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)
$$\begin{tikzcd} & {}_2\dot{S}'_c \arrow[r] & \dot{\mathbf{1}} \arrow[r] & {}_2\dot{S}''_c \arrow[dr] & \\ \dot{\mathbf{1}} \arrow[ur] \arrow[dr] & & & & \dot{\mathbf{1}} \\ & {}_2\dot{S}''_c \arrow[r] & \dot{\mathbf{1}} \arrow[r] & {}_2\dot{S}'_c \arrow[ur] & \end{tikzcd}$$

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:

$$ {}_2\dot{S}'_c \to \mathbf{1} \to {}_2\dot{S}''_c \to \mathbf{1} \to {}_2\dot{S}'_c. \tag{2.9a}$$

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

$$\dot{P}_{{}_2S'_c} \oplus \dot{P}_{{}_2S''_c} \to {}_2S'_c \oplus {}_2S''_c. \tag{2.9b}$$

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. □

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. □

§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 ${}_p^n\tilde{G}$. 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 ${}_p^n\tilde{G}$ 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 ${}_p^n\tilde{G}$ module through ϕ_n. Therefore, it has no proper ${}_p^n\tilde{G}$ module; such would be a proper G submodule. From the first part of the lemma, (2.2a) says ${}_p^n\tilde{G}$ 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 ${}_p^n\tilde{G}$ module homomorphism. So, the projective ${}_p^n\tilde{G}$ module ${}_p^nP_M$ has a map $\psi : {}_p^nP_M \to P_M$ commuting with the maps to M. This is surjective: the quotient of P_M by its radical (as either a G or ${}_p^n\tilde{G}$ module) is just M. $\square$

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

(2.10a) $1 \to \Omega^2(\mathbf{1}) \to P \to \Omega^1(\mathbf{1}) \to 1$, P the minimal projective ${}_p^n\tilde{G}$ 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 $\mathbf{1} = \mathbf{1}_{{}_p^n\tilde{G}}$. Compute boundary maps from the standard exact sequences of cohomology:

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

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

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

PROOF. Follow standard computations for boundary maps. For example, check that ψ defines a homomorphism by computing $\psi(g_1g_2)$ 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 ${}_p^{n+1}\tilde{G}$ is to show pullback of $\psi({}_p^n\tilde{G})$, as an extension of ${}_p^n\tilde{G}$, has the correct 2-cocycle. Suppose α represents a 1-cocycle. Then, $g \mapsto (\alpha(g), g)$ gives a splitting of ${}_p^n\tilde{G}$ in $\Omega^1(\mathbf{1})\times^s {}_p^n\tilde{G}$. For each $g \in {}_p^n\tilde{G}$ 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

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

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

§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, $\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}) \stackrel{\mathrm{def}}{=} P_{\mathbf{1}}$ 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*

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

(2.13d) *Any* B *in* (2.13c) *and* $(\mathbf{O},(1\,2\,3\,4\,5))$ *generate a subgroup* G' *isomorphic to* G *of* $\mathbb{M}(2,\mathbb{F}_4)_0 \times^s SL(2,\mathbb{F}_4)$. *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 semi-direct 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 $p \mid |K|$. So, the action of ${}_p\tilde{K}$ on H is induced from K acting on H. On the other hand, suppose $p \mid |H|$. 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, $p \mid |G|$, 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). □

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. □

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 $\{\mathcal{H}_n = \mathcal{H}({}^n_p\tilde{G}, {}^n_p\tilde{\mathbf{C}}), | \; n = 0, 1, \ldots\}$ 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 $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_r)$ 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*:

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

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 *course* 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, $i = 1, \dots, r-1$, with these relations:

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

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

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

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:

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

This action commutes with conjugation by any element of $N_{S_n}(\mathbf{C})$. Thus, it induce 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 $\Psi : \mathcal{H}_O^{\mathrm{in}} \to \mathcal{H}_O^{\mathrm{ab}}$ (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*

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

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 $\mathrm{Ni}(G, \mathbf{C}) = \mathrm{Ni}(G, \mathbf{C})$, 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, and restrict* Ψ *to* $\mathcal{H}_O^{\mathrm{in}}$. *Over* $\mathbb{C}$, Ψ *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* $D_{\boldsymbol{p}} = N^{\mathrm{out}}_{\mathrm{in}}(\mathbf{C})$ *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 $G \le S_n$.

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 $\mathcal{H}^{\mathrm{in}}_O \to \mathbb{P}^r \setminus D_r$ (resp., $\mathcal{H}^{\mathrm{ab}}_O \to \mathbb{P}^r \setminus D_r$) as a pure cover. The goal is a model for such a cover whose points represent solutions for a specific moduli problem. For $\mathcal{H}^{\mathrm{ab}}_O$ the problem is finding representative covers in the given orbit of H_r on the Nielsen class. Then, $\mathcal{H}^{\mathrm{in}}_O$ 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 transivity 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 $\Psi : \mathcal{H}^{\rm in}_O \to \mathcal{H}^{\rm ab}_O$ 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 $\boldsymbol{p} \in \mathcal{H}^{\rm in}_O(\bar{\mathbb{Q}})$ with $D_{\boldsymbol{p}}$ in (3.4d) equal $G(\mathcal{H}^{\rm in}_O/\mathcal{H}^{\rm ab}_O)$ 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 $\mathcal{H}(\mathbf{C})^{\rm in}(\mathbb{Q})$ is nonempty. Such rational points, however, require finding orbits O for which $\mathcal{H}^{\rm in}_O$ 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 *rigidying 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 ${}^n_p\tilde{G}$ 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. $\square$

§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

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

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 $o(\mathrm{C}_i)$; $\phi : {}_p^1\tilde{G} \to G$ is the natural map.

