The small Heisenberg group and ℓ-adic representations from Hurwitz spaces

Michael D. Fried and Mark van Hoeij

Abstract. The Hurwitz space approach to the regular Inverse Galois Problem was the only successful approach to Galois group realizations beyond nilpotent groups. It gave regular realizations of many series of groups. More significantly, the **M**(odular) **T**(ower) program identified *obstructions* to systematically finding regular realizations. Finding a way around those obstructions generalize renown results on modular curves.

We use the **MT** program to explicitly construct towers over a number field whose components are upper half plane quotients. Our main example was chosen close to topics that attracted those interested in Theta functions (the Schottky problem). This produces families of ℓ-adic representations. The surprising ingredient is the appearance of a Heisenberg group that controls the components that define the tower.

We model our results on properties Serre used in achieving his O(pen) I(mage) T(heorem) on ℓ-adic representations from projective systems of points on modular curves. There are two types of systems of ℓ-adic representations: *Frattini* and *Split*. Each type generalizes aspects of modular curve systems.

Contents

2000 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11R58; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.

http://www.math.uci.edu/~mfried has been revamped for adding/updating definitions/aids in understanding **MT**s. The end of §A has the paths to two definition helpfiles.

1. Outline of results with emphasis on spaces of upper half-plane quotients

The framework for considering ℓ-adic representations attached to specific (projective) sequences of (reduced) Hurwitz spaces is , for some purposes, in place. There are two types of applications: those resembling results on modular curve towers, and those in the service of the Inverse Galois Problem. Since Hurwitz spaces are families of sphere covers, there is a key parameter: the number of branch points, r, of the covers, giving the dimension of the spaces as $r-3$, with $r \geq 4$. To make that modular curve comparison we concentrate on $r = 4$ for our 1st two major examples, leaving for the 3rd a generalization where r must exceed 4 to produce the ℓ-adic representations.

When $r = 4$, all spaces are natural upper half plane quotients and j-line covers ramified (only) over $j = \infty$, $j = 0$ (with ramification index 1 or 3) and over $j = 1$ (with ramification index 1 or 2). The concept of an ℓ-Frattini cover is what produces canonical sequences of spaces and the ℓ-adic representation.

1.1. Data for the spaces of this paper. A **M**(odular) **T**(ower) of Hurwitz spaces (Def. 1.1) starts with a finite group G_0 and a prime ℓ dividing the order of G_0. In addition, we have a collection of r, ℓ' (elements of order prime to ℓ) conjugacy

classes in G_0. We denote those (unordered) conjugacy classes $\{C_1, \dots, C_r\}$ by $\mathbf{C}$, usually with some extra decoration. Attached to our tower types are extensions

$$\psi_{k+1,0} : G_{k+1} \to G_0, k \geq 0.$$

Denote the kernel of $\psi_{k+1,0}$ by $\mathrm{Ker}_{k+1,0}$. Here are properties of these extensions.

(1.1a) $\psi_{k+1,0}$ is an ℓ-Frattini cover.

(1.1b) $\mathrm{Ker}_{k+1,0}$ is a $\mathbb{Z}/\ell^{k+1}[G_0]$ module, and a free $\mathbb{Z}/\ell^{k+1}$ module.

Here is a list of our examples.

(1.2a) A Frattini Case: G_0 is A_5 and $\ell = 5$, with $\mathbf{C} \stackrel{\text{def}}{=} \mathbf{C}_{3^4}$, 4 repetitions of the 3-cycle conjugacy class.

(1.2b) A Split Case: The G_0s running over a series of groups

$$\{G_{\ell,0} = (\mathbb{Z}/\ell)^2 \times^s A_3 | \ell \neq 3 \text{ a prime}\}, \text{with } \mathbf{C} \stackrel{\text{def}}{=} \mathbf{C}_{3^4},$$

4 repetitions of the class of order 3 elements in $G_{\ell,0}$.

(1.2c) For each of the alternating groups A_n with $n \equiv 5 \mod 8$, two tower types attached to (n, ℓ), $G_{n,\ell,0} = (\mathbb{Z}/\ell)^{n-1} \times^s A_n$ and $\mathbf{C}_{(\frac{n+1}{2})^4}$, 4 repetitions of same order lifts of the class of $\frac{n+1}{2}$-cycles.

We direct the paper to those interested in ℓ-adic representations; and those interested in the Inverse Galois Problem. The problems with which those two groups identify will be different (see §1.4). Another paper has worked out the properties of the *base* Hurwitz spaces, denoted here $\bar{\mathcal{H}}(A_n, \mathbf{C}_{(\frac{n+1}{2})^4})^{\text{in,rd}}$.

§1.2 explains in detail what our results, and expectations. Each Hurwitz space component corresponds to a braid orbit on a Nielsen class. §1.5 reviews this, with new observations beyond those made in previous papers. §2.1 lists basics on these particular **MT**s, which we call *abelianized*. They are natural quotients – suitable for ℓ-adic representations of the general **MT**s.

1.2. More about the cases in (1.2)**.** §1.3 explains the finite group extensions that produce the system of spaces to which are attached ℓ-adic representations.

Each $(G, \mathbf{C})$ defines a *Nielsen class*: a collection, $\mathrm{Ni}(G, \mathbf{C})$ of r-tuples (in this paper, usually $r = 4$), characterized by properties listed in (1.4). Our examples in (1.1) keep the group theory modest. When $r = 4$, all the (reduced) Hurwitz spaces will be upper half-plane quotients and natural j-line covers. This allows side comparisons with modular curves. §2.1 explains computing the rank of $\mathrm{Ker}_{k+1,0}$ in the Frattini case, especially why it is 6 for (1.2a).

The main result, Prop. 3.13, produces a family over $\mathbb{Q}$ of 5-adic ($\ell = 5$) representations. The sequence of groups seeding the **MT** tower levels are Frattini 5-group extensions of A_5. None of these have ever been realized as Galois groups. Finding K rational points on the tower levels is equivalent to their regular realization over K; even their $\mathbb{Q}_p$-adic realization with 4 branch point covers would be new. The heart of the result is that the braid group acts transitively on the Nielsen classes defining each tower level.

It is our first test case for the possibility of an Open Image Theory beyond modular curve towers. The formulation of that uses the monodromy over the j-line of the tower levels. It is a perfect case for looking back at [**Se68**] and extending a number of its fundamental lemmas (as in §2.1.2).

The Split case (1.2b) and (1.2c) use the natural $n-1$ dimensional represent V_n of A_n. (Mod out by the 1-dimensional trivial representation in standard (degree n)

permutation representation for A_n.) Then, $(\mathbb{Z}/\ell^{k+1})^{n-1}$ is just $V_n \mod \ell^{k+1}$. The case (1.2b) where $n = 3$, differs from (1.2a) in involving all primes ℓ (for technical reasons, excluding $\ell = 3$ at the moment). Here, for each ℓ there is more than one braid orbit at each level.

That can be scary, but [**Fr06**, §A.2] formulated the modular curve case using the (small) Heisenberg group (§4.2.1). That "Heisenberg Analysis of modular curve Nielsen classes" was a limitation on what can serve as a modular curve. Here, though – by luck, maybe – it generates a positive result. We take advantage of two types Nielsen class 4-tuples $\boldsymbol{g} = (g_1, \dots, g_4)$.

(1.3a) *Harbater-Mumford* (see Def. 2.8): $g_1 = g_2^{-1}$.

(1.3b) *Double identity*: $g_i = g_j$, for some $i \neq j$.

Braid orbits containing elements of either type in (1.3), are distinctly different from those that don't. No orbit contains both types (Prop. 4.11). Several orbits in each case contain type (1.3b), and their corresponding Hurwitz space components are conjugate over a cyclotomic field (Prop. 4.19).

Finally, it makes sense to consider **MT**s of a type combining both type (1.2a) and (1.2b). For the alternating group part we use Frattini cases from (1.2c) ($n \equiv 5 \mod 8$) for which give examples with $r = 4$. There is only one difficulty in adding the $n-1$-dimensional module to it, for new split cases. In order to get nonempty Hurwitz spaces we must increase r beyond 4. §2.2 tells about these cases and why we chose that congruence.

1.3. Extensions produce MTs. Let $\psi : H \to G$, be a *cover* (surjective homomorphism) of (profinite) groups. When $(\mathrm{Ker}(\psi), |G|) = 1$, the Schur-Zassenhaus Theorem says it automatically splits; ψ maps some copy of G in H one-one. Further, that splitting is unique up to conjugacy within H.

Exactly the opposite is a *Frattini* cover: No proper subgroup of H maps surjectively by ψ to G. For many problems, consideration of extensions divides into considering a Frattini cover followed by a split cover.

We will show how to figure properties of the two types of ℓ adic representation families that arise from the Frattini and split cases of (1.11.2). In general, we need a sequence of groups $\mathcal{G} \stackrel{\text{def}}{=} \{G_k\}_{k=0}^{\infty}$ with each $G_k \to G_{k-1}$ an ℓ-Frattini cover, $k \geq 1$, and some conjugacy classes $\mathbf{C} = \{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ for which ℓ divides no element in these classes. In this paper, $\mathrm{Ker}(G_k \to G_0)$ is free abelian of exponent ℓ^{k+1}. So, it is a natural $\mathbb{Z}/\ell^{k+1}[G_0]$ module.

From the data $(G, \mathbf{C})$ comes a projective sequence of reduced inner Hurwitz spaces, $\mathbb{H}_{\mathcal{G},\mathbf{C}} \stackrel{\text{def}}{=} \{\mathcal{H}(G_k, \mathbf{C})^{\mathrm{in,rd}}\}_{k=0}^{\infty}$, with $G_0 = G$. We often drop the extra notation, referring to the sequence just as $\{\mathcal{H}_k\}_{k=0}^{\infty}$. Such spaces are naturally normal varieties. Since the varieties are normal, their geometric components don't meet. So, we can define their projective normalizations in the field of fractions of each component separately. Each member of that collection, $\{\bar{\mathcal{H}}(G_k, \mathbf{C})^{\mathrm{in,rd}}\}_{k=0}^{\infty}$, maps to projective r-space, $\mathbb{P}^r$, modulo a natural $\mathrm{PGL}_2(\mathbb{C})$ action. We denote the quotient, $\mathbb{P}^r/\mathrm{PGL}_2(\mathbb{C})$, by J_r. The natural map is then $\bar{\mathcal{H}}_k \to J_r$.

Definition 1.1. A **M**(odular)**T**(ower) (on $\mathbb{H}_{\mathcal{G},\mathbf{C}}$) is a projective sequence of (non-empty) geometric components of the varieties in $\mathbb{H}_{\mathcal{G},\mathbf{C}}$.

Certain components, called **H**(arbater-**M**(umford) have played an inordinate role in the theory (see Def. 2.8). App. C shows how we detect the existence of

MTs. The easiest case is when there are H-M components because knowledge of the Nielsen class alone provides at least one such tower (Lem. 2.9). We call such a tower an H-M **MT**.

Many, but not all, **MT**s in this paper will be such. For trivial reasons there are no such **MT**s if $r = 3$. That still leaves the possibility that there are several distinct H-M towers defined by **MT** data: $\mathrm{Ni}(G, \mathbf{C})$ and the prime ℓ.

The case $r = 3$ is familiar as talk about dessins d'enfant. Somewhat artificially, these are λ-line covers with no meaning for cusps or elliptic ramfication (see §3.3.3). Sometimes this must be included for a complete analysis. We use the notation for general r only to put our special case, $r = 4$, in a context. Here is the first major problem with which we deal: The *U(niform) D(efinition) P(roblem)*.

PROBLEM 1.2 (UDP). Decide when $\mathbb{H}_{\mathcal{G},\mathbf{C}}$ contains a **MT**, $\mathbb{H}' \stackrel{\text{def}}{=} \{\mathcal{H}'_k\}_{k=0}^{\infty}$, where all the spaces – including the maps between them – in $\mathbb{H}'$ have a fixed number field K as definition field. We say K is a *definition field for* for $\mathbb{H}'$.

Even going back to modular curve towers, we have reason to generalize this definition by considering towers where each $\mathcal{H}'_k$ has an attached cyclotomic field CYC_k so that there is a number field K for which $K \cdot \mathrm{CYC}_k$ gives a compatible set of definition fields $K \cdot \mathrm{CYC}_{\mathbb{H}'}$ for the spaces and maps between them analogous to the outcome in Prob. 1.2. Assuming we are able to label the fields CYC_k explicitly, we say that K is a *cyclotomic definition field* for $\mathbb{H}'$.

PROBLEM 1.3 (CDP). Decide when $\mathbb{H}_{\mathcal{G},\mathbf{C}}$ contains a **MT**, $\mathbb{H}' \stackrel{\text{def}}{=} \{\mathcal{H}'_k\}_{k=0}^{\infty}$, with a cyclotomic definition field.

LEMMA 1.4. *If there is a k-independent bound on the number of components on $\mathcal{H}_k$, then any* **MT** *on $\mathbb{H}_{\mathcal{G},\mathbf{C}}$ has a definition field. If there is a uniform bound on the number of* H-M *components, then any* H-M **MT** *has a definition field.*

[**Fr95**, Thm. 3.21] is the forerunner of such results, providing a testable criterion for $\mathbf{C}$ that produces the conclusion of Lem. 1.4 for H-M **MT**s, but it never applies when $r = 4$. Prop. 3.13 includes showing an affirmative solution to Prob. 1.2 for example (1.2a). This is the first example, outside modular curves, where the conclusion of Lem. 1.4 has been shown for $r = 4$. §3 uses (1.2a) to show the properties we are after when $r = 4$. This includes an example giving a positive conclusion to Prob. 1.3, that is not an example of Prob. 1.2.

Then, §4 – with its consideration of all but the prime 3 – does the same thing for the split case (1.2b). It's called the split case, but it is still ℓ-Frattini properties that dominate. The results we need for this are analogous to those appearing in the consideration of the role of the Spin cover of A_n, $n \geq 4$, and $\ell = 2$, and we play on that. Yet, here we've gone far out of the territory of spin covers, for the prime 2 appears as ℓ in just one case. Finally, §7.3 explains why (1.2c) doesn't work for $r = 4$, and gives values of r where it does. Then, we compare with the previous results to see what it would take to show similar outcomes.

1.4. Types of applications. We have occasionally used the computer program [**GAP00**], though our choices have allowed us to revert to 'standard ' proof. Traditional journals limit publication in this area. Some type of literature change as suggested by [**Da12**] may be necessary to make such publications useful.

A refined generalization of the *Torsion Conjecture* on abelian varieties suggests that there are few cyclotomic torsion points on the general collection of abelian

varieties defined over number fields of a bound degree. Then, a refined version of the The Regular Inverse Galois Problem generalizes that. That generalization starts with this result.

For each finite group G, and any prime ℓ dividing $|G|$ for which G is ℓ-perfect. As in §2.1, consider the sequence of groups $\{G_{\mathrm{ab},\ell^{k+1}}\}_{k=0}^{\infty}$ which form ℓ-Frattini covers of G so that $\mathrm{Ker}(M_{G,\mathrm{ab},\ell^{k+1}} \to M_{G,\mathrm{ab},\ell^k})$, $k \geq 0$, is $M_{G,\ell}$, the characteristic exponent ℓ-Frattini module for G. The following is [**FrK97**, Thm. 4.4].

PROPOSITION 1.5. *Suppose for some number field K and integer r_0, each $G_{\mathrm{ab},\ell^{k+1}}$, $k \geq 0$, has a regular realization over K with $\leq r_0$ branch points.*

Then, there is a **MT** *of inner space components $\{\mathcal{H}_k\}_{k=0}^{\infty}$ with the common dimension of the spaces bounded by r_0-3 and with $\mathcal{H}_k(K)$ nonempty for each k.*

Then, we conjecture that no system of **MT** components as in the last paragraph can have K points at every level. Assuming well-accepted Diophantine conjectures, this fits within expectations (and is true for $r \leq 4$) if, as conjectured in [**FrK97**, Conj. 0.5],the compactified normalization of $\mathcal{H}_k$ has *general type*. (Some power of its line bundle of holomorphic 1-forms embeds the space in projective space.) For $r = 4$, where general type means the genus of a high tower level exceeds 1, [**Fr06**, Thm. 5.1] shows this follows from the eventual existence of ℓ-cusps on the tower levels, and it describes a limited set of possibilities where this might not happen.

Therefore, computing the cusps as in §3.3.3 for the $n = 5$ ℓ-Frattini case and the $n = 3$, $\ell \neq 3$ cases, is an explicit realization of why there are no rational points at high levels on those **MT** s.

Prop. 6.8 says the components with non-zero lift invariant are a cyclotomic orbit of spaces. They therefore they have no fixed (number) field of definition. Being normal varieties, they can't have K points up the tower. Still, they are appropriate for asking about a Serre OIT as in §2.2.3 as are the other examples: $n = 3$ and the **MT**s over the H-M components (with 0 lift invariant), and the $n = 5$ ℓ-Frattini case where all components have definition field $\mathbb{Q}$. Even, for the higher $n \equiv 5 \mod 8$, we can approach an OIT result without waiting on some still unknown conjectures referenced above.

1.5. Nielsen classes, covers and cusps. This is a brief review of [**BFr02**, §3,1 and §3.7] or [**Fr12a**, §6.1].

1.5.1. *Nielsen classes: absolute and inner.* Given $(G, \mathbf{C})$, *Nielsen classes* $\mathrm{Ni}(G, \mathbf{C})$, list precisely degree n covers of the z-sphere, $\varphi : X \to \mathbb{P}^1_z$, branched at r distinct points $\boldsymbol{z} \stackrel{\mathrm{def}}{=} \{z_1, \ldots, z_r\} \subset \mathbb{P}^1_z$ that have the r conjugacy classes of $\mathbf{C}$ as local monodromy (in some order).

Such covers correspond to $\boldsymbol{g} \stackrel{\mathrm{def}}{=} (g_1, \ldots, g_r) \in G^r$, where these conditions hold:

(1.4a) *Generation*: $\langle g_i | i = 1, \ldots, r\rangle = G$; and

(1.4b) *Product-one*: $g_1 \cdots g_r = 1$.

When necessary for clarity, we write $\boldsymbol{g} \in \mathbf{C}$ to mean that for some $\pi \in S_r$, $g_i \in \mathrm{C}_{(i)\pi}$, $i = 1, \ldots, r$. From (1.4b), any $r-1$ of the g_i s in (1.4a) generate G. Those who use the *monodromy method* call such g_i s satisfying (1.4a) and (1.4b) *branch cycles*. The collection of all such, in the respective conjugacy classes $\mathbf{C}$, is the *Nielsen class* $\mathrm{Ni}(G, \mathbf{C})$ of the cover.

Covers corresponding to two choices of r-tuples satisfying (1.4) will be isomorphic covers (of $\mathbb{P}^1_z$) if and only if some $h \in S_n$ conjugates the one r-tuple to the

other. That is, degree n covers, with $\boldsymbol{z}$ as branch points, monodromy G and local monodromy $\mathbf{C}$, correspond to the elements of $\mathrm{Ni}(G,\mathbf{C})/N_{S_n}(G) \stackrel{\mathrm{def}}{=} \mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$. These are the *absolute Nielsen classes*.

There is a similar notion called *inner Nielsen classes*, replacing $\mathrm{Ni}(G,\mathbf{C})/N_{S_n}(G)$ by $\mathrm{Ni}(G,\mathbf{C})/G = \mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$. Suppose two covers are both Galois, with their covering groups identified with G by some isomorphism. Then, the covers are equivalent if there is an isomorphism commuting with their projects to $\mathbb{P}^1_z$ that induces an inner automorphism on G.

1.5.2. *The groups B_r and H_r.* Denote the space of r distinct, but unordered, points on $\mathbb{P}^1_z$ by U_r. Start with one cover $\varphi : X \to \mathbb{P}^1_z$ branched over $\boldsymbol{z}'$. Then, deform the punctures $\boldsymbol{z}'$, keeping them distinct, to another set of r points $\boldsymbol{z}''$. That is, give a path (continuous and piecewise differentiable) $\mathcal{L}$: $t \in [0,1] \mapsto \boldsymbol{z}'(t)$, in U_r, with $\boldsymbol{z}'(0) = \boldsymbol{z}'$ and $\boldsymbol{z}'(1) = \boldsymbol{z}''$.

If $\boldsymbol{z}'' = \boldsymbol{z}'$, then the cover at the end of the path corresponds to an element $\boldsymbol{g}'$ whose entries are words – independent of $\boldsymbol{g}$ – in the entries of $\boldsymbol{g}$. The collection of words forms the Hurwitz monodromy group H_r, a quotient of the Artin Braid group B_r. The following two words generate H_r.

(1.5a) $q_1 : \boldsymbol{g} \mapsto (g_1 g_2 g_1^{-1}, g_1, g_3, \dots, g_r)$ the *1st* (coordinate) *twist*, and

(1.5b) $sh : \boldsymbol{g} \mapsto (g_2, g_3, \dots, g_r, g_1)$, the *left shift*.

They both preserve generation, product-one and the conjugacy class collection conditions of (1.4), Conjugating q_1 by $\mathbf{sh}$, gives q_2, the twist moved to the right. Repeating gives $q_3, \dots, q_{r-1}$. Three relations generate all relations for H_r:

(1.6a) Sphere: $q_1 q_2 \cdots q_{r-1} q_{r-1} \cdots q_1$;

(1.6b) Commuting: $q_i q_j = q_j q_i$, for $|i-j| \geq 2$ (read subscripts mod $r-1$); and

(1.6c) (Braid) Twisting: $q_i q_{i+1} q_i = q_{i+1} q_i q_{i+1}$.

The group H_r inherits (1.6b) and (1.6c) from B_r.

1.5.3. *The cusp group and reduced Nielsen classes.* In general the spaces are defined by a quotient of the braid group B_r acting on Nielsen classes, $\mathrm{Ni}(G,\mathbf{C})$. §3.1 discusses precisely our main cases , where $r = 4$, and the spaces are natural upper half-plane quotients and j-line covers. We keep the general case mainly for context because some older results were only possible for $r > 4$ (possibly very large).

The *moduli group*, $\mathcal{Q}''$, generated by $\mathbf{sh}^2$, and $q_1 q_3^{-1}$ acts through a Klein 4-group on Nielsen classes. It is a normal subgroup of H_4. The *cusp group* $\mathrm{Cu}_4 \leq H_4$ is generated by $\mathcal{Q}''$ and q_2.

Define the *reduced inner* Nielsen classes to be $Ni^{\mathrm{in}}/Q'' = \mathrm{Ni}^{\mathrm{in,rd}}$. That is, mod out by G and also be equivalencing elements by the action of Q''.

2. The universal ℓ-Frattini cover

Our opening remarks are in either edition of [**FrJ86**], or – right to the point for this paper – in [**BFr02**, §3.3]. For any finite group G and $\ell || G|$, there is a maximal sequence of groups $G_0 = G$, G_1, …, such that the projective limit of these defines the universal ℓ-Frattini cover, $\psi_{G,\ell} : \tilde{G}_\ell \to G$, of G.

For any ℓ-Frattini cover $\psi : H \to G$. $\psi_{G,\ell}$ factors through ψ. The key 1st observation is that the whole ℓ-Sylow of $\tilde{G}_\ell$ is a pro-free pro-ℓ group. Therefore, so is $\ker(\psi_{G,\ell})$. The rank – minimal number of generators – of the latter is of equals the rank of $M_{G,\ell} \stackrel{\mathrm{def}}{=} \mathrm{Ker}(G_1 \to G_0)$ as a $\mathbb{Z}/\ell$ module. We call this the *characteristic module* of (G,ℓ) and denote its rank by $\mathrm{rk}_{G,\ell}$.

2.1. Abelianization of the Frattini part of G_ℓ. We can abelianize the kernel of $G_\ell \to G$: $M_{G,\mathrm{ab},\ell^\infty} \stackrel{\mathrm{def}}{=} \ker(\psi_{G,\ell})/(\ker(\psi_{G,\ell}, \ker(\psi_{G,\ell}))$, is a free abelian $\mathbb{Z}_\ell$ module of rank $\mathrm{rk}_{G,\ell}$. Denote the maximal exponent ℓ^k quotient of $M_{G,\mathrm{ab},\ell^\infty}$ by M_{G,ab,ℓ^k}. Then, the $\mathrm{Ker}(M_{G,\mathrm{ab},\ell^{k+1}} \to M_{G,\mathrm{ab},\ell^k})$, $k \ge 0$, is also $M_{G,\ell}$ in a natural way, essentially given by multiplying by ℓ^{k-1}.

2.1.1. *Quotients of the abelianization.* Just as the sequence $G_0, G_1, \dots$ defines G_ℓ, by modding out $M_{G,\mathrm{ab},\ell^\infty}$ by powers of ℓ we get the corresponding series, $G = G_0, G_{\mathrm{ab},1}, G_{\mathrm{ab},2}, \dots$, of covers of G for which $G_{\mathrm{ab},k} \to G$ is the maximal ℓ-Frattini cover of G with abelian kernel of exponent ℓ^k. This is the characteristic abelianized ℓ-Frattini series of G.

Definition 2.1. We say $M_{G,\mathrm{ab},\infty}$ has a $\mathbb{Z}_\ell$ *quotient* if it has a proper $\mathbb{Z}_\ell[G]$ module quotient M' that is a free $\mathbb{Z}_\ell$ module (of rank, say, $m' \ge 1$).

By modding out by the kernel of $M_{G,\mathrm{ab},\infty} \to M'$ we produce another series, $G = \{G_{M',k}\}_{k=0}^\infty$ with $G_{0,M'} = G_0 = G$, of ℓ-Frattini covers of G with the kth cover kernel isomorphic to $(\mathbb{Z}/\ell^k)^{m'}$.

Definition 2.2. Refer to a sequence of groups arising from a $\mathbb{Z}_\ell$ Frattini quotient as an abelian ℓ-Frattini sequence.

The ℓ-adic representations of that arise in this paper arise from abelian ℓ-Frattini sequences.

[**Fr95**, Part II] gives each of $M_{A_5,\ell}$ explicitly (see Rem. B.1). [**BFr02**, Prop. 5.6 and Cor. 5.7] makes $M_{A_5,2}$ explicit, especially the Loewy display of its simple module constitutions. Since [**BFr02**] for $\ell = 2$ is our model (the toughest case), we use that to compare to $\ell = 5$ (see Prop. 2.1.3). As $\ell = 3$ is excluded by our choice of conjugacy classes, we put that case totally aside.

All examples in this paper are formed around alternating groups. Our main examples use a quotient of the abelianized 5-Frattini over A_5 and all the abelianized ℓ-Frattini covers of the natural semidirect product $(\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/3$ (excluding $\ell = 3$).

2.1.2. *Notes on* PSL_2. This subsection covers what we need of two roles of the group $\mathrm{PSL}_2(\mathbb{Z}/\ell^k)$ (§A.1). When $\ell \ne 2$ (resp. $\ell = 2$), $\mathrm{Ker}((\mathbb{Z}_\ell)^* \to (\mathbb{Z}/\ell)^*)$ is cyclic, generated by $1 + \ell$ (resp. has – multiplicative – generators 1+4 and -1).

Lemma 2.3. *For $\ell \ge 3$, $\mathrm{Ker}((\mathbb{Z}_\ell)^* \to (\mathbb{Z}/\ell)^*)$ (resp. $\mathrm{Ker}((\mathbb{Z}_2)^* \to (\mathbb{Z}/2^3)^*)$) is a rank 1 pro-free pro-ℓ (resp. pro-2) group.*

Proof. In each case the designated kernel is cyclically generated as a profinite group. For example, for $\ell = 2$ the kernel is $\langle 1 + 4 \rangle$. Example: The kernel of $\mathrm{Ker}((\mathbb{Z}/2^{k+1})^* \to (\mathbb{Z}/2^k)^*)$ is $\{1, 1{+}2^k = (1{+}4)^{2^{k-2}}\} \mod 2^{k+1}$. □

Our main Frattini example (as in (1.1)) uses the classical identification of A_5 with $\mathrm{PSL}_2(\mathbb{Z}/5)$, 2×2 matrices over $\mathbb{Z}/5$ of determinant 1, mod $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. This acts as conjugation on Ad_{ℓ^k}, the 2×2 matrices of trace 0 over $\mathbb{Z}/\ell^k$. This is the adjoint action for conjugation by G_1.

An element g of order 3 acts on it as if it is a sum of the identity representation and a 2-dimensional irreducible representation. You can canonically define the 2-dimensional space as the image of Ad_ℓ (in this additive notation) by the homomorphism $A \mapsto A^g - A$. The kernel of this map is the centralizer Cen_g.

PROPOSITION 2.4. *If $\ell \neq 2$, the additive group of 2×2 matrices over $\mathbb{Z}/\ell^k$ of trace 0 identifies with the $\mathbb{Z}/\ell^{k+1}[\mathrm{PSL}_2(\mathbb{Z}/\ell)]$ module*

$$\mathrm{Ad}_{\ell^k} = \mathrm{Ker}(\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)), k \geq 0.$$

The analogue for $\ell = 2$ replaces Ad_{ℓ^k} by $\mathrm{Ker}(\mathrm{PSL}_2(\mathbb{Z}/2^{k+3}) \to \mathrm{PSL}_2(\mathbb{Z}/2^3))$.

