Monodromy, ℓ-adic Representations & the Regular Inverse Galois Problem

Michael D. Fried

Emeritus, University of California at Irvine

1106 W 171st Ave, Broomfield CO, 80023
E-mail address: mfried@math.uci.edu

Contents

Abstract. Since Abel and Galois, modular curves have always joined algebra and complex analysis. Since 1960, strongly in two considerations: *Serre's Open Image Theorem* (**OIT**); and the *Shimura-Taniyama-Weil Conjecture* that postulated a formula by which an elliptic curve over $\mathbb{Q}$ (of given conductor) might be uniformized by a modular curve whose upper half plane quotient was defined by a specific congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. There were some small accidents with modular curves producing new groups as Galois groups over $\mathbb{Q}$, but not regularly. So, there was no general relation between ℓ-adic representations, say as in generalizing Serre's **OIT**, and the Regular version of the Inverse Galois Problem that came together over generalizing modular curves.

Ch. 1 and Ch. 2 tie up threads that came just before Modular Towers (**MT**s). They show how Hurwitz spaces encode versions of the Inverse Galois Problem. Also, by geometrically connecting with classical problems, why the Inverse Galois Problem has been so difficult. We modernize our approach to investigating moduli (definition) fields of Hurwitz space components vis-a-vis *lift invariants* with examples.

Ch. 3 joins the first third and last third of the book in a new approach to the *lift invariant* and Hurwitz space components based on the *universal Frattini cover* of a finite group, the main ingredient behind **MT**s.

Ch. 4 explains **MT**s – started in 1995 – as a program giving such a relationship. We use that to interpret the **OIT** in a generality not indicated by Serre's approach. Ch. 5 uses one example, close to modular curves, that is clearly not of modular curves. This explains why our approach to (families of) covers of the projective line can handle a barrier noted by Grothendieck to generalizing the **OIT**.

Primary 11F32, 11G18, 11R58; Secondary 20B05, 20C25, 20D25, 20E18, 20F34

Moduli of covers, j-line covers, braid group and Hurwitz monodromy group, action on cohomology, Frattini and Spin covers, Lift invariants

List of Tables

List of Figures

Contents

This book naturally divides into two parts of two chapters each, flanked by two chapters of a bridge nature. Part I: Hurwitz spaces and the Inverse Galois Problem, comprising Ch. 1 and Ch. 2. Both include much exposition and observations/examples we didn't have time for in the original papers.

Then, Part II: Hurwitz Monodromy on ℓ-adic representations and Modular Towers comprising Ch. 4 and Ch. 5. Most of Part II is new, but we will publish separately many of the proofs. Between these two parts lies the first bridge, Ch. 3, based on using Frattini covers of groups. It completes Part I, sliding it into the main issues in Part II, expanding territory untreated since the publication of [**FrV91**].

Ch. 1 and Ch. 2 show how Hurwitz spaces interpret problems that require understanding solutions to equations that relate two complex variables. The foremost relation is given by a compact Riemann surface W mapping to the Riemann sphere $\mathbb{P}^1_z$ in a variable z: $\varphi_W : W \to \mathbb{P}^1_z$. The foremost problem is the *Regular Inverse Galois Problem*, **RIGP**.

Interpreting diophantine problems assiduously uses the Galois closure, and its monodromy group, of such a cover. There have been papers with examples, where the two halves of the title

$$[\ell\text{-adic representations}] \text{ and } [\text{the } \mathbf{RIGP}]$$

could be said to relate. Yet, we use generalizing Serre's Open Image Theorem (**OIT**), a result about points on modular curves, to show that relation has not previously aimed at a fitting conclusion. The group theory of this extension depends on the universal ℓ-Frattini cover of the finite group G. The exposition on this topic is not found anywhere else. This device gives **M**odular **T**owers (**MT**s) whose tower levels generalize classical modular curve levels.

The definition of **MT** first appears in Ch. 3 Def. 3.3 as a tower of absolutely irreducible components of a sequence of Hurwitz spaces for which the base Hurwitz space is defined by group G, a prime ℓ dividng $|G|$, and ℓ' conjugacy classes $\mathbf{C}$ of G. The main ingredient in forming the tower is a sequence of ℓ-Frattini extensions of G. Modulo testable conditions, the data $(G, \mathbf{C}, \ell)$ produces a canonical, nonempty, tower of Hurwitz spaces.

The group for the data of each level is a cover ${}^k_\ell\tilde{\psi} : {}^k_\ell G \to G$ with:

$$\begin{gathered} \ker({}^k_\ell\tilde{\psi}) = (\mathbb{Z}/\ell^k)^\nu \text{ a } \mathbb{Z}/\ell^k[G] \text{ module; and} \\ \nu > 0 \text{ independent of } k,\ k \geq 0. \end{gathered} \tag{0.1}$$

For given (G, ℓ), Ch. 6 Prop. 1.28 describes a maximal (finite) $\nu \stackrel{\text{def}}{=} \nu(G,\ell)_{\max}$.

We state the the rubric for the typical case that G is ℓ-perfect (has no $\mathbb{Z}/\ell$) quotient) although circumstances and comparison with classical results sometimes require modification to include this case. The main point is that without excluding nontrivial nilpotent quotients of ${}^k_\ell G$, there won't be a canonical construction.

(0.2a) For $\nu = \nu(G,\ell)_{\max}$, $(\mathbb{Z}/\ell^k)^\nu$ has these properties:

- It is an indecomposable $\mathbb{Z}/\ell^k[G]$ module;
- ${}^k_\ell\tilde{\psi}$ is universal for covers of G with abelian exponent ℓ^k kernel; and
- $\nu(G,\ell)_{\max} > 1$ except when G is a slight generalization of dihedral.

(0.2b) The (Hurwitz) monodromy action arises on the $\mathbb{Z}_\ell[G]$ module kernels, $L_{G,\ell}$, of $\lim_{\leftarrow k} {}^k_\ell G \to G$.

(0.2c) The action of (0.2b) identifies with an action on flags in $H_1(X_0, \mathbb{Z}_\ell)$ with X_0 a curve in the family.

