the branch points. Identify $G$ with the monodromy group of the cover. For $i = 1, \ldots, r$, let $C_i$ be the conjugacy class of the branch cycles associated with $x_i$. That is, the cover is in $\text{sni}(C_1, \ldots, C_r)$. We divide the proof into 2 cases. Let $C$ be the conjugacy class of all involutions in $G$: $C = \{(a, 1) | a \in \mathbb{Z}/m\}$.

1st case. One of $C_1, \ldots, C_r$, say $C_i$, is different from $C$. Let $(a, 0) \in C_i$. This is an element of order $m$ and its nontrivial powers lie in $(m - 1)/2$ distinct conjugacy classes of $G$. We show that $r \geq (m - 1)/2 \geq 5$. Indeed, this follows from the rationality properties that the inertia groups inherit from the rationality of the cover. Specifically, apply the branch cycle argument §3.7, expression (3.9) in the following form. The order of $C_i$ is the order of the elements in $C_i$.

(5.1) For each $i \in \{1, \ldots, r\}$, for all $\alpha$ relatively prime to the order of $C_i$, $c_i^\alpha = C_j$ for some $j \in \{1, \ldots, r\}$.
To complete the first case we show $r \neq 5$. For $r = 5$, $G = D_{11}$ and $C_1, \ldots, C_5$ are conjugacy classes of 11-cycles. These classes, however, do not generate $D_{11}$, a contradiction.

2nd case. $C_1 = \cdots = C_r = C$. Observe that $r \neq 2$ when $g$ is not a cyclic group. Also, that $r \neq 3, 5$; the relation $s_1 \cdots s_r = 1$ implies that $r$ is even. Assume $r = 4$. The Riemann-Hurwitz formula yields the genus $g$ of the cover $\Phi: Y_C \to \mathbb{P}^1$:

$$m + m + m + m = 2(n + g - 1).$$

That is, $g = 1$. In addition, the elliptic curve $Y_C$ has an automorphism $\chi$ of order $m$, for example $(1, 0)$.

Assume first that $Y_C(\mathbb{Q}) \neq \emptyset$: $Y_C$ is an elliptic curve over $\mathbb{Q}$. Translation by a point $p$ of order $m$ on $Y_C$ gives $\chi$. Since $Y/\mathbb{Q}(X)$ is regular, $\chi$ is defined over $\mathbb{Q}$ and $p$ is a rational point in $Y_C$.

Thus, we have produced an elliptic curve $Y_C$ and a point $p$ of order $m$. Both are defined over $\mathbb{Q}$. It is classical that the data $(Y_C, p)$ corresponds to a rational point on the modular curve $X_1(m) \setminus \{\text{cusps}\}$. As $m > 7$, this contradicts Mazur's theorem [Sel; Theorem 3] (or [M], [MS]).

If $Y_C(\mathbb{Q}) = \emptyset$, the same argument works on the Jacobian $\text{Pic}^0(Y_C)$ of $Y_C$. Recall: $\text{Pic}^0(Y_C)$ consists of divisor classes of degree 0 on $Y_C$. The automorphism group of $Y_C$ naturally embeds as automorphisms of $\text{Pic}^0(Y_C)$. Thus, this is an elliptic curve over $\mathbb{Q}$. And, it has an automorphism of order $m$ defined over $\mathbb{Q}$. Therefore, $r \neq 4$. \hfill \Box

5.2. Bounding $r$ with dihedral groups. This subsection discusses Conjecture 5.2.

Conjecture 5.2. Let $m$ run over odd primes. There is no finite $r_0$ such that each $D_m$ is the group of a regular Galois extension $L/\mathbb{Q}(x)$ with at most $r_0$ branch points.

Kamienny and Mazur have recent results that approach what we need to show this conjecture [M]. Suppose that such a bound $r_0$ as in the conjecture exists. The proof of Theorem 5.1 shows we can realize only a finite number of the $D_m$s under the following conditions. At least one inertia group generator is an $m$-cycle and there are no more than $r_0$ branch points. We restate the conjecture as follows.

Conjecture 5.2'. Realization of $L/\mathbb{Q}(x)$ with group $D_m$ and all inertia group generators involutions requires more than $r_0$ branch points if $m$ is suitably large.
We call a Galois realization of $D_m$ over $\mathbb{Q}$ satisfying the condition that all inertia group generators are involutions an \textit{involution realization} of $D_m$. Consider such an involution realization.