PROOF. For the statement for $\ell \neq 2$, do an induction on k, assuming its truth for k, compute $\mathrm{Ker}(\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+2}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1}))$ as

$$\left\{ \begin{pmatrix} 1+\ell^{k+1}a & \ell^{k+1}b \\ \ell^{k+1}c & 1+\ell^{k+1}d \end{pmatrix} \mid \text{ of Det equal to } 1 \right\} \mod \ell^{k+2}.$$

The determinant condition then requires $d = -a$. Finally, Lem. 2.3 equates the units $\{1+\ell a \mod \ell^{k+1} \mid a \in \mathbb{Z}_\ell\}$ with the additive group $\mathbb{Z}/\ell^k$. The adjustment for the case $\ell = 2$ is from the same lemma, which restricts that identification to units of form $1+2^3a \mod 2^{k+3}$. □

2.1.3. *Characteristic A_5 modules.* We handle some technicalities in using characteristic Frattini modules while bordering territory recognizable from, say, [**Se68**].

From Schur-Zassenhaus, for $n = 5$, the only ℓ for which we can expect ℓ-Frattini covers of A_5 are $\ell = 2, 3$ or 5. This subsection tells enough about ℓ-Frattini examples to show their significance, without – we hope – inundation. Much of the basic material is in either edition of [**FrJ86**] (Chap. 20, 1st edition, Chap. 22 in 2nd). Especially we add comments to [**FrJ86**, §22.13] and [**Se68**, IV, §3.4].

PROPOSITION 2.5. *The $\mathbb{Z}/\ell[G]$ module $M_{G,\ell}$ is always indecomposable (contains no direct summand). If the order of $g \in G_{k_0}$ is $u \cdot \ell^v$, with $\gcd(u, \ell) = 1$ and $v > 0$, then any $g' \in G_k$, $k \geq k_0$ over g has order $u \cdot \ell^{v+k-k_0+1}$.*

The $\mathbb{Z}/5[A_5]$ module $M_{A_5,5}$ has rank 6. it is an extension of Ad_5 by Ad_5. In particular, $M_{A_5,\mathrm{ab},5^\infty}$ has Ad_{5^∞} as a $\mathbb{Z}_5$ quotient (of rank 3).

PROOF. The 1st sentence is [**FrK97**, Indecomposability Lem. 2.4]. The 2nd sentence is [**FrK97**, Lift Lem. 4.1].

Here is one description of $G_{\ell,1} \to G_0$ [**Fr02**, Prop. 2.8]. Let $\tilde{\psi}_P \tilde{P}_\ell \to P_\ell$ be the minimal pro-free pro-ℓ cover of P_ℓ. The kernel, Ker_ℓ is also pro-free pro-ℓ. Mod out by its Frattini subgroup (generated by ℓth powers and commutators). That induces $\psi_{P_\ell,1} : G_1(P_\ell) \to P_\ell$ with kernel $M(P_\ell, \ell)$ in our previous notation. Take the normalizer, $N_G(P_\ell)$, of P_ℓ in G. Then, $\mathrm{Ker}(\psi_{P_\ell,1})$ is a $N_G(P_\ell)$ module. The Frattini module $M(G, \ell)$ is a quotient of the natural $\mathbb{Z}/\ell[G]$ module induced from inducing $\mathrm{Ker}(\psi_{P_\ell,1})$ from $N_G(P_\ell)$ to G. App. B.1 says more on two different approaches to this construction that give it precisely.

[**Fr02**, Ex. 2.11] applies the above argument by noting that the normalizer of a 5-Sylow in A_5 is a copy of D_5. Note that the 6-dimensional module can't be the decomposable direct sum of two copies of Ad_5. So, this is an extreme case where the induced module gives the whole characteristic 5-Frattini module. □

PROPOSITION 2.6. *By contrast with $M_{A_5,\mathrm{ab},5^\infty}$, for the prime $\ell = 2$, $M_{A_5,\mathrm{ab},2^\infty}$ has no $\mathbb{Z}_2$ quotient.*

PROOF. When $\ell = 2$ where $M_{A_5,2}$ identifies with the $\mathbb{Z}/2[A_5]$ module of dimension 5 consisting of the sum of the six $D_5 \leq A_5$ cosets, $T_1, \ldots, T_6$, in A_5 modulo the sum of them all [**BFr02**, Prop. 5.6] (or [**Fr95**, Part III]). Write a nonzero representative of $M_{A_5,2}$ as $\sum_{i=1}^6 a_i T_i$, with 1, 2, or 3 of the a_i s nonzero. Restricting to

A_4 identifies $M_{A_5,2}$ with the analogous sum of $\mathbb{Z}/2 \le A_4$ cosets. [**BFr02**, Cor. 5.7] describes $M_{A_5,2}$ as being an extension of $\mathbb{Z}/2[A_5]$ modules

$$V \to M_{A_5,2} \xrightarrow{\text{Aug}} \mathbf{1}$$

with these two properties.

(2.1a) Aug: $\sum_{i=1}^6 a_i T_i \mapsto \sum_{i=1}^6 a_i$; and

(2.1b) elements in $V \setminus \{\mathbf{0}\}$ are represented by sums with two a_i s nonzero.

Clearly, V is irreducible since A_5 is transitive on its nonzero elements.

Now suppose $M_{A_5,\text{ab},2^\infty}$ has a proper $\mathbb{Z}_2$ quotient M'_∞. Then, there is a proper quotient M' of $M_{A_5,2}$ so that the natural $\mathbb{Z}/2^2[A_5]$ quotient of M'_∞ is an extension of M' by M'. From the irreducibility of V, $M' = \mathbf{1}$ and therefore A_5 has a central 2-Frattini extension with kernel $\mathbb{Z}/2^2$. This contradicts that the universal central extension of A_5 has kernel $\mathbb{Z}/2$ (the Schur multiplier of A_5. □

REMARK 2.7 (Existence of $\mathbb{Z}_\ell$ quotients). It is suspicious, but easy to guess that the only time $M_{G_\ell,\text{ab},\ell^\infty}$ has a $\mathbb{Z}_\ell$ quotient is when G is naturally related to a classical arithmetic groups over $\mathbb{Z}_\ell$. Maybe, if G is simple, it might be true only if G is also a Chevalley group with characteristic prime ℓ where the $\mathbb{Z}_\ell$ quotient is given by the adjoint representation.

2.2. More about $n \equiv 5 \mod 8$ ($n \ge 5$). We discuss the general case for which $n = 5$ is one of our main examples.

2.2.1. *More Frattini Principles.* The main stays of this paper are the use of Frattini Principles and Nielsen class elements given by Def. 2.8.

DEFINITION 2.8. Suppose r is even. Then, a **H**(arbater-**M**(umford) representative of $\text{Ni}(G, \mathbf{C})$ is an element of form $(g_1, g_1^{-1}, \dots, g_r, g_r^{-1})$. A braid orbit containing an H-M rep. is called an H-M orbit.

Lem. 2.9 is an easy clue as to why Frattini covers are *so* essential in using Hurwitz spaces for ℓ-adic representations. We apply a far-reaching generalization of it in the last part of the proof of Prop. 3.3.3.

LEMMA 2.9. *If $\psi : H \to G$ is a Frattini cover, with $\gcd(|\text{Ker}(\psi)|, N_{\mathbf{C}}) = 1$, Then an* H-M *orbit of* $\text{Ni}(G, \mathbf{C})$ *has at least one* H-M *orbit over it in* $\text{Ni}(H, \mathbf{C})$.

PROOF. Assume $\boldsymbol{g}_{\text{H-M}} = (g_1, g_1^{-1}, \dots, g_r, g_r^{-1}) \in \text{Ni}(G, \mathbf{C})$. Let $h_1, \dots, h_r$ be same order lifts to H lying, respectively, over $g_1, \dots, g_r$. Since H is a Frattini cover, $\langle h_1, \dots, h_r \rangle = H$ is automatic, and $\boldsymbol{h} = (h_1, h_1^{-1}, \dots, h_r, h_r^{-1}) \in \text{Ni}(H, \mathbf{C})$. □

The following is a special case of [**BFr02**, Prop. 2.17] (with clarification in [**Fr06**, Frat. Princ. 1, Princ. 3.5]). Recall that $\text{Cen}(G)$ denotes the center of G.

PROPOSITION 2.10. *Assume G is centerless. Then, the q_2^2 orbit on $\boldsymbol{g} \in \text{Ni}(G, \mathbf{C})^{\text{in}}$*

$$\textit{has length } o(g_2, g_3) \stackrel{\text{def}}{=} o_{\boldsymbol{g}} = \text{ord}(g_2 \cdot g_3)/|\langle g_2 \cdot g_3 \rangle \cup \text{Cen}(g_2, g_3)|.$$

Then, one of the following holds for the length o' of the q_2 orbit on the class of $\boldsymbol{g}$.

(2.2) *Either: $g_2 = g_3$ and $o' = 1$, or; if $o = o_{\boldsymbol{g}}$ is odd and $g_3(g_2 \cdot g_3)^{o-1}$ has order 2, then $o = o'$; or else $o' = 2 \cdot o$.*

We need two more Frattini Principles: (2.3a) is [**Fr06**, Frat. Princ. 1, Princ. 3.5] (2.3b) is [**Fr06**, Frat. Princ. 2, Princ. 3.6]. Assume $\{G_i\}_{i=0}^\infty$ is an abelianized ℓ-Frattini sequence (Def. 2.2), and $\mathbf{C}$ are ℓ' conjugacy classes of G_0. Then, a Cu_4

orbit, ${}_{\mathbf{c}}O = {}_{\mathbf{c}}O_{\boldsymbol{g}}$, on $\mathrm{Ni}(G_{k_0}, \mathbf{C})^{\mathrm{in,rd}}$ defines a cusp. It is an *ℓ-cusp* if $\ell | o_{\boldsymbol{g}}$. Almost the opposite of this is the following.

DEFINITION 2.11. Assume for $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ that $\langle g_2, g_3\rangle$ and $\langle g_1, g_4\rangle$ are ℓ' groups. Then, we call ${}_{\mathbf{c}}O_{\boldsymbol{g}}$ a g(roup)-ℓ'-cusp.

(2.3a) Suppose ${}_{\mathbf{c}}O$ is an ℓ-cusp. Then, for all $k \geq k_0$, the width of any level k cusp orbit above ${}_{\mathbf{c}}O$ is ℓ^{k-k_0} times the width of ${}_{\mathbf{c}}O$.

(2.3b) : For $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$, $r = 4$ if ${}_{\mathbf{c}}O_{\boldsymbol{g}}$ is a g(roup)-ℓ'-cusp. Then, for $H \to G$ an ℓ-Frattini cover, there is a g-ℓ'-cusp in $\mathrm{Ni}(H, \mathbf{C})$ over ${}_{\mathbf{c}}O_{\boldsymbol{g}}$ (generalizing the conclusion of Lem. 2.9).

2.2.2. *Alternating group Hurwitz spaces.* Suppose α is an automorphism of G that permutes the conjugacy classes (retaining their multiplicities) in $\mathbf{C}$.

DEFINITION 2.12. Suppose $O\boldsymbol{g}$ is a braid orbit of $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$. We say α is braidable, if $\alpha(\boldsymbol{g}) \in O_{\boldsymbol{g}}$.

[**Fr12a**, §B.2.2] is an exposition on braidable outer automorphisms. This is a big issue in Hurwitz space components, but we give just one example.

[**Fr12b**, Prop. D.2] gives the monodromy groups for all the Nielsen classes given by $G = A_n$, $n \equiv 1 \mod 4$, and the conjugacy classes $\mathbf{C}_{(\frac{n+1}{3})^4}$. The cases $n \equiv 5 \mod 8$, and $n \equiv 1 \mod 8$ have important differences.

There is one braid orbit in the former case. There are two braid orbits, each orbit taken to the other by the outer automorphism of A_n in the latter. In this case, the outer automorphism of A_n (which preserves the Nielsen class) is not braidable. Further, the two components are conjugate over a quadratic extension of $\mathbb{Q}$.

For $n \equiv 5 \mod 8$ the absolute reduced Hurwitz space has geometric monodromy A_N, $N = \frac{n+1}{2}$, as a $\mathbb{P}^1_j$ cover. In the inner case the geometric monodromy is the wreath product of A_N with $\mathbb{Z}/2$. The arithmetic monodromy (inner case) is the wreath product of S_N with $\mathbb{Z}/2$.

2.2.3. *Framework for ℓ-adic representations.* There are families of ℓ-adic representations attached to each of the Frattini and Split cases of (1.2). There are just two primes, $\ell = 2$ and 5 (resp. $\ell \leq n$, not dividing $\frac{n+1}{2}$) in (the) Frattini case (1.2a) (resp. (1.2c). So, we start by explaining that case. Then, in the split cases like (1.2b), we see a further set of the attributes like that for modular curves.

The essential ingredient that gets us started is an affirmative answer to Prob. 1.2. Prop. 3.13 provides this. There is one braid orbit on on each of the Nielsen classes $\mathrm{Ni}(G_{k+1}) = \mathrm{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4})$. Then, the family of reduced Hurwitz spaces $\{\mathcal{H}_{k+1}\}_{k=0}^{\infty}$ supports a family of 5-adic representations in the following sense.

For each $\boldsymbol{p}' \in \mathcal{H}_0$ (an open subset of the projective line, but not the j-line), consider any projective sequence of points on $\{\mathcal{H}_{k+1}\}_{k=0}^{\infty}$ lying over $\boldsymbol{p}'$. This corresponds to a copy of $(\mathbb{Z}_5)^3 = V_{\boldsymbol{p}'}$ where $\mathbb{Z}_5$ is the 5-adic integers. To simplify notation, assume $\boldsymbol{p}'$ has coordinates in the rational numbers $\mathbb{Q}$.

Then, the absolute Galois group, $G_{\mathbb{Q}}$, of $\mathbb{Q}$ maps $V_{\boldsymbol{p}'}$ to another projective system of points over $\boldsymbol{p}'$ (and copy of $(\mathbb{Z}_5)^3$). If these were spaces were modular curves – one case of reduced Hurwitz spaces – then Serre's O(pen)I(mage)T(heorem) qualititatively describes when $G_{\mathbb{Q}}$ is transitive on these projective systems over $\boldsymbol{p}'$.

This, and our other examples, are test cases. For example, for the OIT to be possible (or serious) in this context, we need that some conclusion like that of

Lem. 1.4 holds. That would be the case if all the spaces $\{\mathcal{H}_{k+1}\}_{k=0}^{\infty}$ were irreducible. Also, Def. 7.1 states precisely the "eventually ℓ-Frattini" condition on the monodromy of $\mathcal{H}_{k+1} \to J_r$ that must hold.

3. Frattini properties of spaces in (1.2a)

For $n = 5$ there are two values of ℓ (2 and 5) that satisfy condition (1.2c): ℓ divides $n!/2$; but it does not divide $\frac{n+1}{2}$. As in §3.3, the former condition guarantees a non-trivial natural ℓ-adic Frattini extension of A_n. The latter that the conjugacy class $\mathrm{C}_{\frac{n+1}{2}}$ lifts uniquely to same order conjugacy class in any such an extension.

§3.3.1 and §3.3.2 do the example Frattini case where $n = 5$, and $\ell = 5$ where the group series is $H_{5,k} \stackrel{\text{def}}{=} \mathrm{PSL}_2(\mathbb{Z}/5^{k+1}) \to \mathrm{PSL}_2(\mathbb{Z}/5) = H_{5,0}$, $k \geq 0$. [**BFr02**] has our model for the case $\ell = 2$ and $n = 5$. That may be the most exciting Frattini case, but $\ell = 5$ will help us flesh out what happens in the general Frattini case.

3.1. Producing the spaces. Braid elements acting on Nielsen classes will produce the cusps and genuses of compactifications of $\mathcal{H}(H_{5,k}, \mathbf{C}_{3^4})^{\mathrm{in,rd}} \stackrel{\text{def}}{=} \mathcal{H}'_k$.

Problem 3.1 (Uniform Definition). Afirming (3.1) strongly affirms Prob. 1.3 (Lem. 1.4). When is there a uniform bound (as a function of k) in these cases:

(3.1a) On the number of components of $\bar{\mathcal{H}}'_k$?

(3.1b) Failing that, on the number of H-M components on these spaces?

Our major result in this Frattini example is Prop. 3.13 showing $\{\mathcal{H}'_k\}_{k=0}^{\infty}$ satisfies the very strong (3.1a). By definition a *reduced* Hurwitz space is a Hurwitz space modulo a natural action that equivalences covers $\varphi_i : X_i \to P^1_z$, $i = 1, 2$, when there is $\alpha \in \mathrm{PGL}_2(\mathbb{C})$, so that $\alpha \circ \varphi_1 = \varphi_2$.

Recall the cusp group in (1.5.3). The following elements all act on $\mathrm{Ni}^{\mathrm{in,rd}}$.

$$\gamma_0 = \mathbf{sh}, \gamma_1 = q_1 q_2, \text{ and } \gamma_\infty = q_2. \tag{3.2}$$

The *index* of a permutation $g \in S_n$ is n minus the number of orbits of g. We denote it $\mathrm{ind}(g)$.

Take the actions of γ_0, γ_1 and γ_∞ on a (reduced) braid orbit O in $\mathrm{Ni}^{\mathrm{in,rd}}$. Compute their corresponding indices, as $\mathrm{ind}(\gamma'_0)$, $\mathrm{ind}(\gamma'_1)$ and $\mathrm{ind}(\gamma'_\infty)$. Also, let $t_O(q)$ be the number of fixed points of a braid on O.

Definition 3.2. Given a (nonsingular curve) cover $\bar{\mathcal{H}} \to \mathbb{P}^1_j$ ramified only over $0, 1, \infty$, the *cusps* are the points over $j = \infty$. The respective *widths* of the cusps are the ramification indices of those corresponding points.

The γ_∞ orbits are the (combinatorial) cusps, which correspond to the geometric (physical?) cusps on the Hurwitz space component $\bar{\mathcal{H}}_O$ corresponding to O. We often denote γ_∞ orbits on O by notation like $O(u, v; a)$, where u and v are integers and a is extra notation distinguishing orbits that have the same values u and v. Here is what u and v signify. If $\boldsymbol{g} = (g_1, g_2, g_3, g_4) \in O(u, v; a)$, then $u = \mathbf{mp}(g) \stackrel{\text{def}}{=} \mathrm{ord}(g_2 g_3)$ is the *middle product* of $\boldsymbol{g}$. Also, $v = \mathbf{wd}(\boldsymbol{g})$ is the actual length of the orbit under γ_∞. Given $\boldsymbol{g} \in O(u, v; a)$, refer to its orbit type as $(u, v) = (\mathbf{mp}(g), \mathbf{wd}(g))$. It can (though not always) be easy to compute v, as in our examples. We say more on that below.

Then the genus of the component corresponding to O is $\mathbf{g}_O$ in the following formula [**BFr02**, (8.1)]:

$$2(|O|+\mathbf{g}_O-1) \begin{array}{l} = \mathrm{ind}(\gamma_0')+\mathrm{ind}(\gamma_1')+\mathrm{ind}(\gamma_\infty') \\ = \frac{2(|O|-t_O(\gamma_0))}{3}+\frac{2(|O|-t_O(\gamma_1))}{2}+\sum_{O(u,v;a)\subset O} v-1. \end{array} \tag{3.3}$$

This is Riemann-Hurwitz applied to the (compactified) Hurwitz space component as a j-line cover.

In a standard normalization the only possible points of ramification are where $j = 0$, 1 or ∞. The points over 0 correspond to the orbits of the order 3 element γ_0', and the points over 1 correspond to the orbits of the order 2 element γ_1'. The fixed points of these elements are the *elliptic fixed points*.

3.2. PSL_2 **Frattini properties.** This subsection considers Frattini properties of the $\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1})$ groups.

Definition 3.3. Let $\cdots \to H_{k+1} \to H_k \to \cdots \to H_0$ be any sequence of (finite group) covers. We say it is *eventually Frattini* if there is a k_0 with $H_{k+1} \to H_k$ a Frattini cover for $k \geq k_0$. A composition of homomorphisms is Frattini if and only if each is. So, that is equivalent to $H_k \to H_{k_0}$ is Frattini for $k \geq k_0$.

Lemma 3.4. *The natural cover* $\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$ *is a Frattini cover for all* k *if* $\ell > 3$. *For* $\ell = 3$ *(resp. 2),* $\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell^{k_0+1})$, $k \geq k_0$ *where* $k_0 = 1$ *(resp. 2), is the minimal value for which these are Frattini covers. That is, for all* ℓ *the sequence* $\{\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1})\}_{k=0}^{\infty}$ *is eventually Frattini.*

Proof. The first sentence is [**FrJ86**, Cor. 22.13.4] which is a detailed repeat of the [**Se68**, Lem. 3, IV-23] proof. The latter also has as an exercise that the same statement and proof applies to $\mathrm{PSL}_d(\mathbb{Z}/\ell)$. We now add to those exercises for the cases $\ell = 2$ and 3. It is often here easier to work in $\mathrm{SL}_2(R)$ rather than $\mathrm{PSL}_2(R)$ but the outcome is essentially the same, with $\ell = 2$ slightly trickier.

For $\ell = 3$, [**Se68**, IV-28, Exer. 3] asks to show that $\mathrm{SL}_2(\mathbb{Z}/3^2) \to \mathrm{SL}_2(\mathbb{Z}/3)$ is not Frattini. We say it purely cohomomologically. Let $\mu \in H^2(\mathrm{SL}_2(\mathbb{Z}/3), \mathrm{Ad}_3)$ define the cohomology class of this extension. ([**Nor62**, p. 241] gives a comfortable treatment of H^2.) For any cohomology group, $H^*(G, M)$, with M a $\mathbb{Z}/\ell[G]$ module, restriction to an ℓ-Sylow $P_\ell \leq G$ is an isomorphism onto the G invariant elements of $H^*(P_\ell, M)$ [**Br82**, Prop. 10.4]. So, the extension μ splits if μ_ℓ splits.

There is an element, g_3, of order 3 in $\mathrm{SL}_2(\mathbb{Z})$ – $\mathrm{PSL}_2(\mathbb{Z})$ is well-known to be freely generated by an element of order 3 and an element of order 2 – and so in $\mathrm{SL}_2(\mathbb{Z}/3^2)$. This element of order 3 – given, say, by $A = \left(\begin{smallmatrix} 1 & -3 \\ 1 & -2 \end{smallmatrix}\right)$ (as in [**Fr95**, Ex. 3.9]) – generates a 3-Sylow. (Later we have reason to use a different element – see §4.2.1 – $A^* = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.) So μ_3 splits. Denote the conjugacy class of A by C_3, and note that its characteristic polynomial is $x^2 + x + 1$.

Any lift of any non-trivial element in $\mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/3^2) \to \mathrm{SL}_2(\mathbb{Z}/3)) = (\mathbb{Z}/3)^3$ lifts to an element of order 3^2 in

$$\mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/3^3) \to \mathrm{SL}_2(\mathbb{Z}/3)) = (\mathbb{Z}/3^2)^3,$$

as in Prop. 2.4. That is, $\mathbb{Z}/3^{k+1} \to \mathbb{Z}/3^k$, $k \geq 1$, is a Frattini extension. So, the extension $\mathrm{SL}_2(\mathbb{Z}/3^3) \to \mathrm{SL}_2(\mathbb{Z}/3^2)$ certainly does not split.

[**Se68**, IV-28, Exer. 1.b] states that $\mathrm{SL}_2(\mathbb{Z}/3^{k+2}) \to \mathrm{SL}_2(\mathbb{Z}/3^2)$, $k \geq 0$, is Frattini. Take $v \in \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/3^2) \to \mathrm{SL}_2(\mathbb{Z}/3))$. Then, for any $\tilde{v} \in \mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/3^3) \to$

$\mathrm{SL}_2(\mathbb{Z}/3))$ lifting v, $\tilde{v}^3$ identifies with v, but in $\mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/3^3) \to \mathrm{SL}_2(\mathbb{Z}/3^2))$. So, from that stage on, any subgroup mapping onto $\mathrm{SL}_2(\mathbb{Z}/3)$ has the kernel in it.

The case $\ell = 2$ is similar. Go up a modulus higher (as in Prop. 2.4) to exploit the free-abelianness of $\mathrm{Ker}(\mathrm{SL}_2(\mathbb{Z}/2^k) \to \mathrm{SL}_2(\mathbb{Z}/2^3))$. [**Se68**, IV-28, Exer. 2] produces a D_3 in $\mathrm{SL}_2(\mathbb{Z}_2)$ showing that $\mathrm{SL}_2(\mathbb{Z}_2) \to \mathrm{SL}_2(\mathbb{Z}/2)$ splits. □

REMARK 3.5. Let $\{G_k\}_{k=0}^{\infty}$ by the Characteristic ℓ-Frattini series for $G_0 = G$. [**FrK97**, Lem. 4.1] shows that any lift of an order ℓ in $G = G_0$ to G_1 has order ℓ^2. Therefore all lifts to $G_{\mathrm{ab},k+1}$ have order ℓ^{k+1}. This lifting property, however, does not characterize the characteristic ℓ-Frattini module $M_{G,\ell}$. Even 'small' ℓ-Frattini covers could have this property. Witness $\mathrm{PSL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$.

3.3. The Nielsen classes $\mathrm{Ni}(H_{5,k}, \mathbf{C}_{3^4})$. Now we discuss the data that produces the spaces in the Frattini case when $\ell = 5$ and $G = A_5$.

3.3.1. *$\mathcal{Q}''$ invariant orbits.* The technique we refer to as **H**(arbater)**M**(umford) originated in [**Fr95**, Part III]. Recall the dihedral group D_d of order $2d$ (App. A.1).

DEFINITION 3.6. Suppose G^* is generated by three involutions $\{\alpha_1, \alpha_2, \alpha_3\}$. We say they form a *2-dihedral* group if $G^* = \langle \alpha_1\alpha_2, \alpha_1\alpha_3 \rangle$.

The essential ingredient is that pairwise products generate a group including α_1. Two dihedral subgroups come together at α_1 to generate G^*. There is another group generated by three involutions that properly contains a 2-dihedral.

DEFINITION 3.7. Suppose $G^\dagger$ is generated by three involutions $\{\alpha_1', \alpha_2', \alpha_3'\}$ where $\langle \alpha_1', \alpha_3' \rangle$ is a Klein 4-group and $\langle \alpha_1', \alpha_2', \alpha_3'\alpha_2'\alpha_3' \rangle$ is a 2-dihedral. We call G^* a *Klein-dihedral* group if in addition $G^* = \langle \alpha_1\alpha_2, \alpha_1\alpha_3\alpha_2\alpha_3 \rangle$.

When $\mathcal{Q}''$ fixes elements in a braid orbit, Nielsen classes and reduced Nielsen classes in that orbit are the same. Thm. 3.8 characterizes such H-M braid orbits.

For $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$, we denote its (inner) braid orbit by $O_{\boldsymbol{g}}$. Lem. 2.9 applies to any ℓ Frattini cover, $\psi : H \to G$, with ℓ' conjugacy classes, $\mathbf{C}$, in G. It says that over any H-M rep. $\boldsymbol{g}_{\text{H-M}} \in \mathrm{Ni}(G, \mathbf{C})$, there exists another H-M rep. $\boldsymbol{h} \in \mathrm{Ni}(H, \mathbf{C})$.

Write $\boldsymbol{g}_{\text{H-M}}$ as $(g_1, g_1^{-1}, g_2, g_2^{-1})$. It is automatic that if $\boldsymbol{g}_{\text{H-M}}$ is $\mathcal{Q}''$ invariant, then the collection $\{g_1, g_1^{-1}, g_2, g_2^{-1}\}$ consists of conjugate elements. Denote their common orders by d. We always assume G is not cyclic.

THEOREM 3.8. *If $q' \in \mathcal{Q}'' \setminus \{1\}$ fixes $\boldsymbol{\sigma} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$, then $q^{-1}q'q$ is in $\mathcal{Q}'' \setminus \{1\}$, and it fixes $(\boldsymbol{\sigma})q$. Therefore, invariance by $\mathcal{Q}''$ is a braid invariant. Condition* (3.4) *characterizes invariance of $\boldsymbol{\sigma}_{\text{H-M}}$ under two particular elements of $\mathcal{Q}''$.*

(3.4a) $\mathbf{sh}^2$ *invariance: For some involution σ', $\sigma_2 = \sigma'\sigma_1(\sigma')^{-1}$.*

(3.4b) $q_1q_3^{-1}$ *invariance: For some involution $\sigma'' \in G$, $\langle \sigma'', \sigma_i \rangle$, $i = 1, 2$, are dihedral groups; or (degenerate case) $\sigma_i = \sigma_i^{-1}$, $i = 1, 2$.*

Then, $\mathcal{Q}''$ invariance of $O_{\boldsymbol{\sigma}_{\text{H-M}}}$ is equivalent to both (3.4a) *and* (3.4b) *holding. In turn, that is equivalent to the following:*

(3.5) *$\langle \sigma'', \sigma', \beta \rangle$ is a Klein-dihedral with $\sigma_1 = \sigma'\beta$ and $\sigma_2 = \sigma'\sigma''\beta\sigma''$; or (degenerate case) σ_1 and σ_2 are conjugate involutions.*

If $\ell \neq 2$, then $\mathcal{Q}''$ fixes an H-M *rep. in* $\mathrm{Ni}(H, \mathbf{C})^{\mathrm{in}}$ *over $\boldsymbol{g}_{\text{H-M}}$.*

PROOF. Consider $(\boldsymbol{g})q \in O_{\boldsymbol{g}}$, and $q' \in \mathcal{Q}''$. Suppose $\boldsymbol{g}$ is invariant under $\mathcal{Q}''$. Since $\mathcal{Q}''$ is a normal subgroup of H_4 [**BFr02**, (2.11b)], then $qq'q^{-1} \in \mathcal{Q}''$. So,

$$((\boldsymbol{g})q)q' = ((((\boldsymbol{g})q)q')q^{-1})q = (\boldsymbol{g})q.$$

That is, invariance under $\mathcal{Q}''$ is a braid invariant.

