Contemporary Mathematics
Volume **00**, 0000

Introduction to MODULAR TOWERS:

Generalizing dihedral group–modular curve connections

MICHAEL D. FRIED

1991 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11R58; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.

Supported by NSF #DMS-99305590, RIMS Institute March 1994, Alexander von Humboldt Foundation during a stay at Erlangen Universität, Fall 1994.

Y. Ihara, M. Matsumoto and H. Nakamura listened to me justify the first presentation of these topics. W. Feit, R. Howe, J. G. Thompson and H. Voelklein helped me with modular representations. An unpublished 1987 preprint included construction of the universal exponent p-Frattini covers of A_5. J.-P. Serre gave an Ext interpretation to simplify my arguments to efficient use of Loewy displays of projective indecomposables (§II.B). R. Guralnick advised on many matters, including part of Ex. D.4 of §App.D. F. Leprévost produced dihedral group challenge problems, from which I developed the $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization lemma of §I.D. G. Malle suggested the $\mathrm{PSL}_2(q)$ example of exceptionally ramified primes in §III.E. D. Benson completed my argument the Center Hypothesis (Def. 3.5 and Lemma 3.6) holds for perfect groups. Lectures at Erlangen gave me confidence applications of modular towers to arithmetic and geometry could surmount their technicalities. My hosts, D. Geyer and G. Frey, were particularly enthusiastic on the mix of problems. They influenced the balance of group theory and arithmetic geometry in this introduction to modular towers. I apologize in advance to any group theorists who already knew how to explicitly produce the universal p-Frattini covers. P. Debes and M. Emsalem improved the paper with comments from a thorough reading.

Abstract. We join *Hurwitz space* constructions and the *universal Frattini cover* of a finite group. The goal is to form and apply generalizations of the towers $X_0(p) \leftarrow X_0(p^2) \cdots \leftarrow X_0(p^n) \leftarrow \cdots$ of modular curves. This generalization relies on the appearance of the dihedral group D_p and its companion group $\mathbb{Z}_p \times^s \{\pm 1\}$ in the theory of modular curves. We replace D_p by any finite group G, and p by any prime dividing the order of G. The replacement for $\mathbb{Z}_p \times^s \{\pm 1\}$ is the Universal p-Frattini Cover of G.

Diophantine motiviations include an outline for using the Ihara-Drinfeld relations for the *Grothendieck-Teichmüller group.* Conjecturally this is the absolute Galois group of $\mathbb{Q}$. We consider how finding fields of definition of absolutely irreducible components of Hurwitz spaces can test this. There are many applications to finite fields. The simplest bounds the exceptional primes to realizing any finite group G as the Galois group of a regular extension of $\mathbb{F}_p(x)$. The structure of Modular Towers connects this problem to other diophantine problems.

Alternating groups test the modular representation theory that appears in Part II of the paper. These give a modular tower different from modular curves. The classical link here is to theta functions with characteristic.

Summary. To each finite group G we can attach a projective profinite group, $\tilde{G}$: the *universal Frattini cover* of G [**FrJ**, §20.6] (§II.A-B). Further, for any collection of r conjugacy classes $\mathbf{C}$ of G, there is a natural moduli space. Its points are equivalence classes of covers of the Riemann sphere $\mathbb{P}^1$ ramified over r points. The particular covers have geometric monodromy group G; $\mathbf{C}$ is the set of conjugacy classes of branch cycles of the cover. We conjoin these two constructions. The moduli space construction applies to a natural cofinal collection of finite quotients of $\tilde{G}$. This produces arithmetic invariants for the theory of curve covers. A special case uses a prime p dividing $|G|$ and conjugacy classes $\mathbf{C}$ of orders relatively prime to p. This *p-unramified lifting invariant*, $\nu(G, p, \mathbf{C})$, is compatible with terminology of [**Se3**]. It also produces a tower of moduli spaces. We denote them formally as $(G, p, \mathbf{C})$-moduli spaces. Informally, these are a *modular tower*. This moduli space material is in Part III.

Arithmetic geometers know a special case: the tower of covers $X_0(p) \leftarrow X_0(p^2) \leftarrow X_0(p^3) \cdots$ of modular curves. Points on $X_0(p^n)$ correspond to pairs of elliptic curves with a cyclic p^n-power isogeny. Here G is the dihedral group D_p of order $2p$. Also, $r = 4$ and $\mathbf{C}$ is four repetitions of the involution conjugacy class in D_p [**DFr**, §5.1–5.2]. Part I (especially, §I.D) discusses example problems with ready applications for modular towers. These include highly structured versions of the inverse Galois problem and construction of *general exceptional covers*.

Part II discusses *universal Frattini covers* of a finite group. Each level of a modular tower comes from a quotient of a universal p-Frattini cover. Moduli space difficulties at a particular level will have a modular representation interpretation. For example, this holds for the appearance of a center in the quotient group for a particular level (see The Center Hypothesis of §III.B). We illustrate these matters with an application to A_n and 3-cycles. This is another classical connection: to theta functions with characteristics. Much we know of any modular tower comes from the lifting invariant. This lives in the p-part of the kernel $\tilde{G} \to G$. Part II shows it is possible to compute this invariant. The A_n examples (§III.C) show the lifting invariant detecting obstructed towers. Sometimes a component of a modular tower attached to $(G, p, \mathbf{C})$ has finite length. Modular curve towers have only one component and that has no obstruction.

Applications of $\nu(G, p, \mathbf{C})$ point to a test for the *Drinfeld-Grothendieck-Ihara relations on* $G_{\mathbb{Q}}$ [**I**]. Conjectures on the *Grothendieck Teichmüller group* imply it should detect fields of definition of components of these moduli spaces (when $r \geq 5$). Modular towers have suitable profinite aspects to make this test explicit. Ihara and Matsumoto [**IM**] have reproduced the appearance of $\widehat{\mathcal{G}T}$ making it applicable to Hurwitz spaces. Their construction produces a natural section to the map from the arithmetic fundamental group of projective r-space minus the discriminant locus. §App.C suggests a use for [**IM**] by modeling how to precisely find the field of definition of Hurwitz space components. It bases the model on a special case: How to decide if a component has field of definition $\mathbb{R}$. §App.D considers the compatible problem of finding *real points on modular towers*. §I.B summarizes Parts IV and V, to appear in the continuation paper. This includes a discussion of the $\widehat{\mathcal{G}T}$ action on modular towers.

Points over finite fields are a persistent diophantine subtopic. In particular, consider realizing a given group G as a regular extension of $\mathbb{F}_p(x)$. [**FrV**] notes there are only finitely many p exceptional for G. It, however, gives no bound on these. A more refined form, for realizations with branch cycles in a given *Nielsen class*, has many applications. In this form, §App.E gives an explicit upper bound on exceptional p. Such a realization, however, comes from one $\mathbb{F}_p$ point on an infinite collection of varieties over $\mathbb{F}_p$. We use the Lang-Weil bound. Yet, modular towers call for an analog of [**I2**] and later works. Lang-Weil can tell us little of the points on modular towers over a given finite field.

PART I. INTRODUCTION AND MOTIVATING PROBLEMS

This part motivates generalizing the connection between the inverse Galois problem and modular curves. §I.A explains what about modular curves we want to generalize. Later parts of the paper refer to this introduction to connecting dihedral groups to modular curves. §I.B tells the main contributions of the paper. §I.C gives notation for the theory of covers. Finally, §I.D and §I.E give diophantine motivation for the generalization of natural towers of modular curves we call *modular towers*. Previous results of the author applied modular curves to investigate cases of these topics. These fall under the heading $(G, \hat{G}, \mathbf{C})$ *realizations* by regular extensions $L/F(x)$. Usually, F is a number field or finite field. These include diophantine results about modular curves that haven't appeared in quite this form. Still, we mean §I.D and §I.E to show diophantine problems appropriate for modular towers. (Part V in the continuation of this paper goes further.) These sections emphasize the role of counting points on curves over finite fields. The influence for this came from papers of Y. Ihara, and a result of Frey. The latter used Faltings' proof of Lang's conjecture. He thereby gave an insight into simple finite field questions and points over number fields.

§I.F and §I.G present different views on the Galois closure process. Especially, the construction of §I.G gives a geometric view of automorphisms in the arithmetic theory of covers. Throughout, G_F is the absolute Galois group of a given field F. Unless otherwise said, all curves will be projective and nonsingular. Further, points on varieties means *geometric* points.

§I.A. Focus on modular curves. Part III has reminders of the properties of Hurwitz spaces. These join Part I motivations to Part II group theory to produce modular curve generalizations. The modular curve tower $X_0(p) \leftarrow X_0(p^2) \leftarrow X_0(p^3)\cdots$ (and $X_1(p) \leftarrow X_1(p^2) \leftarrow X_1(p^3)\cdots$) encodes collective information on ℓ-adic ($\ell = p$ here) representations of subgroups of $G_{\mathbb{Q}}$.

For example, suppose you have a projective sequence $\boldsymbol{p}_i \in X_1(p^i)$, $i = 1, \dots$: for each i, $\boldsymbol{p}_i$ maps to $\boldsymbol{p}_{i-1}$. When $i = 1$ this means $\boldsymbol{p}_1$ maps to the j-invariant $j(\boldsymbol{p}_1)$ of the common elliptic curve supporting these points (see §I.D). Suppose $j(\boldsymbol{p}_1)$ lies in a number field F. Then, G_F acts on the sequence $\{\boldsymbol{p}_i\}_{i=1,\dots}$. There is a standard interpretation. Let $\boldsymbol{x} = \{x_1, x_2, x_3, x_4\}$ be the four branch points of the elliptic curve $E_{\boldsymbol{x}}$ in Weierstrass normal over the x-line $\mathbb{P}^1 = \mathbb{P}^1_x$. (Weierstrass normal form takes x_4 to be ∞, lying under the origin for addition on $E_{\boldsymbol{x}}$. The main point is x_4 is rational over $\mathbb{Q}$. Eventually we allow any collection of four distinct points on $\mathbb{P}^1_x$.) Regard $\boldsymbol{p}_i \in X_1(p^i)$ as a pair $(E_{\boldsymbol{x}}, e_i)$ with e_i a point of order p^i (exactly) on $E_{\boldsymbol{x}}$. The map from $X_1(p^i) \to X_1(p^{i-1})$ derives from $e_i \mapsto pe_i$. The isogeny $E_{\boldsymbol{x}} \to E_{\boldsymbol{x}}/e_i$ has a *dual isogeny*: $E_{\boldsymbol{x}}/e_i \to E_{\boldsymbol{x}}$, Galois with group $\mathbb{Z}/p^i$. Such a cover comes from a homomorphism $\psi_i : \pi_1(E_{\boldsymbol{x}}) \to \mathbb{Z}/p^i$. Actually, it comes from an equivalence class of homomorphisms: The same cover derives from composing ψ_i with an automorphism of $\mathbb{Z}/p^i$. To normalize, choose from this equivalence class the homomorphism sending e_i to $1 \in \mathbb{Z}/p^i$.

To put all these covers together, identify integral homology with a lattice $L \cong \mathbb{Z}^2$ for the complex structure $\mathbb{C}/L$ on $E_{\boldsymbol{x}}$. The projective limit $\lim_{\infty\leftarrow i} L/p^iL$ equals $\lim_{\infty\leftarrow i} \frac{1}{p^i}L/L$. Therefore, it is the projective limit of p^i division points on $E_{\boldsymbol{x}}$. The system of points e_i, $i = 1, \dots$, forms a p-adic line $\mathcal{L}$ in the two dimensional p-adic space $L \otimes \mathbb{Z}_p$. Let $\hat\pi_1^{(p)}(E_{\boldsymbol{x}}) = V_p$ be the pro-p quotient of the algebraic fundamental group. The group G_F acts on $E_{\boldsymbol{x}}$ torsion points. Therefore, it acts through $\mathrm{GL}(V_p) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ on $\hat\pi_1^{(p)}(E_{\boldsymbol{x}})$.

A celebrated theorem of Serre implies the following [**Se5**]. If $E_{\boldsymbol{x}}$ is without complex multiplication, the image of G_F in $\mathrm{GL}(V_p)$ is an open subgroup. Further, for almost all primes p it is $\mathrm{GL}(V_p)$. So, for $[K : F] < \infty$, only finitely many p division points of $E_{\boldsymbol{x}}$ have field of definition K. For almost all primes p, none have. (This follows from [**Se5**] even if $E_{\boldsymbol{x}}$ has complex multiplication.)

Now we rephrase this discussion using the fundamental group of $\mathbb{P}^1 \setminus \boldsymbol{x}$. The projective system of unramified (Galois) covers of $E_{\boldsymbol{x}}$ comes from a quotient of the algebraic fundamental group $\hat{\pi}(\mathbb{P}^1 \setminus \boldsymbol{x})$. An explicit presentation of this quotient comes from Riemann's Existence Theorem (§1.F). Let $\sigma_1, \dots, \sigma_4$ freely generate $F_{\boldsymbol{\sigma}}$ subject to the identity

$$(*) \qquad \sigma_1\sigma_2\sigma_3\sigma_4 = 1.$$

Then, $\hat{\pi}(\mathbb{P}^1 \setminus \boldsymbol{x})$ is the profinite completion of all quotients of $\hat{F}_{\boldsymbol{\sigma}}$ by subgroups of finite index. Let $E' \to E_{\boldsymbol{x}}$ be any unramified cover. Compose this with the degree 2 cover $E_{\boldsymbol{x}} \to \mathbb{P}^1$ unramified outside of $\boldsymbol{x}$. Such covers correspond to representations of $\hat{F}_{\boldsymbol{\sigma}}$ that send $\sigma_1, \dots, \sigma_4$ into elements of order (exactly) 2. That is, the cover $E' \to \mathbb{P}^1$ ramifies of order 2 over each of the four branch points. Let $\hat{D}_{\boldsymbol{\sigma}}$ be the quotient of $\hat{F}_{\boldsymbol{\sigma}}$ by the relations

$$(**) \qquad \sigma_i^2 = 1, \ i = 1, 2, 3, 4 \text{ (so } \sigma_1\sigma_2 = \sigma_4\sigma_3).$$

Geometry shows $\hat{D}_{\boldsymbol{\sigma}}$ is $\hat{\mathbb{Z}}^2 \times^s \{\pm 1\}$, with $\hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$ with respect to all subgroups. Here is a combinatorial group theory argument. We show $\sigma_1\sigma_2$ and $\sigma_1\sigma_3$ are independent generators of $\hat{\mathbb{Z}}^2$. Then, σ_1 is a generator of $\{\pm 1\}$. First: $\sigma_1(\sigma_1\sigma_2)\sigma_1 = \sigma_2\sigma_1$ shows σ_1 conjugates $\sigma_1\sigma_2$ to its inverse. Also,

$$(\sigma_1\sigma_2)(\sigma_1\sigma_3) = (\sigma_1\sigma_3)\sigma_3(\sigma_2\sigma_1)\sigma_3 = (\sigma_1\sigma_3)(\sigma_1\sigma_2)$$

shows the said generators commute. The maximal pro-p quotient is $\mathbb{Z}_p^2 \times^s \{\pm 1\}$. Any line (pro-cyclic group) in $\mathbb{Z}_p^2$ produces a *dihedral group* D_{p^∞} from multiplication by -1 on this line.

The $\mathbb{P}^1$ cover approach has advantages. Suppose $\boldsymbol{x}$ is invariant as a set under G_F. Then, any degree 2 cover ramified at these four points is equivalent to a cover defined over F. Investigating covers of $\mathbb{P}^1$ ramified only over $\boldsymbol{x}$ includes realizing dihedral groups as Galois groups. To consider all realizations, we can't insist on a priori conditions on the branch points. This is especially true for showing realizations of certain type aren't possible (see §I.D). Also, this form allows us to replace dihedral groups by any finite group G.

Even a finite *simple* group G produces a tower of moduli spaces that encodes information on natural profinite representations of $G_{\mathbb{Q}}$. What is the analog of the dihedral group D_p acting on lines in a two dimensional p-adic space? Replacing the line is a free pro-p group mapping surjectively to a p-Sylow of G. The kernel, ker, of this map comes with a filtration from its association with G. Here, p is a prime dividing the order of G. There is a short exact sequence $\ker \to {}_p\tilde{G} \xrightarrow{\phi} G$ in place of $\mathbb{Z}_p \to D_{p^\infty} \to D_p$. Part II shows how to compute much about ${}_p\tilde{G}$. Such computations aren't yet trivial. Still, we illustrate our principles by displaying this group when $G = A_5$ and $p = 2, 3$ or 5 (Prop. 2.9 and Remark 2.10).

§I.B. Introduction. Modular towers (§III.C) generalize towers of modular curves. These moduli spaces encode information on a collection of *nilpotent* representations of subgroups of $G_{\mathbb{Q}}$. It is the *universal Frattini cover* $\tilde{G}$ of G that allows these constructions (§II.A). §II.B develops material for computing the kernel of the natural map $\tilde{G} \to G$. §II.C applies this in detail to A_5. Alternating groups also illustrate the lifting invariant $\nu(G, p, \mathbf{C})$ of §III.D. We note this example's relation to theta functions with characteristics and [**Se3,4**] and [**EKV**] in Remark 3.14. It illustrates properties that recommend it among our motivations, only second to modular curves.

The inductive process of §II.D evaluates successive *Frattini* quotients of ${}_p\tilde{G}$, the universal p-Frattini cover of G. §II.E produces the first nontrivial Frattini quotient of ${}_2\tilde{A}_5$. Finally, §II.F displays ${}_2\tilde{A}_5$. While the principles aren't the same, it may be no more (no less) difficult to compute in universal p-Frattini covers than in, say, $\mathrm{PSL}_n(\mathbb{Z}_p)$. This analogy is apt because $\mathrm{PSL}_n(\mathbb{Z}_p) \to \mathrm{PSL}_n(\mathbb{Z}/p)$ is a Frattini cover whenever $\mathrm{PSL}_n(\mathbb{Z}/p)$ is simple. Thus, the universal p-Frattini cover of $\mathrm{PSL}_n(\mathbb{Z}/p)$ is a proper cover of $\mathrm{PSL}_n(\mathbb{Z}_p)$ (see (2.5) and Remark 2.10).

It is easy to prove the (absolute) irreducibility of modular curves. Yet, their irreducibility is significant. For modular curve covers of the j-line, this follows from a *rigidity* type property, which we now explain. Classical rigidity is the simplest of a set of criteria ([**Se4**, Chap. 7] or [**Fr6**, §4]) for asserting the field of a definition of a cover is $\mathbb{Q}$.

Theorem 3.4 quotes [**FrV**] for generalizations of rigidity that depend on several assumptions. Most important is transitive action of the *Hurwitz monodromy group* H_r on *Nielsen classes*. The data for a Nielsen class comes from a collection of conjugacy classes in a finite group (§III.A). When this transitivity assumption holds, it is an analog for a level of a modular tower of the irreducibility of modular curves. (From [**Fr1**§3] or [**Fr4**]: Irreducibility of $X_1(p^n)$ follows from transitivity of H_4 on the Nielsen class of four repetitions of the conjugacy class of involutions in D_{p^n}. As in Theorem 3.4, this gives a transparent geometric reason for $\mathbb{Q}$ being a field of definition for these curves.) [**FrV**] sought applications to the inverse Galois problem. The tools, however, allow precise statements about fields of definition of these moduli spaces even when we relax the transitivity assumption (§III.B). This will breach ground between braid group representations in the Ihara, Matsumoto and Nakamura program and the moduli approach to the inverse Galois problem of myself, Debes and Völklein. Practical applications in [**DFr**], [**FrV**], [**Ma**^{2}], and papers these reference, already show the way. We now connect Part III results to those of the continuation of this paper, Parts IV and V (to appear elsewhere).

The lowest level of a modular tower is a Hurwitz space $\mathcal{H} = \mathcal{H}(G, p, \mathbf{C})$. A simplifying assumption is the collection $\mathbf{C}$ of conjugacy classes of G is a *rational union* (§III.A). In this case, when G has no center, $\mathbb{Q}$ is a field of definition of $\mathcal{H}$. All arithmetic applications of these spaces require knowing fields of definition of (absolutely irreducible) components of these spaces. It can even aid an applications that $\mathcal{H}$ is reducible, if it has a $\mathbb{Q}$ component. The spaces arise abstractly from covering space theory. So, it can be *extremely* difficult to catch the field of definition of components. Transitivity of the Hurwitz monodromy group is equivalent to there being one component. The lifting invariant $\nu = \nu(G, p, \mathbf{C})$ gives a more general criterion. Regard $\nu(G, p, \mathbf{C})$ as a function on components of $\mathcal{H}$. Its values are collections of conjugacy classes in the kernel of the universal p-Frattini kernel of G. The Main Theorem of §III.D says the following. If $\mathcal{H}_1$ is a component of $\mathcal{H}$, and $\sigma \in G_{\mathbb{Q}}$, then $\nu(\mathcal{H}_1) = \nu(\mathcal{H}_1^{\sigma})^{{}_p\psi(\sigma)}$. Here ${}_p\psi$ is the p-cyclotomic character. So, suppose $\mathcal{H}_2$ is another component of $\mathcal{H}$. If $1 \notin \nu(\mathcal{H}_2)$ and $1 \in \nu(\mathcal{H}_1)$, then $\mathcal{H}_1$ and $\mathcal{H}_2$ aren't conjugate. Part II applies in §III.D to show we can compute information about ν.

§III.F has a criterion that guarantees every level of a modular tower has a $\mathbb{Q}$ absolutely irreducible component. This gives a second approach to detecting $\mathbb{Q}$ components. The example criterion introduces H(arbater)M(umford) representatives in a Nielsen class. This is the most practical criterion we have. It, however, applies less often than does the lifting invariant. Part IV relates the lifting invariant and generalizations of HM representatives.

[**IM**] produces a section β to the natural map from the arithmetic fundamental group of $\mathbb{P}^r \setminus D_r$ to $G_{\mathbb{Q}}$. Any such section gives an action of $G_{\mathbb{Q}}$ (faithful, in this case) on the profinite completion of $\pi_1(\mathbb{P}^r \setminus D_r)$ with respect to all subgroups of finite index. The latter group identifies with the pro-finite *Hurwitz monodromy group*. Different sections β, however, give different actions. [**IM**] uses a Deligne *Tangential Basepoint* to create a section with valuable properties. In particular, it identifies this action with the embedding of $G_{\mathbb{Q}}$ in the Grothendieck-Teichmüller group, $\widehat{\mathcal{G}T}$.

There is speculation $\widehat{\mathcal{G}T}$ might contain $G_{\mathbb{Q}}$ as an open subgroup. Parts IV and V consider the action of $\widehat{\mathcal{G}T}$ on components of modular towers at each level. The conjectured $\widehat{\mathcal{G}T}$-$G_{\mathbb{Q}}$ relation gives results for $G_{\mathbb{Q}}$ action on components of the modular towers. Part IV gives meaning to the statement that $\widehat{\mathcal{G}T}$ preserves the lifting invariant. As a prelude, §App.C reinterprets the criterion of [**DFr2**] for describing all real points on a Hurwitz space. This resembles the construction of the [**IM**] section. So, it lets us compare their $G_{\mathbb{Q}}$ action with the lifting invariant. This is appropriate because both limit the action of $G_{\mathbb{Q}}$ on Hurwitz space components.

This material also supports a companion topic, *real points on modular towers* (§App.D). This interprets existence of a projective system of real points on a given modular tower. Other groups appear here, natural for the problem at hand, yet not the universal Frattini cover. In this case, it is the *universal Artin-Schreier cover* of a finite group G' equipped with a collection of conjugacy classes of involutions. Constructions in [**H**] are a forerunner. This shows the value of going beyond the elementary elegance of the p-unramified case of modular towers in this paper. (Part IV, in particular, computes a low level quotient of the 2-ramified invariant of L. Schnepp's 3-branch point cover of degree 20.) This is one from the summary of problems in the Appendix. Many of these problems belong to modular representations. Part IV compares this with the generators and relation presentation of $\widehat{\mathcal{G}T}$.

Part V concentrates on diophantine topics. For these we consider especially how to apply results of G. Faltings (say, using G. Frey's Finite Field Principle as in Theorem 1.1) and H. Nakamura (as in [**Na**, Thm. 2.3.1]). Every finite group G is a Galois group of a regular extension of $\mathbb{F}_p(x)$ for almost all primes p [**FrV**]. §App.E gives an explicit bound on the exceptional primes to this statement for a specific group G. A realizing cover for a given group G has an associated *Nielsen class*. This comes from the conjugacy classes of the r branch points of the realizing extension. We state our result depending on the Nielsen class of the realization. It is possible to get a statement bounding these primes, dependent only on G. Still, this reduces the structure in the problem. While we believe this result new, for the aspirations of this paper it is inadequate. We accept the primes dividing $|G|$ as exceptional. Assume p does not divide $|G|$. Our test produces an infinite number of varieties over every finite field. One $\mathbb{F}_p$ point on any one of them gives a regular realization of G. Further, there's the tower above the lowest level (on each one). It is a waste to apply the standard Riemann hypothesis estimate to this situation. The curves of statement D_1 (below) motivate going far beyond this limited result. Our introduction concludes with two structured, yet opposed, diophantine themes.

$\mathbf{D}_1$*: Non-congruence subgroup curves. Non-congruence* subgroup curves are an entertaining place to apply the above diophantine discussion. These are quotients of the upper half (complex) plane by a subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index. (Technically, Γ shouldn't contain a congruence subgroup to deserve the non-congruence appellation.) Suppose Γ is a subgroup of the congruence subgroup $\Gamma_0(2)$. Then, ([**Fr4**] or [**Fr7**]) *every* such curve appears in the pullback to $(\mathbb{P}^1)^4$ of a component of a Hurwitz space of four branch point covers (see Problem (B.2) of §App.B). Thus, to each, §III.C associates a modular tower. This view offers chances to reconsider the special role of modular curves. These are curves. So, we need no extra machinery likely necessary to consider diophantine questions in full generality on modular towers. We don't yet know, for example, what is the analog of Theorem 1.1 for these non-congruence modular towers.

$\mathbf{D}_2$*: Changing the number of branch points.* Classical diophantine topics are primarily limitation results. No problem suggested by this paper has more applications than producing rational points on Hurwitz spaces $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ or $\mathcal{H}(G,\mathbf{C})^{\mathrm{ab}}$ (§III.A) where $\mathbf{C}$ has many repetitions of conjugacy classes. [**FrV**] and [**FrV2**] show this would give much more than the inverse Galois problem; much more than Shafarevich's conjecture. This is part of the $(G,\hat{G},\mathbf{C})$-realization topic in §I.D. The $(D_p,\mathbb{A}_p,\mathbf{C}_{p+1})$-Lemma gives a success here. It produces the analog for suitably large genus hyperelliptic curves of $\mathbb{Q}$ non-cusp points on $X_0(p)$. (beginning of §App.D).

§**I.C. Notation.** Suppose x is an indeterminate over a perfect field F. An extension $L/F(x)$ is *regular* if $\bar{F}\cap L = F$ where $\bar{F}$ denotes the algebraic closure of F. Such an extension has *branch points*: values $x_1,\dots,x_r$ of x with fewer than $[L:\mathbb{Q}(x)] = n$ places of L lying over the place of $F(x)$ corresponding to the specialization $x\mapsto x_i$ (§I.F). Let $\hat{L}$ be the Galois closure of the extension $L/F(x)$. Suppose the extension is *tamely ramified*, say, as when the characteristic of F is 0. Then, associate a cyclic subgroup $\langle\sigma_i\rangle$ to each place $\boldsymbol{p}_i$ of $\hat{L}$ lying over x_i. The *ramification index* of x_i is the minimal integer e_i for which $\hat{L}$ embeds in the formal Laurent series field $\bar{F}(((x-x_i)^{1/e_i}))$.

Let ζ_e be a primitive e-th root of 1. Assume $\{\zeta_e \mid e = 1,2,\dots\}$ forms a compatible system: $\zeta_{e_1e_2}^{e_2} = \zeta_{e_1}$. In characteristic 0 choose $\zeta_e = e^{2\pi i/e}$. Denote formal Laurent series in x over a field F by $F((x))$. From this define an automorphism σ of $\bar{F}(((x-x_i)^{1/e_i}))$ fixed on $\bar{F}$ that maps $(x-x_i)^{1/e_i}$ to $\zeta_{e_i}(x-x_i)^{1/e_i}$. Then, σ_i is restriction to $\hat{L}$ of σ. The collection $\sigma_1,\dots,\sigma_r$ is a *description of the branch cycles* of the cover when the following hold. First: $\sigma_1,\dots,\sigma_r$ generate $G = G(\bar{F}\hat{L}/\bar{F}(x)$, the *geometric* monodromy group of $L/F(x)$. Second: The product of $\sigma_1,\dots,\sigma_r$, in some order, is 1. §I.F has more on Riemann's existence theorem: production of covers from branch cycles.

The varieties of this paper are either affine or projective. For example, Hurwitz spaces are affine varieties. (Don't, however, expect to see equations for them.) Suppose Y is an algebraic variety (an irreducible locally closed subset of projective space) defined over a field F. (It may not be *absolutely irreducible*: over the algebraic closure, $\bar{F}$, Y may have several components.) Denote the field generated by coordinates of a point $\boldsymbol{p}\in Y$ by $F(\boldsymbol{p})$. In particular, if $\boldsymbol{p}$ is a (Weil) generic point of Y, then $F(\boldsymbol{p})$ is the function field of Y. Let $\phi: X\to Y$ be a finite cover. Further, suppose X and Y are *normal varieties*, and ϕ and the varieties have F as a field of definition. Let $\mathrm{Aut}_F(X/Y)$ denote the algebraic isomorphisms $\psi: X\to X$ defined over F with $\phi\circ\psi=\phi$ when applied to the points of X. We say ϕ is a *Galois cover* when the order of $\mathrm{Aut}_F(X/Y)$ equals the degree of ϕ. For any (separable) cover, $\phi: X\to Y$, over F, §I.G does a fiber product construction of the Galois closure over F. This is the minimal Galois cover of Y, defined over F, factoring through X. The group of this cover is the *arithmetic* monodromy group of $\phi: X\to Y$. The corresponding cover and group over $\bar{F}$ is the *geometric* monodromy group. If $\tau\in G_F$, then Y^τ is the variety you get by applying τ to coefficients of polynomials giving Y. In the next section $\mathbb{F}_q$ is the finite field of order q.

§**I.D. Motivating problems.** This section discusses two example problems.

They interpret points on modular curves as realization of certain pairs of groups as (arithmetic and geometric) monodromy groups of a cover. More formally, let G and $\hat{G}$ be transitive subgroups of S_n for some integer n, with G normal in $\hat{G}$. Further, consider $(G, \hat{G}, \mathbf{C})$ where $\mathbf{C}$ is a collection of r conjugacy classes (with possible repetitions) of G.

DEFINITION. *$(G, \hat{G}, \mathbf{C})$-realizations.* Let $L/F(x)$ be a regular *tame* extension. We say it is a $(G, \hat{G}, \mathbf{C})$-realization under the following conditions.

(c_1) $L/F(x)$ has arithmetic monodromy group $\hat{G}$.
(c_2) $\bar{F}L/\bar{F}(x)$ has geometric monodromy group G.
(c_3) Branch cycle descriptions of $L/F(x)$ have attached conjugacy classes $\mathbf{C}$.

Problem statements.

