Pacific Journal 163(1994), 81–122.

NONRIGID CONSTRUCTIONS IN GALOIS THEORY

Pierre Debes *, *Institute Henri Poincaré*
*Michael D. Fried***, *UC Irvine*

Abstract: 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 $R(X)$ 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 $\mathcal{P}^1$ [FrD]. We also use Fried and Völklein [FrV] and Pop [P] to show each finite group is the Galois group of a Galois regular extension of $Q^{\rm tr}(X)$. Here $Q^{\rm tr}$ is the field of all totally real algebraic numbers (Theorem 5.7). §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 R to Q. Use of Hurwitz families reduces the problem to finding Q-rational point on a special algebraic curve. Our first application considers realizing the symmetric group S_m as the group of a Galois extension of $Q(X)$, regular over 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 $2m$ isn't the group of a Galois regular extension of $Q(X)$ 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 [KM] suggest that no bound on the number of branch points will allow realization of *all* D_ms.

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

The map φ is ramified over a finite number of points $x_1, \dots, x_r$. 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 $R(X)$ with only real branch points.

This happens if and only if G is generated by involutions.

Grants: * Support from University of California (Irvine) and NSF grant DMS-8702150
** Supported by BSF grant #87-00038, NSA grant MDA 904-91-H-0057, the Institute for Advanced Studies in Jerusalem and IFR Grant #90/91-15.

AMS Subject classification: 11G35, 12F10, 14E20, 14G05, 20B25, 20C25

Keywords: coverings of $\mathcal{P}^1$; defined over R; fields of definition; Galois groups; group extensions; Hurwitz monodromy group; modular curves.

Theorem 1.1 uses formulas for the action of complex conjugation on the fundamental group of $\mathcal{P}^1\backslash\{x_1,\dots,x_r\}$ (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 Q? As do others, we approach this through its geometric analog. That is, we consider it over $Q(X)$ rather than Q. This is a descent problem. Suppose we are given a group G, a suitably large integer r and r points $x_1,\dots,x_r \in \mathcal{P}^1(C)$. Topology then constructs a Galois extension of $C(X)$ with Galois group G and branch points $x_1,\dots,x_r$. One must then restrict the scalars from C to Q. Theorem 1.1 gives a form of descent from C to 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 Q (or even R) using r branch points in $\mathcal{P}^1(R)$ only if r elements of order 2 generate G. Therefore, in practice, classical "rigidity" [Se3; Theorem 9.1] realizes only groups over $Q(X)$ 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* (c.f. §1.2) that is not the Galois group of a regular extension of $R(X)$ with only real branch points. Nevertheless, every finite group is the Galois group of a regular extension of $R(X)$, 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 $Q^{\rm tr}(X)$. Here $Q^{\rm tr}$ is the field of all totally real algebraic numbers.

§**0.3. Extension of Theorem 1.1:** Theorem 1.1 has a (b) part that applies to not necessarily Galois extensions. Finite group G is the monodromy group of a cover $\varphi: Y_C \to \mathcal{P}^1$ defined over R with only real branch points if and only if

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

Of course, (*) holds if G is generated by elements of order 2. §1.2–§1.5 has 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 nonsplit* cover of G that doesn't 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. §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 to simplify this using the algebraic fundamental group rather than the classical topological fundamental group. §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 $\varphi: Y_C \to \mathcal{P}^1$ 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. (§3.7 has a precise formulation.) We note that no naive p-adic analog of this representation of complex conjugation holds for the Frobenius $F_p \in G(\bar{Q}_p/Q_p)$ (§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 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? After [D], the non-archimedean completions pose no obstruction. 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) 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) doesn't answer the global question.

Descent to 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 $\varphi : Y_C \to \mathcal{P}^1$ derived from Theorem 1.1 can be defined over Q. "Rigidity assumptions" from [Se3; Ch. 8, 9] don't apply. They rarely do when there are 4 (or more) branch points.

In §4.1 and §4.2, we recall from [Fr1] how to handle nonrigid cases. Hurwitz family ideas reduce the problem to finding a rational point on a certain curve $C(C)$. §4.3 gives a formula for the genus of $C(C)$ when $r = 4$. 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 $Q(X)$ 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 don't 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 R to 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 $Q(X)$. Mazur has formulated conjectures that imply that realization of all D_ms will require an unbounded number of branch points [KM]. We borrow some of his formulation from e-mail discussion with him.

§**0.5. Acknowledgements:** David Harbater made expositional simplications 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 $\varphi : Y_C \to \mathcal{P}^1$ the associated cover. That is, Y_C is the set of places of the field YC and φ is the natural restriction of places—points of $\mathcal{P}^1$—to $C(X)$. Branch points $x_1, \dots, x_r$ are the places ramified in the extension $YC/C(X)$.

§**1.1. Statement of Theorem 1.1:** Let x_0 be a point in $\mathcal{P}^1(R) \setminus \{x_1, \dots, x_r\}$. Denote the fundamental group $\pi_1(\mathcal{P}^1 \setminus \{x_1, \dots, x_r\}, x_0)$ for short by π_1. There is a natural action T of π_1 called the *monodromy action* on the points of the fiber $\varphi^{-1}(x_0)$. 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 γ through φ with initial point y.

The permutation $T([\gamma])$ is independent of the representative of $[\gamma]$. Fix a labeling $y_1, \dots, y_n$ of the points of the fiber $\varphi^{-1}(x_0)$. Regard T as an action $T : \pi_1 \to S_n$ of π_1 on the integers $1, \dots, n$. Up to conjugation by an element of S_n, this action does not depend on labeling the y_is 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 $R(X)$ with only real branch points exactly when*

(1.1) $$G \text{ is generated involutions.}$$

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

$$\begin{aligned} &\exists h \in \mathrm{Aut}(G),\ \exists \alpha_1, \dots, \alpha_s \in G \mid \\ &\qquad \langle \alpha_1, \dots, \alpha_s \rangle = G, h(\alpha_i) = \alpha_i^{-1},\ i = 1, \dots, s. \end{aligned} \tag{1.2}$$

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 $R(X)$ in the statement.

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

$$(\alpha_1, \alpha_1^{-1}\alpha_2, \dots, \alpha_{s-1}^{-1}\alpha_s, \alpha_s^{-1})$$

(c.f. §2.3). It is Galois over C. Indeed, it is Galois over 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 $(Z/2)^m$ satisfy (1.2) but not (1.1). For example, the cyclic group Z/m is the monodromy group of the Galois cover $\varphi : \mathcal{P}^1 \to \mathcal{P}^1$ given by $\varphi(y) = y^m$. For $m \neq 2$, it is defined over R with only real branch points. Yet, the corresponding function field extension $R(y)/R(y^m)$ 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) $G = Z/2$ or $\mathrm{Aut}(G)$ 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 the semi-direct product $G' = G \times^s \langle h \rangle$ of G and the group generated by the automorphism h. The elements (α_i, h), $i = 1, \dots, s$, 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 $\alpha_i h'$, $i = 1, \dots, s$.

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

Take H to be the subgroup that the β_is 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 $g_{i_1} \cdots g_{i_t}$ in the g_is. Assume words of length at most $t-1$ are in one of the cosets H or $g_0 H$. Now do cases for $g_{i_2} \dots g_{i_t} = \sigma$ in H or $g_0 H$. If $\sigma \in H$, then $g_0 g_{i_1} \sigma$ is also in H. Multiply by g_0 to see $g_{i_1}\sigma \in g_0 H$. On the other hand, if $\sigma \in g_0 H$, then multiply by $(g_{i_1} g_0)g_0$ to get $g_{i_1}\sigma$ in H. We're done.

(1.3) ⇒ (1.4): Suppose G' contains τ of order 2 not in the centralizer $\mathrm{Cen}_{G'}(G)$ in G'. Then, conjugation by τ is an automorphism of G of order 2. Thus, $|\mathrm{Aut}(G)|$ is even. Assume all elements of G' of order 2 are in $\mathrm{Cen}_{G'}(G)$. Pick an element a of order 2 from $G' \setminus G$. Then $a \in \mathrm{Cen}_{G'}(G)$. 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 $\mathrm{Cen}_{G'}(G)$, the group G is abelian. Conclude: $|\mathrm{Aut}(G)|$ is even unless $G = Z/2$. □

So, groups distinct from $Z/2$, with odd order automorphism group, aren't monodromy groups of a cover over R with only real branch points. Here is how to get such a group. Consider a p-group P with p odd. Then, $\mathrm{Aut}(P)$ 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 isn't the group of a regular Galois extension of $R(X)$ 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 isn't 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) ψ is surjective and $\ker(\psi)$ is contained in the frattini group of H.

(ii) A 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; Prop. 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 $\mathrm{gen}_2(F_i)$ be the subset of F_i^n consisting of all n-tuples $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$ 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 $\mathrm{gen}_2(F_i)$ of the natural map induced by π_{ij} on F_i^n by $\pi_{ij} : \mathrm{gen}_2(F_i) \to \mathrm{gen}_2(F_j)$.

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

Next, set $F = \tilde{G}/(\ker\tilde{\psi}\cap N_i)$. 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 don't generate F. The finite cover $\psi : F \to G$ is the required cover. □

§**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 containing at least one non-cyclic group. 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 don't know the answer to Question 1.5. We conclude this section by showing that the universal frattini cover $\tilde{G}$ of G isn't 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 Z/p act on $A = (Z/q)^p$ as cyclic permutations of the coordinates. Consider the semi-direct product $B = A \times^s Z/p$ generated by this action.