By assumption $\mathbf{sh}^2$ and $q_1q_3^{-1}$ respectively take $\boldsymbol{g}_{\text{H-M}}$ to $\boldsymbol{g}' = (g_2, g_2^{-1}, g_1, g_1^{-1})$ and $\boldsymbol{g}'' = (g_1^1, g_1, g_2^{-1}, g_2)$ respectively. That Q'' is trivial on $\boldsymbol{g}_{\text{H-M}}$ means there are respective $g', g'' \in G$ with these properties.

(3.6a) g' conjugates g_1 to g_2 and g_2 to g_1.

(3.6b) g'' conjugates g_1 to g_1^{-1} and g_2 to g_2^{-1}.

That is, $\mathcal{Q}''$ induces a regular Klein 4-group action on the following 4 pairs $\{(g_1, g_2), (g_1^{-1}, g_2^{-1}), (g_2, g_1), (g_2^{-1}, g_1^{-1})\}$ through a homomorphism into G. Then, g' and g'' play the roles of the elements in (3.4). Denote the image of $\mathcal{Q}''$ by K.

Since ψ is an $2'$-cover, we can lift K isomorphically to $K' \le \psi^{-1}(K)$. All such lifts are conjugate in $\psi^{-1}(K)$. Denote the respective lifts of g' and g'' by h' and h''. The group $\langle g', g_1\rangle$ is the dihedral group D_d of order $2d$. Since $\ell \neq 2$, by Schur-Zassenhaus we can lift this group to $D_d' = \langle h^*, h_1\rangle \le H$. where h^* is conjugate to h' by an element of $\text{Ker}(\psi)$. Therefore we can conjugate D_d^* to assume $h^* = h'$.

Now pick h_2 to be $h'h_1(h')^{-1}$. To see that h_2 is appropriate, we only have to check that that $h''h_2(h'')^{-1} = h_2^{-1}$. This follows since h'' commutes with h'.

For our special case, when $G = A_5$, take $g_1 = (1\,2\,3)$, and $g_2 = (1\,4\,5)$. Then, we can take $g' = (2\,4)(3\,5)$ and $g'' = (2\,3)(4\,5)$. That completes the proof. □

Recall, $G_{\ell,\text{ab},k}(G)$ is the kth abelianized characteristic ℓ-Frattini cover of G.

COROLLARY 3.9. *All elements in* H-M *braid orbits in* $\text{Ni}(G_{5,\text{ab},k}(A_5), \mathbf{C}_{3^4})^{\text{in}}$ *(and so in* $\text{Ni}(\text{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4})$*), $k \ge 0$, are $\mathcal{Q}''$ invariant.*

Above an H-M *rep. in* $\text{Ni}(\text{PSL}_2(\mathbb{Z}/5^{k+1}, \mathbf{C}_{3^4})$ *there are 5 inner classes of* H-M *reps. in* $\text{Ni}(\text{PSL}_2(\mathbb{Z}/5^{k+2}, \mathbf{C}_{3^4})$.

PROOF. Use the characterization (and notation) of $\mathcal{Q}''$ invariance on H-M reps. from Thm. 3.8. Consider the $\mathcal{Q}''$ invariant H-M rep. $\boldsymbol{h}_{\text{H-M}} = (h_1, h_1^{-1}, h_2, h_2^{-1})$ with $h_2 = h'h_1h'$. A list of all the H-M reps. lying over $\boldsymbol{g}_{\text{H-M}}$ is given by replacing the given h_2 by mh_2m^{-1} with $m \in M_{A_5,\text{ab},5^k}$. There is, however, a precise characterization of the conclusion.

Consider the subgroup $K_{h'} \le M_{A_5,\text{ab},5^k}$ consisting of those k' that centralize h'. Similarly, consider the subgroup $K_{h_1} \le M_{A_5,\text{ab},5^k}$ of those k_1 that centralize h_1. Notice that $k_{h_1}h'k_{h_1}^{-1}$ conjugates $k_{h_1}k_{h'}h''h_1h''k_{h'}^{-1}k_{h_1}^{-1}$ to its inverse.

So, we conclude if and only if $K_{h'}$ and K_{h_1} generate $M_{A_5,\text{ab},5^k}$, which we now establish. As in the Thm. 3.8 proof, this easily reverts to an induction on k, which comes to the case $k = 1$. It is therefore a statement about $\mathbb{Z}/\ell[A_5]$ modules.

Prop. 2.4 notes that $M_{A_5,\text{ab},5}$ is an Ad_5 by Ad_5 extension. Since $\ell \neq 2$, the actions of h_1 and h' (the same as the respective actions of g_1 and g') on $M_{A_5,\text{ab},5}$ are completely reducible. This reduces the conclusion to considering the respective analog groups $K_{g'}^*$ and $K_{g_1}^*$ on Ad_5. Check that there is no common centralizer to $g_1 = (1\,2\,3)$ and $g' = (2\,3)(4\,5)$. Also, the centralizer, Cen_{g_1}, of the former has dimension 1, and the latter dimension 2, as prior to Prop. 2.4.

You get the 5 H-M reps. of distinct classes above $\boldsymbol{g}_{\text{H-M}}$ from conjugating h'' by elements of Cen_{g_1}. As with the other parts of the argument this works for all values of k, concluding the proof. □

REMARK 3.10. For $\ell = 2$, and $G_{2,k}(A_5)$ the characteristic kth 2-Frattini cover of A_5, then $\mathcal{Q}''$ orbits on $\text{Ni}(G_{2,k}(A_5), \mathbf{C}_{3^4})$, $k \ge 1$, all have length 4 [**BFr02**, Lem. 7.5]. For $k = 0$, of course, it is the same space as for $\ell = 5$, length 1.

3.3.2. H-M *reps. in* $\mathrm{Ni}(\mathrm{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4})^{\mathrm{in,rd}}$. Our goal is Prop. 3.13: there is one braid orbit on $\mathrm{Ni}(\mathrm{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4})^{\mathrm{in,rd}}$. The following, from [**BFr02**, Lem. 7.1], succinctly states what we need from this holding for $k = 0$.

PROPOSITION 3.11. *The degree 18 cover* $\bar{\mathcal{H}}(A_5, \mathbf{C}_{3^4})^{\mathrm{in,rd}} \to \mathbb{P}^1_j$ *has monodromy* $(\mathbb{Z}/2)^9 \times^s A_9$*, the wreath product of* $\mathbb{Z}/2$ *and* A_9*. There were no elliptic fixed points:* γ_0 *and* γ_1 *have no fixed points. The genus* $\mathbf{g}_0$ *of* $\bar{\mathcal{H}}(A_5, \mathbf{C}_{3^4})^{\mathrm{in,rd}}$ *is 0.*

COMMENTS. The map

$$\bar{\mathcal{H}}(\mathrm{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4})^{\mathrm{in,rd}} \to \mathbb{P}^1_j$$

factors through $\bar{\mathcal{H}}(A_5, \mathbf{C}_{3^4})^{\mathrm{in,rd}}$. On the latter there are 2 cusps of each of the widths 5 and 3, and one of width 2. The width 5 cusps are H-M, and the 2 elements in the width 2 cusp are the shifts of the two inner H-M representatives. So, computing the genus of the space is a good exercise in using (3.3).

Here the inner Hurwitz space covers the absolute space by a degree 2 map, a special case of the main Theorem in [**FrV91**, §2.1]. The natural outer automorphism of A_n comes from S_n conjugating on it [**BFr02**, Exmp. 3.4]. The only extra ingredient is that you can braid that outer automorphism (§2.2.2). [**BFr02**, Exmp. 3.6] shows how we can effectively identify the real points on these Hurwitz spaces, also in terms of branch cycles. □

We use notation like that of §3.3.1. Start with an H-M rep.

$$\boldsymbol{h}_{\text{H-M}} = (h_1, (h_1)^{-1}, h_2, (h_2)^{-1}) \in \mathrm{Ni}(\mathrm{PSL}_2(\mathbb{Z}/5^{k+1}), \mathbf{C}_{3^4}) = \mathrm{Ni}_{k+1},$$

lying over H-M rep. $\boldsymbol{g}_{\text{H-M}} = (g_1, (g_1)^{-1}, g_2, (g_2)^{-1}) \in \mathrm{Ni}_k$ at level k. With no loss all elements lying above $\boldsymbol{g}_{\text{H-M}}$ have h_1 in the 1st slot. From Cor. 3.9, the full set of H-M elements have the Klein-dihedral situation with $h_2 = h'' h_1 h''$, with h'' one of 5 involutions that commute with an involution h' that conjugates h_1 to h_1^{-1}.

Lem. 3.12 includes a simpler, but less precise way to say the paragraph above.

LEMMA 3.12. *Suppose* $\boldsymbol{g}_{\text{H-M}}$ *is an* H-M *rep. at level* k*, and* (h_1, h_2) *are fixed lifts of* g_1, g_2*. Then, the* H-M *reps. above it at level* $k{+}1$ *are*

$$_A\boldsymbol{h}_{\text{H-M}} \stackrel{\text{def}}{=} (h_1, h_1^{-1}, Ah_2A^{-1}, Ah_2^{-1}A^{-1}),$$

with A *running over the 5 elements of* $\mathrm{Ad}_5/\mathrm{Cen}_{h_1}\mathrm{Cen}_{h_2}$*. That gives at least 25 elements over* $\boldsymbol{g}_{\text{H-M}}$ *at level* $k{+}1$*: 5 for each* $_A\boldsymbol{h}_{\text{H-M}}$ *under the orbit of* $q_2^{5^{k+1}}$*.*

PROOF. Prop. 2.10 tells us how to compute the width of the cusp orbit of an element $\boldsymbol{g} = (g_1, g_2, g_3, g_4) \in \mathrm{Ni}(G, \mathbf{C})$ in terms of the q_2^2 orbit length

$$o_{\boldsymbol{g}} \stackrel{\text{def}}{=} \mathrm{ord}(g_2 \cdot g_3)/|\langle g_2 \cdot g_3\rangle \cup \mathrm{Cen}(g_2, g_3)|.$$

The q_2 orbit has length $2o_{\boldsymbol{g}}$ unless $o_{\boldsymbol{g}}$ is odd, and $(g_2g_1)^{(o_{\boldsymbol{g}}-1)/2}g_2$ has order 2. Since our groups have odd order, the second condition doesn't hold.

The middle product of the level 0 element below $\boldsymbol{g}_{\text{H-M}}$ is 5. From Prop. 2.5, the order of any lift of any element of order 5 goes up by a multiple of 5 for each rise in level. So, $\mathbf{mp}(\boldsymbol{g}_{\text{H-M}}) = 5^{k+1}$. Apply (2.3a) for the result. □

For inner reps. of anything over $\boldsymbol{g}_{\text{H-M}}$, conjugate each of $(h_1)^{-1}, h_2, (h_2)^{-1}$, respectively, by A_2, A_3, A_4 in Ad_5. Denote the result by $\boldsymbol{h}_{\text{H-M},\mathbf{A}}$. Prop. 3.13 finishes the description of all $\boldsymbol{h}_{\text{H-M},\mathbf{A}}$ by interpreting the product-one condition (1.4b).

Again, take $\boldsymbol{g}_{\text{H-M}}$ at level k an H-M rep. Then, at level $k+1$, From that, with $B_A = (h_1^{-1}Ah_2A^{-1})^{5^{k+1}}$, we have these 5^2 inner representatives over $\boldsymbol{g}_{\text{H-M}}$:

$$ {}_{A,B_A^j}\boldsymbol{h}_{\text{H-M}} \stackrel{\text{def}}{=} (h_1, B_A^j h_1^{-1} B_A^{-j}, B_A^j h_2 B_A^{-j}, Ah_2^{-1}A^{-1}), j = 0, \dots, 4. \tag{3.7}$$

Prop. 3.13 is one case where the induction on k is not reducible to ℓ' statements that become independent of k.

Proposition 3.13. *The list of* (3.7) *consists of representatives of all the distinct elements of* $\text{Ni}(\text{PSL}_2(\mathbb{Z}/5^{k+1}, \mathbf{C}_{3^4})$ *lying above* $\boldsymbol{g}_{\text{H-M}}$. *Therefore, there is a one braid orbit on this Nielsen class.*

Proof. Lem. 3.12 shows A is anything in $\text{Ker}(\text{PSL}_2(\mathbb{Z}/5^{k+1}) \to \text{PSL}_2(\mathbb{Z}/5^k))$. So, with no loss for the 1st sentence, replace Ah_2A^{-1} by h_2. Simplify by designating the 2nd and 3rd entries of ${}_{A,B_A^j}\boldsymbol{h}_{\text{H-M}}$ by u_2 and u_3, order 3 generators of $\text{PSL}_2(\mathbb{Z}/5^{k+1})$ lying, respectively, over $g_2, g_3 \in \text{PSL}_2(\mathbb{Z}/5^k)$. We must prove this:

(3.8) the only possible such (u_2, u_3) with product equal to $h_1^{-1}h_2 = h^*$ are the conjugates of the pair (h_1^{-1}, h_2) by the powers of $(h^*)^{5^k}$.

For our notation it simplifies to refer to (h_1^{-1}, h_2) as (u_1', u_2'). Since we are in $\text{PSL}_2(\mathbb{Z}/5^{k+1})$, we know there is just one conjugacy class of elements of order 5^{k+1} represented by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, we can take this to be h^*. So, the conclusion follows from this computation.

For (C_1, C_2), a pair in Ad_5 (identify with $\text{Ker}(\text{PSL}_2(\mathbb{Z}/5^{k+1}) \to \text{PSL}_2(\mathbb{Z}/5^{k+1}))$, assume $(C_1u_1'C_1^{-1}, C_2u_1'C_2^{-1})$ is an allowable (u_1, u_2). Then, with no loss (adjust by the centralizers of C_1, C_2), we may assume $C_1 = C_2$. Therefore C_1 centralizes h^*. But, the only centralizer of h^* is a power of h^*, and the result follows.

We induct on k to show there is just one braid orbit on $\text{Ni}(\text{PSL}_2(\mathbb{Z}/5^{k+1}, \mathbf{C}_{3^4})$. Assume there is one braid orbit at level k. It suffices to show that one braid orbit contains all the inner classes above any fixed level k element. Our choice of level k element is $\boldsymbol{g}_{\text{H-M}}$. We are done if the elements of (3.7) are contained in one orbit.

Application of q_1^2 to the 5 H-M reps over $\boldsymbol{g}_{\text{H-M}}$ leaves each of them invariant. We, however, get four 5-cycles applied to the remaining 20 elements in (3.7). For each fixed $j \neq 0 \mod 5^{k+1}$ the following happens. The product of the 1st two entries $h_1, B_A^j h_1^{-1} B_A^{-j}$ has order 5. Then, as with the above general application of q_2^2, q_1^2 conjugates the 1st two elements by that order 5 element in Ad_5.

So, the application of powers of q_1^2 to $\boldsymbol{g}_{\text{H-M},B_A^j}$ for $j \neq 0$ is an inner orbit of length five, joining each fixed cusp orbit with A fixed. That concludes the proposition. □

3.3.3. *Genus computation.* The genus of $\bar{\mathcal{H}}(\text{PSL}_2(\mathbb{Z}/5), \mathbf{C}_{3^4})^{\text{in,rd}}$ is 0 (Prop. 3.11). We can calculate the genus, $\mathbf{g}_k$, of $\bar{\mathcal{H}}(\text{PSL}_2(\mathbb{Z}/5^k), \mathbf{C}_{3^4})^{\text{in,rd}}$ from Riemann-Hurwitz for all k. Prop. 3.14 does that explicitly for $k = 1$.

Proposition 3.14. *For the degree* $18 \cdot 25$ *cover* $\bar{\mathcal{H}}(\text{PSL}_2(\mathbb{Z}/5^2), \mathbf{C}_{3^4}) \to \mathbb{P}^1_j$ *here is the count of the cycles in of* $\gamma_0, \gamma_1, \gamma_\infty$ *in* (3.3).

(3.9)
γ_0 *has 225 2-cycles, and* γ_1 *has 150 3-cycles .*
γ_∞ *has five 2-cycles and four 10-cycles,*
ten 3-cycles and eight 15-cycles, and ten 25-cycles.

From this the indices are respectively:

$$\begin{array}{ll} \text{ind}(\gamma_0): & 225\cdot(2-1) \qquad \text{ind}(\gamma_1): 150\cdot(3-1) \\ \text{ind}(\gamma_\infty): & 5\cdot(2-1)+4\cdot(10-1)+10\cdot(3-1)+8\cdot(15-1)+10\cdot(25-1) \end{array} \tag{3.10}$$

The genus of the compactified level 1 space $\bar{\mathcal{H}}(\mathrm{PSL}_2(\mathbb{Z}/5^2), \mathbf{C}_{3^4})$ *is then* $\mathbf{g}_1$ *in*

$$2(450+\mathbf{g}_1-1) = 225 + 2\cdot 150 + 413 \text{ or } \mathbf{g}_1 = 20.$$

Proof. Since γ_0 and γ_1 have no fixed points on the level 0 Nielsen class, they will have none at any higher level, so the degree of the cover determines the number of cycles in the order 2 (resp. order 3) element γ_0 (resp. γ_1). Once we have computed the index of γ_∞, everything follows from (3.3), and we do that by computing the relative orders of ramification of points at level 1 over their images at level 0.

There is one point at level 0 with ramification index 2 over $j=\infty$, two each with index 3 and index 5. Points above each have relative ramification either 1 (relatively unramified) or 5. So we have only to count respective points at level 1 with no new ramification or index 5 relative ramification over each x_0 over $j=\infty$ of respective ramification index 2, 3 and 5.

If x_0 has index 5 over $j=\infty$, since $\ell=5$ Prop. 2.5 (as in the proof of Lem. 3.12) shows the relative index of each point above it is 5. That gives five points over x_0 at level 1 with ramification index 25 over $j=\infty$.

We review why we've already handled x_0 ramified over ∞ of index $e=2$. The level 0 cusp is the γ_∞ orbit of the shift of an H-M rep. It is, according to Lem. 2.9, the image of the shift, $\boldsymbol{h} = (h_1^{-1}, h_2, h_2^{-1}, h_1)$, of an H-M rep. at level 1. There are five total such shifts of H-M reps. at level 1 lying over x_0. Cor. 3.9 says we can take for their Nielsen class representatives $\boldsymbol{h}_A = (h_1^{-1}, Ah_2A^{-1}, Ah_2^{-1}A^{-1}, h_1)$ with A running over the 5 elements of $\mathrm{Ad}_5/\mathrm{Cen}_{h_1}\mathrm{Cen}_{h_2}$.

As in Prop. 3.13 we get four q_2 orbits giving cusps of width 10 corresponding to B_As in (3.7) that are nontrivial. Now we adjust this to do the case $e=3$. It isn't hard to write out the level 0 Nielsen class, but to be explicit, we quote from [**Fr99**, §7.4 Fig. 1] (resp. [**Fr99**, §7.9 Fig. 2]) for the absolute (resp. inner) case. One γ_∞ orbit on $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\text{in}}$ is represented by $X_7 = ((2\,1\,4), (2\,4\,5), (5\,3\,2), (1\,2\,3))$, the other by conjugation by $(3\,5)$.

So, as in the previous case, we want to lift X_7 to a $\boldsymbol{h}$ at level 1. We do so using that $\langle (2\,4\,5), (5\,3\,2)\rangle$ and $\langle (1\,2\,3), (2\,1\,4)\rangle$ are $5'$ groups (order prime to 5), actually isomorphic to A_4. That is, the cusp defined by X_7 is a g-5' cusp, so named in [**Fr06**, (3.4a)]. Thus, as a special case of [**Fr06**, Princ. 3.6] (called there Frattini Principle 2) there is a corresponding g-5' lift over it extending to the whole universal 5-Frattini cover, but here we just go to level 1 of our example. Frattini Principle 2 is a far-reaching generalization of Lem. 2.9.

Now we can generalize the work of $e=2$ by taking as A a generator of the submodule of Ad_5 fixed by the product of $(1\,2\,3)$ and $(2\,1\,4)$ and for B_A the same expression used in (3.7). That completes the proof. □

4. Properties of split case spaces in (1.2b)

We use the name "split" on situation (1.2b). Still, it is ℓ-Frattini principles that dominate. Unless otherwise said, we exclude $\ell=3$.

Further notation: $V_{\ell^{k+1}} \stackrel{\text{def}}{=} (\mathbb{Z}/\ell^{k+1})^2$. We use an element, α, of order 3 to act on a number of groups. On $V_{\ell^{k+1}}$ its action is through the matrix $A^* = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$.

That action extends to the free group $F_2 = \langle u_1^*, u_2^* \rangle$ on two generators by

$$\alpha^* : (u_1^*, u_2^*) \mapsto ((u_2^*)^{-1}, u_1^*(u_2^*)^{-1}) \text{ [Fr95, end of Rem. 2.10].} \tag{4.1}$$

That induces an action on the profinite completion of F_2, which we denote by $\hat{F}_2$.

Define the semidirect product of $F_2 \times^s \mathbb{Z}/3$, and $\hat{F}_2 \times^s \mathbb{Z}/3$ by taking $\mathbb{Z}/3 = \langle \alpha^* \rangle$. Use the 2×2 matrix notation of §A.1. For any α^*-invariant quotient, H, of $\hat{F}_2$, with α induced from α^*, write elements of $H \times^s \mathbb{Z}/3$ as $\left(\begin{smallmatrix} \alpha^j & 0 \\ h & 1 \end{smallmatrix}\right)$, $h \in H$, $j \in \mathbb{Z}/3$. With the induced action from α^*, denote $V_{\ell^{k+1}} \times^s \mathbb{Z}/3$ by $G_{\ell^{k+1}}$.

§4.1 has preliminaries on the Nielsen classes, $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$, of the rest of this paper. §4.2 introduces the (small) Heisenberg group and the *lift invariant* that allows us to label braid orbits on these Nielsen classes.

§4.3 gives the 1st of our main theorems (Prop. 4.19). With it we compute the value of the lift invariant and its relation to the respective Nielsen class representatives we call *double identity* and H-M(as in (1.3)). These correspond to braid orbits with the following lift invariant values:

(4.2) either ℓ' (prime to ℓ) or trivial lift invariant.

Braid orbits for these cases, $\ell > 3$ and all k, exhibit disparate and interesting phenomena. The types of cusps in these two cases are similar to the cusps of main concentration on modular curves, though modular curves have trivial lift invariant. §7.1 comments on the remaining – intermediary – cases of ℓ-divisible lift invariant (Def. 4.16) for each fixed $\ell \neq 3$, and for each value of $k \geq 0$. The case $\ell = 2$ has some special properties. We use it to show how the lift invariant works in §4.3.2 for $k = 0$, and then finish it for $k > 0$ in §7.2.

4.1. Preliminaries on $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$. Define $\alpha_0 = \left(\begin{smallmatrix} \alpha & 0 \\ \mathbf{0} & 1 \end{smallmatrix}\right)$ to be the natural lift of of α to $G_{\ell^{k+1}}$. The conjugacy class of α_0 is

$$\{\left(\begin{smallmatrix} 1 & 0 \\ \boldsymbol{v} & 1 \end{smallmatrix}\right)\alpha_0\left(\begin{smallmatrix} 1 & 0 \\ -\boldsymbol{v} & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{v}^\alpha - \boldsymbol{v} & 1 \end{smallmatrix}\right) \stackrel{\text{def}}{=} {}_{\boldsymbol{v}}\alpha_0 \mid \boldsymbol{v} \in V_{\ell^{k+1}}\}. \tag{4.3}$$

Replacing α by α^{-1} in this expression gives the inverse, ${}_{\boldsymbol{v}}\alpha_0^{-1}$, of ${}_{\boldsymbol{v}}\alpha_0$.

For $\boldsymbol{g} \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ we indicate a *configuration type* by whether – in order – it is α or α^{-1} that lies in its (upper left) matrix entry. Example: For $\boldsymbol{g}_{\text{H-M}}$ in the proof of Prop. 4.19, the configuration type is $\pm\pm$. Write this as $\boldsymbol{g} \in T_{\ell^{k+1},\pm\pm}$, or just $T_{\pm\pm}$ if k is understood, or is 0.

Our main concern is braid orbits, So, we often assume a Nielsen class rep. is of a particular type as a consequence of the following statement.

(4.4) You can braid an inner Nielsen class rep. of one type to any other type and take any fixed entry (often the 1st, g_1) to be either α_0 or α_0^{-1}.

Given an entry of $\boldsymbol{g}$ as α_0, normalize further by conjugating all entries by α_0.

Consider H-M reps. in $T_{\ell^{k+1},\pm\pm}$: ${}_{\boldsymbol{w},3,4}\boldsymbol{g} = (\alpha_0, \alpha_0^{-1}, {}_{\boldsymbol{w}}\alpha_0, {}_{\boldsymbol{w}}\alpha_0^{-1})$. Note: ${}_{\boldsymbol{w},3.4}\boldsymbol{g}$ and ${}_{-\boldsymbol{w},3,4}\boldsymbol{g}$ are reduced equivalent.

LEMMA 4.1. *Since $G_{\ell^{k+1}} \to G_\ell$ is a Frattini cover, $\boldsymbol{v} \in V_{\ell^{k+1}}$ generates $G_{\ell^{k+1}}$ as an α module if and only if $\boldsymbol{v} \mod \ell$ generates G_ℓ as an α module.*

To count the reduced classes of H-M *reps, count the $\boldsymbol{v} \mod \ell$ that generate G_ℓ as an α module, multiply by ℓ^{2k}, and divide by 6. For $\ell \equiv 2 \mod 3$, α acts irreducibly on V_ℓ. Otherwise V_ℓ is a sum of two 1-dimensional α-eigenspaces, with distinct eigenvalues, both different from 1.*

For $\boldsymbol{v} \in V_{\ell^{k+1}}$, $\boldsymbol{v}$ and $\boldsymbol{v}^\alpha - \boldsymbol{v} \bmod \ell$ are both α eigenvectors or neither is.

(4.5) *In the 2nd case $\left(\begin{smallmatrix} \alpha & 0 \\ \mathbf{0} & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{v}^\alpha - \boldsymbol{v} & 1 \end{smallmatrix}\right)$ generate G_ℓ.*

All elements in $G_{\ell^{k+1}}$ of form $\left(\begin{smallmatrix} \alpha^{\pm 1} & 0 \\ \boldsymbol{w} & 1 \end{smallmatrix}\right)$ have order 3.

Given $g_1 = \alpha_0$, $g_2 = \left(\begin{smallmatrix} \alpha^{-1} & 0 \\ \boldsymbol{v}_2^{\alpha^{-1}} - \boldsymbol{v}_2 & 1 \end{smallmatrix}\right)$ and $g_3 = \left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{v}_3^{\alpha} - \boldsymbol{v}_3 & 1 \end{smallmatrix}\right)$, there is

$$\boldsymbol{g} = (\alpha_0, g_2, g_3, g_4) \in T_{\pm\pm} \cap \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2}) \tag{4.6}$$

for (a unique) $g_4 = \left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{v}_4^{\alpha} - \boldsymbol{v}_4 & 1 \end{smallmatrix}\right)$ if and only if $\langle \boldsymbol{v}_2 \bmod \ell, \boldsymbol{v}_3 \bmod \ell, \alpha_0 \rangle = G_\ell$. That is, $\boldsymbol{v}_2 \bmod \ell$ and $\boldsymbol{v}_3 \bmod \ell$ are not in the same α_0 eigenspace.

Proof. Take $\mathcal{O}_K$ to be the ring of integers of the number field generated by a zero of $x^2 + x + 1$, and ζ_3 to be a primitive 3rd root of 1. The group $(\mathbb{Z})^2 \times^s \mathbb{Z}/3$ is isomorphic to $\mathcal{O}_K \times^s \langle \zeta_3 \rangle$ where multiplication by ζ_3 takes the role of α. The 1st sentence of the 2nd paragraph follows from the 1st paragraph.

The 2nd sentence comes to checking primes ℓ for which $x^2 + x + 1 \equiv 0 \mod \ell$, or $x^3 - 1 \equiv 0 \mod \ell$, has a solution (not equal to 1). The cyclic group $(\mathbb{Z}/\ell)^*$ contains a nontrivial root of 1 if and only if 3 divides $\ell - 1$.

For $\ell \equiv 2 \mod 3$, any $\boldsymbol{v} \neq \mathbf{0}$ gives $\boldsymbol{v}^\alpha - \boldsymbol{v}$ generating $(\mathbb{Z}/\ell)^2$ as an $\langle \alpha \rangle$ module. So, V_ℓ is a cyclic module for this action: some vector generates this $\mathbb{Z}/3$ module.

Now assume $\ell \equiv 1 \mod 3$ and suppose $\boldsymbol{v}_i$, $i = 1, 2$, are respective generators of α-eigenspaces, with respective eigenvalues k_1, k_2. With $\boldsymbol{v} = a_1\boldsymbol{v}_1 + a_2\boldsymbol{v}_2$,

$$\boldsymbol{w} = \boldsymbol{v}^\alpha - \boldsymbol{v} = a_1(k_1 - 1)\boldsymbol{v}_1 + a_2(k_2 - 1)\boldsymbol{v}_2.$$

Since $k_1 \neq k_2$ (and not 1), either of $\boldsymbol{v}$ and $\boldsymbol{w}$ are α-eigenvectors if and only if one a_i is 0 (and the other is not). Then, they are simultaneously eigenvectors in the same subspace. Conclude: $\langle \boldsymbol{v}^\alpha - \boldsymbol{v}, \alpha \rangle = \langle \boldsymbol{v}, \alpha \rangle = G_\ell$ if both a_is are nonzero. This is clearly equivalent to the statement centered on (4.5).