The fixed field $T$ of an automorphism of order $m$ is a degree 2 extension of $\mathbb{Q}(x)$ ramified over $r$ (even) points. Also, $L/T$ is a cyclic unramified extension of degree $m$. That is, $T$ is the function field of a hyperelliptic curve of genus $\frac{r-2}{2}$.

We want $\varphi: \tilde{X} \to \mathbb{P}^1$ of degree $2m$ with a description of the branch cycles of form $(\sigma_1, \ldots, \sigma_r)$. Here, each $\sigma_i$ is in the conjugacy class $C$ (§5.1) of involutions. A complete combinatorial count of these is easy. At least two of these are not equal (to generate $D_m$). Write $\sigma_i = (a_i, 1)$. Then, the product of the $\sigma$s is 1 reduces to $a_1 - a_2 - \cdots - a_r = 0$. Calculations are sufficiently easy to compute elements $a_{ij}, j = 2, \ldots, r$ that generalize those in §4.2. Their action on $\text{sn}i(C)$ is transitive. Formula (4.11), with $r$ replacing 4, gives the genus of the analog of $C(C)$. The computation shows this grows quadratically with $r$ when $m$ is fixed. The 1st complex cohomology group of a projective algebraic variety is a birational invariant. Consider the analog for general $r$ of Theorem 4.5. Conclude that the variety $\mathcal{H}(C)'$ for this Nielsen class cannot be \textit{unirational} if $r$ is large. (See Problem 5.6.)

The variety $\mathcal{H}(C)'$ covers the actual variety $\mathcal{H}(C) = \mathcal{H}(r, m)$ that parametrizes the equivalence classes of covers that we want. Consider $\mathcal{H}(C)'$ as the parameter space for these covers with some ordering on the branch points of the covers. From [FrV2] there is a variety $\mathcal{H}(C)^{\text{in}} = \mathcal{H}(r, m)^{\text{in}}$, defined over $\mathbb{Q}$, whose rational points give us the desired extensions. Rational points exactly correspond to regular field extensions $L/\mathbb{Q}(x)$ that give involution realizations of $D_m$. Below we use cover notation. These field extensions correspond to Galois covers $\varphi: \tilde{X} \to \mathbb{P}^1$ defined over $\mathbb{Q}$ with group $D_m$. Our problem is to decide if $\mathcal{H}(r, m)^{\text{in}}$ has $\mathbb{Q}$ points. We relate $\mathcal{H}(r, m)^{\text{in}}$ to more classical looking objects.

Take $\alpha \in D_m$ of order $m$. Form $\tilde{X}/\langle \alpha \rangle = Y$, the quotient of $\tilde{X}$ by the group generated by $\alpha$. The degree 2 cover $Y \to \mathbb{P}^1$ presents $Y$ as a hyperelliptic curve of genus $\frac{r-2}{2}$. Also, $\tilde{X}$ is a cyclic degree $m$ unramified cover of $Y$. Lemma 5.3 interprets existence of $\tilde{X}$ as a property of $\text{Pic}^0(Y)$, the Picard group of divisor classes of degree 0 on $Y$. Denote the points of order $m$ on $\text{Pic}^0(Y)$ by $T_m = T_m(Y)$. Then, $G(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ acts on $T_m$. If $p \in T_m \setminus \{0\}$ is a point defined over $\mathbb{Q}$, then $G(\overline{\mathbb{Q}}/\mathbb{Q})$ has trivial action $\langle p \rangle$. When a point has this property, denote the group it generates by $\mathbb{Z}/m$. This says $G_{\mathbb{Q}}$ has trivial action on it.
Similarly, $G_Q$ acts on the $m$th roots of 1. This is another copy of $\mathbb{Z}/m$, but to show $G_Q$ has a particular nontrivial action on it, denote it by $\mu_m$. Consider the set $G_m(d) = \mathbb{Z}/2$, of involution realizations of $D_m$, as above with $r$ branch points, defined over $\mathbb{Q}$. Let $Pic^1(Y)$ be the Picard space of divisor classes of degree 1 on $Y$.