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

Proof: Assume we've shown B to have the properties of the proposition. From above, we are done if the non-nilpotent group B is a quotient of $\hat{F}_{s'}(\mathcal{C})$. 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 $\hat{F}_{s'}(\mathcal{C})$ on B. It remains to show the properties of B.

Here are two generators of B: $\alpha = (1, 0, \ldots, 0) \in A$ and $\tau = 1 \in Z/p$. Indeed, the Z/p orbit of α gives a basis for A. Finally, Z/p is a p-sylow for B. It isn't, however, normal: $\alpha\tau\alpha^{-1}$ is $(1, -1, 0, \ldots, 0) \times \tau$. Thus, B isn't 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 $\varphi : Y_C \to \mathcal{P}^1$ is projection: $(x, y) \to x$. Take x_0 to be distinct from the branch points of the cover.

Let $\widehat{YC}$ be the Galois closure of $YC/C(X)$. The Galois group $G(\widehat{YC}/C(X))$ 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 $YC \to C((X - x_0))$ in the Laurent series around x_0 determines a point $p_i \in Y$ above x_0. Since x_0 isn't a branch point, there are n such embeddings. Each corresponds to one of the y_is.

From now on, fix an embedding $\widehat{YC} \to C((X - x_0))$. That is, regard $\widehat{YC}$ 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 $G(\widehat{YC}/C(X))$ are the same. Denote this common group by Γ_Y (or simply Γ). Furthermore, denote the image in Γ of an element $s \in T(\pi_1)$ by $\bar{s}$, and the image in Γ of an element $\sigma \in G(\widehat{YC}/C(X))$ by $\bar{\sigma}$. Even in the case where $Y_C \to \mathcal{P}^1$ is Galois, automorphisms of this cover do not naturally identify with automorphisms of $\widehat{YC}/C(X)$. In particular, restriction of the former automorphisms to the fiber over x_0 don't correspond to automorphisms of $\widehat{YC}/C(X)$.

We make an assumption a little stronger than saying that x_0 isn't 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 $\mathcal{P}^1(Q)$. Consider the automorphism group $\mathrm{Aut}(C)$. An automorphism $\tau \in \mathrm{Aut}(C)$ acts coordinatewise on the geometric points of any affine variety defined over 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_C^τ and the associated cover by $\varphi_C^\tau : Y_C^\tau \to \mathcal{P}^1$.

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

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

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

Proof: Let $\hat{K}$ be the constant field of the extension $\hat{Y}/K(X)$: $\hat{K} = \hat{Y} \cap \bar{K}$. Clearly, $\widehat{YC} = \hat{Y}C$; restriction $G(\widehat{YC}/C(X)) \to G(\hat{Y}/\hat{K}(X))$ is an isomorphism. In particular, Γ is the image of $G(\hat{Y}/\hat{K}(X))$ in S_n. It is a normal subgroup of $\hat{\Gamma}$ because $\hat{K}/K$ is Galois. The map $\mathrm{Aut}_K(C)$ to $G(\hat{K}/K)$ is onto. Therefore, $\bar{\tau}$, with $\tau \in \mathrm{Aut}_K(C)$, 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 $\pi_1 = \pi_1(\mathcal{P}^1 \setminus \{x_1, \dots, x_r\}, x_0)$. These are homotopy classes $[\gamma_i]$ of suitably chosen loops starting from x_0 around the branch points x_i, $i = 1, \dots, r$. These freely generate except for one relation, $[\gamma_1][\gamma_2] \cdots [\gamma_r] = 1$. For $i = 1, \dots, r$, set $s_i = T([\gamma_i])$; the s_is generate the monodromy group of the cover and satisfy $s_1 s_2 \cdots s_r = 1$.

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

- degree n covers $\varphi : Y_C \to \mathcal{P}^1$ (up to equivalence of covers) ramified over the points $x_1, \dots, x_r$; and
- r-tuples $(s_1, \dots, s_r) \in S_n^r$ (modulo coordinatewise conjugation by S_n) with $s_1 s_2 \cdots s_r = 1$ and $\langle s_1, \dots, s_r \rangle$ transitive on $1, \dots, n$.

Unless otherwise specified, assume from here the following.

(2.1) Branch points $x_1, \dots, x_r$, $r \geq 3$, are in $\mathcal{P}^1(R)$ and $x_1 < x_2 < \cdots < x_r \leq \infty$.

Fix the base point $x_0 \in \mathcal{P}^1(Q) \setminus \{\infty\}$ on the arc between x_1 and x_r not containing x_2 on the real projective line. Denote complex conjugation on C by c. It maps the homotopy class $[\gamma] \in \pi_1$ of a closed path γ based at x_0 to the homotopy class $[\gamma^c]$ of the conjugate path γ^c. With suitable loops around the x_is, we write this action explicitly. For the rest of §2 and §3 use the specific bouquet $(\gamma_1, \dots, \gamma_r)$ from [FrD; §2.1]. For this we have the following.

Proposition 2.2: *The paths $\gamma_1^c, \dots, \gamma_r^c$ are respectively homotopic to*

$$(\gamma_2 \cdots \gamma_r)^{-1}{\gamma_1}^{-1}(\gamma_2 \cdots \gamma_r), (\gamma_3 \cdots \gamma_r)^{-1}{\gamma_2}^{-1}(\gamma_3 \cdots \gamma_r), \dots, (\gamma_r)^{-1}{\gamma_{r-1}}^{-1}\gamma_r, {\gamma_r}^{-1}.$$

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 $\mathcal{C}_r : U^r \to U^r$ to send $\boldsymbol{u} = (u_1, \dots, u_r) \in U^r$ to $\mathcal{C}_r(\boldsymbol{u}) \stackrel{\text{def}}{=} (u_1^{\mathcal{C}}, \dots, u_r^{\mathcal{C}})$ with $u_r^{\mathcal{C}} = u_r^{-1}$ and

$$u_i^{\mathcal{C}} = (u_{i+1} \cdots u_r)^{-1} u_i^{-1} (u_{i+1} \cdots u_r), \quad i = 1, \dots, r-1. \tag{2.2}$$

We also have

$$u_i^{\mathcal{C}} \cdots u_r^{\mathcal{C}} = (u_i \cdots u_r)^{-1}, \quad i = 1, \ldots, r-1. \tag{2.3}$$

Consider a cover $\varphi : Y_C \to \mathcal{P}^1$ and its conjugate $\varphi^c : Y_C^c \to \mathcal{P}^1$. 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 γ based at x_0, we have $T^c([\gamma^c])(p_i^c) = [T([\gamma])(p_i)]^c$. Replace γ by γ^c and apply c to both sides. This gives the equivalent expression:

$$T^c([\gamma])(p_i^c)^c = T([\gamma^c])(p_i). \tag{2.4}$$

From (2.4):

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

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 $\boldsymbol{s} = (s_1, \ldots, s_r)$ is the branch cycle description of the cover $\varphi : Y_C \to \mathcal{P}^1$ associated with the bouquet $(\gamma_1, \ldots, \gamma_r)$. Then, $\mathcal{C}_r(\boldsymbol{s}) = (s_1^{\mathcal{C}}, \ldots, s_r^{\mathcal{C}})$ is the branch cycle description of the cover $\varphi^c : Y_C^c \to \mathcal{P}^1$ associated with the bouquet $(\gamma_1, \ldots, \gamma_r)$.*
(b) *If $R \supset K$ then $\mathcal{C}_r(\bar{\boldsymbol{s}}) = \bar{c}\bar{\boldsymbol{s}}\bar{c}$. That is $\bar{s}_i^{\mathcal{C}} = \bar{c}\bar{s}_i\bar{c}$, $i = 1, \ldots, r$.*

§**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 $\Psi : E \to \mathcal{P}^1$ be a Galois cover, and let H be the subgroup of $\mathrm{Aut}(C)$ given as

$$\{\tau \in \mathrm{Aut}(C/Q) \mid \Psi : E \to \mathcal{P}^1 \text{ and } \Psi^\tau : E^\tau \to \mathcal{P}^1 \text{ are equivalent covers}\}.$$

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 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 $\varphi : Y_C \to \mathcal{P}^1$ is equivalent to the cover $\Psi : E \to \mathcal{P}^1$, 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 $\tau \in H$ (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 $\tau \in H$. 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 $\hat{K}$ be the constants of the Galois closure of the extension $Y/K(X)$. Then, $\hat{K} = K$ 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 $\hat{K}$. Therefore, if these points are defined over K, then $\hat{K} = K$.

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 δ_τ 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 $\Psi^\tau : E^\tau \to \mathcal{P}^1$ 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^τ. Denote the isomorphism $\chi_\tau \circ \delta_\tau$ by c_τ. The collection $\{c_\tau\}_{\tau \in H}$ satisfies the cocycle condition: $c_{\tau_1}^{\tau_2} \circ c_{\tau_2} = c_{\tau_1\tau_2}$ for all $\tau_1, \tau_2 \in H$. Indeed:

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

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

(2.6)(a) $$\Psi \circ \Theta = \varphi_K, \text{ and}$$

(b) $$\Theta^\tau \circ \Theta^{-1} = c_\tau, \text{ for all } \tau \in H.$$

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, $\varphi : Y_C \to \mathcal{P}^1$ is the cover $\varphi_K : E_K \to \mathcal{P}^1$.