Thoughout the book we use the abbreviation **RIGP** for the sl Regular Inverse Galois Problme, and **OIT** for some version of the *Open Image Theorem*. Often, $\nu(G,\ell)_{\max}$ is the only possible value of ν (> 0) in (0.1). Each possible value of ν presents its own challenges to the **RIGP** and the **OIT**. When G is close to a dihedral or alternating group, points on tower levels include *classical problems* for both the **RIGP** and **OIT**. It is, though, the relation between them that is most interesting.

For a version of the **OIT** like Serre's – including all modular curves – for us there are two collections of related groups,

$$\{D_\ell\}_{\text{primes } \ell} \text{ and } \{(\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/2\}_{\text{primes } \ell}.$$

For each group in each series, the conjugacy classes naturally extend from four repetitions of the non-trivial class in $\mathbb{Z}/2$.

To show how generalizing the **OIT** works, we use one example (in the sense that all modular curves are one example). Our example exhibits the features of Serre's example, though our **MT** levels are not modular curves. A striking difference is the appearance of the *lift invariant*) among the levels of our **MT**s. At all times we note comparisons (cusps included) with modular curves. This approach circumvents a difficulty noted by Grothendieck – stemming from the many correspondences on Jacobians – for generalizing the full force of Serre's **OIT**, Ch. 6 6.3. A reader can see this in following the Hurwitz monodromy approach to computing the monodromy action (Ch. 4) on the ℓ-adic representations.

Before getting to the **RIGP** or **OIT**, we develop the basics of how Hurwitz spaces work. The first basic is to describe equivalence classes of covers associated to a group G and conjugacy classes $\mathbf{C}$ – whose elements generate G; we suppress these in this exposition – from which we produce a Hurwitz space $\mathcal{H}(G,\mathbf{C})$. The second basic is conditions that guarantee that any point on the Hurwitz spaces will produce a curve cover that solves the arithmetic problem for which we aim.

This comes together in the description of the *moduli field* $\mathbb{Q}_{G,\mathbf{C}}$ of the Hurwitz space $\mathcal{H}(G,\mathbf{C})$. This depends on the equivalence class of covers representing those points, which in turn is fashioned toward the desired arithmetic problem. For a point

$\boldsymbol{p}$ on a Hurwitz space component $\mathcal{H}$ to corresponds to a cover in the equivalence class represented by $\boldsymbol{p}$, its coordinates *must* generate over $\mathbb{Q}$, $\mathbb{Q}(\boldsymbol{p})$, a field containing the moduli field $\mathbb{Q}_{\mathcal{H}}$ of the Hurwitz space. Further, $\mathcal{H}$ having *fine moduli* then guarantees such a representing cover over $\mathbb{Q}(\boldsymbol{p})$. The moduli field appears from the appropriate version of the *Branch Cycle Lemma* (**BCL**), Ch. 2 Lem. 4.1.[1]

When, however, $\mathcal{H}$ has more than one component, any given component, say $\mathcal{H}'$, has its own moduli field $\mathbb{Q}_{\mathcal{H}'}$ containing $\mathbb{Q}_{G,\mathbf{C}}$. Further, often a treatment of it is similar to the **BCL** using a *lift invariant*, a major topic in this book.

Ch. 6, has its own overview of the book. Material serves as appendices that enhance our examples. Note Ch. 6 §1.1.1: For permutation groups we usually use right actions, though occasionally concede to linear algebra matrix left action.

[1]Called the Branch Cycle Argument on [**Fr77**, p. 62].

CHAPTER 1

Covers and monodromy groups

The key inputs for a cover of the Riemann sphere, $\mathbb{P}^1_z$, uniformized by a fixed complex variable z, are a finite group G and a choice of its (unordered) conjugacy classes, $\mathbf{C} = \{\mathrm{C}_1, \ldots, \mathrm{C}_r\}$. We start slowly with the case $W = \mathbb{P}^1_w$, as a reminder examples of such appeared in High School math classes.

From $(G, \mathbf{C})$ we form a Nielsen class, $\mathrm{Ni}(G, \mathbf{C})$; an equivalence on Nielsen class elements; and an action of the braid group (actually its quotient, the *Hurwitz monodromy group*, H_r) on r-strings (§2 and §3).

We can understand algebra and (complex) geometry coming together with one of the beginning formulas that connects the spaces of covers to the absolute Galois group of $\mathbb{Q}$ through the *Branch Cycle Lemma* (**BCL**). Among its applications it gives the minimal definition (a precise *cyclotomic*) field of these spaces. That gives us the tools to introduce **MT**s, Ch. 4, and the ℓ-adic representations they support.

Fundamental properties of the spaces come from braid group action on Nielsen classes. The first use is that Hurwitz space components correspond to the orbits of the action. While the Nielsen class of a cover is a strong invariant, when there is more than one component to a Hurwitz space – one cover will not deform into all other covers in the Nielsen class – there are often good explanations. The long history of applications to easily stated problems using the components of these spaces (and their definition fields) is not well known. We give many examples.

1. The Regular inverse Galois Problem

Assume $K \subset \bar{\mathbb{Q}}$, the algebraic numbers, with $\mathcal{G}_K$ its absolute Galois group. §1.1 differentiates the Inverse Galois Problem from the **RIGP**. We cannot escape using some specific group theory for results, and for enriched examples. Our introduction to this is §1.2 which has the homological algebra to differentiate the many examples of split and none split extensions of groups we use to illustrate our main theorems. Then, §1.3 introduces *Frattini covers*. Recall the group, (H, H) generated by commutators of H.

The spaces that we form are based on starting with a centerless finite group G, and a prime p dividing $|G|$. Constructions use profinite collections of finite group covers $\psi : H \to G$ with the following properties:

(1.1a) ψ is a Frattini cover; and

(1.1b) $\ker(\psi)$ is an ℓ-group contained in (H, H).