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

Proof. Choose any $g_i \in C_i$. Let H_i be $\phi^{-1}(\langle g_i \rangle)$ in ${}_p^1\tilde{G}$. 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 ${}_p^1\tilde{G}$ and ${}_p^1\tilde{\mathbf{C}}$. Assume we have constructed a Nielsen class from ${}_p^n\tilde{G}$ and ${}_p^n\tilde{\mathbf{C}}$. Continue by induction to define a Nielsen class $\mathrm{Ni}({}_p^{n+1}\tilde{G}, {}_p^{n+1}\tilde{\mathbf{C}})$ by putting $({}_p^n\tilde{G}, {}_p^n\tilde{\mathbf{C}})$ in place of $({}_p^1\tilde{G}, {}_p^1\tilde{\mathbf{C}})$. $\square$

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 ${}_p^n\tilde{G} \to G$ contains a copy of $G(1)$, unique up to conjugacy. The representation T_n of ${}_p^n\tilde{G}$ on the cosets of $G(1)$ extends the corresponding representation in ${}_p^k\tilde{G}$, $k \leq n$. 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 $\alpha \in {}_p^n\tilde{G}$ normalizes $G(1)$. Then, the image of α in ${}_p^{n-1}\tilde{G}$ normalizes $G(1)$ there. Thus, assume $G(1)$ is self-normalizing in ${}_p^{n-1}\tilde G$. Then, it is also in ${}_p^{n}\tilde G$, 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 $T_n : {}_p^n\tilde G \to S_{m_n}$ 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 ${}_5^{n-1}\tilde A_5$ is self-normalizing. Then, it is self-normalizing in ${}_5^{n}\tilde A_5$ 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 $({}_p^n\tilde G, T_n)$ 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 ${}_p^n\tilde G$, and $\mathbf{C}$ by ${}_p^n\tilde{\mathbf{C}}$ in Def. 3.1b. Call the corresponding normalizing group $N_n({}_p^n\tilde{\mathbf{C}}) = N_n$. The action of H_r on $\mathrm{Ni}({}_p^n\tilde G, {}_p^n\tilde{\mathbf{C}})/N_n$ produces the space

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

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

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

induced by reduction modulo $\ker_n / \ker_{n+1}$. An r-tuple $\tilde{\boldsymbol\sigma} \in \mathrm{Ni}({}_p^{n+1}\tilde G, {}_p^{n+1}\tilde{\mathbf{C}})$ modulo $\ker_n / \ker_{n+1}$ maps to $\boldsymbol\sigma \in \mathrm{Ni}({}_p^n\tilde G, {}_p^n\tilde{\mathbf{C}})$. Suppose $\tilde\alpha \in N_{n+1}({}_p^{n+1}\tilde{\mathbf{C}})$. From the meaning of extension representations, $\tilde\alpha$ induces an element of $N_n({}_p^n\tilde{\mathbf{C}})$. 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 $\mathrm{Ni}({}_p^{n+1}\tilde G, {}_p^{n+1}\tilde{\mathbf{C}})^{\mathrm{ab}}$ extends its action on $\mathrm{Ni}({}_p^n\tilde G, {}_p^n\tilde{\mathbf{C}})^{\mathrm{ab}}$. 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. $\square$

EXAMPLE 3.13. *Modular towers obstructed at level 1.* Take $G = A_n$ (alternating group), $p = 2$, and $C_1, \dots, C_{n-1} = C$, 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_is 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 $\mathbf{g}$:

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

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_1g_2. Suppose g_1 and g_2 are 3-cycles of A_5 which generate distinct subgroups. Assume g_1g_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

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

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. $\square$

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 $\nu_n(\mathcal{H}_O^\tau)^{{}^n_p\psi(\tau)} = \nu_n(\mathcal{H}_O)$ for each positive integer n. From this the theorem follows.

Use notation from Def. 3.11: for each lift $\tilde{\mathbf{g}} \in {}^n_p\tilde{\mathbf{C}}$ 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 ${}_p^n\tilde{\mathbf{C}}$. The last is in the conjugacy class of $m(\tilde{\mathbf{g}})^{-{}_p^n\psi(\tau)}$. 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 $\nu_n(\mathcal{H}_O)^{-{}_p^n\psi(\tau)}$. 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 ${}_p^n\psi(\tau)=s'$ where $s't'=1 \bmod p^n$. 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 $G = PSL_2(q)$, 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