Geometric Galois Actions II Dessins d'Enfants, Mapping Class Groups and Moduli 243, London Mathematical Society Lecture Note series, (1997) 172–197.

Applying Modular Towers to the Inverse Galois Problem

Michael D. Fried and Yaacov Kopeliovich

Let G be a finite (possibly simple) group, and let p be a prime dividing the order of G. The characteristic finite quotients ${}_p^k\tilde{G}$ of the universal p-Frattini cover of G are strikingly similar groups. It takes an effort to distinguish them for finding $\mathbb{Q}$ regular realizations for the Inverse Galois problem. This paper starts a program to show one can't realize *all* these groups as Galois groups of extensions $L/\mathbb{Q}(x)$ with at most r (fixed) branch points. Let $\mathbf{C}$ be an r-tuple of p-regular conjugacy classes of G. To compare realizations of these groups we use a sequence of varieties—a *Modular Tower*—attached to $(G, p, \mathbf{C})$. The notation for this sequence is $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})$, $k = 0, 1, \ldots$: $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})$ is the kth *level* of the Modular Tower. Crucial properties of level k translate to properties of the characteristic modular representation of ${}_p^k\tilde{G}$. Properties of these representations support the following statement.

Conjecture. *For each r there exists k_r so that for $k > k_r$, $\mathbb{Q}$ regular realization of ${}_p^k\tilde{G}$ requires more than r branch points.*

For $r = 4$ this reduces to showing two pieces of geometric information.

(a) There is a uniform (with k) bound on the number of absolutely irreducible components at the kth level.

(b) For k large $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})$ has no *obstructed* components.

The main example of this paper and [FrK] is $G = A_5$, $p = 2$ and $\mathbf{C} = \mathbf{C}_{3^r}$ with $r = 4$ repetitions of the conjugacy class of 3-cycles. It allows full explanation and illustration of the significance of obstructed components.

§0. Introduction to the main problem.

[MT] introduced Modular Towers. This paper concentrates on exactly one application of these to the Inverse Galois Problem. Fix an indeterminate x

Support from NSF #DMS-9622928 for both authors; first author support from Alexander von Humboldt Foundation and Institut für Experimentalle Mathematik, July 1996. Correspondence with John Thompson, after an Oct. 1996 conference at UF, induced us to write §4 reducing our Main Conjecture to a diophantine statement on points on Modular Towers. Conversations with Bob Guralnick improved our confidence with the group theory parts of the paper. Finally, Elena Black's conference talk exclamation, "Do you know how hard it is to work with one group at a time?" inspired the philosophy of §1.B: Fix conjugacy classes and change the group.

as a uniformizing parameter for the projective x line $\mathbb{P}^1 = \mathbb{P}^1_x$. For any field K let $\bar{K}$ be an algebraic closure of K. The characteristic of K is 0, and K is usually a subfield of the complex numbers $\mathbb{C}$. The symmetric group of degree n is S_n and its alternating subgroup is A_n.

The framework of this paper has appeared nowhere else. It includes an introduction to more comprehensive results of [Fr1] and [FrK]. These will quote this paper. Modular Towers join *Hurwitz space* constructions and the *universal Frattini cover* of a finite group. App.I reviews relevant definitions from [MT]. One crucial point: Levels of a Modular Tower aren't (usually) homogeneous spaces. Yet, modular representation theory provides a replacement for the semisimple Lie group theory often attached to homogeneous spaces.

§**0.A. Basic Notation.** Recall what is a K *regular realization* of a finite group G: G is the Galois group of an extension $L/K(x)$ with $L \cap \bar{K} = K$.

The main combinatorial data for a regular realization is a set of conjugacy classes $\mathbf{C}$ from G. A place x' of $\mathbb{C}(x)$ denotes the specialization of the elements of $\mathbb{C}(x)$ associated to $x \mapsto x'$. Consider any place $\mathfrak{p}$ of $\mathbb{C} \cdot L$ over x'. Let $e = e(\mathfrak{p}/x')$ be the ramification index of $\mathfrak{p}$ over x'. If $e > 1$ for some $\mathfrak{p}$ over x', call x' a *branch point* of the extension $\mathbb{C} \cdot L/\mathbb{C}(x)$. Then, the completion $L_{\mathfrak{p}}$ of L at $\mathfrak{p}$ embeds in the Laurent field $\mathbb{C}\{\{(x - x')^{\frac{1}{e}}\}\}$. Restricting the automorphism $(x - x')^{\frac{1}{e}} \mapsto \exp^{2\pi i/e}(x - x')^{\frac{1}{e}}$ to L gives $g_{\mathfrak{p}} \in G$. Referencing only x', and not $\mathfrak{p}$, defines $g_{\mathfrak{p}}$ up to conjugacy in G.

This attaches a unique conjugacy class C of G to x'. Thus, the complete set $\mathfrak{x} = \{x_1, \dots, x_r\}$ of branch points of the extension produces a collection $\mathbf{C} = \{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ of conjugacy classes in G. A description of branch cycles for $L/K(x)$ consists of an r-tuple $\mathfrak{g} = (g_1, \dots, g_r) \in G^r$ with these properties:

(0.0a) $\mathfrak{g} \in \mathbf{C}$, $g_1 \cdots g_r = \Pi(\mathfrak{g}) = 1$; and
(0.0b) $\langle \mathfrak{g} \rangle = G$.

Here $\mathfrak{g} \in \mathbf{C}$ means, in some order, entries of $\mathfrak{g}$ are in the classes $\mathbf{C}$.

For any regular extension $L/\mathbb{Q}(x)$ such an r-tuple satisfying (0.0) always exists. It isn't, however, unique. The *Nielsen class* $\mathrm{Ni}(G, \mathbf{C})$ of a cover is the complete collection of elements $\mathfrak{g}$ satisfying the conditions (0.0). This codifies the relation between different covers and all descriptions of branch cycles (see App.I).

§**0.B. The Main Conjectures.** Let G be a finite group and p a prime dividing $|G|$. Also, assume G is centerless (has no center). The pair (G, p)

produces an infinite sequence of *characteristic Frattini covers*:

$$(0.1) \qquad \cdots \to {}_p^k\tilde{G} \to {}_p^{k-1}\tilde{G} \to \cdots \to {}_p^0\tilde{G} = G.$$

§1.B reminds of the basics. The characteristic homomorphism $\phi_k : {}_p^k\tilde{G} \to G$ has p-group kernel for each nonnegative integer k. Let ${}_p\mathcal{C}(G)$ be those conjugacy classes of G whose elements have order prime to p. These are the *p-regular conjugacy classes* of G. Thus, $\mathrm{C} \in {}_p\mathcal{C}(G)$ lifts uniquely to a conjugacy class in ${}_p^k\tilde{G}$ of elements with the same order. Also, refer to this lifted conjugacy class as C: $\mathrm{C} \in {}_p\mathcal{C}({}_p^k\tilde{G}) = {}_p\mathcal{C}(G)$. Denote the cardinality of the conjugacy classes in $\mathbf{C}$ by $r = r(\mathbf{C})$.

Main Conjecture 0.1. *Let r_0 be any positive integer.*

(†.a) *$\exists\ k_a = k_a(G, p, r_0)$ with this property. For $k > k_a$, $\mathbb{Q}$ regular realization of ${}_p^k\tilde{G}$ with r branch cycles in ${}_p\mathcal{C}(G)$ requires $r > r_0$.*

(†.b) *$\exists\ k_b = k_b(G, p, r_0)$ with this property. For $k > k_b$, $\mathbb{Q}$ regular realization of ${}_p^k\tilde{G}$ requires $r > r_0$ branch cycles.*

It simplifies notation to consider this over $\mathbb{Q}$. So, we restrict often to that case. Still, for K finitely generated over $\mathbb{Q}$ replacing $\mathbb{Q}$ this should hold with k_a and k_b depending on K.

Let r be an integer and $\mathbf{C}$ a collection of r conjugacy classes (possibly with repetitions) from ${}_p\mathcal{C}(G)$. To this data [MT] canonically attaches a sequence of reduced Hurwitz spaces (App.II):

$$(0.2) \qquad \cdots \mathcal{H}({}_p^{k+1}\tilde{G}, \mathbf{C})^{\mathrm{rd}} \to \mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}} \to \cdots \to \mathcal{H}({}_p^0\tilde{G}, \mathbf{C})^{\mathrm{rd}}.$$

The kth level is the manifold $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ and ${}_p^0\tilde{G} = G$. Special Case: $G = D_p$ is the dihedral group of order $2p$, p is an odd prime and $\mathbf{C}$ is $r = 4$ repetitions of the conjugacy class of involutions. Then, (0.2) is the classical sequence of modular curves:

$$\cdots \to Y_1(p^{k+2}) \to Y_1(p^{k+1}) \to \cdots \to Y_1(p).$$

This case agrees with the conclusion of the Main Conjecture. For this case, however, it is easy to show the levels have only one (unobstructed) component. [Fr3, §7] gives the reduction of (†.b) to (†.a) for $G = D_p$ and for any value of r_0.

For D_p and $r_0 = 4$ (or 5) the results are very strong; they translate to known results of Frey, Kamienny, Mazur and Merrill. They even give a statement uniform in p ([DFr, §5] or [Fr3, §7]). Conjecture 0.1 asks for less in this case: that $\mathbb{Q}$ regular D_{p^k} realization requires at least 6 branch points if $k > k_b$. (Also, k_b here may depend on p.)

The goal is to generalize the following argument. Fix p and let K be any finitely generated extensions over $\mathbb{Q}$. The genus (of the single component) of $Y_1(p^k)$ goes up (quickly) with k. Thus, Falting's Theorem implies the K points $Y_1(p^k)(K)$ on $Y_1(p^k)$ are finite, excluding finitely many values of p^k. The conjecture thus comes to eliminating a possible projective system $\mathfrak{y}_k \in Y_1(p^{k+1})$ of K rational points. [Fr3, §7] handles this when $G = D_p$ and $r_0 = 4$ (or 5).

For an arbitrary finite group G, each step above encounters problems. [FrK] reveals the main difficulties. This case has $G = A_n$ and $\mathbf{C} = \mathbf{C}_{3^r}$, r repeats of the conjugacy class of 3-cycles. The Nielsen class $\mathrm{Ni}_{n,r}$ of r 3-cycles in A_n appears often. Use the notation $\mathcal{H}_{n,r}$ for the corresponding (inner) Hurwitz space (App.I). Though most groups produce difficulties that don't appear for the dihedral group, conjecturally Modular Towers do mimic properties of modular curve towers. Even, however, with $G = D_p$ the conjecture is open if $r_0 > 5$.

Here are three accomplishments of this paper.

(0.3a) For any G it shows that the (†.b) version of Main Conjecture 0.1 reduces to showing (†.a): For k large, $\mathcal{H}({}^k_p\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ has no $\mathbb{Q}$ points.

(0.3b) For $G = A_5$, $p = 2$ and $\mathbf{C} = \mathbf{C}_{3^r}$ it describes progress on bounding components of the kth level, $k \geq 0$, in the Modular Tower.

(0.3c) It shows how *obstructed components* (§0.C) affect the Main Conjecture. Further, A_5 examples support their disappearance for k large.