If G has no $\mathbb{Z}/\ell$ quotient – G is ℓ-perfect, Def. 1.2 – then the commutator condition is automatic, and that is the easiest case to consider. There is a universal cover of G §1.3, giving all elements of $\mathcal{E}_{G,p}$ as a quotient. The ℓ-group kernel is finitely generated, and it leads to several universal objects that are quotients of this, and sequences of spaces that are somewhat maximal challenges to unsolved problems, say, about the **RIGP**. As we see, however, by looking at the **OIT**, even given one (G, p), there is a whole world of spaces with modular curve-like sequences of spaces attached to it, with conjectured diophantine properties. Most of these come from smaller quotients of the universal cover. We can be more explicit about the group theory for constructing these. Therefore, in our examples, we tend to use these, leaving their descriptions to Ch. 6 §1.5.5.

1.1. The IGP **vs the RIGP.** A group G is a Galois group over K, if G is a quotient of $\mathcal{G}_K$: There exists an exact sequence $\psi : \mathcal{G}_K \to G \to 1$. We say, K satisfies the IGP if this holds for all finite groups G. This isn't known for any finite extension K – a number field – of $\mathbb{Q}$. One aspect of Ch. 2 is to show you just how far from known it is, and how much that is related to many renown problems that don't at first seem to have much to do with it.

Similarly, G is a regular Galois group over K if for each G,

$$\text{there exists } \psi : \mathcal{G}_{K(x)} \to G \to 1, \text{ with (the fixed field of } \ker(\psi)) \cap \bar{K} = K.$$

The major success on the IGP has come through the **RIGP** for which the basic tools are versions of *Riemann's existence theorem* followed by specialization (Hilbert's irreducibility theorem). That is, an **RIGP** realization gives ∞-ly many independent realizations of G as a quotient of $\mathcal{G}_{\mathbb{Q}}$. Constructing just one out of thin air doesn't seem to work well, except for groups regarded as obvious in the history of group theory: abelian groups, S_n s and groups close to dihedral groups.

Mysteries for Rational functions?: Even for dihedral groups, there is a simple mystery connected to famous problems about modular curves (§6.1.3), whose description we can give naturally using rational functions in one variable. Applying serious Galois theory is wholly different than quoting the technical equivalences around its fundamental theorem. We illustrate with many examples.

Here z indicates the complex variable from a 1st year graduate course. Changing from the High School x to w or z just indicates we intend to plug in complex values. Each Hurwitz space is seeded by a finite group G and $r \geq 3$ *conjugacy classes* $\mathbf{C}$ of G. These indicate our concentration on the type of ramification of covers of the projective line $\mathbb{P}^1_z$. For the cycle type of an element $g \in S_n$, the symmetric group

of degree n, a reasonable notation would be $(u_1)(u_2)\cdots(u_t)$, indicating that g is a product of disjoint cycles of respective lengths $u_1,\dots,u_t$.

For example, in S_5, (5) indicates a disjoint cycle of length 5. This stipulates g as a representative of the unique conjugacy class of 5-cycles in S_5. Yet, we can also regard a 5-cycle as an element of A_5, which has two (conjugacy) classes of 5-cycles, represented by (1 2 3 4 5) and (1 2 3 5 4).

For an example of a cover of compact Riemann surfaces, consider

$$f:\mathbb{P}^1_w\to\mathbb{P}^1_z \text{ by } f: w\mapsto \frac{w^3-1}{w^2+w+1}=\frac{f_1(w)}{f_2(w)},$$

with $f_1, f_2\in\mathbb{C}[w]$. This might have appeared in a high school SAT exam, with this question: what is f in *lowest terms*?

We would expect a student to see that the numerator and denominator have a common factor, and $f=w-1$. The degree, $\deg(f)$, then is $\max(f_1,f_2)$, *if* they are in lowest terms. The correct value of $\deg(f)$ is 1.

The Hurwitz spaces $\mathcal{H}(G,\mathbf{C})$ appeared in [**Fr77**] along with the first applications of the **BCL** giving their precise moduli fields. We concentrate on how they are *moduli spaces* of equivalence classes of covers. For given $(G,\mathbf{C})$ there are several Hurwitz spaces, depending on our choice of equivalence between covers.

Yet, all equivalences (denote such here by †) have direct interpretation on the Nielsen class, $\mathrm{Ni}(G,\mathbf{C})^\dagger$. Then the permutation representation of H_r on $\mathrm{Ni}(G,\mathbf{C})^\dagger$ produces $\mathcal{H}(G,\mathbf{C})^\dagger$ as a cover of U_r, projective r-space, $\mathbb{P}^r$, minus its descriminant locus. We use dihedral groups and alternating groups as running examples throughout the book.

Our example(s), §4.2 and §1.1, are handy in following this. The former is an exemplar continuing in several places, that starts with §2.7. That presents the absolute version as a space of rational function covers. Like in high school; as above, though not the ones you had in high school; those behind the scenes you had if you studied modular curves as in §4.2.

A context for statements on the **RIGP***:* One should be suspicious, 120+ years after Hilbert's formulation, that some *magic* – without considerable additional insight – might suddenly produce all groups as Galois groups over $\mathbb{Q}$. Generally, *nilpotent* G (product of its ℓ-Sylows) have been realized through the IGP, but mostly not at all through the **RIGP**. [1]

[1]Dividing finite groups between abelian and non-abelian, or between solvable and non-solvable, fails to capture how we display and control the relation between the **RIGP** and ℓ-adic representations. Key words for that put *nilpotent groups* on one side, and *ℓ-perfect* – referencing a prime ℓ dividing the order of the group – on the other (§1.3).

DEFINITION 1.1. If a variable ℓ, say, clearly indicates a prime, then the phrase ℓ', applied to any collection related to groups means that the collection consists of elements whose orders are prime to ℓ.

DEFINITION 1.2 (ℓ-perfect G). Complementary to nilpotent is ℓ-perfect:

$$\ell||G|, \text{ but } \mathbb{Z}/\ell \text{ is not a quotient of } G.$$

Then, ℓ' elements generate G. It is elementary that *ℓ-perfect* for all $\ell||G|$, is equivalent to G is its own commutator subgroup $[G, G]$ (again, take its closure for the profinite case): G is *perfect*.