**Lemma 5.3.** Continue the notation above. The set of involution realizations of $D_m$ associated to a fixed $Y$ as above naturally inject into the set of $G_Q$ equivariant injections from $\mu_m$ into $T_m(Y)$. The image of this map includes all $G_Q$ equivariant injections $\mu_m \to T_m(Y)$ when $Pic^1(Y)$ has a $\mathbb{Q}$ point.

**Proof.** Consider multiplication by $m$ on $Pic^0(Y)$. Denote this endomorphism by $\psi_m$. The kernel is exactly $T_m$. Since $Y$ consists of positive divisors of degree 1, $Y$ naturally embeds in $Pic^1(Y)$ (assuming $g(Y) > 0$—that is, $r \geq 4$). Suppose we have an involution realization of $D_m$ attached to $Y$ as above. Universal properties of $Pic^0(Y)$ produce a natural surjective $G_Q$ equivariant map $T_m(Y) \to \mathbb{Z}/m$. Here $\mathbb{Z}/m$ represents the Galois group of the cover $\tilde{X} \to Y$ as above. Below we show how this gives an injection from $\mu_m$ into $T_m(Y)$.

Suppose $q \in Pic^1(Y)$ is defined over $\mathbb{Q}$. Define translation $\lambda_q: Pic^1(Y) \to Pic^0(Y)$ as the map that takes a divisor class $[D]$ of degree 1 to $[D - q]$. Denote the image of $Y$ under $\lambda_q$ by $Y_q$. This curve in $Pic^0(Y)$ is isomorphic to $Y$ over $\mathbb{Q}$. The preimage $\psi_m^{-1}(Y) = Y_{m,q}$ is the maximal exponent $m$ abelian unramified geometric cover of $Y$. At least that is correct over $\overline{\mathbb{Q}}$. We cannot expect the automorphisms to be defined over $\mathbb{Q}$.

We want a $G_Q$ invariant hyperplane $V$ in $T_m$ such that the quotient $T_m/V$ is a copy of $\mathbb{Z}/m$. That is, $G_Q$ acts trivially on the quotient. In more homological terms, we want a surjective element $\beta \in Hom_{G_Q}(T_m, \mathbb{Z}/m) \overset{\text{def}}{=} M$. Then, $V$ is the kernel of $\beta$.

**Conclusion.** The quotient $Y_{m,q}/V = Y_{m,q}/T_m = Y_q$ is the cyclic unramified cover we seek. We have identified its automorphism group with $\mathbb{Z}/m$ with trivial $G_Q$ action. That is, the automorphisms are defined over $\mathbb{Q}$. The lemma is complete—from the first paragraph of proof—when we have shown how to go from an injective map $\beta: \mu_m \to T_m$ to a $\beta$ above.

The abelian variety $Pic^0(Y)$ is principally polarized. That means it is isomorphic to its dual abelian variety. This is the abelian variety of
linear equivalence classes of divisors on \( \text{Pic}^0(Y) \) that are algebraically equivalent to 0. In particular, the Weil pairing produces a nondegenerate symplectic form \( w: T_m \times T_m \to \mu_m \) [L]. Thus, \( \text{Hom}_{G_Q}(T_m, \mu_m) \) is isomorphic to \( T_m \) as a \( G_Q \) module.

Apply \( \text{Hom}_{G_Q}(. , \mu_m) \) to the map \( \beta: \mu_m \to T_m \). This gives

\[
\beta: \text{Hom}_{G_Q}(\Gamma_m, \mu_m) \to \text{Hom}_{G_Q}(\mu_m, \mu_m).
\]

The first term identifies to \( T_m \). Check easily that the second term is just \( \mathbb{Z}/m \) acting as multiplications.

\[\square\]

 Remark 5.4. When \( \text{Pic}^1(Y)(\mathbb{Q}) \) is empty. The proof of Lemma 5.3 used a \( \mathbb{Q} \) point in \( \text{Pic}^1(Y) \) to construct the cover \( Y_m \to Y \) canonically. We have not shown that a \( \mu_p \) point on \( \text{Pic}^0(Y) \) produces the Galois sequence of an involution realization of \( D_m \). This is a subtler problem.