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

(3.1) $$\bar{c}\alpha_i\bar{c} = \alpha_i^{-1}, i = 1, \dots, r-1.$$

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

§3.2. Proof of Theorem 1.1 (a) ⇒: 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 $\hat{\Gamma}_Y = \Gamma_Y$, we have $\bar{c} \in G$ (statement prior to Prop. 2.1). Thus, $\bar{c}, \bar{c}\bar{\alpha}_1, \dots, \bar{c}\bar{\alpha}_{r-1}$ are of order ≤ 2 and they generate G. □

§3.3. Proof of Theorem 1.1 (b) ⇐: 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 $\boldsymbol{s} = (s_1, \dots, s_r) \in S_n^r$ defined by

(3.2) $$\boldsymbol{s} = (\alpha_1, \alpha_1^{-1}\alpha_2, \alpha_2^{-1}\alpha_3, \dots, \alpha_{r-2}^{-1}\alpha_{r-1}, \alpha_{r-1}^{-1}).$$

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

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

(3.3) $s_i^{\mathcal{C}} = \kappa s_i \kappa^{-1}$ for $i = 1, \dots, r$.

From Riemann's Existence Theorem (§2.3), the covers $\Psi : E \to \mathcal{P}^1$ and $\Psi^c : E^c \to \mathcal{P}^1$ are equivalent covers. Apply Theorem 2.4 to conclude there exists a regular extension $Y/R(X)$ with these properties.

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

(ii) $R((X-x_0))$ contains Y.

The cover $\varphi: Y_C \to \mathcal{P}^1$ is defined over R. It is the desired cover. □

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

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

From Prop. 2.3 (b), we also have $s_i^{\mathcal{C}} = \bar{c}s_i\bar{c}$, $i=1,\dots,r$. Therefore, $\bar{c}\in \mathrm{Cen}_{S_n}(G)$. Since $R((X-x_0))$ contains Y, $\bar{c}$ has a fixed point. Conclude that $\bar{c}=1$. Therefore, from Prop.2.1, $\hat{\Gamma}_Y = \Gamma_Y$: $Y/R(X)$ is a Galois regular extension with Galois group $\Gamma_Y = G$. □

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

§**3.5. Comments:** This section consists of three 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 R.

Comment1: *Dropping the assumption "the branch points are real."* The "real branch point situation" of Theorem 1.1 allowed special generators $[\gamma_1],\dots,[\gamma_r]$ of the fundamental group π_1 from §2.3. Explicit formulas gave $[\gamma_1^c],\dots,[\gamma_r^c]$ as words in $[\gamma_1],\dots,[\gamma_r]$ (cf. Prop. 2.2). We can work with the general cover defined over 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 $Y/R(X)$ 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 $Y/R(X)$ of group G, with r branch points $t_1,\dots,t_{r_1},\bar{z}_{r_2},\dots,\bar{z}_1,z_1,\dots,z_{r_2}$, where $t_i\in R$, $i=1,\dots,r_1$, and $z_i\notin R$, $i=1,\dots,r_2$.

(b) There exists $(g_1',\dots,g_r')\in G^r$ which satisfy these conditions:

(i) $g_1'\cdots g_r' = 1$

(ii) $\langle g_1',\dots,g_r'\rangle = G$

(iii) $\exists g_0'\in G$ such that $(g_0'\cdots g_i')^2=1,\ i=0,\dots,r_1-1$,
$g_{r-i}' = g_0'(g_{r_1+1+i}')^{-1}g_0',\ i=0,\dots,r_2-1$.

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 $R(X)$.

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 r-tuple of (3.2) by $\boldsymbol{s}(\boldsymbol{\alpha})$. Let $x_0, x_1, \ldots, x_r$ be $r+1$ points in $\mathcal{P}^1(R)$. Take $(\gamma_1, \ldots, \gamma_r)$ to be a bouquet as in §2.3 with $\boldsymbol{s}(\boldsymbol{\alpha})$ 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 $\Psi_{\boldsymbol{s}(\boldsymbol{\alpha}),\boldsymbol{x}} : E \to \mathcal{P}^1$. We ask if we can define this cover over 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 $\{c_\tau\}_{\tau \in G(C/R)}$ as in Theorem 2.4. It must satisfy the cocycle condition $c_{\tau_1}^{\tau_2} \circ c_{\tau_2} = c_{\tau_1\tau_2}$, for all $\tau_1, \tau_2 \in G(C/R)$. For example, you can do this when the cover $\Psi : E \to \mathcal{P}^1$ has no nontrivial automorphism. This is the same as the condition $\mathrm{Cen}_{S_n}(G) = \{1\}$.

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

(*) The set $N_{\boldsymbol{\alpha}} = \{\kappa \in S_n : \kappa\alpha_i\kappa^{-1} = \alpha_i^{-1}, i = 1, \ldots, r-1\}$ 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:

(**) There is a cover equivalent to $\psi : E \to \mathcal{P}^1$ defined and Galois over R.

It is tempting to answer: $N_{\boldsymbol{\alpha}} \cap G$ 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:

(***) $\exists \kappa \in N_{\boldsymbol{\alpha}} \cap G$ with $\kappa^2 = 1$.

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

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

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 C/R. Recall the dictionary between covers and branch cycle descriptions (for the bouquet $\boldsymbol{\gamma}$). An isomorphism $\delta : E \to E^c$ such that $\psi^c \circ \delta = \psi$ comes from an element κ in $N_{\boldsymbol{\alpha}}$.

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

(†) $\delta_c^c \circ \delta_c = 1$; and

(††) δ_c commutes with the action of c that takes automorphisms of $E \to \mathcal{P}^1$ to automorphisms of $E^c \to \mathcal{P}^1$.

Indeed, (†) follows because the effect of the left side of (†) on $\boldsymbol{p}$ is given by κ^2. As for (††), automorphisms of the covers commute with a renaming of the points of $\boldsymbol{p}$.

For convenience take δ_1 to be the identity. Condition (†) guarantees that the collection $\{\delta_\tau\}$ satisfies the cocycle condition

$$\delta_{\tau_1}^{\tau_2} \circ \delta_{\tau_2} = \delta_{\tau_1\tau_2}.$$

Therefore, one can descend the field of definition of the cover to R. Condition (††) assures that the automorphisms are also defined over R.

§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 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 $x_1, \dots, x_r$ be r distinct points in $\mathcal{P}^1(\bar{K})$. Denote the maximal algebraic extension of $\bar{K}(X)$ unramified outside $x_1, \dots, x_r$ by Ω. The extension $\Omega/\bar{K}(X)$ is Galois. Its group is the *algebraic fundamental group* of $\mathcal{P}^1(\bar{K}) \setminus \{x_1, \dots, x_r\}$. Denote this profinite group by π^{alg}.

When $\bar{K} = C$, π^{alg} is the profinite completion $\hat{\pi}$ of the topological fundamental group π [Se3; Th. 7.5, p. 69]. By analogy with the complex case, denote the free group on r generators $\Gamma_1, \dots, \Gamma_r$ with the single relation $\Gamma_1 \cdots \Gamma_r = 1$ by π. There is a map $i : \pi \to \pi^{\text{alg}}$ with the following properties.

(i) $i(\Gamma_i) \stackrel{\text{def}}{=} \Gamma_i$ is a generator of an inertia group of the extension $\Omega/\bar{K}(X)$ above x_i, $i = 1, \dots, r$.

(ii) The map i extends to an isomorphism $\hat{i} : \hat{\pi} \to \pi^{\text{alg}}$.

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

$$1 \to \pi^{\text{alg}} \to \pi_K \to \Lambda_K \to 1. \tag{3.5}$$

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

Given a finite group G, a surjective homomorphism $\psi \in \text{Hom}(\pi^{\text{alg}}, G)$ produces a Galois extension $E/\bar{K}(X)$ with Galois 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 ψ extends to π_K.

In our context, $K = R$ and the branch points $x_1, \dots, x_r$ are real. §2.3 gives generators $\Gamma_1, \dots, \Gamma_r$ of π^{alg} so that complex conjugation $c \in \Lambda_R$ acts on them by the formulas (2.2). Recall from §2.3 the operator $\mathcal{C}$ in our next result.

Proposition 3.2: *Assume the branch points $x_1, \dots, x_r$ are real. Then, π_K is isomorphic to the semi-direct product $\pi^{\text{alg}} \times^s Z/2$ with $c = 1 \in Z/2$ mapping $\Gamma \in \pi^{\text{alg}}$ to Γ^c satisfies*

$$\Gamma_i^c = \Gamma_i^{\mathcal{C}}, \ i = 1, \dots, r. \tag{3.6}$$

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 $g_i = \psi(\Gamma_1) \cdots \psi(\Gamma_i)$, $i = 1, \dots, r$. Then, ψ extends to $\tilde{\psi} \in \text{Hom}(\pi^{\text{alg}} \times^s Z/2, G)$ if and only if there exists an involution $\kappa \in G$ with all of $\kappa g_1, \dots, \kappa g_r$ involutions.*

Proof: Assume $\tilde{\psi} \in \text{Hom}(\pi^{\text{alg}} \times^s Z/2, G)$ extends ψ. Set $\kappa = \tilde{\psi}(c)$; $|\kappa| = 2$ and

$$\psi(\Gamma^c) = \kappa \psi(\Gamma) \kappa \tag{3.7}$$

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

For the converse, define $\tilde{\psi} \in \pi^{\text{alg}} \times^s Z/2$ by $\tilde{\psi}(\Gamma, \epsilon) = \psi(\Gamma)\kappa^\epsilon$ for each $\Gamma \in \pi^{\text{alg}}$ and $\epsilon = 0, 1$. Use (3.6) to check that (3.7) holds for $\Gamma = \Gamma_i$, $i = 1, \dots, r$, and so for all $\Gamma \in \pi^{\text{alg}}$. This guarantees that $\tilde{\psi}$ is a homomorphism of groups. □

§**3.7. p-adic Analogs:** Prop. 3.2 gives the effect of complex conjugation c:

(3.8) Γ_i^c is conjugate in π to Γ_i^{-1}, $i = 1, \dots, r$.