Any nilpotent group G for which $\ell||G|$ has both a nontrivial ℓ center and a nontrivial $\mathbb{Z}/\ell$ quotient. While nilpotent groups naturally generalize abelian groups, because of their nontrivial centers, they don't amend themselves to the Hurwitz space approach. Therefore, if we consider Hurwitz spaces based on them, a $\mathbb{Q}$ point on such a space doesn't automatically give a regular realization.

This is as in Ch. 2 Thm. 1.7 whose proof uses the idea that for any G, we may form a cover $H \to G$ where H has no center. Yet, H will fail being ℓ-perfect if G is not ℓ-perfect, Still, we may substitute H for G to assume G has no center. Any regular realization of this new G makes moot one for the old G.

One problem: Most finite groups requires a different approach than anything akin to the finite group classification. For example, let us start from any group G, that is, say, ℓ-perfect and centerless. Then, there exists $v(G) > 0$ (outside a slight generalization of dihedral groups, > 1) giving the universal exponent ℓ^{k+1}-Frattini extensions

$$(\mathbb{Z}/\ell^k)^{v(G)} \to {}^{k+1}_{\ell}G \to G, k = 0, 1, \ldots, \infty \text{ (§1.4).}$$

Even for $G = A_5$, and $\ell = 2$ where $v(G) = 5$ (§1.6) for no $k > 0$ has any of these been realized over $\mathbb{Q}$, regularly or not.

PROBLEM 1.3 (Basic **RIGP** problem). For a given centerless finite group G, and field K, what are the conjugacy classes $\mathbf{C}$ for which there is a solution to the **RIGP** for $(G, \mathbf{C})$?

DEFINITION 1.4. A standout case in Cor. 4.7 has

$$\mathbb{Q}(G, \mathbf{C}) = \mathbb{Q} : \mathbf{C}^n = \mathbf{C}, \text{ for all } n \in (\mathbb{Z}/N_{\mathbf{C}})^* \text{ (2.42).}$$

We say $\mathbf{C}$ is a *rational union* of conjugacy classes; it is *necessary* for an **RIGP** solution for $(G, \mathbf{C})$ to exist over $\mathbb{Q}$, with or without fine moduli.

If we take $K = \mathbb{Q}$, then we would be satisfied with an answer like this.

Consider distinct conjugacy classes $\mathbf{C}'$ in G that form a rational union (Def. 1.4). Assume $\mathbf{C}$ runs over rational unions of conjugacy classes with support in $\mathbf{C}'$.[2] Must there be infinitely many such $\mathbf{C}$ fwith a solution to the **RIGP** for $(G, \mathbf{C})$?

For a first engagement with this problem, consider this result with the hypotheses for $\mathbf{C}'$ and $\mathbf{C}$ above. There is a solution to the **RIGP** for $(G, \mathbf{C})$ for every **PAC** subfield of $\bar{\mathbb{Q}}$ precisely for those $\mathbf{C}$ for which $\mathcal{H}(G, \mathbf{C})^{\text{in}}$ has an absolutely irrducible $\mathbb{Q}$ component as a moduli space. This holds for all but finitely many $\mathbf{C}$ satisfying this additional hypothesis:

(1.2) Each element of $\mathbf{C}'$ appears in $\mathbf{C}$ sufficiently often.

§2 discusses present knowledge of irreducible $\mathbb{Q}$ components on inner Hurwitz spaces given by such $(G, \mathbf{C}')$. On these components, running over the finite set of possible $\mathbf{C}'$, are located the $\mathbb{Q}$ points that correspond to any possible **RIGP** solutions over $\mathbb{Q}$ for G.

[**Se92**] lists just three rank > 1 *Chevalley groups* which were known to have **RIGP** realizations over $\mathbb{Q}$ in the early '90s as he completed his book. Thompson and Voeklein gave positive solutions to the **RIGP** over $\mathbb{Q}$ for many series of simple Chevalley groups of arbitrary high rank, including [**Th90**], [**Vo92**], [**Vo94**]. These all used versions of the braid group monodromy method producing explicit Hurwitz spaces with rational points from the technique behind Ch. 2 Thm. 1.7.

The **A***(*bsolute*)*IGP*:* More often we seek regular extensions $L/K(z)$ with Galois closure $\hat{L}/K(z)$ where, with $\hat{K}$ the constant field of $\hat{L}$, $G(\hat{L}/\hat{K}(z))$ is G. Then, G is the *geometric* monodromy group (of $L/K(z)$), a normal subgroup of the *arithmetic* monodromy $\hat{G} = G(\hat{L}/K(z))$ (also, $\leq S_n$).

This is a $(G, \hat{G})$ *realization*. Finding such for some $\hat{G}$ is the A(bsolute)IGP (we often care which $\hat{G}$s are achieved). For example, consider rational functions f over a number field K that have the *Schur cover property* of Prob. 1.5. Denote the residue class field of K at a prime $\boldsymbol{p}$ by $\mathbb{F}_{\boldsymbol{p}}$.

Problem 1.5. Find pairs (f, K) for which $f : \mathbb{P}^1_w(\mathbb{F}_{\boldsymbol{p}}) \to \mathbb{P}^1_z(\mathbb{F}_{\boldsymbol{p}})$ as a map is one-one for infinitely many primes $\boldsymbol{p}$ of K.

We described the solution of this problem in [**Fr17**, §2.3.2] (based on [**Fr78**, §2] and [**GuMS03**]) as leading to the relation between *absolute* and *inner* Hurwitz spaces (Thm. 3.5). That gave a general tool, for which one corollary was the first presentation of $G_{\mathbb{Q}}$ (Ch. 3 Prop. 5.9). Many practical problems that engage the properties of functions have a strong connection to the **A**(bsolute)IGP.

[2]If $\mathbf{C}$ is a rational union of classes, then the union of the distinct classes in $\mathbf{C}$ is automatically a rational union since the definition applies to the underlying sets of elements.

1.2. Groups through matrix multiplication. Behind all our geometric objects lies an interplay between non-nilpotent finite groups and actions of a quotient of the braid group. Except for the phrase "Frattini cover" (Def. 1.14) all our example finite groups appear in a first graduate algebra course.