We can interpret this as a question on the fibers of a map of the Hurwitz space \( \mathcal{H}(C)^{\text{in}} = \mathcal{H}(r,m)^{\text{in}} \) to the space of cyclic order \( m \) subgroups of \( m \) division points on hyperelliptic jacobians. These fibers are homogeneous spaces for the action of \( \text{PGL}(2) \). If the image of a fiber is a \( \mu_m \) point, when does the fiber have a rational point?

We list some boundedness assertions. Then, we comment on how these effect Conjecture 5.2.

1. Let \( S(d) \) be primes that are orders of rational points on the elliptic curve defined over some number field \( K \) with \( [K: \mathbb{Q}] \leq d \).

2. Let \( T(d) \) be primes that are orders of rational points on some abelian variety of dimension \( d \) over \( \mathbb{Q} \).

3. Let \( V(d) \) be primes \( m \) that are orders of \( G_Q \) modules isomorphic to \( \mu_m \) in abelian varieties over \( \mathbb{Q} \) of dimension \( d \).

4. Let \( W(d) \) be elements of \( V(d) \) from jacobians of hyperelliptic curves of genus \( d \).

The results of [M] include this: \( S(d) \) is finite for \( d < 9 \). In addition, \( S(d) \) is of density zero for all \( d \). According to Lemma 5.3, a density 0 result for \( V(d) \) would be a satisfactory contribution to Conjecture 5.2. Mazur communicated the following observations.

Proposition 5.5. We have \( S(d) \subset T(d) \). Also, if \( m \in V(d) \), then \( m \in T((m - 1)d) \).

Proof. Suppose \( E \) is an elliptic curve over \( K \) with \( [K: \mathbb{Q}] \leq d \). Denote the Galois closure of \( K/\mathbb{Q} \) by \( \bar{K} \). It is common to call the following formalism, “taking the Weil trace” of the elliptic curve over
the number field down to \( \mathbb{Q} \). Choose a primitive element \( \alpha = \alpha_1 \) for \( K/\mathbb{Q} \). Let \( \alpha_1, \ldots, \alpha_d \) be the complete list of conjugates of \( \alpha_1 \).

Each conjugate \( \alpha_i \) gives a conjugate elliptic curve \( E_i \), defined over \( \mathbb{Q}(\alpha_i) \). Let \( G = G(\overline{K}/\mathbb{Q}) \) act on \( A = E_1 \times E_2 \times \cdots \times E_d \) by permutation of the coordinates. For \( \sigma \in G \) indicate this action by \( T(\sigma)(A) \). In addition, regard \( \sigma \) as giving a conjugate of \( A \) by its action on the coefficients of the equations for \( A \). Call the conjugate \( A^\sigma \). Thus, for each \( \sigma \in G \), the sets \( T(\sigma^{-1})(A^\sigma) \) and \( A \) are identical. Now apply Weil’s cocycle condition to assert that we can define \( A \) over \( \mathbb{Q} \). To draw the strongest conclusions, we note this construction is universal in the following sense [FrJ; Proposition 9.34].

Consider \( A^n \) defined over \( K \). There is a linear map \( L : A^{nd} \to A^n \) defined over \( K \) with the following general property. For any subvariety \( V \subset A^n \) defined \( K \), there is a subvariety \( W \subset A^{nd} \) defined over \( \mathbb{Q} \) such that \( (L_1, L_2, \ldots, L_d) : A^{nd} \to (A^n)^d \) maps \( W \) isomorphically to \( V_1 \times \cdots \times V_d \). Here the \( L_i \)s are the conjugates of \( L \) and the \( V_i \)s are the conjugates of \( V \). This means that we also can apply this to the \( K \) subvarieties in \( V \). This produces a \( \mathbb{Q} \) rational subvariety of \( W \) from the product of their conjugates. Thus, conjugates of a \( K \) point \( p \in E \) of order \( m \) produce a \( \mathbb{Q} \) point of order \( m \) on the \( \mathbb{Q} \) form of \( A \). From this conclude \( S(d) \subset T(d) \).

Now suppose \( m \in V(d) \). Apply the Weil trace to \( K = \mathbb{Q}(\zeta_m) \) as above to conclude that \( m \in T((m-1)d) \).

**Problem 5.6.** For each prime \( m \) consider the spaces \( \mathcal{H}(r, m)^{in} \) at the beginning of this subsection. Is there a value \( r_0 \) such that \( \mathcal{H}(r, m)^{in} \) is unirational over \( \mathbb{C} \) for \( r > r_0 \)?