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

(3.9) Γ_i^τ is conjugate in π^{alg} to $\Gamma_j^{\chi(\tau)}$ where $x_j = x_i^\tau$.

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

We aren't tempted to use the exponent p when we recognize a simple property of the Frobenius F_p. It acts on μ_N as p-th powers only when p does not divide N. Question 3.4 below is subtler. Say that a finite extension $L/\bar{Q}_p(X)$ is p'-ramified if p does not divide any of the orders e_i of the inertia groups above x_i, $i = 1, \dots, r$. For such extensions, p is relatively prime to $N = \text{lcm}(e_1, \dots, e_r)$. In this case, the value in $G(K(\mu_N)/K)$ of the cyclotomic character at F_p is p. Define π_p^{alg} to be the projective limit $\varprojlim \pi^{\text{alg}}/D$. Here D ranges over normal subgroups of π 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 $\tilde{\pi} \cong \pi_p^{\text{alg}}$ induced by an action on π such that $\Gamma_i^{F_p}$ is conjugate in π to Γ_j^p where $x_j = x_i^{F_p}$, $i = 1, \dots, r$?*

We believe the answer is still "No!" Here is an outline in this direction in the case of covers with branch points in Q_p. Such a "frobenius" action would give a formula like this:

$$F_p \sigma_i F_p^{-1} = \omega_i(\boldsymbol{\sigma}) \sigma_i^p \omega_i^{-1}(\boldsymbol{\sigma}), \quad i = 1, \dots, r. \tag{3.10}$$

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

Suppose we ask that $\boldsymbol{\omega}(\boldsymbol{\sigma})$ be independent of the branch points and the choice of elements in the conjugacy classes given by the entries of $\boldsymbol{\sigma}$. 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 $\text{SL}_2(Z)$ on the upper half plane. Our assumptions on $\boldsymbol{\omega}(\sigma)$ 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 aren't. 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 $Q_p(X)$ 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 Q_p. □

§4. HURWITZ SPACES AND RATIONALITY OVER Q.

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

(4.1) $G \to S_n$ is the regular representation or $\mathrm{Cen}_{S_n}(G) = \{1\}$.

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

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

We use *Nielsen classes* and *Hurwitz families* to investigate this. Branch cycle descriptions provide much information (c.f. §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 $x_1, \dots, x_r$ and a sample bouquet $\gamma_1, \dots, \gamma_r$. There an intrinsic notion.

Consider the data attached to any branch cycle description $(s_1, \dots, s_r)$ of a cover. Most importantly, there is the group $< \boldsymbol{s} >$ generated by the s_is. Up to conjugation by S_n, this is the monodromy group of the cover. Secondly, there is the collection $\{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ of conjugacy classes of $s_1, \dots, s_r$ in the group $< \boldsymbol{s} >$. 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 $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ be an r-tuple of nontrivial (not necessarily distinct) conjugacy classes of G.

Definition 4.2: To the data $(G, \mathbf{C})$ we associate its *Nielsen class*:

$$\mathrm{ni}(\mathbf{C}) = \{s \in G^r \mid < \boldsymbol{s} > = G,\ s_1 \cdots s_r = 1 \\ \text{and there exists } \omega \in S_r, s_{(i)\omega} \in \mathrm{C}_i, i = 1, \dots, r\}.$$

Suppose a cover $\Psi : E \to \mathcal{P}^1$ has any branch cycle description $\boldsymbol{s}$, up to conjugation by elements of S_n, in $\mathrm{ni}(\mathbf{C})$. We say the cover is in $\mathrm{ni}(\mathbf{C})$. Alternatively, $\mathrm{ni}(\mathbf{C})$ is the Nielsen class of the cover. The order we list the conjugacy classes doesn't matter. The *straight Nielsen class* of $(\mathbf{C}, G)$ is

$$\mathrm{sni}(\mathbf{C}) = \{\boldsymbol{s} \in \mathrm{ni}(\mathbf{C}) \mid s_i \in \mathrm{C}_i, i = 1, \dots, r\}.$$

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

$$N(\mathbf{C}) = \{\kappa \in S_n \mid \text{ conjugation by } \kappa \text{ permutes } \mathrm{C}_1, \dots, \mathrm{C}_r\}$$
$$SN(\mathbf{C}) = \{\kappa \in S_n \mid \text{ conjugation by } \kappa \text{ fixes } \mathrm{C}_1, \dots, \mathrm{C}_r\}.$$

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

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

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

$$(4.2)(a) \qquad Q_iQ_{i+1}Q_i = Q_{i+1}Q_iQ_{i+1}, i = 1, \dots, r-2;$$

$$(b) \qquad Q_iQ_j = Q_jQ_i, \ |i-j| > 1; \text{ and}$$

$$(c) \qquad Q_1Q_2 \cdots Q_{r-1}Q_{r-1} \cdots Q_1 = 1.$$

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

$$(4.3) \qquad (\boldsymbol{s})Q_i = (s_1, \dots, s_{i-1}, s_is_{i+1}s_i^{-1}, s_i, s_{i+2}, \dots, s_r), i = 1, \dots, r-1.$$

Thus they induce a permutation representation of H_r on $\mathrm{ni}(\mathbf{C})^{\mathrm{ab}}$: the Hurwitz monodromy action on the Nielsen class $\mathrm{ni}(\mathbf{C})^{\mathrm{ab}}$.

Denote the kernel of the natural permutation representation $H_r \to S_r$ 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 $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. 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* $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ *and that* $\mathrm{C}_1, \dots, \mathrm{C}_r$ *are rational conjugacy classes. Then there is an algebraic family $\mathcal{F}(\mathbf{C})$ of covers of $\mathcal{P}^1$ (a priori over C)*

$$\mathcal{F}(\mathbf{C}) : \mathcal{T}(\mathbf{C}) \to \mathcal{H}(\mathbf{C}) \times \mathcal{P}^1.$$

This, the universal Hurwitz family associated to $\mathrm{ni}(\mathbf{C})$*, satisfies (4.4)–(4.7).*

(4.4) $\mathcal{F}(\mathbf{C})$ is a finite morphism of quasiprojective varieties, $\mathcal{H}(\mathbf{C})$ is irreducible and the generic fiber of $\mathrm{pr}_1 \circ \mathcal{F}(\mathbf{C}) : \mathcal{T}(\mathbf{C}) \to \mathcal{H}(\mathbf{C})$ is irreducible.

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

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

(4.7) Denote the subvariety of $(\mathcal{P}^1)^r$ 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" $\Psi(\mathbf{C}) : \mathcal{H}(\mathbf{C}) \to U_r$ sends each $\boldsymbol{h} \in \mathcal{H}(\mathbf{C})$ to the branch point set of the fiber cover $\mathcal{F}(\mathbf{C})_{\boldsymbol{h}} : \mathcal{T}(\mathbf{C})_{\boldsymbol{h}} \to \mathcal{P}^1$. This is an étale morphism of degree $|\mathrm{ni}(\mathbf{C})^{\mathrm{ab}}|$ defined over Q.

The original conjugacy classes, $\mathrm{C}_1, \dots, \mathrm{C}_r$, are the conjugacy classes in G of the entries of the r-tuple $\boldsymbol{s}(\boldsymbol{\alpha})$. 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, $x_1, \dots, x_r \in \mathcal{P}^1(Q)$, so that the point $\boldsymbol{h} \in \mathcal{H}(\mathbf{C})$ that corresponds to the cover $\Psi_{\boldsymbol{s}(\boldsymbol{\alpha}),\boldsymbol{x}} : E \to \mathcal{P}^1$ is a Q-rational point on $\mathcal{H}(\mathbf{C})$.*

§**4.2. Description of $\mathcal{H}(\mathbf{C})$ for $r = 4$:** See [BFr; §1, Lemma 1.6)], [Fr2; §4.1]. Both our examples will be 4 branch point situations. In this case, $\mathcal{H}(\mathbf{C})$ has a more explicit description. Consider natural map $U^r \to U_r$. Let $\mathcal{H}(\mathbf{C})'$ be an irreducible component of the fiber product $\mathcal{H}(\mathbf{C}) \times_{U_r} U^r$ and $p : \mathcal{H}(\mathbf{C})' \to U^r$ the natural projection. Theorem 4.5 uses the permutations of $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ 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 $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. The transitivity hypothesis of Theorem 4.3 implies that the a_{1j}s are transitive on $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$.

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

$$\mathcal{H}(\mathbf{C})'(x_2, x_3, x_4) \to \mathcal{P}^1 \setminus \{x_2, x_3, x_4\}.$$

Complete this to a (ramified) cover $C(\mathbf{C}) \to \mathcal{P}^1$ of projective nonsingular curves. This will have the following properties.
(4.8) *The points x_2, x_3, x_4 are the 3 branch points of the cover.*
(4.9) *(a_{12}, a_{13}, a_{14}) (acting on $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$) is a branch cycle description of the cover.*
(4.10) *The cover is defined over Q.*

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

Proof: For (x_2, x_3, x_4) take the generic point of U^3 in the above. The birational equivalence $\mathcal{H}(\mathbf{C})'(x_2, x_3, x_4) \cong C(\mathbf{C})$ induces a birational map

$$\mathcal{H}(\mathbf{C})' \to C(\mathbf{C}) \times \mathcal{P}^1 \times \mathcal{P}^1 \times \mathcal{P}^1. \qquad \square$$

§4.3 has examples where $C(\mathbf{C})$ is $\mathcal{P}^1$ (over Q). Consequently, the space $\mathcal{H}(\mathbf{C})'$ is a Q-rational variety. In particular, the Q-rational points on $\mathcal{H}(\mathbf{C})'$ form a dense subset of $\mathcal{H}(\mathbf{C})'(R)$ (for the complex topology) and Question 4.1 has an affirmative answer.