We introduce the notation for semidirect products. As we will see, the same notation gives a memorable device for understanding some of the cohomology statements on extensions that we often use. While many readers likely have seen a treatment of this at some time, these reminders will come in handy. [**Br82**, p. 87–90] is an alternative consultation point, even if our notation differs, since we use that text and [**Nor62**], often later.

Start with an action of any group G on an abelian group A, using the notation $g * a$, $g \in G$, $a \in A$ for that action. Consider a short exact sequence

$$0 \to A \to E \xrightarrow{\psi} G \to 1, \text{ with } G \text{ acting by a fixed action on } A. \tag{1.3}$$

1.2.1. *Splittings.* Start with ψ *splittings*. This is a homorphism $G \xrightarrow{s} E$ for which $\psi \circ c_{\rm sp} = {\rm I}_G$ – the identity map on G – for which the following hold:

$$\begin{array}{c} s(G) \cap A = \{1_E\};\ s(G) \cdot A = E, \cdot \text{ indicating set theoretic product; and} \\ \text{the conjugation action of } s(G) \text{ on } A \text{ is the original action of } G \text{ on } A. \end{array}$$

DEFINITION 1.6. If ψ has a splitting, this identifies E set theoretically with $G \times A$. Denote that identification by $A \times^s G$, or $A_{\,\psi} \times^s G$ if we must indicate G acting on A through $g * a \stackrel{\rm def}{=} eae^{-1}$ for any lift e of g to E.[3]

By explicitly denoting $s(g) \in G \times A$ as $(g, c_{\rm sp}(g) \stackrel{\rm def}{=} a_g)$ we recapture that s is a homomorphism through 2×2 matrix multiplication.[4]

$$\left(\begin{smallmatrix} g_1 & a_{g_1} \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g_2 & a_{g_2} \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} g_1g_2 & g_1 * a_{g_2} + a_{g_1} \\ 0 & 1 \end{smallmatrix}\right), \text{ or } c_{\rm sp}(g_1g_2) = g_1 * c_{\rm sp}(g_2) + c_{\rm sp}(g_1).$$

Once you have determined what s does, embedding of A by $a \mapsto \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ determines the rest of the multiplication through

$$\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g & a_g \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} g & a_g + a \\ 0 & 1 \end{smallmatrix}\right).$$

The *1-cocycle* $c_{\rm sp}$ is called a *derivation*. [**Br82**, p. 88] suggests the name looks more reasonable by regarding G as acting on the right of A with the trivial action. That is, $a_{g_1} = a_{g_1} * g_2$. Maybe!

---

[3] We will take advantage of familiarity with matrix multiplication, but for permutation actions to act on the "integers" of the representation on the right.

[4] For G action on the right (as in §1.1.1): $\left(\begin{smallmatrix} g_1 & 0 \\ a_1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g_2 & 0 \\ a_2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} g_1g_2 & 0 \\ a_1 * g_2 + a_2 & 1 \end{smallmatrix}\right)$. Or when we want to include A not abelian replace $a_1 * g_2 + a_2$ by $a_1 * g_2 \cdot a_2$, as in, say, Ch. 6 §3.3.2.

We often identify the splitting s with another, say s', that differs by conjugation by an element of A. That is, if the latter were given by $g \mapsto c'_s(g)$ with

$$\left(\begin{smallmatrix} g & a'_g \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g & a_g \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right),\ a \in A \text{ independent of } g.$$

Multiplying the matrices gives $c'(g) - c(g) = a - g * a$, a *bounding* 1-cycle.

DEFINITION 1.7 ($H^1(G, A)$). The quotient, splitting 1-cycles mod bounding 1-cycles, are the elements of the first cohomology, $H^1(G, A)$, of G with coefficients in A. Given one splitting of a semidirect product, $A \times^s G$, all others are a homogenous space whose elements correspond to $H^1(G, A)$.

1.2.2. *Extensions.* Use notation for G acting on A above. Consider an extension E of G with $\ker(\psi)$ in (1.3). Refer to another extension E' of G replacing E as equivalent to (1.3) if an isomorphism $E \to E'$ induces the identity on G and on A. Even if ψ doesn't split, we may still consider a section $s : G \to E$ for ψ, though now we don't assume s is a homomorphism.

To put a group structure on $G \times A$ compatible with s, write $s(g) = (g, a_g)$ as above. We can simplify by adjusting the section so that $s(1_G) = (1_G, 0_A)$. Indeed, here we expect our choice of section only to modify the multiplication in a standard way, so to simplfy our first attempt take $a_g = 0, g \in G$.

Once we have a multiplication of the elements of the form $s(g)$, then the automatic multiplication by the elements of the form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ completes the multiplication (and so an extension E) if and only it has an identify, is associative and elements have inverses. For simplicity here denote a_{g_i} by a_i, $i = 1, 2$.

Similar to the previous, any "multiplication" on $G \times A$ forces a matrix product from a function, $c_{\mathrm{e}} : G \times G \to A$:

$$\left(\begin{smallmatrix} g_1 & a_1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g_2 & a_2 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} g_1 g_2 & g_1 * a_2 + a_1 + c_{\mathrm{e}}(g_1, g_2) \\ 0 & 1 \end{smallmatrix}\right).$$

We have just stipulated an identify. The group multiplication is associative if and only if multiplying the matrices for $(s(g_1)s(g_2))s(g_3)$ and $s(g_1)(s(g_2)s(g_3))$ have the same upper-right entry. This is equivalent to

$$c_e(g_1, g_2) + c_e(g_1 g_2, g_3) = g_1 * c_e(g_2, g_3) + c_e(g_1, g_2 g_3). \tag{1.4}$$

As for the inverse, solving for a' in

$$\left(\begin{smallmatrix} g & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} g^{-1} & a' \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \text{ gives } a' = -g^{-1} * (c_{\mathrm{e}}(g, g^{-1}) + a).$$

With the multiplication in the other direction, the unique solution for a' is $-g^{-1} * a - c_{\mathrm{e}}(g^{-1}, g)$. Apply (1.4) with $g_1 = g^{-1}, g_2 = g, g_3 = g^{-1}$ to see the inverses are the same.[5]

[5]Matrix multiplication is useful for working out particular cases, as we will, though it is equivalent to [**Br82**, p. 92], which only lists the inverse, and includes a peculiar typo.