§**0.C. Obstructed components of a Modular Tower.** The projective limit of sequence (0.1) is the *universal p-Frattini cover* ${}_p\tilde{G}$ of G. §1.C explains how similar are all the groups ${}^k_p\tilde{G}$.

Subtheme 0.2 Replacing G with ${}_p\tilde{G}$ produces conclusions on regular realizations of all ${}_p\tilde{G}$ characteristic quotients.

For fixed r, computations suggest there is a uniform bound on absolutely irreducible components of $\mathcal{H}({}^k_p\tilde{G}, \mathbf{C})^{\mathrm{rd}}$. When r=4, reduced Hurwitz spaces are curves. Bounding the number of components in the kth level is necessary to assure Falting's Theorem applies. That is, the genus of absolutely irreducible components at level k must exceed 1 for k large. Still, that doesn't preclude rational points at arbitrary high levels on the most mysterious of components, those we call *obstructed*.

Suppose no points of $\mathcal{H}({}^{k+1}_p\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ lie above a component $\mathcal{H}'$ of $\mathcal{H}({}^k_p\tilde{G}, \mathbf{C})^{\mathrm{rd}}$. We say $\mathcal{H}'$ is obstructed. [MT, §III.D] gave a *big invariant* detecting obstructed components. Obstruction Lemma 3.2 reformulates this invariant using modular representations.

There is good news and bad news in the appearance of obstructed components. The former occurs if there is exactly one component at level k and it is obstructed. Then, (0.3a) has a positive answer. The reduced Hurwitz space at level $k+1$ is empty, so it has no rational points. [Fr1] gives examples of exactly that (see Thm. 3.1 in §3.A).

Many cases, however, have at least one unobstructed component. General results describing components of a level of a Modular Tower require conjugacy classes in $\mathbf{C}$ to appear with high multiplicity. The rest of this subsection illustrates this.

Definition 0.3 Consider a collection $\mathbf{C}$ of conjugacy classes from a finite group G. Let s_0 be a positive integer. Then, $\mathbf{C}$ has *multiplicity* at least s_0 if *each* conjugacy class in $\mathbf{C}$ appears at least s_0 times.

Suppose $\mathbf{C}$ has suitably (explicitly) high multiplicity compared to k. Then, an effective version of a Conway and Parker result precisely bounds the components at level k. The following is a special case of a result from [FrK]. Here $M({}_p^k\tilde{G})$ is the *Schur multiplier* of ${}_p^k\tilde{G}$.

Theorem 0.4 *Fix a value of k. Assume G is perfect and centerless, $p \mid |G|$, all classes in $\mathbf{C}$ are from ${}_p\mathcal{C}(G)$ and $\mathbf{C}$ has multiplicity at least s_0. Decompose $\mathcal{H}({}_p^k\tilde{G},\mathbf{C})^{\mathrm{rd}}$ into absolutely irreducible (dimension $r-3$) components $\cup_{i=0}^{t_k}\mathcal{H}'_i$. Then, there is an explicit $s_0(G,k) = s_0$ so the following hold.*

(0.4a) $t_k + 1 = |M({}_p^k\tilde{G})|$.

(0.4b) $\mathcal{H}'_0$ *is unobstructed.*

(0.4c) *If $\mathbf{C}$ is a rational union (see* §1.A*), $\mathcal{H}'_0$ has field of definition $\mathbb{Q}$.*

(0.4d) $\mathcal{H}'_i$ *is obstructed, $i = 1,\dots,t_k$.*

§0.D. Disappearance of obstructed components for k large. Suppose G has a nontrivial Schur multiplier (as does A_n). Then, so does ${}_p^k\tilde{G}$ for all k (Schur Multipliers Result 3.3). Thus, Theorem 0.4 implies obstructed components appear in $\mathcal{H}_{n,r}^{\mathrm{rd}}$ for r large (notation from §0.B). The crucial investigation must consider minimal values $r_0 = r_0(n,k)$ of r that produce obstructed components in $\mathcal{H}({}_2^k\tilde{G},\mathbf{C}_{3^r})^{\mathrm{rd}}$. By contrast, a particular Modular Tower considers k large compared to a fixed value of $r = r(\mathbf{C})$. There are serious diophantine troubles for the Main Conjecture should new obstructed components appear at each level.

For example, suppose there is an s_0 giving the following.

(0.5a) Theorem 0.4 holds with s_0 independent of k.

(0.5b) There is a bound on $|M({}_p^k\tilde{G})|$ independent of k.

This would produce a bound in (0.3b), at least for r large. That wouldn't, however, contribute to the Main Conjecture. Even the strongest diophantine conjectures can't eliminate rational points on obstructed components at arbitrary high levels of a Modular Tower. Worse yet, (0.5b) doesn't hold.

So, it is a surprise that the case $G = A_5$, $p = 2$ and $\mathbf{C} = \mathbf{C}_{3^r}$ supports the following conjecture. Recall: A projective nonsingular variety V is of *general type* if it's canonical bundle is ample. If V is a curve this means V has genus at least two. Using the phrase *general type* on $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ means apply it to some nonsingular compactification of its components.

Conjecture 0.5. *Assume G is centerless, $p \,|\, |G|$ and $\mathbf{C}$ are conjugacy classes from ${}_p\mathcal{C}(G)$. Then, there are two constants $B = B(G, r)$ and $k_0 = k_0(G, r)$ so that for $k \geq k_0$, the following hold.*

(0.6a) $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ *has at most B absolutely irreducible components.*

(0.6b) *Each component of $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ is of general type.*

(0.6c) *No components of $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ are obstructed.*

The classical connection has $G = D_p$, p is an odd prime, and $\mathbf{C}$ is $r = 2r'$ repetitions of the conjugacy class of involutions for some integer r'. Braid group action on Nielsen classes here is easy to calculate. As in App.I, orbits of the braid group B_r on Nielsen classes $\mathrm{Ni}(G, \mathbf{C})$ correspond to the components of $\mathcal{H}(G, \mathbf{C})$. [Fr4, §3] shows there is one orbit. So (0.6a) and (0.6c) hold. When $r' = 2$, §0.B notes (0.6b) holds. This seems to be unknown for higher values of r'.

Beyond dihedral groups, evidence for (0.6c) is from the case $G = A_5$. Lemma 3.2 uses the action of the characteristic quotient ${}_p^k\tilde{G}$ on the characteristic kernel $\ker_k / \ker_{k+1}$ for all values of k. Consider this contrast with k_0 fixed and r large. Then, Theorem 0.4 says $\mathcal{H}({}_2^{k_0}\tilde{A}_5, \mathbf{C}_{3^r})^{\mathrm{rd}}$ has at least two absolutely irreducible components; one unobstructed and all others obstructed. For $r = 4$, however, we expect—a result of [FrK] for k small—no obstructed components for any value of k. There should be a minimal value $r' = r'(k_0)$ of r for which there are no obstructed components in $\mathcal{H}({}_2^k\tilde{A}_5, \mathbf{C}_{3^{r'}})^{\mathrm{rd}}$ for $k \geq k_0$. In support of (0.6c), [FrK] makes an explicit guess for $r' = r'(k_0)$.

§1. Precise versions of the main conjecture.

Here is the data for a Modular Tower: a finite group G, a prime $p \,|\, |G|$ and a collection of r conjugacy classes $\mathbf{C}$ from ${}_p\mathcal{C}(G)$. Recall: D_r is the *discriminant locus* in projective r-space. We concentrate on $\mathbb{Q}$ realizations of a centerless group G. [FrV] shows this is equivalent to finding a $\mathbb{Q}$ point on an *inner* Hurwitz space $\mathcal{H}(G,\mathbf{C}) = \mathcal{H}(G,\mathbf{C})^{in}$ for some $\mathbf{C}$. See §0.A and App.I for *Nielsen classes* and how $(G,\mathbf{C})$ canonically produces the moduli space $\mathcal{H}(G,\mathbf{C})$ with a cover $\Phi_{G,\mathbf{C}} = \Phi : \mathcal{H}(G,\mathbf{C}) \to \mathbb{P}^r \setminus D_r$. Suppose K is a field of definition of $\mathcal{H}(G,\mathbf{C})$ and $\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})$. Denote the field generated by coordinates of $\mathfrak{p}$ over K as $K(\mathfrak{p})$. In this paper points are *geometric* points. Also, having coordinates for $\mathfrak{p}$ means $\mathcal{H}(G,\mathbf{C})$ is a quasi-projective (even affine) algebraic set ([Fr2], [FrV] or [V]).

§1.A. Notation for $\mathbb{Q}$ moduli spaces. Let $N_{\mathbf{C}} = N$ be the least common multiple of the orders of elements in the collection $\mathbf{C}$. The group $\hat{\mathbb{Z}}^*$ is the projective limit of the invertible elements of $\mathbb{Z}/N$ over all positive integers N. Consider a field K (a subfield of $\mathbb{C}$). A Galois extension $L/K(x)$ is a K regular $(G,\mathbf{C})$ *realization* if the following hold.

(1.1a) $G(L/\mathbb{Q}(x)) = G$ and $L \cap \bar{K} = K$, and

(1.1b) points of the x line ramified in L have associated *branch cycles* in $\mathbf{C}$.

Covers associated to such extensions have r branch points. According to the *branch cycle argument* ([Fr2, before Thm. 5.1], [Fr3], [V, p. 34]), there is a first criterion for such a realization. The minimal field containing all roots of 1 is $\mathbb{Q}^{cyc}$, the cyclotomic closure of $\mathbb{Q}$. The formulation uses the K-cyclotomic group:

$$H_K = \{\sigma \in G(\mathbb{Q}^{cyc}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \mid \ \sigma \text{ fixes elements of } K \cap \mathbb{Q}^{cyc}\}.$$

Each $n \in H_K$ defines an invertible integer modulo $N_{\mathbf{C}}$. So $\mathbf{C}^n$, all elements of $\mathbf{C}$ to the power n, makes sense.

Definition 1.1 Call $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ a *K-rational union* if $\mathbf{C}^n = \mathbf{C}$ for each $n \in H_K$. Then, $\mathbf{C}$ is a rational union if $\mathbf{C}^n = \mathbf{C}$ for each $n \in \hat{\mathbb{Z}}^*$.

[MT, p. 161] explains the meaning of this phrase: $\mathcal{H}(G,\mathbf{C})$, as a *moduli space* has field of definition K. Roughly: For any point $\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})$ the least field of definition of a Galois cover in the Nielsen class representing $\mathfrak{p}$ is $K(\mathfrak{p})$. The K-rational condition in the next result is necessary for $\mathcal{H}(G,\mathbf{C})$ to be a moduli space over K. Again, the elementary branch cycle argument gives this. That K-rationality suffices is tougher—see [FrV] or [V, §10.3.2].

K-Branch Cycle Argument 1.2 [Fr2, §5] Assume G is a centerless group. The moduli space $\mathcal{H}(G,\mathbf{C})$ (with its morphism Φ) has field of definition K if and only if $\mathbf{C}$ is a K-rational union. If $\mathcal{H}(G,\mathbf{C})(K)$ is nonempty, then $\mathbf{C}$ is a K-rational union and $\mathcal{H}(G,\mathbf{C})$ contains an absolutely irreducible component over K. Also, K points on $\mathcal{H}(G,\mathbf{C})$ produce K regular $(G,\mathbf{C})$ realizations.