§4.3. A formula for the genus of the curve $C(\mathbf{C})$: The Riemann-Hurwitz formula gives the genus $g(\mathbf{C})$ of the curve $C(\mathbf{C})$ (cf. Theorem 4.5):

(4.11) $\mathrm{ind}(a_{12}) + \mathrm{ind}(a_{13}) + \mathrm{ind}(a_{14}) = 2(N + g(C) - 1)$ with $N = |\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}|$.

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

$$\mathrm{ind}(a_{1j}) = \sum_{\boldsymbol{s} \in \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}} \frac{i_{1j}(\boldsymbol{s}) - 1}{i_{1j}(\boldsymbol{s})}. \tag{4.12}$$

Check easily that

$$\begin{aligned}(\boldsymbol{s})a_{12} =& ((s_1s_2)s_1(s_1s_2)^{-1}, s_1s_2s_1^{-1}, s_3, s_4)\\ =& (s_1, s_2, (s_1s_2)^{-1}s_3(s_1s_2), (s_1s_2)^{-1}s_4(s_1s_2)) \text{ (in } \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}).\end{aligned} \tag{4.13}$$

Thus, a_{12} acts by conjugation by s_1s_2 on the third and fourth components and leaves the others unchanged. It follows that $(\boldsymbol{s})(a_{12})^q = \boldsymbol{s}$ in $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ if and only if

$$(s_1, s_2, (s_1s_2)^{-q}s_3(s_1s_2)^q, (s_1s_2)^{-q}s_4(s_1s_2)^q) = \kappa(s_1, s_2, s_3, s_4)\kappa^{-1} \tag{4.14}$$

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

(4.15) There exists $\gamma \in Z(s_1, s_2)$ such that $\gamma(s_1s_2)^{-q} \in Z(s_3)$.

Hence, $i_{12}(\boldsymbol{s})$ is the smallest integer $q > 0$ with $(s_1s_2)^{-q} \in Z(s_1, s_2)Z(s_3)$. Therefore, the factor group $< s_1s_2 > / < s_1s_2 > \cap Z(s_1, s_2)Z(s_3)$ has order $i_{12}(\boldsymbol{s})$. Similarly, check that

$$\begin{aligned}(\boldsymbol{s})a_{12} &= ((s_2s_4)^{-1}s_1(s_2s_4), s_2, (s_4s_2)^{-1}s_3(s_4s_2), s_4), \text{ and}\\ (\boldsymbol{s})a_{14} &= (s_1, (s_4s_1)^{-1}s_2(s_4s_1), (s_4s_1)^{-1}s_3(s_4s_1), s_4) \text{ (in } \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}).\end{aligned}$$

Thus, the integer $i_{13}(\boldsymbol{s})$ (resp., $i_{14}(\boldsymbol{s})$) is the smallest integer $q>0$ such that $(s_4s_2)^q \in Z(s_2,s_4)Z(s_3)$ (resp., $(s_4s_1)^q \in Z(s_1,s_4)Z(s_3)$). Finally, we get

$$
\begin{aligned}
i_{12}(\boldsymbol{s}) &= |<s_1s_2>/<s_1s_2>\cap Z(s_1,s_2)Z(s_3)| \\
i_{13}(\boldsymbol{s}) &= |<s_4s_2>/<s_4s_2>\cap Z(s_4,s_2)Z(s_3)| \\
i_{14}(\boldsymbol{s}) &= |<s_4s_1>/<s_4s_1>\cap Z(s_4,s_1)Z(s_3)|.
\end{aligned} \tag{4.16}
$$

Theorem 4.7: *Assume the hypotheses of Theorem 4.3 and Theorem 4.5. Then, (4.11) gives the genus $g(\mathbf{C})$, where (4.12) and (4.16) give* $\mathrm{ind}(a_{12})$, $\mathrm{ind}(a_{13})$ *and* $\mathrm{ind}(a_{14})$.

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

$$
\begin{aligned}
\alpha_1 &= (2\,n{-}1)(3\,n{-}2)\cdots(p{-}1\,p{+}3)(p\,p{+}2); \\
\alpha_2 &= (1\,n)(2\,n{-}1)(3\,n{-}2)\cdots(p{-}1\,p{+}3)(p\,p{+}2); \\
\alpha_3 &= (1\,n{-}1)(2\,n{-}2)(3\,n{-}3)\cdots(p{-}1\,p{+}2)(p\,p{+}1).
\end{aligned}
$$

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 $\boldsymbol{s}(\alpha)=(s_1,s_2,s_3,s_4)$ of (3.2):

$$
\begin{aligned}
s_1 &= \alpha_1 = (2\,n{-}1)(3\,n{-}2)\cdots(p{-}1\,p{+}3)(p\,p{+}2); \\
s_2 &= \alpha_1\alpha_2 = (1\,n); \\
s_3 &= \alpha_2\alpha_3 = (n\,n{-}1\ldots2\,1); \\
s_4 &= \alpha_3 = (1\,n{-}1)(2\,n{-}2)(3\,n{-}3)\cdots(p{-}1\,p{+}2)(p\,p{+}1).
\end{aligned}
$$

Order $\mathrm{C}_1,\mathrm{C}_2,\mathrm{C}_3,\mathrm{C}_4$ so they respectively denote the conjugacy classes of s_4,s_1,s_2,s_3. Thus $(s_1,s_2,s_3,s_4)\in \mathrm{ni}(\mathbf{C})^{\mathrm{ab}}$ and $(s_4,s_1,s_2,s_3)\in \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. Specifically, we have: $\mathrm{C}_1=\{$products of p disjoint 2-cycles$\}$; $C_2=\{$products of $p{-}1$ disjoint 2- cycles$\}$; $C_3=\{$ 2-cycles$\}$; $C_4=\{n$-cycles$\}$. Any conjugacy class in S_n is rational. In particular, these are.

We now investigate the Hurwitz monodromy action on $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. First, a lemma that helps us list the elements in $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. In the following, for any $s,\omega\in S_n$, we let s^ω denote the conjugate of s under ω (i.e., $s^\omega=\omega^{-1}s\omega$). For $i\in\{1,\ldots,n\}$, i^ω 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 ρ_0 fixed by b. There are two possibilities.*
(i) *$O=(\rho_0\rho_1\ldots\rho_t\rho_t^b\ldots\rho_1^b)$ with $t\ge0$ and none of the integers ρ_i, $i>0$, fixed by b; ρ_t is then fixed by a and O is a cycle of odd length.*
(ii) *$O=(\rho_0\rho_1\ldots\rho_t\rho_0^*\rho_t^b\ldots\rho_1^b)$ with $t\ge0$ and none of the integers ρ_i, $i>0$, fixed by b; ρ_0^* is then fixed by b and O is a cycle of even length.*
Conversely, we have these partial products from Ob.
(i′) *$(\rho_0\rho_1\ldots\rho_t\rho_t^b\ldots\rho_1^b)(\rho_1\rho_1^b)\ldots(\rho_t\rho_t^b)$ is a product of t disjoint 2-cycles.*
(ii′) *$(\rho_0\rho_1\ldots\rho_t\rho_0^*\rho_t^b\ldots\rho_1^b)(\rho_1\rho_1^b)\ldots(\rho_t\rho_t^b)$ 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 ρ_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. □

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

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

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

Lemma 4.9: *The group S_n is generated by σ_3 and σ_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 $(n\, n{-}1 \ldots 1)$ are the cosets modulo a nontrivial divisor of n. Since n is prime, $< \sigma_3, \sigma_4 >$ is a primitive subgroup of S_n, which contains a 2-cycle. Therefore, it is all of S_n. □

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

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

Both σ_1 and σ_2 are of order 2 and σ_2 fixes 3 integers. Lemma 4.8 shows that only one of of these integers, say β, occurs in the odd length cycle $(1\, 2 \ldots 2\mu{-}1)$ of $\sigma_1\sigma_2$. The two other integers fixed by σ_2 appear in the even length cycle $(2\mu\, 2\mu{+}1 \ldots n)$. Denote the integer fixed by σ_2 that is in the second half of $\{2\mu, 2\mu{+}1, \ldots, n\}$ by γ. That is, γ 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 isn't terribly positive, §4.6 makes further comment on what we can expect from variations of this technique.

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

$$|\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}| = \sum_{1 \le \mu \le p} (2\mu - 1)(p - \mu + 1) = \frac{p(p+1)(2p+1)}{6}.$$

Proof: Let $[\mu, \beta, \gamma]$ be a triple in S. Set $\sigma_4 = (n\, n-1 \ldots 1)$ and $\sigma_3 = (1\, 2\mu)$. We need to show that there is a unique pair (σ_1, σ_2) with these properties:

(4.16) $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3, \sigma_4) \in \mathrm{sni}(\mathbf{C})$ and β and γ are fixed by σ_2.