Finally, suppose you take another choice s' of s, with $s(1) = (1_G, 0_A)$. Then, $s - s'$ is given by any function $c_{\rm b} : G \to A$ – an *A-modification* of the splitting – taking 1_G to 0_A. To compute $c'_{\rm e}$ associated to s' calculate the term that belongs in the slot labeled {??}:

$$\begin{pmatrix} g_1 & a_1+c_{\rm b}(g_1) \\ 0 & 1 \end{pmatrix}\begin{pmatrix} g_2 & a_2+c_{\rm b}(g_2) \\ 0 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} g_1g_2 & g_1*(a_2+c_{\rm e}(g_1,g_2)+c_{\rm b}(g_2))+a_1+c_{\rm b}(g_1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} g_1g_2 & \{??\}+c_{\rm b}(g_1g_2) \\ 0 & 1 \end{pmatrix}.$$

The difference $c_{\rm e}(g_1, g_2) - c'_{\rm e}(g_1, g_2)$ is

$$g_1 * c_{\rm b}(g_2) - c_{\rm b}(g_1g_2) + c_{\rm b}(g_1). \tag{1.5}$$

DEFINITION 1.8 ($H^2(G, A)$). Denote quivalence classes of extensions (1.3) with the given G action on A, modulo the A-modifications, by $H^2(G, A)$. The identity element of this abelian group is the split extension.

Why $H^2(G, A)$ is $H^2(G, A)$: We now say why this "definition" actually is what the literature calls $H^2(G, A)$. Our goal is to place the extensions of Def. 1.14) among all extensions, rather than developing cohomology theory. Still, cohomology will give us tools (as in Prop. 1.28) for actually displaying extensions in the main objects of our study.

The elements of $\mathrm{Hom}_G(\mathbb{Z}[G]^n, A)$ are given by functions from $G^n \to A$ (then extend linearly). In this case $c_{\rm e} \in C^2(G, A)$ is a function – called a *factor set* in the literature – $G^2 \to A$. Then, $\partial(c_{\rm e})(g_1, g_2, g_3)$ is just what you get from subtracting the term of (1.4) on the right, from the left side.

This piece of the projective resolution of $\mathbf{1}_G$, with this coboundary operator, is the degree 2 part of the bar resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$ module, with the cohomology defined by the quotient of the kernel of ∂ by the image of ∂ from $\mathrm{Hom}_G(\mathbb{Z}[G], A)$. That is, by applying ∂ to functions $c_{\rm b} : G \to A$ to get (1.5). Between these two examples, it should now be clear what ∂ does for general n.

REMARK 1.9. When G acts trivially on A, a 1-cocycle (derivation) is just a homomorphism $G \to A$, or $H^1(G, A) = \mathrm{Hom}(G, A)$.

REMARK 1.10 (Schur-Zassenhaus). We don't intend to limit discussing extensions, split and otherwise, to only those statements we prove. Rather to have, when we need it, appropriate reminders. For example, the following results from composing the restriction and corestriction maps on cohomology/homology (as in (6.33)).

PROPOSITION 1.11. *For $[G : H] < \infty$, A a G module, if $H^n(H, A) = 0$, then multiplication by $[G : H]$ annihilates $H^n(G, A)$.* [**Br82**, III. Prop. 10.1]

Thus, [**Br82**, IV. Cor. 3.13]) gives Schur-Zassenhaus: If $(|A|, |G|) = 1$, there is a unique, so split, extension of G when A is abelian, an essential case – the one

we use. Once you know *Feit-Thompson* – odd order groups are solvable – it is true even if A is not abelian.

REMARK 1.12 (Affect of endomorphisms). Suppose $\psi \in \mathrm{End}_G(A)$[6] (a module homorphism that commutes with the action of G). Then, ψ acts on an extension cocycle by $c_e \mapsto c_e^{\psi} : G \times G \to A$ by compositing with ψ. This, however, won't be a new cocycle, but rather one that differs from c_e by the coboundary of $a - a^{\psi}$ from replacing the original section given by $g \mapsto a_g$ by $g \mapsto a_g^{\psi}$, as in (1.5).

1.3. Frattini extensions. Groups theorists tend to love classifications, and they will tell you that there are many types of extensions of groups.

We emphasize: This book is not classifying extenions.

The group extensions – Frattini covers – of our concentration can be applied to the moduli spaces of sphere covers that appear in Ch. 2 to canonically produce the sequences of moduli spaces we call **MT**s in Ch. 4. For any finite group G and prime ℓ dividing its order, this Frattini property is what produces such towers of spaces canonically. Indeed, we can illustrate most everything in the book staying very close to one example of a pair (G, ℓ), so long as $\ell || G|$ and G has no $\mathbb{Z}/\ell$ quotient (is ℓ-perfect). To show how much the book is about classical diophantine problems, we can take the case G is a dihedral group of order 2ℓ with ℓ odd. To, however, seriously open the territory, we have only to go beyond that case, still using groups known to any graduate student in mathematics.

Going beyond the dihedral group case, requires group theory outside a 1st year graduate course. The goal of the book is to explain the properties of these tower levels, including how they get right to the heart of the **RIGP** and generalizations of the **OIT**. Especially, we require control over the components of these spaces, and of the fields over which we can assure that points of the spaces are producing sphere covers that are give positive conclusions to the diophantine problems. For starting **RIGP** applications, Ch. 3 concentrates on those *central* Frattini extensions $E \to G$ with the kernel in the commutator subgroup of G.

For any G and ℓ as above, there is a concise maximal object that gives all ℓ-Frattini covers as quotients. §1.3.1 produces that, and then §1.3.2 gives the universal object, the characteristic ℓ-Frattini module ${}_{\ell}M_G$ which controls all Frattini covers with ℓ-group kernel, and also their universal objects with abelian ℓ-group kernel. It is from these that the ℓ-adic representations of the title appear. Denote an ℓ-Sylow of G by P_{ℓ}. For very good reason[7] we divide these objects into two types.

(1.6a) Those directly derived from ${}_{\ell}M_G$.

[6]endomorphism: action on a cocycle

[7]To avoid entanglement in aspects of modular representations of finite groups classify .