Finally, consider $\left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{v} & 1 \end{smallmatrix}\right)$. It has order 3 if and only if $\boldsymbol{v} + \boldsymbol{v}^\alpha + \boldsymbol{v}^{\alpha^2} = \mathbf{0}$. This says that every nontrivial vector is killed by the characteristic polynomial of α. The remainder of the lemma follows because the condition on g_2 and g_3 is just generation for $\boldsymbol{g}$. Now, determine g_4 from the product-one condition for all k.

For $\ell \equiv 1 \mod 3$, as zeros of $x^2 + x + 1 \mod \ell$ are distinct, they lift to zeros of $x^2 + x + 1$ in $\mathbb{Z}_\ell$. So, the corresponding eigen-modules generate $O_K \otimes \mathbb{Z}_\ell$. The characteristic polynomial for α is now $x^2 + x + 1$. □

Definition 4.2. Refer to $\boldsymbol{v} \in V_{\ell^{k+1}}$ as an α-generator if it satisfies 1st paragraph condition of Lem. 4.1.

4.2. Appearance of a Heisenberg group. We still exclude $\ell = 3$. Here we identify the Universal central ℓ-extension, $R_{\ell^{k+1}}$, of $G_{\ell^{k+1}}$. There is a startling difference between $\ell = 2$ and $\ell > 3$, though $\ell = 2$ braid orbits resemble those for the other cases. For $\ell = 2$, and $k = 0$, R_2 is the pullback of $A_4 \leq A_5$ in $\mathrm{SL}_2(\mathbb{Z}/5)$, via the identification of $\mathrm{PSL}_2(\mathbb{Z}/5)$ and A_5. In this pullback the lift of any nontrivial element in V_2 to $\mathrm{SL}_2(\mathbb{Z}/5)$ has order 4.

For $\ell \geq 3$ and each k, the lift of any element of order ℓ^{k+1} in $V_{\ell^{k+1}}$ to $R_{\ell^{k+1}}$ has order ℓ^{k+1}. §4.2.1 shows both cases come from a *Heisenberg extension*.

4.2.1. *Heisenberg central extension.* In the proof of Lem. 3.4 we have the matrix $A = \left(\begin{smallmatrix} 1 & -3 \\ 1 & -2 \end{smallmatrix}\right)$, giving an element of order 3 in $\mathrm{PSL}_2(\mathbb{Z})$. That gives a copy of the Klein 4-group in A_5 generated by $\boldsymbol{v}_1 = \left(\begin{smallmatrix} 2 & 0 \\ 0 & 3 \end{smallmatrix}\right)$ and $\boldsymbol{v}_2 = \left(\begin{smallmatrix} 0 & 2 \\ 2 & 0 \end{smallmatrix}\right)$.

Reduce A mod 5. Then, $\langle A, \boldsymbol{v}_1, \boldsymbol{v}_2\rangle$ gives a natural copy of A_4 inside $\mathrm{PSL}_2(\mathbb{Z}/5)$ as $V_2 \times^s \mathbb{Z}/3$ with $(\mathbb{Z}/2)^2 = V_2 = \{\boldsymbol{v}_1, \boldsymbol{v}_2\}$ and A generates $\mathbb{Z}/3$ acting on V_2 by matrix conjugation: it takes $\boldsymbol{v}_1$ to $\boldsymbol{v}_2$ and $\boldsymbol{v}_2$ to the sum of $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$. The matrix A is useful, but we use its conjugate, $A^* = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$, induced from (4.1).

Consider the matrix

$$M(x,y,z) \stackrel{\text{def}}{=} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, \text{ with inverse } \begin{pmatrix} 1 & -x & xy-z \\ 0 & 1 & -y \\ 0 & 0 & 1 \end{pmatrix}.$$

For R a commutative ring, we use the 3×3 *Heisenberg group* with entries in R:

$$\mathbb{H}_R = \{M(x,y,z)\}_{x,y,z \in R}.$$

When $R = \mathbb{Z}/\ell^{k+1}$, denote $\mathbb{H}_R$ by $\mathbb{H}_{\ell^{k+1}}$, and its 3×3 identity matrix by I_3. We now relate $\mathbb{H}_{\ell^{k+1}}$ to $G_{\ell^{k+1}}$ after pointing to a potential notation confusion.

§2.1 denotes the 1st characteristic ℓ-Frattini cover of a group designated G_0 by G_1. Since we will be dealing with infinitely values ℓ, it simplies notation to refer the groups corresponding to $k = 0$ as $G_\ell = V_\ell \times^s \mathbb{Z}/3$, without a decoration – like $G_{0,\ell}$ – including a 0 subscript. See the comments in the proof of Prop. 2.5.

Cor. B.3 describes the universal central ℓ-extension of G_ℓ^{k+1}. For each prime ℓ, V_ℓ has just two non-abelian central ℓ-Frattini extensions (say, [**Fr02**, §4.2]):

(4.7a) for $\ell = 2$: the order 8 quaternion, Q_8, and dihedral, D_4, groups; and

(4.7b) for ℓ odd: $\mathbb{H}_\ell$ and $\mathbb{Z}/\ell^2 \times^s \mathbb{Z}/\ell$ (a generator of the right copy of $\mathbb{Z}/\ell$ acts as multiplication by $1+\ell$).

As in §B.1, each group in (4.7) is an ℓ-representation cover of V_ℓ. More than one is possible because V_ℓ is not ℓ-perfect. For the ℓ-perfect G_ℓ, however, we figure its universal ℓ-central – Frattini – extension by identifying the restriction of the unique ℓ representation cover, $\psi : R \to G_\ell$, to an ℓ-Sylow.

For that we identify, for H in (4.7), when α extends from V_ℓ to $\psi_H : H \to V_\ell$. Consider the homomorphism $\psi_{\ell^{k+1}} : \mathbb{H}_{\ell^{k+1}} \to V_{\ell^{k+1}}$, by $M(x,y,z) \mapsto (x,y)$, $k \geq 0$.

LEMMA 4.3. *Any lift to $\mathbb{H}_{\ell^{k+1}}$ of an order ℓ^{k+1} element of $V_{\ell^{k+1}}$ has order ℓ^{k+1}, except for $\ell = 2$ and $k = 0$ the order is 4. The groups $\mathbb{H}_2$ and D_4 are isomorphic.*

Each element of $\ker(\psi_{\mathbb{Z}})$ *(or* $\ker(\psi_{\ell^{k+1}})$ *is a commutator (see 4.9). Conclude:*

(4.8a) *$\psi_{\ell^{k+1}}$ is a central ℓ-Frattini extension.*

(4.8b) *$\mathbb{H}_{\mathbb{Z}}$ is a quotient of F_2, and the action of α^* induces $\alpha_{\ell^{k+1}}$ on $\mathbb{H}_{\ell^{k+1}}$, with $\alpha_{\ell^{k+1}}$ trivial on* $\ker(\psi_{\ell^{k+1}})$.

(4.8c) *The same notation gives a cover $\psi_{\ell^{k+1}} : H_{\ell^{k+1}} \to G_{\ell^{k+1}}$ presenting the maximal central extension of $G_{\ell^{k+1}}$ with exponent ℓ^{k+1} kernel.*

(4.8d) *The* (4.1) *action of α on V_ℓ doesn't extend to $\mathbb{Z}/\ell^2 \times^s \mathbb{Z}/\ell$ unless $3|\ell-1$.*

(4.8e) *In case* (4.8d)*, the extending action of α on the kernel of $\mathbb{Z}/\ell^2 \times^s \mathbb{Z}/\ell$ is nontrivial; so it does not give a central extension of $V_\ell \times^s \mathbb{Z}/3$.*

PROOF. Write an element of $\mathbb{H}_{\ell^{k+1}}$ as $I_3 + U(x,y,z)$. Putting it to the ℓ^{k+1}-th power gives I_3 if $\ell^{k+1} \geq 3$. To the 2nd power gives $I_3 + U(x,y,z)^2$ if $\ell^{k+1} = 2$, and

that has xy in the $(1,3)$ position. To see that $\mathbb{H}_2$ is D_4, use the D_4 characterization: it has two noncommuting involutions, $M(1,0,0)$ and $M(0,1,0)$, for generators.

Now consider the statements in (4.8). Let $M(x_1,y_1,z_1)$ and $M(x_2,y_2,z_2)$ be (any) lifts of any generators $\boldsymbol{v}_1,\boldsymbol{v}_2$ of V_ℓ. Consider their commutator:

$$M(x_1,y_1,z_1)M(x_2,y_2,z_2)M(x_1,y_1,z_1)^{-1}M(x_2,y_2,z_2)^{-1} = M(0,0,x_1y_2-x_2y_1). \tag{4.9}$$

That $\ker(\psi)$ (in each case) consists of commutators follows easily.

See §2.1 for this and our next two paragraphs for producing the ℓ-Frattini properties. The kernel of $H_R \to V_R$ is in the center of $\mathbb{H}_R$, for R any quotient of $\mathbb{Z}$. So, the commutator in (4.9) depends only on $\boldsymbol{v}_1,\boldsymbol{v}_2$. Thus,

$$\langle M(x_1,y_1,z_1), M(x_2,y_2,z_2)\rangle = \mathbb{H}_{\mathbb{Z}}.$$

This is a characterization of $\psi_{\mathbb{Z}}$ (and therefore of $\psi_{\ell^{k+1}}$) being a Frattini cover. Therefore $\mathbb{H}_{\mathbb{Z}}$ is generated by 2 elements; so it is a quotient of F_2.

For notational simplicity we do just the case $k=0$, but, the ingredients are the same for general k, given the result of §B.2 (which does the reduction to $k=0$). The universal ℓ-Frattini cover of V_ℓ is the profinite completion, $F_{2,\ell}$, of F_2 with respect to subgroups of index a power of ℓ.

Consider the kernel, $K_\ell^\dagger$, of $\psi_\ell : F_{2,\ell} \to V_\ell$. The following Frattini statements are proved in [**FrJ86**, Chap. 21]. The Frattini subgroup of the kernel of ψ_ℓ – $K_{1,\ell}^\dagger = \langle (K_\ell^\dagger)^\ell, (K_\ell^\dagger, K_\ell^\dagger)\rangle$ – is generated by ℓth powers and commutators in $K_\ell^\dagger$. The universal exponent ℓ-Frattini cover of V_ℓ is $F_{2,\ell}/K_{1,\ell}^\dagger \stackrel{\text{def}}{=} V_{1,\ell} \to V_\ell$.

The α action on F_2 preserves the map to V_ℓ. So, α also acts on $K_\ell^\dagger$, on its characteristic subgroup $K_{1,\ell}^\dagger$, and on the quotient $V_{1,\ell}$ preserving its map to V_ℓ. Therefore, α acts on $M_\ell = \ker(V_{1,\ell} \to V_\ell)$. The maximal central extension of $V_\ell \times^s \mathbb{Z}/3 = G_\ell$ has its kernel to V_ℓ identified with the maximal quotient of M_ℓ on which α acts trivially. According to §B.2, this quotient has dimension 1. That gives the maximal central ℓ-Frattini extension of G_ℓ, with exponent ℓ kernel, as H_ℓ.

Now consider (4.8e). An actual element, say c, affecting α then has order 3 in $(\mathbb{Z}/\ell)^*$. We can write an extension of it to $\mathbb{Z}/\ell^2$ as $c(1+u\ell) \mod \ell^2$ for some value of u. The result of multiplying by this on the kernel has the same affect as multiplication by c on $\mathbb{Z}/\ell$, so it is not trivial. That concludes the proof. □

Corollary 4.4. *For all odd primes $\ell > 3$ (resp. $\ell = 2$), the unique central ℓ-Frattini extension of G_ℓ) is H_ℓ (resp. $Q_8 \times^s \mathbb{Z}/3$). Indeed, Q_8 identifies with the 2-Sylow in the spin cover of A_4.*

Proof. The 1st sentence is in Lem. 4.3. The product of the involutions in D_4 gives a subgroup of order 4, that is normal, and so $D_4 = (\mathbb{Z}/4) \times^s \mathbb{Z}/2$ (with the generator of $\mathbb{Z}/2$ acting as multiplication by -1). In particular, (4.8d) applies to say the action of α in G_2 does not extend to $\mathbb{H}_2$.

That leaves the extension of $\mathbb{Z}/3$ to Q_8 as the only possible 2-Frattini central extension of G_2. See this is right by looking at $\mathrm{Spin}_4 \to A_4$. For any $n \geq 4$, if $g \in A_n$ is an involution, then if it is product of $2s$ 2-cycles. [**BFr02**, Prop. 5.10] says any lift of it to Spin_n has order 4 if and only if s is odd. That is a characterization of Q_8 by its cover to V_2: each order 2 element lifts to only order 4 elements. □

4.2.2. *Heisenberg lift invariant.* Regard $\mathbb{H}_{\ell^{k+1}} \times^s \mathbb{Z}/3 \stackrel{\text{def}}{=} H_{\ell^{k+1}}$ as a cover of $G_{\ell^{k+1}} = V_{\ell^{k+1}} \times^s \mathbb{Z}/3$. The kernel of $\psi_{\ell^{k+1}} : H_{\ell^{k+1}} \to G_{\ell^{k+1}}$ has order prime to 3, so (a trivial case of) Schur-Zassenhaus gives a unique conjugacy class of order 3 elements over such elements in $G_{\ell^{k+1}}$.

As the kernel of $\psi_{\ell^{k+1}}$ is in center, there is a unique order 3 lift of any order 3 element of $G_{\ell^{k+1}}$. For $\boldsymbol{g} = (g_1, g_2, g_3, g_4) \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$, denote the order 3 lift of g_i by $\hat{g}_i \in H_{\ell^{k+1}}$. Then, form

$$s_{\ell^{k+1}}(\boldsymbol{g}) = \hat{g}_1\hat{g}_2\hat{g}_3\hat{g}_4 \in \ker(H_{\ell^{k+1}} \to G_{\ell^{k+1}}) = \mathbb{Z}/\ell^{k+1}. \tag{4.10}$$

Sometimes we use this in *multiplicative notation*, identifying the right side of (4.10) with $\langle \zeta_{\ell^{k+1}} \rangle$, as in (5.16), with $\zeta_n = e^{2\pi \mathrm{i}/n}$. As a special case of a general situation, we call $s_{\ell^{k+1}}(\boldsymbol{g})$ the (Heisenberg) *lift invariant*.

Proposition 4.5 (Braid invariance). *Braids always preserve the lift invariant* [**Fr95**, Part III, Lem. 3.12].

We use both additive (0 is the identity; value in an abelian group) and multiplicative (1 is the identity; inside a nonabelian group) notation for it. We clarify which when we use it. The inverse of A^* is $(A^*)^{-1} = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

(4.11) Denote the order 3 element over $\left(\begin{smallmatrix} \alpha & 0 \\ \boldsymbol{w} & 1 \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} \alpha & 0 \\ M(\boldsymbol{w}, z_{\boldsymbol{w}}) & 1 \end{smallmatrix}\right)$, or with $\boldsymbol{w} = (x, y)$, use $M(x, y, z_{(x,y)})$ for $M(\boldsymbol{w}, z_{\boldsymbol{w}})$.

Conjugation by α_0 preserves order 3 elements. Conclude:

$$\alpha_0^{-1}\left(\begin{smallmatrix} \alpha & 0 \\ M(x,y,z_{(x,y)}) & 1 \end{smallmatrix}\right)\alpha_0 = \left(\begin{smallmatrix} \alpha & 0 \\ M(x,y,z_{(x,y)})^{\alpha} & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \alpha & 0 \\ M(-y,x-y,z_{(-y,x-y)}) & 1 \end{smallmatrix}\right), \tag{4.12}$$

since the element on the right side is the unique order 3 lift of $\left(\begin{smallmatrix} \alpha & 0 \\ (-y,x-y) & 1 \end{smallmatrix}\right)$.

Define $z^*_{(x,y)}$ analogously as the unique z for which $\left(\begin{smallmatrix} \alpha^{-1} & 0 \\ M(x,y,z) & 1 \end{smallmatrix}\right)$ has order 3.

4.2.3. *Relating $z_{(x,y)}$ and $z^*_{(x,y)}$.* Prop. 4.6 lets us compute the lift invariant. Using $z_{(x,y)}$, (4.13) lists – with no repetition – all order 3 elements of $H_{\ell^{k+1}}$.

Imitating the notation of (4.3), the conjugacy class of $\alpha_0^{\pm 1}$ in $H_{\ell^{k+1}}$ is

$$\begin{aligned} \{_{M(x,y,0)}\alpha_0^{\pm 1} \stackrel{\text{def}}{=} & \left(\begin{smallmatrix} 1 & 0 \\ M(x,y,0) & 1 \end{smallmatrix}\right)\alpha_0^{\pm 1}\left(\begin{smallmatrix} 1 & 0 \\ M(-x,-y,xy) & 1 \end{smallmatrix}\right) = \\ & \left(\begin{smallmatrix} \alpha^{\pm 1} & 0 \\ M(x,y,0)^{\alpha^{\pm 1}} M(x,y,0)^{-1} & 1 \end{smallmatrix}\right)\}_{(x,y)\in V_{\ell^{k+1}}}. \end{aligned} \tag{4.13}$$

Proposition 4.6. *Both $\{M(x, y, z_{(x,y)})\}_{(x,y)\in V_{\ell^{k+1}}}$ and $\{M(x, y, z^*_{(x,y)})\}_{(x,y)\in V_{\ell^{k+1}}}$ are invariant under $\alpha^{\pm 1}$. For $(x, y) \in V_{\ell^{k+1}}$, two formulas relate $z_{(x,y)}$ and $z^*_{(x,y)}$:*

(4.14a) $z^*_{(x,y)} = xy - z_{(-x,-y)}$; *and*

(4.14b) $z_{(x,y)} - z^*_{(x,y)} = (x^2 - xy + y^2)/3$.

Proof. The 1st sentence says that conjugation by $\alpha^{\pm 1}$ maps order 3 elements to order 3 elements. From (4.12), the substitution of $M(x, y, z_{(x,y)})^{\alpha}$ for

$M(x,y,z_{(x,y)})$ gives the effect of conjugation by α_0 on $\left(\begin{smallmatrix}\alpha & 0\\ M(x,y,z_{(x,y)}) & 1\end{smallmatrix}\right)$. Similarly, substitute $M(x,y,z^*_{(x,y)})^\alpha = M(-y,x-y,z^*_{(-y,x-y)})$ for $M(x,y,z^*_{(x,y)})$ for conjugation by α_0 on $\left(\begin{smallmatrix}\alpha^{-1} & 0\\ M(x,y,z^*_{(x,y)}) & 1\end{smallmatrix}\right)$.

Consider $B_{x,y} \stackrel{\text{def}}{=} \left(\begin{smallmatrix}\alpha^{-1} & 0\\ M(-x+y,-x,z^*_{(-x+y,-x)}) & 1\end{smallmatrix}\right)$. It and its inverse have order 3. Multiplying on the right by $B^{-1}_{x,y}$ shows $B^{-1}_{x,y}$ lies over $\left(\begin{smallmatrix}\alpha & 0\\ (-x,-y) & 1\end{smallmatrix}\right) \in G_{\ell^{k+1}}$. It must therefore be $\left(\begin{smallmatrix}\alpha & 0\\ M(-x,-y,z_{(-x,-y)}) & 1\end{smallmatrix}\right)$.

Multiply $B_{x,y}B^{-1}_{x,y}$ out to get the identity if and only if

$$M(-x+y,-x,z^*_{(-x+y,-x)})^\alpha M(-x,-y,z_{(-x,-y)}) = I_3.$$

The left term is $M(x,y,z^*_{(x,y)})$. So, its inverse, is $M(-x,-y,xy-z^*_{(x,y)})$ from (4.2.1). Equate the z-values of the two expressions for the inverse for (4.14a).

Now consider (4.14b). For each (x,y), write

$$M(x,y,z_{(x,y)}) = M(x,y,z^*_{(x,y)})M(0,0,c_{(x,y)}).$$

Temporarily refer to the effect of $\alpha^{\pm1}$ on (x,y) as $(x,y)_{\alpha^{\pm1}} \stackrel{\text{def}}{=} (x_{\alpha^{\pm1}}, y_{\alpha^{\pm1}})$. As α acts trivially on the center of $H_{\ell^{k+1}}$, the 1st sentence says $c_{(x,y)} = z_{(x,y)_{\alpha^{\pm1}}} - z^*_{(x,y)_{\alpha^{\pm1}}}$. Use this to determine $c_{(x,y)}$ from $\left(\begin{smallmatrix}\alpha & 0\\ M(x,y,z_{(x,y)}) & 1\end{smallmatrix}\right)^3 = \left(\begin{smallmatrix}1 & 0\\ I_3 & 1\end{smallmatrix}\right)$ and the corresponding formula with the substitution

$$\alpha \mapsto \alpha^{-1}, z_{(x,y)} \mapsto z^*_{(x,y)}. \tag{4.15}$$

The result, given that $x_{\alpha^{-1}}+x_\alpha+x = y_{\alpha^{-1}}+y_\alpha+y = 0$ is

$$\begin{aligned} &M(x_{\alpha^{-1}}, y_{\alpha^{-1}}, z_{(x,y)_{\alpha^{-1}}})M(x_\alpha, y_\alpha, z_{(x,y)_\alpha})M((x,y,z_{(x,y)}) = \\ &M(0,0,z_{(x,y)_{\alpha^{-1}}}+z_{(x,y)_\alpha}+z_{(x,y)}+x_{\alpha^{-1}}y_\alpha+(x_{\alpha^{-1}}+x_\alpha)y). \end{aligned} \tag{4.16}$$

Apply the substitution (4.15) to conclude that not only is the z value 0, but so is

$$z^*_{(x,y)_{\alpha^{-1}}}+z^*_{(x,y)_\alpha}+z^*_{(x,y)}+x_\alpha y_{\alpha^{-1}}+(x_{\alpha^{-1}}+x_\alpha)y.$$

Subtract those two z values to conclude

$$3c_{(x,y)} = x_\alpha y_{\alpha^{-1}} - x_{\alpha^{-1}}y_\alpha = yx + (x-y)^2. \tag{4.17}$$

That gives (4.14b).

The conjugacy classes of $\alpha_0^{\pm1}$ are the orbits from conjugating by the kernel of the map to $H_{\ell^{k+1}} \to \mathbb{Z}/3$. Since conjugation by $M(x,y,z)$ is independent of z (Rem. 4.7), those conjugacy classes give the elements of order 3. □

REMARK 4.7 (Homogeneous action). As $M(x,y,z+z') = M(x,y,z)M(0,0,z')$, since α acts trivially on $M(0,0,z')$, we have $M(x,y,z+z')^\alpha = M(x,y,z)^\alpha M(0,0,z')$. Still, that doesn't yet pin down $z_{(x,y)}$ as a function of (x,y).

REMARK 4.8. Lem. 4.3 also showed that for ℓ odd and $\equiv 1 \mod 3$ there is an ℓ-Frattini extension of G_ℓ to $(\mathbb{Z}/\ell^2 \times^s \mathbb{Z}/\ell) \times^s \mathbb{Z}/3$. But, this isn't a central extension. Replacing $\mathbb{Z}/\ell^2 \times^s \mathbb{Z}/\ell$ by $\mathbb{Z}/\ell^2 \times \mathbb{Z}/\ell$ (an abelian group: $\times^s \mapsto \times$) gives another with the same properties (same ℓs; same argument). This covers all ℓ-Frattini extensions of G_ℓ with 1-dimensional kernel, where the restriction to the ℓ-Sylow is abelian.

REMARK 4.9. Often, applying Prop. 4.5 shows the lift invariant – defined on any Nielsen class for any central Frattini extension – precisely finds braid orbits. [**Fr10**, Thms. A and B] is a series of examples. The case $G = A_4$ and $r = 4$ meets the case of Prop. 4.19 (appearing as $\ell = 2, k = 0$; see Rem. 4.13).

4.3. The lift invariant separates many braid orbits. For $m \in \mathbb{Z}/\ell^{k+1}$, denote the braid orbit union of $\boldsymbol{g} \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ with $s_{\ell^{k+1}}(\boldsymbol{g}) = m$ by O_m.

Also, denote the union of reduced (inner and compactified) Hurwitz space components with lift invariant m by $\bar{\mathcal{H}}_{\ell^{k+1},m}$. Prop. 4.19 shows, for $\ell \neq 3$ and each $m \in \mathbb{Z}/\ell^{k+1}$ satisfying (4.2), that O_m is nonempty. We explicitly find that the braid orbits with lift invariant satisfying (4.2) contain, respectively, double identity (as in (1.3b))) or H-M reps.

Prop. 6.3 and Prop.6.8 produce the version of this result for $\ell > 3$. §4.3.2 redoes a previously known result for $\ell = 2$. A nontrivial lift invariant distinguished that braid orbit from all others. There are several braid orbits with trivial lift invariant, but we do know how many there are and key data on what they contain.

4.3.1. *Counting:* H-M *and double identity reps.* The notation $T_{\pm\pm}$ is from §4.1. We use the moduli group, $\mathcal{Q}''$, of §3.1. [**Fr06**, Prop. 6.1.2] did the computation of braid orbits where $G_0 = A_4$ – our case here, where $\ell = 2$ and $k = 0$ – on the Nielsen class $\mathrm{Ni}(A_4, \mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$. Here is a compendium of those results.

(4.18a) The two braid orbits on this Nielsen class correspond to Hurwitz space components $\mathcal{H}^{\mathrm{in}}_{\pm}$. Both inner spaces have genus 0 [**Fr06**, (6.9)].

(4.18b) $\mathcal{H}_+$, corresponding to an H-M orbit, is the space of covers with branch cycles of lift invariant +1. Its compactification has degree 9 over $\mathbb{P}^1_j$.

(4.18c) $\mathcal{H}_-$, corresponding to a double identity rep. orbit., is of covers with lift invariant -1. Its compactification has degree 6 over $\mathbb{P}^1_j$.

(4.18d) Orbits of $\mathcal{Q}''$, restricted to each of the two braid orbits, have length 2.

LEMMA 4.10. *A $\boldsymbol{g} \in T_{\pm\pm}$ cannot simultaneously be a double identity rep. and either an* H-M *or shift of an* H-M *rep.*

PROOF. Assume $\boldsymbol{g}$ is double identity and H-M, or it is double identity and the shift of an H-M. Applying **sh**, we may assume $g_1 = g_3$. By assumption, in either case, $g_2 = g_1^{-1} (= g_3^{-1})$. But then $\langle \boldsymbol{g} \rangle = G_\ell$ would be cyclic. A contradiction: □

Lem. 4.11 gives many critical cusp widths.

(4.19a) ${}_{\boldsymbol{v},3,4}\boldsymbol{g} \stackrel{\mathrm{def}}{=} (\alpha_0, \alpha^{-1}, {}_{\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1})$ (resp.) for an H-M rep. and
${}_{\boldsymbol{v},2,3}\boldsymbol{g} \stackrel{\mathrm{def}}{=} (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{\boldsymbol{v}}\alpha_0, \alpha_0^{-1})$ for the shift of an H-M rep.

(4.19b) ${}_{\boldsymbol{v},1,3}\boldsymbol{g} \stackrel{\mathrm{def}}{=} (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, \alpha_0, {}_{-\boldsymbol{v}}\alpha_0^{-1})$ and ${}_{\boldsymbol{v},2,4}\boldsymbol{g} \stackrel{\mathrm{def}}{=} (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{2\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1})$ for the two types of double identity reps.

LEMMA 4.11. *Assume $\ell > 3$. The element* $\mathbf{sh}^2$ *maps ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$ to the inner class of ${}_{-\boldsymbol{v},3,4}\boldsymbol{g}$, and the two inner classes are distinct. Also,*

(4.20) *The inner class of $(({}_{\boldsymbol{v},3,4}\boldsymbol{g})\mathbf{sh})q_1q_3^{-1} = {}_{-\boldsymbol{v}^\alpha,2,3}\boldsymbol{g}$ (inner equivalent to ${}_{-\boldsymbol{v},2,3}\boldsymbol{g}$) is reduced inequivalent to ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$.*

Also, with $L_{-2\boldsymbol{v}}$ conjugation by $-2\boldsymbol{v}$:

(4.21a) $(({}_{\boldsymbol{v},1,3}\boldsymbol{g})\mathbf{sh})q_1^{-1}q_3 = ({}_{\boldsymbol{v},1,3}\boldsymbol{g})q_2^{-2}$*; and*

(4.21b) $(((({}_{\boldsymbol{v},2,4}\boldsymbol{g})\mathbf{sh})L_{-2\boldsymbol{v}})q_1^{-1}q_3) = ({}_{\boldsymbol{v},2,4}\boldsymbol{g})q_2^{-2}$.

So, $\mathcal{Q}''$ has length 4 orbits on H-M *or double identity braid orbits.*

For $\ell \equiv 2 \mod 3$ *(resp.* $\ell \equiv 1 \mod 3$*) there are* $d_{\ell^{k+1}}$
$= (1-\ell^{-2})\ell^{2(k+1)}$*(resp.* $(1-\ell^{-2})\ell^{2(k+1)} - 2(1-\ell^{-1})\ell^{k+1}+\ell^k$)

α*-generators (Def. 4.2) in* $\boldsymbol{v} \in V_{\ell^{k+1}}$*. Then, there are* $\frac{d_{\ell^{k+1}}}{6}$ *reduced inequivalent* H-M*, shift of* H-M*, or double identity reps. of either type in* (4.21).