Existence : One has $(\sigma_3\sigma_4)^{-1} = (1\, 2 \ldots 2\mu{-}1)(2\mu\, 2\mu{+}1 \ldots n)$. Using Lemma 4.8 (i′) and (ii′), write $(1\, 2 \ldots 2\mu{-}1) = a'b'$ with a' and b' products of $(\mu - 1)$ 2-cycles with support in $\{1, 2, \ldots, 2\mu{-}1\}$ and β fixed by b'. Also, $(2\mu\, 2\mu{+}1 \ldots n) = a''b''$ 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 γ fixed by b''. Take $\sigma_1 = a'a''$ and $\sigma_2 = b'b''$. The 4-tuple $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ has the required properties (4.16).

Uniqueness: σ_1 and σ_2 satisfy $\sigma_1\sigma_2 = (1\, 2 \ldots 2\mu{-}1)(2\mu\, 2\mu{+}1 \ldots n)$. From Lemma 4.8 (i) and (ii), $(1\, 2 \ldots 2\mu{-}1)$ is of the form $(\rho_0\rho_1 \ldots \rho_t\rho_t^{\sigma_2} \ldots \rho_1^{\sigma_2})$ with $\rho_0 = \beta$, and $(2\mu 2\mu + 1 \ldots n)$ is of the form $(\tau_0\tau_1 \ldots \tau_t\tau_0^*\tau_t^{\sigma_2} \ldots \tau_1^{\sigma_2})$ with $\tau_0 = \gamma$. This determines σ_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 $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ with its image in S. The next step consists in computing indices of a_{12}, a_{13}, a_{14} acting on $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$.

Index of a_{12}: Let $\boldsymbol{s} = [\mu, \beta, \gamma] \in \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$; the centralizer $Z(s_1, s_2)$ is the subgroup of S_n generated by $(2\mu\, 2\mu{+}1 \dots n)^{p-\mu+1}$. Indeed, let $t \in Z(s_1, s_2)$. Then t commutes with $s_1 s_2 = (1\, 2 \dots 2\mu{-}1)(2\mu\, 2\mu{+}1 \dots n)$. Therefore t is of the form $(1\, 2 \dots 2\mu{-}1)^h (2\mu\, 2\mu{+}1 \dots n)^k$. Since t fixes β and permutes the 2 other fixed points of s_2, $h = 0$ and $k = \lambda(p{-}\mu{+}1)$, for some integer λ. Recall from §4.3, the integer $i_{12}(\boldsymbol{s})$ is the smallest integer $q > 0$ such that, for some integer λ,

$$(1\, 2 \dots 2\mu{-}1)^q (2\mu\, 2\mu{+}1 \dots n)^{q-\lambda(p+\mu-1)}$$

commutes with $s_3 = (1\, 2\mu)$ (i.e., fixes the pair $\{1, 2\mu\}$).

The two disjoint cycles $(1\, 2 \dots 2\mu{-}1)$ and $(2\mu\, 2\mu{+}1 \dots n)$ of $s_1 s_2$ are of relatively prime order. Thus, $i_{12}(\boldsymbol{s}) = (2\mu{-}1)(p{-}\mu{+}1)$. Formula (4.16) gives this:

$$\begin{aligned} \mathrm{ind}(a_{12}) &= \sum_{1 \le \mu \le p} (2\mu - 1)(p - \mu + 1)\Big(1 - \frac{1}{(2\mu - 1)(p - 2\mu + 1)}\Big) \\ &= N - p = \frac{p(p-1)(2p+5)}{6} \end{aligned}$$

Index of a_{13}: Let $\boldsymbol{s} = [\mu, \beta, \gamma] \in \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. We easily see the centralizer $Z(s_2, s_4)$ is trivial. The integer $i_{13}(\boldsymbol{s})$ is the smallest integer $q > 0$ such that $(s_4 s_2)^q$ fixes the pair $\{1, 2\mu\}$. Let a and b in $\{1, \dots, n\}$. These observations are helpful:

(4.17)(i) if $a^{s_4} = b \in \{2\mu, \dots, n\}$ and $b^{s_2} \neq 2\mu$, then $a(s_4 s_2)^2 = a^{s_3}$;

(ii) if $a^{s_4} = b \in \{1, \dots, 2\mu - 1\}$ and $b^{s_2} \neq 1$, then $a(s_4 s_2)^2 = a^{s_3}$.

We prove (i)—(ii) is similar. From Lemma 4.8, s_2 fixes the set $\{2\mu, \dots, n\}$. Thus, $b^{s_2} \in \{2\mu, \dots, n\}$ and $b^{s_2} \neq 2\mu$. Therefore $(b^{s_2})s_3 = b^{s_2}$ and

$$(a)(s_4 s_2)^2 = (b^{s_2})s_3 s_2 s_1 s_2 = (b)s_1 s_2 = (a)s_3 s_2 s_1 s_1 s_2 = (a)s_3.$$

Let $a = 1$. We have $1^{s_4} = n \in \{2\mu, \dots, n\}$ and $n^{s_2} \neq 2\mu$. Indeed, from Lemma 4.8 (ii), no two consecutive integers in the even length orbit of $s_1 s_2$ can be images of one another by s_2. The even length orbit of $s_1 s_2$ is $(2\mu\, 2\mu{+}1 \dots n)$. From (4.17)(i), $(1)(s_4 s_2)^2 = 2\mu$. Let $a = 2\mu$. We have $(2\mu)^{s_4} = 2\mu{-}1 \in \{1, \dots, 2\mu{-}1\}$. Lemma 4.8 (i) implies $(2\mu{-}1)^{s_2} = 1$ if and only if $2\mu - 1 = \rho_t$. Distinguish two cases.

- If $2\mu - 1 \neq \rho_t$, (4.17) (ii) gives $(2\mu)(s_4 s_2)^2 = 1$ and $i_{13}(\boldsymbol{s}) = 2$. (Note: $i_{13}(\boldsymbol{s}) \neq 1$ because $(1)(s_4 s_2) = n^{s_2} \neq 1, 2\mu$.)
- •• If $2\mu - 1 = \rho_t$, we obtain $(2\mu)(s_4 s_2)^3 = 2\mu$ and $(1)(s_4 s_2)^3 = 1$. Hence $i_{13}(\boldsymbol{s}) = 3$.

  The number of occurrences of •• is

$$\sum_{1 \le \mu \le p} (p - \mu + 1) = \frac{p(p+1)}{2},$$

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

Index of a_{14}: Let $\boldsymbol{s} = [\mu, \beta, \gamma] \in \mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. Again, the centralizer $Z(s_1, s_4)$ is trivial. The integer $i_{14}(\boldsymbol{s})$ is the smallest integer $q > 0$ such that $(s_4 s_1)^q = (s_2 s_3)^{-q}$ 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 $[\mu, \beta, \gamma]$, $1 \le 1^{s_2} \le 2\mu{-}1$ and $2\mu \le (2\mu)^{s_2} \le n$. So we only have 4 cases to consider.

1st case: $1^{s_2} = 1$ *and* $(2\mu)^{s_2} = 2\mu$. That is, $\boldsymbol{s} = [\mu, 1, \mu{+}p{+}1]$. Here, $i_{14}(\boldsymbol{s}) = 1$.

2nd case: $1^{s_2} \neq 1$ *and* $(2\mu)^{s_2} = 2\mu$. That is, $\boldsymbol{s} = [\mu, \beta, \mu{+}p{+}1]$ with $\beta \neq 1$. Here, $(2\mu)(s_2s_3)^3 = 2\mu$ and therefore $(1)(s_2s_3)^3 = 1$. Thus $i_{14}(\boldsymbol{s}) = 3$. (Note that $i_{14}(\boldsymbol{s}) \neq 1$ since $1^{s_2} \neq 1, 2\mu$.)

3rd case: $1^{s_2} = 1$ *and* $(2\mu)^{s_2} \neq 2\mu$. That is , $\boldsymbol{s} = [\mu, 1, \gamma]$ 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 $i_{14}(\boldsymbol{s}) = 2$.

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

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

Finally, $\mathrm{ind}(a_{14}) = \frac{p(p-1)(p+4)}{6}$.
Now (4.11) gives the genus $g(\mathbf{C})$ of the curve $C(\mathbf{C})$ (cf. Theorem 4.5):

$$g(\mathbf{C}) = \frac{(p-2)(p-3)}{6}.$$

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 haven't checked yet: transitivity of SH_r on $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$. We proceed in two steps.

From (4.13), $a_{12} = Q_1^2$ conjugates by s_1s_2 on the first two components of the 4-tuple $\boldsymbol{s}$ and leaves the others unchanged. So for $\boldsymbol{s} = [\mu, \beta, \gamma]$, we obtain:

$$[\mu, \beta, \gamma]a_{12} = [\mu, (\beta)(s_1s_2)^{-1}, (\gamma)(s_1s_2)^{-1}].$$

Still, the two disjoint cycles $(1\,2 \ldots 2\mu{-}1)$ and $(2\mu\, 2\mu{+}1 \ldots n)$ 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 $1 \leq \beta \leq 2\mu - 1$ and $p + \mu + 1 \leq \gamma \leq n$. Conclude that the orbits of a_{12} are the p subsets of $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ corresponding to each value of μ.

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

$$(s_4s_2)^{-1}s_3(s_4s_2) = (1^{s_4s_2}\, 2^{s_4s_2}) = (n^{s_2}\, 1).$$

That is, a_{13} sends some element $[1, 1, \gamma]$ on some element $[\mu, \beta', \gamma']$ with $(1\,2\mu) = (1\, n^{s_2})$, up to conjugation by a power of s_4.