A. Involution realizations of dihedral groups as regular extensions over $\mathbb{Q}$ [**DFr**, §5.1-5.2].
B. Production of *median value curves*—projective nonsingular curves C over $\mathbb{F}_q$—with exactly q^t+1 points over $\mathbb{F}_{q^t}$ for infinitely many t. [**Fr1**, §3]

Problem A: $(D_p, D_p, \mathbf{C}_r)$-realizations; $\mathbf{C}_r$ being r repetitions of the class of involutions. Problem A comes from [**DFr**]. Let p be an odd prime. It is easy to realize the dihedral groups D_{p^n} as regular extensions $L/\mathbb{Q}(x)$ over $\mathbb{Q}$. Known ways, however, require many branch points—at least $p^n - p^{n-1} + 1$—for primes p larger than 7. It is *impossible* to get fewer branch points in a $\mathbb{Q}$ regular realization unless all the branch cycles are involutions. When $r = 4$, such *involution realizations* correspond to $\mathbb{Q}$ non-cusp points on the modular curves classically called $X_1(p^n)$ [**DFr**, Theorem 5.1]. Here is why for the case $n = 1$.

Suppose $L/\mathbb{Q}(x)$ is a degree p regular extension ramified at $r = 4$ points. Further, assume its Galois closure is an involution realization of D_p. Apply the Riemann-Hurwitz formula to $L/\mathbb{Q}(x)$. Since $r = 4$, the genus $g(L)$ of L is 0:

$$2([L : \mathbb{Q}(x)] + g(L) - 1) = 4([L : \mathbb{Q}(x)] - 1)/2$$

with $[L : \mathbb{Q}(x)] = p$. This is because involutions in the degree p representation fix one integer, and switch $(p-1)/2$ others in pairs. The Galois closure, however, is the regular function field $\hat{L}$ of a genus 1 curve $\hat{X}$. Further, the automorphisms—also defined over $\mathbb{Q}$—have among them one, say α, of order p. Consider the quotient $\hat{X}/\langle\alpha\rangle$ of $\hat{X}$ by the group α generates. The degree p map $\hat{X} \to \hat{X}/\langle\alpha\rangle$ is unramified. While $\hat{X}$ and $\hat{X}/\langle\alpha\rangle$ may not have rational points, their jacobians, elliptic curves, do. Further, the genus 0 function field L, of odd degree over $\mathbb{Q}(x)$, must be $\mathbb{Q}(x')$ for some transcendental x'. This is the classical Hilbert-Hurwitz argument. In summary: The original extension has form $\mathbb{Q}(x')/\mathbb{Q}(x)$, arising from a rational function $f(x') = x$. Trace f to an isogeny of degree p from a rational p-division point on an elliptic curve [**Fr1**, §3].

This isogeny produces a $\mathbb{Q}$ rational non-cusp point on $X_1(p^n)$: the moduli space of pairs of elliptic curves with a p-division point. Mazur's Theorem says such rational points don't exist if $p > 7$ [**M**]. Thus, for $r = 4$ and $p > 7$ there is no regular realization of D_p as a Galois group. Let r_0 be any integer. A conjecture of [**DFr**] states: Only finitely many values of p^n produce regular realizations of D_{p^n} with fewer than r_0 branch points.

This conjecture, however, doesn't tell our full ignorance on involution realizations of D_{p^n}. We suspect there *exist* many involution realizations of D_{p^n} over $\mathbb{Q}$. F. Leprévost suggested an example that isn't an involution realization of D_p. Still, it is close. Further, it shows why variants on the pair $X_0(p^n)$ and $X_1(p^n)$ appear everywhere in modular tower theory (as in Problem D.1 of §App.D).

Consider the Fermat curve W, complete and nonsingular, with associated affine set $\{(u, v) \mid u^p + v^p = 1\}$. As usual, p is an odd prime. Take Z to be the hyperelliptic curve with associated affine set $\{(x, y) \mid y^2 = 4x^p + 1\}$: $\psi : Z \to \mathbb{P}^1_x$ is the canonical degree 2 cover.

The genus of W is $g(W) = (p-1)(p-2)/2$ and $g(Z) = (p-1)/2$. Consider $\phi : W \to Z$ by $\phi(u, v) = (x, y)$ with $x = -uv$ and $y = u^p - v^p$: $(u^p - v^p)^2 = 4(-uv)^p + 1$. To simplify notation denote the semi-direct product $\mathbb{Z}/p \times^s (\mathbb{Z}/p)^*$ (multiplication action of $(\mathbb{Z}/p)^*$ on $\mathbb{Z}/p$) by $\mathbb{A}_p$. With C the conjugacy class of involutions in D_p, let $\mathbf{C}_r$ be r repetitions of C.

LEMMA: $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-REALIZATION OVER $\mathbb{Q}$. *The morphism ϕ is of degree p, unramified and defined over $\mathbb{Q}$. The cover $\phi' = \psi \circ \phi : W \to \mathbb{P}^1_x$ is a $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization over $\mathbb{Q}$.*

PROOF. Write $u + v = u + x'/v$, subject to relations $u^p + v^p = 1$ and $x = -uv = -x'$. Part A below shows properties of a polynomial $T_p(z) \in \mathbb{Q}[x, z]$. It is of degree p in z, and $T_p(u+x'/u) = u^p + (x'/u)^p$. Further, $T_p(z) - 1$ is (absolutely) irreducible as a polynomial in $\mathbb{Q}[x, z]$. Conclude: $L = \mathbb{Q}(x', u + x'/u)$ is a degree p extension of $\mathbb{Q}(x)$. Now, $F = \mathbb{Q}(u, v)$ is a degree 2 extension of L. Also, $K = \mathbb{Q}(x, y)$ is a degree 2 extension of $\mathbb{Q}(x)$, contained in L. Apply transitivity of degrees to compute that F is a degree p extension of K. There remain three parts: construction of T_p; computing a Galois closure; and concluding remarks.

Part A: How to get T_p. There exists an odd polynomial C_p giving the relation $C_p(t + 1/t) = t^p + 1/t^p$. Indeed, choose C_p from DeMoivre's formula:

$$e^{i\theta p} = (\cos(\theta) + i\sin(\theta))^p = \cos(p\theta) + i\sin(p\theta). \tag{†}$$

Take real parts of both sides, and re-express $\sin^2$ as $1 - \cos^2$. This gives H_p satisfying $H_p(\cos(\theta)) = \cos(p\theta)$. Write $C_p(z) = 2H_p(z/2)$. Since $C_p(t + 1/t) = t^p + 1/t^p$ for all t of form $e^{i\theta}$, it holds for all t. Exchange θ for $-\theta$ to see C_p is an odd polynomial: $C_p(-x) = -C_p(x)$.

Now, make a substitution: $t = u/a$, or

$$(\ddagger)\qquad C_p(u/a + a/u) = C_p(1/a(u + a^2/u)) = 1/a^p(u^p + a^{2p}/u).$$

Let $a^2 = x'$. Since C_p is an odd polynomial, deduce this gives T_p. Finally, we show $T_p(z) - 1$ is irreducible. By construction, the leading term of $T_p(z) - 1$ is $(p+1)z^p$: from the coefficient of $\cos^p$ in

$$\cos^p + p(\cos^{p-2})(-\sin^2) = (p+1)\cos^p + p\cos^{p-2}.$$

Excluding the lead and constant terms, the other coefficients of $T_p(z) - 1$ have a positive power of x as a factor. As p is a prime, if $T_p(z) - 1$ factors, it must have proper factors with coefficients in $\mathbb{Q}[x]$. Now specialize x to 0 to conclude $(p+1)z^p - 1$ has proper factors over $\mathbb{Q}$. This is clearly false.

Part B: Properties of the Galois closure of $L/\mathbb{Q}(x)$. Let $\hat{L}$ be the Galois closure of the extension of $L/\mathbb{Q}(x)$. A trick simplifies this. Adjoin $x^{\frac{1}{2}}$ to L. Then, $L(x^{\frac{1}{2}}) = \mathbb{Q}(x^{\frac{1}{2}}, u + v) = \mathbb{Q}((1/x^{\frac{1}{2}})(u + v), x^{\frac{1}{2}})$. From ($\ddagger$), the splitting field of $L(x^{\frac{1}{2}})/\mathbb{Q}(x^{\frac{1}{2}})$ is the splitting field of $C_p(z) - (1/x^{\frac{1}{2}})^p$ over $\mathbb{Q}(x^{\frac{1}{2}})$. Let $t + 1/t = z$ and $s = (1/x^{\frac{1}{2}})^p$. Then, the splitting field $\Omega_{C_p - s}$ of $C_p(z) - s$ over $\mathbb{Q}(s)$ is $\mathbb{Q}(\zeta_p^i t + 1/(\zeta_p^i t), i = 0, \dots, p-1)$. Add $\zeta_p^i t + 1/(\zeta_p^i t)$ to its complex conjugate to see $\cos(2\pi/p)(t + 1/t)/(t + 1/t) = \cos(2\pi/p)$ is in $\Omega_{C_p - s}$.

Thus, $\mathbb{Q}(\cos(2\pi/p)$ is the extension of constants (see §I.E) from going to the Galois closure of $\mathbb{Q}(z)/\mathbb{Q}(s)$: $\Omega_{C_p - s} = \mathbb{Q}(t + 1/t, \zeta_p t + 1/(\zeta_p t), \cos(2\pi/p))$. The Galois group $G(\Omega_{C_p - s}/\mathbb{Q}(s))$ is $\mathbb{A}_p$, and the geometric monodromy group is D_p. Adjoin $i = \sqrt{-1}$ to the splitting field of $C_p(z) - s$ over $\mathbb{Q}(x^{\frac{1}{2}})$ to get $\mathbb{Q}(t, \zeta_p, x^{\frac{1}{2}}) = L'$. As $t + x'/t$ is in this field, take $t = u$ to see L' contains F. Do the remainder of the lemma by working in L'.

Part C: Comments on the proof. This example centered on the cover of the x-line defined by $C_p(z) - x^p = 0$. All other covers come from pullback of this one, which had geometric monodromy group D_p. For this cover, ramification over ∞ is a p-cycle. Pulling this back over a cover ramified of order p over ∞ gives an involution realization. Still, the real subfield of $\mathbb{Q}(\zeta_p)$ appears in the Galois closure. □

Earlier we found that a $(D_p, D_p, \mathbf{C}_4)$-realization over $\mathbb{Q}$ produces a non-cusp $\mathbb{Q}$ point on $X_1(p)$. Similarly, for $\hat{G}$ with $D_p \triangleleft \hat{G} \le S_p$. Finding a $(D_p, \hat{G}, \mathbf{C}_4)$-realization over $\mathbb{Q}$ produces a non-cusp $\mathbb{Q}$ point on $X_0(p)$.

§App.D and §App.E explain natural diophantine generalizations to every finite group G, prime p dividing the order of G, and collection of conjugacy classes of G. Suppose the conjugacy classes of G are of elements of orders relatively prime to p. Then, we construct a *tower* of varieties from the Hurwitz spaces $\mathcal{H}(G, \mathbf{C})^{\mathrm{ab}}$. This generalizes the tower $X_0(p) \leftarrow X_0(p^2) \cdots$. (Hurwitz spaces $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$ give the analog of $X_1(p) \leftarrow X_1(p^2) \cdots$.) This also produces a $G_{\mathbb{Q}}$ invariant of the *braid group orbit* of any curve cover (§III.D). Now turn to Problem B.

Problem B: $(G, \hat{G}, \mathbf{C})$*-realizations over finite fields.* Let $\mathbb{F}_q$ be the finite field of order q. Suppose a pair of groups $(G, \hat{G})$ is the respective geometric/arithmetic monodromy group pair of an extension $L/\mathbb{F}_q(x)$. (Assume, also, G has no center.) Necessary conditions are

(a) $G \triangleleft \hat{G}$, $\hat{G}/G$ is cyclic, and
(b) no element of $\hat{G} \setminus G$ centralizes G [**Fr5**, Prop. 2].

Then, [**Fr1**, Th. 2.5] shows this converse.

Theorem: G/A monodromy existence over finite fields. *$(G, \hat{G})$ is the geometric/arithmetic monodromy group pair of a regular extension $L/\mathbb{F}_{p'}(x)$ for all but finitely many primes p'.*

§App.E bounds exceptional primes to this statement. Still, as in §I.B, there is so much structure here, it behooves us to toss Lang-Weil estimates. We explain with the special case $G = D_p$, and $\hat{G}$ is a proper overgroup normalizing G. These produce examples of median value curves sought by Problem B.

Construction of *exceptional covers* is a recurrent application. These give function field extensions $L/\mathbb{F}_q(x)$ where each $x \in \mathbb{F}_{q^t} \cup \{\infty\}$ has exactly one $\mathbb{F}_{q^t}$ place of L above it for infinitely many t.

Exceptionality Statement [**Fr1–3**]. *Regular extension $L/\mathbb{F}_q(x)$ is exceptional exactly when each orbit of $\hat{G}(1)$ acting on $\{2, \ldots, n\}$ breaks into strictly smaller orbits under $G(1)$. Equivalently: If $(t, |\hat{G}/G|) = 1$, each $x \in \mathbb{F}_{q^t} \cup \{\infty\}$ has exactly one $\mathbb{F}_{q^t}$ place of L above it.*

The unique nonsingular projective curve, up to isomorphism, with function field L, is a *median value curve*. It has exactly $q^t + 1$ rational points in $\mathbb{F}_{q^t}$ for infinitely many t. Potential applications of median value curves require explicit realizations of them.

Take $q = r^a$ for some odd prime $r \neq p$. [**Fr1**, Cor. 3.5] produces genus 0 exceptional covers of degree p. Reduce $X_0(p)$ modulo r. Call this $X_0(p)^{(r)}$. You get one of these degree p rational functions over $\mathbb{F}_q$ for each $\mathbb{F}_q$ point of $X_0(p)^{(r)}$ with nontrivial frobenius in the cover $X_1(p)^{(r)} \to X_0(p)^{(r)}$ (see §I.E). We don't know of refined estimates for such points on $X_0(p)^{(r)}$. Still, Lang-Weil applied to twists of modular curves is not the right tool. Over $\mathbb{F}_{p^2}$ we could use the same supersingular curves that appear in the proof of Theorem 1.1. Complex multiplication (as [**Fr4**] notes) precisely describes this problem. Again, these ideas generalize. The variant question in Theorem 1.1 is the production of such rational functions f over number fields that reduce modulo infinitely many primes to these examples.

§I.E. Exact Constants Sequence. Suppose $L/F(x)$ is a regular extension with Galois closure $\hat{L}$. This gives an exact sequence

$$1 \to G(\hat{L}/\hat{F}(x)) \to G(\hat{L}/F(x)) \to G(\hat{F}/F) \to 1. \tag{1.1}$$

Consider realizing a group G as a Galois group of a regular extension of F. We might want the first term of (1.1) to be G and $G(\hat{F}/F)$ to be 1. Recognize $\hat{F}$ as the smallest extension of F containing the constants of a Galois closure of $L/F(x)$. Especially, the functions giving the automorphisms of the extension have field of definition $\hat{F}$. For other applications, including Problems A and B, $G(\hat{F}/F)$ should be as large as possible. Either way, we need to know the possibilities for $G(\hat{F}/F)$. With $\hat{G} = G(\hat{L}/F(x))$ this is the topic of $(G, \hat{G})$-realizations over a field F: we've dropped explicit dependence on $\mathbf{C}$.

For example, again take $G = D_p$ with p an odd prime. Let F be an algebraic number field: $[F : \mathbb{Q}] < \infty$. Suppose $L/F(x)$ is of degree p, with geometric monodromy group D_p. Since $G(\hat{L}/F(x))$ is in S_p, §I.D shows the largest group it can be is $\mathbb{A}_p$.

Suppose the extension has involutions as branch cycles and there are $r = 4$ branch points. If it's not an involution realization of D_p, then $\hat{F} \neq F$. From §I.D, the extension gives a rational function f with $f : \mathbb{P}^1 \to \mathbb{P}^1$ an exceptional cover for infinitely many primes $\boldsymbol{r}$ of the number field F. To be precise, let $\mathbb{F}_{\boldsymbol{r}}$ be the residue class field of $\boldsymbol{r}$.

Assume $\boldsymbol{r}$ does not divide p where f reduces to a rational function $f_{\boldsymbol{r}}$ of degree p. Let $\Omega_{f_{\boldsymbol{r}}}$ be the splitting field of $f_{\boldsymbol{r}}(y) - x$ over $\mathbb{F}_{\boldsymbol{r}}(x)$. With care, we can assure there is a corresponding sequence to (1.1):

$$1 \to D_p = G(\Omega_{f_{\boldsymbol{r}}}/\hat{\mathbb{F}}_{\boldsymbol{r}}(x)) \to G(\Omega_{f_{\boldsymbol{r}}}/\mathbb{F}_{\boldsymbol{r}}(x)) \to G(\hat{\mathbb{F}}_{\boldsymbol{r}}/\mathbb{F}_{\boldsymbol{r}}) \to 1. \tag{1.2}$$

Let $\mathcal{T}_F$ be the primes of F whose frobenius element in the extension $\hat{F}/F$ is non-trivial. For almost all $\boldsymbol{r} \in \mathcal{T}_F$ the Exceptionality Statement (§I.D) shows $f_{\boldsymbol{r}}$ to be an *exceptional rational function* [**Fr4**, §4]. So, now we look at how abundant are these fields F producing such rational functions f.

Follow classical terminology. Write $\mathbb{Q}(X_0(1)) = \mathbb{Q}(j)$ with j the j-invariant of the generic elliptic curve over $\mathbb{Q}$. Results of Faltings give a goal for concise statements on the diophantine properties of modular towers. The analog of $\mathbb{A}_p$ for D_{p^n} is $\mathbb{A}_{p^n} = \mathbb{Z}/p^n \times^s (\mathbb{Z}/p^n)^*$.

THEOREM 1.1. *Let p be any odd prime and n a positive integer. An infinity of $\boldsymbol{x} \in X_0(p^n)(\bar{\mathbb{Q}})$ produce a $(D_{p^n}, \mathbb{A}_{p^n}, \mathbf{C}_4)$-realization over $F = \mathbb{Q}(\boldsymbol{x})$. Suppose, however, we fix F. Then, for p^n large, only finitely many $\boldsymbol{x} \in X_0(p^n)$ have coordinates in F. Even stronger, fix an integer d. Assume p^n large (dependent on d). Only finitely many $\boldsymbol{x} \in X_0(p^n)$ have coordinates in a field of degree at most d over $\mathbb{Q}$.*

PROOF. For the first part apply Hilbert's irreducibility theorem (HIT), done as follows for this point in [**Fr4**]. The extension $\mathbb{Q}(X_1(p^n))/\mathbb{Q}(X_0(p^n))$, has degree $p^{n-1}(p-1)/2$. Pick a specialization ν of $\mathbb{Q}(X_1(p^n))$ over $j_0 \in \mathbb{Q}$. Let its residue class field be $\hat{F}$. Let the residue class field of restriction of ν to $\mathbb{Q}(X_0(p^n))$

be F. From HIT, $[\hat{F} : F]$ has degree $p^{n-1}(p-1)/2$ for infinitely many $j_0 \in \mathbb{Q}$. Conclude from the discussion of §I.D.

Now for the second part where we fix F. The classical Riemann-Hurwitz computation for $X_0(p^n)$ (as a cover of the j-line) shows its genus grows large with p^n. Apply Faltings' Theorem: Over any number field F, a curve of genus exceeding 1 has only finitely many F points.

Consider the statement on bounding the values p^n for which $X_0(p^n)$ has infinitely many points over fields F with $[F : \mathbb{Q}] \le d$. This is from [**F**, Cor. 2]. Frey's argument was for p, but applies to p^n. The conclusion of the theorem holds for $p^n > 120d$ using [**Fa2**] and a subtle finite field argument.

Let W_d be the d-th symmetric product of $X_0(p^n)$ in its Picard component of degree d. Suppose W_d contains an infinite number of F rational points. Then, [**Fa2**] says W_d contains the translate of an abelian variety. Further, $\mathbb{Q}$ is a field of definition for the translating divisor, the abelian variety and infinitely many of its points. [**F**, Cor. 2] concludes with 2-steps. First: It shows this implies there is a cover $\phi : X_0(p) \to \mathbb{P}^1$, over $\mathbb{Q}$, of degree no more than $2d$. This argument is general, having nothing to do with modular curves. Reducing this situation modulo a prime $\boldsymbol{r} \ne p$ produces $\phi_{\boldsymbol{r}} : X_0(p^n)^{(\boldsymbol{r})} \to \mathbb{P}^1$ (as in §I.D), with $\phi_{\boldsymbol{r}}$ of degree at most $2d$. Such a reduction is possible; Frey quotes Deuring's reduction theory results. Now we come to the final argument.

Take any finite field $\mathbb{F}'$ containing $\mathbb{F}_{\boldsymbol{r}}$. Existence of $\phi_{\boldsymbol{r}}$ bounds $X_0(p^n)(\mathbb{F}')$ independently of p^n by $(|\mathbb{F}'|+1)2d$. Take, however, $\boldsymbol{r} = 2$, and $\mathbb{F}'$ the quadratic extension of $\mathbb{F}_{\boldsymbol{r}}$. Then, [**I2**] (or [**R**, pgs. 226–239]) shows $X_0(p)(\mathbb{F}')$ has at least $\left[\frac{p^n}{12}\right] + 1$ points. These points derive from *supersingular elliptic curves* for the prime 2. Supersingular curves have defining field the quadratic extension of $\mathbb{F}_2$. This contradiction gives explicit bounds on exceptional values of p^n. $\square$

§I.F. Algebraist's version of Riemann's existence theorem. Consider an extension $L/\mathbb{C}(x)$ of degree n. Suppose its Galois closure $\hat{L}/\mathbb{C}(x)$ has group G. Then, $G(\hat{L}/\mathbb{C}(x))$ faithfully embeds in S_n. The image is unique up to conjugation by an element of S_n.

For any $x' \in \mathbb{C} \cup \{\infty\}$, consider the formal Laurent series $\mathbb{C}((x-x'))$ in $x - x'$. Replace $x - x'$ by $1/x$ if $x' = \infty$. The algebraic closure of $\mathbb{C}((x-x'))$ is $\cup_{e=1}^{\infty}\mathbb{C}(((x-x')^{\frac{1}{e}}))$. Thus, the absolute Galois group of $\mathbb{C}((x-x'))$ is pro-cyclic. Its generator $\sigma_{x'}$ has the effect $(x-x')^{\frac{1}{e}} \mapsto \zeta_e(x-x')^{\frac{1}{e}}$, $e = 2, 3, \dots$. Here $\zeta_e = e^{2\pi i/e}$. There is a minimal integer e with $\hat{L}$ embedding in $\mathbb{C}(((x-x')^{\frac{1}{e}}))$ as the identity on $\mathbb{C}(x)$. Compose any one embedding $\psi_{x'} : \hat{L} \to \mathbb{C}(((x-x')^{\frac{1}{e}}))$ with an automorphism of $\hat{L}$, to get any other. Therefore, restriction of $\sigma_{x'}$ to $\hat{L}$ defines a conjugacy class of elements in $G(\hat{L}/\mathbb{C}(x))$.

Only finitely many x' have $e = e_{x'} > 1$. Label these $\boldsymbol{x} = (x_1, \dots, x_r)$, the *branch points* of the cover. For embeddings ψ attached to these points, name the corresponding automorphisms by $\boldsymbol{\sigma} = (\sigma_1, \dots, \sigma_r)$. Let e_i be the e attached to x_i: the *ramification index* at x_i.

RIEMANN'S EXISTENCE THEOREM. *For some choice of ψ s,*

(i) $\sigma_1 \cdots \sigma_r = 1$, *and*
(ii) *the σ_i s generate G.*

Conversely, suppose $x_1, \dots, x_r$, and $\sigma_1, \dots, \sigma_r \in S_n$ satisfy (i) *and* (ii) *with G transitive in S_n. Then, there exists $L/\mathbb{C}(x)$ producing this data as above.*

§**I.G. Geometric Galois closure.** Riemann's existence theorem gives topological existence to the covers of $\mathbb{P}^1$. It is, however, harder to see the relation between a cover and its automorphisms. For example, if a field F is the field of definition of a cover, what is the defining field of the cover's Galois closure?

The Galois closure construction (below) reduces finding the field of definition of automorphisms to finding a connected component of a curve. It is a form of Kronecker's old construction of the Galois group of a polynomial. Its use of fiber products lends itself to forming Galois closures of families of covers.

Consider a cover $\phi : X \to \mathbb{P}^1$ of degree n. Assume X is absolutely irreducible. Suppose F is a field of definition of the cover. Form the fiber product of the curve with itself n times. This is $X^n_{\mathbb{P}^1}$, n-tuples from X whose coordinates have a common image under ϕ. Remove an obvious set of components where two or more coordinates are equal, the *fat diagonal* Δ. Denote $X^n_{\mathbb{P}^1} \setminus \Delta$ by $X_1^{(n)}$. Note: S_n acts as permutations of the coordinates of $X_1^{(n)}$. Normalize this curve so the result is complete and nonsingular. It may not be absolutely irreducible. Still call this $X_1^{(n)}$. Let $\hat{X}$ be an F-connected component of $X_1^{(n)}$. Projection on the first coordinate gives a map

$$\hat{\psi} : \hat{X} \to X \xrightarrow{\phi} \mathbb{P}^1. \tag{1.3}$$

THEOREM: GALOIS CLOSURE CONSTRUCTION. *The cover $\phi \circ \hat{\psi} : \hat{X} \to \mathbb{P}^1$ is the Galois closure of ϕ over F. The group of $\hat{X} \to \mathbb{P}^1$ is the subset of S_n that leaves $\hat{X}$ invariant.*

PROOF. We derive this from the function field use of Galois theory. The curves in the cover are normal. Therefore, elements of $\mathrm{Aut}(\hat{X}/\mathbb{P}^1)$ correspond to automorphisms of $F(\hat{X})/F(x)$ where x uniformizes $\mathbb{P}^1$. Let α be a primitive element for the field extension $F(X) = F(\alpha, x)$ over $F(x)$.

Conjugates $\alpha_1, \dots, \alpha_n$ of α over $F(x)$ correspond to points of X over the generic point x on $\mathbb{P}^1$. Thus, there is a one-one relation between points of $X_1^{(n)}$ over x and different n-tuples

$$\{(\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}), \pi \in S_n\}.$$

Let $\hat{\boldsymbol{p}} = (\boldsymbol{p}'_1, \dots, \boldsymbol{p}'_n)$ be a generic point of $\hat{X}$ over x: the $\boldsymbol{p}'$ s are an ordering of the points of X over x. Let $\hat{G}$ be the group of the Galois closure of $F(X)/F(x)$. This has an orbit on ordered n-tuples of conjugates of α. Conjugates of $\hat{\boldsymbol{p}}$ are permutations of the entries of $\hat{\boldsymbol{p}}$. Further, such conjugates are exactly the points of $\hat{X}$ over x. Conclude: $\hat{X}/\mathbb{P}^1$ is Galois. Its automorphisms are permutations of $\alpha_1, \dots, \alpha_n$ by $\hat{G}$. $\square$

PART II. UNIVERSAL FRATTINI COVERS

The *rank* of a profinite group G is the minimal number of elements that topologically generate G. Again, D_n is the dihedral group of order $2n$. For $G \le H$ groups and M a representation module for G, $\mathrm{ind}_G^H(M)$ is the induced representation module for H. This is G-equivariant functions from H into M:

$$\{f \in \mathrm{Maps}(H, M) \mid g(f(h)) = f(gh),\ g \in G, h \in H\}.$$

§II.A. Universal p-Frattini cover of a finite group G.

The profinite limit

$$\lim_{\infty \leftarrow n} D_{p^n} = D_{p^\infty} = {}_p\tilde{G} = \mathbb{Z}_p \times^s \mathbb{Z}/2$$

collects the finite groups D_{p^n} for all integers n. This section discusses the analog of this for any finite group G and any prime p dividing $|G|$. For later reference replace D_{p^∞} by ${}_p\tilde{G}$ and D_p by G.

Recover finite quotients of ${}_p\tilde{G}$ through the Frattini kernel of the natural map $\ker \to {}_p\tilde{G} \to G$. This produces a sequence of characteristic subgroups of ${}_p\tilde{G}$:

$$(2.1)\quad \ker = \ker_0,\ \ker_0^p[\ker_0, \ker_0] = \ker_1, \dots, \ker_{n-1}^p[\ker_{n-1}, \ker_{n-1}] = \ker_n, \dots$$

As usual, we understand $\ker_{n-1}^p[\ker_{n-1}, \ker_{n-1}]$ to be the closed subgroup of ${}_p\tilde{G}$ with generators from the elements of this set. The quotient ${}_p\tilde{G}/\ker_n$ is $D_{p^{n+1}}$. Since ker is $p\mathbb{Z}_p$, commutators $[\ker_n, \ker_n]$ here are trivial. They won't be in the general case. Summarizing [**FrJ**, §20.7], we explain how this applies to the universal Frattini cover of any finite group G.

A *Frattini cover* is a surjective homomorphism $\psi : H \to G$ of groups with this property. For a subgroup $H' < H$, if $\psi(H') = G$, then $H' = H$. Two Frattini covers $\psi_1 : H_1 \to G$ and $\psi_2 : H_2 \to G$ have a common cover. Indeed, let $H = H_1 \times_G H_2$ be the fiber product:

$$H = \{(h_1, h_2) \in H_1 \times H_2 \mid \psi_1(h_1) = \psi_2(h_2)\}.$$

Suppose H' is a minimal subgroup of H that projects surjectively onto each factor of H. Then, H' is a common Frattini cover of H_1 and H_2. There is a universal object: $\tilde{G}$ is the minimal *projective* cover of G. [**FrJ**, Prop. 20.33]: If $\psi : H \to G$ is any Frattini cover, there exists a cover $\gamma : \tilde{G} \to H$ with $\psi \circ \gamma = \tilde{\psi}$.

Furthermore, $\tilde{G}$ is a profinite projective group. That is, given a cover $\tilde{G} \to A$ and a cover $B \to A$, there is a homomorphism $\psi : \tilde{G} \to B$ completing a natural commutative triangle. Note: Don't expect ψ to be a cover (surjective) even when B is a quotient of $\tilde{G}$ [**FrJ**, Ex. 23.27]. Nor is there a unique ψ. One construction explains this projective property almost trivially. Let $\sigma_1, \dots, \sigma_r$ be generators of G and let $\tilde{F}_r$ be the free profinite group on r generators. That is, $\tilde{F}_r$ is the profinite completion, using all subgroups of finite index, of the free group on r generators. Map $\tilde{F}_r$ to G by mapping its canonical generators to the collection $\sigma_1, \dots, \sigma_r$. Since $\tilde{F}_r$ is a profinite group, any descending chain $H_1 > H_2 > \cdots$ of closed subgroups has nontrivial (closed subgroup) intersection. Apply this to find a minimal subgroup $\tilde{G} < \tilde{F}_r$ that maps surjectively by restriction to G. This is a Frattini cover because no proper closed subgroups maps surjectively to G. A closed subgroup of a projective group is projective. Thus, $\tilde{G}$ is projective. Other easy points are in [**FrJ**,§20.7]. Characterize $\tilde{G} \to G$ as a Frattini cover where the p-Sylows of $\tilde{G}$ are projective, and therefore free profinite groups.

The Frattini kernel of the map ${}_p\tilde{G} \to G$ is a nilpotent group $\ker = \ker_0$. Its nilpotency is the profinite analog of knowing the Frattini subgroup of any finite group is nilpotent. For each $p \mid |G|$, there is a *universal p-Frattini cover*. Call this ${}_p\tilde{G}$. It is universal for Frattini covers of G with p-group kernel. The p-Sylows of ker are nontrivial exactly for those primes dividing $|G|$: $\ker = \prod_{p \mid |G|} P_p$. Each P_p is a characteristic closed subgroup of $\tilde{G}$, so ${}_p\tilde{G} = \tilde{G} / \prod_{p' \mid |G|, p' \neq p} P_p$. Compare with the universal central extension of a perfect group.

Suppose G is perfect: generated by its commutators $[G, G]$. Then, $\tilde{G}$ is the closure of $[\tilde{G}, \tilde{G}]$ because the commutator image generates G. The universal central extension of a perfect group is a finite group. Yet, the universal Frattini cover, being a projective group, has no elements of finite order. An important point: The universal Frattini cover factors through the universal central extension.