For simplicity, the remainder of the paper concentrates on $K = \mathbb{Q}$. In particular, assume the conjugacy classes $\mathbf{C}$ from G is a rational union.

§1.B. Fix conjugacy classes, change the group. Our Main Conjecture divides into cases: $(p, N_{\mathbf{C}}) = 1$ and $p \,|\, N_{\mathbf{C}}$. §2 and §3 consider the case $(p, N_{\mathbf{C}}) = 1$. The Main Conjecture reduces to this case according to Theorem 4.4. Analysis of components of $\mathcal{H}({}^k_p\tilde{G}, \mathbf{C})$ as k varies requires information about ${}_p\tilde{G}$. To help, we expand here on [FrJ, Chap. 20] and [MT, Part II]. This discussion will continue in [FrK].

The universal p-Frattini cover $\phi_G : {}_p\tilde{G} \to G$ of G is *versal* for embedding problems with p-group kernel. The meaning of versal: Given $\psi : A \to G \to 1$ exact, there is a map $\psi' : {}_p\tilde{G} \to A$ giving the obvious commutative diagram. Versal, unlike universal, does not mean ψ' is unique. If G is perfect, the universal p-central extension of G is an example of a natural quotient of ${}_p\tilde{G}$. It is, however, a very small quotient. We explain this.

Let $\ker_0 \to {}_p\tilde{G} \to G$ be the natural short exact sequence. Then, $\ker_0$ is a pro-free p-group of finite rank. Define $\ker_k$ inductively: It is the closed subgroup of ${}_p\tilde{G}$ that $[\ker_{k-1}, \ker_{k-1}] \ker_{k-1}^p$ generates. Then, ${}^k_p\tilde{G} = {}_p\tilde{G}/\ker_k$. Follow [FrJ, Chap. 20] in calling the minimal number of elements that generate it its *rank*.

The hypothesis $(p, N_{\mathbf{C}}) = 1$ allows a special choice of lift of entries of $\mathbf{C}$ to corresponding conjugacy classes of ${}_p\tilde{G}/\ker_k = {}^k_p\tilde{G}$. Choose lifting representatives with the same orders as their images in G. To emphasize this choice of conjugacy classes in ${}^k_p\tilde{G}$, keep the notation $\mathbf{C}$ for these *lifted* classes. Further, as conjugacy classes in ${}^k_p\tilde{G}$, $\mathbf{C}$ is also a rational union, inheriting this property from G.

The Frattini cover property appears here. Suppose elements of ${}^k_p\tilde{G}$ are entries of $\mathfrak{g}' \in \mathbf{C}$. Also, assume $\mathfrak{g}'$ lifts entries of $\mathfrak{g} \in \mathrm{Ni}(G, \mathbf{C})$. Then, $\langle \mathfrak{g}' \rangle = {}^k_p\tilde{G}$. From the character theory viewpoint—including generalizations of *rigidity*—$({}^k_p\tilde{G}, \mathbf{C})$ realizations are much like $(G, \mathbf{C})$ realizations.

Reminder Statement 1.3. [**MT**, Lemma 3.6] Suppose G is centerless and perfect. Then, so is ${}^k_p\tilde{G}$, $k \ge 0$. In particular, a $\mathbb{Q}$ point on $\mathcal{H}({}^k_p\tilde{G}, \mathbf{C}) = \mathcal{H}_k$ is equivalent to giving a $\mathbb{Q}$ regular $({}^k_p\tilde{G}, \mathbf{C})$ realization [FrV]. Such a point automatically gives $\mathbb{Q}$ regular $({}^j_p\tilde{G}, \mathbf{C})$ realizations, from the images of the corresponding point in $\mathcal{H}_j$, $0 \le j \le k$.

One goal of this paper is to show progress on the following problem.

Modular Tower Conjecture 1.4. *Suppose G is a centerless group and r is a positive integer. With $k = k(G, r)$ suitably large the following hold.*

(1.2a) *For any prime p dividing $|G|$ and conjugacy classes* $\mathbf{C}$ *supported in* ${}_p\mathcal{C}(G)$*,* $\mathcal{H}({}^k_p\tilde G, \mathbf{C})^{\mathrm{rd}}(\mathbb{Q})$ *is empty.*

(1.2b) *More generally, there are no* ${}^k_p\tilde G$ *realizations with at most r branch points.*

Theorem 4.4 shows (1.2a) (for some value of $k(G,r)$) implies (1.2b) (for a possibly larger value of $k(G,r)$). [MT] concentrated on the standard Hurwitz spaces (as in [FrV]) arising from representations of the fundamental group of $\mathbb{P}^r \setminus D_r$ acting on Nielsen classes. App.II explains reduced Hurwitz spaces as a $\mathrm{PSL}_2(\mathbb{C})$ quotient of standard Hurwitz spaces.

§**1.C. Braid action and** $\mathrm{PSL}_2(\mathbb{C})$ **quotients.** Let G be a finite group with conjugacy classes $\mathbf{C}$. Consider one $\mathbb{Q}$ regular $(G,\mathbf{C})$ realization of a group by a cover $\phi : X \to \mathbb{P}^1_x$. This produces infinitely many $\mathbb{Q}$ regular realizations; compose ϕ with any $\alpha \in \mathrm{PSL}_2(\mathbb{Q})$. Thus, to measure $({}^k_p\tilde G, \mathbf{C})$ realizations requires counting $\mathbb{Q}$ points on reduced Hurwitz spaces $\{\mathcal{H}({}^k_p\tilde G, \mathbf{C})^{\mathrm{rd}} = \mathcal{H}^{\mathrm{rd}}_k\}_{k=0}^{\infty}$. These spaces have natural maps

$$\ldots \to \mathcal{H}^{\mathrm{rd}}_{k+1} \to \mathcal{H}^{\mathrm{rd}}_k \to \ldots \to \mathcal{H}^{\mathrm{rd}}_0 \to J_r.$$

App.II gives the definition of J_r. Since $\mathbf{C}$ is a rational union, these spaces and maps have field of definition $\mathbb{Q}$. Investigating this tower requires information on absolutely irreducible components of $\mathcal{H}^{\mathrm{rd}}_k$ for each level k. We explain more of the group theory behind these diophantine problems.

Statement 1.3 says a $\mathbb{Q}$ regular $({}^{k+1}_p\tilde G, \mathbf{C})$ realization produces a $\mathbb{Q}$ $({}^k_p\tilde G, \mathbf{C})$ realization. It also suggests these groups are similar, for example, when G is perfect and centerless. Lifting Lemma 4.1 adds to this. It characterizes ${}_p\tilde G$ quotients giving a cover $\psi : H \to G$ as having the following properties.

(1.3a) The kernel of ψ has p-group kernel.

(1.3b) For $\mathfrak{g}' = \{g'_1, \ldots, g'_s\} \in H$ elements of order prime to p, $\langle \mathfrak{g}' \rangle = H$ if and only if $\langle \psi(\mathfrak{g}') \rangle = G$.

Here is a more subtle similarity between H and G satisfying (1.3). Brauer's Theorem [MT, §II.B] says there as many simple $\bar{\mathbb{F}}_p$ modules as there are p-regular conjugacy classes. Therefore, the two groups have the same simple $\bar{\mathbb{F}}_p$ modules. §3 shows the significance of an appearance of the module $\mathbf{1}$ (for ${}^k_p\tilde G$) in the Loewy display of the $\mathbb{F}_p$ module $\ker_k / ker_{k+1}$. It is the whole story of obstructed components.

Fix r_0 and a field K. Theorem 4.4 says the following are equivalent.

(1.4a) There are K regular ${}^k_p\tilde G$ realizations with at most r_0 branch points for each $k \ge 0$.

(1.4b) For some $r \le r_0$ there is an r-tuple $\mathbf{C}$ of p-regular conjugacy classes of G and for each $k \ge 0$, there are K regular $({}^k_p\tilde G, \mathbf{C})$ realizations.

The Main Conjecture reduces to showing (1.4b) is impossible when K is a number field for each r-tuple $\mathbf{C}$ of p-regular conjugacy classes of G. Proving the Main Conjecture comes to considering rational points on reduced Hurwitz spaces ($\mathrm{PSL}_2(\mathbb{C})$ quotients), curves when $r_0 = 4$ (App.II).

Suppose you show (0.6a) (for large k). Falting's Theorem [Fa] applies if (0.6b) holds: the genus of the components at level k goes up with k. [FrK] gives evidence for this rise in genus from our special case.

§**1.D. Projective systems of rational points.** Suppose the program of §1.C works. Then, there are only finitely many $\mathbb{Q}$ points on some level k_0 of Modular Towers satisfying the hypotheses. It is, however, a formidable task to eliminate the possibility of a nontrivial set of $\mathbb{Q}$ points at every level. This is where hypothesis (0.6c) enters. It assumes there are no obstructed components at level k_0 or beyond. Then, having points at each level above k_0 produces a *projective system* of rational points $\{\mathfrak{p}_k \in \mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}\}_{k=0}^{\infty}$. That is, the canonical map ${}_p^{k+1}\tilde{G} \to {}_p^k\tilde{G}$ inducing $\mathcal{H}({}_p^{k+1}\tilde{G}, \mathbf{C})^{\mathrm{rd}} \to \mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ gives $\mathfrak{p}_{k+1} \mapsto \mathfrak{p}_k$. Precluding projective systems is the last leg for $r = r_0 = 4$. To do so for any value of r is a separate problem independent of other diophantine considerations.

Projective System Conjecture 1.5. *Assume the setup for the Modular Tower above associated to* $(G, \mathbf{C})$*, with* r *arbitrary and* K *finitely generated over a number field. Then, there exists no projective system of* K *rational points on the Modular Tower.*

§2. Construction of universal Frattini covers.

[FrK] expands the Normalizer Observation of [MT, Remark 2.10]. It helps decipher the whole universal p-Frattini cover from representation observations on the original group G. Thus, representation facts about G translate to a presentation of the universal p-Frattini cover of G, and so of its infinite string of characteristic quotients. This section presents two preliminary results in this direction.

§**2.A. Relation of ${}_p\tilde{G}$ to ${}_p\tilde{H}$ with $H \le G$.** Let $P = P_p = P_{G,p}$ be a p-Sylow subgroup of G. The notation $\ker_0(G)$ allows simultaneously distinguishing the characteristic kernels of the universal p-Frattini covers for G and for a subgroup H. Use $\phi_G : {}_p\tilde{G} \to G$ for the canonical map. Also, denote $\ker_i(G)/\ker_{i+1}(G)$ by $M_i(G)$. For any subgroup H of G, restricting H to $M_i(G)$ gives an H module, $M_i(G)_H$. The *rank* of any profinite group G is the smallest number of elements that topologically generate it. Finally, $\tilde{P}_{G,p} = \phi_G^{-1}(P_{G,p})$ is the p-Sylow subgroup of ${}_p\tilde{G}$.

Example 2.1. *The p-Sylow Frattini hull.* Let G be any finite group. Suppose P_p has rank u. The free pro-p group on u generators is ${}_p\tilde{F}_u$. Let $N_G(P_p)$ be the normalizer of P_p in G. Then, the universal p-Frattini cover of $N_G(P_p)$ is ${}_p\tilde{F}_u \times^s N_G(P_p)/P_p$ [Ri, Th. 3.2]. This a special case of Principle 2.3 (below) by extending the action of $N = N_G(P_p)/P_p$ to ${}_p\tilde{F}_u$. Since ${}_p\tilde{F}_u$ is pro-free, there is a subgroup B of $\mathrm{Aut}({}_p\tilde{F}_u)$ mapping surjectively to N.