(1.6b) Those from quotients of the characteristic module for P_ℓ induced to G.

Ch. 3 §2.3.2 has a homological characterization of (1.6a), using this as a primer in more sophisticated used of the Ext functor. Ch. 6 §1.5.5 gives a homological characterization of (1.6b), which is especially intended to illustrate the great number of definitions of modules for the group algebras $\mathbb{Z}/\ell[G]$ that can be so overwhelming to a beginner, including working examples of specific modular representations Ch. 6 §1.6, which we reference when suitable in earlier chapters.

1.3.1. *The Frattini construction.* A homomorphism $\psi : H \to G$ is a *cover* if it is surjective. A cover automatically produces an extension, but the kernel (as in (1.3)) is not necessarily abelian. Even so, the extensions we are about to construct, which are extreme in that they are the opposite of split, can mostly be understood from extensions with abelian kernel.

DEFINITION 1.13. Given two covers $\psi : H_i \to G$, $i = 1, 2$, their *fiber product*

$$H_1 \times_G H_2 = \{(h_1, h_2) \mid \psi_1(h_1) = \psi_2(h_2)\}$$

is a *universal target* for covers $\psi : H \to G$ factoring through ψ_i, $i = 1, 2$.

That is, given $\psi = \psi_1 \circ \psi_1' = \psi_2 \circ \psi_1'$ with $\psi_i' : H \to H_i$, there is a natural homomorphism $(\psi_1', \psi_2') : H \to H_1 \times_G H_2$. This doesn't mean ψ factors as a *cover* of the fiber product. Compare Lem. 1.16 with Lem. 2.4.

Frattini covers and kernels: For ℓ a prime, a pro-ℓ group is a profinite group for which all its finite quotients are ℓ-groups. A *projective profinite* group, P, has the property that for any cover $\psi : P \to G$, if $\psi' : H \to G$ is a cover, then there is a homomorphism (not necessarily a cover) $\psi'' : P \to H$ for which $\psi' \circ \psi'' = \psi$.

DEFINITION 1.14. We say ψ is *Frattini* if it is a group cover, and if $H^* \le H$ maps by restriction of ψ as a cover of G, then $H^* = H$.

Lem. 1.15 in some form is due to Frattini. It is akin to [**FrJ86**, Lem. 20.2]$_1$ or [**FrJ86**, Lem. 22.1.2]$_2$. While both its statements are valuable, we primarily use the former. Denote the Frattini subgroup of any (pro-)finite group G – the intersection of all (proper) maximal subgroups of G – by $\Phi(G)$.

LEMMA 1.15. *For Frattini covers $\psi : H \to G$,* $\ker(\psi)$ *is nilpotent (*Ch. 6 §1.1.1). Further, given G, $G \to G/\Phi(G)$ is the maximal Frattini cover by G.

PROOF. For the first statment, consider any $g \in G$, and choose a lift $h_g \in H$ of g to H. Then, $h_g P h_g^{-1}$ is another ℓ-Sylow of H. Apply the Sylow theorems: all ℓ-Sylows in P are conjugate in $\ker(\psi)$. Thus, $h_g P h_g^{-1} = u_g P u_g^{-1}$ for some $u_g \in \ker(\psi)$. That is, $h_g u_g^{-1}$ is in the normalizer, $N_H(P)$, of P in G.

Now consider the subgroup $N' = \langle h_g u_g^{-1} \mid g \in G \rangle$. It is in $N_H(P)$ and it covers G. Since ψ is a Frattini cover, $N' = N_H(P) = H$. Therefore P is a normal subgroup of $\ker(\psi)$ and $\ker(\psi)$ is nilpotent.

Now consider any profinite G. Suppose $M < G$ maps surjectively to $G/\varphi(G)$. With no loss, take M maximal. Since it contains $\Phi(G)$, $M/\Phi(G)$ is a proper subgroup of $G/\Phi(G)$, contrary to assumption. □

Recall the *rank*, $\mathrm{rk}(G)$, of a profinite group is the minimal number of elements generating a subgroup whose closure is G. We easily extend the notion of Frattini cover to profinite groups. Immediately, if $H \to G$ is a Frattini cover of profinite groups, then the lift of any generators of G to H gives a subgroup whose closure maps onto G. Therefore $\mathrm{rk}(H) = \mathrm{rk}(G)$. See Rem. 1.18.

LEMMA 1.16. *Assume $\psi_i : H_i \to G$, $i = 1, 2$, are Frattini covers. Then, any $H \le H_1 \times_G H_2$ that covers G automatically covers H_i, $i = 1, 2$.*

A minimal (not necessarily unique) subgroup of $H_1 \times_G H_2$ is a Frattini cover of G. From Def. 1.14, a Frattini cover $\psi : H \to G$, $\mathrm{rk}(H) = \mathrm{rk}(G)$.

Also, Frattini covers of perfect groups are perfect.

PROOF. Suppose $H \le H_1 \times_G H_2$ covers G by restriction of (ψ_1, ψ_2). Then, the image of H in H_i by projection is a subgroup of H_i that is a cover of G. Since ψ_i is a Frattini cover, the image must be all of H_i, $i = 1, 2$. If H is minimal as a cover of G, then, by definition, it must be a Frattini cover.

Now suppose G is a perfect group, and $\psi : H \to G$ is a Frattini cover. Consider the commutator subgroup $[H, H]$ of H. (If the groups are profinite, consider the *closed* subgroup generated by $[H, H]$.) It maps onto $[G, G] = G$ by ψ, and so it covers G. Since ψ is a Frattini cover, $[H, H] = H$. This concludes the proof. □

DEFINITION 1.17. Since Frattini covers of G form a projective system, they produce a profinite cover, the *Universal Frattini cover*, $\tilde{\psi}_G : \tilde{G} \to G$ that factors surjectively through any Frattini cover of G.

REMARK 1.18. [**FrJ86**, Chap. 22]$_2$ is more encyclopedic than we will be. In particular, our Frattini covers will usually have finite (or at worst, countable) rank. Larger cardinality can require more careful proof.