§II.B. Properties of ${}_p\tilde{G}$. Sequence (2.1) helps check properties of ${}_p\tilde{G}$. Denote the quotient ${}_p\tilde{G}/\ker_n$ by ${}^n_p\tilde{G}$. When $n = 0$ this gives ${}^0_p\tilde{G} = G$. Suppose M is a G module and $\alpha \in H^i(G, M)$. Say α is *supported* by $\mathbb{F}_p[G]$ module $M'' \subset M$ if α is the image of $\beta \in H^i(G, M'')$ (from inclusion).

LEMMA 2.1. *For any integer $n \geq 0$, the universal p-Frattini cover of ${}^n_p\tilde{G}$ is ${}_p\tilde{G}$. There is a natural action of ${}^n_p\tilde{G}$ on the $\mathbb{F}_p$ vector space $\ker_n / \ker_{n+1}$. Characterize $M = \ker_0 / \ker_1$ as the maximal $\mathbb{F}_p[G]$ module having $\alpha \in H^2(G, M)$ with this property. For any nontrivial $\mathbb{F}_p[G]$ module quotient M' of M, the natural image α' of α in $H^2(G, M')$ is nonzero. Equivalently: M is maximal for having $\alpha \in H^2(G, M)$ not supported by a proper submodule of M.*

PROOF. ${}_p\tilde{G}$ is the smallest Frattini cover of G with a projective p-Sylow. Thus, the first sentence restates the projectivity property of ${}_p\tilde{G}$. The action of ${}^n_p\tilde{G}$ on $\ker_n / \ker_{n+1}$ is conjugation. That is, $g \in {}^n_p\tilde{G}$ lifts to $\tilde{g} \in {}_p\tilde{G}$; define $g(k \cdot \ker_{n+1})$ to be $\tilde{g}k\tilde{g}^{-1} \ker_{n+1}$ for each $k \in \ker_n$. Two lifts $\tilde{g}_1$ and $\tilde{g}_2$ produce the same action because $\tilde{g}_1\tilde{g}_2^{-1} = k_1$ is in $\ker_n$: $k_1 k k_1^{-1} = k$ modulo $\ker_{n+1}$.

The last sentence is cohomology for the existence of a universal exponent p Frattini cover of G with abelian kernel. For example see [**N**, §10.10–replace $\mathbb{Z}$-

modules there with $\mathbb{F}_p$-modules]. Suppose $H \to G$ is any exponent p Frattini cover with G module kernel M. This defines a nontrivial element $\alpha \in H^2(G, M)$. Moreover, if M/Q is a nontrivial G-quotient, the natural extension $H/Q \to G$ also is nontrivial. Otherwise, let G_1 be a splitting of G. Then, $\langle Q, G_1 \rangle$ would be a proper subgroup of H mapping surjectively to G. This contradicts the Frattini cover property. $\square$

REMARK 2.2. Call $\ker_0 / \ker_1$ in Lemma 2.1 the universal *p-Frattini module* for G. The groups $\ker_0 / \ker_1$ and $\ker_0$ in Lemma 2.1 have the same rank. Lemma 2.1 makes computation of $\ker_0$ effective (see Prop. 2.3). This allows an inductive approach to computing properties of ${}_p^n\tilde{G}$ (see Prop. 2.7). So, what would it mean to *know* the universal p-Frattini cover of a finite group G? The display of ${}_2A_5$ in §II.F gives a model for this. $\square$

Denote the algebraic closure of $\mathbb{F}_p$ by K_p. We list ingredients from the theory of *modular representations* [**A**, Chaps. 1-3]. Brauer's Theorem (below) on simple G modules forces considering, at times, $\dot{\mathcal{G}} = K_p[G]$ modules instead of $\mathbb{F}_p[G] = \mathcal{G}$ modules. Translation between statements about $\mathcal{G}$ modules to $\dot{\mathcal{G}}$ modules is usually straightforward. A $\dot{}$-over notation for a $\mathcal{G}$ module means we've tensored with K_p to make it a $\dot{\mathcal{G}}$ module. An *indecomposable* $\dot{\mathcal{G}}$ module is one without a nontrivial direct summand. A *simple* (or *irreducible*) $\dot{\mathcal{G}}$ module is one with no proper submodules. Let M be a $\dot{\mathcal{G}}$ module. Its *radical* is the smallest submodule $\mathrm{rad}(M)$ whose quotient $M/\mathrm{rad}(M)$ is a direct sum of simple modules [**A**, p. 3].

Let H be any subgroup of G. Denote the corresponding subalgebra by $\dot{\mathcal{H}}$. For M a $\dot{\mathcal{G}}$ module, let M_H be the corresponding $\dot{\mathcal{H}}$ module. The dimension of M is its vector space dimension over K_p.

(2.2a) *Brauer's theorem.* Simple $\dot{\mathcal{G}}$ modules have the same cardinality as G conjugacy classes whose elements have order prime to p [**A**, p. 14].
(2.2b) Indecomposable projectives M correspond to simple $\dot{\mathcal{G}}$ modules via the map $M \to M/\mathrm{rad}(M)$ [**A**, p. 31].
(2.2c) M is a projective $\dot{\mathcal{G}}$ module if and only if M_{P_p}, P_p the p-Slow of G, is a free $K_p[P_p]$ module [**A**, p. 33 and 66].

Lemma 2.3 describes the maximal pair (M_G, α_G). This is the universal exponent p Frattini cover of G with abelian kernel in Lemma 2.1. The universal p-Frattini module is M_G. Any $\mathbb{F}_p$ module A has a smallest projective cover

$$0 \to I \to P \to A \to 0,$$

where P is projective and has minimal dimension. This sequence is unique up to an obvious equivalence. Denote I by $\Omega(A)$. Benson [**Be**] calls this Heller's construction. Inductively, define $\Omega^r(A)$ for any $r \geq 1$ by iterating this on $\Omega^{r-1}(A)$. Apply this to the trivial module $\mathbf{1} = \mathbb{F}_p$. The next result follows [**Se2**].

PROJECTIVE INDECOMPOSABLE LEMMA 2.3. *M_G is isomorphic to $\Omega^2(\mathbf{1})$. The class α_G is canonically defined in $H^2(G, \Omega^2(\mathbf{1}))$.*

PROOF. All modules in the proof are finitely generated. Note: $H^r(G,A)$ is just $\mathrm{Ext}^r_G(\mathbf{1},A)$ [**N**, p. 223, Th. 4]. We show $\Omega^2(\mathbf{1}) = M$ is the maximal module having $\alpha \in \mathrm{Ext}^2_G(\mathbf{1},M)$ not supported on a submodule M'' (see Lemma 2.1). Use induction. For each integer $r \geq 1$ and $\mathcal{G}$ module B, consider pairs (M,α), $\alpha \in \mathrm{Ext}^r_G(B,M)$ not supported on a proper submodule. We show there is a maximal such, $M = \Omega^r(B)$. Further, the universal element of $\mathrm{Ext}^r_G(B,\Omega^r(B))$ represents α.

Let P be the smallest projective cover of B. Dimension shift on the canonical sequence $0 \to \Omega(B) \to P \to B \to 0$ in the first position of Ext_G. This shows $\mathrm{Ext}^r_G(B,M) = \mathrm{Ext}^{r-1}_G(\Omega(B),M)$. Suppose the *maximal* M for $r=1$ is $\Omega(B)$. Then, inductively, $\Omega(\Omega^{r-1}(B))$ is the *maximal* M for general r.

We now show $\Omega(B)$ is the maximal M for $r=1$. First: $\mathrm{Ext}^1_G(B,M)$ is equivalence classes of extensions of B by M [**N**, p. 129]. As in Lemma 2.1, first show no proper submodule M'' of M supports the canonical sequence. With no loss, replace B by a nontrivial simple quotient of one of its direct summands. Suppose, contrary to this, there is a split sequence: $M/M'' \to P/M'' \to B$ (with B simple). A splitting would show P/M'' to have a quotient with two (or more) simple summands. This contradicts (2.2b): B uniquely determines P by being its unique simple quotient (with multiplicity 1).

Finally, consider the relation of P to any short exact sequence $M' \to W \to B$. Since P is projective, the morphism $P \to B$ induces the short exact sequence $\Omega_1 \to P \xrightarrow{\tau} W$ that gives a natural diagram:

$$\begin{array}{ccccc} \Omega_1 & \longrightarrow & P & \xrightarrow{\tau} & B \\ \downarrow & & \downarrow & & \| \\ M' & \longrightarrow & W & \longrightarrow & B \end{array} \tag{2.3}$$

From [**N**, p. 129], the exact sequence of cohomology on the covariant 2nd slot produces $\mathrm{Ext}^1_G(B,\Omega_1) \to \mathrm{Ext}^1_G(B,M')$. The element of $\mathrm{Ext}^1_G(B,\Omega_1)$ defining the upper row of (2.3) maps to the element of $\mathrm{Ext}^1_G(B,M')$ defining the lower row of (2.3). This shows universality of the upper row extension of (2.3). □

§**II.C.** A_5—**checking properties of** ${}_p\tilde{G}$**.** Consider $A_5 = G$. The next statement is central to [**Se1**, p. 658]. The universal central extension $\bar{A}_5$ of A_5 fits in a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \langle \pm 1 \rangle & \longrightarrow & \bar{A}_5 & \xrightarrow{\delta} & A_5 \\ \| & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \langle \pm 1 \rangle & \longrightarrow & \mathrm{Spin}(5,\mathbb{Q}) & \longrightarrow & \mathrm{SO}(5,\mathbb{Q}) \end{array} \tag{2.4}$$

This is important for the determination of the universal 2-Frattini module of A_5.

A classical identification has A_5 equal to $\mathrm{PSL}_2(\mathbb{Z}/5)$. This allows us to identify $\bar{A}_5$ with $\mathrm{SL}_2(\mathbb{Z}/5)$. The first invariant of the universal Frattini cover of a group

G is the collection of ranks of the universal p-Frattini modules. In particular, we now show how to compute these. For A_5 these are the ranks of P_2, P_3 and P_5 with $\ker = P_2 \times P_3 \times P_5$ (§II.A). For any group G, if you compute the groups ${}_p\tilde{G}$ for $p \mid |G|$, then $\tilde{G}$ is the fiber product of these groups over G.

To orient to this problem, note A_5 has a cyclic 5-Sylow. Further,

$$\ker' \to \mathrm{PSL}_2(\mathbb{Z}_5) \to \mathrm{PSL}_2(\mathbb{Z}/5) = A_5 \tag{2.5}$$

is a Frattini cover. For example, combinatorially check that any lift of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ will generate $\mathrm{PSL}_2(\mathbb{Z}_5)$. Still, $\mathrm{PSL}_2(\mathbb{Z}_5)$ is not the universal 5-Frattini cover of A_5 (Remark 2.10). The adjoint representation of $\mathrm{PSL}_2(\mathbb{Z}_5)$ appears as

$${}_5S_c = \ker' / (\ker')^p[\ker', \ker'],$$

2×2 matrices of trace 0. Here $\mathrm{PSL}_2(\mathbb{Z}/5)$ acts by conjugation.

There are three conjugacy classes of A_5 of orders relatively prime to 5. Thus, (2.2a) says there are three simple $\dot{\mathcal{G}}$ modules when $p = 5$:

(2.6a) ${}_5S_a = \mathbf{1}$;
(2.6b) ${}_5S_b$, the standard degree 5 representation modulo $\mathbf{1}$; and
(2.6c) ${}_5S_c$ as above.

We explain ${}_5S_b$ further. Suppose G is a doubly transitive subgroup of S_n, and p is relatively prime to n. Then, the standard representation is a direct sum of the identity and an irreducible representation of degree $n-1$. When, however, $p|n$, the one dimensional space of G invariant vectors isn't a direct summand of the standard representation. Here, restriction of the degree 5 standard representation to the cyclic 5-Sylow gives its regular representation. From (2.2c) it is the principal indecomposable for the 4-dimensional simple representation. See Remark 2.10 for completion of this case.

Similarly, there are four simple $\dot{\mathcal{G}}$ modules when $p = 2$:

(2.7a) ${}_2S_a = \mathbf{1}$;
(2.7b) ${}_2S_b$, reduction modulo 2 of the degree 4 summand of the standard representation; and
(2.7c) ${}_2S'_c$ and ${}_2S''_c$, conjugate degree two representations from $A_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$.

The elements of the 2-Sylow of S_5 are representatives of the four nontrivial cosets of the stabilizer of 1 in the standard representation of A_5. Since these four nontrivial cosets span ${}_2S_b$, the 2-Sylow acts freely on it. Thus, (2.2c) says it is a projective indecomposable.

Simple representations for $p = 3$ follow those of (2.7) except use ${}_2S'_c$ and ${}_2S''_c$, reductions modulo 3 of the complex degree 3 representations. There is a standard procedure for this. Find a lattice L in the representation module invariant under G and form the quotient L/pL. For K a subgroup of A_5, denote $\mathrm{ind}_K^{A_5}(\mathbf{1})$ (of dimension $(A_5 : K)$) by $\mu_K(\mathbf{1})$.

PROPOSITION 2.4. *Take $p = 2$. Identify the normalizer of the subgroup $\langle(1\,2\,3\,4\,5)\rangle$ with the dihedral group $\mathbb{Z}/5 \times^s \langle\pm 1\rangle = H$. The universal 2-Frattini module of A_5 is the dimension 5 quotient $\mu_H(\mathbf{1})/\mathbf{1}$. Also, any Frattini cover of A_5 with 2-group kernel factors through $\bar{A}_5 \to A_5$.*

PROOF. Apply Lemma 2.3. Let $P_{\mathbf{1}}$ be the projective indecomposable of $\mathbf{1}$ for the prime $p = 2$. We show this is the induced module $\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}) \stackrel{\mathrm{def}}{=} N_{\mathbf{1}}$. Since $\mathbb{Z}/5$ has order relatively prime to 2, all modules for it are projective (Mashke's Theorem). From (2.2c), $\mu_H(\mathbf{1})$ is projective. It has $\mathbf{1}$ as the augmentation ideal quotient: a formal sum $\sum_{i=1}^t a_i\tau_i$ of cosets of $\mathbb{Z}/5$ maps to $\sum_{i=1}^t a_i$. We have only to show it is indecomposable.

Apply Frobenius reciprocity in the form

$$\mathrm{Hom}_{\mathbb{Z}/5}(\mathbf{1}, M_{|\mathbb{Z}/5}) = \mathrm{Hom}_{A_5}(\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}), M)$$

with M a simple A_5 module. By direct check on the simple A_5 modules in (2.7), the left side of this expression is of dimension 0 unless $M = \mathbf{1}$. Thus $\mu_H(\mathbf{1})$ has only one simple quotient and is indecomposable.

The composition series for $N_{\mathbf{1}}$ is in [**AJL**]. The Loewy display shows composition factors of $\dot{N}_{\mathbf{1}}$. We write this left to right instead of top to bottom:

$$(2.8)\qquad \begin{array}{ccccccc} & & {}_2\dot{S}'_c \to & \dot{\mathbf{1}} \to & {}_2\dot{S}''_c & & \\ & \nearrow & & & & \searrow & \\ \dot{\mathbf{1}} & & & & & & \dot{\mathbf{1}} \\ & \searrow & & & & \nearrow & \\ & & {}_2\dot{S}''_c \to & \dot{\mathbf{1}} \to & {}_2\dot{S}'_c & & \end{array}$$

Vertical columns show simple summands of $\mathrm{rad}(\dot{\mathcal{A}}_5)^i\dot{N}_{\mathbf{1}}/\mathrm{rad}(\dot{\mathcal{A}}_5)^{i+1}\dot{N}_{\mathbf{1}}$. The arrows indicate the indecomposables in $\dot{N}_{\mathbf{1}}/\mathrm{rad}(\dot{\mathcal{A}}_5)^{i+1}\dot{N}_{\mathbf{1}}$. Note: Such a display uniquely determines a module.

Also, the projective indecomposable $\dot{P}_{{}_2S'_c}$ corresponding to ${}_2\dot{S}'_c$ is uniserial:

$$(2.9a)\qquad {}_2\dot{S}'_c \to \mathbf{1} \to {}_2\dot{S}''_c \to \mathbf{1} \to {}_2\dot{S}'_c.$$

Lemma 2.3 lets us compute the universal 2-Frattini kernel from the map

$$(2.9b)\qquad \dot{P}_{{}_2S'_c} \oplus \dot{P}_{{}_2S''_c} \to {}_2S'_c \oplus {}_2S''_c.$$

Here, $\dot{P}_{{}_2S'_c} \oplus \dot{P}_{{}_2S''_c}$ covers the part of (2.8) to the left of the first column. The kernel from this has composition factors that identify it with $N_{\mathbf{1}}/\mathbf{1}$. Thus, the universal 2-Frattini kernel is $\mu_H(\mathbf{1})/\mathbf{1}$. From its composition series, the only simple quotient of $N_{\mathbf{1}}/\mathbf{1}$ by any A_5 invariant submodule is $\mathbf{1}$. This gives the last sentence of the proposition. $\square$

REMARK 2.5. *An exceptional property of A_5.* Applications of Part III use that all nontrivial 2-Frattini covers of A_5 factor through the universal central extension of A_5. We don't know which alternating groups have this property.

Not all do. Two standard series of simple groups come together when $n = 8$: $A_8 \cong \mathrm{SL}(4, \mathbb{Z}/2)$. For this, [Be] shows $H^2(A_8, M_4)$ has dimension 1 where M_4 is the standard 4 dimensional representation of $\mathrm{SL}(4, \mathbb{Z}/2)$. This gives an extension of A_8 that doesn't factor through the universal central extension of A_8. $\square$

§II.D. Inductive construction of ${}^n_p\tilde{G}$. Continue notation of §II.B. Use $\phi_n : {}^n_p\tilde{G} \to G$ for the natural map. As in §II.B, $\ker_n / \ker_{n+1}$ is ${}^n_p\Omega^2(\mathbf{1})$.

LEMMA 2.6. *Conjugacy classes in G of elements of orders prime to p correspond one-one to such conjugacy classes in ${}^n_p\tilde{G}$. In particular, there is a natural one-one correspondence between simple G modules and simple ${}^n_p\tilde{G}$ modules. Further, suppose M is a simple G, or ${}^n_p\tilde{G}$, module. Let P_M be the principal indecomposable for M as a G-module. Then, P_M is a quotient of the principal indecomposable ${}^n_pP_M$ for M as a ${}^n_p\tilde{G}$ module.*

PROOF. Take $g \in G$ of order prime to p. Let H_g be the subgroup $\phi_n^{-1}(\langle g \rangle)$ in ${}^n_p\tilde{G}$. We have an exact sequence $\ker_n / \ker_{n+1} \to H_g \to \langle g \rangle$. By Schur-Zassenhaus, this sequence splits, uniquely up to conjugation. So, elements over g, of the same order as g, are all conjugate. Also, ϕ_n maps elements in ${}^n_p\tilde{G}$ of order prime to p to elements of the same order in G. This proves the first part.

Let M be a simple G module. Then, M is a ${}^n_p\tilde{G}$ module through ϕ_n. Therefore, it has no proper ${}^n_p\tilde{G}$ module; such would be a proper G submodule. From the first part of the lemma, (2.2a) says ${}^n_p\tilde{G}$ and G have the same number of simple modules. Thus, we have a natural correspondence between them.

Consider the last statement of the lemma. The homomorphism $P_M \to M$ is also a ${}^n_p\tilde{G}$ module homomorphism. So, the projective ${}^n_p\tilde{G}$ module ${}^n_pP_M$ has a map $\psi : {}^n_pP_M \to P_M$ commuting with the maps to M. This is surjective: the quotient of P_M by its radical (as either a G or ${}^n_p\tilde{G}$ module) is just M. $\square$

Lemma 2.3 shows how to construct the group ${}^n_p\tilde{G}$ inductively in n. In particular, $\mathrm{Ext}^2_{{}^n_p\tilde{G}}(\mathbf{1}, \Omega^2(\mathbf{1})) = \mathrm{Ext}^1_{{}^n_p\tilde{G}}(\Omega^1(\mathbf{1}), \Omega^2(\mathbf{1}))$. These modules are the natural ${}^n_p\tilde{G}$ modules from §II.B. We construct ${}^{n+1}_{\ p}\tilde{G}$ given solid information on the following short exact sequences of ${}^n_p\tilde{G}$ modules.

(2.10a) $1 \to \Omega^2(\mathbf{1}) \to P \to \Omega^1(\mathbf{1}) \to 1$, P the minimal projective ${}^n_p\tilde{G}$ module covering $\Omega^1(\mathbf{1})$.

(2.10b) $1 \to \Omega^1(\mathbf{1}) \to P_{\mathbf{1}} \to \mathbf{1} \to 1$.

Here, $P_{\mathbf{1}}$ is the principal indecomposable for $\mathbf{1} = \mathbf{1}_{{}^n_p\tilde{G}}$. Compute boundary maps from the standard exact sequences of cohomology:

$$H^0({}^n_p\tilde{G}, \mathbf{1}) \xrightarrow{\delta_0} H^1({}^n_p\tilde{G}, \Omega^1(\mathbf{1})) \xrightarrow{\delta_1} H^2({}^n_p\tilde{G}, \Omega^2(\mathbf{1})). \tag{2.11}$$

Let $1_{\mathbf{1}}$ be a vector space generator of $\mathbf{1}$.

PROPOSITION 2.7. *The element* $\delta_1 \circ \delta_0(1_{\mathbf{1}}) \in H^2({}^{\,n}_{p}\tilde{G}, \Omega^2(\mathbf{1}))$ *represents a group extension* ${}^{n+1}_{\;\;p}\tilde{G}$ *whose class generates* $H^2({}^{\,n}_{p}\tilde{G}, \Omega^2(\mathbf{1}))$. *To be explicit, consider the semi-direct product* $\Omega^1(\mathbf{1}) \times^s {}^{\,n}_{p}\tilde{G}$. *Choose* $m \in P_{\mathbf{1}}$ *lying over* $1_{\mathbf{1}}$. *The cocycle* $g \mapsto g(m) - m$ *for* $g \in G$ *represents* $\delta_0(1_{\mathbf{1}})$. *This cocycle defines a splitting* $\psi : {}^{\,n}_{p}\tilde{G} \to \Omega^1(\mathbf{1}) \times^s {}^{\,n}_{p}\tilde{G}$ *by* $g \mapsto (g(m) - m, g)$. *Then,* ${}^{n+1}_{\;\;p}\tilde{G}$ *is the preimage in* $P \times^s {}^{\,n}_{p}\tilde{G}$ *of* $\psi({}^{\,n}_{p}\tilde{G})$ *in* $\Omega^1(\mathbf{1}) \times^s {}^{\,n}_{p}\tilde{G}$ *from sequence* (2.10a).

PROOF. Follow standard computations for boundary maps. For example, check that ψ defines a homomorphism by computing $\psi(g_1 g_2)$ as

$$((g_1g_2)(m) - m, g_1g_2) = ((g_1g_2)(m) - g_1(m) + g_1(m) - m, g_1g_2) = \psi(g_1)\psi(g_2).$$

The essence of identifying ${}^{n+1}_{\;\;p}\tilde{G}$ is to show pullback of $\psi({}^{\,n}_{p}\tilde{G})$, as an extension of ${}^{\,n}_{p}\tilde{G}$, has the correct 2-cocycle. Suppose α represents a 1-cocycle. Then, $g \mapsto (\alpha(g), g)$ gives a splitting of ${}^{\,n}_{p}\tilde{G}$ in $\Omega^1(\mathbf{1}) \times^s {}^{\,n}_{p}\tilde{G}$. For each $g \in {}^{\,n}_{p}\tilde{G}$ let $\bar{\alpha}(g)$ be an element of P lying over $\alpha(g) \in \Omega^1(\mathbf{1})$. The boundary map *differentiates* the 1-cycle $g \mapsto \alpha(g)$ to give

$$(g_1, g_2) \mapsto g_1(\bar{\alpha}(g_2)) - \bar{\alpha}(g_1g_2) + \bar{\alpha}(g_1).$$

[**N**, p. 241] shows this 2-cocycle is the factor system for the associative multiplication on the pullback group. □

§II.E. Explicit computation of $\frac{1}{2}\tilde{A}_5$**.** This subsection applies Prop. 2.7 to A_5 to construct its universal exponent 2-Frattini cover $\frac{1}{2}\tilde{A}_5$. Then, §II.F displays the whole universal 2-Frattini cover. The two processes use different principles. For much work, we need ${}_p\tilde{G}$, even if this doesn't reveal the fine tuning. Still, it is comforting to get the detail in ${}^{\,n}_{p}\tilde{G}$ we illustrate with $\frac{1}{2}\tilde{A}_5$. This requires explicit exact sequences for (2.10). From Prop. 2.4, $\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}) \stackrel{\text{def}}{=} P_{\mathbf{1}}$ is the projective indecomposable of $\mathbf{1}$. Identify this with linear functionals, $\mathrm{Hom}_{\mathbb{F}_2[\mathbb{Z}/5]}(\mathbb{F}_2[A_5], \mathbb{F}_2)$, on right cosets of $\mathbb{Z}/5$ in A_5. Here, $g \in A_5$ acts on the left of $\phi \in P_{\mathbf{1}}$ by $g(\phi)(x) = \phi(x \cdot g^{-1})$ for $x \in \mathbb{F}_2[A_5]$. Let ϕ_1 take the coset of 1 to 1, and the other cosets to 0. Following Prop. 2.7, form the section

$$\psi : A_5 \to \Omega^1(\mathbf{1}) \times^s A_5 \text{ by } g \mapsto (g(\phi_1) - \phi_1, g). \tag{2.12}$$

The next theorem gives P with an explicit map to $\Omega^1(\mathbf{1})$ to complete identification of $\frac{1}{2}\tilde{A}_5$ from (2.10b).

Choice of P. Our identification of $\frac{1}{2}\tilde{A}_5$ will have kernel an $\mathbb{F}_2$ module. So, we reduce scalars on the module ${}_2S'_c$ in (2.7c) to $\mathbb{F}_2$. This gives a $\mathcal{G} = \mathbb{F}_2[A_5]$ module ${}_2S_c$ whose $\bar{\mathbb{F}}_2$ tensor is ${}_2S'_c \oplus {}_2S''_c$.

Thus, (2.8) and (2.9) give the Loewy display of the projective indecomposables $P_{\mathbf{1}} = \mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1})$ and $P_{{}_2S_c}$ for $\mathbf{1}$ and ${}_2S_c$ respectively. Precisely:

$$\mathbf{1} \;\to\; {}_2S_c \;\to\; \begin{matrix}\mathbf{1}\\ \oplus\\ \mathbf{1}\end{matrix} \;\to\; {}_2S_c \;\to\; \mathbf{1}$$

and

$${}_2S_c \;\to\; \begin{matrix}\mathbf{1}\\ \oplus\\ \mathbf{1}\end{matrix} \;\to\; {}_2S_c \;\to\; \begin{matrix}\mathbf{1}\\ \oplus\\ \mathbf{1}\end{matrix} \;\to\; {}_2S_c$$

Let the kernel of the natural augmentation map $P_{\mathbf{1}} \to \mathbf{1}$ be $M_{\mathbf{1}}$. Thus, P is the projective indecomposable for ${}_2S_c$. From (2.9b), the universal 2-Frattini kernel is the kernel of the natural map $P \to \ker(P_{\mathbf{1}} \to \mathbf{1})$. Use the modules ${}_2S_b$ from (2.7b) and ${}_2S'_c$ from (2.7c). Let $\mathbb{M}(2,F)$ be 2×2 matrices with entries in F. The set of trace 0 matrices is $\mathbb{M}(2,F)_0$. With $F = \mathbb{F}_4$, both are $A_5 \cong \mathrm{SL}(2,\mathbb{F}_4)$ modules via conjugation. Here $\mathbf{O}$ is the zero element in this additive group.

Theorem 2.8. *The following properties hold.*

(2.13a) *P is isomorphic to reduction of scalars of ${}_2S'_c \otimes_{\mathbb{F}_4} {}_2S_b$ to $\mathbb{F}_2$.*

(2.13b) *The submodule of $P/{}_2S_c$ with Loewy display $\mathbf{1}\oplus\mathbf{1} \to {}_2S_c$ is isomorphic to $\mathbb{M}(2,\mathbb{F}_4)_0$.*

(2.13c) *For any $A \in \mathbb{M}(2,\mathbb{F}_4)_0$ with $A \neq \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right) A \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, the element*

$$B \stackrel{\text{def}}{=} \left(A, \begin{pmatrix}1&1\\0&1\end{pmatrix}\right) \in \mathbb{M}(2,\mathbb{F}_4)_0 \times^s \mathrm{SL}(2,\mathbb{F}_4) \quad \textit{is of order 4.}$$

(2.13d) *Any B in (2.13c) and $(\mathbf{O},(1\,2\,3\,4\,5))$ generate a subgroup G' isomorphic to G of $\mathbb{M}(2,\mathbb{F}_4)_0 \times^s \mathrm{SL}(2,\mathbb{F}_4)$. This is a section coming from (2.12).*

In particular, the pullback of G' to $P \times^s A_5$ is an explicit identification of ${}_2\bar{A}_5$.

Proof. From previous comments, (2.13a–d) gives the last line. (2.13c) is a trivial check. We show the others in order.

(2.13a) holds. Since ${}_2S_b$ is a projective $\bar{\mathbb{F}}_2[A_5]$ module, so is ${}_2S'_c \otimes_{\mathbb{F}_4} {}_2S_b$ ([**A**, p. 47, Lemma 4] or use a similar statement with free replacing projective). Thus, this 8 dimensional (over $\mathbb{F}_4$) module is a sum of projective indecomposables. From (2.7), either it is ${}_2S_b \oplus {}_2S_b$, or its reduction of scalars to $\mathbb{F}_2$ is the projective indecomposable P for ${}_2S_c$. We show the former can't happen.

Let $\alpha \in A_5$ be of order 3. Its trace, $\mathrm{Tr}_4(\alpha)$, on ${}_2S_b$ is 1. For a basis of ${}_2S'_c$ take eigenvectors of α. The trace of α on ${}_2S'_c \otimes_{\mathbb{F}_4} {}_2S_b$ is $(\lambda+\lambda^{-1})\mathrm{Tr}_4(\alpha)$. Here, λ generates $\mathbb{F}_4^*$. This is different from $2\mathrm{Tr}_4(\alpha)$; (2.13a) holds.

(2.13b) holds. In analogy to (2.5), $\mathbb{M}(2,\mathbb{F}_4)_0$ is the adjoint representation of $A_5 = \mathrm{SL}_2(\mathbb{F}_4)$. So, it is indecomposable. It has a 2-dimensional irreducible quotient: $\left(\begin{smallmatrix}0&0\\1&0\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0&1\\0&0\end{smallmatrix}\right)$ generate this modulo the 1-dimensional subspace of scalar matrices. It is then a quotient of P. The result follows from the Loewy display of P in (2.9b).

(2.13d) HOLDS. The group B and $(\mathbf{O}, (1\,2\,3\,4\,5))$ generate has A_5 as a quotient. Check: B^2 generates the kernel of the quotient map. This requires knowing you can't split off A_5 in this group. Any element of order 2 (they are all conjugate) and $(1\,2\,3\,4\,5)$ generate A_5. It suffices to note lifts of elements of order 2 are of order 4. $\square$

§II.F. Displaying the universal p-Frattini cover. Suppose G is a semidirect product $H \times^s K$ with $(|H|, |K|) = 1$. Then, for each prime p dividing $|G|$, ${}_p\tilde{G}$ is ${}_p\tilde{H} \times^s {}_p\tilde{K}$ [**Ri**, Thm. 3.2]. (If $(p, |G'|) = 1$ the universal p-Frattini cover of G' is just G'.) Suppose $p \,|\, |K|$. So, the action of ${}_p\tilde{K}$ on H is induced from K acting on H. On the other hand, suppose $p \,|\, |H|$. Explicitly extending the action of K from H to ${}_p\tilde{H}$ may require some cleverness (Remark 2.10 gives an easy example). Conclude from the Schur-Zassenhaus lemma, we know the universal p-Frattini cover of a group G when its p-Sylow Q_p is normal. Suppose the rank of Q_p is t. Let $\hat{F}_t^{(p)}$ be the free pro-p group on t generators. Then, $G \cong Q_p \times^s G/Q_p$ and ${}_p\tilde{G} \cong \hat{F}_t^{(p)} \times^s G/Q_p$.