Proof. The only element of $\mathcal{Q}''$ that might fix the inner class of ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$ is $\mathbf{sh}^2$. Compute easily that $({}_{\boldsymbol{v},3,4}\boldsymbol{g})\mathbf{sh}^2 = {}_{-\boldsymbol{v},3,4}\boldsymbol{g}$. To show this is not in the same inner class as ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$ comes to showing that $(-\boldsymbol{v})\alpha^j \neq \boldsymbol{v}$. This follows from ℓ is odd and Lem. 4.1: ± 1 are not eigenvalues of α. Showing (4.20) is similar, with ${}_{-\boldsymbol{v},2,3}\boldsymbol{g}$ conjugate by α_0 to ${}_{-\boldsymbol{v}^\alpha,2,3}\boldsymbol{g}$.

Now consider (4.21) applied to ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$. Then,

$$(({}_{\boldsymbol{v},1,3}\boldsymbol{g})\mathbf{sh})q_1^{-1}q_3 = ({}_{\boldsymbol{v}}\alpha^{-1}, \alpha_0, {}_{-\boldsymbol{v}}\alpha_0^{-1}, \alpha_0) = (\alpha_0, {}_{\boldsymbol{v}^\alpha}\alpha^{-1}, {}_{\boldsymbol{v}^\alpha-\boldsymbol{v}}\alpha_0, {}_{-\boldsymbol{v}}\alpha_0).$$

The middle product of ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ is $\boldsymbol{v}-\boldsymbol{v}^\alpha$. Take its negative to see that q_2^{-2} applied to ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ is conjugation of the 2nd and 3rd terms by the middle product, $\boldsymbol{v}^\alpha-\boldsymbol{v}$. That gives (4.21a). Similarly,

$$(((({}_{\boldsymbol{v},2,4}\boldsymbol{g})\mathbf{sh})L_{-2\boldsymbol{v}})q_1^{-1}q_3 = (\alpha_0, {}_{-\boldsymbol{v}}\alpha_0^{-1}, {}_{-\boldsymbol{v}^\alpha-\boldsymbol{v}}\alpha_0, {}_{-\boldsymbol{v}}\alpha_0^{-1}).$$

Since the middle product of ${}_{\boldsymbol{v},2,4}\boldsymbol{g}$ is $v-v^\alpha$, conjugating by its inverse gives (4.21b).

As already noted, the only element that could possibly fix any H-M or double identity inner rep. is $\mathbf{sh}^2$, but according to (4.21) that would imply q_2^{-4} fixes that inner class. Since $q_2^{2\ell}$, does also, the Chinese remainder theorem implies that so does q^2. But that is clearly false.

A simple if and only if condition gives (1.4a) (generation) for any of an H-M, shift of H-M, or double identity rep. Using the notation of (4.19), In each case, α_0 and $\boldsymbol{v}$ $(= \left(\begin{smallmatrix} 1 & 0 \\ \boldsymbol{v} & 1 \end{smallmatrix}\right))$ generate $G_{\ell^{k+1}}$. Select $\boldsymbol{v}$ according to Lem. 4.1, There is no other constraint to forming the Nielsen class rep.

We have the further equivalence of conjugating by powers of α_0, and for the elements we are discussing, there is the $\mathbf{sh}^2$ keeping them of the same type, but not fixing them. That accounts for the division by 6 of $d_{\ell^{k+1}}$. □

Respective to $\ell \equiv 1$ and $2 \mod 3$, Lem. 4.1 and Lem. 4.12 count the elements in our Nielsen classes. Lem. 4.12 uses that $G_{\ell^{k+1}} \to G_\ell$ is an ℓ-Frattini cover to guarantee generation for a 4-tuple at level k lying over a Nielsen class at level 0.

Lemma 4.12. *For* $\ell \equiv 2 \mod 3$ *there are* $c_\ell \stackrel{\text{def}}{=} \ell^4-1$ *inner Nielsen classes* $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$*. If each of these is in an* H-M *or double identity braid orbit, then the reduced classes,* $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{in,rd}}$*, contain* $\frac{c_\ell}{2}$ *elements.*

For $\ell \equiv 1 \mod 3$ *they contain* $c'_\ell \stackrel{\text{def}}{=} \ell^4 - 2\ell^2 + 1$ *inner classes, and if each is in an* H-M *or double identity braid orbit, then there are* $\frac{c'_\ell}{2}$ *reduced classes.*

There are ℓ^k H-M *(resp. double identity) reps. in* $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})^{\mathrm{in,rd}}$ *lying over a given* H-M *(resp. double identity) rep. in* $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{in,rd}}$*,* $k \geq 0$.

Proof. For $\ell \equiv 2 \mod 3$, according to Lem. 4.1 we can form an element in $T_{\pm\pm}$ by choosing $\boldsymbol{v}_2$ and $\boldsymbol{v}_3$ in $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = (\alpha_0, {}_{\boldsymbol{v}_2}\alpha_0^{-1}, {}_{\boldsymbol{v}_3}\alpha_0, \bullet)$ subject to not both being $\mathbf{0} \mod \ell$. The count of those $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ is $c_\ell \stackrel{\text{def}}{=} \ell^4-1$.

Among all these we can conjugate by α_0, and move the $+$ among the 2nd through 4th positions by braids. Thus, c_ℓ also counts inner equivalence classes.

For reduced classes, under the assumption that the braid orbits are of either H-M or double identity reps., Lem. 4.11 says an element of $\mathcal{Q}''$ that doesn't change the type equivalences distinct pairs of inner classes. Example: Pairs of elements of $T_{\pm\pm}$ are reduced equivalent by $\mathbf{sh}^2$. So, there are $\frac{c_\ell}{2}$ reduced classes.

Now consider $\ell \equiv 1 \mod 3$. Here we must adjust $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ so both of $\boldsymbol{v}_2$ and $\boldsymbol{v}_3$ are not in a particular eigenspace for the action of α_0. There are two distinct eigenspaces, so there are $\ell^4-2\ell^2+1$ such allowable pairs, and the rest of the calculation proceeds as previously.

To find all H-M (resp. double identity) reps. in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})^{\mathrm{in,rd}}$ over ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$, or ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$, etc. requires only listing the distinct elements ${}_{\tilde{\boldsymbol{v}},3,4}\boldsymbol{g}$, or ${}_{\tilde{\boldsymbol{v}},1,3}\boldsymbol{g}$, etc. with $\tilde{\boldsymbol{v}} \in V_{\ell^{k+1}}$ over $\boldsymbol{v}$. Given one such this is equivalent to listing the ℓ^{2k} distinct values of $\boldsymbol{w}^\alpha - \boldsymbol{w}$ as $\boldsymbol{w}$ runs over $\ker(V_{\ell^{k+1}} \to V_\ell)$. □

Remark 4.13 (Overlapping case). One case, $\ell = 2 = n$, overlaps between [**Fr10**, Thm. B] (giving the braid orbits for $\mathrm{Ni}(A_n, \mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$, $n \geq 4$, $r \geq n-1$) and Prop. 4.19. That inspired a formula for the lift invariant for the central extension being the spin cover of A_n. Rem. 4.7 and Lem. 5.10 give an algorithm for the lift invariant for $G_{\ell^{k+1}}$ Nielsen classes. It is an analog of the explicit [**Fr10**, Thms. 1 and 2] proof for the lift invariant for branch cycles in $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$.

Remark 4.14. For $k = 0$, d_l in Lem. 4.11 is $K_\ell(\ell-1)$ with K_ℓ defined in (5.1).

4.3.2. *Identifying the lift invariant when $\ell = 2$.* The Nielsen class $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$, in Lem. 4.15 has $r = 3$; the classes are three repetitions of C_3. This subsection has a key argument that finds the braid orbits on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$, just for $\ell = 2$.

Lemma 4.15. *An* H-M *rep. (in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$) has trivial lift invariant. There is a lift invariant preserving correspondence between*

$$\begin{aligned} \boldsymbol{g}' = &\quad (g_1', g_2', g_3') \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{3^3}) \text{ and double identity reps.} \\ {}_{1,4}\boldsymbol{g} = &\quad ((g_1')^{-1}, g_2', g_3', (g_1')^{-1}) \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2}). \end{aligned}$$

In place of ${}_{1,4}\boldsymbol{g}$ we could also use

$${}_{2,1}\boldsymbol{g} = ((g_2')^{-1}, (g_2')^{-1}, g_3', g_1') \text{ or } ({}_{2,1}\boldsymbol{g})q_2^{-1} = ((g_2')^{-1}, (g_2')^{-1} g_3' g_2', (g_2')^{-1}, q_1'),$$

or other variants placing the doubled pair where ever we want.

Proof. Assume generation holds for $\boldsymbol{g}_{\text{H-M}} = (g_1, g_1^{-1}, g_3, g_3^{-1}) \in \mathbf{C}_{+3^2-3^2}$: $\langle g_1, g_3 \rangle = G_{\ell^{k+1}}$. Take $g_1 = \alpha_0$ and $\hat{g}_3 = {}_{\hat{\boldsymbol{v}}}\alpha_0$ (as in (4.19b)) with $\boldsymbol{v}$ outside any eigenspace for α_0. Then, the lift invariant is the product of the entries in $(\hat{g}_1, (\hat{g}_1)^{-1}, \hat{g}_3, (\hat{g}_2)^{-1})$. In multiplicative notation, the lift invariant is trivial.

Now consider $\boldsymbol{g}' = (g_1', g_2', g_3') \in \mathrm{Ni}(G_\ell, \mathbf{C}_{3^3})$. In (4.11) notation, compute the lift invariant, $s_{\ell^{k+1}}(\boldsymbol{g}')$, using element lifts where

$$\hat{g}_1' = \alpha_0 \text{ and } \hat{g}_i' = \begin{pmatrix} \alpha & 0 \\ M(x_i, y_i, z_{(x_i,y_i)}) & 1 \end{pmatrix},\ i = 2, 3.$$

Since $\hat{g}_1$ has order 3, $\hat{g}_1^{-1}\hat{g}_1^{-1} = \hat{g}_1$, a computation in an order 3 group subgroup of $H_{\ell^{k+1}}$. So, whatever is $s_{\ell^{k+1}}(\hat{\boldsymbol{g}}') = \hat{g}_1'\hat{g}_2'\hat{g}_3' \in \mathbb{Z}/\ell^{k+1}$, it is the same as

$$(\hat{g}_1')^{-1}\hat{g}_2'\hat{g}_3'(\hat{g}_1')^{-1} = s_{\ell^{k+1}}(\boldsymbol{g}).$$

This association between $\boldsymbol{g}'$ and $\boldsymbol{g}$ is clearly reversible, as are the variants. □

According to Cor. 4.4, $Q_8 \times^s \mathbb{Z}/3$ is the 2-Frattini central extenson of G_2. We can't use the same notation as in the Heisenberg group. Still, the arguments of Prop. 4.6 apply. There is a unique element $Q(x,y) \in Q_8$ that lies over (x,y) such that $\left(\begin{smallmatrix} \alpha & 0 \\ Q(x,y) & 1 \end{smallmatrix}\right)$ has order 3, and α acts on these $Q(x,y)$ s.

Consider the Nielsen class element $(\alpha_0, \left(\begin{smallmatrix} \alpha & 0 \\ Q(x,y) & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \alpha & 0 \\ Q(x',y') & 1 \end{smallmatrix}\right))$. Then, use the product one condition to compute the lift invariant as $Q(x,y)^\alpha Q(x',y')$. But, product-one implies the original Nielsen element we must have $(x,y)^\alpha = -(x',y')$. Since $\ell = 2$, that means $Q(x,y)^\alpha = Q(x',y')$. The necessary condition for generation is just that $(x,y) \neq (0,0)$.

Definition 4.16. Refer to $u \in \mathbb{Z}/\ell^{k+1}$ as ℓ-divisible if $u \equiv 0 \mod \ell$. In our cases, with lift invariants in $\mathbb{Z}/\ell^{k+1}$, we also apply this name (and ℓ') to a Nielsen classes rep. or braid orbit having such a lift invariant.

Corollary 4.17. *All elements of* $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})^{\mathrm{in}}$ *have representatives of form* $_{\boldsymbol{w}}\boldsymbol{g} = (\alpha_0, {}_{\boldsymbol{w}_2}\alpha_0, {}_{\boldsymbol{w}_3}\alpha_0)$*, where* $\boldsymbol{w}_3 = -\boldsymbol{w}_2^\alpha$*. Assume for* $\ell \neq 3$*, that*

(4.22) *all elements of* $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$ *have* ℓ' *lift invariant.*

Then, so do all double identity reps. of $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$*. Elements with* ℓ*-divisible lift invariant and double identity reps. have distinct braid orbits.*

When $\ell = 2$*,* $k = 0$*,* (4.22) *applies.*

Proof. From product-one for the entries of $_{\boldsymbol{w}}\boldsymbol{g}$, easily compute that

$$\boldsymbol{w}_2^\alpha - \boldsymbol{w}_2 + \boldsymbol{w}_3 - \boldsymbol{w}_3^{\alpha^{-1}} = \mathbf{0} \text{ in additive notation.} \tag{4.23}$$

As α is invertible, the unique expression for $\boldsymbol{w}_3$ in $\boldsymbol{w}_2$ is given in the statement.

The first sentence of the 2nd paragraph follows immediately from Lem. 4.15. Since lift invariants are braid invariants (Prop. 4.5), the hypothesis of nontrivial lift invariant for double identity reps. means they are in distinct orbits from H-M reps.

That leaves proving that double identity reps. have nontrivial lift invariants when when $\ell = 2$. From the above we have computed the lift of any Nielsen class element is $Q(x,y)^2$, for some $(x,y) \in V_2 \setminus \{\mathbf{0}\}$. But the lift of any nontrivial element in V_2 to Q_8 has order 4, so its square is nontrivial. □

Remark 4.18. The case $\ell = 2$ is the meeting point for the general result (on the lifting invariant in [**Fr10**, Invariance Cor. 2.3]) about the braid orbits of $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$ (3-cycle Nielsen classes in A_n) and the Nielsen classes of this paper. That result applies because the genus, g', of degree 4 covers with 3 branch points, each with a 3-cycle as its branch cycle is 0:

$$2(4 + g' - 1) = 3(3 - 1) \implies g' = 0.$$

That proof, however, where the central extension is the spin cover, won't generalize to our Heisenberg extension. We see, however, the argument we gave above does.

4.3.3. *Lift invariants; all* ℓ*.* For $\boldsymbol{h} = (\alpha_0, {}_{(x',y')}\alpha_0, {}_{(x,y)}\alpha_0) \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$, the element in $(H_{\ell^{k+1}})^4 \cap \mathbf{C}_{3^3}$ whose entries give its lift invariant is

$$\boldsymbol{\alpha}_{x,y} \stackrel{\text{def}}{=} (\alpha_0, \left(\begin{smallmatrix} \alpha & 0 \\ M(x',y',z_{(x',y')}) & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} \alpha & 0 \\ M(x,y,z_{(x,y)}) & 1 \end{smallmatrix}\right)).$$

Here, (x, y) is not in an α-eigenspace on V_ℓ. As in Cor. 4.17, $(x', y')^\alpha = -(x, y)$. Then, the lift invariant is the z value in

$$M(-x, -y, z_{(-x,-y)})M(x, y, z_{(x,y)}) = M(0, 0, z_{(-x,-y)}+z_{(x,y)}-xy). \tag{4.24}$$

PROPOSITION 4.19. *The lift invariant of $\boldsymbol{\alpha}_{x,y}$ is*

$$f(x, y) = (x^2 - xy + y^2)/3. \tag{4.25}$$

All elements of $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$ have ℓ' lift invariant. We achieve all such lift invariants by running over them. Therefore, these statements also hold for all double identity reps. in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$.

Conclude, a double identity rep. and $\boldsymbol{g} \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ with ℓ-divisible lift invariant have distinct braid orbits.

PROOF. Add (4.14a) to (4.14b) to get the z value in (4.24) and conclude (4.25). If the first sentence holds for elements of $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^3})$, then Cor. 4.17 shows the second sentence for elements of $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$.

Suppose the two statements about lift invariants in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$ are correct. Then, Lem. 4.15 shows these are equivalent to the statement about double identity lift invariants in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$.

We now restrict attention to the lift invariant for elements of $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^3})$. Fix a particular $(x_0, y_0) \neq (0, 0)$ that gives an element of the Nielsen class. Suppose it has lift invariant $a' \in (\mathbb{Z}/\ell)^*$. Then, the line in V_ℓ of multiples, (ax_0, ay_0), $a \in (\mathbb{Z}/\ell)^*$, runs over lift invariants in the coset of a' in the squares of $(\mathbb{Z}/\ell)^*$.

Now we show we get only nontrivial values of the lift invariant; then that we get both the trivial and nontrivial cosets of the squares. There are no solutions with $y = 0$. Without loss, along a given line in V_ℓ, take $y_0 = 1$, to see 0 lift invariant comes from x_0 satisfying $x_0^2-x_0+1 = 0$. Changing x to $-x$ changes nothing. Therefore, from Lem. 4.1, there is no solution if $\ell \equiv 2 \mod 3$. Also, if $\ell \equiv 1 \mod 3$, any solution gives an α-eigenspace, and so is excluded by the generation condition for entries of $\boldsymbol{\alpha}_{x,y}$.

We are done if we show x^2+x+1 achieves both squares and nonsquares. For the former take $x_0 = 0$. Since $\ell \neq 2$, we can make the substitution $x \mapsto x-\frac{1}{2}$ whereby the invariant values run over the range of $x^2 + \frac{3}{4}$. Then, multiplying by the square 4, we are reduced to showing that $x^2 + 3$ has nonsquare values. If 3 is a nonsquare, then take $x = 0$. If not, $3 = m^2$, in which case substitute $x \mapsto mx$. This reverts us to showing $x^2 + 1$ takes on values in nonsquares. Rem. 4.20 is probably overkill, but it concludes the proposition.

Now consider higher levels ($k > 0$). The case $\ell = 2$ is different, so we reserve that for Rem. 7.2. Suppose $(x_1, y_1) \in V_{\ell^{k+1}}$ lies over $(x_0, y_0) \in V_\ell$ and that $\boldsymbol{\alpha}_{x_0,y_0}$ has lift invariant m_0. Given $\boldsymbol{\alpha}_{x_1,y_1}$ at level k lying over (x_0, y_0), form $\boldsymbol{\alpha}_{x_1,y_1}$ (formula (**??**)). It will lie in the Nielsen class $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^3})$, over $\boldsymbol{\alpha}_{x_0,y_0}$, and its lift invariant m_1 is also over m_0. Now, suppose, $m' \in \mathbb{Z}/\ell^{k+1}$ lies over m_0.

To achieve every ℓ' lift invariant at level k only requires finding (x', y') over (x_0, y_0) so the lift invariant of $\boldsymbol{\alpha}_{x',y'}$ is m'. The general case is a standard induction on k. So we take just the case $k = 1$. Again, apply the lift invariant value in (4.25). So, this amounts to finding (x'_1, y'_1) with $x' = x_1 + \ell x'_1$ and $y' = y_1 + \ell y'_1$, with

$$2x_1x'_1 + (x_1y'_1 + y_1x'_1) + 2y_1y'_1 = m' - m_1.$$

Given $(x_1, y_1, m'-m_1)$, there is no soluton (x_1', y_1') mod ℓ only if $2y_1+x_1 = 0$ and $2x_1+y_1 = 0$. Since the determinant of the matrix of coefficients is -3, the only solution is $(x_1, y_1) \equiv \mathbf{0}$ mod ℓ, contrary to (x_1, y_1) not being an α eigenvector.

Finally, let $\boldsymbol{g}_{\ell-\text{div}}, \boldsymbol{g}_{\text{D-E}} \in \text{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$, respectively, be ℓ-divisible and double identity reps. at level k. From above, they have distinct lift invariants. Prop. 4.5 says they are in distinct braid orbits. This concludes the proposition. □

REMARK 4.20. [**Mont91**, p. 149, Exer. 18] defines $N_{++}(\ell)$ to be the number of squares n mod ℓ for which $n+1$ is also a square, with $1 \le n \le \ell-2$. The (H) at the end of the exercise means there is a hint. Use the quadratic residue symbol $(\frac{n}{\ell})$ ($+1$ if $n \neq 0$ is a square mod ℓ, -1 otherwise). Then, $N_{++}(\ell) = (\ell-(\frac{-1}{\ell})-4)/4$. We add to the hints using $u(\ell) = \sum_0^{\ell-1}(\frac{n}{\ell})$ $(= 0)$ and $s(\ell, a) = \sum_{n=1}^{\ell-2}(\frac{n(n+a)}{\ell}) = -1$.

(4.26a) Substitute $n \mapsto na$; multiplicativeness of the Jacobi symbol shows $s(\ell, a)$ is independent of a for $a \not\equiv 0$ mod ℓ.

(4.26b) Rewrite $u(\ell)^2$ as $\sum_{a=0}^{\ell-1} s(\ell, a)$; conclude $s(\ell, a) = -1$ for $(a, \ell) = 1$.

(4.26c) Show that $N_{++}(\ell) = \sum_{n=1}^{\ell-2}(1 + (\frac{n}{\ell})(1+(\frac{n+1}{\ell})))/4$ [**Mont91**, p. 506].

5. Braid orbits on $\text{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})^{\text{rd}}$

Assume (4.2): component lift invariants are 0 or ℓ'. The two cases account for all components of $\mathcal{H}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\text{rd}}$, for $\ell \neq 3$. For the latter case, we will identify all components of $\mathcal{H}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})^{\text{rd}}$ with ℓ' lift invariant, for each $\ell \neq 3$, $k \ge 0$.

From this comes the ℓ-adic representations in the paper title. The main device is special Nielsen class representatives called *1-degenerate* (5.7).

DEFINITION 5.1. We slightly extend §4.1 notation to refer to $T_{\ell^{k+1},\pm\pm,1-\text{deg}}$: The set of 1-degenerates in $T_{\pm\pm} \cap \text{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3-3})^{\text{rd}}$.

§5.1 shows how these give us precise orbit statements. §5.2 gives tools for dealing directly with orbits of 1-degenerate elements; §5.3 explicitly gives the lift invariants of 1-degenerate elements; and §5.4 produces all level $k = 0$ orbits.

5.1. 1-degenerate Nielsen reps. and orbit statements. We will show that orbits with trivial lift invariant differ substantially from those with nontrivial lift invariant. We state this, for $k = 0$, using this quantity:

(5.1) $K_\ell = \frac{\ell\pm1}{6}$ for $\ell \equiv \mp 1$ mod 3.

(5.2a) Classes with trivial lift invariant fall in H-M braid orbits. There are K_ℓ of these: each contains $2(\ell-1)$ elements of $T_{\ell^{k+1},\pm\pm,1-\text{deg}}$.

(5.2b) Orbits with nontrivial lift invariant are double identity, distinguished by that invariant. Each contains $K_\ell(\ell-1)$ elements of $T_{\ell^{k+1},\pm\pm,1-\text{deg}}$.

Further clarifying points showing the value of concentrating on $T_{\ell^{k+1},\pm\pm,1-\text{deg}}$.

(5.3a) Elements of (5.2a) in $T_{\ell^{k+1},\pm\pm,1-\text{deg}}$ consist precisely of H-M and shift of H-M reps.

(5.3b) There are K_ℓ of each type – $\boldsymbol{v}_{,1,3}\boldsymbol{g}$ and $\boldsymbol{v}_{,2,4}\boldsymbol{g}$ – of double identity elements in (5.2b).

See (6.16) for analogous statements for higher k.

Contrast the two pieces of (5.2) with the result if we replace $\text{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\text{rd}}$ by $\text{Ni}(G_\ell, \mathbf{C}_{+3^d-3^d})^{\text{rd}} \stackrel{\text{def}}{=} \text{Ni}_d$ with $d >> 2$: Conway-Fried-Parker-Völklein result [**FrV91**, Appendix] or improvements from [**Fr10**, Main. Thm.].

(5.4a) (5.2b) *is* what we get for Ni_d, $d >> 2$, but for Ni_2 it is harder.

(5.4b) Instead of (5.2a), there is just one H-M orbit for $d >> 2$.

H-M orbits – especially because the absolute Galois group recognizes their geometry – have been a continual mainstay since their introduction in [**Fr95**, Thm. 3.21] and continuation in [**DE06**] to produce systems of Modular Tower components defined over $\mathbb{Q}$. Rem. 6.9, however, lists examples of them where they produce components not distinguished by the pair (Nielsen class, lift invariant).

5.1.1. *1-degenerate Definition.* Use the notation ${}_{\boldsymbol{v}}\alpha_0$ as in (4.3), so we can express a representative of any inner Nielsen class in $T_{\pm\pm}$ in a *standard* form:

$$\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = (\alpha_0, {}_{\boldsymbol{v}_2}\alpha_0^{-1}, {}_{\boldsymbol{v}_3}\alpha_0, {}_{\boldsymbol{v}_4}\alpha_0^{-1}). \tag{5.5}$$

Express the product-one condition as

$$(\boldsymbol{v}_2 - \boldsymbol{v}_2^{\alpha}) + (\boldsymbol{v}_3^{\alpha} - \boldsymbol{v}_3) + (\boldsymbol{v}_4 - \boldsymbol{v}_4^{\alpha}) = \mathbf{0}. \tag{5.6}$$

Using the operator $1-\alpha$, this is equivalent to $\boldsymbol{v}_2 - \boldsymbol{v}_3 + \boldsymbol{v}_4 = \mathbf{0}$.

Generation (1.4a) is equivalent (Def. 4.2) to $\langle \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\rangle$ contains an α-gen. of $V_{\ell^{k+1}}$; nontrivial from Lem. 4.1 only when $\ell \equiv 1 \mod 3$. A significant special case:

(5.7) 1-*degeneracy*: $\langle \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\rangle \le V_{\ell^{k+1}}$ is a 1-dimensional $\mathbb{Z}_{\ell^{k+1}}$ module.

By writing the $\boldsymbol{v}$s as multiples $(0, m_2, m_3, m_4)$ of a given $\boldsymbol{v} \in V_{\ell^{k+1}}$. Both H-M and shift of H-M (either m_2 or m_4 is 0) and double identity reps. (either $m_3 = 0$ or $m_2 = m_4$) are cases of (5.7). The following conditions are necessary and sufficient for elements to be in the Nielsen class.

(5.8a) $\boldsymbol{v}$ is an α-gen. (If $\ell \equiv 2 \mod 3$, then $\boldsymbol{v} \bmod \ell$ is not $\mathbf{0}$.)

(5.8b) $m_2 - m_3 + m_4 = 0$.

By writing $\boldsymbol{v}$ as (x, y), expression (4.25) explicitly computes the lift invariant. We will find the lift invariant is the *unique* separator of the ℓ' braid orbits.

5.1.2. *Locating 1-degenerates in braid orbits.* The last line of Lem. 5.2 gives a symmetry between the operators q_i^2, $i = 1, 2, 3$, that explains why we use $T_{\pm\pm}$ as our target configuration. The basic idea is in the proof of Lem. 5.2 where $\ell \equiv 2 \mod 3$. Lem. 5.5 adjusts this for when $\alpha \bmod \ell$ has eigenvectors.

With $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ in $T_{\pm\pm}$ in (5.5), write ${}_{\boldsymbol{v}_3}\alpha_0\,{}_{\boldsymbol{v}_4}\alpha_0^{-1} = \left(\begin{smallmatrix} 1 & 0 \\ \boldsymbol{w} & 1 \end{smallmatrix}\right)$, where $\boldsymbol{w}$ is

$$\boldsymbol{v}_3 - \boldsymbol{v}_3^{\alpha^{-1}} + \boldsymbol{v}_4^{\alpha^{-1}} - \boldsymbol{v}_4 = (\boldsymbol{v}_3 - \boldsymbol{v}_4)^{1-\alpha^{-1}} = \boldsymbol{v}_2^{1-\alpha^{-1}}. \tag{5.9}$$

Then, $\boldsymbol{w} = \mathbf{0}$ $(= \boldsymbol{v}_2)$ if and only if $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = \boldsymbol{g}$ is an H-M rep. Consider the line

$$L_{\boldsymbol{v}_3,\boldsymbol{w}} = \{\boldsymbol{v}_3 + u\boldsymbol{w}\}_{u\in\mathbb{Z}/\ell}.$$

LEMMA 5.2 (Case $\ell \equiv 2 \mod 3$). *If $\boldsymbol{g}$ is an* H-M *rep., then $(\boldsymbol{g})q_3^{2u_3} = \boldsymbol{g}$ for all u_3. Now assume $\boldsymbol{g}$ is not an* H-M *rep.*

Then, there is a unique $u_3 \mod \ell^{k+1}$ for which $(\boldsymbol{g})q_3^{2u_3}$ is 1-degenerate. It corresponds to the unique intersection of $L_{\boldsymbol{v}_3,\boldsymbol{w}}$ and the subspace generated by $\boldsymbol{v}_2$. That 1-degenerate is a double identity rep. if and only if $L_{\boldsymbol{v}_3,\boldsymbol{w}}$ goes through the origin.

You can substitute q_2^2 in the above, except, substitute the shift of an H-M *rep. for an* H-M *rep. for the excluded cases of $\boldsymbol{g}$.*

PROOF. The first paragraph is easy. Assume $\boldsymbol{g}$ is not an H-M rep. Compute:

$$(\boldsymbol{g})q_3^{2u} = (\alpha_0, {}_{\boldsymbol{v}_2}\alpha_0^{-1}, {}_{\boldsymbol{v}_3+u\boldsymbol{w}}\alpha_0^{-1}, {}_{\boldsymbol{v}_4+u\boldsymbol{w}}\alpha_0^{-1}). \tag{5.10}$$

Then, 1-degeneracy holds for the value u if and only if either $\boldsymbol{v}_3 + u\boldsymbol{w} = \mathbf{0}$, or $\boldsymbol{v}_2$ and $\boldsymbol{v}_3 + u\boldsymbol{w}$ generate the same 1-dimensional subspace. We show there is a unique value of u for which one or the other of these holds.