The essential point is that the kernel of the map $B \to N$ is a pro-p-group. (Prove this by inductively considering the characteristic Frattini quotients of ${}_p\tilde{F}_u$.) Apply Schur-Zassenhaus to split off a copy of N. Thus produce the action of N on ${}_p\tilde{F}_u$ [FrJ, Lemma 20.45]. Important point: Action of N is unique only up to conjugation by an automorphism of ${}_p\tilde{F}_u$. □

Let $\ker_0^*$ be the kernel of ${}_p\tilde{F}_u \to P_p$ as in Ex. 2.1. For Ex. 2.1, the action of $N_G(P_p)$ on $\ker_0^* / \ker_1^*$ extends to G.

Example 2.2. *The p-Sylow Frattini hull can be all of ${}_p\tilde{G}$.* Take $G = A_5$, $p = 2$ and $N_G(P_p) = A_4 \le A_5$. Then, we can identify $\ker_0^*$ as the kernel of the universal 2-Frattini of A_5 [MT, Prop. 2.9]. When, however, $p = 3$ or 5 (and $G = A_5$) $\ker_0^* / \ker_1^*$ is cyclic, and not an A_5 module. In particular, $\ker_0^*$ for these values of p isn't the kernel of ${}_p\tilde{G} \to G$. □

[FrK] generalizes the observation of Ex. 2.2. Principle 2.3 characterizes the universal p-Frattini cover ${}_p\tilde{G}$ of G to relate it to that of its subgroups.

Subgroup Frattini Principle 2.3. Let G be any profinite group and p any prime dividing $|G|$. Then ${}_p\tilde{G}$ is the smallest group that covers G and has its p-Sylow subgroup pro-free.

Suppose $H \le G$ are profinite groups. Then, there is a surjective pro-p group homomorphism $\rho_{G,H} : \ker_0(G) \to \ker_0(H)$. Further, $\rho_{G,H}$ is unique up composition on the left with an automorphism of $\ker_0(G)$. This induces a surjective H module morphism $\rho^*_{G,H} : M_0(G) \to M_0(H)$. Finally, if G is a finite group, the following are equivalent:

(2.1a) $\rho^*_{G,H}$ is an isomorphism.

(2.1b) $\dim_{\mathbb{F}_p}(M_0(G)) = \dim_{\mathbb{F}_p}(M_0(H))$.

(2.1c) $\phi_G^{-1}(H) = {}_p\tilde{H}$.

Proof. First consider the opening characterization of ${}_p\tilde{G}$. For G any profinite group, a simple property determines the universal Frattini cover of $\tilde{G}$. It is the minimal projective cover of G [FrJ, Prop. 20.33]. A profinite group is projective if and only if each p-Sylow subgroup of it is pro-free [FrJ, Prop. 20.47]. The kernel of ϕ_G is a nilpotent group [FrJ, Prop. 20.44]. So $\tilde{G}$ is the fiber product over G of closed subgroups ${}_p\tilde{G}$ for each prime $p \mid |G|$.

Suppose ${}_p\phi^* : {}_p\tilde{G}^* \to G$ is any profinite group cover of G for which ${}_p\tilde{G}^*$

has a pro-free p-Sylow subgroup. Consider the fiber product over G of the groups ${}_p\tilde{G}^*$ and ${}_{p'}\tilde{G}$ for all primes p', $p' \neq p$, dividing $|G|$. Call this fiber product $\tilde{G}^*$. From the Sylow subgroup characterization of projective groups, $\tilde{G}^*$ is projective. Also, it is a minimal projective cover of G if and only if ${}_p\tilde{G}^*$ is a minimal cover of G having a pro-free p-Sylow. This concludes the opening characterization of ${}_p\tilde{G}$.

The remainder of the proof concentrates on universal p-Frattini covers. All notation (say, for $\ker_i$) refers to the fixed prime p. Now consider $H \le G$ profinite groups. Then, $\tilde{H}^* = {}_p\phi_G^{-1}(H)$ is a closed subgroup of ${}_p\tilde{G}$. The p-Sylow subgroup of $\tilde{H}^*$ is a closed subgroup of the p-Sylow of ${}_p\tilde{G}$. Thus, it is projective and therefore pro-free.

Apply the characterization above for the universal p-Frattini cover of H. Conclude there is a surjective map $\beta : \tilde{H}^* \to {}_p\tilde{H}$ commuting with the natural surjective maps to H. The image of β is a closed subgroup of ${}_p\tilde{H}$ mapping surjectively to H. Since ${}_p\tilde{H}$ is a Frattini cover of H, β is surjective. So, it induces the surjective map $\rho_{G,H} : \ker_0(G) \to \ker_0(H)$ in the statement. The rest follows because the 1st characteristic Frattini quotient determines the rank of a pro-free p-group. □

§**2.B. Decomposing Frattini cover kernels.** The following is a special case of [Be, Exer. 1, p. 11]. We fill in details, isolating it from its generalities.

Indecomposability Lemma 2.4. *The ${}_p\tilde{G}/\ker_k(G)$ module $M_k(G)$ is indecomposable.*

Proof. Let M be any G module. Define $\Omega(M)$ to be the kernel of a surjective G module homomorphism $\psi : P \to M$ with P a projective module, minimal for direct sum decomposition. Suppose P' is another module with these properties. Then, projectivity of the two modules gives maps $\alpha : P \to P'$ and $\beta : P' \to P$, each commuting with the surjective maps from P and P' to M. Define $f = \alpha \circ \beta$ and the composition of f, n times, by f_n. Similarly, for g_n with g the composition $\beta \circ \alpha$. If n is large, then $P = \ker(g_n) \oplus \mathrm{Im}(g_n)$. Note: $\ker(g_n)$, being a summand of a projective module, is also projective.

Suppose P and P' aren't isomorphic. Then $\ker(g_n)$ goes to 0 under the map from P to M. This contradicts the minimality of P, and proves that $\Omega(M)$ is well defined. Further, from Schanuel's Lemma [Be, Lemma 1.5.3], up to projective summands $\Omega(M)$ is well defined. Similarly, there is the operator $\Omega^{-1}(M)$: the cokernel of the embedding of M in a minimal injective module.

In the category of finite dimensional modules over group rings, projectives and injectives are the same [Be, Prop. 1.6.2]. Thus, P above is both the minimal projective covering M and an injective module containing $\Omega(M)$.

That is, up to addition of a projective module, $\Omega^{-1}(\Omega(M)) = M$. So, M is indecomposable, if and only if $\Omega(M)$ is. Apply Ω twice to the indecomposable module $M = \mathbf{1}_{{}_p^k\tilde{G}}$. From [MT, Proj. Indecomp. Lemma 2.3], $\ker_k / \ker_{k+1} = \Omega^2(M)$. So, $\Omega^2(M)$ is indecomposable. □

Consider any cover $\phi : H \to G$ with abelian kernel M. Then G acts on M: $g \in G$ maps $m \in M$ to $\bar{g}m\bar{g}^{-1}$ where $\bar{g}$ is any lift of g to H.

Remark 2.5. *Frattini kernels may decompose.* Let M_1 and M_2 be nonisomorphic simple modules appearing as respective kernels for nonsplit extensions G_1 and G_2 of G. Consider the fiber product $H = G_1 \times_G G_2$ and the natural map $\phi_{1,2} : H \to G$. We show $\phi_{1,2}$ is a Frattini cover.

Suppose H_1 is a subgroup of H mapping surjectively to G. As $G_1 \to G$ and $G_2 \to G$ are Frattini covers, H_1 factors surjectively through them both. Thus, by the Jordan-Hölder Theorem, the composition series of the kernel of $H_1 \to G$ includes M_1 and M_2. It must therefore be $M_1 \oplus M_2$.

Two series of simple groups agree when $n = 8$: $A_8 \cong \mathrm{SL}(4, \mathbb{Z}/2)$. Let M_4 be the standard 4 dimensional representation of $\mathrm{SL}(4, \mathbb{Z}/2)$. [Be] shows $H^2(A_8, M_4)$ has dimension 1. This gives a Frattini extension of A_8 not factoring through the universal central extension of A_8. It is an example of the above. □

§3. Progress on the case A_5 and $\mathbf{C} = \mathbf{C}_{3^r}$.

The main example of [FrK] is the A_5 Modular Tower associated with $r = 4$, $p = 2$, and all conjugacy classes those of the 3-cycle in A_5: $\mathbf{C} = \mathbf{C}_{3^4}$. Denote the corresponding reduced Modular Tower (of inner spaces) by

$$\cdots \to \mathcal{H}({}_2^{k+1}\tilde{A}_5, \mathbf{C})^{\mathrm{rd}} \to \mathcal{H}({}_2^{k}\tilde{A}_5, \mathbf{C})^{\mathrm{rd}} \to \cdots \to \mathcal{H}(A_5, \mathbf{C})^{\mathrm{rd}}. \tag{3.1}$$

This example reveals major phenomena that don't occur for modular curves.

§3.A. Illustration of obstructed components. Obstructed components produce both encouraging and discouraging diophantine results. First we illustrate the former. Actual examples go precisely as the outline in §0.C. The proof of the next result explains the variety $\mathcal{H}(G, \mathbf{C})^{\mathrm{abs}}$.

Theorem 3.1. ([Fr1]) *Assume $n \geq 5$ is odd. Then, $\mathcal{H}(A_n, \mathbf{C}_{3^{n-1}})^{\mathrm{rd}}(\mathbb{Q})$ is dense in $\mathcal{H}(A_n, \mathbf{C}_{3^{n-1}})^{\mathrm{rd}}$. Now assume $n \geq 6$ is even. Then, there are no $\mathbb{Q}$ regular $(\frac{1}{2}\tilde{A}_n, , \mathbf{C}_{3^{n-1}})$ realizations.*

Further, there is a $\mathbb{Q}$ unramified cover $\mathcal{H}(G, \mathbf{C})^{in} \to \mathcal{H}(G, \mathbf{C})^{\mathrm{abs}}$, Galois with group $\mathbb{Z}/2$ with the following properties.