Consider any finite group G, $p \,|\, |G|$, and a p-Sylow Q_p of G. Let $N_G(Q_p) = G'$ be the normalizer of Q_p in G. From above, the universal p-Frattini cover of G' is $\hat{F}_t^{(p)} \times^s G'/Q_p$. Let $\ker_0'$ be the kernel of $\hat{F}_t^{(p)} \to Q_p$. This is a free group on $1 + (t-1)|Q_p|$ generators [**FrJ**, p. 195]. As in §II.A, form $\ker_n'$, $n = 1, \dots$. Then, $M' = \ker_0' / \ker_1'$ is a G' module of rank $1 + (t-1)|Q_p|$. Finally, let $\phi^{-1}(G')$ be the pullback of G' in the universal p-Frattini cover ${}_p\tilde{G} \to G$.

PROPOSITION 2.9. *There is a surjective homomorphism $\psi : \phi^{-1}(G') \to {}_p\tilde{G}'$. Suppose the rank of $\ker_0' / \ker_1'$ equals the rank of $\ker_0 / \ker_1$. Then, ψ is an isomorphism. In particular, this holds when $G = A_5$ and $p = 2$.*

PROOF. Both $\phi^{-1}(G')$ and ${}_p\tilde{G}'$ are semidirect products of a free pro-p group and G'/Q_p. Both have natural maps to G'. As the universal Frattini cover is the minimal projective group covering G' [**FrJ**, loc. sit.], ${}_p\tilde{G}'$ is the minimal group with these properties. Thus, ψ exists. The ranks of $\ker_0 / \ker_1$ and $\ker_0' / \ker_1'$ determine the respective ranks of $\ker_0$ and $\ker_0'$. Thus, the hypothesis says the latter two have the same ranks. A surjective map of isomorphic pro-p groups is an isomorphism [**FrJ**, Prop. 15.3].

We show these hypotheses hold for $G = A_5$ and $p = 2$. The normalizer of the 2-Sylow in A_5 is $G' = A_4$, the subgroup of order 12. The rank of $\ker_0'$ is five, the same as the rank of $\ker_0$ (Prop. 2.4). $\square$

REMARK 2.10. *Intuitive approach to identifying Frattini kernels.* Use the notation before Prop. 2.9 for $N_G(Q_p) = G'$, etc. Then, $\ker_0' / \ker_1' = M'$ is a G' module. Yet, it may not be a natural G module. The induced module (top of Part II), $M = \mathrm{ind}_{G'}^{G}(M')$, always is a G module. Apply Shapiro's Lemma: $H^2(G,M) = H^2(G',M')$. Let $\alpha \in H^2(G',M')$ define the natural p-Frattini extension of G' by $\ker_0' / \ker_1'$. Thus, use α to define an extension $\tilde{G}^* \to G$ with kernel M. This is a valuable extension. It isn't, however, always the universal p-Frattini module.

For example, when $G = A_5$ and $p = 2$, M' (resp., M) has dimension 5 (resp., 25). Prop. 2.9 explains this case; M' is a G module.

When, however, $p = 5$, the dihedral group normalizing the cyclic 5-Sylow in A_5 has index 6. Apply Frobenius reciprocity (proof of Prop. 2.4) to see $\mathrm{ind}_{G'}^{G}(\mathbb{Z}/5)$ has Loewy display ${}_5S_c \to {}_5S_c$ (as in (2.6c)). This is $\ker_0 / \ker_1$ when $p = 5$.

Finally: How can we answer serious questions about ${}_2\tilde{A}_5 = \tilde{G}$ from Prop. 2.4? Take for example the Loewy display of $\ker_n / \ker_{n+1}$. Restrict the action of ${}_2^n\tilde{G}$ to ${}_2^n\tilde{G}'$ to consider the Loewy display of $\ker_n / \ker_{n+1}$. The action of $G'/Q_p = \mathbb{Z}/3$ is completely reducible (Mashke's Theorem). Suppose we know the action of $\ker_0 / \ker_n$ on $\ker_n / \ker_{n+1}$. Then, we can find the G'/Q_p modules in this if we have explicit action of G'/Q_p on the generators of $\hat{F}_t^{(p)}$. That is, let $\boldsymbol{v}_1, \dots, \boldsymbol{v}_t$ be a basis for $\ker_0 / \ker_1 = M$. Consider just the case where G'/Q_p is cyclic (as in ${}_2A_5$). Let A be a matrix representing the action of a generator of this group on M. Lift this to a t-tuple of words $w(\boldsymbol{v}_1, \dots, \boldsymbol{v}_t)_1, \dots, w(\boldsymbol{v}_1, \dots, \boldsymbol{v}_t)_t$ that induces an automorphism $\tilde{A}$ of the same order on the group generated freely by $\boldsymbol{v}_1, \dots, \boldsymbol{v}_t$. Example: $(\boldsymbol{v}_1, \boldsymbol{v}_2) \mapsto (\boldsymbol{v}_2^{-1}, \boldsymbol{v}_1\boldsymbol{v}_2^{-1})$ gives an element of order 3. The last step is to decipher the G modules from the G' modules. For the case of discussion, this appears feasible. $\square$

PART III. FOUNDATIONS OF MODULAR TOWERS

§I.A, and §I.D–E remind us the modular curve $X_0(p)$ for p a prime is a *moduli space*. It parametrizes degree p covers $E \to E'$ of genus 1 curves that have $\mathbb{Z}/p$ as geometric monodromy group. Such a cover arises canonically from a genus 0 degree p cover $X \to \mathbb{P}^1$ having four involutions in D_p for branch cycles. Thus, a moduli space $\mathcal{H} = \mathcal{H}(D_p, \mathbf{C}_4)$ of such genus 0 covers has more data than does $X_0(p)$. Note: Neither the genus 0 covers nor the cover of the j-line by X_0 are Galois covers. We remind how conjugacy classes in a finite group G produce *Hurwitz* moduli spaces. Versions of this appear in [**Fr5**] and [**FrV**].

Consider a prime p dividing $|G|$. Let $\mathbf{C}$ be conjugacy classes of G of order prime to p. Then, §III.C constructs the spaces $\{\mathcal{H}_n = \mathcal{H}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}}), \mid n = 0, 1, \dots\}$ attached to the characteristic quotients of ${}_p\tilde{G}$. §III.D produces an invariant $\nu(G,p,\mathbf{C})$ on which $G_{\mathbb{Q}}$ acts through the p-cyclotomic character. We apply this to a recurring example where G is an alternating group.

In some groups there are primes p exceptional for this process: conjugacy classes in G of order prime to p don't generate G. We say these primes are *exceptionally ramified* (§III.E). §III.F returns to the main technical topic behind this paper: finding fields of definition of components of a modular tower. Cor. 3.23, in particular, shows that each level of certain modular towers for a perfect group contains an absolutely irreducible variety over $\mathbb{Q}$. Finally, the Appendix discusses problems from our main themes. These motivate our next installment (Parts IV and V) of modular towers.

The number of branch points, r, of a cover $X \to \mathbb{P}^1$ is always at least 3. Consider any cover $\phi : W \to V$ with field of definition K. Denote the set of geometric points that lie over $v_0 \in V$ by $\phi^{-1}(v_0)$. The absolute Galois group G_L of the field $L = K(v_0)$ acts on $\phi^{-1}(v_0)$. Suppose G is any group acting on this fiber. The *decomposition* group D_{w_0}, $w_0 \in \phi^{-1}(v_0)$ is the (sub)group of G that preserves the orbit of G_L. The traditional situation has $\phi : W \to V$ a Galois cover of normal varieties and G is the Galois group. If the cover isn't Galois, go to the Galois closure $\hat{W} \to V$ (§I.G). Then, choose any point $\hat{w}_0 \in \hat{W}$ over v_0. Declare D_{w_0} to be the decomposition group of v_0. The abuse is this only defines the decomposition group up to conjugacy in G.

§III.A. Data for Hurwitz spaces attached to G. Let G be a *transitive* subgroup of S_n and let $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ be an r-tuple of nontrivial conjugacy classes of G. Some may occur several times. We often equip G with a faithful transitive permutation representation $T : G \to S_n$. Then $G(1)$ denotes the subgroup of $G \le S_n$ stabilizing 1. Sometimes this is the regular representation, often it is not (§III.C).

Definition 3.1a. To the data $(G, \mathbf{C})$ associate its *Nielsen class*:

$$\begin{aligned}\mathrm{Ni}(G,\mathbf{C}) = \mathrm{Ni}(\mathbf{C}) = \{&\mathbf{g} \in G^r \mid \langle \mathbf{g} \rangle = G,\ g_1 \cdots g_r = 1 \\ &\text{and there exists } \omega \in S_r, g_{(i)\omega} \in \mathrm{C}_i, i = 1, \dots, r\}.\end{aligned}$$

Occasions will arise when $\mathrm{Ni}(G,\mathbf{C})$ is empty. Still, unless we say otherwise, assume it is nonempty. There are several variants to $\mathrm{Ni}(G,\mathbf{C})$. Equivalence relations on $\mathrm{Ni}(\mathbf{C})$ and its variants produce moduli spaces related as are $X_0(n)$ and $X_1(n)$. Let $N_{S_n}(\mathbf{C})$ be the subgroup of S_n that normalizes G and permutes the conjugacy classes in $\mathbf{C}$. Suppose the embedding of G in S_n is the regular representation. Then, $N_{S_n}(\mathbf{C})$ acts by conjugation through the full subgroup of automorphisms of G permuting the conjugacy classes in $\mathbf{C}$.

Definition 3.1b. Let G' be a group between G and $N_{S_n}(\mathbf{C})$. Associate to $(G, G', \mathbf{C})$ its G'-Nielsen class $\mathrm{Ni}(\mathbf{C})/G'$: the quotient of $\mathrm{Ni}(\mathbf{C})$ by the conjugation action of G'. There is a special notation for $\mathrm{Ni}(G,\mathbf{C})/N_{S_n}(\mathbf{C})$, $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{ab}}$, and for $\mathrm{Ni}(G,\mathbf{C})/G$, $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$.

Suppose a cover $\phi : X \to \mathbb{P}^1$ has any branch cycle description $\mathbf{g}$, 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.

DEFINITION 3.2. *Rational union of conjugacy classes.* Consider the union $S = \cup_{i=1}^r \mathrm{C}_i$ of elements in all conjugacy classes of $\mathbf{C}$. Let N be the least common multiple of all elements in S. Suppose $(a, N) = 1$. Let S^a be the set of a powers of elements of S. We say $\mathbf{C}$ is a *rational union* of conjugacy classes if $S^a = S$ for all $(a, N) = 1$.

Nielsen classes address the existence of a space representing this *moduli problem*. Parametrize equivalence classes of covers in a given Nielsen class. There are, however, immediate subtleties. To assure exactly one point of the space represents each equivalence class of covers, we must equivalence branch cycles descriptions by the action of $N_{S_n}(\mathbf{C})$. That is, constructions for this space use $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$. Even then, this is only a *coarse* moduli space unless representing covers have no automorphisms.The exact condition for this is $G(1)$ is self-normalizing (in G) [**Fr5**, §4]. Arithmetic matters require using such a *fine* moduli space. Thus, the self-normalizing condition appears in Addendum 3.4. No suitable replacement for it holds if G has a non-trivial center. The moduli problem for realizing groups as Galois groups of regular extensions over $\mathbb{Q}$ must take account of the Galois closure of a cover and the corresponding automorphisms. The moduli space that keeps book on automorphisms of a cover uses $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$. For Galois group realization over $\mathbb{Q}$ the Branch Cycle Argument (see the proof of Part A in Theorem 3.16) requires $\mathbf{C}$ is a rational union of conjugacy classes. Theorem 3.4 summarizes basic moduli properties under this assumption ([**DFr**, §4], [**Fr5**, §4 and 5] or [**FrV**, Prop. 3]).

Hurwitz monodromy action interprets properties of moduli spaces attached to Nielsen classes. We explain the monodromy action. Consider the free group on generators Q_i, $i = 1, \ldots, r-1$, with these relations:

$$(3.1a) \qquad Q_i Q_{i+1} Q_i = Q_{i+1} Q_i Q_{i+1}, \ i = 1, \ldots, r-2;$$

$$(3.1b) \qquad Q_i Q_j = Q_j Q_i, \ |i-j| > 1; \text{ and}$$

$$(3.1c) \qquad Q_1 Q_2 \cdots Q_{r-1} Q_{r-1} \cdots Q_1 = 1.$$

Conditions (3.1a) and (3.1b) define the *Artin braid group*. The full set defines the *Hurwitz monodromy group* H_r of degree r as a quotient of the braid group. The Q_i s act on $\mathbf{g} \in \mathrm{Ni}(\mathbf{C})$ by this formula:

$$(3.1\mathrm{d}) \qquad (\mathbf{g})Q_i = (g_1, \ldots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \ldots, g_r), \ i = 1, \ldots, r-1.$$

This action commutes with conjugation by any element of $N_{S_n}(\mathbf{C})$. Thus, it induces a permutation representation of H_r on $\mathrm{Ni}(\mathbf{C})$ and its quotients in Def. 3.1b: Hurwitz monodromy action on the Nielsen class.

The fundamental group of $\mathbb{P}^r \setminus D_r$ is H_r. Thus, each orbit O of H_r on $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ (resp., on $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$) produces an irreducible unramified cover $\mathcal{H}_O^{\mathrm{in}}$ (resp., $\mathcal{H}_O^{\mathrm{ab}}$) of $\mathbb{P}^r \setminus D_r$. Further, this produces a natural unramified *Galois* cover $\Psi_O : \mathcal{H}_O^{\mathrm{in}} \to \mathcal{H}_O^{\mathrm{ab}}$

(see Th. 3.4). We use O for its image in $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$. This can be an abuse of notation: different orbits of H_r on $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ may be the same in $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$.

Denote the disjoint union of $\mathcal{H}_O^{\mathrm{in}}$ over the orbits of $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ by $\mathcal{H}(\mathbf{C})^{\mathrm{in}}$. Use a similar notation, $\mathcal{H}(\mathbf{C})^{\mathrm{ab}}$, for the disjoint union of $\mathcal{H}_O^{\mathrm{ab}}$ over the orbits of $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$. Theorem 3.4 includes the main application of the assumption of transitivity of H_r on Nielsen classes. Lemma 3.3 applies in Theorem 3.4 to show orbits of the braid action on $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ and on $\mathrm{Ni}(\mathbf{C})$ are the same. We also use it in the main result of §III.F.

LEMMA 3.3 [**BFr**, Lemma 3.8]. *Consider* $\mathbf{g} \in \mathrm{Ni}(\mathbf{C})$. *Suppose there are consecutive integers* $i, i+1, \dots, j \bmod r$ *with* $g_i \cdot g_{i+1} \cdots g_j = 1$. *(This includes* $i, i+1, \dots, r-1, r, 1, 2, \dots$.*) Let* $\gamma \in \langle g_i, \dots, g_j\rangle$. *Then, there is* $Q \in H_r$ *with*

$$(\mathbf{g})Q = (g_1, \dots, g_{i-1}, \gamma g_i \gamma^{-1}, \dots, \gamma g_j \gamma^{-1}, g_{j+1}, \dots). \tag{3.2}$$

The following rephrases [**FrV**, Th. 1]. It contains three major assumptions, (3.3a)–(3.3c). §III.B inspects these more closely. The decomposition group $D_{\boldsymbol{p}}$ for $\boldsymbol{p} \in \mathcal{H}^{\mathrm{ab}}$ is one of the conjugacy class of decomposition groups $D_{\hat{\boldsymbol{p}}}$ for $\hat{\boldsymbol{p}} \in \mathcal{H}^{\mathrm{in}}$ over $\boldsymbol{p}$. (See top of Part III.) Recall: The outer automorphism group $\mathrm{Out}(G)$ is the automorphisms of G modulo the group of inner automorphisms. Conjugation of $N_{S_n}(\mathbf{C})$ on G gives a natural map into $\mathrm{Out}(G)$. For any orbit of H_r on $\mathrm{Ni}(G, \mathbf{C})$, denote the subgroup of $N_{S_n}(\mathbf{C})$ that stabilizes the whole set O by $N_O(\mathbf{C})$. Denote its image in $\mathrm{Out}(G)$ by $N_O^{\mathrm{out}}(\mathbf{C})$ and the image of $N_{S_n}(\mathbf{C})$ in $\mathrm{Out}(G)$ by $N_{\mathrm{in}}^{\mathrm{out}}(\mathbf{C})$.

THEOREM 3.4. *The* H_r*-orbits on* $\mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$ *correspond one-one to the* H_r*-orbits on* $\mathrm{Ni}(\mathbf{C})$. *Let* O *be such an orbit. Restrict attention to* $\Psi_O : \mathcal{H}_O^{\mathrm{in}} \to \mathcal{H}_O^{\mathrm{ab}}$. *Over* $\mathbb{C}$, Ψ_O *is a Galois cover with group* $N_O^{\mathrm{out}}(\mathbf{C})$. *Assume the following.*

(3.3a) *G has trivial center:* **center condition**.
(3.3b) *$\mathbf{C}$ is a rational union of conjugacy classes:* **rationality condition**.
(3.3c) *H_r is transitive on* $\mathrm{Ni}(\mathbf{C})$ *(so* $O = \mathrm{Ni}(\mathbf{C})^{\mathrm{in}}$*):* **transitivity condition**.

Then, the following hold.

(3.4a) $\Psi : \mathcal{H}^{\mathrm{in}} \to \mathcal{H}^{\mathrm{ab}}$ *is a Galois cover of absolutely irreducible varieties over* $\mathbb{Q}$, *with automorphisms defined over* $\mathbb{Q}$ *and group* $N_{S_n}(\mathbf{C})/G$.
(3.4b) *Any point* $\boldsymbol{p} \in \mathcal{H}^{\mathrm{ab}}$ *and* $\hat{\boldsymbol{p}} \in \mathcal{H}^{\mathrm{in}}$ *over* $\boldsymbol{p}$, *produces a Galois field extension* $L'_{\boldsymbol{p}}/\mathbb{Q}(\boldsymbol{p})(x)$ *with the algebraic closure of* $\mathbb{Q}(\boldsymbol{p})$ *in* $L'_{\boldsymbol{p}}$ *equal to* $\mathbb{Q}(\hat{\boldsymbol{p}})$.
(3.4c) *The data of* (3.4b) *produces an exact sequence of groups as in* (1.1)

$$1 \to G = G(L'_{\boldsymbol{p}}/\mathbb{Q}(\hat{\boldsymbol{p}})(x)) \to G(L'_{\boldsymbol{p}}/\mathbb{Q}(\boldsymbol{p})(x)) \to G(\mathbb{Q}(\hat{\boldsymbol{p}})/\mathbb{Q}(\boldsymbol{p})) \to 1.$$

(3.4d) $G(L'_{\boldsymbol{p}}/\mathbb{Q}(\boldsymbol{p})(x))$ *in* (3.4c) *is a subgroup* H *of* $N_{S_n}(\mathbf{C})$ *for which no element of* $H \setminus G$ *centralizes* G. *Also, the decomposition group* $D_{\boldsymbol{p}}$ *in* Ψ *is* H/G.

The set $\boldsymbol{p} \in \mathcal{H}^{\mathrm{in}}(\bar{\mathbb{Q}})$ *with* $D_{\boldsymbol{p}} = N_{\mathrm{in}}^{\mathrm{out}}(\mathbf{C})$ *in* (3.4d) *is dense in the complex topology.*

Proof. The first sentence follows from Lemma 3.3 with $i = 1$ and $j = r$. Hilbert's irreducibility theorem gives the last sentence as in the argument of Theorem 1.1. Explanation of (3.4d): The condition on H is a statement about the Galois closure process for an extension $L/\mathbb{Q}(x)$ and not pure group theory [**Fr1**, Prop. 2] or [**Fr6a**, §4]. Everything else is from [**FrV**, Th. 1]. □

The Hurwitz spaces $\mathcal{H}^{\mathrm{ab}}$ are as important as $\mathcal{H}^{\mathrm{in}}$. The following addendum clarifies the role of the points of (3.4c), $\boldsymbol{p} \in \mathcal{H}^{\mathrm{ab}}$. It rephrases [**FrV, Cor. 1**]. It would be valuable for applications to go beyond (3.5) in supporting the conclusion of the Addendum. As before, $G(1)$ is the stabilizer of 1 in $G \leq S_n$.

Addendum to Theorem 3.4. *Assume* (3.3a)–(3.3c). *Also, assume either*

(3.5a) $G(1)$ *is the trivial group, or*

(3.5b) *the normalizer of* $G(1)$ *in* G *is just* $G(1)$.

Then, $\boldsymbol{p} \in \mathcal{H}^{\mathrm{ab}}$ *produces a degree* n *field extension,* $L^{\mathrm{ab}}/\mathbb{Q}(\boldsymbol{p})(x)$, *regular over* $\mathbb{Q}(\boldsymbol{p})$. *It is unique up to isomorphism over* $\mathbb{Q}(\boldsymbol{p})(x)$. *Further, its Galois closure gives the field* $L'_{\boldsymbol{p}}$ *in* (3.4c).

Here is a final word of caution. We aren't interested in the minimal field of definition of $\mathcal{H}_O^{\mathrm{in}} \to \mathbb{P}^r \setminus D_r$ (resp., $\mathcal{H}_O^{\mathrm{ab}} \to \mathbb{P}^r \setminus D_r$) as a pure cover. The goal is a model for such a cover whose points represent solutions for a specific moduli problem. For $\mathcal{H}_O^{\mathrm{ab}}$ the problem is finding representative covers in the given orbit of H_r on the Nielsen class. Then, $\mathcal{H}_O^{\mathrm{in}}$ adds to this finding a Galois cover with given automorphisms. See §App.C, especially between (C.8) and Theorem C.3, for further discussion on when the model satisfies properties (3.4b-c) and the conclusion of Add. to Th. 3.4.

§III.B. Weakening the hypotheses of Theorem 3.4. [**FrV**] shows any finite group G has a covering group G' and a collection of conjugacy classes $\mathbf{C}'$ of G' satisfying all conditions of (3.3). Given the other conditions, it is a minor issue to relax the rationality condition (3.3b). Thus, we continue using this simplifying assumption. Crucial applications, however, require us to go beyond transitivity condition (3.3c). Suppose the following holds instead of (3.3c), and we still have (3.3a) and (3.3b).

(3.4)′ There exists an H_r orbit O for which $\Psi : \mathcal{H}_O^{\mathrm{in}} \to \mathcal{H}_O^{\mathrm{ab}}$ is a Galois cover of absolutely irreducible varieties over $\mathbb{Q}$.

Then, the conclusions of Th. 3.4 and the addendum hold with minor adjustments. For example, instead of the last sentence of Th. 3.4, conclude the following. The set of $\boldsymbol{p} \in \mathcal{H}_O^{\mathrm{in}}(\bar{\mathbb{Q}})$ with $D_{\boldsymbol{p}}$ in (3.4d) equal $G(\mathcal{H}_O^{\mathrm{in}}/\mathcal{H}_O^{\mathrm{ab}})$ is dense in the complex topology. In particular, it still holds that a cover in $\mathrm{Ni}(G, \mathbf{C})$ gives a regular realization of G as a Galois group over $\mathbb{Q}$ exactly when $\mathcal{H}(\mathbf{C})^{\mathrm{in}}(\mathbb{Q})$ is nonempty. Such rational points, however, require finding orbits O for which $\mathcal{H}_O^{\rm in}$ is an absolutely irreducible $\mathbb{Q}$ component of $\mathcal{H}(\mathbf{C}^{\rm in})$.

The most difficult hypothesis to relax is the center condition (3.3a). There will be situations where we wish to add more conditions to the group G. For example, [**FrV**] needed to cover G by a group satisfying (3.5b) for which

(†) G has its *Schur multiplier* generated by commutators.

Lemma 3.15 explains (†) and gives an application. Here, however, let us deal just with the center condition. Classical geometry often remedied a situation with a center by adding *rigidifying data* to the moduli problem. A natural rigidifying method here is to cover G by another group satisfying desirable conditions. Then, use the relation between the Hurwitz space for G and for its covering group. We explore why that isn't satisfactory here.

First: Consider the [**FrV**] methods for covering G with a group having no center. Assume G is not cyclic (eventually, we assume G is not nilpotent).

Suppose we don't mind replacing G by a group of higher rank. We can form a *wreath product*: $H^{|G|} \times^s G = G'$. Here H is a nontrivial centerless group and G acts on $H^{|G|}$ by permutation of the coordinates [**FrV**, Lemma2]. Or, to keep the same rank, [**FrV**, Lemma 3] suggests an inductive construction for covering G by G' with a smaller center. For that, consider $g \neq 1$ in the center of G. Let p be a prime not dividing $|G|$. Then, g acts nontrivially on the group ring M of G over $\mathbb{F}_p$. By Maschke's Theorem, M is completely reducible. So, it has an irreducible G module summand V on which g acts nontrivially. Now, let H be $V \times^s G$. Fix generators $(g_1, \dots, g_t)$ of G. Let $\boldsymbol{h} = (h_1, \dots, h_t) \in H^t$ be one of the $|V|^t$ tuples mapping to $g_1, \dots, g_t$. Since V is irreducible, either $\langle \boldsymbol{h} \rangle = H$, or $\langle \boldsymbol{h} \rangle$ is a complement to V in H. From Schur-Zassenhaus, all such complements are conjugate. There are no more than $|V|$ of them. In each such complement there is a unique lift of the g_i s. Since $t \geq 2$, conclude there exists $\boldsymbol{h}$ with $H = \langle \boldsymbol{h} \rangle$. The center of H injects into the center of G; yet, its image does not contain g (see computation following Lemma 3.6).

The §III.C construction, however, requires uniformly covering characteristic quotients ${}_p^n\tilde{G}$ of ${}_p\tilde{G}$. This is to get a corresponding modular tower whose properties help analyze those of the tower for $(G, p, \mathbf{C})$. Further, we've added new primes to the group. Conclude: Dealing directly with modular towers may prevent us from using [**FrV**] tricks for replacing G by a cover having property (3.3a). This justifies our next definition.

Definition 3.5. *Center Hypothesis.* Let G be a finite group and p a prime dividing $|G|$. Let ${}_p^n\tilde{G}$ be the the n-th Frattini quotient of ${}_p\tilde{G}$ (§II.B). Then, G satisfies the Center Hypothesis if ${}_p^n\tilde{G}$ has no center for each integer n.

The following lemma gives many examples when the Center Hypothesis holds. Let $\phi : G' \to G$ be a cover of groups. Consider the group of inner automorphisms from elements $g' \in G'$ with $\phi(g')$ in the center of G and g' commutes with $\ker(\phi)$.

Denote the subgroup of inner automorphisms from $\ker(\phi)$ by $\ker'$. Finally, let $\mathrm{Aut}(G', \ker(\phi))$ be the automorphisms of G' fixed on $\ker(\phi)$ and inducing the identity on G.

LEMMA 3.6. *If $g' \in G'$ is in the center of G', then $\phi(g')$ is in the center of G and g' centralizes $\ker(\phi)$. Now assume $\ker(\phi)$ is abelian. If G has no center, the maximal submodule of $\ker(\phi)$ on which G acts trivially is the center of G'. In particular, suppose ${}_p^n\tilde{G}$ has no center. Then, the center of ${}_p^{n+1}\tilde{G}$ is the largest submodule of $\ker_n / \ker_{n+1}$ on which ${}_p^n\tilde{G}$ acts trivially.*

If G is perfect, the sequence $\mathbf{1} \to \mathbf{1}$ appears nowhere in the Loewy display for $\ker_n / \ker_{n+1}$. Conclude: A perfect group satisfies the Center Hypothesis. Finally, $H^1(G, \ker(\phi)) = \mathrm{Aut}(G', \ker(\phi)) / \ker'$.

PROOF. The first paragraph of the lemma is elementary. The last sentence is [**N**, p. 244, Th. 13]. Identify the two groups by mapping $\phi \in \mathrm{Aut}(G', \ker(\phi))$ to the cocycle $g \in G \mapsto \psi(g')(g')^{-1}$ where g' lifts g.

Now consider the Loewy display statement on existence of $\mathbf{1} \to \mathbf{1}$. This says there is a ${}_p^n\tilde{G}$ module with Loewy display $\mathbf{1} \to \mathbf{1}$. Such a module gives a representation of ${}_p^n\tilde{G}$ in the 2×2 upper triangular matrices with ones on the diagonal. The commutators of these matrices are trivial. By assumption G is perfect. Therefore, so is ${}_p^n\tilde{G}$ (§II.A). The image, however, of the commutators in this representation is trivial. So, the whole representation is trivial. The module is $\mathbf{1} \oplus \mathbf{1}$ and not $\mathbf{1} \to \mathbf{1}$, a contradiction.

Assume G is perfect, and ${}_p^n\tilde{G}$ has no center. To show the Center Hypothesis holds, we need only show $\ker_n / \ker_{n+1}$ contains no nontrivial module V on ${}_p^n\tilde{G}$ acts trivially. Suppose P is a projective indecomposable summand of the minimal projective that maps surjectively to the kernel of $P_{\mathbf{1}} \to \mathbf{1}$. If $\mathbf{1}$ appears at the far right of the Loewy display of P, then $\mathbf{1} \to \mathbf{1}$ would appear in the Loewy display of $P_{\mathbf{1}}$. As above, this can't be. From [**Be2**, Prop. 3.1.2], the same module appears at the far right of the Loewy display of a principle indecomposable as at the far left of the Loewy display. Thus, $\mathbf{1}$ can't appear at the far left of the Loewy display of P either. Prop. 2.7, however, says $\Omega^2(\mathbf{1}) = \ker_n / \ker_{n+1}$ is some part on the left of the P Loewy display. Thus, $\mathbf{1}$ is not a submodule of $\ker_n / \ker_{n+1}$. Apply the first paragraph of the lemma inductively to conclude the Center Hypothesis holds for G. □

§App.A comments on the Center Hypothesis when G is not perfect. There is no simple converse to the opening sentence of Lemma 3.6. For example, consider a semidirect product $M \times^s G$ with M a G module. Suppose $g \in G$ is in the center of G and g acts trivially on M. Then, for any $m \in M$, (m, g) acts trivially by conjugation on M: $(m, g)(m', 1)(-m, g^{-1}) = (m', 1)$. Still, (m, g) is in the center of $M \times^s G$ only if G acts trivially on M:

$$(m, g)(m', g')(-m, g^{-1}) = (m + m' - g'(m), g').$$

§III.C. A tower of Hurwitz spaces. Suppose G is a finite group, and p is a prime dividing $|G|$. Let r be a positive integer and $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ conjugacy classes in G whose elements have orders prime to p. Note: §III.A (around (3.1)) doesn't require the orders of elements to be prime to p. That is specific to our next construction. We produce the moduli spaces

$$\mathcal{H}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}}) = \mathcal{H}_n, \ n = 1, 2, \dots.$$

The collection is the modular tower $\mathcal{T}(G, p, \mathbf{C})$ attached to $(G, p, \mathbf{C})$.