First: $L_{\boldsymbol{v}_3,\boldsymbol{w}}$ has a unique intersection – giving the unique value of u – with the subspace generated by $\boldsymbol{v}_2$ unless they are parallel: $\boldsymbol{w}$ is a multiple of $\boldsymbol{v}_2$. That, however, would make $\boldsymbol{w}$ an eigenvector of $1-\alpha^{-1}$, contrary – here – to Lem. 4.1.

If $L_{\boldsymbol{v}_3.\boldsymbol{w}}$ contains $\mathbf{0}$, say, for $u = u^0$, then $(\boldsymbol{g})^{2u_0}$ is a double identity rep., a special case of 1-degeneracy. The argument for q_2^2 replacing q_3^2 is identical. □

Lem. 5.3 generalizes Lem. 5.2 to all levels k. The notation of (5.6) for $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ still works, but the exceptional case of H-M rep. must be rethought. Refer to a copy of $\mathbb{Z}/\ell^{k+1}$ in $V_{\ell^{k+1}}$ as a *line*, as in the proof of Lem. 5.2.

LEMMA 5.3. *Make the following assumptions:*

(5.11a) $\boldsymbol{w}$ *in* (5.9) *is not* $\equiv \mathbf{0} \mod \ell$.

(5.11b) *No point of* $L_{\boldsymbol{v}_3,\boldsymbol{w}}$ *is* $\equiv \mathbf{0} \mod \ell$.

Then, there is a unique (invertible) $u \mod \ell^{k+1}$ *for which* $(\boldsymbol{g})q_3^{2u}$ *is 1-degenerate.*

PROOF. Induct on k. Such a u exists when $k = 0$, so assume the result holds – there is a u' – for k'. We show there is a corresponding u for $k = k'+1$ by reducing $\boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{w}$ modulo $\ell^{k'}$. Select any $u^* \in \mathbb{Z}/\ell^{k+1}$ over $u' \in \mathbb{Z}/\ell^{k'+1}$. This u^* will be invertible, because it lies over an invertible value $\mod \ell$. From u', we want a value u satisfying the conclusion following (5.10). We have $r^*\boldsymbol{v}_2 = \boldsymbol{v}_3 + u^*\boldsymbol{w} \mod \ell^k$. Let $\boldsymbol{w}' = (u^*)^{-1}(r^*\boldsymbol{v}_2 - \boldsymbol{v}_3)$.

Now consider the equation

$$(r^* + r'\ell^k)\boldsymbol{v}_2 = \boldsymbol{v}_3 + (u^* + m\ell^k)\boldsymbol{w} \text{ with } \boldsymbol{w} = \boldsymbol{w}' + \ell^k\boldsymbol{w}''.$$

Thus, $r'\boldsymbol{v}_2 = u^*\boldsymbol{w}'' + m\boldsymbol{w}' \mod \ell$. Since $\boldsymbol{v}_2$ and $\boldsymbol{w}'$ are independent $\mod \ell$, given $u^*\boldsymbol{w}''$, we can find r' and m solving this equation. That concludes the proof. □

REMARK 5.4 (1-degenerate circuits). Denote the full orbit of reduced elements of the operator q_i^2 – the q_i^2 *circuit* – on a Nielsen rep. $\boldsymbol{g}$ by $O_{q_i^2}(\boldsymbol{g})$. Lem. 5.2 says: If $\boldsymbol{g}$ is a 1-degenerate Nielsen rep., then the only 1-degenerate in $O_{q_i^2}(\boldsymbol{g})$ is $\boldsymbol{g}$. The q_2^2 and q_3^2 circuits of $\boldsymbol{g}$ won't, however, be the same.

LEMMA 5.5. *If* $\ell \equiv 1 \mod 3$ *adjust the statement of Lem. 5.5 to this. The* q_3^2 *(resp.* q_2^2*) circuit contains a (unique) 1-degenerate element if and only if* $\boldsymbol{v}_2$ *(resp.* $\boldsymbol{v}_4$*) is not an* α *eigenvector. If two of* $(\boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4)$ *are both* α *eigenvectors,then they are for distinct eigenvalues. So, the 3rd is not an* α *eigenvector.*

PROOF. The proof of Lem. 5.2 applies to the q_3^2 circuit so long as $\boldsymbol{v}_2$ is not an α eigenvector. A 1-degenerate element can't have any of $\boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4$ an α eigenvector, because then all of them will be as they will all be multiplies of that one. This is contrary to generation holding for $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$.

Since any of the q_i^2 circuits leaves one of the $\boldsymbol{v}_j$ s fixed, that circuit can't contain a 1-degenerate if that $\boldsymbol{v}_j$ is an α eigenvector. Further, if two of the $\boldsymbol{v}_j$ s are eigenvectors for the same eigenvalue, then, so the 3rd, from (5.6) will be also, again contradicting generation. If all three are eigenvectors for α, then two are eigenvectors with the same eigenvalue, contrary to the above. So at least one of the $\boldsymbol{v}_i$ s will not be an α eigenvector. □

For elements $\boldsymbol{g} \in T_{\pm\pm}$ we have two natural operators that preserve $T_{\pm\pm}$ defined as follows using the notation of (5.6).

$$\begin{aligned} I_1(\boldsymbol{g}) &\stackrel{\text{def}}{=} (\alpha_0, \boldsymbol{v}_4\alpha_0^{-1}, \boldsymbol{v}_3\alpha_0, \boldsymbol{v}_2\alpha_0^{-1}); \text{ and} \\ I_2(\boldsymbol{g}) &\stackrel{\text{def}}{=} (\boldsymbol{v}_4\alpha_0, \boldsymbol{v}_3\alpha_0^{-1}, \boldsymbol{v}_2\alpha_0, \alpha_0^{-1}). \end{aligned} \tag{5.12}$$

Note: $I_2(\boldsymbol{g}) = (g_4^{-1}, g_3^{-1}, g_2^{-1}, g_1^{-1})$ is inner equivalent (the line below (4.3)) to

$$(\alpha_0, \boldsymbol{v}_3-\boldsymbol{v}_4\alpha_0^{-1}, \boldsymbol{v}_2-\boldsymbol{v}_4\alpha_0, -\boldsymbol{v}_4\alpha_0^{-1}). \tag{5.13}$$

(5.14) Unless otherwise said, until §6.4 we assume $k = 0$.

5.2. Orbits of 1-degenerate elements. We know two elements, $\gamma_0 = q_1q_2$ mod $\mathcal{Q}''$ (order 3) $\gamma_1 = q_1q_2q_3 \mod \mathcal{Q}''$ (order 2) generate the mapping class group $\bar{M}_4 = H_4/\mathcal{Q}''$ acting on reduced Nielsen classes. There is the natural map $\psi_4 : H_4 \to S_4$. Denote the subgroup $\langle (1\,3), (2\,4)\rangle \le S_4$ by K. Then, $\psi_4^{-1}(K) \le H_4$ is the subgroup of elements that maps $T_{\pm\pm}$ onto itself.

We can regard $K^* = \psi_4^{-1}(K)/\langle q_1q_3^{-1}\rangle$ as an index 3 subgroup of $\bar{M}_4$. Since $\bar{M}_4$ has two generators, a famous result of Schreier says that a subgroup of index 4 in the free group on two generators requires at most 1 + 3(2-1) =4 elements to generate it. Also, we can compute these from coset representatives and the generators (say, [**FrJ86**, Lem. 15.22]). Note the careful rules on coset representatives, easy to apply in our case, where γ_0 and its powers work as coset reps. for K^* in $\bar{M}_4$.

Therefore that same computation gives generators, and a bound on their number, for any subgroup of index 4 in a group given by two generators.

PROPOSITION 5.6. *The following elements generate K^*: γ_1 (represented by $q_1q_2q_1$); $\gamma_0\gamma_1\gamma_0$ (represented by $q_2^{-1}q_1q_2$) and $\gamma_0^{-1}\gamma_1\gamma_0^{-1}$ (represented by $q_1q_2^{-1}q_1^{-1}$). The possible fourth generator turns out trivial.*

Therefore, $K^* = \langle \mathbf{sh}, q_1^2, q_2^2\rangle \mod \mathcal{Q}''$, and it contains $\langle q_2^2, q_3^2\rangle \mod \mathcal{Q}''$ as an index 2 subgroup: K^* is the union of the $\langle q_2^2, q_3^2\rangle \mod \mathcal{Q}''$ cosets of 1 and $\mathbf{sh}$.

PROOF. The Schreier construction finds the generators of the finite index subgroup $F^\dagger$ of the free group F using the symbols x (with decoration) for the generators of the free group and s for the selected coset reps. Then, running over the s s and x s, you form all expressions sxs' where you select s' (uniquely) so that the result is in the $F^\dagger$. Finally, you toss all those that tautalogically come out trivial. That's what we did to get the generators above.

To see that $\langle \mathbf{sh}, q_1^2, q_2^2\rangle$ is the same group just note that $q_1^2\mathbf{sh}$ is represented by $q_1^2(q_1^{-1}q_2^{-1}q_1^{-1}) = q_1q_2^{-1}q_1^{-1}$. Find the other generator of K^* similarly.

Finally, the identity $(q_1q_2q_3)q_i(q_1q_2q_3)^{-1} = q_{i+1}$, with the subscript i written mod 3, holds on Nielsen class representatives in general. Therefore, $\mathbf{sh}$ normalizes $\langle q_2^2, q_3^2\rangle \mod \mathcal{Q}''$. That concludes the proof. □

Suppose S is a subset of a Nielsen class Ni, and $G \le \bar{M}_4$. We apply Princ. 5.7 to find braid orbits in the Nielsen classes under study when $S = T_{\ell,\pm\pm,1-\deg}$.

PRINCIPLE 5.7 (1-degenerate). *With notation as above, assume there is a braid from any element in* Ni *to some element of S. Also, assume every element of $\bar{M}_4$ that braids between elements of S is in G. Then, the orbits of $\bar{M}_4$ on* Ni *are in one-one correspondence with the orbits of S under G.*

There is a one-one correspondence between braid orbits of $T_{\ell,\pm\pm,1-\deg}$ under K^* and braid orbits on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$.

PROOF. Let $O_{\boldsymbol{g}}$ (resp. $O_{\boldsymbol{g},G}$ be the braid orbit (resp. G orbit) of $\boldsymbol{g} \in S$. If two elements $\boldsymbol{g}_1, \boldsymbol{g}_2 \in S$ have $O_{\boldsymbol{g}_1} = O_{\boldsymbol{g}_2}$, then there is a braid that connects $\boldsymbol{g}_1$ and $\boldsymbol{g}_2$. So, this braid is in G: $O_{\boldsymbol{g}_1,G} = O_{\boldsymbol{g}_2,G}$. This finishes the first paragraph.

Lem. 5.2 and Lem. 5.5 gives a braid of any element of $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$ to $T_{\ell,\pm\pm,1-\deg}$. Prop. 5.6 shows K^* consists of the elements that map any one element of $T_{\pm\pm}$ into the same set. So, the orbits of $T_{\ell,\pm\pm,1-\deg}$ under K^* correspond to the braid orbits on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$. □

We seek braid orbits on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$ by producing braids between elements – with the same lift invariant – of $T_{\ell,\pm\pm,1-\deg}$. We can start with a 1-degenerate with a particular lift invariant in $T_{\pm\pm}$ using Prop. 4.19. Then, apply Prop. 5.6 to get new elements in $T_{\pm\pm}$. Finally, for each of these apply Lem. 5.2 or 5.5 as appropriate to get new 1-degenerates. Eventually this process of forming K^* *chains on* $T_{\ell,\pm\pm,1-\deg}$ ends.

REMARK 5.8. For $\boldsymbol{g} \in \mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ as in (5.5), a more general condition than $g_1 = \alpha_0$ in 1-degeneracy assumes $g_1 = {}_{\boldsymbol{v}_1}\alpha_0$, and $\boldsymbol{v}_1, \dots, \boldsymbol{v}_4$ are translates by a fixed $\boldsymbol{v}'$ of generators of a line (copy of $\mathbb{Z}/\ell^{k+1}$) in $V_{\ell^{k+1}}$.

5.3. Characterizing H-M **and double identity rep. orbits.** Braid orbits on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3-3})^{\mathrm{rd}}$ correspond to K^* chains on $T_{\ell,\pm\pm,1-\deg}$ (Rem. **??**). Cor. 5.9 reveals much of that. As in (5.1), K_ℓ is $\frac{\ell\pm1}{6}$ for $\ell \equiv \mp 1 \mod 3$. We use the multiplicative notation for the lift invariant as in (4.10) with $\zeta_n = e^{2\pi \mathrm{i}/n}$.

COROLLARY 5.9. *The following table breaks* $T_{\ell,\pm\pm,1-\deg}$ *into two types.*

(5.15a) $\frac{K_\ell(\ell-1)}{2}$ *elements of* $T_{\ell,\pm\pm,1-\deg}$ *are* H-M *(resp. shifts of* H-M*) reps.*

(5.15b) *Excluding* (5.15a) *there are* $K_\ell(\ell-1)^2$ *elements in* $T_{\ell,+-+-,1-\deg}$.

Suppose we know the following.

(5.16) *The braid orbit containing a particular double identity rep. intersects* $T_{\ell,\pm\pm,1-\deg}$ *in* $K_\ell(\ell-1)$ *elements.*

Then, we also know the following.

(5.17a) *The elements of* $T_{\ell,\pm\pm,1-\deg}$ *with trivial lift invariant are either* H-M *or shift of* H-M*reps.*

(5.17b) *The elements with a particular lift invariant fall in one braid orbit given by a double identify rep. (with that lift invar. value).*

Now take $k \geq 0$ *and* $\boldsymbol{g} \in T_{\pm\pm}$. *If* $s_{\ell^{k+1}}(\boldsymbol{g}) = \zeta_{\ell^{k+1}}^j$, *then,* $s_{\ell^{k+1}}(I_2(\boldsymbol{g})) = \zeta_{\ell^{k+1}}^{-j}$.

PROOF. We make the count in (5.17a). For $\ell \equiv 2 \mod 3$, if for $\boldsymbol{g}$, g_2 is α_0^{-1}. Then, $g_3 = {}_{\boldsymbol{v}_3}\alpha_0$, $\boldsymbol{v}_3 \in V_\ell \setminus \{\mathbf{0}\}$ and $g_4 = g_3^{-1}$. As in Lem. 4.11, there are $\frac{\ell^2-1}{6}$ reduced classes from modding out by the action of α and $\mathbf{sh}^2$. These are all H-M reps. and so have trivial lift invariant. Similarly, if $g_4 = \alpha_0^{-1}$, for which the resulting Nielsen rep. is the shift of an H-M rep.

Now count the elements where $g_2 = {}_{\boldsymbol{v}_2}\alpha_0^{-1}$ with $\boldsymbol{v}_2 \in V_\ell \setminus \{\mathbf{0}\}$ and $g_4 = {}_{\boldsymbol{v}_4}\alpha_0^{-1}$, with $\boldsymbol{v}_4 \in \langle \boldsymbol{v}_2 \rangle \setminus \{\mathbf{0}\}$. Our conditions exclude H-M and shift of H-M reps. Given a particular $\boldsymbol{v}_2 \neq \mathbf{0}$, there are $\ell-1$ choices for $\boldsymbol{v}_4 \neq \mathbf{0}$ that are non-zero multiples of $\boldsymbol{v}_2$, for a total of $\frac{(\ell^2-1)(\ell-1)}{6}$ (dividing out by the action of α_0 and $\mathbf{sh}^2$). These numbers agree with (5.15).

Now consider $\ell \equiv 1 \mod 3$. For the H-M case, avoid choosing $\boldsymbol{v}_3$ as one of the $2\ell-1$ elements that might be in eigenspaces for α, so there are $(\ell-1)^2$ choices.

Similarly for the complementary set, avoid taking $\boldsymbol{v}_2$ among those $2\ell-1$ eigenvectors of α, but then multiply those choices by the $\ell-1$ possible values in $\langle \boldsymbol{v}_2\rangle \setminus \{\mathbf{0}\}$.

Now assume (5.16) holds. Then, multiplying by the $\ell-1$ values of the lift invariant, there are a total of $K_\ell(\ell-1)^2$ distinct elements in the braid orbits of double identity elements, so they must include the complete set of elements in (5.15b), which we now know would have nontrivial lift invariant. The only elements left are the H-M and shift of H-M reps. listed in (5.15b), which we now know give all classes with trivial lift invariant in $T_{\ell,\pm\pm,1-\deg}$.

Now we conclude the lemma. From (4.10),

$$s_{\ell^{k+1}}(I_2(\boldsymbol{g})) = (\hat{g}_4)^{-1}(\hat{g}_3)^{-1}(\hat{g}_1)^{-1}(\hat{g}_1)^{-1} = (s_{\ell^{k+1}}(\boldsymbol{g}))^{-1}.$$

This is equivalent to the last sentence of the lemma. □

We can use Prop. 4.19 to compute – from its entries – the lift invariant of any element in the Nielsen class. An effective result follows by applying Lems. 5.2 and 5.5 by restricting how that works on 1-degenerate Nielsen reps. Use the notation $f(\boldsymbol{w})$ for the lift invariant of $\boldsymbol{w} = (x, y)$ as in (4.25). This is the z-value in the Heisenberg group, so the additive form in Lem. 5.10 is correct.

To the notation simple, we restrict in Lem. 5.10 to calculating the lift invariant of a 1-degenerate element. The same idea effectively calculates the lift invariant of any element of the Nielsen class. We use $I_2(\boldsymbol{w})$ as in (5.8b).

LEMMA 5.10. *Assume $\boldsymbol{v} \in V_\ell$ is not an α eigenvector. The lift invariant of*

$$\boldsymbol{\alpha}_{\boldsymbol{v},m} \stackrel{\text{def}}{=} (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{m\boldsymbol{v}}\alpha_0, {}_{(m-1)\boldsymbol{v}}\alpha_0^{-1}) \text{ is } f(-m\boldsymbol{v}^{\alpha}) - f(-m\boldsymbol{v}^{\alpha}-\boldsymbol{v}^{\alpha^{-1}}). \tag{5.18}$$

In particular, for each lift invariant value $\zeta \in (\mathbb{Z}/\ell)^*$ and each $\boldsymbol{v} \in V_\ell$, there is a unique m for which $\boldsymbol{\alpha}_{\boldsymbol{v},m}$ is in Nielsen class and has ζ as lift invariant. So, these give all the 1-degenerate elements with that lift invariant.

PROOF. Braids preserves the lift invariant. So, the lift invariant of

$$({}_{\boldsymbol{v}^{\alpha^{-1}}}\alpha_0^{-1}, \alpha_0, {}_{m\boldsymbol{v}}\alpha_0, {}_{(m-1)\boldsymbol{v}}\alpha_0^{-1}) \tag{5.19}$$

is the same. Between the 3rd and 4th terms of (5.19) juxtapose $({}_{-m\boldsymbol{v}^{\alpha}}\alpha_0, {}_{-m\boldsymbol{v}^{\alpha}}\alpha_0^{-1})$, an element with its inverse. Conclude: this 6-tuple Nielsen class element has the same lift invariant as does (5.18). Now, apply the shift to see the lift invariant as the product of the lift invariants of two 3-tuples satisfying product 1:

$$(\alpha_0, {}_{m\boldsymbol{v}}\alpha_0, {}_{-m\boldsymbol{v}^{\alpha}}\alpha_0) \text{ and, as in (5.12), } I({}_{\boldsymbol{v}^{\alpha^{-1}}}\alpha_0, {}_{(m-1)\boldsymbol{v}}\alpha_0, {}_{-m\boldsymbol{v}^{\alpha}}\alpha_0). \tag{5.20}$$

Use that $\boldsymbol{v}^{\alpha^{-1}}$ is $-\boldsymbol{v}-\boldsymbol{v}^{\alpha}$ after conjugating the 2nd 3-tuple by $-\boldsymbol{v}^{\alpha^{-1}}$. The result is

$$I_2(\alpha_0, {}_{m\boldsymbol{v}+\boldsymbol{v}^{\alpha}}\alpha_0, {}_{-m\boldsymbol{v}^{\alpha}-\boldsymbol{v}^{\alpha^{-1}}}\alpha_0).$$

Now apply formula (4.25) to establish the lemma.

For each given $\boldsymbol{v}$ as above, the expression

$$F(\boldsymbol{v}, m) \stackrel{\text{def}}{=} f(-m\boldsymbol{v}^{\alpha}) - f(-m\boldsymbol{v}^{\alpha}-\boldsymbol{v}^{\alpha^{-1}})$$

is at most quadratic in m. By inspection, the degree 2 terms in m vanish. Therefore, $F(\boldsymbol{v}, m)$ has degree 1 in m. Setting it equal to ζ therefore gives a unique solution for m. The corresponding $(\boldsymbol{v}, m)$ gives a 1-degenerate Nielsen class element. We already know all of them have the form $\boldsymbol{\alpha}_{\boldsymbol{v},m}$. □

5.4. Braid orbits for $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$, $\ell \neq 2, 3$. Prop. 6.3 and Prop. 6.8 computes the braid orbits. These explicit results contend with all issues that have to-date occurred in computing braid orbits.

5.4.1. *Setup for finding braid orbits.* The following is immediate. Suppose O is a braid orbit on a Nielsen class, and β is a $\mathbf{C}$ preserving outer automorphism of G. Then, applying β to O gives another braid orbit O' in the same Nielsen class.

If $\boldsymbol{g} \in O$ has $g_j = g_i^u$, for some integer u and some $i \neq j$, then, applying β to $\boldsymbol{g}$ gives $\boldsymbol{g}'$ where $g'_j = (g'_i)^u$.

Definition 5.11. With the above notation, call β *braidable* on O if $O = O'$.

Lemma 5.12. *The outer automorphism from S_3, acting by conjugation on A_3, extends to an automorphism of $H_{\ell^{k+1}}$. Its extension, though, sends commutators in $H_{\ell^{k+1}}$ to their inverses.*

Proof. With no loss take the automorphism β from S_3 to be conjugation by $(1\,2)$. Then, β maps $\alpha = (1\,2\,3)$ to its inverse. When we extend β to S_3 (the special case $n = 3$ in §A.1) if, as in §4.2.1, we use $A^* = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ for the action of $\alpha = (1\,2\,3)$, then we can use $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ for the action of β. Extend β to $H_{\ell^{k+1}}$ by sending $M(x, y, z)$ to $M(y, x, -z)$. Apply this formula to the commutator expression in (4.9) to see the final statement. □

If $\boldsymbol{g} \in T_{\pm\pm}$ (resp. T_{++--}) then $\mathbf{sh}^2$ (resp. $q_1 q_3^{-1}$) fixes its type. Otherwise, no element of $\mathcal{Q}''$ fixes the type of $\boldsymbol{g}$. In dealing with reduced classes, we may mod out by the action of $\mathcal{Q}''$. Any configuration type is reduced equivalent to one with $+$ in the 1st position. We make that assumption.

Denote by $\mathcal{O}_{\text{H-M},\ell^{k+1}}$ (resp. $\mathcal{O}_{\text{D-E},\ell^{k+1}}$) those braid orbits in $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ containing H-M (resp. double identity) reps. From Prop. 4.19 there is no overlap between $\mathcal{O}_{\text{H-M},\ell^{k+1}}$ and $\mathcal{O}_{\text{D-E},\ell^{k+1}}$. For any $\boldsymbol{g} \in \mathrm{Ni}(G_{\ell^{k+1}}\mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$, even if it is not the shift of an H-M rep., its reduction $\bmod \ell^t$, $1 \leq t \leq k$, may be.

Definition 5.13. Let $i_{\text{H-M},\boldsymbol{g}}$ be the maximal integer – its H-M *index* – such that $\boldsymbol{g} \bmod \ell^{i_{\text{H-M},\boldsymbol{g}}}$ is the shift of an H-M rep. Set this to 0 if there is no such value.

When $r = 4$ we must consider the difference between the orbit widths of q_2 (resp. γ_∞; cusp widths) on inner (resp. reduced) Nielsen classes. This topic is called q_2 *orbit shortening* in [**BFr02**, §7.2.3]. The widths are the same on a given q_2 orbit if and only if $\mathcal{Q}''$ equivalences no two elements the orbit. In our case, Prop. 5.14 shows there is no q_2 orbit shortening. That puts less of a burden on computing braid orbits, since it makes the easier to compute q_2 orbits longer.

Proposition 5.14. *For $\boldsymbol{g} \in (T_{\pm\pm} \cup T_{++--}) \cap \mathrm{Ni}(G_{\ell^{k+1}}\mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$, its middle product order,* $\mathrm{ord}(\mathbf{mp}(\boldsymbol{g}))$*, is $\ell^{k+1-t_{\text{H-M},\boldsymbol{g}}}$; and its q_2 orbit width is twice that.*

For $\boldsymbol{g} \in T_{+--+} \cap \mathrm{Ni}(G_{\ell^{k+1}}\mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$, its q_2 orbit width is 1 (resp. 6) if $\boldsymbol{g}$ is (resp. is not) a double identity rep. with repeating elements at positions 2 and 3.

For all elements in H-M *or double identity braid orbits, their q_2 orbit widths are also their cusp widths.*

Proof. The calculation for T_{++--} is similar to that for $T_{\pm\pm}$. We do just the latter. Write a typical element in $T_{\pm\pm}$ as

$$\boldsymbol{g} \stackrel{\text{def}}{=} \boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = (\alpha_0, \boldsymbol{v}_2\alpha_0^{-1}, \boldsymbol{v}_3\alpha_0, \cdot).$$

Then, $\mathbf{mp}(\boldsymbol{g} \bmod \ell^t)$ is

$$\boldsymbol{v}_2 - \boldsymbol{v}_2^{\alpha} + \boldsymbol{v}_3^{\alpha} - \boldsymbol{v}_3, \text{ which has order } \ell^u \text{ for some } u.$$

So, $\mathbf{mp}(\boldsymbol{g} \bmod \ell^t)$ has order 1 if and only if $\boldsymbol{g} \bmod \ell^t$ is the shift of an H-M rep., or $u \geq t$. For $t \leq u$, $\mathbf{mp}(\boldsymbol{g}) \bmod \ell^t$ has order 1. That makes $u = k+1-i_{\text{H-M},\boldsymbol{g}}$.

Prop. 2.10 gives the precise width, $o_{\boldsymbol{g}}$, of the q_2^2 orbit on $\boldsymbol{g}$. It also tells when $o_{\boldsymbol{g}}$ is also the q_2 orbit width: when $o_{\boldsymbol{g}}$ is odd and $(g_2g_3)^{\frac{o-1}{2}}g_2$ has order 2. Since $|G_{\ell^{k+1}}|$ is odd, the second condition fails. Otherwise, the q_2 orbit width is $2o_{\boldsymbol{g}}$.

Now consider $\boldsymbol{g} \in T_{\pm\mp}$. Here (Lem. 4.1) the order of the middle product is 3. Then, the q_2 orbit width is 6, from the above, unless $\langle g_2\rangle = \langle g_3\rangle$ which implies we have a double element rep. (as in (1.3)). Conclude by noting we have recorded the middle product in each case.

Rem. 5.15 – which has notation we will use later – shows why there is no q_2 orbit shortening (by $\mathcal{Q}''$). In the cases noted there, the contradictions are to the assumptions under the conditions that the parameter k is even (since $v/2$ is odd) or odd (since $v/4$ is not an integer). That concludes the proposition. □

REMARK 5.15. [**BFr02**, §7.2.3] introduces notation for a γ_∞ orbit of $\boldsymbol{g}$ in an inner, reduced Nielsen class: ${}_{\mathbf{c}}O_{u,v/m,*}$. Here u is $o_{\boldsymbol{g}}$, the q_2^2 orbit width (as in the proof of Prop. 5.14), v is the q_2 orbit width, m is a factor indicating any orbit shortening from $\mathcal{Q}''$ and * indicates a slot for extra decoration if necessary.

If the length of the $\mathcal{Q}''$ orbits is 4 (maximal), then the orbit shortening amounts to finding if there is a $0 < k < v$ for which the inner classes of $(\boldsymbol{g})q_2^k$ is inner equivalent to $(\boldsymbol{g})q'$ for some nontrivial $q' \in \mathcal{Q}''$. [**BFr02**, Lem. 7.7] says if k is even, then $k = v/2$. This is based on the action of $\mathcal{Q}''$ commuting with q_2^k if k is even. If k is odd, the lemma uses that $\mathcal{Q}''$ is a normal subgroup of H_4, and conjugation by q_2 has a nontrivial action. So, for example, if $q' = q_1q_3^{-1}$ we find $k = v/4$.

5.4.2. *Process for finding braid orbits.* As in Cor. 5.9, $T_{\ell,\pm\pm,1-\deg}$ is the 1-degenerate elements in $T_{\pm\pm}$. As in (5.1), K_ℓ is $\frac{\ell\pm1}{6}$ for $\ell \equiv \mp 1 \mod 3$.

Prop. 6.3 shows the intersection of the orbits of H-M reps. with $T_{\ell,\pm\pm,1-\deg}$ consists of H-M and shift of H-M reps. The result depends on putting together the following ingredients. Use the notation of (4.19) for H-M, shift of H-M and double identity reps. For example, denote the H-M rep. $(\alpha_0, \alpha_0^{-1}, {}_{\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1})$ by ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$.

Denote the image of $\langle q_2^2, q_3^2\rangle$ in $\bar{M}_4$ by $K^*_{q^2}$. Cor. 5.9 says that to capture the braid orbits in $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$ we have only to show the items of (5.21) hold.