(3.2a) *Each $\mathfrak{p} \in \mathcal{H}(G, \mathbf{C})^{\mathrm{abs}}$ corresponds to a degree n cover $\phi_{\mathfrak{p}} : X \to \mathbb{P}^1_x$ whose Galois closure represents $\mathfrak{p}' \in \mathcal{H}(G, \mathbf{C})^{in}$ lying over $\mathfrak{p}$.*

(3.2b) *For* $\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$*,* $\phi_{\mathfrak{p}} : X \to \mathbb{P}^1_x$ *has (minimal) field of definition* $\mathbb{Q}(\mathfrak{p})$*. Its Galois closure is defined over* $\mathbb{Q}(\mathfrak{p}')$ *with* $\mathfrak{p}'$ *lying over* $\mathfrak{p}$*.*

(3.2c) $\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$ *corresponds to a* $\mathbb{Q}(\mathfrak{p})$ *regular* $(A_n, \mathbf{C}_{3^{n-1}})$ *realization if and only if* $\mathbb{Q}(\mathfrak{p}') = \mathbb{Q}(\mathfrak{p})$*.*

For all $n \ge 5$*, the set* $\{\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}(\bar{\mathbb{Q}})$ *with* $\mathbb{Q}(\mathfrak{p}') \ne \mathbb{Q}(\mathfrak{p})\}$ *is dense. For* $n = 5$*, even* $\{\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}(\mathbb{Q})$ *with* $\mathbb{Q}(\mathfrak{p}') \ne \mathbb{Q}(\mathfrak{p})\}$ *is dense.*

Proof. This example compares the group theoretic Hurwitz space ideas, with explicit equation calculation. Hurwitz space computations are explicit group theory computations. It's more than a matter of taste, for we are after *properties* of the spaces, not their equations. Other examples of this are in [Fr3] and [Fr4]. The remaining proof has four parts, starting from statements relating inner Hurwitz spaces to absolute Hurwitz spaces. This lets us focus on the effect of Mestre's calculation for n odd, distinguishing this from the more mysterious case when n is even. Note: If $\mathbb{Q}(\mathfrak{p}') \ne \mathbb{Q}(\mathfrak{p})$ (notation as in (3.2c)), then the Galois closure of $\phi_{\mathfrak{p}} : X \to \mathbb{P}^1_x$ in (3.2b) has group S_n (see below).

Part 1: Absolute Nielsen classes. For $k = 0$, a special case of [Fr1] shows there is one B_{n-1} orbit on $\mathrm{Ni}(A_n, \mathbf{C}_{3^{n-1}})$. Another Hurwitz space is handy for this problem. It is closest to Mestre's computations [Me] below.

For any $G \le S_n$, consider the normalizer $N_{S_n}(G)$ of G in S_n. Let $N(\mathbf{C}) = N_{S_n}(G,\mathbf{C})$ be the subgroup of $N_{S_n}(G)$ whose elements conjugate the entries of $\mathbf{C}$ among themselves. We also use $G(1)$, the stabilizer of 1 in this degree n representation. Form the natural quotient $\mathrm{Ni}(G,\mathbf{C})/N(\mathbf{C}) = \mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$. Then, B_{n-1}, and its Hurwitz monodromy group $H_{n-1} = \pi_1(\mathbb{P}^{n-1} \setminus D_{n-1})$ quotient, act on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$. Covering space theory produces a sequence of unramified covers

$$(3.3) \qquad \mathcal{H}(G,\mathbf{C}) = \mathcal{H}(G,\mathbf{C})^{in} \to \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}} \to \mathbb{P}^{n-1} \setminus D_{n-1}.$$

As in [Fr2], [FrV] and [V], interpret $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$ as a moduli space of equivalence classes of degree n covers. For $\mathfrak{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$, let $\phi_{\mathfrak{p}} : X_{\mathfrak{p}} \to \mathbb{P}^1_x$ be a representing cover. Cover equivalence here is (II.1a) (in App.II). This cover has the following properties.

(3.4a) The Galois closure $\hat{X} \to \mathbb{P}^1_x$ of $\phi_{\mathfrak{p}}$ represents $\mathfrak{p}' \in \mathcal{H}(G,\mathbf{C})^{in}$ over $\mathfrak{p}$.

(3.4b) X is the quotient of $\hat{X}$ by $G(1)$.

Suppose $\mathcal{H}^{in}_*$ is a connected component of $\mathcal{H}^{in}$ and $\mathcal{H}^{\mathrm{abs}}_*$ is the image of $\mathcal{H}^{in}_*$ in $\mathcal{H}^{\mathrm{abs}}$. Then, $\mathcal{H}^{in}_*$ corresponds to an orbit O^{in}_1 of B_r on $\mathrm{Ni}(G,\mathbf{C})$. The natural image O^{abs}_1 of O^{in}_1 in $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ corresponds to $\mathcal{H}^{\mathrm{abs}}_*$. The following set is actually a group:

$$\mathcal{G}(\mathbf{C}) = \{h \in N(\mathbf{C}) \mid \exists\ Q \in B_{n-1} \text{ and } \mathfrak{g} \in O^{in}_1 \text{ with } (\mathfrak{g})Q = h\mathfrak{g}h^{-1}\}.$$

The cover $\mathcal{H}(G, \mathbf{C})^{in} \to \mathcal{H}(G, \mathbf{C})^{\text{abs}}$ on the left of (3.3) is Galois with group $\mathcal{G}(\mathbf{C})/G$. Note: [MT, Lemma 3.3] says $G \le \mathcal{G}(\mathbf{C})$.

Part 2: Using $\mathcal{G}(\mathbf{C}_{3^{n-1}})/G \equiv \mathbb{Z}/2$. With $A_n \le S_n$ the standard representation of the alternating group, $N(\mathbf{C}) = S_n$. Thus, $\mathcal{G}(\mathbf{C})$ is a subgroup of $S_n/A_n = \mathbb{Z}/2$. Also, $\mathcal{H}(G, \mathbf{C})^{\text{abs}}$ is the moduli space of degree n covers with $n{-}1$ 3-cycles as branch cycles. From the Riemann-Hurwitz formula, this is a moduli space of genus 0 covers. Further, as in [Fr2], since the subgroup $G(1) = A_n(1)$ is self normalizing in A_n, $\mathcal{H}(G, \mathbf{C})^{\text{abs}}$ is a *fine* moduli space. In particular, $\mathfrak{p} \in \mathcal{H}(G, \mathbf{C})^{\text{abs}}(K)$ corresponds to a K cover $\phi_{\mathfrak{p}} : X_{\mathfrak{p}} \to \mathbb{P}^1_x$.

[Fr1] says B_{n-1} is transitive on $\text{Ni}(A_n, \mathbf{C}_{3^{n-1}})$. Thus, $\mathcal{G}(\mathbf{C}_{3^{n-1}}) = \mathcal{G} = \mathbb{Z}/2$. An example gives the sense of why this holds. Take $n = 5$. From the transitivity result, $\mathcal{G}/G = \mathbb{Z}/2$ if and only if there exists $\mathfrak{g} \in \text{Ni}(A_n, \mathbf{C}_{3^{n-1}})$ and $Q \in B_4$ with $(\mathfrak{g})Q = (4\,5)\mathfrak{g}(4\,5)$. Take

$$\mathfrak{g} = ((1\,2\,3), (1\,2\,3)^{-1}, (1\,4\,5), (1\,4\,5)^{-1}).$$

Here applying Q_3 (App.I) has the same affect on $\mathfrak{g}$ as conjugating by $(4\,5)$.

Apply Hilbert's irreducibility theorem to the sequence of covers in (3.3). This says a dense set of points $\mathfrak{x} \in \mathbb{P}^{n-1}(\mathbb{Q})$ have above them $\mathfrak{p}' \in \mathcal{H}(G, \mathbf{C})^{in}$ lying over $\mathfrak{p} \in \mathcal{H}(G, \mathbf{C})^{\text{abs}}$ for which $\mathbb{Q}(\mathfrak{p}') \ne \mathbb{Q}(\mathfrak{p})$. Excluding the statement about $\mathbb{Q}$ points, this completes the proof.

Part 3: Interpreting Mestre's calculation. Continue the discussion at the beginning of Part 2. Here is the first place where there is a distinction between n even and odd. If $\phi_{\mathfrak{p}}$ has odd degree, then $X_{\mathfrak{p}}$ has a rational point over $\mathbb{Q}(\mathfrak{p})$. In particular, $\phi_{\mathfrak{p}}$ is $\mathbb{Q}(\mathfrak{p})$ equivalent (in the sense of (II.1a) in App.II) to a cover $\mathbb{P}^1_y \to \mathbb{P}^1_x$. [DFr1, p. 115] and [DFr2, p. 115] discuss whether this means a space like $\mathcal{H}^{\text{abs}}_{n,n-1}$ is a *family of rational functions*. That would mean, there is a natural map $\Psi^{\text{abs}} : \mathcal{H}^{\text{abs}}_{n,n-1} \times \mathbb{P}^1_y \to \mathcal{H}^{\text{abs}}_{n,n-1} \times \mathbb{P}^1_x$. Also, for any $\mathfrak{p} \in \mathcal{H}^{\text{abs}}_{n,n-1}$, $\Psi_{\mathfrak{p}}$ is a rational function cover representing $\mathfrak{p}$. We don't think there is such a map Ψ^{abs}, though we haven't excluded it.

Still, as in [DFr1, 2], if you add the branch points of the cover to the moduli space, you nearly have coordinates for a family of rational functions. When n is odd that is exactly what [Me] does. In fact, he gives a dense set of rational points in $\mathcal{H}^{in}_{n,n-1}$. Here is how it goes [Se, p. 100–101].

Let $P(y) = \prod_{i=1}^{n}(y - a_i)$ with the a_i algebraically independent indeterminants over $\mathbb{Q}$. If $Q(y)$ is a polynomial of degree $n{-}1$, then Q/P maps ∞ to 0. We look to choose those polynomials Q so the derivative of $Q(y)/P(y)$ is a square $(R(y)/P(y))^2$. If Q and R are suitably generic, that means the cover from Q/P has 3-cycles as branch cycles. It is then in the Nielsen class of our interest. Here are the expressions for Q and R:

$$(3.5\text{a}) \qquad Q(y)/P(y) = \sum_{i=1}^{n} -c_i^2/(y-a_i), \qquad R/P = \sum_{i=1}^{n} c_i/(y-a_i)$$

where the c_i s satisfy

$$(3.5\text{b}) \qquad \sum_{\substack{j=1\\ j\neq i}} c_j/(a_i-a_j) = 0 \text{ for all } i.$$

This is the second place using n odd. The matrix with $i\times j$ entry $1/(a_i-a_j)$ for $i\neq j$ and 0 for $i=j$ is skew-symmetric and $n\times n$. Thus, for n odd its determinant is 0. So, there is a line of solutions for the vector of c_i s.

[Fr1] says $\mathcal{H}(A_n,\mathbf{C}_{3^{n-1}})^{in}$ is an absolutely irreducible $\mathbb{Q}$ variety. So, Mestre's collection of rational functions shows $\mathcal{H}^{\text{abs}}$ is a unirational variety ([Me] when n is odd; [Se, p. 100-101] asserts a variant works for even n, too). So it gives a $\mathbb{Q}$ dense subset of $\mathcal{H}^{\text{abs}}$. These points are the image of $\mathbb{Q}$ points of $\mathcal{H}^{in}$. This is a dense set of $\mathfrak{p}\in\mathcal{H}(G,\mathbf{C})^{\text{abs}}(\mathbb{Q})$ for which $\mathbb{Q}(\mathfrak{p}')=\mathbb{Q}(\mathfrak{p})$. When $n=5$, [Fr5, Thm. 5.9] shows there is a dense set of $\mathfrak{p}\in\mathcal{H}(G,\mathbf{C})^{\text{abs}}(\mathbb{Q})$ for which $\mathbb{Q}(\mathfrak{p}')\neq\mathbb{Q}(\mathfrak{p})$.