We have $s_1s_2 = (1)(2\,3 \ldots n)$. Lemma 4.8 (ii) implies the cycle $(2\,3 \ldots n)$ has form $(\rho_0\rho_1 \ldots \rho_t\rho_0^*\rho_t^b \ldots \rho_1^b)$ with $\rho_0 = \gamma$. Check easily that when γ ranges over $\{p{+}2, \ldots, n\}$, n^{s_2} takes on all values in $\{3, 5, ..., n\}$. 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 $E/Q(T)$ with these properties :*
(i) *$E/Q(T)$ 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/Q is a totally real extension.*

End of proof: For $n = 5$, 7, (4.18) yields $g(\mathbf{C}) = 0$. Hence, the curve $C(\mathbf{C})$ is $\mathcal{P}^1$ if it has a Q-rational point. The disjoint cycles in the permutation a_{12} of $\mathrm{sni}(\mathbf{C})^{\mathrm{ab}}$ are in 1-1 correspondence with the points over the branch point $x_2 \in \mathcal{P}^1$ in the cover $C(\mathbf{C}) \to \mathcal{P}^1$ 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 $Q(x_2, x_3, x_4)$.

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

Pick a 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 Section 2.3.) The Q-points are dense in the space $\mathcal{H}(\mathbf{C})'(R)$. 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, $\bar{c} = 1$. Let $E/Q(T)$ be the Galois closure of the extension $Y/Q(T)$. It is a regular extension with properties (i) and (ii). □

4.6. Additions to Theorem 4.11:

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

$$\begin{aligned}
\alpha_1 &= (1\,n)\\
\alpha_2 &= (2\,n)(3\,n{-}1)(4\,n{-}2)\cdots(p{-}1\,p{+}3)(p\,p{+}2)\\
\alpha_3 &= (1\,n)(2\,n{-}1)(3\,n{-}2)\cdots(p{-}1\,p{+}2)(p\,p{+}1).
\end{aligned}$$

The associated curve $C(\mathbf{C})$ has genus $g(\mathbf{C}) = \frac{1}{8}(p-3)(p-5)$. 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 $\alpha_3 = (1\,3)$.

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 $Z/m \times^s Z/2$, for $m = 2$, 4, 6. Moreover, the group $Z/2 \times Z/2$ does satisfy the conclusions of Theorem 4.11 for 3 branch points.

§5. TWO FURTHER APPLICATIONS

The dihedral group D_m is the easiest non-abelian finite group. The reader must be surprised to hear there are serious questions about realizing it as a Galois group of a regular extension $L/Q(x)$. The problem isn't 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 Q as in §4.5. There we could only precede when we knew that a certain curve $C(\mathbf{C})$ was of genus 0.

Suppose, however, that 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. §5.1 gives a definitive result when the number of branch points is less than 6. §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 $Q^{\rm tp}$, the *totally p-adic* algebraic numbers. An algebraic number α is in $Q^{\rm tp}$ if each conjugate of α is in Q_p, the p-adic numbers. §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 $D_m = Z/m \times^s Z/2$ 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 $Q(X)$ with 5 or fewer branch points.*

Proof: Assume that $G = D_m$ is the Galois group of a regular extension $Y/Q(X)$. Let $\Phi : Y_C \to \mathcal{P}^1$ be the associated cover. Take $x_1, \dots, x_r$ to be an ordering of the branch points. Identify G with the monodromy group of the cover. For $i = 1, \dots, r$, let C_i be the conjugacy class of the branch cycles associated with x_i. That is, the cover is in $\mathrm{sni}(\mathrm{C}_1, \dots, \mathrm{C}_r)$. We divide the proof into 2 cases. Let C be the conjugacy class of all involutions in G: $\mathrm{C} = \{(a, 1) \mid a \in Z/m\}$.

1st case: *One of* $\mathrm{C}_1, \dots, \mathrm{C}_r$, *say* C_i, *is different from* C. Let $(a, 0) \in \mathrm{C}_i$. This is an element of prime order 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 $i \in \{1, \dots, r\}$, for all α relatively prime to the order of C_i, $\mathrm{C}_i^{\alpha} = C_j$ for some $j \in \{1, \dots, r\}$.

To complete the first case we show $r \neq 5$. For $r = 5$, $G = D_{11}$ and $\mathrm{C}_1, \dots, \mathrm{C}_5$ are conjugacy classes of 11-cycles. These classes, however, don't generate D_{11}, a contradiction.

2nd case: $\mathrm{C}_1 = \cdots = \mathrm{C}_r = \mathrm{C}$. Observe that $r \neq 2$ when G is not a cyclic group. Also, that $r \neq 3, 5$; the relation $s_1 \dots s_r = 1$ implies that r is even. Assume $r = 4$. The Riemann-Hurwitz formula yields the genus g of the cover $\Phi : Y_C \to \mathcal{P}^1$:

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

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

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

Thus, we have produced an elliptic curve Y_C and a point $\boldsymbol{p}$ of order m. Both are defined over Q. It is classical that the data $(Y_C, \boldsymbol{p})$ corresponds to a rational point on the modular curve $X_1(m) \setminus \{\text{cusps}\}$. As $m > 7$, this contradicts Mazur's theorem [Se1; Theorem 3] (or [M], [MS]).

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

§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 $L/Q(x)$ with at most r_0 branch points.*

Kamienny and Mazur have recent results that approach what we need to show this conjecture [KM]. 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_ms 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 $L/Q(x)$ 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 bQ satisfying the condition that all inertia group generators are involutions an *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 $Q(x)$ 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 $\varphi : \hat{X} \to \mathcal{P}^1$ of degree $2m$ with a description of the branch cycles of form $(\sigma_1, \ldots, \sigma_r)$. Here, each σ_i is in the conjugacy class C (§5.1) of involutions. A complete combinatorial count of these is easy. At least two of these aren't equal (to generate D_m). Write $\sigma_i = (a_i, 1)$. Then, the product of the σs is 1 reduces to $a_1 - a_2 + \ldots - a_r = 0$. Calculations are sufficiently easy to compute elements a_{1j}, $j = 2, \ldots, r$ that generalize those in the §4.2. Their action on $\mathrm{sni}(\mathbf{C})$ is transitive. Formula (4.11), with r replacing 4, gives the genus of the analog of $C(\mathbf{C})$. 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 $\mathcal{H}(\mathbf{C})'$ for this Nielsen class cannot be *unirational* if r is large. (See Problem 5.6.)

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

Take $\alpha \in D_m$ of order m. Form $\hat{X}/\langle\alpha\rangle = Y$, the quotient of $\hat{X}$ by the group generated by α. The degree 2 cover $Y \to \mathcal{P}^1$ presents Y as a hyperelliptic curve of genus $\frac{r-2}{2}$. Also, $\hat{X}$ is a cyclic degree m unramified cover of Y. Lemma 5.3 interprets existence of $\hat{X}$ as a property of $\mathrm{Pic}^0(Y)$, the Picard group of divisor classes of degree 0 on Y. Denote the points of order m on $\mathrm{Pic}^0(Y)$ by $T_m = T_m(Y)$. Then, $G(\bar{Q}/Q) = G_Q$ acts on T_m. If $\boldsymbol{p} \in T_m \setminus \{0\}$ is a point defined over Q, then $G(\bar{Q}/Q)$ has trivial action on $< \boldsymbol{p} >$. When a point has this property, denote the group it generates by Z/m. This says G_Q has trivial action on it.

Similarly, G_Q acts on the m-th roots of 1. This is another copy of Z/m, but to show G_Q has a particular nontrivial action on it, denote it by μ_m. Consider the set $G_m(d)$, $d = \frac{r-2}{2}$, of involution realizations of D_m, as above with r branch points, defined over Q. Let $\mathrm{Pic}^1(Y)$ 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 μ_m into $T_m(Y)$. The image of this map includes all G_Q equivariant injections $\mu_m \to T_m(Y)$ when $\mathrm{Pic}^1(Y)$ has a Q point.*

Proof: Consider multiplication by m on $\mathrm{Pic}^0(Y)$. Denote this endomorphism by ψ_m. The kernel is exactly T_m. Since Y consists of positive divisors of degree 1, Y naturally embeds in $\mathrm{Pic}^1(Y)$ (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 $\mathrm{Pic}^0(Y)$ produce a natural surjective G_Q equivariant map $T_m(Y) \to Z/m$. Here Z/m represents the Galois group of the cover $\hat{X} \to Y$ as above. The end of this proof shows how this gives an injection from μ_m into $T_m(Y)$.

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

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

Conclude: The quotient $Y_{m,\boldsymbol{q}}/V \to Y_{m,\boldsymbol{q}}/T_m = Y_{\boldsymbol{q}}$ is the cyclic unramified cover we seek. We have identified its automorphism group with Z/m with trivial G_Q action. That is, the automorphisms are defined over 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 β above.

The abelian variety $\mathrm{Pic}^0(Y)$ 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 $\mathrm{Pic}^0(Y)$ 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, $\mathrm{Hom}_{G_Q}(T_m, \mu_m)$ is isomorphic to T_m as a G_Q module.