A variety \( W \) is unirational if there is a map \( \varphi : \mathbb{P}^l \to W \) defined on an open subset of \( \mathbb{P}^l \) with image a zariski open subset of \( W \). If \( W \) and \( \varphi \) are defined over \( \mathbb{Q} \), we say \( W \) is unirational over \( \mathbb{Q} \). Since \( \mathbb{P}^l \) has so many rational points, this would imply \( W \) has a dense set of rational points. Thus, if Problem 5.6 has an affirmative answer for a given prime \( m \), there are many involution realizations of \( D_m \) for an arbitrary prime \( m \). (Although it is not hard to realize \( D_m \) as a Galois group of a regular extension of \( \mathbb{Q}(X) \).)

### 5.3. Descent to the totally real algebraic number field

Denote the field of all totally real algebraic numbers by \( \mathbb{Q}^{tr} \). These are the algebraic numbers whose complete set of conjugates are real. In this section we prove the following result.
Theorem 5.7. Each finite group $G$ is the Galois group of a regular extension of $\mathbb{Q}^\text{tr}(X)$.

Section 4.1 recalls the theory of Hurwitz spaces of covers. [FrV2] develops a similar theory, but for $G$-covers—Galois covers given with their automorphisms. Consider a centerless group $G$ and an $r$-tuple of conjugacy classes of $G$. The Hurwitz space $\mathcal{H}^{\text{in}}(G, C)$ is a (reducible) algebraic variety defined over an explicitly computable field $K(C)$. Here is the key property of this space. Let $K$ be a field containing $K(C)$. Then, $G$-covers in the Nielsen class $\text{ni}(C)$, defined over $K$, correspond to $K$-rational points on $\mathcal{H}^{\text{in}}(G, C)$.

Proof of Theorem 5.7. Consider a finite group $G$. Lemma 2 of [FrV2] constructs a cover $G' \to G$ with these properties.

(5.2) The center of $G'$ is trivial and commutators generate the Schur multiplier of $G'$.

We do not explain the commutator statement in (5.2). It appears as a condition in the main theorem of [FrV2] which carefully explains it. Suppose we realize $G'$ as a Galois group of a regular extension of $\mathbb{Q}^\text{tr}(X)$. Then we automatically realize the quotient $G$ as such a Galois group. Therefore, without loss, assume $G$ satisfies (5.2).

Let $b$ be an integer. Let $C_1, \ldots, C_s$ be an ordering of nontrivial conjugacy classes of $G$. Assume each conjugacy class of $G$ appears in this list with the same multiplicity, say $m$. It is automatic that if we pick $g_i$ out of the conjugacy class $C_i$, then

(5.3) $g = (g_1, \ldots, g_s)$ generate $G$.

With $r = 2sb$, consider the $r$-tuple $C$

$$(C_s^{-1}, \ldots, C_1^{-1}, \ldots, C_s^{-1}, \ldots, C_1^{-1}, C_1, \ldots, C_s, \ldots, C_1, \ldots, C_s).$$

Here, the first $sb$ components are the conjugacy classes $C_s^{-1}, \ldots, C_1^{-1}$ repeated in this order $b$ times. The last $sb$ components are the conjugacy classes $C_1, \ldots, C_s$ repeated in this order $b$ times. The Nielsen class $\text{ni}(C)$ is not empty. With $g$ from (5.3), the $r$-tuple

$$(g_s^{-1}, \ldots, g_1^{-1}, \ldots, g_s^{-1}, \ldots, g_1^{-1}, g_1, \ldots, g_s, \ldots, g_1, \ldots, g_s)$$

lies in the Nielsen class $\text{ni}(C)$. Observe that all conjugacy classes appear the same number of times, namely $2bm$, in the $r$-tuple $C$. 
The main theorem of [FrV2; Appendix] shows that, if $b$ is suitably large, then $\mathcal{H} = \mathcal{H}^{\text{in}}(G, C)$ is defined over $\mathbb{Q}$ and irreducible over $\overline{\mathbb{Q}}$. This uses (5.2) to apply a theorem of Conway and Parker [FrV2; Appendix].