Part 4: For n even, $\mathcal{H}(A_n,\mathbf{C}_{3^{n-1}})$ is obstructed. There is nothing in the Nielsen class $\text{Ni}(\frac{1}{2}\tilde{A}_n,\mathbf{C}_{3^{n-1}})$ when n is even. It goes like this. Let $\hat{A}_n$ be the universal central exponent 2 extension of A_n. Then, $\frac{1}{2}\tilde{A}_n\to A_n$ factors through $\hat{A}_n\to A_n$. Suppose $\frac{1}{2}\tilde{\mathfrak{g}}\in\text{Ni}(\frac{1}{2}\tilde{A}_n,\mathbf{C})$. The canonical map $\frac{1}{2}\tilde{A}_n\to\hat{A}_n$ sends $\frac{1}{2}\tilde{\mathfrak{g}}$ to $\hat{\mathfrak{g}}\in\hat{A}_n^r$ with $\Pi(\hat{\mathfrak{g}})=1$. Let $\mathfrak{g}$ be the image of $\hat{\mathfrak{g}}$ in $\text{Ni}(A_n,\mathbf{C}_{3^{n-1}})$. Again use transitivity of B_{n-1} on $\text{Ni}(A_n,\mathbf{C}_{3^{n-1}})$. So, if one element of $\text{Ni}(A_n,\mathbf{C}_{3^{n-1}})$ lifts to an element of $\text{Ni}(\hat{A}_n,\mathbf{C}_{3^{n-1}})$, then any element does. On the other hand, [MT, Ex. III.12] explicitly gives $\mathfrak{g}\in\text{Ni}(A_n,\mathbf{C}_{3^{n-1}})$ with no lift to $\text{Ni}(\hat{A}_n,\mathbf{C}_{3^{n-1}})$. Thus, level one of the Modular Tower for $(A_n,\mathbf{C}_{3^{n-1}})$ is an empty variety. □

§**3.B. Invariants for obstructed components.** Obstructed components and pure group theory establish Modular Tower Conjecture 1.4 for $(A_n,\mathbf{C}_{3^r})$ with even $n\geq 6$ and $r=n-1$. [Fr1], however, shows a different outcome for the cases (n,r), $r\geq n$ that Theorem 3.1 doesn't cover. There are unobstructed components in all levels of the Modular Tower.

Lemma 3.2 is a completely general result applying to all levels of any Modular Tower. As in §0.A, with $\mathfrak{g}=(g_1,\dots,g_r)\in G^r$ denote the product $g_1\cdots g_r$ by $\Pi(\mathfrak{g})$. Let G be a finite group. Suppose $\phi: H\to G$ is a central extension. Then, any $g\in G$ of order prime to $|\ker(\phi)|$, has a *unique* lift $\hat{g}$ to an element of H of the same order as G. Assume $\ker(\phi)$ has order prime to the orders of all entries of $\mathfrak{g} = (g_1, \dots, g_r) \in G^r$. For $\Pi(\mathfrak{g}) = 1$ let $s(\mathfrak{g})$ be $\Pi(\hat{g}_1 \cdots \hat{g}_r)$. In Lemma 3.2, the exact sequence has $\mathbf{1}$ as kernel. Here $\mathbf{1}$ is the identity module for the action of ${}_p^k\tilde{G}$.

Obstruction Lemma 3.2. *Suppose O is a B_r orbit in $\mathfrak{g} \in \mathrm{Ni}({}_p^k\tilde{G}, \mathbf{C})$. Let*

$$S(O) = \{\Pi(\hat{\mathfrak{g}}) \mid \hat{\mathfrak{g}} \in {}_p^{k+1}\tilde{G},\ \hat{\mathfrak{g}} \in \mathbf{C} \text{ and } \hat{\mathfrak{g}} \bmod \ker_k = \mathfrak{g}\}.$$

This is a union of conjugacy classes in ${}_p^{k+1}\tilde{G}$. Then, $1 \notin S(O)$ exactly if there exists a sequence of covers

$${}_p^{k+1}\tilde{G} \to H_2 \to H_1 \to {}_p^k\tilde{G}$$

with the following properties.

(3.6a) *The kernel of $H_2 \to H_1$ is $\mathbf{1}$.*

(3.6b) *There exists $\mathfrak{g}^* \in \mathrm{Ni}(H_1, \mathbf{C})$, $\mathfrak{g}^* \bmod \ker_k = \mathfrak{g}$ and $s(\mathfrak{g}^*) \neq 0$.*

Suppose $\mathcal{H}_O$ is the level k component of $\mathcal{H}_k$ corresponding to O. The previous condition holds exactly when $\mathcal{H}_O$ is obstructed.

Proof. Use induction on the Loewy layers of $\ker_k / \ker_{k+1}$. Replace $\mathbf{1}$ in the kernel in $H_2 \to H_1$ by an irreducible module $A \neq \mathbf{1}$. Consider the set S' of $\Pi(\mathfrak{g}')$ as $\mathfrak{g}'$ runs over all allowable lifts of r-tuples $\mathfrak{g} \in H_2^r$ with $\Pi(\mathfrak{g}) = 1$. Then $S' = A$. Here is the argument, using that the set S' is a braid invariant set. That is, let $\tilde{\mathfrak{g}}^0$ be one lift. In the orbit, you can braid $\mathfrak{g}^0$ to something whose lift has the same product, but in the braid g_i^0 appears on the right side. Now form a lift replacing g_i^0 by $ag_i^0a^{-1} = g_i^0a^{g_i^0}a^{-1}$. So, this lift gives $\tilde{\mathfrak{g}}^0a^{g_i^0}a^{-1}$. You can do this for any i and any $a \in A$. If $A \neq \mathbf{1}$ is irreducible, the possible products of lifts gives $\tilde{\mathfrak{g}}^0a$ with $a \in A$ arbitrary. So, the corresponding Nielsen class is empty only if $A = \mathbf{1}$. □

Schur Multipliers Result 3.3. *Assume $n \geq 4$. For each $k \geq 0, {}_2^k\tilde{A}_n$ has a nontrivial Schur multiplier. Generally, suppose ${}_p^k\tilde{G}$ has a nontrivial Schur multiplier. That is, there is a sequence ${}_p^{k+1}\tilde{G} \to H_1 \to {}_p^k\tilde{G}$ with $\mathbf{1} \to H_1 \to {}_p^k\tilde{G}$ short exact as in Obstruction Lemma 3.2. Then, $[\ker_k, H_1]H_1^p$ generates a proper closed subgroup H_2 of $\ker_{k+1}$. Also, ${}_p^{k+1}\tilde{G}$ has trivial action on $M = \ker_{k+1} / H_2$, producing a nontrivial Schur multiplier for ${}_p^{k+1}\tilde{G}$.*

Proof. As is well-known [MT, §II.C], the exponent 2-part of the Schur multiplier of A_n ($n \geq 4$) is $\mathbb{Z}/2$. Thus, the statement on the alternating groups follows from the general inductive statement. Since $\ker_k$ is a pro-free group, H_2 is a proper subgroup of $\ker_{k+1}$. The action of ${}_p^{k+1}\tilde{G}$ on M is trivial if it is trivial on generators of M. One type of generator is v^p with $v \in \ker_k$. Conjugating v by $g \in {}_p^{k+1}\tilde{G}$ gives vh for some $h \in H_1$. Modulo

$H_1^p[\ker_k, H_1]$, set $h^p = 1$ for $h \in H_1$ and $vh = hv$ for $v \in \ker_k$ and $h \in H_1$. Thus, the following hold.

(3.7a) $gv^pg^{-1} = (vh)^p = v^p \bmod H_1^p[\ker_k, H_1]$.

(3.7b) $g[v, v']g^{-1} = [vh, v'h'] = [v, v'] \bmod H_1^p[\ker_k, H_1]$. □

§4. When $p|N_{\mathbf{C}}$.

Let G be a finite group and let $\mathbf{C}$ be a collection of conjugacy classes in G. Theorem 4.4 assumes Modular Tower Conjecture 1.4 in the form (1.2a) holds. From this it concludes Conjecture 1.4 is true. The core of the proof starts by assuming $\mathbf{C}$ contains at least one conjugacy class that isn't p-regular. It then shows, for k large, lifts of $\mathbf{C}$ to conjugacy classes in ${}_p^k\tilde{G}$ can't be a rational union. The gist of this is it suffices to establish our major conjectures when $(p, N_{\mathbf{C}}) = 1$.

§4.A. Lifting elements of order p.

Continue notation from §2.A: $\phi = \phi_G : {}_p\tilde{G} \to G$ is the canonical map having kernel $\ker_0(G, p) = \ker_0(G)$.

Lifting Lemma 4.1. *The following are equivalent.*

(4.1a) $\mathbf{C}$ *consists of p-regular conjugacy classes.*

(4.1b) *For each $k \geq 1$, classes from $\mathbf{C}$ lift uniquely to classes ${}_p^k\tilde{\mathbf{C}}$ of the same order in ${}_p^k\tilde{G}$.*

(4.1c) (4.1b) *holds for $k = 1$.*

Further, let $\mathfrak{g}$ any set of generators of G, with each having order prime to p. Let $\alpha : H \to G$ be a cover of G with p-group as kernel. Then, α is a Frattini cover if and only if lifts of $\mathfrak{g}$ to elements $\tilde{\mathfrak{g}}$ of the same order in H implies $\langle\tilde{\mathfrak{g}}\rangle = H$.

Proof. Let g be in a conjugacy class from $\mathbf{C}$. Apply Schur-Zassenhaus [MT, Intro. to Part III] to the sequence

$$\ker_0(G, p) \to \phi^{-1}(\langle g\rangle) \to \langle g\rangle.$$

This shows (4.1a) implies (4.1b).

For the converse, assume p divides the order of g. Suppose g lifts to ${}^k\tilde{g} \in {}_p^k\tilde{G}$ of the same order, for each k. Then, so does g^a with a the order of g divided by p. The result follows if we show lifts of g to higher characteristic quotients must increase their order when g has order exactly p. A p-Sylow $\tilde{P}_G$ of ${}_p\tilde{G}$ is a pro-free p-group. The projective limit $\lim_{\infty \leftarrow k} {}^k\tilde{g}$ is an element of order p in the pro-free group $\tilde{P}_G$. Nontrivial projective profinite groups have no elements of finite order [FrJ, Cor. 20.14]. So, this is impossible.

Equivalence of (4.1a) and (4.1b) with (4.1c) follows by showing g, of order p, lifts to no element of order p in ${}_p^1\tilde{G}$. Assume $P = P_G$ is a p-Sylow of G containing g. Let $\tilde{F}_P$ be the pro-free p-group of the same rank as P. Choose a surjective map $\alpha : \tilde{F}_P \to P$. Then, $\tilde{F}_P$ is the universal p-Frattini cover of P [FrJ, Chap. 20]. Denote its kernel by $\ker_0(P)$. As $\tilde{P}_G$ is also free and covers P, there is a surjective homomorphism $\psi : \tilde{P}_G \to \tilde{F}_P$ commuting with the respective maps ϕ and α of $\tilde{P}_G$ and $\tilde{F}_P$ to P. Hypothesis (4.1c) says g lifts to g' of order p in $\tilde{P}_G/\langle[\ker_0(G), \ker_0(G)]\ker_0(G)^p\rangle$.