- (5.21a) K^* orbits of H-M reps. intersect $T_{\ell,\pm\pm,1-\deg}$ entirely in H-M and shift of H-M reps. and $\mathbf{sh}q_1q_3^{-1}$ joins pairs of $K^*_{q^2}$ orbits (see (5.15a)).
- (5.21b) In (5.21a) there are a total of K_ℓ braid orbits each of length $2(\ell-1)$.
- (5.21c) As in (5.16), a double identity K^* orbit – according to (4.21), the same as a $K^*_{q^2}$ orbit – intersection with $T_{\ell,\pm\pm,1-\deg}$ has length $K_\ell(\ell-1)$.
- (5.21d) K^* joins nothing in $T_{\ell,\pm\pm,1-\deg}$ beyond (5.21b) and (5.21c).

For $\ell \equiv 2 \mod 3$, $\boldsymbol{g}' \in T_{\pm\pm}$ has a unique $m_i \stackrel{\text{def}}{=} m_{i,\boldsymbol{g}'} \mod \ell$ with

$$(\boldsymbol{g}')q_i^{2m_i} \in T_{\ell,\pm\pm,1-\deg}, i = 2,3 \text{ (Lem. 5.2)}. \tag{5.22}$$

For $\ell \equiv 1 \mod 3$, Lem. 5.5 gives (5.22) only for $i = 3$ (resp. $i = 2$) for $\boldsymbol{g}' = (\alpha_0, {}_{\boldsymbol{v}_2}\alpha^{-1}, {}_{\boldsymbol{v}_3}\alpha^{-1}, {}_{\boldsymbol{v}_4}\alpha^{-1})$ if both $\boldsymbol{v}_2$ and $\boldsymbol{v}_3$ (resp. $\boldsymbol{v}_3$ and $\boldsymbol{v}_4$) are α eigenvectors.

DEFINITION 5.16. When $\boldsymbol{g}' = (\boldsymbol{g})q_2^{2u_2}$, refer to $2u_3 \stackrel{\text{def}}{=} 2u_{3,\boldsymbol{g}'}$ as the exponent *complement* to $(\boldsymbol{g}, q_2^{2u_2})$; and $((\boldsymbol{g})q_2^{2u_2})q_3^{2u_3}$ merely its *complement*, when $0 < u_2 < \ell$. Use the same names with 2 and 3 switched in the various sub and super scripts.

In strings of computations we often use $(\boldsymbol{g}, q_2^{2u_2}, q_3^{2u_3})$, and variants, as clearer notation for the complement $((\boldsymbol{g})q_2^{2u_2})q_3^{2u_3}$. Prop. 6.8 completes the description of the level 0 braid orbits by showing (5.21c) and (5.21d).

6. Separating H-M and Double Identity orbits by lift invariants

This section has our main technical results on braid orbits for the Nielsen classes $\text{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ Rem. 4.9 tells how the lift invariant in many alternating group Nielsen classes gives us a precise listing of braid orbits. [,] takes those alternating group examples and corroborates the abstract results of [], in a way so explicit, that it really makes you think that there might be a compelling statement RETURN

The hardest point in establishing the braid orbits on the level $k = 0$ Nielsen classes is concluding that the elements with a given nontrivial lift invariant fall in one braid orbit. There is a simplifying statement about 1-degenerate elements – of form $\boldsymbol{\alpha}_{\boldsymbol{v},m} \stackrel{\text{def}}{=} (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{m\boldsymbol{v}}\alpha_0, {}_{(m-1)\boldsymbol{v}}\alpha_0^{-1})$ as in (5.18), with $m-1$ not 0. Here is the heart of Prop. 6.8, holding for a given braid orbit O restricted to T_{+-+-}.

(6.1a) In the Nielsen class with no equivalence, each $\boldsymbol{v} \in V_\ell$, not an α eigenvector, appears in O as an element $\boldsymbol{\alpha}_{\boldsymbol{v},m}$ *exactly once*.

(6.1b) There are exactly K_ℓ reduced Nielsen classes corresponding to a given value of $m-1 \in (\mathbb{Z}/\ell)^*$.

Prop. 6.3 describes the orbits of H-M reps. Then, Prop. 6.5 shows (6.1) holds, and computes the complements of the elements.

6.1. 1-degenerate elements with trivial lift invariant. First we consider the H-M and shift of H-M elements. Recall Def. 5.1 for K_ℓ.

LEMMA 6.1. *The argument just before Lem. 4.1 shows there are $K_\ell(\ell-1)\ell^{2k}$ reduced inner* H-M *reps. Applying* $\mathbf{sh}^2$ *maps $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ to $\boldsymbol{g}_{-\boldsymbol{v}_2,-\boldsymbol{v}_3}$. It preserves $T_{\ell^{k+1},\pm\pm,1-\deg}$.*

If $\boldsymbol{g} \in T_{\ell^{k+1},\pm\pm,1-\deg}$ is (resp. is not) an H-M *rep., then its q_3^2 orbit has length 1 (resp. ℓ^{k+1}). Further, there is at most one 1-degenerate Nielsen rep. in this orbit.*

According to, there are $\frac{\ell^4-1}{2}$ reduced Nielsen reps. in the union of all double identity and H-M *braid orbits. We can count these by taking the reduced elements in $T_{\pm\pm}$ and multiplying by 3.*

Therefore the totality of reduced classes, $\mathcal{N}_1$, represented by applying (iterates of) q_3^2 to 1-degenerate Nielsen reps. is $\frac{(\ell^2-1)(1+\ell^2)}{6}$. Multiply by 3 to count the distinct reduced Nielsen classes, $\mathcal{N}_2$, from adding to $\mathcal{N}_1$ the classes from applying q_2 and q_3 to $\mathcal{N}_1$. The result is $\frac{c_\ell}{2}$, as in Lem. 4.12.

PROOF. The set of reduced elements of $T_{\pm\pm}$ are mapped to reduced elements, respectively, in T_{++--} (resp. T_{+--+}) by q_3 (resp. q_2). That gives the second sentence of the first paragraph.

If $\boldsymbol{g} \in T_{+-+-}$, then the effect of q_3^2 on it is by conjugating (g_3, g_4) by powers of g_3g_4. Calculate:

$$g_3g_4 = \boldsymbol{v}_3 - \boldsymbol{v}_3^{\alpha^{-1}} + \boldsymbol{v}_4^{\alpha^{-1}} - \boldsymbol{v}_4 = (\boldsymbol{v}_3 - \boldsymbol{v}_4)^{1-\alpha^{-1}}.$$

So long as $\boldsymbol{v}_3 \neq \boldsymbol{v}_4$ (that is $\boldsymbol{g}$ is not an H-M rep.), then no nontrivial iteration of $1-\alpha^{-1}$ maps $\boldsymbol{v}_3-\boldsymbol{v}_4$ into $\langle \boldsymbol{v}_3-\boldsymbol{v}_4\rangle$. Further, since all these elements have the same first two entries, they are reduced inequivalent to each other.

There are (ℓ^2-1) nonzero choices for $\boldsymbol{v}_2$. For any one of these there are ℓ choices for $\boldsymbol{v}_3$ that give 1-degenerate elements in $T_{\pm\pm}$. If $\boldsymbol{v}_2 = \boldsymbol{0}$, then there are (ℓ^2-1) choices for $\boldsymbol{v}_3$ that give 1-degenerate Nielsen reps. in $T_{\pm\pm}$. In each case divide these numbers by 6 to get the corresponding count of the reduced Nielsen classes, but then consider this set and the application of q_2 and q_3 to get a total count of assured reduced Nielsen classes equal to $\frac{c_\ell}{2}$. □

RETURN

LEMMA 6.2. *If you apply $q_1q_3^{-1}$ to an* H-M *rep. ${}_{\boldsymbol{w}}\boldsymbol{g}$, and then apply* $\mathbf{sh}$*, you get the shift of an* H-M *rep., also in $T_{\ell^{k+1},\pm\pm,1-\deg}$. That gives $\frac{\ell^2-1}{3}$ 1-degenerate reps. Similarly, for $\ell \equiv 1 \mod 3$, you get $\frac{(\ell-1)^2-1}{3}$ 1-degenerate reps. in* H-M *orbits this way.*

Also, $\mathbf{sh}\, q_1q_3^{-1}$ sends an H-M *rep. shift to an* H-M *rep. (in $T_{\ell^{k+1},\pm\pm,1-\deg}$). These give the precise ways $\mathbf{sh}\, q_1q_3^{-1}$ or $q_1q_3^{-1}\mathbf{sh}$ map elements of $T_{\ell^{k+1},\pm\pm,1-\deg}$ into $T_{\ell^{k+1},\pm\pm,1-\deg}$.*

PROOF. The effect of $\mathbf{sh}^2$ on $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ is to send it to

$$(\alpha_0, \boldsymbol{v}_4-\boldsymbol{v}_3\alpha_0^{-1}, -\boldsymbol{v}_3\alpha_0, \boldsymbol{v}_2-\boldsymbol{v}_3\alpha_0^{-1}).$$

Use that $\boldsymbol{v}_2 - \boldsymbol{v}_3 + \boldsymbol{v}_4 = \boldsymbol{0}$ to conclude the first statement. The next statement is also a simple direction calculation except the last sentence. That will follow if $q_1q_3^{-1}$ applied to a 1-degenerate

$$(6.2)\quad {}_{\boldsymbol{v}}\boldsymbol{g} = (\alpha_0, \boldsymbol{v}\alpha_0^{-1}, {}_{m_3\boldsymbol{v}}\alpha_0, {}_{m_4\boldsymbol{v}}\alpha_0^{-1}), \text{ neither H-M nor the shift of an H-M rep.,}$$

is not 1-degenerate. The conditions are $m_4 \neq 0$, $\boldsymbol{v}$ is not an eigenvector for α and $1 - m_3 + m_4 = 0$. It suffices to show that this applies to

$$(q_1q_2q_3)^{-1}q_1q_3^{-1} = (q_3q_2q_3)^{-1}$$

or its inverse, $q_3q_2q_3$, equal to $Q_{2,3} = q_2q_3q_2$ as a braid. Apply $Q_{2,3}$ to ${}_{\boldsymbol{v}}\boldsymbol{g}$ to get

$$(\alpha_0, \bullet, {}_{\boldsymbol{v}^{\alpha^{-1}}-(1-m_3)\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}).$$

As $\boldsymbol{v}^{\alpha^{-1}}$ and $\boldsymbol{v}$ span different subspaces, the result can't be 1-degenerate. □

RETURN 02/03/14

PROPOSITION 6.3 (Precise H-M orbits). *From* (4.20)*, $\mathbf{sh}\, q_1q_3^{-1}$ toggles* H-M *and shift of* H-M *reps. The complement of $(\boldsymbol{v},3,4\boldsymbol{g}, q_2^{2u_2})$ (resp. $(\boldsymbol{v},2,3\boldsymbol{g}, q_3^{2u_3'})$) is*

$$(6.3)\quad (\boldsymbol{v},3,4\boldsymbol{g}, q_2^{2u_2}, q_3^{2u_3}) \text{ (resp. } (\boldsymbol{v},2,3\boldsymbol{g}, q_3^{2u_3'}, q_2^{2u_2'}),\ u_3 \equiv (3u_2)^{-1} \mod \ell$$
$$\text{(resp. } u_2' \equiv (3u_3')^{-1} \mod \ell) \text{ a shift of an H-M (resp. H-M) rep.}$$

That establishes (5.21a)*.*

For $1 < u_2 < \ell$, the complement of $(\boldsymbol{v},3,4\boldsymbol{g}, q_2^{2u_2})$ is the same as for $(\boldsymbol{v},3,4\boldsymbol{g}, q_2^{2\ell-2u_2})$.

For any $\boldsymbol{v} \in V_\ell$, not an α eigenvalue, 1-degenerates in the braid orbit of ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$ are the $2(\ell-1)$ elements ${}_{t\boldsymbol{v},3,4}\boldsymbol{g}$, $t \in (\mathbb{Z}/\ell)^*$ and their shifts. That establishes (5.21b)*.*

PROOF. To show (6.3) we produce the complement of $({}_{\boldsymbol{v},3,4}\boldsymbol{g}, q_2^{2u_2})$:

$$(\alpha_0, {}_{u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})}\alpha_0^{-1}, {}_{\boldsymbol{v}+u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})}\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}).$$

The product of the 3rd and 4th entries is $u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})-u_2(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})$. Since $\boldsymbol{v}+\boldsymbol{v}^\alpha+\boldsymbol{v}^{\alpha^{-1}}$ is $\mathbf{0}$, this gives $-3u_2\boldsymbol{v}$. The effect, therefore of applying q_3^{2u} is to change the 4th entry to ${}_{\boldsymbol{v}-3u_2u\boldsymbol{v}}\alpha_0^{-1}$. Choose u_3 so that

$$1-3u_2u_3\equiv 0 \mod \ell, \text{ or } u_3\equiv (3u_2)^{-1} \mod \ell.$$

The other case of (6.3) is similar.

The complement $({}_{\boldsymbol{v},3,4}\boldsymbol{g}, q_2^{2u_2}, q_3^{2u_3})$ is

$$(\alpha_0, {}_{u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})}\alpha_0^{-1}, {}_{u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})}\alpha_0, \alpha^{-1}) : \tag{6.4}$$

the same as $({}_{\boldsymbol{v},3,4}\boldsymbol{g}, q_2^{2\ell-2u_2}, q_3^{2u_3})$, precisely because $u_2^2\equiv(\ell-u_2)^2 \mod \ell$.

Prop. **??** says that any chain from ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$ to another element $\boldsymbol{g}_2\in T_{\ell,\pm\pm,1-\deg}$ is 1-degenerate. So, to understand what in $T_{\ell,\pm\pm,1-\deg}$ is in the braid orbit of ${}_{\boldsymbol{v},3,4}\boldsymbol{g}$, from the above we have only to iterate twice what (6.3) gives.

The first iterate gives (6.4), which is ${}_{\boldsymbol{w},2,3}\boldsymbol{g}$ with $\boldsymbol{w}=u_2(\boldsymbol{v}^\alpha-\boldsymbol{v})$. The second iterate $({}_{\boldsymbol{w},2,3}\boldsymbol{g}, q_3^{2u_3'}, q_2^{2u_2'})$ is

$$(\alpha_0, \alpha_0^{-1}, {}_{u_3'(\boldsymbol{w}-w^{\alpha^{-1}})}\alpha_0, {}_{u_3'(\boldsymbol{w}-w^{\alpha^{-1}})}\alpha_0^{-1}).$$

The subscripts on the 3rd and 4th entries are

$$u_3'u_2(\boldsymbol{v}^\alpha-\boldsymbol{v}-(\boldsymbol{v}^\alpha-\boldsymbol{v})^{\alpha^{-1}}) = 3u_3'u_2\boldsymbol{v}.$$

The result is that 1-degenerate chains of length 2 applied to starting at ${}_{\boldsymbol{v},3,4}$ end up back at ${}_{t\boldsymbol{v},3,4}\boldsymbol{g}$ running over all $t\in(\mathbb{Z}/\ell)^*$, passing length 1, 1-degenerate chains of elements of form ${}_{\boldsymbol{w},2,3}\boldsymbol{g}$. By their form, any even length 1-degenerate chains will contribute nothing beyond the length 2 chains. This establishes (5.21b) by applying the same division by 6 to $k+1$ elements that are in $V_\ell\setminus\{\mathbf{0}\}/(\mathbb{Z}/\ell)^*$ that appears in our previous equivalences from modding out by the action of $\mathbf{sh}^2$ and $\langle\alpha\rangle$. □

6.2. ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ **orbits.** For ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ to be a Nielsen class element requires $\boldsymbol{v}$ is not an α eigenvector. Still, the formulas below apply to $\ell\equiv 2 \mod 3$, except, in lieu of Prop. 5.6, there won't be a complement for $i=2$ (resp. $i=3$) precisely when

(6.5) in the 2nd (resp. 4th) entry, ${}_{\boldsymbol{w}}g$, of $({}_{\boldsymbol{v},1,3}\boldsymbol{g})q_2^{u_2}$ (resp. $({}_{\boldsymbol{v},1,3}\boldsymbol{g})q_3^{u_3'}$), $\boldsymbol{w}$ is an α eigenvector.

Lem. 6.4 computes how $q_2^{2u_2}q_3^{2u_3}$ and $q_3^{2u_3'}q_2^{2u_2'}$ act on ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$. It also shows precisely when (6.5) holds.

LEMMA 6.4. *The action of $q_2^{2u_2}$ (resp. $q_3^{2u_3'}$) on ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ gives:*

$$\begin{array}{ll} & (\alpha_0, {}_{u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha)+\boldsymbol{v}}\alpha_0^{-1}, {}_{u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha)}\alpha_0, {}_{-\boldsymbol{v}}\alpha_0^{-1}) \\ (\textit{resp.} & (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})}\alpha_0, {}_{u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})-\boldsymbol{v}}\alpha_0^{-1})). \end{array} \tag{6.6}$$

There is a (q_2,u_2) (resp. (q_3,u_3')) where (6.5) *holds if and only if*

$$\ell=1 \mod 3 \text{ and } u_2(\textit{resp. } u_3') \textit{ satisfies } 3u^2+3u+1(\textit{resp. } 3u^2-3u+1). \tag{6.7}$$

Note: (6.7) *is independent of $\boldsymbol{v}$. The effect of $q_3^{2u_3}$ (resp. $q_2^{2u_2'}$) on the respective terms of* (6.6) *appears in* (6.8) *and* (6.9).

$$\begin{array}{l} (\alpha_0, {}_{(2u_2+1)\boldsymbol{v}+u_2\boldsymbol{v}^{\alpha^{-1}}}\alpha_0^{-1}, \\ {}_{(u_3(3u_2+1)+2u_2)\boldsymbol{v}+(u_2-u_3)\boldsymbol{v}^{\alpha^{-1}}}\alpha_0, {}_{(u_3(3u_2+1)-1)\boldsymbol{v}-u_3\boldsymbol{v}^{\alpha^{-1}}}\alpha^{-1}). \end{array} \tag{6.8}$$

$$(\alpha_0, {}_{(1+2u_2'-3u_2'u_3')\boldsymbol{v}+u_2'\boldsymbol{v}^{\alpha^{-1}}}\alpha_0^{-1}, \quad {}_{(2u_2'+u_3'-3u_2'u_3')\boldsymbol{v}+(u_2'-u_3')\boldsymbol{v}^{\alpha^{-1}}}\alpha_0, {}_{(u_3'-1)\boldsymbol{v}-u_3'\boldsymbol{v}^{\alpha^{-1}}}\alpha_0^{-1}). \tag{6.9}$$

Proof. Easily check (6.6). If $u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha)+\boldsymbol{v}=\boldsymbol{w}$ is an α eigenvector, then

$$u_2(2\boldsymbol{v}^\alpha+\boldsymbol{v})+\boldsymbol{v}^\alpha = m(u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha)+\boldsymbol{v}), \text{ using } \boldsymbol{v}+\boldsymbol{v}^\alpha+\boldsymbol{v}^{\alpha^{-1}}=\boldsymbol{0}.$$

Independence of $\boldsymbol{v}$ and $\boldsymbol{v}^\alpha$ implies $mu_2+2u_2+1=0$ and $mu_2+m-u_2=0$. Add u_2m to both sides to conclude $2u_2+1=m-u_2$, or $m=3u_2+1$ and $3u_2^2+3u_2+1=0$.

There can be no complement if $\boldsymbol{w}$ is an α eigenvector since applying $q_3^{2u_3}$ to ${}_{\boldsymbol{v},1,3}\boldsymbol{g})q_2^{u_2}$ wouldn't change that the result could not be 1-degenerate.

Rewrite $3u^2+3u+1 \equiv 0 \mod \ell$ as $3(u+\frac{1}{2})^2+\frac{1}{4} \equiv 0$. This has a solution $u \mod \ell$, if and only if -3 is a quadratic residue mod ℓ. As $(-1)^{(\frac{3-1}{2})(\frac{\ell-1}{2})}=(-1)^{\frac{\ell-1}{2}}$, quadratic reciprocity shows having a solution is equivalent to

$$(-1)^{\frac{\ell-1}{2}}(-1)^{\frac{\ell-1}{2}}\left(\frac{\ell}{3}\right)=\left(\frac{\ell}{3}\right)=1.$$

Clearly, ℓ is a square mod 3 if and only if $\ell \equiv 1 \mod 3$.

Conversely, suppose $u_2=u$ is a solution of $3u^2+3u+1$. Then, the computation above inverts giving $\boldsymbol{w}$ as an α eigenvector with eigenvalue $m=3u+1$ (can't be 0).

Similarly, consider the other case of (6.5) with the critical possibility that $\boldsymbol{w}=u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})-\boldsymbol{v}$ is an α eigenvector. Analogously, the eigenvalue would satisfy $2mu_3'=m-u_3'=2(u_3'-1)$ or $m=3u_3'-2$ and $3(u_3')^2-3u_3'+1=0$.

With $\boldsymbol{w}=u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha)=2u_2\boldsymbol{v}+u_2\boldsymbol{v}^{\alpha^{-1}}$, apply $q_3^{2u_3}$ to (6.6):

$$\mapsto (\alpha_0, {}_{\boldsymbol{w}+\boldsymbol{v}}\alpha_0^{-1}, {}_{u_3((\boldsymbol{w}-\boldsymbol{w}^{\alpha^{-1}})+(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}}))+\boldsymbol{w}}\alpha_0, {}_{u_3((\boldsymbol{w}-\boldsymbol{w}^{\alpha^{-1}})+(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}}))-\boldsymbol{v}}\alpha_0^{-1}). \tag{6.10}$$

Also, $\boldsymbol{w}-\boldsymbol{w}^{\alpha^{-1}}$ is $u_2(\boldsymbol{v}-\boldsymbol{v}^\alpha-\boldsymbol{v}^{\alpha^{-1}}+\boldsymbol{v})=3u_2\boldsymbol{v}$. Rewrite (6.10) so that every subscript is a linear combination of $\boldsymbol{v}$ and $\boldsymbol{v}^{\alpha^{-1}}$. This gives (6.8).

Start again with ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$, but this time find the action of

$$q_3^{2u_3'} \mapsto (\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})}\alpha_0, {}_{u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})-\boldsymbol{v}}\alpha_0^{-1}).$$

With $\boldsymbol{w}'=u_3'(\boldsymbol{v}-\boldsymbol{v}^{\alpha^{-1}})$, apply $q_2^{2u_2'}$ to $(\alpha_0, {}_{\boldsymbol{v}}\alpha_0^{-1}, {}_{\boldsymbol{w}'}\alpha_0, {}_{\boldsymbol{w}'-\boldsymbol{v}}\alpha_0^{-1})$:

$$\mapsto (\alpha_0, {}_{u_2'((\boldsymbol{v}-\boldsymbol{v}^\alpha)+((\boldsymbol{w}')^\alpha-\boldsymbol{w}'))+\boldsymbol{v}}\alpha_0^{-1}, {}_{u_2'((\boldsymbol{v}-\boldsymbol{v}^\alpha)+((\boldsymbol{w}')^\alpha-\boldsymbol{w}'))+\boldsymbol{w}'}\alpha_0, {}_{\boldsymbol{w}'-\boldsymbol{v}}\alpha_0^{-1}). \tag{6.11}$$

Also, $(\boldsymbol{w}')^\alpha-\boldsymbol{w}'$ is $-3u_3'\boldsymbol{v}$. Rewrite (6.11) with every subscript a linear combination of $\boldsymbol{v}$ and $\boldsymbol{v}^{\alpha^{-1}}$ to get (6.9). □

We now show (6.1) holds. That will end with showing each nontrivial lift invariant value in $(\mathbb{Z}/\ell)^*$ distinguishes a unique braid orbit on $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$.

Proposition 6.5. *Excluding* (6.7) *– so a complement exists – the complement in each case of* (6.6) *is independent of* $\boldsymbol{v}$.

Given $\boldsymbol{v}' \in V_\ell$, *that is not an* α *eigenvector, Lem. 5.10 uniquely determines* $m=m_{\boldsymbol{v}'}$ *so that* $\alpha_{\boldsymbol{v}',m_{\boldsymbol{v}'}}$ *(equation* (5.18) *) with the same lift invariant as* ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$. *Thus, there is exactly one braid orbit on* $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})$ *with a given nontrivial braid invariant. This completes are identification of all level* $k=0$ *braid orbits.*

Proof. In the first case of (6.6), the goal given u_2, is to find what value of u_3 makes $({}_{\boldsymbol{v},1,3}\boldsymbol{g}, q_2^{2u_2}, q_3^{2u_3})$ 1-degenerate.

Then, (6.8) being 1-degenerate is equivalent to there is an s for which:

$$s((2u_2{+}1)\boldsymbol{v}{+}u_2\boldsymbol{v}^{\alpha^{-1}}) = (u_3(3u_2{+}1){-}1)\boldsymbol{v}{-}u_3\boldsymbol{v}^{\alpha^{-1}}.$$

Given $u_2 \not\equiv 0 \bmod \ell$, find (s, u_3) by equating the coefficients ($\bmod \ell$) of $\boldsymbol{v}$ and $\boldsymbol{v}^{\alpha^{-1}}$ on both sides. From the coefficients of $\boldsymbol{v}^{\alpha^{-1}}$: $s = \frac{-u_3}{u_2}$. From the coefficient of $\boldsymbol{v}$:

$$-u_3(2u_2{+}1) \equiv u_2(u_3(3u_2{+}1){-}1) \text{ or } u_3 \equiv \frac{u_2}{3u_2^2{+}3u_2{+}1} \mod \ell. \tag{6.12}$$

Given u_3', we find u_2' for which (6.9) is 1-degenerate: Find an s' with

$$s'((1{+}2u_2'{-}3u_2'u_3')\boldsymbol{v}{+}u_2'\boldsymbol{v}^{\alpha^{-1}}) = (u_3'{-}1)\boldsymbol{v}{-}u_3'\boldsymbol{v}^{\alpha^{-1}}.$$

Given $u_3' \not\equiv \mathbf{0} \bmod \ell$, find (s_2', u_2') by equating the coefficients ($\bmod \ell$) of $\boldsymbol{v}$ and $\boldsymbol{v}^{\alpha^{-1}}$ on both sides. From the coefficients of $\boldsymbol{v}^{\alpha^{-1}}$ (resp. $\boldsymbol{v}$): $s' = \frac{-u_3'}{u_2'}$

$$\text{(resp. } u_2'(u_3'{-}1) \equiv -u_3'(1{+}2u_2'{-}3u_2'u_3') \text{ or } u_2' \equiv \frac{u_3'}{3u_3'^2{-}3u_3'{+}1} \mod \ell.) \tag{6.13}$$

For clarity: Translating the notation $(\boldsymbol{v}', m_{\boldsymbol{v}'})$ to that of our first go around above would have $\boldsymbol{v}' = (2u_2{+}1)\boldsymbol{v}{+}u_2\boldsymbol{v}^{\alpha^{-1}}$ and $m_{\boldsymbol{v}'} = s{+}1$.

Now we show, one braid orbit contains all elements with a given prime to ℓ lift invariant. Prop. 4.19 produces ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ achieving any such lift invariant: we can apply braids to that ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$.

To find the complete braid orbit of ${}_{\boldsymbol{v},1,3}$, Princ. 5.7 says we need only all elements of $T_{\ell,\pm,\pm,1-\deg}$ braid equivalent to it. Suppose we braid to the (5.5) standard form:

$$\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = (\alpha_0, {}_{\boldsymbol{v}_2}\alpha_0^{-1}, {}_{\boldsymbol{v}_3}\alpha_0, {}_{\boldsymbol{v}_4}\alpha_0^{-1}) : \boldsymbol{v}_2 \text{ or } \boldsymbol{v}_4 \text{ any } \boldsymbol{v}', \text{ not an } \alpha \text{ eigenvector.} \tag{6.14}$$

As in Proposition's statement, if we can do this were $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3}$ is 1-degenerate and $\boldsymbol{v}'$ is otherwise arbitrary, then we have the complete braid orbit. If $\boldsymbol{v}' = \boldsymbol{v}_2$, construct the 1-degenerate target by applying a power of q_3, as in Lem. 5.2 or Lem. 5.5. In the latter case, apply $q_3^{-1}q_2^{-1}$ first to put ${}_{\boldsymbol{v}'}\alpha_0^{-1}$ in the 2nd position, reverting to the 1st case.

Then, we have filled out all possibilities by showing: we can braid ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ to an element of form (6.8) or of form (6.9) where ${}_{\boldsymbol{v}'}\alpha_0^{-1}$ appears in some entry.

This is done if $\boldsymbol{v}'$ appears as

(6.15a) $(2u_2{+}1)\boldsymbol{v}{+}u_2\boldsymbol{v}^{\alpha^{-1}}$ or $(u_3(3u_2{+}1){-}1)\boldsymbol{v}{-}u_3\boldsymbol{v}^{\alpha^{-1}}$ for some (u_2, u_3); or as

(6.15b) $(1{+}2u_2'{-}3u_2'u_3')\boldsymbol{v}{+}u_2'\boldsymbol{v}^{\alpha^{-1}}$ or $(u_3'{-}1)\boldsymbol{v}{-}u_3'\boldsymbol{v}^{\alpha^{-1}}$ for some (u_3', u_2').