We are left with finding $\mathbb{Q}^{\text{irr}}$-points on the absolutely irreducible variety $\mathcal{H}$. Pop [P] proved that every absolutely irreducible variety defined over $\mathbb{Q}^{\text{irr}}$ has $\mathbb{Q}^{\text{irr}}$-points provided it has $\mathbb{R}$-points. This reduces the problem to finding $\mathbb{R}$-points on $\mathcal{H}^{\text{in}}(G, C)$. And their existence follows from Theorem 3.1. Indeed, take $g'_0 = 1$ and $r_1 = 1$ in (iii) of condition (b) of Theorem 3.1. This shows that $(g_1, \ldots, g_r)$ satisfies the hypotheses of that theorem. 

**Remark.** [FrV] consists of applications of [FrV2]. In particular, this observes that each finite complex extension $L$ of $\mathbb{Q}^{\text{irr}}$ is

\[
P(\text{pseudo})A(\text{gebraically})C(\text{losed})
\]

and Hilbertian. A field $P$ has the PAC property if each absolutely irreducible variety over $P$ has a $P$-point. The main theorem of [FrV] applies to show that the absolute Galois group $G(\overline{\mathbb{Q}}/L)$ is a free profinite group.

On the other hand, $\mathbb{Q}^{\text{irr}}$ is not even Hilbertian. In fact, involutions—conjugates of complex conjugation—generate the absolute Galois group of $\mathbb{Q}^{\text{irr}}$. Thus, Galois extensions of $\mathbb{Q}^{\text{irr}}$ have only groups that are generated by involutions. 

**References**


A. Grothendieck, Géométrie formelle et géométrie algébrique, Seminaire Bourbaki, t. 11 182 (1958/59).


Received April 1, 1992. The first author received support from the University of California (Irvine) and NSF grant DMS-8702150. The second author was supported by BSF grant #87-00038, NSA grant MDA 904-910-H-0057, the Institute for Advanced Studies in Jerusalem and IFR Grant #90/91-15.

UNIVERSITY OF CALIFORNIA, IRVINE
IRVINE, CA 92717
E-mail address: mfried@math.uci.edu

AND

INSTITUTE HENRI POINCARE
11 RUE P. ET M. CURIE
75231 PARIS, FRANCE
E-mail address: pde@ccr.jussieu.fr
CONTENTS

P. Ahern and W. Cohn, Weighted maximal functions and derivatives of invariant Poisson integrals of potentials .......................................................... 1
V. Ancona, T. Peternell, and J. A. Wiśniewski, Fano bundles and splitting theorems on projective spaces and quadrics .................................................. 17
G. M. Beffa, A transverse structure for the Lie-Poisson bracket on the dual of the Virasoro algebra .......................................................... 43
C. Biasi, On ambiential bordism .......................................................... 73
P. Debes and M. D. Fried, Nonrigid constructions in Galois theory .............. 81
K. Dykema, Interpolated free group factors ............................................. 123
S.-A. Kim and D. Minda, Two-point distortion theorems for univalent functions 137
X. Mo, Value distribution of the Gauss map and the total curvature of complete minimal surface in $R^m$ ................................................. 159
Z. Shen, On complete Riemannian manifolds with collapsed ends .............. 175
F. Zheng, Curvature characterization of certain bounded domains of holomorphy 183
S. Zhu, The classification of complete locally conformally flat manifolds of non-negative Ricci curvature ................................................. 189
Weighted maximal functions and derivatives of invariant Poisson integrals of potentials

Patrick Robert Ahern and William S. Cohn

Fano bundles and splitting theorems on projective spaces and quadrics

Vincenzo Ancona, Thomas Peternell and Jaroslaw Wisniewski

A transverse structure for the Lie-Poisson bracket on the dual of the Virasoro algebra

Gloria Mari Beffa

On ambiental bordism

Carlos Biasi

Nonrigid constructions in Galois theory

Pierre Dèbes and Michael Fried

Interpolated free group factors

Kenneth Jay Dykema

Two-point distortion theorems for univalent functions

Seong-A Kim and C. David (Carl) Minda

Value distribution of the Gauss map and the total curvature of complete minimal surface in $R^m$

Xiaokang Mo

On complete Riemannian manifolds with collapsed ends

Zhongmin Shen

Curvature characterization of certain bounded domains of holomorphy

Fangyang Zheng

The classification of complete locally conformally flat manifolds of nonnegative Ricci curvature

Shun-Hui Zhu