Since $\ker_0(G)$ maps surjectively to $\ker_0(P)$, $\ker_0(G)^p$ maps onto $\ker_0(P)^p$ and $[\ker_0(G), \ker_0(G)]$ maps onto $[\ker_0(P), \ker_0(P)]$. Thus, $\ker_0(G)/\ker_1(G)$ maps surjectively to $\ker_0(P)/\ker_1(P)$. The image of g' in $\ker_0(P)/\ker_1(P)$ has order p and it is also a lift of g. Thus, a lift of g to something of order p in ${}_p^1\tilde{G}$ implies a lift of it has order p in $\ker_0(P)/\ker_1(P)$. Assume $g' \in \tilde{F}_P/\ker_1(P)$ of order p maps to g. Here, apply a similar argument. Consider the pullback $\alpha^{-1}(\langle g\rangle)$ of $\langle g\rangle$ in $\tilde{F}_P$. This must map surjectively to $\mathbb{Z}_p$, the universal p-Frattini cover of $\langle g\rangle$. Therefore, an element of order p in $\mathbb{Z}/p^2$ would map to the generator of $\mathbb{Z}/p$. This contradiction concludes the first part of the lemma.

Now consider the last condition in the lemma. If $H \to G$ is a Frattini cover the condition holds by definition. Suppose, however, it holds and $H \to G$ is not a Frattini cover. Then, a proper subgroup H_1 of H maps surjectively to G. Apply Schur-Zassenhaus to H_1. This lifts the entries of $\mathfrak{g}$ to elements $\mathfrak{g}_1$ of H_1 of the same respective orders. By hypothesis, $H_1 \ge \langle\mathfrak{g}_1\rangle = H$. This contradicts H_1 being a proper subgroup of H. □

§**4.B. Irrational characters.** Consider the universal p-Frattini cover of G. For $g \in G$ let $\tilde{g} \in {}_p\tilde{G}$ be a lift of g. The p'-order of g is the prime to p part of the order of g. This subsection discusses the values of the irreducible characters of ${}_p^k\tilde{G}$ on the image ${}^k\tilde{g}$ of $\tilde{g}$ in ${}_p^k\tilde{G}$. The p'-order of $\tilde{g}$ equals that of g. A relevant example might have $A_n = G$, $n \ge 5$, $p = 3$, and the conjugacy classes those of 3-cycles. Then, given a 3-cycle, choose lifts to 3-power orders in ${}_3^k\tilde{A}_n$.

Lift Question 4.2. The values of all irreducible G characters at g generate a field $\mathbb{Q}_g$. Similarly, let $\mathbb{Q}_{\tilde{g}}$ be the direct limit of the fields generated by the values of ${}^k\tilde{g}$ at irreducible characters of ${}_p^k\tilde{G}$. Suppose G is perfect and p divides the (supernatural) order of ${}^k g$. Is it possible that $\mathbb{Q}_g = \mathbb{Q}_{\tilde{g}}$?

If yes, it could be all characteristic ${}_p\tilde{G}$ quotients are groups of regular Galois extensions of $\mathbb{Q}(x)$ having a bounded number of branch points, yet infinite inertia groups. The answer, however, is “No!” Call $\tilde{g} \in {}_p\tilde{G}$ rational if its image in ${}_p^k\tilde{G}$ defines a rational conjugacy class for each $k \ge 0$.

Lemma 4.3. *If the order of g is prime to p, then $\mathbb{Q}_g = \mathbb{Q}_{\tilde g}$. Now suppose g (of any order) defines a rational conjugacy class in G. Then, Lift Question 4.2 has a yes answer if and only if there is a rational lift $\tilde g \in {}_p\tilde G$ of g.*

Proof. Suppose g and $\tilde g$ have p'-order. Then, characters of ${}^k_p\tilde G$ restricted to $\langle \tilde g\rangle$, give sums of characters of the cyclic group $\langle g\rangle$. Thus, $\mathbb{Q}_{{}^k\tilde g} = \mathbb{Q}_g$ for each $k \ge 0$.

Assume g defines a rational conjugacy class in G. Suppose $\tilde g$ is a lift of g with $\mathbb{Q} = \mathbb{Q}_{\tilde g}$. This means ${}^k\tilde g$ has a rational value in each irreducible representation of ${}^k_p\tilde G$. Assume u is prime to the order of ${}^k\tilde g$. Then, ${}^k\tilde g^u$ also takes the same values under each irreducible representation of ${}_p\tilde G$. Values of a conjugacy class on irreducible characters determine the conjugacy class. Thus, ${}^k\tilde g^u$ is conjugate to ${}^k\tilde g$ in ${}^k_p\tilde G$, so ${}^k\tilde g$ determines a rational conjugacy class in ${}^k_p\tilde G$. □

§4.C. Conjecture 1.4 reduces to Modular Tower property (1.2a).

Now consider g having order a power of p. Let ${}^k_p\tilde P$ be the p-Sylow of ${}^k_p\tilde G$. The zeroth characteristic quotient is G; denote ${}^0_p\tilde P$ by $P = P_p$. Lemma 4.1 shows any lift of g to ${}^1_p\tilde P$ has larger order than does g.

Theorem 4.4. *Only p' elements of ${}_p\tilde G$ can be rational. In particular, let r_0 be any positive integer and let K be a number field. There is an integer $k_0 = k_0(r_0, K, G)$ with the following property. Suppose $k > k_0$ and there is a K regular realization of ${}^k_p\tilde G$. Then, one of the following holds:*

(4.2a) *there is a regular realization corresponding to a point of $\mathcal{H}({}^{k_0}_p\tilde G, \mathbf{C})^{\mathrm{rd}}(K)$ for some $\mathbf{C}$ with at most r_0 entries from ${}_p\mathcal{C}(G)$; or*

(4.2b) *the regular realization has more than r_0 branch points.*

Proof. Suppose $g \in {}_p\tilde G$ is a rational element and g is not a p'-element. For any integer v, g^v is also a rational element of ${}_p\tilde G$. Let v be the order of the image of g in G. Then, from Lemma 4.1 as restated above, g^v is a nontrivial p-power element in $\ker_0$. Replace g by g^v. Find the minimal integer n with $g \in \ker_n \setminus \ker_{n+1}$. In particular, $g = g_1$ has nontrivial image in $\ker_n / \ker_{n+1}$. Since $\ker_n$ is a pro-free pro-p group, any collection of representatives of the nontrivial cosets of $\ker_n / \ker_{n+1}$ give topological generators of $\ker_n$. Compliment g_1 with elements $g_2, \dots, g_u$ that freely generate $\ker_n$. Now, we show g_1 is not a rational element of ${}_p\tilde G$.

For each p'-integer m, our rationality assumption says there is an $h_m \in {}_p\tilde G$ for which $g^m = h_m g h_m^{-1}$. Since ${}_p\tilde G / \ker_m$ is a finite group, there are infinitely many p'-powers g^m of g with corresponding h_m in $\ker_n$. Let m' be a nontrivial choice of such an integer.

This is our setup. Let $B = \langle g \rangle$ and $D = \langle g_2, \dots, g_u \rangle$. Then, the groups B and D freely generate $\ker_n$. Further, there exists $h_{m'} \in \ker_n$ with $h_{m'} B h_{m'}^{-1} = B$. Now apply [HR]. This says, for each $h' \in \ker_n$, either $h' \in B$ (and $B^g = B$) or $h' B (h')^{-1} \cap B = 1$. Taking $h' = h_{m'}$ violates both these conclusions. Therefore, g is not a rational element.

To finish the proof, consider the conclusion on regular realizations. Suppose ${}^k_p\mathbf{C}$ is any set of r conjugacy classes (not necessarily p-regular) of ${}^k_p\tilde{G}$. A K regular $({}^k_p\tilde{G}, {}^k_p\mathbf{C})$ realization corresponds to a point of $\mathcal{H}({}^k_p\tilde{G}, {}^k_p\mathbf{C})^{\mathrm{rd}}(K)$ (end of App.I). Further, this produces a K regular $({}^j_p\tilde{G}, {}^j_p\mathbf{C})$ realization with ${}^j_p\mathbf{C}$ the conjugacy class image of ${}^k_p\mathbf{C}$ in ${}^j_p\tilde{G}$, $0 \le j \le k$. There are only finitely many choices of p-regular conjugacy classes $\mathbf{C}$ with at most r_0 entries. So, if (4.2a) holds for each k, there exists some $\mathbf{C}$ (independent of k) consisting of p-regular classes. Suppose there are ${}^k_p\tilde{G}$ realizations for every k with at most r_0 branch points, and (4.2a) does not hold with $k \ge k_0'$. Then, for large k, the following hold.

(4.3a) There exists ${}^k_p\mathbf{C} = ({}^k\mathrm{C}_1, \dots, {}^k\mathrm{C}_r)$ and a point of $\mathcal{H}({}^k_p\tilde{G}, {}^k_p\mathbf{C})^{\mathrm{rd}}(K)$ giving a ${}^k_p\tilde{G}$ realization with $r \le r_0$ branch points.

(4.3b) At least one entry of ${}^k_p\mathbf{C} \bmod \ker_{k_0'}$ is not p-regular.

Reorder the entries of ${}^k_p\mathbf{C}$ to assume C_1 is not p-regular. The branch cycle argument (§1.A) says ${}^k_p\mathbf{C}$ must be a K-rational union. Let $g \in \mathrm{C}_1$. This puts a bound of r_0 on $\mathcal{G}_k = \{g^n \mid (n, N_{{}^k_p\mathbf{C}}) = 1\}/{}^k_p\tilde{G}$. For suitably large k, this contradicts the first part of the proof. □

Remark 4.5. *Effective k_0 in Theorem 4.4.* The proof of Theorem 4.4 assumes existence of k_0' with no p-regular realizations of ${}^k_p\tilde{G}$ for $k > k_0'$. Assuming an explicit such k_0', it is possible to produce an explicit k_0. The proof above returns this to the following. Let $a \in {}_p\tilde{F}_u$ have nontrivial image in the first Frattini quotient of ${}_p\tilde{F}_u$. Then, we must give an explicit lower bound c_k on the number of prime to p powers of a in ${}_p\tilde{F}_u/\ker_k$ conjugate to a, where $\lim_{k \mapsto \infty} c_k \mapsto \infty$. The argument of [HR] can give such a bound.

§App.I. Nielsen classes and Modular Towers.

This is a quick review of fundamental definitions from [MT]. Excluding Theorem 3.1, Hurwitz spaces in this paper are the $\mathcal{H}(G, \mathbf{C})^{in}$ inner spaces of [FrV] and [MT]. These parametrize Galois covers $X \to \mathbb{P}^1_x$ whose branch cycles fall in the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ and have a fixed isomorphism of the automorphism group of $X \to \mathbb{P}^1_x$ with G. Let ${}^k_p\tilde{\mathbf{C}}$ be any conjugacy classes in ${}^k_p\tilde{G}$—not necessarily p-regular classes as in §0.B—mapping to $\mathbf{C}$ by the canonical quotient with $\ker_0$.

Suppose $\mathfrak{g} \in \mathbf{C}$ with $\langle \mathfrak{g} \rangle = G$ lifts to $\tilde{\mathfrak{g}} \in {}_p^k\mathbf{C}$. The Frattini covering property means $\langle \tilde{\mathfrak{g}} \rangle = {}_p^k\tilde{G}$ is automatic. So, after the first level, $\Pi(\tilde{\mathfrak{g}}) = 1$ is the significant formula for defining the Nielsen class (§0.A). Specifically:

$$\mathrm{Ni}({}_p^k\tilde{G}, {}_p^k\tilde{\mathbf{C}}) = \{\tilde{\mathfrak{g}} \in {}_p^k\tilde{\mathbf{C}} \mid \tilde{\mathfrak{g}} \bmod \ker_0 \in \mathrm{Ni}(G, \mathbf{C}) \text{ and } \Pi(\tilde{\mathfrak{g}}) = 1\}$$

is the kth level Nielsen class.