To simplify, we construct $\mathcal{H}_n$ when $n = 1$. Then, continue by induction. Let the order of elements in C_i be $o(\mathrm{C}_i)$; $\phi : {}^{1}_{p}\tilde{G} \to G$ is the natural map.

LEMMA 3.7. *Each C_i lifts uniquely to a conjugacy class $\tilde{\mathrm{C}}_i$ of ${}^{1}_{p}\tilde{G}$ where $o(\tilde{\mathrm{C}}_i) = o(\mathrm{C}_i)$. For each $n \geq 0$ this defines a Nielsen class $\mathrm{Ni}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})$.*

PROOF. Choose any $g_i \in C_i$. Let H_i be $\phi^{-1}(\langle g_i \rangle)$ in ${}^{1}_{p}\tilde{G}$. This gives an exact sequence $\ker_0 / \ker_1 \to H_i \to \langle g_i \rangle$. By Schur-Zassenhaus, this sequence splits, uniquely up to conjugation. All elements over g_i, of the same order as g_i, are conjugate. Thus, define a Nielsen class from ${}^{1}_{p}\tilde{G}$ and ${}^{1}_{p}\tilde{\mathbf{C}}$. Assume we have constructed a Nielsen class from ${}^{n}_{p}\tilde{G}$ and ${}^{n}_{p}\tilde{\mathbf{C}}$. Continue by induction to define a Nielsen class $\mathrm{Ni}({}^{n+1}_{p}\tilde{G}, {}^{n+1}_{p}\tilde{\mathbf{C}})$ by putting $({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})$ in place of $({}^{1}_{p}\tilde{G}, {}^{1}_{p}\tilde{\mathbf{C}})$. □

Let $\phi : G' \to G$ be a cover of groups. Suppose $T' : G' \to S_{n'}$ (resp., $T : G \to S_n$) is a faithful permutation representation with corresponding stabilizer $G'(1)$ (resp., $G(1)$). Assume there is a conjugate $G'(i)$ of $G'(1)$ with this property: $\phi(G'(i)) = G(1)$. We say T' *extends* T. In any cover the regular representation of the covering group extends that of the image group. There are, however, other situations of extending representations. For example, let p be a prime not dividing $G(1)$. Apply Schur-Zassenhaus, as in the proof of Lemma 3.7. Thus, the preimage of $G(1)$ in all extensions ${}^{n}_{p}\tilde{G} \to G$ contains a copy of $G(1)$, unique up to conjugacy. The representation T_n of ${}^{n}_{p}\tilde{G}$ on the cosets of $G(1)$ extends the corresponding representation in ${}^{k}_{p}\tilde{G}$, $k \leq n$. It has degree $m_n = n|\ker_0 / \ker_n|$.

This is the analog of the representation of D_{p^n} on cosets of the subgroup generated by an involution. An involution, however, generates its own normalizer in D_{p^n}. In the situation above, suppose $\alpha \in {}^{n}_{p}\tilde{G}$ normalizes $G(1)$. Then, the image of α in ${}^{n-1}_{p}\tilde{G}$ normalizes $G(1)$ there. Thus, assume $G(1)$ is self-normalizing in ${}^{n-1}_{p}\tilde{G}$. Then, it is also in ${}^{n}_{p}\tilde{G}$, unless restriction of $G(1)$ to $\ker_n / \ker_{n+1}$ contains the identity representation, $\mathbf{1}_{G(1)}$.

SELF-NORMALIZING PROBLEM 3.8. *Assume p does not divide $|G(1)|$ as above. Also, assume $G(1)$ is self-normalizing in G (condition (3.5b)). For what G is the stabilizer in the representation $T_n : {}^{n}_{p}\tilde{G} \to S_{m_n}$ self-normalizing, for each integer n? Equivalently, for what G is $\mathbf{1}_{G(1)}$ absent from the far left of the Loewy display of $\ker_n / \ker_{n+1}$, for each integer n?*

EXAMPLE 3.9. $G = A_5$, *and* $p = 5$. Irreducible A_5 modules are in (2.6). Restrict A_4 to the standard representation modulo the identity. This gives the standard degree 4 representation of A_4. It does contain the identity. Now check restriction of A_4 to the adjoint representation (2.6c).

The following is automatic in A_4. An element of order 3 (a 3-cycle) and an element of order 2 (conjugate to $(1\,2)(2\,4)$) generate all of A_4. To compute the effect of A_4 in the adjoint action (${}_5S_c$ of (2.6c)), find $A \in \mathrm{PSL}_2(\mathbb{Z}/5)$ of order 3 for use with $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Take $A = \begin{pmatrix} 1 & 2 \\ 1 & 3 \end{pmatrix}$. Check that no nontrivial trace zero matrix centralizes both. Suppose the image of A_4 in ${}^{n-1}_{\ 5}\tilde{A}_5$ is self-normalizing. Then, it is self-normalizing in ${}^{n}_{5}\tilde{A}_5$ exactly when neither $\mathbf{1}$ nor ${}_5S_b$ appears at the far left of the $\ker_n / \ker_{n+1}$ Loewy decomposition. The adjoint representation is the only simple submodule of $\ker_0 / \ker_1$ (with $p = 5$; see Remark 2.10). Thus, this holds for $n = 1$. $\square$

DEFINITION 3.10. *Modular towers.* Suppose $({}^{n}_{p}\tilde{G}, T_n)$ is a system of extending permutation representations of the characteristic quotients of ${}_p\tilde{G}$. For this situation, replace T by T_n, G by ${}^{n}_{p}\tilde{G}$, and $\mathbf{C}$ by ${}^{n}_{p}\tilde{\mathbf{C}}$ in Def. 3.1b. Call the corresponding normalizing group $N_n({}^{n}_{p}\tilde{\mathbf{C}}) = N_n$. The action of H_r on $\mathrm{Ni}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})/N_n$ produces the space

$$\mathcal{H}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})^{\mathrm{ab}} = \mathcal{H}_n^{\mathrm{ab}},\ n = 1, 2, \ldots.$$

Attach the collection of these to $(G, p, \mathbf{C})$. This is the *absolute* modular tower $\mathcal{T}(G, p, \mathbf{C})^{\mathrm{ab}}$. Similarly, there is the *inner* modular tower $\mathcal{T}(G, p, \mathbf{C})^{\mathrm{in}}$.

There is a natural map

$$\Psi_{n+1,n} : \mathcal{H}({}^{n+1}_{\ \ p}\tilde{G}, {}^{n+1}_{\ \ p}\tilde{\mathbf{C}})^{\mathrm{ab}} \to \mathcal{H}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})^{\mathrm{ab}}$$

induced by reduction modulo $\ker_n / \ker_{n+1}$. An r-tuple $\tilde{\boldsymbol{\sigma}} \in \mathrm{Ni}({}^{n+1}_{\ \ p}\tilde{G}, {}^{n+1}_{\ \ p}\tilde{\mathbf{C}})$ modulo $\ker_n / \ker_{n+1}$ maps to $\boldsymbol{\sigma} \in \mathrm{Ni}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})$. Suppose $\tilde{\alpha} \in N_{n+1}({}^{n+1}_{\ \ p}\tilde{\mathbf{C}})$. From the meaning of extension representations, $\tilde{\alpha}$ induces an element of $N_n({}^{n}_{p}\tilde{\mathbf{C}})$. Thus, the map on Nielsen classes induces a map on absolute Nielsen classes. Action of H_r commutes with this equivalence and reduction modulo $\ker_n / \ker_{n+1}$. So, action of H_r on $\mathrm{Ni}({}^{n+1}_{\ \ p}\tilde{G}, {}^{n+1}_{\ \ p}\tilde{\mathbf{C}})^{\mathrm{ab}}$ extends its action on $\mathrm{Ni}({}^{n}_{p}\tilde{G}, {}^{n}_{p}\tilde{\mathbf{C}})^{\mathrm{ab}}$. Covering space theory thus gives the map $\Psi_{n+1,n}$. There is a similar map for the inner version of these spaces.

Again, back to modular curves. Take p odd, ${}^{n}_{p}\tilde{G} = D_{p^n}$ and $\mathbf{C} = \mathbf{C}_r$, the repetition r times of the conjugacy class of involutions. (Little Note: The Nielsen class would be empty if r is odd. Tacitly here, r is even.) Let T_n be the standard representation of D_{p^n} of degree p^n. When $r = 4$, Hurwitz space $\mathcal{H}(D_{p^n}, {}^{n}_{p}\tilde{\mathbf{C}}_r)^{\mathrm{ab}}$ naturally maps to $X_0(p^n)$ from §I.A. Similarly, $\mathcal{H}(D_{p^n}, {}^{n}_{p}\tilde{\mathbf{C}}_r)^{\mathrm{in}}$ maps to $X_1(p^n)$.

§App.B explains pullback of $\mathcal{H}(D_{p^n}, {}^{n}_{p}\tilde{\mathbf{C}}_r)^{\mathrm{in}}$ over the symmetry map Θ_r : $(\mathbb{P}^1)^r \to \mathbb{P}^r$. Denote this pullback by $\mathcal{H}'$. In the case $r = 4$, the fibers of the induced map $\mathcal{H}'$ to $X_1(p^n)$ are homogeneous spaces for $\mathrm{PSL}_2(\mathbb{C})$ acting on ordered 4-tuples of distinct points in $\mathbb{P}^1$. Similarly, the map from $\mathcal{H}(D_{p^n}, {}^n_p\tilde{\mathbf{C}}_4)^{\mathrm{in}}$ to $X_1(p^n)$ has 3-dimensional Brauer-Severi varieties as fibers. Over $\mathbb{C}$ these fibers look like $\mathbb{P}^3$. Arithmetically, however, there is more going on. For example, suppose a point in $X_0(p^n)$ or $X_1(p^n)$ has field of definition K. Then, the fiber of the map from the Hurwitz space to the corresponding modular curve will be a variety over K. Yet, it may not be the trivial homogeneous space over K.

§III.D. An arithmetic invariant and an obstructed tower. We define the lifting invariant from §I.B. Then, we give an example of the following phenomenon. Even if $\mathrm{Ni}(G, \mathbf{C})$ is nonempty, $\mathrm{Ni}({}^1_p\tilde{G}, {}^1_p\tilde{\mathbf{C}})$ may be empty. Example 3.13 has classical connotations. This illustrates the main result of the subsection. Other than the action of the p-cyclotomic character, the lifting invariant is invariant under $G_{\mathbb{Q}}$. Following natural notation, we say $\tilde{\mathbf{g}} \in {}^n_p\tilde{\mathbf{C}}$ is a lift of $\mathbf{g} \in \mathrm{Ni}(G, \mathbf{C})$ if each coordinate of $\tilde{\mathbf{g}}$ maps to the corresponding coordinate of $\mathbf{g}$ modulo $\ker_0$. Recall from §III.A, $\mathbf{g} \in \mathbf{C}$ means the coordinates of $\mathbf{g}$ (in some order) are in the respective conjugacy classes of $\mathbf{C}$.

DEFINITION 3.11. Let O be an H_r orbit on $\mathrm{Ni}(G, \mathbf{C})$. Choose $\mathbf{g} \in O$. For each integer $n \geq 1$ define $\nu_n(O) \subset \ker_0 / \ker_n$ to be

$$\{\tilde{g}_1 \cdots \tilde{g}_r \mid \tilde{\mathbf{g}} \in {}^n_p\tilde{\mathbf{C}},\ \tilde{\mathbf{g}} \text{ lifts } \mathbf{g}\}. \tag{3.6}$$

Finally, $\nu(O) = \nu(G, p, \mathbf{C})(O)$ is the projective limit in $\ker_0$ of these sets. The absolute analog of this is to define this set for an orbit of H_r on $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$.

Consider a Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ and the corresponding level n Nielsen class $\mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$. Let O be an H_r orbit on $\mathrm{Ni}(G, \mathbf{C})$. We say O is obstructed at level n if it isn't in the image of the natural map $\mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}}) \to \mathrm{Ni}(G, \mathbf{C})$. This means $\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}}) \to \mathcal{H}(G, \mathbf{C})$ is empty over the component $\mathcal{H}_O$ of $\mathcal{H}(G, \mathbf{C})$.

LEMMA 3.12. *The set $\nu_n(O) \subset \ker_0 / \ker_n$ depends only on O (not on $\mathbf{g}$ in Def. 3.11). Also, $\nu_n(O)$ is a union of conjugacy classes of $\ker_0 / \ker_n$. The modular tower over O is obstructed at level n if and only if $1 \notin \nu_n(O)$.*

PROOF. Take any other $\mathbf{g}' \in O$. Then, there exists $Q \in H_r$ with $(\mathbf{g})Q = \mathbf{g}'$. Apply Q to each $\tilde{\mathbf{g}}$ whose product of entries appears in the set (3.6). Notice: If Q_i is from (3.1d), the product of entries for $(\tilde{\mathbf{g}})Q_i$ equals the corresponding product of entries for $\tilde{\mathbf{g}}$. Thus, $Q \in H_r$ preserves the set (3.6). Conclude the invariant depends only on O.

To see $\nu_n(O)$ is a union of conjugacy classes in $\ker_0 / \ker_n$, consider $k \in \ker_0 / \ker_n$. If $\tilde{\mathbf{g}}$ is a lift of $\mathbf{g}$, then so is $k\tilde{\mathbf{g}}k^{-1}$. The product of the entries of this element is the k conjugate of the product of the entries of $\mathbf{g}$. The last sentence reverts to the definition of Nielsen classes. □

EXAMPLE 3.13. *Modular towers obstructed at level 1.* Take $G = A_n$ (alternating group), $p = 2$, and $\mathrm{C}_1, \dots, \mathrm{C}_{n-1} = \mathrm{C}$, where C is the conjugacy class of

3-cycles. Assume $n \geq 5$. (For $n = 4$, 3-cycles aren't rational conjugacy classes.) Use $\mathbf{C}_{3^r}$ to mean r repetitions of C. Riemann-Hurwitz gives $r - (n-1)$ for the genus of a cover in $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$. Thus, the minimal value, $n-1$, for r corresponds to genus 0 covers. The lifting invariant will show there are two orbits (at least) when $r+1 > n$ and one orbit (exactly) when $r+1 = n$. The lifting invariant, ν_1, on one orbit contains 1, while on the other it does not. When $r = n-1$ the lifting invariant contains 1 exactly when n is odd. Thus, for n even, Lemma 3.12 says the modular towers are obstructed at level 1. For $r > n-1$, a component of the modular tower is obstructed at level 1, and another component is unobstructed at all levels. The rest of the example has five parts. Starting with the genus 0 case, there is an induction on the pair (n, r).

Part A: Reversion to the universal central extension. Let O be an H_r orbit on $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$. Let $\bar{A}_n$ be the universal central extension of A_n (see (2.4)). Identify the kernel of $\bar{A}_n \to A_n$ with $\{\pm 1\}$. Since the universal central extension is an exponent 2 Frattini cover, $\frac{1}{2}\tilde{A}_n \to A_n$ factors through it. Denote the image of $\nu_1(O)$ in $\bar{A}_n$ by $s(O)$. Use $\bar{g}$ for the image of $\tilde{g} \in \frac{1}{2}\tilde{A}_n$ in $\bar{A}_n$.

Part B: The case $r = n-1$. When n is odd, we easily compute some Nielsen class representative lifting invariants. Consider:

$$((1\,2\,3), (1\,2\,3)^{-1}, (1\,4\,5), (1\,4\,5)^{-1}, \dots, (1\,n{-}1\,n), (1\,n{-}1\,n)^{-1}). \tag{3.7a}$$

Indeed, whatever the lifts of $g_1, g_3, \dots, g_{n-2}$ in $\bar{A}_n$, lift the g_i s with even subscripts to the inverse of the lifts of g_{i-1}. Thus, the lifts consist of elements paired with their juxtaposed inverses. If $\mathbf{g}$ is (3.7a), $s(\mathbf{g}) = 1$ and $\nu_n(\mathbf{g})$ contains 1 for all n. For n even use this test $\mathbf{g}$:

$$\begin{gathered}((1\,2\,3), (1\,2\,3)^{-1}, \dots, (1\,n{-}4\,n{-}3), (1\,n{-}4\,n{-}3)^{-1},\\ (1\,n{-}2\,n{-}1), (1\,n{-}1\,n), (1\,n\,n{-}2)).\end{gathered} \tag{3.7b}$$

Now lift these elements to $\bar{\mathbf{g}}$. Consider, also, the $(n-2)$-tuple $\mathbf{g}'$ where the first $n-3$ entries are the same as in (3.7b), and the $n-2$ entry is

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

Part C shows $s(\mathbf{g}) = -s(\mathbf{g}')$. Now continue by induction using the case where n is odd above. Conclude: $s(\mathbf{g}) = -1$ and $\nu_n(\mathbf{g})$ doesn't contain 1 if n is even.

Part C: Lifting $g_1 g_2$. Suppose g_1 and g_2 are 3-cycles of A_5 which generate distinct subgroups. Assume $g_1 g_2$ is also a 3-cycle. We show their lifts $\bar{g}_1$ and $\bar{g}_2$ (of order 3) to $\bar{A}_5$ have product of order 6. Any 3-tuple (τ_1, τ_2, τ_3) of 3-cycles in A_5 with $\langle \tau_1 \rangle \neq \langle \tau_2 \rangle$ and $\tau_1 \cdot \tau_2 = \tau_3$ is conjugate to $((1\,2\,3), (1\,4\,2), (4\,2\,3))$ in A_5. So, check by multiplying two appropriate elements in $\mathrm{SL}_2(\mathbb{Z}/5)$. For example,

$$\begin{pmatrix} 0 & 2 \\ 2 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -2 & -2 \\ 1 & 3 \end{pmatrix}$$

is of order 6.

Part D: Lifting invariant to $\bar{A}_5$ for $r > n-1$. Assume $r > n-1$. We show there are $\mathbf{g}_{\pm 1} \in \mathrm{Ni}(A_n, \mathbf{C}_{3^r})$ with $s(\mathbf{g}_{\pm 1}) = \pm 1$.

Start with $n = 5$ and $r = 5$. Consider:

$$\begin{aligned} \mathbf{g}_{5,+} =&((1\,2\,3),(3\,2\,1),(1\,4\,5),(1\,4\,5),(1\,4\,5)) \text{ and} \\ \mathbf{g}_{5,-} =&((1\,2\,3),(3\,2\,1),(1\,3\,4),(1\,4\,5),(1\,5\,3)). \end{aligned} \tag{3.8a}$$

The former has lifting invariant $+1$; the latter has lifting invariant -1. Similarly, for $n = 6$ and $r = 6$ consider

$$\begin{aligned} \mathbf{g}_{6,+} =&((1\,2\,3),(3\,2\,1),(1\,4\,5),(1\,5\,4),(1\,5\,6),(1\,6\,5)) \text{ and} \\ \mathbf{g}_{6,-} =&((1\,2\,3),(1\,2\,3),(1\,2\,3),(1\,4\,5),(1\,5\,6),(1\,6\,4)). \end{aligned} \tag{3.8b}$$

Again, $s(\mathbf{g}_{6,\pm 1}) = \pm 1$.

For all cases with $g = 1$ proceed inductively on r. Suppose $\mathbf{g}_{n-2,\pm 1} \in \mathrm{Ni}(A_{n-2}, \mathbf{C}_{3^{n-2}})$ has $s(\mathbf{g}_{n-2,\pm 1}) = \pm 1$. Juxtapose the pair $((1\,n{-}1\,n),(1\,n\,n{-}1))$ on the end of each of these to get similar elements $\mathbf{g}_{n,\pm 1}$. With starting points at $n = 5$ and 6, this concludes the case $g = 1$ (or, $r = n$).

Now consider each fixed n and general $r > n-1$. Do induction on r. Take any $\mathbf{g}$ in the case for $r-1$. Replace the single entry g_{r-1} by the 2-tuple $(g_{r-1}^{-1}, g_{r-1}^{-1})$. The new r-tuple $\mathbf{g}'$ has these two entries on the end. Clearly, $s(\mathbf{g}') = s(\mathbf{g})$.

Part E: For $g = 0$, $s(\mathbf{g}) = (-1)^{n-1}$ for all $\mathbf{g} \in \mathrm{Ni}(A_n, \mathbf{C}_{3^{n-1}})$. Part B above gives examples of this case for each n having the appropriate lifting value. Lemma 3.12 implies the full result if H_{n-1} is transitive on each of the corresponding Nielsen classes. This is the lead theorem of [**Fr8**]. □

REMARK 3.14. *Other developments from Ex. 3.13.* I responded to an e-mail question from Serre with the Part E formula. (This included a suggestion of the proof of [**Fr8**].) He used the braid action and proved it without the complete transitivity result for genus 0 [**Se3**]. He generalized the formula of Part E (when $g = 0$) to all cases where $G = A_n$ and the branch cycles are of odd order. Here is the significance of the example.

Let $\phi : X \to \mathbb{P}^1$ be a cover in the Nielsen class of this example (or for one of those considered by Serre). Then, the (2nd kind) differential $d\phi$ on X has divisor of the shape $2D$. That's not equivalence, that's equality (although D isn't a positive divisor). So, over each point of the Hurwitz space $\mathcal{H}$ of the Nielsen class you have a specific *half-canonical* class $[D]$. Serre proved the classical invariant–dimension of the linear system of D, modulo 2–gives the lifting invariant [**Se6**]. Another proof of this appears in [**EKV**]. I didn't publish [**Fr8**] because I hadn't proven my suspicion there are *exactly* two connected components of $\mathcal{H}(A_n, \mathbf{C}_{3^r})$ when $r \geq n$ (the genus of the covers is at least 1). Newer ideas, following §III.F now improve this. □

Suppose $\mathbf{C}$ has its entries from the distinct conjugacy classes $\mathrm{C}'_1, \dots, \mathrm{C}'_t$. [**Fr8**] contains a generalization of Ex. 3.13 to any pair $(G, \mathbf{C})$ appropriate for the general theory of modular towers. This tells exactly what are the connected components of $\mathcal{H}(G, \mathbf{C})$ and their fields of definition under the following hypothesis.

(3.9) Each C'_i appears with suitably many repetitions in $\mathbf{C}$, $i = 1, \dots, t$.

Here we make no assumption about a prime p. This result in full generality helps relax the assumption p is relatively prime to the orders of the conjugacy classes. It requires notation to say completely. This uses an unpublished result of Conway and Parker (see [**FrV**, Appendix] for a special case) with a fine idea and some gaps. We state only enough to compare with Ex. 3.13. Part IV will say more on how this goes with the main result of §III.F and its application to modular towers.

Suppose G is perfect and $\bar{G}$ is its universal central extension. Let $\overline{\ker}$ be the kernel of the natural map $\bar{G} \to G$. Assume the conjugacy classes of G in $\mathbf{C}$ have orders prime to $|\overline{\ker}|$. As in Lemma 3.7, each C_i lifts to a unique conjugacy class $\bar{\mathrm{C}}_i$ of $\bar{G}$ of elements of the same order. Condition (†) of §III.B is equivalent to $m_{\mathbf{C}}$ below is trivial.

Schur Multiplier Lemma 3.15. *Let $U_{\mathbf{C}}$ be (the set of) commutators in $\bar{G}$ of form $[\bar{g}_1, \bar{g}_2]$ with $\bar{g}_j \in \cup_{i=1}^r \bar{\mathrm{C}}_i$, $j = 1, 2$. Form $m_{\mathbf{C}} = \overline{\ker}/\langle \overline{\ker} \cap U_{\mathbf{C}} \rangle$. If* (3.9) *holds, irreducible components of $\mathcal{H}(G, \mathbf{C})$ correspond naturally to elements of $\overline{\ker}/m_{\mathbf{C}}$. Further, suppose $\mathbf{C}$ is a rational union of conjugacy classes. Then, the component corresponding to the identity of $\overline{\ker}/m_{\mathbf{C}}$ has field of definition $\mathbb{Q}$.*

Apply Lemma 3.15 to Ex. 3.13. A commutator of 3-cycles in A_n can be any product of two 3-cycles. Thus, computing $\overline{\ker} \cap U_{\mathbf{C}}$ reduces to asking this. Can $\bar{g}_1 \bar{g}_2$ be the nontrivial element of $\overline{\ker}$ if g_1 and g_2 are 3-cycles. No, because, this implies $g_2 = g_1^{-1}$. From uniqueness of their lifts, $\bar{g}_2 = \bar{g}_1^{-1}$. For this case, $\overline{\ker}/m_{\mathbf{C}} = \mathbb{Z}/2$. If for a given n, r is suitably large, then $\mathcal{H}(A_n, \mathbf{C}_{3^r})$ has exactly two components, both defined over $\mathbb{Q}$.

Now we prove the $G_{\mathbb{Q}}$ invariance properties of the lifting invariants of Def. 3.11. Orbits of H_r on $\mathrm{Ni}(G, \mathbf{C})$ correspond to components of $\mathcal{H}(G, \mathbf{C})$. So, replace an orbit O by the corresponding component $\mathcal{H}_O$ in the next theorem. For $\tau \in G_{\mathbb{Q}}$, $\mathcal{H}_O^\tau$ is its conjugate by τ. From the definition of the filtration on ${}_p\tilde{G}$, elements of $\ker_0 / \ker_n$ have order dividing p^n. Let

$$(3.10) \qquad {}_p^n\psi : G_{\mathbb{Q}} \to G(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) = (\mathbb{Z}/p^n)^*$$

be restriction. Use ${}_p\psi : G_{\mathbb{Q}} \to (\mathbb{Z}_p)^*$ for the projective limit of these homomorphisms. Any nontrivial $\alpha \in \ker_0$ generates a cyclic subgroup isomorphic to $\mathbb{Z}_p$. Thus, α^t makes sense for $t \in (\mathbb{Z}_p)^*$. Similar remarks apply for the full cyclotomic character $\psi : G_{\mathbb{Q}} \to (\hat{\mathbb{Z}})^*$. As in §App.C (see the end of §III.B), saying $\mathcal{H}$ has field of definition $\mathbb{Q}$ means this variety with its moduli space properties.

GALOIS INVARIANCE THEOREM 3.16. *Assume G has trivial center. With $\mathbf{C}$ a rational union of conjugacy classes in G, let $p \mid |G|$ be prime to the orders of $\mathbf{C}$. Write $\mathcal{H}(G,\mathbf{C})$ as a disjoint union $\cup_{i=1}^t \mathcal{H}_i$ with each $\mathcal{H}_i$ (absolutely) irreducible. Then (as after Th. 3.4), $G_{\mathbb{Q}}$ permutes the $\mathcal{H}_i$ s. For any $\tau \in G_{\mathbb{Q}}$,*

$$\nu(\mathcal{H}_i^\tau)^{p^{\psi(\tau)}} = \nu(\mathcal{H}_i),\ i = 1, \dots, t. \tag{3.11a}$$

Conclude:

(3.11b) *For given $i \neq j$, if $\nu(\mathcal{H}_i) \neq \nu(\mathcal{H}_j)^t$ for each $t \in (\mathbb{Z}_p)^*$, then $\mathcal{H}_i$ is not conjugate to $\mathcal{H}_j$ by $G_{\mathbb{Q}}$.*

(3.11c) *If $\nu(\mathcal{H}_i) \neq \nu(\mathcal{H}_i)^t$ for some $t \in (\mathbb{Z}_p)^*$, then $\mathcal{H}_i$ is not defined over $\mathbb{Q}$.*

In particular, if $\nu(\mathcal{H}_i)^t = \nu(\mathcal{H}_i)$ for all $t \in (\mathbb{Z}_p)^*$ and $\nu(\mathcal{H}_i) \neq \nu(\mathcal{H}_j)$ for $j \neq i$, then $\mathbb{Q}$ is a field of definition for $\mathcal{H}_i$.

PROOF. Let O be an orbit of H_r on $\mathrm{Ni}(G,\mathbf{C})$. Choose a representative (geometrically Galois) cover $\hat\phi : \hat X \to \mathbb{P}^1$ with branch cycle description $\mathbf{g}$ in this orbit. Further, make a choice with branch points in $\bar{\mathbb{Q}}$. Now, $(\hat\phi, \hat X)$ has field of definition $\bar{\mathbb{Q}}$ (see, for example [**Fr5**, Lemma 1.2]). We show $\nu_n(\mathcal{H}_O^\tau)^{p^{n\psi(\tau)}} = \nu_n(\mathcal{H}_O)$ for each positive integer n. From this the theorem follows.

Use notation from Def. 3.11: for each lift $\tilde{\mathbf{g}} \in {}_p^n\tilde{\mathbf{C}}$ of $\mathbf{g}$, form

$$\tilde{\mathbf{g}}' = (\tilde{\mathbf{g}}, m(\tilde{\mathbf{g}})^{-1}) \text{ with } m(\tilde{\mathbf{g}}) = \tilde g_1 \cdots \tilde g_r. \tag{3.12}$$

The product of the $\tilde{\mathbf{g}}'$ entries is 1. Thus, $\tilde{\mathbf{g}}'$ are branch cycles for a cover ${}_n\hat X \to \mathbb{P}^1$ that factors through $\hat X \to \mathbb{P}^1$. Extend τ to the diagram ${}_n\hat X \to \hat X \to \mathbb{P}^1$. The moduli space component $\mathcal{H}_O^\tau$ therefore includes a point corresponding to $\hat X^\tau \to \mathbb{P}^1$. Further, this cover supports the extension ${}_n\hat X^\tau \to \mathbb{P}^1$.

Let $\boldsymbol{x} = (x_1, \dots, x_r)$ be branch points corresponding to the branch cycle description $\mathbf{g}$ for $\hat X \to \mathbb{P}^1$. Similarly, let $(\boldsymbol{x}, x_{r+1})$ be branch points for ${}_n\hat X \to \mathbb{P}^1$. (Leave x_{r+1} out if $m(\tilde{\mathbf{g}}) = 1$.) Let $\tilde{\mathbf{g}}'_\tau$ be a branch cycle description for ${}_n\hat X^\tau \to \mathbb{P}^1$. Reducing entries of $\tilde{\mathbf{g}}'_\tau$ module $\ker_0$ gives a branch cycle description $\mathbf{g}_\tau$ of $\hat X^\tau \to \mathbb{P}^1$. The remainder is in two parts: applying the Branch Cycle Argument (implicit in Theorem 3.4); and conclusions from this.

Part A: Branch Cycle Argument [**Fr6–Fr6a**, §3]. Indicate the entry in $\tilde{\mathbf{g}}'_\tau$ corresponding to $\tau(x_i)$ by $\tilde g'_{\tau,i}$. Then,

(3.13) $(\tilde g'_{\tau,i})^{\psi(\tau)}$ is conjugate to $\tilde g'_i$.

One aside, before we continue to draw deductions. The argument of [**Fr5**, before Th. 5.1] has explicit identifications for choosing representative branch cycles of ${}_n\hat X^\tau \to \mathbb{P}^1$. Suppose L is a field of definition for ${}_n\hat X^\tau \to \mathbb{P}^1$. Statement (3.13) derives from embedding the Galois closure of $L({}_n\hat X)/L(x)$ into Puiseux expansions about $(x - x_i)$. Compare this with a similar embedding of $L^\tau({}_n\hat X^\tau)/L^\tau(x)$ into Puiseux expansions about $(x - \tau(x_i))$. From §I.F, restrict the effect of σ_{x_i} (mapping $(x-x_i)^{1/e}$ to $\zeta_e(x-x_i)^{1/e}$) to the image field. Regard this image field as having generators the conjugates $\boldsymbol{y} = (y_1, \dots, y_{n'})$ of a primitive generator y_1 for $L({}_n\hat{X})/L(x)$. (That is, $L(x, y_1) = L({}_n\hat{X})$.) This gives a representative for the conjugacy class of $\tilde{g}'_i$. Then, extend the action of τ on L (fixed on x) to all of $L({}_n\hat{X})$. Do similarly for a conjugacy class representative of the entry of $\tilde{\mathbf{g}}'_\tau$ corresponding to $\tau(x_i)$. Restrict $\sigma_{\tau(x_i)}$ to $\tau(\boldsymbol{y}) = (\tau(y_1), \dots, \tau(y'_n))$.