Apply $\mathrm{Hom}_{G_Q}(\cdot, \mu_m)$ to the map $\beta' : \mu_m \to T_m$. This gives $\beta : \mathrm{Hom}_{G_Q}(T_m, \mu_m) \to \mathrm{Hom}_{G_Q}(\mu_m, \mu_m)$. The first term identifies to T_m. Check easily that the second term is just Z/m acting as multiplications. □

Remark 5.4: *When $\mathrm{Pic}^1(Y)(Q)$ is empty.* The proof of Lemma 5.3 used a Q point in $\mathrm{Pic}^1(Y)$ to construct the cover $Y_m \to Y$ canonically. We haven't shown that a μ_p point on $\mathrm{Pic}^0(Y)$ 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 $\mathcal{H}(\mathbf{C})^{\mathrm{in}} = \mathcal{H}(r, m)^{\mathrm{in}}$ to the space of cyclic order m subgroups of m division points on hyperelliptic jacobians. These fibers are homogeneous spaces for the action of PGL(2). If the image of a fiber is μ_m point, when does the fiber have a rational point? □

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

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

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

(3) Let $V(d)$ be primes m that are orders of subgroups of abelian varieties over Q of dimension d that are G_Q modules isomorphic to μ_m.

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

The results of [KM] 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 $[K : Q] \le d$. Denote the Galois closure of K/Q by $\hat{K}$. It is common to call the following formalism, "taking the *Weil trace*" of the elliptic curve over the number field down to Q. Choose a primitive element $\alpha = \alpha_1$ for K/Q. Let $\alpha_1, \dots, \alpha_d$ be the complete list of conjugates of α_1.

Each conjugate α_i gives a conjugate elliptic curve E_i, defined over $Q(\alpha_i)$. Let $G = G(\hat{K}/Q)$ 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 σ as giving a conjugate of A by its action on the coefficients of the equations for A. Call the conjugate A^σ. 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 we can define A over Q. To draw the strongest conclusions, we note this construction is universal in the following sense [FrJ; Prop. 9.34].

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

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

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

A variety W is unirational if there is a map $\varphi : \mathcal{P}^t \to W$ defined on an open subset of $\mathcal{P}^t$ with image a zariski open subset of W. If W and φ are defined over Q, we say W is unirational over Q. Since $\mathcal{P}^t$ 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. We don't yet, however, know how to produce an involution realization of D_m for an arbitrary prime m. (Although it isn't hard to realize D_m as a Galois group of a regular extension of $Q(X)$.)

§**5.3. Descent to the totally real algebraic number field:** Denote the field of all totally real algebraic numbers by 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 $Q^{\text{tr}}(X)$.*

§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 $\mathcal{H}^{\text{in}}(G, \mathbf{C})$ is a (reducible) algebraic variety defined over an explicitly computable field $K(\mathbf{C})$. Here is the key property of this space. Let K be a field containing $K(\mathbf{C})$. Then, G-covers in the Nielsen class $\text{ni}(\mathbf{C})$, defined over K, correspond to K-rational points on $\mathcal{H}^{\text{in}}(G, \mathbf{C})$.

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 don't explain the commutator statement in (5.2). If 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 $Q^{\rm tr}(X)$. 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 $\mathrm{C}_1,\dots,\mathrm{C}_s$ 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. Choose m suitably large that we can pick g_i out of each conjugacy class C_i so that

(5.3) $\boldsymbol{g}=(g_1,\dots,g_s)$ generate G.

With $r=2sb$, consider the r-tuple $\mathbf{C}$

$$(\mathrm{C}_s^{-1},\dots,\mathrm{C}_1^{-1},\dots,\mathrm{C}_s^{-1},\dots,\mathrm{C}_1^{-1},\mathrm{C}_1,\dots,\mathrm{C}_s,\dots,\mathrm{C}_1,\dots,\mathrm{C}_s).$$

Here, the first sb components are the conjugacy classes $\mathrm{C}_s^{-1},\dots,\mathrm{C}_1^{-1}$ repeated in this order b times. The last sb components are the conjugacy classes $\mathrm{C}_1,\dots,\mathrm{C}_s$ repeated in this order b times. The Nielsen class $\mathrm{ni}(\mathbf{C})$ is not empty. With $\boldsymbol{g}$ from (5.3), the r-tuple

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

lies in the Nielsen class $\mathrm{ni}(\mathbf{C})$. Observe that all conjugacy classes appear the same number of times, namely $2bm$, in the r-tuple $\mathbf{C}$.

The main theorem of [FrV2; Appendix] shows that, if b is suitably large, then $\mathcal{H}=\mathcal{H}^{\rm in}(G,\mathbf{C})$ is defined over Q and irreducible over $\bar{Q}$. This uses (5.2) to apply a theorem of Conway and Parker [FrV2; Appendix].

We are left with finding $Q^{\rm tr}$-points on the absolutely irreducible variety $\mathcal{H}$. Pop [P] proved that every absolutely irreducible variety defined over $Q^{\rm tr}$ has $Q^{\rm tr}$-points provided it has R-points. This reduces the problem to finding R-points on $\mathcal{H}^{\rm in}(G,\mathbf{C})$. 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 $(g_1,\dots,g_r)$ satisfies the hypotheses of that theorem. □

Remark: [FrV] consists of applications of [FrV2]. In particular, this observes that each finite complex extension L of $Q^{\rm tr}$ is

P(seudo)A(lgebraically)C(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 $G(\bar{Q}/L)$ is a free profinite group.

On the other hand, $Q^{\rm tr}$ isn't even Hilbertian. In fact, involutions—conjugates of complex conjugation—generate the absolute Galois group of $Q^{\rm tr}$. Thus, Galois extensions of $Q^{\rm tr}$ have only groups that are generated by involutions. □

Bibliography

[A] R. Atkin, There is no nontrivial Hecke operator theory for noncongruence subgroups, *from a talk by John Thompson at University of Florida in Spring 1988.*

[BK] Bryant and Kovacs, Lie representations and groups of finite order, *J. London Math. Soc.* **17** (1978), 415–421.

[BFr] R. Biggers and M. Fried, Moduli spaces of covers and the Hurwitz monodromy group, *Crelles Journal* **335** (1982), 87–121.

[Bo] F. Bohnenblust, The algebraical braid group, Ann. of Math. **(2) 48** (1947), 127–136.

[CoH] K. Coombes and D. Harbater, Hurwitz families and arithmetic Galois groups, *Duke Math. J.* **52** (1985), 821–839.

[DFr] P. Dèbes and M. Fried, Arithmetic variation of fibers, *Crelles Journal* **409** (1990), 106–137.

[D] E. Dew, Fields of moduli of arithmetic covers, *Thesis* (1991).

[Fr1] M. Fried, Fields of definition of function fields and Hurwitz families–Groups as Galois groups, *Comm. in Alg.* **5(1)** (1977), 17–82.

[Fr2] M. Fried, Arithmetic of 3 and 4 branch point covers, *Sèminaire de Théorie des Nombres, Delange-Pisot-Poitou, Birkhauser* 1987/88).

[FrD] M. Fried and P. Dèbes, Rigidity and real residue class fields, *Acta Arith.* **56, n• 4** (1990), 13–45.

[FrJ] M. Fried and M. Jarden, Field Arithmetic, *Springer, Ergebnisse* **11** (1986).

[FrV] M. Fried and H. Völklein, The embedding problem over a Hilbertian PAC-field, *Annals of Math.*, *Annals of Math* **135** (1992), 1–13.

[FrV2] M. Fried and H. Völklein, The inverse Galois problem and rational points on moduli spaces, *Math. Annalen* **290** (1991), 771–800.

[FrV3] M. Fried and H. Völklein, Unramified abelian extensions of Galois Covers, *Proceedings of Symp. in Pure Math.* **49** (1989), 675–693.

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

[Ha] D. Harbater, Galois covering of the arithmetic line, *Proc. of the NY Number Thy. Conf., LNM* **1240, Springer** (1985).

[Hup] B. Huppert, Endliche Gruppen I, *Springer-Verlag* **134** (1967).

[Hur] A. Hurwitz, Riemann'sche Flächen mit gegebenen Veizweigungspunkten, *Mathematische Werke* **I**, 321–383.

[KM] B. Mazur and S. Kamienny, Rational torsion of prime order in elliptic curves over number fields, preprint 6/92.

[KN] A. Krull and J. Neukirch, Die Struktur der absoluten Galois gruppe über dem Körper $R(T)$, *Math. Ann.* **193** (1971), 197–209.

[L] S. Lang, Abelian Varieties, *Inter. Science Tracts, New York***7** (1959).

[M] B. Mazur, Rational points on modular curves, *Lecture Notes in Math., Springer-Verlag* **601** (1977), 107–148.

[MS] B. Mazur and J.-P. Serre, Points rationnels des courbes modulaires $X_0(N)$,
Séminaire Bourbaki, 27e année (1974/75), *Exposé* **469**, *Lecture Notes in Math., Springer-Verlag* **514** (1976), 238–255.

[P] F. Pop, Fields of totally Σ-adic numbers, preprint 1991.

[Se1] J.-P. Serre, Points rationnels des courbes modulaires, *Séminaire Bourbaki, 30ème année* **n• 511** (1977/78).

[Se2] J.-P. Serre, Groupes de Galois sur Q, *Séminaire Bourbaki* **n• 689** (1987/88).

[Se3] J.-P. Serre, Topics in Galois theory, *Research Notes in Mathematics, Jones and Bartlett* (1992).

[W] A. Weil, The field of definition of a variety, Oeuvres complètes (Collected papers) **II**, Springer-Verlag, 291–306.

Mike Fried

e-mail: mfried@math.uci.edu

Mathematics Department

UC Irvine

Irvine, California 92717

Pierre Debes

e-mail: pde@ccr.jussieu.fr

Univ. Pierre et Marie Curie (Paris 6)

Mathematiques: Tour 45-46, 5 ET,

BP 1724 Place Jussieu

F-75252 PARIS Cedex 05, FRANCE

Problémes Diophantiens