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

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

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

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

Conditions (I.1a) and (I.1b) define the *Artin braid group* B_r. Add (I.1c) to get the *Hurwitz monodromy group* H_r of degree r, a quotient of B_r. The Q_i s in B_r act on $\mathfrak{g} \in \mathrm{Ni}(G, \mathbf{C})$:

(I.1d) $$(\mathfrak{g})Q_i = (g_1, \dots, g_{i-1}, g_ig_{i+1}g_i^{-1}, g_i, g_{i+2}, \dots, g_r),\ i = 1, \dots, r-1.$$

Mod out by inner automorphisms of G to induce an action by H_r. Irreducible components of $\mathcal{H}(G, \mathbf{C})$ correspond to orbits of this action.

Braid group action on $\mathrm{Ni}({}_p^k\tilde{G}, {}_p^k\tilde{\mathbf{C}})$ extends that on the level 0 Nielsen class. This produces the corresponding sequence of moduli spaces

(I.2) $$\cdots \to \mathcal{H}({}_p^{k+1}\tilde{G}, {}_p^{k+1}\tilde{\mathbf{C}}) \to \mathcal{H}({}_p^k\tilde{G}, {}_p^k\tilde{\mathbf{C}}) \to \cdots \to \mathcal{H}(G, \mathbf{C}).$$

Suppose ${}_p^k\tilde{G}$ has no center for $k \ge 0$. ([FrK] shows this holds if G has no center and no $\mathbb{Z}/p$ quotient; in particular, if G is a centerless perfect group [MT, Lemma 3.6].) Let K be a field of characteristic prime to $|G|$. Then, as in [MT, Part III], a K point $\mathfrak{p} \in \mathcal{H}({}_p^k\tilde{G}, {}_p^k\tilde{\mathbf{C}})$ gives a sequence of K covers

(I.3) $${}^kX_{\mathfrak{p}} \to {}^{k-1}X_{\mathfrak{p}} \to \cdots \to {}^0X_{\mathfrak{p}} \to \mathbb{P}^1.$$

Further, ${}^jX_{\mathfrak{p}} \to \mathbb{P}^1$ gives a K regular $({}_p^j\tilde{G}, {}_p^j\tilde{\mathbf{C}})$ realization, $j = 0, \dots, k$. When $\mathbf{C} = {}_p^k\tilde{\mathbf{C}}$ consists of p-regular conjugacy classes, then (I.2) is what we call a *Modular Tower* as in §0.B.

§App.II. Equivalence of covers of the sphere

There are two natural equivalences of covers of the sphere.

(II.1a) $\phi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$, are equivalent if there exists $\alpha : X_1 \to X_2$ with $\phi_2 \circ \alpha = \phi_1$.

(II.1b) As in (II.1a), except there is $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ with $\phi_2 \circ \alpha = \beta \circ \phi_1$.

§App.II.A. Action of $\mathrm{SL}_2(\mathbb{C})$ **on** $\mathbb{P}^r \setminus D_r$**.** Below, $\mathcal{H} = \mathcal{H}(G, \mathbf{C})$ refers to a space of covers in a given Nielsen class up to equivalence (II.1a) .

The group S_r acts on the space $(\mathbb{P}^1)^r$ by permutation of its coordinates. This gives a natural map $\Psi_r : (\mathbb{P}^1)^r \to \mathbb{P}^r$. Consider $\mathfrak{x} = (x_1, \dots, x_r)$ with none of the coordinates equal ∞. The point whose coordinates are the coefficients of the polynomial $\prod_{i=1}^r (z - x_i)$ in z represents the image of $\mathfrak{x}$ under Ψ_r. (If $x_i = \infty$, replace the factor $z - x_i$ by 1.) Also, Ψ_r takes the fat diagonal Δ_r to D_r. This interprets $U^r = \mathbb{P}^r \setminus D_r$ as the space of r distinct unordered points in $\mathbb{P}^1$. Thus, $\Psi_r : U^r \to U_r$ is an unramified Galois cover with group S_r.

Consider $\mathrm{PSL}_2(\mathbb{C})$ as linear fractional transformations acting diagonally on the r copies of $\mathbb{P}^1_x$. For $\alpha \in \mathrm{PSL}_2(\mathbb{C})$ and $\mathfrak{x} \in U^r$, $\mathfrak{x} \mapsto (\alpha(x_1), \dots, \alpha(x_r))$. The action of $\mathrm{PSL}_2(\mathbb{C})$ is on the left, commuting with the coordinate permutation action of S_r. The quotient $\mathrm{PSL}_2(\mathbb{C}) \setminus U^r = \Lambda_r$ generalizes the λ line minus the points $0, 1, \infty$. Further, $\mathrm{PSL}_2(\mathbb{C}) \setminus U_r = J_r$ generalizes the j line minus the point at ∞ from the theory of modular curves. It has complex dimension $r - 3$. The case $r = 4$ is crucial to us, so we reassure the reader by displaying these identifications.

Given $\mathfrak{x} = \{x_1, x_2, x_3, x_4\}$ up to equivalence (II.1a) there is a unique degree 2 cover $X_{\mathfrak{x}} \to \mathbb{P}^1$ ramified exactly at $\mathfrak{x}$. Thus, X is a genus 1 curve; its j invariant determines its isomorphism class. Further, $X_{\mathfrak{x}}$ is equivalent to $X_{\mathfrak{x}'}$ if and only if there exists $\alpha \in \mathrm{PSL}_2(\mathbb{C})$ with $\alpha(\mathfrak{x}) = \mathfrak{x}'$. This identifies J_4 and the j line minus ∞. The natural λ line (ramified) cover of the j line is Galois with group S_3 [R, I.59]. Don't confuse this copy of S_3 with an S_3 inside the coordinate permutation action of S_4.

§App.II.B. Extending $\mathrm{PSL}_2(\mathbb{C})$ **action to** $\mathcal{H}(G, \mathbf{C})$**.** Suppose $\mathfrak{p} \in \mathcal{H}$ has a representative cover $\phi_{\mathfrak{p}} : X_{\mathfrak{p}} \to \mathbb{P}^1$. Extend the action of $\alpha \in \mathrm{PSL}_2(\mathbb{C})$ by composing $\phi_{\mathfrak{p}}$ with α to give $\alpha \circ \phi_{\mathfrak{p}} : X_{\mathfrak{p}} \to \mathbb{P}^1$, a new G cover in the Nielsen class. Thus, $\mathrm{PSL}_2(\mathbb{C})$ action extends to $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})$; denote its quotient by $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$. Since $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})$ is an affine algebraic set, so is $\mathcal{H}({}_p^k\tilde{G}, \mathbf{C})^{\mathrm{rd}}$ [MFo, Thm. 1.1]. These reduced spaces generalize the spaces of modular curves $Y_1(p^{k+1})$ [MT, Intro.].

So, the spaces $\mathcal{H}^{\mathrm{rd}}$ are moduli spaces for covers up to equivalence (II.1b): *reduced* Hurwitz spaces. Many have asked: "Which equivalence is more important?" My answer: Classical geometers often like equivalence (II.1b). (Also, it is usual to use the pulback of $\mathcal{H}^{\mathrm{rd}}$ over Λ_r. When, however, there are repetitions in the conjugacy classes $\mathbf{C}$, this pullback is inappropriate, often wiping out the significant arithmetic information.) Their justification is the complex dimension of $\mathcal{H}^{\mathrm{rd}}$ is 3 less than that of $\mathcal{H}$.

We like that, too. For example, the reduced spaces are curves when $r = 4$, allowing use of Falting's Theorem. Further, any rational point on $\mathcal{H}$ automatically produces infinitely many others in its $\mathrm{PSL}_2(\mathbb{Q})$ orbit. Allowing this would defy the finiteness results this paper conjectures. Still, it is equivalence (II.1a) that supports the Modular Tower construction. From that construction we compatibly reduce all levels of the tower by the $\mathrm{PSL}_2(\mathbb{C})$ action. Conclusion: We require both equivalences for Modular Towers.

References

[Be] D. J. Benson, *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras*, Cambridge studies in Advanced Mathematics **30**, Camb. Univ. Press, 1991.

[Be2] D. J. Benson, The Loewy structures for the projective indecomposable modules for A_8 and A_9 in characteristic 2, *Comm. in Alg.* **11** (1983), 1395–1451.

[DFr1] P. Debes and M. Fried, Arithmetic variation of fibers in families: Hurwitz monodromy criteria for rational points, *J. Crelle* **409** (1990), 106–137.

[DFr2] P. Debes and M. Fried, Integral specialization of rational function families, preprint. Jan. 1997, 20 pgs.

[Fa] G. Faltings, Diophantine approximation on abelian varieties *Annals of Math.* **133** (1991), 549–576

[Fr1] M. Fried, Alternating groups and lifting invariants, Preprint as of 07/01/96.

[Fr2] M. Fried, Fields of Definition of Function Fields and Hurwitz Families and Groups as Galois Groups, *Comm. in Algebra* **5** (1977), 17–82.

[Fr3] M. Fried, Enhanced review of J.-P. Serre's Topics in Galois Theory, with examples illustrating braid ridigity, Proceedings AMS-NSF, Summer Conference Cont. Math series **186**, *Recent Developments in the Inverse Galois Problem* (1995), 15–32.

[Fr4] M. Fried, Global construction of general exceptional Covers: with motivation for applications to encoding Applications and Algorithms, *Cont. Math.* **168**, G.L. Mullen and P.J. Shiue, editors, 1994, 69–100.

[Fr5] M. Fried, Arithmetic of 3 and 4 branch point covers: a bridge provided by noncongruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, in *Progress in Mathematics* **81**, Birkhauser, 1990, 77–117.

[FrJ] M. Fried and M. Jarden, *Field Arithmetic*, Ergebnisse der Mathematik III, **11**, Springer Verlag, Heidelberg, 1986.

[FrK] M. Fried and Y. Kopeliovich, A_5 Modular Towers, 30 page preprint, 1996.

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

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

[HR] W. Herfort and L. Ribes, Torsion elements and centralizers in free products of profinite groups, *J. Crelle* **358** (1985), 155-161.

[Me] J-F. Mestre, Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$, *J. Alg.* **131** (1990), 483-495.

[MFo] D. Mumford and J. Fogarty, Geometric Invariant Theory, *Ergeb. der Math. und ihrer Grenzgebiete* **34**, Springer Verlag, 2nd enlarged edition, 1982.

[Ri] L. Ribes, Frattini covers of profinite groups, *Archiv der Math.* **44** (1985), 390–396.

[R] A. Robert, *Elliptic curves*, Lecture Notes in Mathematics **326**, Springer-Verlag, Heidelberg-New York, 1973.

[Se] J.-P. Serre, *Topics in Galois Theory*, Bartlett and Jones Publishers, 1992.

[V] H. Völklein, *Groups as Galois Groups*, Cambridge Studies in Advanced Mathematics **53**, Cambridge Univ. Press, 1996.

University of California at Irvine, Irvine CA 92717
mfried@math.uci.edu