Compare resulting permutations by identifying permutations of $\boldsymbol{y}$ with permutations of $\tau(\boldsymbol{y})$ in the obvious way. Finally, compare the effect of σ_{x_i} with $\tau^{-1}\sigma_{\tau(x_i)}\tau$ on $(x - x_i)^{1/e}$. The former gives $\tau^{-1}(\zeta_e)(x - x_i)^{1/e}$. The latter gives $\zeta_e(x - x_i)^{1/e}$. Thus, the former to the power $\psi(\tau)$ gives the latter.

Part B: Conclusions from the Branch Cycle Argument. The first r entries of $\tilde{\mathbf{g}}'_\tau$ lie over corresponding entries for $\mathbf{g}_\tau$. These are conjugacy classes permuting those appearing in ${}^n_p\tilde{\mathbf{C}}$. The last is in the conjugacy class of $m(\tilde{\mathbf{g}})^{-{}^n_p\psi(\tau)}$. Thus, the inverse of this last coordinate is in $\nu_n(\mathcal{H}_O)$. Apply this to every element of $\nu_n(\mathcal{H}_0^\tau)$ to see it equals $\nu_n(\mathcal{H}_O)^{-{}^n_p\psi(\tau)}$. This concludes the proof of (3.11a).

(3.11b) restates (3.11a). Now assume $\nu(\mathcal{H}_i) \neq \nu(\mathcal{H}_i)^t$ for some $t \in (\mathbb{Z}_p)^*$. Then, there exists n with $\nu_n(\mathcal{H}_i) \neq \nu_n(\mathcal{H}_i)^{t'}$, $t' \in (\mathbb{Z}/p^n)^*$ the image of t. Choose $\tau \in G_\mathbb{Q}$ with ${}^n_p\psi(\tau) = s'$ where $s't' = 1 \mod p^n$. We showed above $\nu_n(\mathcal{H}_i^\tau) = \nu_n(\mathcal{H}_i)^{t'}$. By assumption, the right side doesn't equal $\nu_n(\mathcal{H}_i)$. Thus, $\mathcal{H}_i^\tau \neq \mathcal{H}_i$. The hypotheses for the final statement say conjugates of $\mathcal{H}_i$ have the same ν invariant, and no $\mathcal{H}_j$ has the same invariant unless $j = i$. Thus, $G_\mathbb{Q}$ fixes $\mathcal{H}_i$; $\mathbb{Q}$ is its field of definition. $\square$

§III.E. Primes dividing $|G|$ that exceptionally ramify. Fix a finite group G and a prime p dividing $|G|$. It may happen $\mathrm{Ni}(G, \mathbf{C})$ is empty for all values of r even if $\mathbf{C}$ contains *every* conjugacy class prime to p. We say p *exceptionally ramifies*. For example, 2 exceptionally ramifies when $G = D_{p^n}$ for p an odd prime. (Reader: Note, we changed the meaning of p in that one sentence.) An element in a group G has p' order if its order is prime to p. Similarly, we say C is a p' conjugacy class if its elements have p' order.

LEMMA 3.17. *If p exceptionally ramifies in G, some proper normal subgroup N of G contains all p' conjugacy classes. In particular, $|G/N|$ is a p power.*

Let N be a proper normal subgroup of G with G/N a p group. Then, N contains all conjugacy classes of elements of order r^t with $r \neq p$ a prime. Further, suppose P_p is a p-Sylow of G and $|G/N| = |P_p|$. Then, $G = N \times^s P_p$ and p exceptionally ramifies (for G). Finally, if G is nilpotent, then all primes dividing G exceptionally ramify.

PROOF. Assume p exceptionally ramifies. We prove all elements of p' order are in a proper normal subgroup. List the complete collection $\{h_1, \dots, h_t\}$ of elements of p' order. This set is closed under conjugation. So, it generates a normal subgroup N. The $2t$-tuple $\{h_1, h_1^{-1}, \dots, h_t, h_t^{-1}\}$ is in a p' Nielsen class. Thus, p ramifies exceptionally implies N is a proper subgroup of G. Suppose

$|G/N|$ is not a power of p. Then, it contains $\bar{g}$, nontrivial and of p' order. The Chinese Remainder Theorem produces $g \in G$ of p' order mapping to $\bar{g}$. Since g is not in N, this is contrary to the assumption N contains all elements of order prime to p. In particular, G/N is a p-group.

Now, assume N is a proper normal subgroup of G and G/N is a p group. Suppose $g \in G$ is a prime power r^t, $r \neq p$. From the Sylow Theorems, the conjugacy class of g meets every r-Sylow. As G/N is a p group, N contains a p-Sylow of G, and so the conjugacy class of r^t meets N. As N is normal, this conjugacy class is in N.

Now add that G/N has the order of a p-Sylow. From Schur-Zassenhaus, $G = N \times^s G/N$. Since G/N is a p-group, it is a p-Sylow of G. Consider any element (h_1, h_2) in the semi-direct product. It is in N if and only if h_2 is trivial. On the other hand, if h_2 is nontrivial, it has order a power of p. Therefore, p divides the order of (h_1, h_2). The last statement follows from this case. □

Lemma 3.17 says modular towers don't apply well to nilpotent groups. More seriously, they don't work for primes that exceptionally ramify. Part IV of the continuation discusses p-ramified modular towers. §App.D motivates this with the universal Artin-Schreier cover of a finite group with given involution classes.

A related problem appears in §III.F. Suppose $\mathbf{C}$ is a collection of conjugacy classes of G. Assume *every* conjugacy class appears among the entries of $\mathbf{C}$. The following is well known [**J**].

(3.14) If $g_i \in \mathrm{C}_i$, $i = 1, \dots, r$, then $\langle g_1, \dots, g_r \rangle = G$.

DEFINITION 3.18. Let $\mathbf{C}$ be a collection of conjugacy classes of the finite group G. We say $\mathbf{C}$ is *g(eneration)complete* if statement (3.14) holds. [**Se4**, §7.3] has a related concept *strictly rigid*. Assume p is a prime dividing $|G|$. We say G is p-gcomplete if (3.14) holds when $\mathbf{C}$ is the set of p' conjugacy classes.

The remainder of this subsection comments on p-gcompleteness of a group. Of course, if p ramifies exceptionally, then G is not p-gcomplete. Consider A_5. It is 2-gcomplete. A subgroup of A_5 containing a 3-cycle and a 5-cycle is A_5. On the other hand, it is neither 3-gcomplete nor 5-gcomplete. The group $D_5 = \langle (1\,3)(5\,4), (2\,3)(1\,4) \rangle$ is a $3'$-complement intersecting nontrivially with every $3'$ conjugacy class. Similarly, A_4 is a $5'$-complement intersecting nontrivially with every $5'$ conjugacy class.

G. Malle suggested the following example. Let $G = \mathrm{PSL}_2(q)$, q a prime power. This is a group of order $(q^2 - q)(q+1)/2$. Assume $p = (q+1)/2$ is a prime. All p' conjugacy classes have representatives in the Borel subgroup

$$\left\{ \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

This too is a p'-complement.

§III.F. $\mathbb{Q}$ components at all levels of a modular tower. We have typical hypotheses for considering (absolutely irreducible) $\mathbb{Q}$ components of a Hurwitz space. These are the center (3.3a) and rationality (3.3b) conditions. Throughout this subsection we assume G and $\mathbf{C}$ satisfy these.

Definition 3.19. *HM-Nielsen classes.* Let $r = 2s$. We say the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ is H(arbater)M(umford) if there exists $\mathbf{g} \in \mathbf{C}$ of this form: $(g_1, g_1^{-1}, \dots, g_s, g_s^{-1})$. Then, $\mathbf{g}$ is an HM representative of the Nielsen class.

Mumford considered curves $\mathcal{C} \to \mathrm{Spec}(\mathbb{Z}_p)$ with nonsingular generic fiber, and totally degenerate special fiber. An analog arises in the proof of Theorem 3.21. Harbater's early deformation approach used this branch cycle condition [**Ha**].

It is easy (and similar to the proofs of the next lemmas) to show there is a $Q \in H_r$ that takes an HM representative as in Def. 3.19 to

$$(g_1, \dots, g_s, g_s^{-1}, \dots, g_1^{-1}) = [g_1, \dots, g_s] \stackrel{\text{def}}{=} [\mathbf{g}]. \tag{3.15}$$

Lemma 3.20. *Suppose* $\mathbf{g}$ *is from* (3.15) *and* $\pi \in S_s$. *Then, there exists* $Q \in H_r$ *for which*

$$[g_1, \dots, g_s]Q = [g_{(1)\pi}, \dots, g_{(s)\pi}].$$

Proof. Transpositions generate S_s. It suffices to show this when $\pi = (1\,2)$ using elements $Q \in H_r$ that only affect the first four coordinates. In the notation of (3.1d) take $Q_{1,2} = Q_1^{-1}Q_3$. Then:

$$\begin{aligned}(g_1, g_2, g_2^{-1}, g_1^{-1})Q_{1,2} &= (g_2, g_2^{-1}g_1g_2, g_2^{-1}, g_1^{-1})Q_3 \\ &= (g_2, g_2^{-1}g_1g_2, g_2^{-1}g_1^{-1}g_2, g_2^{-1}).\end{aligned} \tag{3.16}$$

Lemma 3.3 gives $Q' \in H_r$ conjugating (3.16) by g_2 (fixing the coordinates beyond the first four). Conclude by taking $Q = Q_{1,2}Q'$. □

The next result uses a hypothesis: You can remove any pair of inverse conjugacy classes C_i and C_j from $\mathbf{C}$, with $i \neq j$, and what remains should be gcomplete (Def. 3.18). We call such a $\mathbf{C}$, *HM-gcomplete* because it goes with the HM Nielsen hypothesis. Examples include $\mathbf{C}$ containing every conjugacy class at least 4 times. Also, if G is p-gcomplete, then $\mathbf{C}$ is HM-gcomplete when every p'-conjugacy class appears at least 4 times.

Theorem 3.21. *Assume the following conditions on* $\mathbf{C}$.

(3.17a) $\mathbf{C}$ *is HM-gcomplete.*
(3.17b) $\mathrm{Ni}(G, \mathbf{C})$ *is an HM-Nielsen class.*

Then, all HM representatives of $\mathrm{Ni}(G, \mathbf{C})$ *are in one* H_r *orbit* O. *Further, if* (3.3a) *and* (3.3b) *hold,* $\mathcal{H}_O$ *is an absolutely irreducible component of* $\mathcal{H}(G, \mathbf{C})$ *with field of definition* $\mathbb{Q}$.

PROOF. Apply Lemma 3.20 to an HM representative $[g_1,\dots,g_s]$. Suppose g'_s is conjugate to g_s in G: $\alpha g_s\alpha^{-1}=g'_s$. It suffices to find $Q\in H_r$ with

$$[g_1,\dots,g_s]Q=[g_1,\dots,g_{s-1},g'_s].$$

From (3.17a), among $g_1,\dots,g_{s-1}$ are generators of G. Apply Lemma 3.20 again to assume these are $g_t,\dots,g_{s-1}$ for some t.

Apply Lemma 3.3 to find Q with

$$[g_1,\dots,g_s]Q=[g_1,\dots,g_{t-1},\alpha g_t\alpha^{-1},\dots,\alpha g_s\alpha^{-1}]. \tag{3.18}$$

Lemma 3.20 gives $Q\in H_r$ that sends (3.18) to

$$[g_1,\dots,g_{t-1},\alpha g_s\alpha^{-1},\alpha g_t\alpha^{-1},\dots,\alpha g_{s-1}\alpha^{-1}]. \tag{3.19}$$

Apply Lemma 3.3 to conjugate the entries from $\alpha g_t\alpha^{-1}$ to $\alpha g_{s-1}\alpha^{-1}$ by α^{-1}. A final application of Lemma 3.20 produces $[g_1,\dots,g_{s-1},g'_s]$. This concludes the proof that all HM representatives of $\mathrm{Ni}(G,\mathbf{C})$ are in one H_r orbit O. Now, Lemma 3.22 (below) shows $\mathcal{H}_O$ has $\mathbb{Q}$ as field of definition. $\square$

Recall the discriminant locus D_r in $\mathbb{P}^r$. The fat diagonal $\Delta_r\subset(\mathbb{P}^1)^r$ lies above it in the natural map $(\mathbb{P}^1)^r\to\mathbb{P}^r$. A partition of $\{1,\dots,r\}$ is a collection of disjoint sets $\mathcal{I}=\{I_1,\dots,I_u\}$ with these properties. The union of the I_j s is $\{1,\dots,r\}$, and each I_j consists of consecutive integers. Given $\mathcal{I}$, define $\Delta_{\mathcal{I}}$ to be the subset of Δ_r with equations $x_i=x_j$, if $i,j\in I_k$ for some k. Similarly, let $D_{\mathcal{I}}$ be the image of $\Delta_{\mathcal{I}}$. Inequalities $x_i\ne x_j$, if i and j aren't in a common subset of $\mathcal{I}$, define a Zariski open subset $D^0_{\mathcal{I}}$ of $D_{\mathcal{I}}$. We use the following sequence of partitions:

$$\begin{aligned}\mathcal{I}_0=\{1,\dots,r\},\mathcal{I}_1&=\{\{1,2\},3,\dots,r\},\dots,\\ \mathcal{I}_s&=\{\{1,2\},\{3,4\},\dots,\{r-1,r\}\}.\end{aligned} \tag{3.20}$$

Each partition $\mathcal{I}$ also defines a *coalescing* operator $\mathcal{C}_{\mathcal{I}}$ on $\mathrm{Ni}(G,\mathbf{C})$. Given $\mathbf{g}\in\mathrm{Ni}(G,\mathbf{C})$, $\mathcal{C}_{\mathcal{I}}(\mathbf{g})$ is the u-tuple

$$\Big({\prod_{i\in\mathcal{I}_1}}' g_i,\dots,{\prod_{i\in\mathcal{I}_u}}' g_i\Big).$$

The notation $\prod'$ means take the product of the g_i s in the correct order. Note: The result of coalescing is a u-tuple that may not generate a transitive subgroup of $G\le S_n$. That is, it gives branch cycle descriptions of covers of $\mathbb{P}^1$ that may not be connected.

For the partition of (3.20) we define a *specialization sequence*. This consists of a sequence of étale covers

$$\psi_0:V_0\to\mathbb{P}^r\setminus D_r \text{ and } \psi_{\mathcal{I}_j}:V_{\mathcal{I}_j}\to D^0_{\mathcal{I}_j},\ j=1,\dots,s-1,$$

with the following property. Let $\bar\psi_{\mathcal{I}_j} : \bar V_{\mathcal{I}_j} \to D_{\mathcal{I}_j}$ be the unique normalization of the completion of $\psi_{\mathcal{I}_j}$ to a cover of $D_{\mathcal{I}_j}$. Form this as follows. Let $\bar V_{\mathcal{I}_j}$ be the normalization of $D_{\mathcal{I}_j}$ in the function field of $V_{\mathcal{I}_j}$ [**M**, p. 396-7]. Then,

(3.21a) $\psi_{\mathcal{I}_{j+1}} : V_{\mathcal{I}_{j+1}} \to D^0_{\mathcal{I}_{j+1}}$ factors through the restriction $\bar\psi_{\mathcal{I}_j} : \bar V_{\mathcal{I}_j} \to D_{\mathcal{I}_j}$ over $D^0_{\mathcal{I}_{j+1}}$, $j = 1, \dots, s-2$.

(3.21b) An analog to (3.21a) for relating ψ_0 to $\psi_{\mathcal{I}_1}$.

We say this is a specialization sequence starting at V_0.

Hypotheses (3.3a) and (3.3b) produce a total family $\Phi : \mathcal{T} \to \mathcal{H}(G, \mathbf{C}) \times \mathbb{P}^1$ over $\mathbb{Q}$ with the following property. For $\boldsymbol{p} \in \mathcal{H}$, the fiber $\mathcal{T}_{\boldsymbol{p}} = \Phi^{-1}(\boldsymbol{p} \times \mathbb{P}^1)$ covers $\mathbb{P}^1$ by projection on the second factor. This cover should be in the equivalence class of covers $\boldsymbol{p}$ represents. In particular, each such cover has a fixed degree n. Suppose you have a specialization sequence. Lemma 3.22 requires extra hypotheses to define the pullback over a specialization sequence.

First, consider pullback over V_0. As before, U_r is $\mathbb{P}^r \setminus D_r$. Form the fiber product $V_0 \times_{U_r} \mathcal{H} = \mathcal{H}_{V_0}$. Then, form the fiber product (with obvious maps):

$$\mathcal{T}_{V_0} = \mathcal{T} \times_{\mathcal{H} \times \mathbb{P}^1} (\mathcal{H}_{V_0} \times \mathbb{P}^1). \tag{3.22}$$

Thus, $\mathcal{T}_{V_0}$ is a family of degree n covers by projection onto $\mathcal{H}_{V_0} \times \mathbb{P}^1$. All covers in the family are in the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$. As above, complete and normalize $\mathcal{H}_{V_0}$ to produce $\bar{\mathcal{H}}_{V_0} \to \mathbb{P}^r$. Also, complete and normalize $\mathcal{T}_{V_0}$ over $\bar{\mathcal{H}}_{V_0} \times \mathbb{P}^1$ to get a cover $\bar{\mathcal{T}}_{V_0} \to \bar{\mathcal{H}}_{V_0} \times \mathbb{P}^1$. Finally, let $\mathcal{H}_1$ (resp., $\mathcal{T}_1$) be the normalization of the restriction of $\bar{\mathcal{H}}_{V_0}$ (resp., $\bar{\mathcal{T}}_{V_0}$) over $D^0_{\mathcal{I}_1}$ (resp., $D^0_{\mathcal{I}_1} \times \mathbb{P}^1$). Here is the hypothesis we need.

(3.23a) $\mathcal{T}_1 \to \mathcal{H}_1 \times \mathbb{P}^1$ is a family of degree n covers.

Continue inductively for the analog of property (3.23a).

(3.23b) $\mathcal{T}_j \to \mathcal{H}_j \times \mathbb{P}^1$ is a family of degree n covers; the specialization of the family for $j-1$ using $V_{\mathcal{I}_{j-1}}$, $j = 1, \dots, s-1$.

Some covers in the family may not be irreducible. For example, Lemma 3.22 produces examples were certain covers will be n copies of $\mathbb{P}^1$. Zariski's connectedness theorem say all fibers of a connected family are connected. So, for this example you would think we mean n copies pasted together over s points. That last normalization, however, before declaring the definition of $\mathcal{H}_1$ could disconnect components.

We can restrict a specialization sequence to $\mathcal{H}_O$ for any orbit O of H_r on $\mathrm{Ni}(G, \mathbf{C})$. The proof of Lemma 3.22 needs a technical point. We can restrict construction (3.23) over $\mathbb{A}^r$, the subset of $\mathbb{P}^r$ in the image of $\mathbb{A}^r \subset (\mathbb{P}^1)^r$ where $x_i \ne \infty$, $i = 1, \dots, r$.

LEMMA 3.22. *Assume the hypotheses of Theorem* 3.21. *Let O be any orbit of H_r acting on* $\mathrm{Ni}(G, \mathbf{C})$. *Consider the image $\mathcal{C}_{\mathcal{I}_s}(O)$ of O under the last of the coalescing operators from sequence* (3.20). *Then, $\mathcal{C}_{\mathcal{I}_s}(O)$ contains* $(1, 1, \dots, 1)$ *if* *and only if O contains HM representatives. Further, suppose we have a specialization sequence (over $\mathbb{A}^r$) having property* (3.23). *Restrict the sequence to $\mathcal{H}_O$. The family induced over $V_{\mathcal{I}_s,O}$ consists of covers with branch cycles in $\mathcal{C}_{\mathcal{I}_s}(O)$. Finally, there is a specialization sequence satisfying* (3.23). *In particular, $\mathcal{H}_O$ has $\mathbb{Q}$ as field of definition.*

PROOF. The statement on $\mathcal{C}_{\mathcal{I}_s}(O)$ follows from the definitions once we know there is only one orbit containing HM representatives (Theorem 3.21). Existence and properties of a specialization sequence over $\mathbb{A}^r$ is implicit in [**Fr5**, §4]. In fact, this proves its existence without the center hypothesis. (This is necessary, because after coalescing, we lose that hypothesis.) The difference between $\mathbb{A}^r$ and $(\mathbb{P}^1)^r$ is that there is a (continuous) *section of base points* for $\mathbb{P}^1$ minus its branch points over $V^r = \mathbb{A}^r \setminus \Delta_r$. This means, for each $\boldsymbol{y} \in V^r$, representing r ordered branch points, there is a continuous assignment of $x_0(\boldsymbol{y}) \in \mathbb{P}^1 \setminus \boldsymbol{y}$.

The last statement is like the end of the proof of Galois Invariance Theorem 3.16. Any $\tau \in G_{\mathbb{Q}}$ acts on the whole induced family over a specialization sequence. Suppose $\mathcal{H}_O$ and $\mathcal{H}_{O'}$ are conjugate. Then, τ takes sequence (3.23) applied to $\mathcal{H}_O$ to the sequence applied to $\mathcal{H}_{O'}$. In particular, $\mathcal{C}_{\mathcal{I}_s}(O')$ contains $(1,\dots,1)$. This contradicts the first statement in Theorem 3.21. □

COROLLARY 3.23. *Let p be a prime dividing $|G|$. Assume $\mathbf{C}$ are p' conjugacy classes G satisfying* (3.17) *of Theorem* 3.21. *Assume, also, the Center Hypothesis (Def.* 3.5*) for (G,p). Then, each level $\mathcal{H}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$ of the modular tower for $(G,\mathbf{C})$ has a (nonempty) absolutely irreducible component over $\mathbb{Q}$.*

PROOF. We show (3.17a) and (3.17b) hold for $\mathrm{Ni}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$. First (3.17a). Let $\mathbf{C}'$ be $\mathbf{C}$ after removing two conjugacy classes that must pass the HM-gcomplete test. Let $\mathbf{g} \in \mathbf{C}'$. By assumption, $\langle \mathbf{g} \rangle$ generates G. Now let $\tilde{\mathbf{g}} \in {}_p^n\tilde{\mathbf{C}}'$ lie over $\mathbf{g}$. As ${}_p^n\tilde{G} \to G$ is a Frattini cover, $\langle \tilde{\mathbf{g}} \rangle$ generates ${}_p^n\tilde{G}$. This concludes the proof (3.17a) holds.

That leaves showing $\mathrm{Ni}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$ is nonempty and contains an HM representative. As in Ex. 3.13, the lift of an HM representative to ${}_p^n\tilde{G}$ is automatically an HM representative of $\mathrm{Ni}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$. □

APPENDIX. DISTINGUISHED PROBLEMS

We use the notation of Nielsen classes $\mathrm{Ni}(G,\mathbf{C})$ freely from §III.A.

§**App.A. Modular representation problems.** Recall the Center Hypothesis 3.5 on the characteristic quotients ${}_p^n\tilde{G}$ of the universal p-Frattini cover ${}_p\tilde{G}$ of G. It applies to Th. 3.4 to produce rationality results as in Cor. 3.23. Unless $\mathbf{C}$ is a rational union of conjugacy classes, the Hurwitz space $\mathcal{H}({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$ has *no* component with field of definition $\mathbb{Q}$ (see end of §III.A). This comes from the most mundane use of the Branch Cycle Argument applying the action of the cyclotomic character (Part A of the proof of Theorem 3.16). Thus, for finding $\mathbb{Q}$ components, the hypothesis $\mathbf{C}$ is a rational union of conjugacy classes is both necessary and convenient. The converse, however, that the moduli space $\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ has $\mathbb{Q}$ as field of definition, requires ${}^n_p\tilde{G}$ to have no center. (See Moduli Space Condition (C.8).) While a finer analysis of relaxing this hypothesis is welcome, we should know when it holds. Lemma 3.6 says it holds when G is perfect, including when G is a nonabelian simple group.

PROBLEM A.1. *For what groups (and primes p dividing their orders) does the Center Hypothesis hold?*

LEMMA A.2. *If $\mathbf{1}_{{}^n_p\tilde{G}}$ appears at the left of a Loewy display for $\ker_n / \ker_{n+1}$, then $\mathbf{1}_{{}^k_p\tilde{G}}$ appears at the left of a Loewy display for $\ker_k / \ker_{k+1}$ for $k > n$.*

PROOF. Let $P_{\mathbf{1},k}$ be the projective indecomposable for the trivial representation of ${}^k_p\tilde{G}$. Also, P_k is the minimal projective module for ${}^k_p\tilde{G}$ that maps surjectively to the kernel of $P_{\mathbf{1},k} \to \mathbf{1}$. By hypothesis, $\mathbf{1}$ appears at the far left of the Loewy display of P_n. From the argument of Lemma 3.6, it appears at the far right of the Loewy display of P_n. Lemma 2.6 gives a surjective map $P_{\mathbf{1},k} \to P_{\mathbf{1},n}$ of ${}^k_p\tilde{G}$ modules for $k \geq n$. Thus, the far right of the Loewy display for the kernel of $P_{\mathbf{1},k} \to \mathbf{1}$ contains the far right of the Loewy display for $P_{\mathbf{1},n}$. Conclude: $\mathbf{1}$ appears in the far right of the Loewy display of P_k. So, it appears in the far left of this Loewy display. Conclude this lemma from Lemma 2.3. $\square$

Lemma A.2 says a nontrivial center to ${}^n_p\tilde{G}$ will persist to a nontrivial center of ${}^k_p\tilde{G}$, $k \geq n$. Still, there may be a way around this. Assume n is the first value of k for which ${}^k_p\tilde{G}$ has a nontrivial center. Let V_n be the largest submodule of $\ker_{n-1} / \ker_n$ on which ${}^n_p\tilde{G}$ acts trivially. Then, ${}^n_p\tilde{G} \to G$ factors through a natural Frattini cover $H = {}^n_p\tilde{G}/V_n \to G$. If $\mathbf{1} \to \mathbf{1}$ does not appear at the left of the Loewy display of $\ker_{n-1} / \ker_n$, then H has no center. A further hypothesis would allow replacing ${}^n_p\tilde{G}$ with H in the modular tower construction.

PROBLEM A.3. *In the notation above, for what groups is $\dim_{\mathbb{F}_p}(V_n)$ bounded as a function of n? When this holds, when can we assure ${}^n_p\tilde{G}/V_n$ has no center?*

Self-normalizing stabilizer subgroups arise in interpreting the moduli spaces $\mathcal{H}^{\mathrm{ab}}$ (Addendum to Thm. 3.4). §III.C has a natural case for considering extending permutation representations on the characteristic quotients of ${}^n_p\tilde{G}$. This has $G \leq S_k$ and the stabilizer $G(1)$ in the representation has order prime to p. Then, all characteristic quotients have one conjugacy class of copies of $G(1)$. This is the analog of Problem A.1 for that question.

PROBLEM A.4. *Consider (G, T, p) with G a nonabelian simple group, T a primitive permutation representation of G, and p a prime not dividing $|G(1)|$. For which (G, T, p) does the conclusion of Self-Normalizing Problem 3.8 hold?*

Remark 2.10 notes that $G = A_5$ and $p = 5$ is the other extreme of Prop. 2.9. Here the module $\ker_0 / \ker_1$ is equal to the module induced from the universal 5-Frattini module for A_4. Example 3.9 checks the case $n = 1$ in this example. We haven't yet checked if there is a positive conclusion to Problem A.4 for all n in this example.

Even if p does divide $|G(1)|$, there may be groups ${}^p_n\tilde{G}(1)$ extending $G(1)$ in each of the characteristic quotients ${}^n_p\tilde{G}$. We must, however, assure the extensions of $G(1)$ give a faithful coset representation for each ${}^n_p\tilde{G}$. This doesn't always happen. Again take $G = A_5$ and $p = 2$. From Prop. 2.9, the only subgroup of ${}^n_p\tilde{G}$ mapping surjectively to $G(1) = A_4$ is the full pullback of A_4 in ${}^n_p\tilde{G}$. This can't give a faithful representation of ${}^n_p\tilde{G}$. Is this outcome characteristic of being on the extreme end of the Prop. 2.9 conclusion?

§III.E discusses groups G for which $|G|$ has prime divisors p that ramify exceptionally. Lemma 3.17 says all p' conjugacy classes lie in a proper normal subgroup N of G. Is there a natural converse?

Problem A.5. *Suppose N is a proper normal subgroup of G and N contains all conjugacy classes of elements of order r^t with $r \neq p$ a prime. When does this imply N contains a normal p' complement?*

Kantor used the classification of finite simple groups to show the following (in the notation of Def. 3.18) [**FKS**].

(A.1) (3.14) holds if $\mathbf{C}$ contains each prime-power order conjugacy class of G.

Corollary 3.23 applies to a group that is p-gcomplete. Lemma 3.17 suggests (A.1) could help classify groups with no p' compliment that aren't p-gcomplete.

§**App.B. Curves tesselating a general Hurwitz space.** As in §III.F, let D_r be the discriminant in $\mathbb{P}^r$. The fat diagonal $\Delta_r \subset (\mathbb{P}^1)^r$ lies above it in the symmetry map $\Theta_r : (\mathbb{P}^1)^r \to \mathbb{P}^r$. [**Fr5**] and [**DFr2**] refer to the fundamental group of $(\mathbb{P}^1)^r \setminus \Delta_r$ as the *straight Hurwitz* monodromy group SH_r. It is the kernel of the natural map $H_r \to S_r$ with the effect $Q_i \mapsto (i\,i{+}1)$, $i = 1, \dots, r{-}1$ (§III.A). Given a Hurwitz space cover $\mathcal{H} \to \mathbb{P}^r \setminus D_r$, form the fiber product

$$\mathcal{H}' = \mathcal{H} \times_{\mathbb{P}^r} (\mathbb{P}^1)^r \setminus \Delta_r.$$

Suppose $\mathcal{H}$ comes from H_r acting on some absolute Nielsen classes $\mathrm{Ni}(\mathbf{C})^{\mathrm{ab}}$ (see (3.1d)). Components of $\mathcal{H}'$ correspond to orbits of SH_r on the same absolute Nielsen classes.

Consider Def. 3.1a for Nielsen classes. An $\omega \in S_r$ acts on $\mathbf{C}$ by permuting the entries of $\mathbf{C}$. Form the group of symmetries of $\mathbf{C}$: $I_{\mathbf{C}} = \{\omega \in S_r \mid (\mathbf{C})\omega = \mathbf{C}\}$. Note: SH_r preserves the order of the conjugacy classes in a Nielsen class $\mathrm{Ni}(\mathbf{C})$. Thus, the pullback of each component of $\mathcal{H}$ to $\mathcal{H}'$ breaks into at least $(S_r : I_{\mathbf{C}})$ components. Each ordering $(\mathbf{C})\omega$ of $\mathbf{C}$ produces a union $\mathcal{H}'_\omega$ of components on

$\mathcal{H}'$ lying above the given component of $\mathcal{H}$. To assess the components of $\mathcal{H}'_\omega$ consider the action of SH_r on

$$\mathrm{SNi}((\mathbf{C})\omega) = \{\mathbf{g} \in G^r \mid \langle \mathbf{g} \rangle = G,\ g_1 \cdots g_r = 1,\ g_i \in \mathrm{C}_{(i)\omega}, i = 1, \dots, r\}.$$

Let $N_{S_n}(\mathbf{C})'$ be the subgroup of $N_{S_n}(\mathbf{C})$ that stabilizes $\mathrm{SNi}(G, (\mathbf{C})\omega)$. Orbits, modulo the action of $N_{S_n}(\mathbf{C})'$ corresponds exactly to (absolutely irreducible) components of $\mathcal{H}'_\omega$. Similar statements hold for representations of H_r on $\mathrm{Ni}(\mathbf{C})$ corresponding to components of $\mathcal{H}^{\mathrm{in}}$.