Check with (6.15a). For any $b = u_3 \not\equiv 0 \bmod \ell$ and a, find u_2 in $a = u_3(3u_2{+}1){-}1$, to achieve $\boldsymbol{v}' = a\boldsymbol{v} + b\boldsymbol{v}^{\alpha^{-1}}$. All that we are missing are those $\boldsymbol{v}'$ where $b \equiv 0 \bmod \ell$. But if we apply apply conjugation by α to our Nielsen class representatives, we get representatives for $\boldsymbol{v}'$ of the form $a\boldsymbol{v}^{\alpha} + b\boldsymbol{v}$, and with $a = 0$ we have the nontrivial multiples of $\boldsymbol{v}$. This concludes the proof. □

In Lem. 6.6, the expression $(3u^2{+}3u{+}1)^{-1} \bmod \ell$ really denotes $(3u^2{+}3u{+}1)^{\ell-2}$, which will be 0 when evaluated at a zero of $3u^2{+}3u{+}1$ (rather than ∞). RETURN

LEMMA 6.6. *There is a solution of* $3u^2{+}3u{+}1 \equiv 0 \bmod \ell$ *($\ell > 3$) if and only if* $\ell \equiv 1 \bmod 3$.

PRINCIPLE 6.7 (Coalescing). *We accept that the number of reduced inequivalent double identity elements with a given lift invariant is K_ℓ based on these being the natural covers from coalescings on the boundary that are in* $\mathrm{Ni}(G_\ell, \mathbf{C}_3^3)$ *and have the same lift invariant as prior to coalescing.*

6.3. Counting the 1-degenerate reps.

PROPOSITION 6.8. *There are $K_\ell(\ell-1)$ 1-degenerate elements in a double identity $K_{q^2}^*$ orbit. That establishes* (5.21c) *and (according to* Cor. 5.9*)* (5.21d)*, finishing the list of properties* (5.21) *that describe level 0 of the braid orbits of* $\mathrm{Ni}(G_\ell, \mathbf{C}_{+3^2-3^2})^{\mathrm{rd}}$. *So, all elements of a given nontrivial lift invariant fall in one braid orbit.*

PROOF. Now consider a double identity element of form ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ (as in (4.19b)). As above we consider 1-degenerate chains, starting with one of length 1. For this we compute the complement of

$$({}_{\boldsymbol{v},1,3}\boldsymbol{g}, q_2^{2u_2}) = (\alpha_0, {}_{\boldsymbol{v}}\alpha^{-1}, \alpha_0, {}_{-\boldsymbol{v}}\alpha^{-1}).$$

□

REMARK 6.9. Explain other cases where the Nielsen class and lift invariant didn't distinguish braid orbits.

6.4. Setup for ℓ^{k+1}, $k \geq 1$. Here we deal with the lift invariant for level $k \geq 1$. Instead of saying 'nontrivial lift invariant' (or orbit), we now refer to an $\ell^u\ell'$ lift invariant, and $\ell^u\ell'$ orbits, where the integer u – leave it out if it is 0 – indicates the exact power of ℓ dividing the value of the lift invariant.

6.4.1. *Extending to $k > 0$.* Lem. 5.2 and Lem. 5.5 allowed us to apply the 1-degenerate Princ. 5.7. We need to extend that to higher values of k.

6.4.2. *Finding the orbits.* The last line of Lem. 4.12 counts the H-M and double identity reps. at level k above such reps. at level 0. Inductively, ℓ^2 of each type at level $k+1 \geq 1$ are above the corresponding type at level $k \geq 0$. To structure the braid orbits at level k, we will inductively adjust (5.2) to list the level k+1 braid orbits.

(6.16a) Lift invariant 0 orbits are H-M. Above each k level H-M are ℓ level k+1 H-M orbits. Each contains ℓ H-M reps. above any level k H-M rep.

(6.16b) Nontrivial lift invariant orbits are distinguished by that invariant. They are double identity if and only if they are ℓ'; then they are $K_{q^2}^*$ orbits.

Parallel to (5.3) we have these clarifying points. Recall the two types – ${}_{\boldsymbol{v},1,3}\boldsymbol{g}$ and ${}_{\boldsymbol{v},2,4}\boldsymbol{g}$ – of double identity elements.

(6.17a) Elements of (6.16a) in $T_{\ell^{k+1},\pm\pm,1-\deg}$ consist precisely of H-M and shift of H-M reps.

(6.17b) In (6.16b), above any double identity element (either type) at level k, each of the ℓ distinct ℓ' orbits contains ℓ double identity elements.

(6.17c) In each $\ell^{u+1}\ell'$ orbit, $u \geq 0$, above any level k element in $T_{\ell^k,\pm\pm,1-\deg}$ (in an $\ell^u\ell'$ orbit), there are ℓ^2 elements in $T_{\ell^{k+1},\pm\pm,1-\deg}$.

§6.4.3 explains the orbits for $\ell = 5$ and $k = 1$. It emphasizes the four $5 \cdot 5'$ ($\ell = 5$, $u = 1$) orbits to clarify the transition between $u = 0$ and $u = 1$ in (6.17c).

6.4.3. $\ell = 5$ *and* $k = 1$ *example.* Since $K_5 = 1$, the reduced braid orbits for $\ell = 5$, $k = 0$ fit the statements of (5.2a) and (5.2b): one H-M orbit with 4 each of H-M and shift of H-M reps.

Also, each (of four) double identity orbits intersects $T_{5,\pm\pm,1-\deg}$ in $(5-1) = 4$ elements, but it has just 1 $(= K_5)$ double identity of each type.

There are then three types of level $k = 1$ orbits whose intersections with $T_{5^2,\pm\pm,1-\deg}$ consist of these elements.

(6.18a) A la (6.17a): 5 H-M orbits, each with $5 \cdot 4$ H-M (resp. shift of H-M) reps.

(6.18b) A la (6.17b): Twenty $(= \varphi(5^2))$ $5'$ orbits, each with $5 \cdot 4^2 = 80$ elements in $T_{5^2,\pm\pm,1-\deg}$.

(6.18c) A la (6.17c): Four orbits of nontrivial $5 \cdot 5'$ lift invariant. Each with 5^2 elements in $T_{5^2,\pm\pm,1-\deg}$ over any H-M level 0 element.

That's a total of $5 \cdot 2 \cdot 20 + 20 \cdot 4 \cdot 5 \cdot 4 + 4 \cdot 8 \cdot 5^2 = 2600$ elements in $T_{5^2,\pm\pm,1-\deg}$.

Use the notation (4.19). There is a similarity between two types of elements:

(6.19a) ${}_{\boldsymbol{v},\boldsymbol{v}',1,3}\boldsymbol{g} = (\alpha_0, \boldsymbol{v}\alpha_0^{-1}, {}_{5\boldsymbol{v}'}\alpha_0, {}_{-\boldsymbol{v}+5\boldsymbol{v}'}\alpha_0^{-1})$ in a (6.18b) orbit over the double identity element ${}_{\boldsymbol{v} \bmod 5,1,3}\boldsymbol{g}$; and

(6.19b) ${}_{\boldsymbol{v},\boldsymbol{v}',3,4}\boldsymbol{g} = (\alpha_0, {}_{5\boldsymbol{v}'}\alpha_0^{-1}, {}_{\boldsymbol{v}}\alpha_0, {}_{\boldsymbol{v}-5\boldsymbol{v}'}\alpha_0^{-1})$ in a (6.18c) orbit over an H-M element ${}_{\boldsymbol{v} \bmod 5,3,4}\boldsymbol{g}$.

In both cases, $\boldsymbol{v}$ mod 5 is determined; and being in $T_{5^2,\pm\pm,1-\deg}$ implies $\boldsymbol{v}' = m\boldsymbol{v}$ mod 5, $m \in \mathbb{Z}/5$. in case (6.19a) (resp. (6.19b)) there are then, $5 \cdot 5^2$ (resp. $4 \cdot 5^2$, because $m = 0$ would give an H-M rep. not included in these orbits) choices of the pairs $(m, \boldsymbol{v}')$ subject to one further constraint: the elements have a specific lift invariant value corresponding to their orbit.

7. Frattini monodromy and Interpreting moduli Components

7.1. Are braid components ever accidental? Discuss the different braid components, including those whose lift invariant is ℓ divisible.

7.2. The Nielsen class $\mathrm{Ni}(G_{\ell^{k+1}}, \mathbf{C}_{+3^2-3^2})$ for $\ell = 2$ and $k > 0$.

7.3. Values of r that work on example (1.2c)**.**

Definition 7.1 (Eventually ℓ-Frattini).

Appendix A. Notation

A.1. Group notation. An n dimensional group representation of a group G over a field K is a homomorphism $T : G \to \mathrm{GL}_n(K)$. It's character is the function $g \in G \mapsto \mathrm{t}(T(g))$: t denotes the trace of the matrix. The symmetric group on $\{1, \dots, n\}$, S_n, natural embeds in $\mathrm{GL}_n(\mathbb{Q})$ by mapping a permutation $g(i) = j_i$, $i = 1, \dots, n$, to the matrix with 1 in all (i, j_i) positions, 0 elsewhere. We can apply t to a permutation representation. The result is the number of fixed points of $T(g)$.

If you mod out the center (diagonal matrices) of $\mathrm{GL}_n(K)$, you get $\mathrm{PGL}_n(K)$. Similarly, there is $\mathrm{PSL}_n(K)$, the quotient of the matrices of determinant 1 over the field K by its diagonal matrices.

An elementary abelian group of order 4 is a Klein (or Klein 4-) group. The dihedral group of order $2d$, denoted D_d, is characterized by being generated by two involutions α_i, $i = 1, 2$, with $\mathrm{ord}\alpha_1\alpha_2 = d$. Another characterization is that it has generators $\langle \alpha_1, \beta \rangle$ with $\alpha_1 \beta \alpha^{-1} = \beta^{-1}$, so $\beta = \alpha_1\alpha_2$ in the 1st formulation.

An subset in a group G is called ℓ' if the order of the elements in it is prime to ℓ. We can replace ℓ by any integer for this definition. For example: We can speak of an ℓ' conjugacy class.

Suppose a group G is a semidirect product of a group H that is a quotient of G, and the abelian kernel M of that quotient. It is convenient and memorable to write the elements in $M \times^s H$ in the form $\left(\begin{smallmatrix} h & 0 \\ m & 1 \end{smallmatrix}\right)$ with $h \in H$ and $m \in M$. Then, the standard matrix multiplication of $g_1 = \left(\begin{smallmatrix} h_1 & 0 \\ m_1 & 1 \end{smallmatrix}\right)$ and $g_2 = \left(\begin{smallmatrix} h_2 & 0 \\ m_2 & 1 \end{smallmatrix}\right)$ symbolically gives $\left(\begin{smallmatrix} h_1h_2 & 0 \\ m_1^{h_2}+m_2 & 1 \end{smallmatrix}\right)$. From this we take the semidirect product multiplication, which is compatible with a right-hand action of H on M.

Appendix B. Frattini comments

B.1. Precision on the Frattini module construction. [**Fr06**, §2.1] has an exposition on this topic, mainly because it was not classical restricting to one prime at a time, though it is based on [**Br82**]. An ℓ-representation cover, $\psi : R \to G$, of a finite group G is a cover with kernel a central ℓ extension of G with $\ker(R \to G$ isomorphic to $H_2(G, \mathbb{Z}_\ell)$. Such a cover is maximal in the sense that there is no larger cover $\psi' : R' \to G$ with kernel a central ℓ extension that factors through ψ. Such a representation cover always exists. Main points:

- (2.1a) ψ is an ℓ-Frattini cover; so it is a quotient of the universal ℓ-Frattini cover of G.
- (2.1b) ψ is unique if and only if G is ℓ-*perfect*: $G = G_0$ has no $\mathbb{Z}/\ell$ quotient.
- (2.1c) Its maximal $\mathbb{Z}/\ell$ quotient is a quotient of $G_{\ell,1} \to G_0$.

Then, the Frattini module $M(G, \ell)$ is a quotient of the natural $\mathbb{Z}/\ell[G]$ module induced from inducing $\mathrm{Ker}(\psi_{P_\ell,1})$ from $N_G(P_\ell)$ to G. Nailing the exact module precisely takes advantage of two cohomological facts: $M(G, \ell)$ is indecomposable, and $H^2(G, M(G, \ell))$ is 1-dimensional.

Remark B.1.

Proof. The characteristic Frattini cover $\psi_{1,0} : G_1((\mathbb{Z}/p)^2) \to (\mathbb{Z}/p)^2$ factors through $\psi_{\mathrm{ab}} = (\mathbb{Z}/p^2)^2 \to (\mathbb{Z}/p)^2$ (modding out by p). The nontrivial element of $\mathbb{Z}/2$ acts by multiplication by -1 on $(\mathbb{Z}/p^2)^2$. In fact, ψ_{ab} is the maximal abelian extension through which $\psi_{1,0}$ factors.

Loewy layers of any $(\mathbb{Z}/p)^2 \times^s \mathbb{Z}/2$ module are copies of $\mathbf{1}$ and $\mathbf{1}^-$. So, any proper extension of ψ_{ab} through which $\psi_{1,0}$ factors, also factors through $\psi' : H \to (\mathbb{Z}/p)^2$ with $\ker(\psi')$ of dimension 3 and H not abelian.

We choose the Heller construction (in [**?**, Part II], for example) to describe the characteristic module

$$M_0((\mathbb{Z}/p)^2 \times^s \mathbb{Z}/2) = \ker(G_1((\mathbb{Z}/p)^2 \times^s \mathbb{Z}/2) \to (\mathbb{Z}/p)^2 \times^s \mathbb{Z}/2)(p \text{ odd}).$$

Here is the rubric for this simple, though still nontrivial case. Suppose G_0 is p-split: $G_0 = P^* \times^s H$ with $(|H|, p) = 1$ and P^* the p-Sylow, as in our case. Use the Poincaré-Birkhoff-Witt basis of the universal enveloping algebra (from the proof of Lem. **??**) to deduce the action of H from its conjugation action on P^*. In our case, the ℓth Loewy layer of $\mathbb{Z}/p[P^*] \stackrel{\mathrm{def}}{=} P_{\mathbf{1}}$, with $P^* = (\mathbb{Z}/p)^2$ consists of sums of

$\mathbf{1}$ (resp. $\mathbf{1}^-$) if ℓ is even (resp. odd) from 0 to $2p-2$ (resp. 1 to $2p-1$). That is the projective indecomposable module for $\mathbf{1}$.

Now list the Loewy display for the projective indecomposable modules for G_0 by tensoring the Loewy layers of the projective indecomposables for $\mathbf{1}$ with the semi-simple modules for H [**?**, p. 737]. In our case, the semi-simples for $\mathbb{Z}/2$ are just $\mathbf{1}$ and $\mathbf{1}^-$ giving $P_{\mathbf{1}}$ and $P_{\mathbf{1}^-}$ as the projective indecomposables, the latter having the same look as the former except you switch the levels with $\mathbf{1}$ with those with $\mathbf{1}^-$. Finally, M_0 is $\Omega_2 \stackrel{\text{def}}{=} \ker(\psi_2 : P_{\mathbf{1}^-} \oplus P_{\mathbf{1}^-} \to \ker(P_{\mathbf{1}} \to \mathbf{1}))$ with this understanding: $\ker(P_{\mathbf{1}} \to \mathbf{1})$ has at its head $\mathbf{1}^- \oplus \mathbf{1}^-$ and ψ_2 is the map from the minimal projective $(P_{\mathbf{1}^-} \oplus P_{\mathbf{1}^-})$ that maps onto $\ker(P_{\mathbf{1}} \to \mathbf{1})$. □

B.2. The Schur multiplier for $(\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/3$. [**?**, Cor. 5.7] shows that $V_{2,0} \times^s \mathbb{Z}/3$ (which happens to be A_4), has

$$0 \to V_{2,0} \to V_{2,0} \oplus \mathbf{1}_2$$

for its Loewy display, where $\mathbf{1}_\ell$ is the trivial $\mathbb{Z}/\ell[G]$ module for any G.

Definition B.2. Let $J_{\ell,G}$ be the intersection of the maximal left (or right) ideals of $\mathbb{Z}/\ell[G]$: This is the Jacobson radical of the group ring. The maximal semi-simple quotient of any module M is $M/J_{\ell,G}M$, and it is 1st Loewy layer. Then, proceed inductively, applying this with $M/J_{\ell,G}M$ replacing M. We also need info on the nonsplit subquotients which are obtained from arrows between the layers. [**Fr06**, App. A.2] does an exposition on this.

Jenning's Theorem gives Loewy layer dimensions as coefficients of a Hilbert polynomial $H_G(t)$ when G is a ℓ-group. In that case, since the irreducibles are just $\mathbf{1}_\ell$, we only need the arrows between layers.

[**Fr06**, Lem. A.3] says $H_{(\mathbb{Z}/\ell)^n}(t) = (\frac{1-t^\ell}{1-t})^n$. Then, the respective Loewy layers of $\mathbb{Z}/\ell[(\mathbb{Z}/\ell)^2]$ have dimensions $1, 2, \ldots, \ell, \ell-1, \ldots, 1$. If x_1, x_2 are generators of $(\mathbb{Z}/\ell)^2$, then the symbols $x_1^u x_2^{\ell-u}$, represent generators of copies of $\mathbf{1}_\ell$ at Loewy layer o. Arrows from $\mathbf{1}_\ell$ associated to $x_1^u x_2^{\ell-u}$ go to copies of $\mathbf{1}_\ell$ associated to $x_1^u x_2^{\ell-1-u}$ and $x_1^{u-1} x_2^{\ell-u}$ under the above constraints. Most of this was seen using the Poincare-Birkoff-Witt basis for the universal enveloping algebra of the group ring [**?**, p. 88]. Now we must add the action of $\mathbb{Z}/3$.

§B.1 reminds of the Loewy display of the module $M_{G_{\ell^{k+1}}}$, which we denote by $M_{\ell^{k+1}}$ when there is no confusion. Cor. B.3 shows that, for each ℓ^{k+1}, the maximal $\mathbb{Z}/\ell^{k+1}$ quotient of the Schur multiplier is $\mathbb{Z}/\ell^{k+1}$.

Corollary B.3. *The ℓ-Frattini module M_ℓ of G_ℓ has one copy of $\mathbf{1}_{G_\ell}$ at its head. The extension of V_ℓ defined by $\mathbf{1}_{G_\ell}$ is the Heisenberg group to which the action of $\mathbb{Z}/3$ on G_ℓ extends G_ℓ.*

Appendix C. Detecting a MT

Appendix D. Some comments on using the program [GAP00]

On occasions in this paper we have applied the computer program [**GAP00**] to guide us. Mostly that has been to assure, as in §3.1, there is a chance to divine the braid orbits on Nielsen class elements. We are using 'standard' mathematical proofs, and not relying on [**GAP00**] as the final arbiter. As in [**BFr02**], that assures we understood the nature of components and their cusps. Without exception, in

[**BFr02**], this exposed solid reasons why Schur multipliers of alternating groups where producing interesting phenomena.

If, however, we open up the applications, of braid actions on objects like Nielsen classes, we can't expect to take applications to completion within a reasonable time frame without occasionally moving on with a [**GAP00**]-identified phenomena that momentarily looks accidental. Especially, since we expect this often for families of covers of low numbers of branch points.

A slightly different problem occurs with certain portions of group theory where attempts at classification are out of the question for even group theorists, much less for our applications. For example, §2.1.3 suggests that we understand the characteristic extension of a finite group G reasonably well. That hides delicate points that surely would require [**GAP00**] to complete if we were to take other Frattini cases of **MT**s for, say, all $n \equiv 5 \mod 8$ explicitly.

There is documentation of, say, [**GAP00**] running to many pages, and there is the hope that as it is used, it proves its reliability. [**Da12**] discusses the *implementation* rather than the mathematics of the algorithms that lie behind programs. This brief article discusses a publication format – "literate program ", suggested by D. Knuth – that would validate (in real time, say, during a talk) that a result running under a computer program is accurate and can be checked in a specified time. The article even suggests that this downloading of "literate documents" would validate our checking of citation trails. While the article speaks in terms of *computational mathematics*, so much of mathematics – including the Loewy modules that arise in considering ℓ-Frattini covers – is a black box to most mathematicians, even if they agree to the types of applications we include below. In a 2-page, non-technical article, [**Da12**] suggests that there is a need for a computational mathematics "proof" standard under the heading of literate software. I would include the many places where space limitations are claimed for non-documentation of crucial calculations, even as I'm aware this is asking for a great deal.

Appendix E. Spaces in the split case

Consider any group G and any collection of conjugacy classes $\mathbf{C}'$ whose elements generate G. We restrict to classes $\mathbf{C}$ with support in $\mathbf{C}'$ with these constraints.

(5.1a) $\mathrm{Ni}(G, \mathbf{C})$ must be nonempty (or the Hurwitz spaces are empty).

(5.1b) $\mathbf{C}$ must be $\mathbb{Q}$-rational.

(5.1c) Geometric properties – preserved by $G_{\mathbb{Q}}$ – must separate braid orbits.

Property (E.1b) is necessary and sufficient that the Hurwitz space have $\mathbb{Q}$ as definition field [**FrV91**, Main Thm.]. It is, however, the components that we need over $\mathbb{Q}$, and the much harder check of (E.1c) assures that. Here we seek ℓ-adic representations comparable to those from the series of modular curves $\{X_1(\ell^{k+1})\}_{k=0}^{\infty}$ as ℓ varies in the *split* case of (1.11.2).

We consider building on A_n, as in the Frattini case where

$$G_{n,\ell,0} = (\mathbb{Z}/\ell)^n/\langle(1,\dots,1)\rangle \times^s A_n \stackrel{\text{def}}{=} V_n \times^s A_n,$$

by taking $n = 5$. The first test, (E.1a), is that $\mathrm{Ni}((G_{5,\ell,0}, \mathbf{C}_{3^4})$ is nonempty. We find now that this is not so.

LEMMA E.1. *For all primes ℓ not dividing n, every $\bar{\boldsymbol{a}} \in V_n$ has a unique representative $(a_1,\dots,a_n)$ where $\sum_{i=1}^n a_i = 0 \mod \ell$. In particular, for $n = 5$, and all $\ell \neq 3, 5$, $\mathrm{Ni}(G_{5,\ell,0}, \mathbf{C}_{3^4})$ is empty.*

PROOF. Given a representative $a_1, \dots, a_n$ for $\bar{\boldsymbol{a}}$, since ℓ is prime to n, there is a unique $m \mod \ell$ for which $\sum_{i=1}^n a_i \equiv m \cdot n \mod \ell$. The desired representative is $(a_1, \dots, a_n) - m(t, \dots, 1)$. So, for ℓ not dividing n, we may replace V_n by the submodule of $(\mathbb{Z}/\ell)^n$ consisting of elements whose entries sum to 0.

Now we show the Nielsen class $\mathrm{Ni}(G_{5,\ell,0}, \mathbf{C})$ is empty. Use the semidirect product multiplication in §A.1. Given $g \in A_5$, the elements in $G_{5,\ell,0}$ above g in the conjugacy class of g have the form

$$\{\left(\begin{smallmatrix} 1 & 0 \\ \boldsymbol{a} & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g & 0 \\ \mathbf{0} & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ -\boldsymbol{a} & 1 \end{smallmatrix}\right)\}_{\boldsymbol{a} \in V_5}.$$

We know H_4 is transitive on $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})$. So, if $\mathrm{Ni}(G_{5,\ell,0}, \mathbf{C}_{3^4})$ is nonempty there are elements in it lying above any given element in $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})$. Choose the H-M rep. $\boldsymbol{g}_{\text{H-M}} = (g_1, g_1^{-1}, g_2, g_2^{-1})$; as in Lem. 2.9, where $g_1 = (1\,2\,3)$ and $g_2 = (4\,5\,6)$. With no loss, assume a representative above it has the form

$$\boldsymbol{g}' \stackrel{\text{def}}{=} ((\mathbf{0}, g_1), (\boldsymbol{a}_1, g_1)^{-1}), (\boldsymbol{a}_2 + \boldsymbol{c}, g_2), (\boldsymbol{c}, g_2)^{-1}),$$

for some $\boldsymbol{a}_1$ of form $\boldsymbol{a}^{g_1} - \boldsymbol{a}$ and $\boldsymbol{a}_2$ and $\boldsymbol{c}$ of form $\boldsymbol{a}_2^g - \boldsymbol{a}$. Write $\boldsymbol{a}^{g_1} - \boldsymbol{a}$ explicitly to see its 4th and 5th entries are 0. Similarly, the 1st and 2nd entries of $\boldsymbol{a}^{g_2} - \boldsymbol{a}$ are 0.

Now apply the product-one condition, (1.4b). Conclude: $-(\boldsymbol{a}_1)^{g_1^{-1}} + (a_2)^{g_2^{-1}}$ is $\mathbf{0}$. So, the 4th and 5th (resp. 1st and 2nd) elements of this sum are 0. That means $\boldsymbol{a}_1 = (a', a', a', 0, 0)$ and $\boldsymbol{a}_2 = (0, 0, a'', a'', a'')$. Conclude that $a' = a'' \equiv 0 \mod \ell$. That is, the group generated by the entries of $\boldsymbol{g}'$ does not generate $G_{5,\ell,0}$, a necessary condition for being in the Nielsen class. □

References

[BFr02] Paul Bailey and Michael D. Fried, *Hurwitz monodromy, spin separation and higher levels of a modular tower*, Arithmetic fundamental groups and noncommutative algebra (Berkeley, CA, 1999), Proc. Sympos. Pure Math., vol. 70, Amer. Math. Soc., Providence, RI, 2002, pp. 79–220. MR MR1935406 (2005b:14044)

[Be91] D.J. Benson, *I: Basic representation theory of finite groups and associative algebras*, Cambridge Studies in advanced math., vol. **30**, Cambridge U. Press, Cambridge, 1991.

[Br82] K.S. Brown, *Cohomology of groups*, Springer Graduate Texts **87**, Springer-Verlag New York, 1982.

[Da12] T. Daly, *Publishing Computational Mathematics*, AMS Notices **59**, No. 2, 320–321.

[D06] P. Dèbes, *An introduction to the Modular Tower Program*, Groupes de Galois arithmétiques et différentiels, Séminaires et Congrès **13** (2006), 127–144.

[DE06] Pierre Dèbes and Michel Emsalem, *Harbater-Mumford Components and Towers of Moduli Spaces*, Journal de l'Institut Mathématique de Jussieu, **5/03** (2006), 351–371.

[Fr78] ———, *Galois groups and Complex Multiplication*, Trans.A.M.S. **235** (1978), 141-162.

[Fr95] ———, *Introduction to Modular Towers: Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 111–171.

[Fr99] ———, *Variables Separated Polynomials and Moduli Spaces*, No. Theory in Progress, eds. K. Gyory, H. Iwaniec, J. Urbanowicz, proceedings of the Schinzel Festschrift, Summer 1997 Zakopane, Walter de Gruyter, Berlin-New York (Feb. 1999), 169–228.

[Fr02] ———, *Moduli of relatively nilpotent extensions*, Inst. of Math. Science Analysis **1267**, June 2002, Communications in Arithmetic Fundamental Groups, 70–94.

[Fr06] ———, *The Main Conjecture of Modular Towers and its higher rank generalization*, in *Groupes de Galois arithmetiques et differentiels* (Luminy 2004; eds. D. Bertrand and P. Dèbes), Seminaires et Congres, Vol. **13** (2006), 165–233.

[Fr08a] ———, At http://math.uci.edu/~mfried, section: Ib. Definitions and discussions from Major Article Themes: → * Book: Intro. and Chp.s on Riemann's Existence Thm

[Fr08b] ———, On my home page http://math.uci.edu/~mfried, section: Ib. Definitions and discussions from Major Article Themes: → * Definitions: Arithmetic of covers and Hurwitz spaces.

[Fr10] ———, *Alternating groups and moduli space lifting Invariants*, Arxiv #0611591v4. Israel J. Math. **179** (2010) 57–125 (DOI 10.1007/s11856-010-0073-2).

[Fr12a] ———, *Variables separated equations: Strikingly different roles for the Branch Cycle Lemma and the Finite Simple Group Classification* arXiv:1012.5297v5 [math.NT] (DOI 10.1007/s11425-011-4324-4). Science China Mathematics, vol. **55** (2012), 1–72.

[Fr12b] ———, *Connectedness of families of sphere covers of A_n-Type* preprint as of 6/30/11. http://math.uci.edu~mfried/paplist-mt/twoorbit.pdf.

[FrJ86] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, vol. **11**, Springer Verlag, Heidelberg, 1986 (455 pgs); 2nd Edition 2004 (780 pgs) ISBN 3-540-22811-x. We quote here both the first and second ed., using $[\text{FrJ86}]_1$ and $[\text{FrJ86}]_2$ respectively.

[FrK97] ——— and Y. Kopeliovic, *Applying Modular Towers to the Inverse Galois Problem*, Geometric Galois Actions II Dessins d'Enfants, Mapping Class Groups and Moduli **243**, LMS Lecture Note series, (1997) 172–197.

[FrV91] ——— and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Annalen **290** (1991), 771–800.

[GAP00] The GAP group, **GAP** — *Groups, Algorithms and Programming*, Ver. 4.2; 2000 (http://www.gap-system.org).

[Mont91] I. Niven, H. Zukerman, H. Montgomery, *An introduction to the Theory of Numbers*, 5th Edition, J. Wiley and Sons, 1991.

[Nor62] D.G. Northcott, *An introduction to homological algebra*, Camb. U. press, 1962.

[Se68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, 1968, written in collaboration with Willem Kuyk and John Labute; 2nd corrected ed. by A. K. Peters, Wellesley, MA, 1998.

[Se92] ———, *Topics in Galois Theory*, 1992, Bartlett and Jones Publishers,

UC Irvine, emeritus
E-mail address: mfried@math.uci.edu

Florida State University
E-mail address: mfried@math.uci.edu