Rational Conjugacy Class Observation B.1. The proof of Lemma 3.20 gives a stronger result: HM representatives in $\mathrm{SNi}(\mathbf{C})$ fall in one SH_r orbit. Thus, there is a version of Theorem 3.21 referring to SNi. One point, however, complicates this result and the corresponding corollaries. Assume $\mathbf{C}$ is a rational union of conjugacy classes with a particular conjugacy class, say, C_1, not rational. Suppose $\mathcal{H}_1$ is an absolutely irreducible $\mathbb{Q}$ component of $\mathcal{H}$. Then, no absolutely irreducible component of $\mathcal{H}'$ lying over $\mathcal{H}_1$ will have field of definition $\mathbb{Q}$. So, if our search is for $\mathbb{Q}$ components of $\mathcal{H}'$, *all* conjugacy classes must be rational. This condition holds in many important examples (modular curves and Ex. 3.13 included). Still, this illustrates that adding an ordering to the branch points, defies the generality of our results. □

Suppose $\mathcal{H}' \to (\mathbb{P}^1)^r \setminus \Delta_r$ has field of definition F. Let $(\mathbb{P}^1)^{r-1}$ be the *last* $r-1$ copies of $\mathbb{P}^1$ in the $(\mathbb{P}^1)^r$. Choose any $(x'_2, \dots, x'_r) = \boldsymbol{x}' \in (\mathbb{P}^1)^{r-1} \setminus \Delta_{r-1}$. Regard the fiber of $\mathcal{H}'$ over $\boldsymbol{x}'$ as a curve $\mathcal{H}'_{\boldsymbol{x}'}$ over $\mathbb{P}^1_{x_1} \times \boldsymbol{x}' \cong \mathbb{P}^1$. The copy of $\mathbb{P}^1$ is the first coordinate of $(\mathbb{P}^1)^r$. Here, $\mathcal{H}'_{\boldsymbol{x}'}$ is missing points over the values of x_1 equal to $(x'_2, \dots, x'_r)$. Complete this curve according to Riemann's Existence Theorem to get a ramified cover $\bar{\mathcal{H}}'_{\boldsymbol{x}'} \to \mathbb{P}^1_{x_1} \times \boldsymbol{x}'$. If $\boldsymbol{x}'$ has coordinates in F, this cover has field of definition F. Express a description of the branch cycles of this curve using the classical generators $Q_1, \dots, Q_{r-1}$ (for example, [**Fr7**]) as

$$\begin{aligned} a_{1\,2} = Q_1^{-2}, a_{1\,3} =& Q_1 Q_2^{-2} Q_1^{-1}, \dots, \\ & a_{1\,r-1} = Q_1 \dots Q_{r-2} Q_{r-1}^{-2} Q_{r-2}^{-1} \dots Q_1^{-1}. \end{aligned} \tag{B.1}$$

Notice the product 1 condition ((i) of §I.F) translates to condition (3.1c) for $Q_1, \dots, Q_{r-1}$. The $a_{1\,j}$ s, however, may not generate a transitive group in their action on a given SH_r orbit. For example, we haven't checked the following.

Problem B.2. *Do all HM representatives of* SNi *fall in one orbit under the action of the $a_{1\,j}$ s, $j = 2, \dots, r-1$ (Th. 3.21)?*

One approach to formulating generalizations of Theorem 1.1 is to fix a point $\boldsymbol{x}' \in (\mathbb{P}^1)^{r-1} \setminus \Delta_{r-1}$. Assume a situation with a positive conclusion for Problem B.2 and all conjugacy classes in $\mathbf{C}$ are rational. For each n, let $\mathcal{H}_n$ be the level n Hurwitz space of the modular tower. Then, Corollary 3.23 produces an absolutely irreducible $\mathbb{Q}$ component $\mathcal{H}^*_n$ of the pullback $\mathcal{H}'_n$ of $\mathcal{H}_n$. Choose these compatibly so the natural map $\mathcal{H}'_n \to \mathcal{H}'_{n-1}$ maps $\mathcal{H}^*_n$ to $\mathcal{H}^*_{n-1}$. Finally, restrict these maps to the fibers over any $\mathbb{Q}$ point $\boldsymbol{x}' \in (\mathbb{P}^1)^{r-1} \setminus \Delta_{r-1}$ to get a sequence of curves $\mathcal{H}^*_{n,\boldsymbol{x}'}$ similar to the modular curve tower of §I.A. The first statement in Theorem 1.1, using Hilbert's irreducibility theorem, works as well in application to the sequence of covers $\mathcal{H}^*_{n,\boldsymbol{x}'} \to \mathbb{P}^1_{x_r}$, $n = 0, 1, \ldots$. A precise analog for $({}^n_p\tilde{G}, \widehat{{}^n_p\tilde{G}})$-realization, however, requires knowing something of the corresponding inner version of this sequence of covers to give control of $\widehat{{}^n_p\tilde{G}}$. The second statement of Theorem 1.1 would follow if we knew the genus of $\mathcal{H}^*_{n,\boldsymbol{x}'}$ goes to ∞ with n.

PROBLEM B.3. *Is there a result analogous to the last statement of Theorem 1.1 for the sequence of curves $\mathcal{H}^*_{n,\boldsymbol{x}'}$, $n = 1, 2, \ldots$? In fact, when does the genus of $\mathcal{H}^*_{n,\boldsymbol{x}'}$ go to ∞ with n?*

Recall: A variety W is *unirational* (over a field F) if there is an integer n and a birational map $\mathbb{P}^n \to W$ (over F) onto a Zariski open subset of W. Consider the case of many repetitions of any given conjugacy classes (as in the discussion around condition (3.9)). Then, we've greatly weakened the possible conclusions for the original problem by pulling back to $(\mathbb{P}^1)^r$. For example, if $r = 4$, $\mathcal{H}^*_{n,\boldsymbol{x}'}$ supports the first cohomology of $\mathcal{H}'$. (This is because the first cohomology group of a compactification of $\mathcal{H}'$ is a birational invariant, and this space is birational to $\mathcal{H}^*_{n,\boldsymbol{x}'} \times (\mathbb{P}^1)^3$.) Thus, as [**Fr7**] examples show, even if r is small (like 4), $\mathcal{H}^*_0$ may be far from unirational while its image in $\mathcal{H}$ is. As in Observation B.1, an ordering of the branch points destroys important questions in the area. Part IV of the sequel will refine these questions to deal directly with $\mathcal{H}$.

§**App.C. Complex conjugation on Hurwitz space orbits.** Our diophantine starting point is real points and points over finite fields on a modular tower. We define our terms with real points. Comments C.5 below model, for complex conjugation, applying the Drinfeld-Ihara relations for the Grothendieck-Teichmüller group. The goal is to determine fields of definition of components of a modular tower. §App.D outlines an approach to finding projective sequences of real points on a modular tower. Finally, §App.E discusses analogous ideas over finite fields.

Let $\{\mathcal{H}_n = \mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}}),\ n = 0, 1, \ldots\}$ be a modular tower attached to the characteristic quotients of ${}_p\tilde{G}$. Certain circumstances require treating the action of H_r on inner classes differently than on absolute classes (§III.A). For the former, use the notation $\mathcal{H}^{\rm in}_n$ and for the latter $\mathcal{H}^{\rm ab}_n$. In some contexts we drop this notation, implying one or the other of these hold. Consider finding components of $\mathcal{H}_n$ and points on $\mathcal{H}_n$ defined over $\mathbb{R}$. Thus, we may relax our standard assumption that $\mathbf{C}$ is a rational union of conjugacy classes. If $\mathbf{C}^{-1} = \mathbf{C}$ ($a = -1$ in Def. 3.2) then [**FrV**, Prop. 3] shows (under the assumption G has no center)

$\mathcal{H}_0 = \mathcal{H}(G, \mathbf{C})$ has field of definition $\mathbb{R}$. The argument that shows ${}_n\tilde{\mathbf{C}}^{-1} = {}_n\tilde{\mathbf{C}}$ for all n appears in Ex. 3.13. Putting these conclusions together gives the following criterion for all levels of a modular tower to have field of definition $\mathbb{R}$.

LEMMA C.1. *Assume* $\mathbf{C}$ *is a collection of* p' *conjugacy classes of* G, *and* $\mathbf{C}^{-1} = \mathbf{C}$. *Also, suppose the center hypothesis holds for* (G, p) *as in Def. 3.5. Then, all levels* $\mathcal{H}_n$ *of the modular tower have field of definition* $\mathbb{R}$.

[**DFr2**, Th. 4.4] explicitly describes real points on a Hurwitz space $\mathcal{H}(G, \mathbf{C})^{\mathrm{ab}}$ or $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$. This, however, uses the assumptions of no center. [**DFr**, Comment 3 of §3.5] gives exact criteria without the center hypothesis, for a cover to have field of definition *or* field of moduli in $\mathbb{R}$. Points on $\mathcal{H}^{\mathrm{ab}}$ don't have the interpretation of the Addendum to Theorem 3.4 when G has a center.

PROBLEM C.2. *Generalize* [**DFr2**, Th. 4.4] *even if* G *has a center. In particular, add data to a Hurwitz space so that a real point on this space will produce a representative with a model over* $\mathbb{R}$.

We come to the main discussion of this subsection. Let W be any absolutely irreducible variety over a field F of characteristic 0. The arithmetic fundamental group $\hat{\pi}_1^{ar}(W)$ is the profinite limit of the Galois groups of étale Galois covers $V \to W$. Let M be the maximal extension of $F(W)$ étale over W in the algebra closure $\overline{F(W)}$. Then, $G(M/F(W))$ is isomorphic to $\hat{\pi}_1^{ar}(W)$. Similarly, $\hat{\pi}_1^{ge}$ is isomorphic to $G(M/\bar{F}(W))$. Now suppose F has characteristic 0.

Take $\hat{\pi}_1(W)$ to be the profinite completion of $\pi_1(W)$ over all subgroups of finite index in $\pi_1(W)$. From the Grauert-Remmert generalization of Riemann's Existence Theorem [**GR**]: The natural homomorphism $\pi_1(W) \to \hat{\pi}_1^{ge}$ is surjective. A profinite group is *residually finite* if the intersection of all subgroups of finite index is $\{1\}$. If, however, $\pi_1(W)$ isn't residually finite, then the map is not injective. Serre [**Se4**, p. 60] asks if G. Higman's example of a discrete group with no subgroups of finite index is the fundamental group of an algebraic variety. He mentions $\pi_1(W)$ is residually finite if it embeds in a linear group. See [**I3**] for this result when $W = \mathbb{P}^r \setminus D_r$. Use the notation of (3.1) for the images in $\hat{\pi}_1^{ge}(\mathbb{P}^r \setminus D_r)$ of the generators Q_i, $i = 1, \dots, r-1$. [**T**] produces a projective nonsingular variety whose fundamental group isn't residually finite. This example has many homomorphisms to finite groups, unlike Higman's example.

REAL COMPONENTS-POINTS PROBLEM.

(C.1a) *Give a procedure to identify the existence of a projective system of (absolutely irreducible) components* $\mathcal{H}_n'$ *of* $\mathcal{H}_n$ *with field of definition* $\mathbb{R}$?

(C.1b) *Give a procedure to identify the existence of a projective system of points* $\{\boldsymbol{p}_n \in \mathcal{H}_n\}_{n=0,1,\dots}$ *in* $\mathbb{R}$?

This section translates (C.1a) to a question on the universal Frattini cover of G. §App.D does the same for (C.1b), by introducing the *universal Artin-Schreier* cover of a group with chosen involution conjugacy classes. The meaning of (C.1a) should be clear. By projective system of points in (C.1b) we mean the analog of the situation of §I.A: the natural map (following Def. 3.10) takes $\boldsymbol{p}_n \in \mathcal{H}_n$ to $\boldsymbol{p}_{n-1}$, $n = 1, 2, \dots$. Start with an action of complex conjugation on paths representing homotopy classes in $\mathbb{P}^r \setminus D_r$ from a basepoint $\boldsymbol{x}_0$. Then, this choice produces paths on $\mathbb{P}^1 \setminus \boldsymbol{x}_0$ to decide what complex conjugation does to the covers representing points of $\mathcal{H}_n$. For there to be a projective system of real points over a specific $\boldsymbol{x}_0$, we must have $\boldsymbol{x}_0 \in \mathbb{P}^r \setminus D_r(\mathbb{R})$. This implies $\boldsymbol{x}_0$ is the image from $(\mathbb{P}^1)^r \setminus \Delta_r$ of an ordered r-tuple $\boldsymbol{x}'$ closed under complex conjugation. Thus, we may assume

(C.2) $\boldsymbol{x}' = (x'_1, \dots, x'_r)$ with $x'_1 < x'_2 < \cdots < x'_s$ in $\mathbb{P}^1(\mathbb{R})$ and $x'_{s+j}, x'_{s+r-j+1}$ complex conjugate pairs, $j = 1, \dots, (r-s)/2$.

The relation $x'_1 < x'_2 < \cdots < x'_s$ means these fall on the real circle in the given order on the Riemann sphere ($r \geq 3$). For the sequel include the relation $x'_s < x'_1$, meaning that going counterclockwise around $\mathbb{R} \cup \{\infty\}$, x'_1 follows x'_s.

The case $s = r$ is most significant: other cases revert to this following computations of [**DFr2**]. Therefore, restrict to this case:

(C.3) $\boldsymbol{x}'$ is a set of real points ordered on $\mathbb{P}^1(\mathbb{R})$ according to their subscripts.

Let B_i be a clockwise circle on $\mathbb{P}^1$ with a marked diameter on the real axis having x'_i and x'_{i+1} as endpoints. (One of these has x'_r and x'_1 at the endpoints of the directed diameter.) Parametrize the top of B_i with $t \mapsto B_i^+(t)$ on $[0,1]$, so $B_i^+(0) = x'_i$ and $B_i^+(1) = x'_{i+1}$. Similarly, parametrize the bottom of B_i with $t \mapsto B_i^-(t)$ on $[0,1]$ so $B_i^-(0) = x'_{i+1}$ and $B_i^-(1) = x'_i$. Consider the path

(C.4a) $$t \mapsto (x'_1, \dots, x'_{i-1}, B_i^+(t), B_i^-(t), x'_{i+2}, \dots, x'_r),\ t \in [0,1].$$

The image of (C.4a) in $\mathbb{P}^r \setminus D_r$ represents the braid group generator Q_i^{-1} (from (3.1)). The inverse of path (C.4a) is

(C.4b) $$t \mapsto (x'_1, \dots, x'_{i-1}, \bar{B}_i^-(t), \bar{B}_i^+(t), x'_{i+2}, \dots, x'_r),\ t \in [0,1].$$

where the notation $\bar{B}$ means we applied complex conjugation to the coordinate.

Complex conjugation acts on all paths based at $\boldsymbol{x}_0$. So, it induces an operator κ on homotopy classes of paths and thus on $\hat{\pi}_1^{ar}$ (see Proof–Comments below). Also, κ acts on functions expanded around $\boldsymbol{x}_0$ by acting on their coefficients. This latter action gives a section of $\hat{\pi}_1^{ar} = \hat{\pi}_1^{ar}(\mathbb{P}^r \setminus D_r, \boldsymbol{x}_0) \to G(\mathbb{C}/\mathbb{R})$. Use κ for the corresponding element of $\hat{\pi}_1^{ar}$.

Complex Conjugation Proposition C.2. *Complex conjugation of the image of* (C.4a) *in* $\mathbb{P}^r \setminus D_r$ *is the image of* (C.4b). *Conjugation by* κ *gives an automorphism of* $\hat{\pi}_1^{ge}(\mathbb{P}^r \setminus D_r, \boldsymbol{x}_0)$ *mapping* Q_i *to* Q_i^{-1}.

Exchange $r+1$ *for* r *and consider the induced effect of* κ *on the elements*

(C.5a) $a_{1\,2} = Q_1^{-2}, a_{1\,3} = Q_1 Q_2^{-2} Q_1^{-1}, \dots, a_{1\,r} = Q_1 \cdots Q_{r-1} Q_r^{-2} Q_{r-1}^{-1} \cdots Q_1^{-1}.$

Then, κ maps this set in order to

(C.5b) $$a_{1\,2}^{-1},\ a_{1\,2}a_{1\,3}^{-1}a_{1\,2}^{-1},\dots,\ a_{1\,2}\cdots a_{1\,r-1}a_{1\,r}^{-1}a_{1\,r-1}^{-1}\cdots a_{1\,2}^{-1}.$$

PROOF–COMMENTS. All unramified covers of $\mathbb{P}^r\setminus D_r$ have field of definition $\bar{\mathbb{Q}}$: consequence of the *general* Riemann's existence theorem [**GR**]. For such a cover $Y\to\mathbb{P}^r\setminus D_r$, α in the ordinary fundamental group acts through analytic continuation as a permutation of the fiber on Y above $\boldsymbol{x}_0$. Running through the fibers $Y_{\boldsymbol{x}_0}$ of covers, α produces compatible actions on all these fibers in the following sense. If $\psi: Y'\to\mathbb{P}^r\setminus D_r$ factors through Y then the action of α commutes with ψ. Thus, interpret $\hat{\pi}_1^{ge}(\mathbb{P}^r\setminus D_r,\boldsymbol{x}_0)$ as *all* compatible maps on the system of fibers of covers over $\boldsymbol{x}_0$ (as in [**FrV**, §1.2] or [**I**, §2]). Equivalently, α gives an analytic continuation on the germs of algebraic functions on Y, after expansion around points of the fiber over $\boldsymbol{x}_0$.

Consider $\sigma\in G_{\mathbb{Q}}$ (resp., $\sigma=\kappa$) and $\boldsymbol{x}_0$ with coordinates in $\mathbb{Q}$ (resp., $\mathbb{R}$). Then, σ takes $\alpha\in\hat{\pi}_1^{ge}$ to the element $\sigma(\alpha)$ which has the effect

(C.6) $$\boldsymbol{y}\in Y_{\boldsymbol{x}_0}\mapsto\sigma\circ\alpha\circ\sigma^{-1}(\boldsymbol{y}).$$

Calculate this when $\alpha=Q_i$, $\boldsymbol{x}_0$ is the image of $\boldsymbol{x}'\in(\mathbb{P}^1(\mathbb{R}))^r\setminus\Delta_r$ and $\sigma=\kappa$ as above. Direct application of κ to the representing path $\hat{Q}_i$ for Q_i gives

(C.7) $$\kappa\circ Q_i\circ\kappa^{-1}(\boldsymbol{y})=\kappa(\hat{Q}_i)(\kappa\circ\kappa^{-1}(\boldsymbol{y}))=\hat{Q}_i^{-1}(\boldsymbol{y}).$$

Check κ on (C.5a) by substituting Q_i^{-1} for Q_i. □

Now we interpret if components of $\mathcal{H}(G,\mathbf{C})^{\text{in}}=\mathcal{H}$, *as moduli spaces*, have field of definition in $\mathbb{R}$. Let $\mathcal{H}^*$ be an absolutely irreducible component of $\mathcal{H}$. Consider $\sigma\in G_{\mathbb{Q}}$. Suppose the cover $\Psi:\mathcal{H}^*\to\mathbb{P}^r\setminus D_r$ is a moduli space defined over the fixed field of σ. From [**Fr5**, Th. 5.1] or [**FrV**, Th. 1], this requires more than the field of definition of Ψ is in the fixed field of σ. For $\boldsymbol{p}\in\mathcal{H}^*(\bar{\mathbb{Q}})$, let $\psi:X\to\mathbb{P}^1$ represent $\boldsymbol{p}$. Then, the following holds.

(C.8a) Extension of σ to the cover ψ produces a cover $\psi^\sigma: X^\sigma\to\mathbb{P}^1$ (corresponding to $\boldsymbol{p}^\sigma$) with $\boldsymbol{p}^\sigma\in\mathcal{H}^*(\bar{\mathbb{Q}})$.

For example, it is possible the cover $\Psi:\mathcal{H}^*\to\mathbb{P}^r\setminus D_r$ has a model with field of definition $\mathbb{Q}$ even if $\mathbf{C}$ isn't a rational union of conjugacy classes (Def. 3.2). This condition, however, is necessary for a model of $\Psi:\mathcal{H}^*\to\mathbb{P}^r\setminus D_r$ representing covers in the Nielsen class to have field of definition $\mathbb{Q}$.

Now turn (C.8a) into a combinatorial criterion. Assume (for simplicity) the branch points $\boldsymbol{x}=(x_1,\dots,x_r)$ of ψ are in the fixed field of σ. Let $(g_1,\dots,g_r)$ be a branch cycle description of ψ with respect to a specific set $(\bar{\Sigma}_1,\dots,\bar{\Sigma}_r)$ of homotopy classes of paths on $\mathbb{P}^1\setminus\{\boldsymbol{x}\}$. Thus, $(g_1,\dots,g_r)$ is in an H_r orbit O in $\mathrm{Ni}(G,\mathbf{C})$ (as in §III.A). Using this data, here is the meaning of (C.8a).

(C.8b) The branch cycle description $(g_1',\dots,g_r')$ for $\psi^\sigma: X^\sigma\to\mathbb{P}^1$ relative to the same paths $(\bar{\Sigma}_1,\dots,\bar{\Sigma}_r)$ is also in O.

Similar statements apply for $\sigma \in G(\bar{F}/F)$ where F is any field; choose $\boldsymbol{x}$ with coordinates in F. This includes $F = \mathbb{R}$ or an archimedean completion of $\mathbb{Q}$. Also, we may replace $\mathrm{Ni}(G, \mathbf{C})$ by $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$ corresponding to an appropriate permutation representation of G. Finally, let complex conjugation, κ, act on $\mathrm{Ni}(G, \mathbf{C})$ through the following formula:

$$\text{(C.9)} \qquad \mathbf{g} = (g_1, \dots, g_r) \in \mathrm{Ni}(G, \mathbf{C}) \mapsto \kappa(\mathbf{g}) = \\ (g_1^{-1}, g_1 g_2^{-1} g_1^{-1}, \dots, g_1 \cdots g_{r-1} g_r^{-1} g_{r-1}^{-1} \cdots g_1^{-1}).$$

For H a subgroup of G_F, let $F^{(H)}$ be the fixed field of H in $\bar{F}$.

Theorem C.3. *Assume G has no center. Choose an H_r orbit O on* $\mathrm{Ni}(G, \mathbf{C})$. *Denote the elements $\sigma \in G_{\mathbb{Q}}$ for which* (C.8b) *holds by H_O. Then, the moduli space component $\mathcal{H}^*$ of $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$ corresponding to O has the fixed field $\mathbb{Q}^{(H_O)}$ as its minimal field of definition.*

The analogous result holds if $\mathcal{H}^*$ is an absolutely irreducible component of $\mathcal{H}^{\mathrm{ab}}$ and if (3.5a) *or* (3.5b) *holds for the corresponding permutation representation $G \le S_n$. That is, $\boldsymbol{p} \in \mathcal{H}^*(\mathbb{Q}^{(H)})$ over $\boldsymbol{x}$ produces a regular field extension $L/\mathbb{Q}^{(H)}(x)$ of degree n with branch cycle description (relative to $(\bar{\Sigma}_1, \dots, \bar{\Sigma}_r)$) in the orbit O.*

Replace $\mathbb{Q}$ with $\mathbb{R}$ and $G_{\mathbb{Q}}$ by $G_{\mathbb{R}}$. Then, the results above apply. More explicitly, the following tests for these conditions hold.

(C.10a) (C.8b) *is true if and only if for some $\mathbf{g} \in O$, $\kappa(\mathbf{g}) \in O$. Similarly for the $\mathcal{H}^{\mathrm{ab}}$ version: Replace O by an H_r orbit in* $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$.

(C.10b) *Points $\boldsymbol{p} \in \mathcal{H}^{\mathrm{in}}(\mathbb{R})$ over $\boldsymbol{x}_0$ correspond exactly to $\mathbf{g} \in \mathrm{Ni}(G, \mathbf{C})$ with $\kappa(\mathbf{g}) = \gamma \mathbf{g} \gamma^{-1}$ for some involution $\gamma \in G$.*

(C.10c) *If* (3.5a) *or* (3.5b) *holds, points $\boldsymbol{p} \in \mathcal{H}^{\mathrm{ab}}(\mathbb{R})$ over $\boldsymbol{x}_0$ correspond exactly to $\mathbf{g} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$ with $\kappa(\mathbf{g}) = \gamma \mathbf{g} \gamma^{-1}$ for some involution $\gamma \in N_{S_n}(G)$.*

Proof. We've given references for everything excluding (C.10). Suppose $\psi : X \to \mathbb{P}^1$ has branch points $\boldsymbol{x}'$ (over $\boldsymbol{x}_0$ as above) and $\mathbf{g}$ as a description of branch cycles. [**DFr2**, Fig. 2] gives a set of paths $\mathbf{\Sigma} = (\bar{\Sigma}_1, \dots, \bar{\Sigma}_r)$ on $\mathbb{P}^1 \setminus \{\boldsymbol{x}'\}$ with $\kappa(\mathbf{g})$ a description of branch cycles of $\psi^\kappa : X^\kappa \to \mathbb{P}^1$ relative to $\mathbf{\Sigma}$. Thus, there is a precise condition for complex conjugation to map points of $\mathcal{H}^*$ into $\mathcal{H}^*$. It is that κ maps branch cycle descriptions of covers corresponding to the H_r orbit $O \subset \mathrm{Ni}(G, \mathbf{C})$ into O. From (C.8a) and (C.8b), this proves (C.10a). Replace these statements by $O \subset \mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$ for the $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{ab}}$ analog. Also, (C.7) says the κ operator anti-commutes with the action of H_r: $\kappa \circ Q = Q^{-1} \circ \kappa$. So, we need only check (C.10a) on one element of O.

Statement (C10.b) restates (***) of [**DFr**, §3.5, Comment 3]. Similarly, (C10c) restates [**DFr**, §3.5, Comment 2]. Both statements are addendum to [**DFr**, Th. 1.1]. For the continuing discussion below, we use the equivalent statements from replacing $\mathbf{g}$ by

(C.11a) $$\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_{r-1}) = (g_2 \cdots g_r, \dots, g_{r-1}g_r, g_r).$$

[**DFr**, (2.3)] says γ of (C.10b) or (C.10c) conjugates entries of $\boldsymbol{\alpha}$ to their inverses:

(C.11b) $$\gamma\boldsymbol{\alpha}\gamma^{-1} = (\alpha_1^{-1}, \dots, \alpha_{r-1}^{-1}). \qquad \square$$

Note: Application of [**DFr**, §3.5, Comment 3], to get (C.10b) doesn't require G to have a trivial center. Also, suppose the Center Hypothesis holds and $\{\mathcal{H}_n = \mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})^{\mathrm{in}},\ n = 0, 1, \dots\}$ is a modular tower. Let $\{O_n,\ n = 0, 1, \dots\}$ be a compatible system of H_r orbits on the respective Nielsen classes $\mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$. It is convenient to choose these through a compatible system of representatives ${}^n_p\tilde{\mathbf{g}} \in \mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$. That is, ${}^n_p\tilde{\mathbf{g}} \mapsto {}^{n-1}_p\tilde{\mathbf{g}}$ through the natural map of §III.C. Here is the combinatorial check for $\mathcal{H}_{O_n}$ giving a projective system of (absolutely irreducible) Hurwitz space components over $\mathbb{R}$.

(C.12a) There is $Q_n \in H_r$ with $\kappa({}^n_p\tilde{\mathbf{g}}) = ({}^n_p\tilde{\mathbf{g}})Q_n$, $n = 0, 1, \dots$.

Here is the corresponding statement with $\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})^{\mathrm{ab}}$ replacing $\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})^{\mathrm{in}}$.

(C.12b) There is $Q_n \in H_r$, $\gamma_n \in N_{S_{k(n)}}({}^n_p\tilde{G})$, with $\kappa({}^n_p\tilde{\mathbf{g}}) = \gamma_n({}^n_p\tilde{\mathbf{g}})Q_n\gamma_n^{-1}$, $n = 0, 1, \dots$.

PROBLEM C.4. *Suppose* $(G, p, \mathbf{C})$ *has* G *satisfying the center hypothesis, and* $\mathbf{C}$ *is a set of* p' *conjugacy classes. Give a procedure for checking existence of* ${}^n_p\tilde{\mathbf{g}}$, $n = 0, 1, \dots$ *satisfying* (C.12a) *(or* (C.12b)*).*

COMMENTS C.5. *Relating* Th. C.3 *to the Ihara-Matsumoto section.* With the center hypothesis in force, apply Th. C.3 to the modular tower $\mathcal{H}_n = \mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$, $n = 0, 1, \dots$ (inner or absolute version). Consider the total family $\mathcal{T}_n \to \mathcal{H}_n \times \mathbb{P}^1$ (as in (3.22)) attached to the moduli space $\mathcal{H}_n$. The (ramified) cover $\mathbb{P}^r \times \mathbb{P}^1$ restricts over the open set $\mathbb{P}^{r+1} \setminus D_{r+1}$ to give the (unramified) cover $U_{r+1} \to \mathbb{P}^{r+1} \setminus D_{r+1}$. Restrict $\mathcal{T}_n$ over U_{r+1} to give unramified covers

(C.13) $$\mathcal{T}_n^0 \xrightarrow{\Phi_n} (\mathcal{H}_n \times \mathbb{P}^1)^0 \to U_{r+1}.$$

Here $(\mathcal{H}_n \times \mathbb{P}^1)^0$ is a natural affine subvariety of $\mathcal{H}_n \times \mathbb{P}^1$ from removing the loci $(\boldsymbol{p}, \boldsymbol{x})$ where $\boldsymbol{x}$ is the branch point set of a cover representing $\boldsymbol{p} \in \mathcal{H}_n$.

Take $\boldsymbol{x}_0$, the image of $\boldsymbol{x}' \in (\mathbb{P}^1(\mathbb{R}))^{r+1} \setminus \Delta_{r+1}$ as in (C.2) with $s = 0$ and $r+1$ replacing r. Restrict covers over the locus $(\boldsymbol{x}_0, x)$ (x runs over $\mathbb{P}^1 \setminus \{x_2', \dots, x_{r+1}'\}$). Then, (C.5a) gives words in $Q_1, \dots, Q_r$ expressing convenient paths (based at x_1') for generators of $\pi_1^* = \pi_1(\mathbb{P}^1 \setminus \{x_2', \dots, x_{r+1}'\})$. Let β be the homomorphism $\pi_1^* \to S_n$ sending the r-tuple of (C.5a) to the coordinates of $\mathbf{g} \in \mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$. This extends $\pi_1(\mathbb{P}^r \setminus D_r)$ acting on $\mathrm{Ni}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$. Thus, β maps r-tuple (C.5b) to $\kappa(\mathbf{g})$. This expresses the compatibility of the choice of paths in [**DFr2**, Fig. 2] to those of (C.5a).

These topological considerations defining κ don't depend on $\boldsymbol{x}'$ if we stay in the simply connected set given by (C.2) (with $s = 0$ and $r+1$ replacing r). Consider, however, a *general* $\sigma \in G_{\mathbb{Q}}$. The fixed field $\bar{\mathbb{Q}}^{(\sigma)}$ of σ supports no ordering that allows an analog of a simply connected set like (C.2). (Here's one way to see that. For a measure one subset of $G_{\mathbb{Q}}$, $\bar{\mathbb{Q}}^{(\sigma)}$ is a PAC field [**FrJ**, Th. 16.47]. Then, the Frey-Prestel Theorem shows any Henselian closure of a characteristic 0 PAC field is algebraically closed [**FrJ**, Th. 10.14].) So, it behooves us to find a way to preserve the result for complex conjugation that gives a valuable extension to all $\sigma \in G_{\mathbb{Q}}$. A limit $\boldsymbol{x}' \to (x_1', \dots, x_1')$ in the set (C.2) preserves the construction above. Here $(x_1', \dots, x_1')$ lies in the deepest part of the fat diagonal. We can extend local algebraic functions on an étale cover to a neighborhood of a chosen lift of the simply connected space of (C.2). Thus, we may consider their Puiseux expansions around this point. These expansions will have fractional exponents in local parameters for the point $(x_1', \dots, x_1')$, so there will be several choices for the expansion. [**I**] uses data for a direction from $x_i' \mapsto x_j'$ to normalize these functions to be positive in their values along this direction.

The point $(x_1', \dots, x_1')$ alone, doesn't support this extra information. Thus [**IM**] extends the Puiseux expansions to a point $\boldsymbol{x}''$ on a partial blow-up of the point $(x_1', \dots, x_1')$. An encoding of the direction from the i-th coordinate to the $i{+}1$-th coordinate, $i = 1, \dots, r{+}1$, appears algebraically in the ring structure of this point. This data supports a proof of the Ihara-Drinfield relations.

For a general $\sigma \in G_{\mathbb{Q}}$, the Drinfeld-Ihara action on $\mathbb{P}^{r+1} \setminus D_{r+1}$ maps the r-tuple $(Q_1, \dots, Q_r)$ to

$$A_\sigma(Q_1, \dots, Q_r) \stackrel{\text{def}}{=} (f_{1,\sigma} Q_1^{\psi(\sigma)} f_{1,\sigma}^{-1}, \dots, f_{r,\sigma} Q_r^{\psi(\sigma)} f_{r,\sigma}^{-1}).$$

Here, ψ is the cyclotomic character (as before Th. 3.16). Further, suppose we fix $\lambda = \psi(\sigma)$. Then, A_σ depends only on a single profinite word f. That is $f_{i,\sigma} = f(x_i, y_i)$, $i = 1, \dots, r$. Here, (x_i, y_i) are elements of H_r, independent of σ and $f = f_\sigma$ lies in the commutator subgroup of the free group $\hat{F}_2$ on two generators. [**IM**, Appendix] lists explicit properties of f_σ. The conjecture is this list exactly characterizes the words f that arise as an f_σ, $\sigma \in G_{\mathbb{Q}}$.

Thus, fixing λ, test Ihara-Drinfeld by running through all such allowable fs giving transformations A_f (notationally replacing A_σ). To detect fields of definition of components of the spaces $\mathcal{H}_n$, apply A_f to the elements of (C.5a). Reexpress the result as an r-tuple of words in the r-tuple of (C.5a). This produces an analog κ_f of the κ operator of expression (C.5b) and (C.9). Finally, for all levels of the modular tower $\mathcal{H}_n$, $n = 0, 1, \dots$, apply κ_f to check (C.8b). For example, checking this action against Galois Invariance Th. 3.16 gives information on the $\widehat{\mathcal{G}T}$ conjectures. Is this really possible to carry out? Part IV looks at examples. $\square$

PROBLEM C.6. *Use the computations of* [**DFr**] *and* [**DFr2**] *to give an analog* *to* Th. C.3 *for any real point* $\boldsymbol{x}_0 \in \mathbb{P}^r \setminus D_r$. *That is, instead of* (C.3), *let* $\boldsymbol{x}_0$ *be the image of* $\boldsymbol{x}' \in (\mathbb{P}^1)^r$ *with some coordinates real and others in complex conjugate pairs as in* (C.2).

§**App.D** $\mathbb{R}$ **points on modular towers.** For perspective, reconsider Problem D_2 of §I.B. This is the most important diophantine problem applicable to modular towers at this stage. Assume $G \le \hat{G} \le S_n$ are transitive subgroups with G normal in $\hat{G}$ and G has no center. As in (3.9), suppose $\mathbf{C}$, a rational union of conjugacy classes of G, has its entries from the distinct conjugacy classes $\mathrm{C}'_1, \dots, \mathrm{C}'_t$. Analogous to Problem B of §I.D, here are necessary conditions for a $(G, \hat{G}, \mathbf{C})$-realization over $\mathbb{Q}$.

(D.1a) No element of $\hat{G} \setminus G$ centralizes G [**Fr5**, Prop. 2].
(D.1b) $\hat{G} \le N_{S_n}(\mathbf{C})$ (as in Def. 3.1a).

Problem D.1. *Assume* (D.1) *and* $N > 0$. *Is there* $\mathbf{C}$ *with* C'_i *appearing at least* N *times in* $\mathbf{C}$, $i = 1, \dots, t$, *where* $\mathcal{H}^{\mathrm{in}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ *(resp.,* $\mathcal{H}^{\mathrm{ab}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$*) has* $\mathbb{Q}$ *points? Continue these assumptions. Are there* $\mathbb{Q}$ *points of* $\mathcal{H}^{\mathrm{ab}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ *where* $\hat{G}/G$ *is the decomposition group in the natural cover*

$$\mathcal{H}^{\mathrm{in}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}}) \to \mathcal{H}^{\mathrm{ab}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})?$$

A positive answer to Problem D.1 gives $(G, \hat{G}, \mathbf{C})$-realizations under the hypotheses above (application of Theorem 3.4 following [**FrV**]). (In particular, a $\mathbb{Q}$ point on $\mathcal{H}^{\mathrm{in}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ gives a regular realization of G over $\mathbb{Q}$.) For example, the $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization Lemma of §I.D produces $\mathbb{Q}$ points on $\mathcal{H}(D_p, \mathbf{C}_{p+1})^{\mathrm{ab}}$ for each odd prime p. It shouldn't be hard to improve this to give $(D_{p^n}, \mathbb{A}_{p^n}, \mathbf{C}_{p^n+1})$-realizations. Since D_p is a quotient of D_{p^n}, taking n large automatically produces $(D_p, \mathbb{A}_p, \mathbf{C}_r)$-realizations with r arbitrarily large. This is for the case of fixed D_p, and involutions as conjugacy classes. No one has yet found $\mathbb{Q}$ points on $\mathcal{H}(D_p, \mathbf{C}_r)^{\mathrm{in}}$ (Problem A of §I.D) for each prime p (r depends on p). This is the analog for hyperelliptic curves (of genus $(r-2)/2$) for $\mathbb{Q}$ non-cusp points on $X_1(p)$. §App.E continues these problems over $\mathbb{Q}$ as they apply to modular towers.

Turn now to existence of (a projective system of) real points on a modular tower. Assume G satisfies the Center Hypothesis. Restrict, as in §App.C, to points over $\boldsymbol{x}_0 \in \mathbb{P}^r \setminus D_r$ with $\boldsymbol{x}_0$ the image of an r-tuple with all coordinates real. Apply (C.10b) and (C.10c) to rephrase existence of real points on modular towers. For the absolute version, assume we have transitive representations ${}^n_p\tilde{G} \le S_{k(n)}$. The following joins modular towers with [**DFr**, Th. 1.1]. The involutions $\boldsymbol{\beta}$ in the next lemma arise from (C.11b) by taking $\beta_0 = \gamma$ and $\beta_i = \gamma\alpha_i$, $i = 1, \dots, r-1$.

Real Projective System Lemma D.2. *There exists a projective system* $\{\boldsymbol{p}_n \in \mathcal{H}_n({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})^{\mathrm{in}}(\mathbb{R})\}_{n=0,1,\dots}$ *(over* $\boldsymbol{x}_0$*) if and only if there exists a projective* *system* ${}^n_p\mathbf{g} \in \mathrm{Ni}({}^n_p\tilde G, {}^n_p\tilde{\mathbf{C}})$ *with*

(D.2a) $\kappa({}^n_p\mathbf{g}) = \gamma_n {}^n_p\mathbf{g}\gamma_n^{-1}$ for some involution $\gamma_n \in {}^n_p\tilde G,\ n = 0, 1, \dots .$

This is equivalent to a projective system of r-tuples of involutions

(D.2b) $\boldsymbol{\beta}_n \in ({}^n_p\tilde G)^r$ with $\boldsymbol{\beta}_n$ generating ${}^n_p\tilde G,\ n = 0, 1, \dots .$

Similarly, there exists a projective system $\{\boldsymbol{p}_n \in \mathcal{H}_n({}^n_p\tilde G, {}^n_p\tilde{\mathbf{C}})^{\mathrm{ab}}(\mathbb{R})\}_{n=0,1,\dots}$ *if and only if there exists a projective system* ${}^n_p\mathbf{g} \in \mathrm{Ni}({}^n_p\tilde G, {}^n_p\tilde{\mathbf{C}})^{\mathrm{ab}}$ *with*

(D.2c) $\kappa({}^n_p\mathbf{g}) = \gamma_n {}^n_p\mathbf{g}\gamma_n^{-1}$ for some involution $\gamma_n \in N_{S_{k(n)}}({}^n_p\tilde G),\ n = 0, 1, \dots .$

This is equivalent to a projective system of $r-1$-tuples $\boldsymbol{\alpha}_n \in ({}^n_p\tilde G)^{r-1}$ and an automorphism h_n of ${}^n_p\tilde G$ with these properties.

(D.2d)
$$\boldsymbol{\alpha}_n = (\alpha_{1,n}, \dots, \alpha_{r-1,n}) \text{ generates } {}^n_p\tilde G, \text{ and}$$
$$h(\alpha_i) = \alpha_i^{-1},\ i = 1, \dots, r-1,\ n = 0, 1, \dots .$$

Suppose p is odd and $\boldsymbol{\beta}_0 \in (G)^{r-1}$ exists satisfying (D.2b) *(involutions exist at level 0). Then, there is a complete projective system satisfying* (D.2b)*. If, however, $p = 2$, then no such system as in* (D.2b) *exists.*

The Center Hypothesis assures a γ_n in (D.2b) is an involution. Otherwise its square would centralize ${}^n_p\tilde G$ contrary to statement (3.4d) of Th. 3.4. The version of this in [**DFr**, Th. 1.1] considers the case the Center Hypothesis doesn't hold. There are two natural questions for considering Lemma D.2 further.

Lifting Problem D.3. *Assume G satisfies the Center Hypothesis.*

(D.3a) *Suppose a specific r-tuple $\boldsymbol{\beta}$ of involutions generate G. Characterize quotients H of ${}_2\tilde G$ that have r involutions that map respectively to $\boldsymbol{\beta}$.*

Similarly, suppose $(G^* : G) = 2$ and there are involutions $\boldsymbol{\beta}^*$ from $G^* \setminus G$ generating G^*. Characterize quotients H of $\tilde G$ with the following property.

(D.3b) *H is an index 2 normal subgroup of a group H^* covering G^* where H^* has generating involutions $\boldsymbol{\beta}^*_H$ that lift $\boldsymbol{\beta}^*$.*

For (D.3a), $\boldsymbol{\beta}$ can't lift all the way to ${}_2\tilde G$. For this, [**DFr**, Lemma 1.3] uses that $\tilde G$ is projective (§II.A). It thus contains no involutions (or any element of finite order). We don't know when there is a *maximal* quotient H of ${}_2\tilde G$ fulfilling the conclusion of (D.3a). Involutions generate S_n for any integer n. So, answering (D.3a) for S_n and some set of generating 2-cycles is a valuable test.

Now consider (D.3b). Here we don't even know when $H = \tilde G$ provides a positive answer to this question. The hypothesis that G has no center excludes the case G is a p-group. In that case, however, its universal Frattini cover is a free pro-p-group. Thus, we can lift $\boldsymbol{\alpha}$ and γ in (C.11.b) to $\tilde{\boldsymbol{\alpha}} \in (\tilde G)^{r-1}$ and $\tilde\gamma$, an automorphism of $\tilde{G}$, for which $\tilde{\gamma}\tilde{\alpha}_i\tilde{\gamma}^{-1} = \tilde{\alpha}_i^{-1}$, $i = 1, \dots, r-1$. The key to (D.3b) is the universal *real* Frattini cover $R(\tilde{H}^*)\xrightarrow{\psi}H^*$ of H^* (relative to $\boldsymbol{\beta}_H$). We explain this briefly as it will be the subject of [**Fr9**].

DEFINITION D.4. *Real Frattini covers.* Let $(\mathrm{C}_1, \dots, \mathrm{C}_r) = \mathbf{C}$ be r conjugacy classes of involutions of G. Denote the intersection of all maximal subgroups of G meeting each conjugacy class of $\mathbf{C}$ by $\mathrm{RF}(G) = \mathrm{RF}(G, \mathbf{C})$. This is the *real Frattini* subgroup of G with respect to $\mathbf{C}$. Suppose $\phi : K \to G$ is a cover of groups with r conjugacy classes of involutions $(\mathrm{C}_1^K, \dots, \mathrm{C}_r^K)$ mapping respectively to $(\mathrm{C}_1, \dots, \mathrm{C}_r)$. Then, ϕ is a real Frattini cover if its kernel is in $\mathrm{RF}(K, \mathbf{C}^K)$.

[**HJ**] discusses *real projective* groups. Using these, the analog of the §II.A discussion for the universal Frattini cover gives this result. There is a *universal real Frattini* cover $R(\tilde{G})$ of G: It is universal for all such real Frattini covers (relative to $\mathbf{C}$). [**H**] motivates calling this the universal *Artin-Schreier* cover of G (relative to $\mathbf{C}$). Unlike the Frattini cover case, the kernel ker of the natural cover $R(\tilde{G})\xrightarrow{\psi}G$ may not be nilpotent. Arguments, however, similar to those in [**H**] show the following.

(D.4a) ker has a unique profinite 2-Sylow, P_2, normal in $R(\tilde{G})$.
(D.4b) $\ker/P_2$ is a nilpotent subgroup of $R(\tilde{G})/P_2$.
(D.4c) If G_1 is a subgroup of G that meets none of the conjugacy classes of $\mathbf{C}$, then $\psi^{-1}(G_1)$ is a projective subgroup of $R(\tilde{G})$.

Apply this to the hypotheses from (D.3b). Conclude the pullback of $G \le G^*$ in $R(\tilde{G}^*)$ is a projective group. Call this $\tilde{G}^\diamond$. By assumption there are generators $\tilde{\boldsymbol{\alpha}}^\diamond$ of $\tilde{G}^\diamond$ and an involution $\tilde{\gamma}^\diamond$ of $R(\tilde{G}^*)$ satisfying (C.11b). As $\tilde{G}^\diamond \to G$ is a cover by a projective group, this factors through the universal Frattini cover $\tilde{G} \to G$. Inspecting the action of $\tilde{\gamma}^\diamond$ on the kernel of the surjective induced map $\tilde{G}^\diamond \to \tilde{G}$ gives an effective approach to (D.3b). This motivates considering universal group covers beyond the universal Frattini cover. Finally, the next example shows the universal real Frattini cover of a finite group may not be a Frattini cover.

EXAMPLE D.5. *The universal real Frattini cover of* $G = \mathbb{Z}/3 \times \mathbb{Z}/2$. There is one class of involutions, consisting of $(0,1) = \tau$. The universal Frattini cover $\tilde{G}$ of G is $\mathbb{Z}_3 \times \mathbb{Z}_2$. The universal real Frattini cover $R(\tilde{G})$ of G (relative to $\{\tau\}$) has generators an involution and an element of infinite order generating a group isomorphic to $\mathbb{Z}_3$. Call these τ^* and α^*, lying above τ and $(1,0) = \alpha$, respectively. As previously, denote the kernel of $R(\tilde{G})\xrightarrow{\psi}G$ by ker. Let $\mathcal{D}$ be the group freely generated by an involution τ' and an element α' of infinite order. Form the profinite completion $\tilde{\mathcal{D}}$ of $\mathcal{D}$ using all subgroups of finite index. Inside this group, α' generates a subgroup isomorphic to $\hat{\mathbb{Z}} = \mathbb{Z}_3 \times \prod_{p\ne 3} \mathbb{Z}_p$.

Then, the universal real Frattini cover of G is isomorphic to the closed subgroup of $\tilde{\mathcal{D}}$ generated by the image of α' in $\mathbb{Z}_3$ and τ'. This is clearly a nonabelian group. So, it isn't a quotient of the universal Frattini cover of G. R. Guralnick gives the following explicit example quotient K of $R(\tilde{G})$. It has exactly one conjugacy class of involutions mapping to the involution of G.

Let S be the group freely generated by x_i, $1 \le i \le 3$, subject to these relations: $x_i^2 = 1$, $[x_i,[x_j,x_k]] = 1$. That is, the commutator subgroup is central. Therefore, $C = [S,S] = Z(S)$ is an elementary abelian of order 8 with basis $y_{i\,j} = [x_i,x_j]$, $1 \le i < j \le 3$. The map z of S which permutes the x_1, x_2, x_3 cyclically preserves all relations. So, it defines an automorphism of S. Write C as $C_1 \times C_2$ with these properties.

(D.5a) C_1 is a 4-group and C_2 has order 2.
(D.5b) $\langle S, z\rangle$ centralizes C_2 and z acts nontrivially on C_1.

Denote S/C_1 by M and let K be $M \times^s \langle z\rangle$. Thus K maps to G by sending z to α and x_1 to τ. Automatically, x_i maps to τ for each i. Note: M has commutator subgroup N of order 2. Let w generate this. We list elements that map to τ: x_i, x_iw, $x_1x_2x_3$ and $x_1x_2x_3w$. The last two have order 4 (their square is w), so there are 6 involutions mapping to τ. The x_i s are all conjugate as are the x_iw s. On the other hand, $x_jx_ix_j = x_iw$ for $i \ne j$, so all six involutions are conjugate. There is a unique class of involutions mapping to τ. $\square$

Here is a harder example. Let $G = A_n$ and $G^* = S_n$. Take $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_{n-2})$ equal to $((1\,2\,3),(1\,2\,4),\dots,(1\,2\,n))$. Then, $\boldsymbol{\alpha}$ generates A_n and $\gamma = (1\,2) \in G^*$ conjugates the α_i s to their inverses. That is, (C.11b) holds.

PROBLEM D.6. *For $n \ge 5$, let $\tilde A_n$ be the universal Frattini cover of A_n. Is there a lift of $\boldsymbol{\alpha}$ to $\tilde{\boldsymbol{\alpha}} \in (\tilde A_n)^{n-2}$ and an automorphism h of $\tilde A_n$ with $h(\tilde\alpha_i) = \tilde\alpha_i^{-1}$, $i = 1,\dots,n-2$?*

We don't know the answer to Prob. D.5 even when $n = 5$. Nor, to compare with Prop. 2.9, do we know the universal real Frattini cover of S_5.

§**App.E. Groups as regular extensions over finite fields.** This brief subsection reminds of the most significant diophantine problems. This includes how Thm. 3.21 applies to explicitly bound exceptional primes for the regular realization of a given group over $\mathbb{F}_p(x)$. The essential hypothesis uses a gcomplete collection of rational conjugacy classes from G (§III.E).

Ex. 3.13 produces modular towers obstructed at the first level. Counter to this, Cor. 3.23 gives hypothesis (3.17), on p' conjugacy classes $\mathbf{C}$, which assures some H_r orbit of $\mathrm{Ni}(G,\mathbf{C})$ is unobstructed at every level. The center hypothesis is irrelevant for this question. In particular, if G is p-gcomplete, there are many choices of $\mathbf{C}$ for which $\mathrm{Ni}({}_p^n\tilde G, {}_p^n\tilde{\mathbf{C}})$ is nonempty at every level n. Characterizing those $(G,\mathbf{C})$ unobstructed at every level is a significant problem requiring careful formulation.

PROBLEM E.1. *Suppose G satisfies the center hypothesis, $p \mid |G|$, and $\mathbf{C}$ are p' conjugacy classes of G. Assume $\mathrm{Ni}(G,\mathbf{C})$ is unobstructed at every level. Also,*

$\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ has a $\mathbb{Q}$ absolutely irreducible component at every level. Does there exist an integer n for which $\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ has no $\mathbb{Q}$ points?

PROBLEM E.2. *Suppose given G (a transitive subgroup of S_k), p, n. Let $\mathbf{C}'$ be a fixed union of p' conjugacy classes. These are the only conjugacy classes we allow to appear in $\mathbf{C}$. Assume each element of $\mathbf{C}'$ appears at least a times in $\mathbf{C}$. Is there an a (dependent on G, n and $\mathbf{C}'$) for which $\mathcal{H}^{\mathrm{ab}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$ is $\mathbb{C}$-unirational? There is a similar question for $\mathcal{H}^{\mathrm{in}}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})$.*

The remainder of this subsection applies Th. 3.21 to bound exceptional primes for groups as Galois groups of regular extensions of $\mathbb{F}_p(x)$. The proof is an outline because we apply [**Fu**] for a statement of good reduction of Hurwitz spaces modulo primes not dividing $|G|$. In fact, Fulton didn't have the Nielsen class concept and proved this only for simple branching. A later paper will show this hypothesis in the following form.

REDUCTION HYPOTHESIS E.3. *Assume G has no center and p is a prime not dividing $|G|$. Let $G \le S_n$ be an embedding satisfying* (3.5a) *or* (3.5b)*. Let $\mathbf{C}$ be a rational union of conjugacy classes of G. Then, the natural map $\Psi : \mathcal{H}(G,\mathbf{C})^{\mathrm{in}} \to \mathcal{H}(G,\mathbf{C})^{\mathrm{ab}}$ (before Lemma 3.3) reduces modulo p to produce a cover of smooth affine varieties over $\mathbb{F}_p$. Denote this $\Psi_p : \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}_p \to \mathcal{H}(G,\mathbf{C})^{\mathrm{ab}}_p$. Each G realization over $\mathbb{F}_p$ corresponds to a point of $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}_p(\mathbb{F}_p)$. Further, absolutely irreducible components of $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ (resp., $\mathcal{H}(G,\mathbf{C})^{\mathrm{ab}}$) correspond one-one to absolutely absolutely irreducible components of $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}_p$ (resp., $\mathcal{H}(G,\mathbf{C})^{\mathrm{ab}}_p$).*

PROPOSITION E.4. *Suppose G has no center and $\mathbf{C}$ satisfies the hypotheses of* (3.17)*. Especially,* $\mathrm{Ni}(G,\mathbf{C})$ *is an HM-Nielsen class for which $\mathbf{C}$ is HM-gcomplete and a rational union of conjugacy classes. Then, there is a constant $A = A(\mathrm{Ni}(G,\mathbf{C}))$ for which the following holds. For any p exceeding A, $G = G(\hat{L}/\mathbb{F}_p(x))$ with $\hat{L}$ a regular extension of $\mathbb{F}_p(x)$.*

More generally, for any finite group G, we may explicitly compute a finite covering group G' with no center for which there is an r' and $\mathbf{C}'$ satisfying (3.17)*. Regular realization of G' over $\mathbb{F}_p(x)$ automatically produces regular realization of G over $\mathbb{F}_p(x)$. Thus, the above holds for p exceeding $A(\mathrm{Ni}(G',\mathbf{C}'))$.*

PROOF. Apply Hypoth. E.3 in the case G is in S_n as its regular representation. For $p \not| \, |G|$, we have only to find a $\mathbb{F}_p$ rational point on $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}_p$. From Cor. 3.21, this variety has an $\mathbb{F}_p$ absolutely irreducible component $\mathcal{H}(G,\mathbf{C})'_p$.

The cover $\mathcal{H}(G,\mathbf{C})'_p \to \mathbb{P}^r \setminus D_r$ is a finite morphism of affine varieties. Restrict over the affine subset $\mathbb{A}^r \setminus D_r$ from the embedding $\mathbb{A}^r \to \mathbb{P}^r$. Thus, $\mathcal{H}(G,\mathbf{C})'_p$ is birational to the zero set of a hypersurface V_p defined by $f(\boldsymbol{x},y)_p = 0$. Further, the degree of f_p in y equals the degree of the cover $\mathcal{H}(G,\mathbf{C})'_p \to \mathbb{P}^r \setminus D_r$. Bound d by the cardinality of $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$. Any non-singular $\mathbb{F}_p$ point of V_p corresponds to a $\mathbb{F}_p$ point of $\mathcal{H}(G,\mathbf{C})'_p$. Apply the Lang-Weil estimates to determine an A'

where V_p has a nonsingular $\mathbb{F}_p$ point when p exceeds A'. [**FrHJ**, Prop. 3.3] gives the best estimates we know. This is a function of d, and r.

Apply this to a general group G as follows. The procedure of §III.B (before Center Hypothesis 3.5) explicitly covers G' by a group without a center. Comments before Th. 3.21 (as in the constructions of [**FrV**, §3]) bound the number r' of conjugacy classes you need to produce an HM-Nielsen class. $\square$

Apply Reduction Hypothesis E.3 to a modular tower. In particular, consider the tower attached to $(G, p, \mathbf{C})$ satisfying the hypotheses of Corollary 3.23. This produces a corresponding modular tower $\{\mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}})_r,\ n = 0, 1, \dots\}$ in characteristic r. Here r is *any* prime not dividing the order of G. That is, this tower has all properties we expect of a modular tower in characteristic 0. From Cor. 3.23, this will also have a projective sequence of absolutely irreducible components over $\mathbb{F}_r$. This is suitable for versions of Problem B.3 that deal directly with all points on Hurwitz space components over finite fields.

References

[A] J. L. Alperin, *Local representation theory*, Cambridge studies in advanced mathematics, vol. 11, Cambridge Univ. Press, 1986.

[AJL] H. Andersen, J. Jorgensen and P. Landrock, *The projective indecomposable modules of* $\mathrm{SL}_2(p^n)$, Proc. London Math. Soc. **46** (1983), 38–52.

[Be] 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.

[Be2] D. J. Benson, *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras*, Cambridge studies in Advanced Mathematics, vol. 30, Camb. Univ. Press, 1991.

[BFr] M. Fried and R. Biggers, *Moduli Spaces of Covers of $\mathbb{P}^1$ and Representations of the Hurwitz Monodromy Group*, J. für die reine und angew. Math. **335** (1982), 87–121.

[DFr] P. Debes and M. Fried, *Nonrigid constructions in the Inverse Galois Problem*, PJM **163 #1** (1994), 81–122.

[DFr2] P. Debes and M. Fried, *Rigidity and real residue class fields*, Acta Arith **56** (1990), 13–45.

[De] B. Deschamps, *Points $\mathbb{Q}_p$-rationnels sur un espace de Hurwitz*, Proceedings of the Recent developments in the Inverse Galois Problem conference, AMS Cont. Math series, 1994.

[EKV] H. Esnault, B. Kahn, E. Vieweg, *Coverings with odd ramification and Stiefel-Whitney classes*, J. Crelle **441** (1993), 145–188.

[Fa1] G. Faltings, *Diophantine approximation on abelian varieties*, Annals of Math. **133** (1991), 549–576.

[Fa2] G. Faltings, *The general case of S. Lang's conjecture*, preprint (1992).

[F] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. **85** (1994), 79–83.

[Fr1] M. Fried, *Global construction of general exceptional Covers: with motivation for applications to encoding*, Applications and Algorithms, Cont. Math., G.L. Mullen and P.J. Shiue, editors, vol. 168, 1994, pp. 69–100.

[Fr2] M. Fried, *On a theorem of MacCluer*, Acta Arith. **25** (1974), 122–127.

[Fr3] M. Fried, *Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem*, A.M.S. Publications, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups,, vol. 37, 1980, pp. 571–601.

[Fr4] M. Fried, *Galois groups and Complex Multiplication*, TAMS **235** (1978), 141–162.

[Fr5] M. Fried, *Fields of Definition of Function Fields and Hurwitz Families and; Groups as Galois Groups*, Communications in Algebra **5** (1977), 17–82.

[Fr6] M. Fried, *Review: Serre's* Topics in Galois Theory, BAMS **30 #1** (1994), 124–135.

[Fr6a] M. Fried, *Enhanced review: Serre's* Topics in Galois Theory, Proceedings of the Recent developments in the Inverse Galois Problem conference, AMS Cont. Math series, 1995.

[Fr7] M. Fried, *Arithmetic of 3 and 4 branch point covers: a bridge provided by noncongruence subgroups of* $\mathrm{SL}_2(\mathbb{Z})$, Progress in Mathematics, vol. 81, Birkhauser, 1990, pp. 77–117.

[Fr8] M. Fried, *Alternating groups and lifting invariants*, Preprint, 32 pgs, (1989).

[Fr9] M. Fried, *Real points on moduli spaces and Artin-Schreier covers of a finite group*, In preparation.

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

[FrJH] M. Fried, D. Haran and M. Jarden, *Counting points on definable sets over finite fields*, Israel J. Math. **85** (1994), 103–133.

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

[FrV2] M. Fried and H. Völklein, *The embedding problem over an Hilbertian-PAC field*, Annals of Math **135** (1992), 469–481.

[Fu] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Math. **90** (1969), 542-575.

[GR] H. Grauert and R. Remmert, *Komplexe Räume*, Math. Ann. **136** (1958), 245–318.

[H] D. Haran, *Closed subgroups of* $G(\mathbb{Q})$ *with involutions*, J. Alg. **129** (1990), 393–411.

[HJ] D. Haran and M. Jarden, *The absolute Galois group of a pseudo real closed field*, Ann. Scuola Norm. Sup. Pisa Cl. Sci. **(4) 12** (1988), 147–206.

[Ha] D. Harbater, *Galois coverings of arithmetic line*, Proc. of New York Num. Thy. Conf., LNM, vol. 1240, Springer, 1985.

[I] Y. Ihara, *Braids, Galois groups, and some arithmetic functions*, Proceedings of the International Congress of Mathematicians, Kyoto 1990, Springer-Verlag, Hong Kong, 1991, pp. 99-120.

[I2] Y. Ihara, *On modular curves over finite fields*, Proc. Inter. Colloq. on subgroups of Lie groups and applications to moduli, Ox. Univ. Press, Bombay, 1973, pp. 161–202.

[I3] Y. Ihara, *Profinite braid groups, Galois representations and complex multiplications*, Ann. Math. **123** (1986), 43–106.

[IM] Y. Ihara and M. Matsumoto, *Galois actions on profinite completions of braid groups*, Proceedings of the Recent developments in the Inverse Galois Problem conference, AMS Cont. Math series, 1995.

[J] C. Jordan, *Recherches sur les substitutions*, J. Liouville **17** (1872), 351–367.

[FKS] B. Fein, W. Kantor and M. Schacher, *Relative Brauer groups. II*, J. Reine Ang. Math. **328** (1981), 39–57.

[Ma^2] G. Malle and B.H. Matzat, *Inverse Galois Theory*, Completed pre-book as of Fall 1995.

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

[Mu] D. Mumford, *Introduction to algebraic geometry*, Harvard Univ. Notes, Cambridge, Mass., 1966.

[Na] H. Nakamura, *Galois rigidity of pure sphere braid groups and profinite calculus*, J. Math. Sci. Univ. Tokyo **1** (1994), 71–136.

[N] D. G. Northcott, *An introduction to homological algebra*, Cambridge Univ. Press, Great Britain, 1962.

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

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

[Se1] J.-P. Serre, *L'invariant de Witt de la forme $T(x^2)$*, Math. Helvetici **59** (1984), 651–676.
[Se2] J.-P. Serre, *Letter on Ext*, Private Correspondence (1988).
[Se3] J.-P. Serre, *Relêvements dans $\tilde{A}_n$*, C. R. Acad. Sci. Paris **311** (1990), 477–482.
[Se4] J.-P. Serre, *Topics in Galois Theory*, ISBN 0-86720-210-6, Bartlett and Jones Publishers, 1992.
[Se5] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inv. Math. **15** (1972), 259–331.
[Se6] J.-P. Serre, *Revêtements a ramification impaire et thêta-caractéristiques*, C. R. Acad. Sci. Paris **311** (1990), 547–552.
[T] D. Toledo, *Projective varieties with non-residually finite fundamental groups*, Publ. Math. IHES **77** (1993), 103–119.

UC Irvine, Irvine, CA 92717, USA
E-mail address: mfried@math.uci.edu