Constructing $\tilde{\psi} : \tilde{G} \to G$: A Frattini cover $\psi : H \to G$ is a structural idea. We apply it only to profinite groups – where *subgroup* means *closed* subgroup – and especially to finite groups. Suppose G has rank t. Denote the profinite completion of the free group F_t on t generators with respect to all subgroups of finite index by $\tilde{F}_t$. Consider any fixed map $\tilde{\psi}_t : \tilde{F}_t \to G$, by mapping generators of $\tilde{F}_t$ to $\boldsymbol{g} \stackrel{\mathrm{def}}{=} \{g_1, \dots, g_t\}$, generators of G.

LEMMA 1.19. *The group $\tilde{G}$ is a closed subgroup of $\tilde{F}_t$. Therefore, the cover $\tilde{\psi}$ is projective in the category of profinite groups.*

PROOF. Here is a way to produce $\tilde{G}$. Take the lift to $\tilde{G}$ of any collection, $\tilde{\boldsymbol{g}}$ of t elements that lift to $\tilde{F}_t$, a set of generators of G. Let $\tilde{H}_{\tilde{\boldsymbol{g}}}$ be the closure of the group generated by $\tilde{\boldsymbol{g}}$ in $\tilde{F}_t$. There is no way to assure that the natural map $\tilde{\psi} : \tilde{H}_{\tilde{\boldsymbol{g}}} \to G$ is a Frattini cover.

Still, the *axiom of choice* lets us form a maximal chain (by containment) of such covers, with an indexing $\{\tilde{H}_{\tilde{\boldsymbol{g}}_\alpha}\}_{\alpha\in I}$. By the *Tychonoff Theorem* the intersection, $\tilde{H}_\infty$, of all of the $\tilde{H}_{\tilde{\boldsymbol{g}}_\alpha}$ is closed in $\tilde{F}_t$. We easily show it is a subgroup having a limit set $\tilde{\boldsymbol{g}}_\infty$ that maps onto $\boldsymbol{g}$ by restriction of $\tilde{\psi}$. Since the chain was maximal, $\tilde{H}_\infty \to G$ must be a Frattini cover.

Should $\mu : \tilde{H}_\infty \to V$ and $\nu : V' \to V$ be covers of groups, then we can extend the map μ to $\tilde{F}_t$. Then extend μ to $\mu' : \tilde{F}_t \to V'$ and restrict μ' to give $\tilde{H}_\infty \to V'$ extending ν. This says that $\tilde{H}_\infty$ is projective. □

REMARK 1.20. If we relied on the unconstructive Lem. 1.19, we would know little of the necessary information we will need about characteristic quotients of $\tilde{G}$, as in §1.4. These provide information on the levels of the towers of the moduli spaces at the heart of this book.

REMARK 1.21. The end argument of the proof in Lem. 1.19 is a special case of a general result that closed objects of a free object are projective.

1.3.2. *Universal ℓ-Frattini covers.* Reminder: a profinite group is *nilpotent* (or *pronilpotent* in the profinite case) if it is a product of its (pro-ℓ) ℓ-Sylows. For each prime ℓ dividing the order of a nilpotent group N, there is a cover $N \to \mathbb{Z}/\ell$.

For $\psi : H \to G$ a Frattini cover, write $\ker(\psi) = \prod_{\ell_i||G|,i=1,\dots t} \ker(\psi)_{\ell_i}$ (Def. 1.14) indicating the product is over its ℓ-Sylows. For each ℓ_i, quotient out by all the ℓ_j-Sylows, $j \neq i$, in $\ker(\psi)$ to form $\psi_{\ell_i} : H_{\ell_i} \to G$.

The fiber product of the H_{ℓ_i} s over G equals H. Many structural statements on $\tilde{\psi} : \tilde{G} \to G$ appear in [**FrJ86**, Chap. 22]$_2$. We have picked some that are essential to understanding $\tilde{\psi}$ and its quotient groups. Especially as they apply to detecting components of Hurwitz spaces and constructing **M**(odular)**T**(owers).

Now decompose $\ker(\tilde{\psi}_G)$ as a product of its ℓ-Sylows.

Here are some valuable conceptual statements on pro-ℓ groups.

(1.7a) *Tate*: A closed subgroup of a pro-free pro-ℓ group is a pro-free (pro-ℓ) group, and a pro-ℓ group is projective if and only if it is pro-free, [**FrJ86**, Cor. 22.7.6 and Cor. 22.7.7]$_2$.

(1.7b) Schreier: For $\tilde{F}_t$, pro-free on t generators, a constructive procedure finds $1+n(t-1)$ independent pro-free generators of a finite index subgroup $U \leq \tilde{F}_t$ with $(\tilde{F}_t : U) = n$ [**FrJ86**, §17.5]$_2$.

(1.7c) The expression $1+n(t-1)$ from (1.7b) is a bound on the rank of any subgroup of index n in a group of rank t.

PROBLEM 1.22. Use Lem. 1.24 as a characterization of a pro-ℓ group to show (1.7a). Use (1.7b) to show that the projective cover $\tilde{\psi}_G : \tilde{G} \to G$ cannot be a profree group if at least two primes divide $|G|$. Hint: A profree group cannot be the product of 2 or more ℓ-Sylows.

DEFINITION 1.23. For each prime $\ell||G|$, there is a profinite Frattini cover

$$_\ell\tilde{\psi}_G : {}_\ell\tilde{G} \to G \text{ with } \ker({}_\ell\tilde{\psi}_G) \text{ profree, pro-}\ell\text{, of finite rank, } \mathrm{rk}({}_\ell\tilde{G}).$$

Especially, consider these points running over all such ℓ.

(1.8a) $\tilde{G}$ is projective, and equal to the fiber product over G of the ${}_\ell\tilde{G}$s (§1.3).

(1.8b) $\tilde{\psi}$ is the minimal (profinite) cover of G with all its ℓ-Sylows projective, and so pro-free pro-ℓ finitely generated groups (Prop. 1.30).

1.4. Characteristic quotients of $\tilde{\psi}_G$. We will see that Frattini covers are determined by statements about ℓ-Sylows. Although extensions given by Frattini covers do not necessarily have abelian kernels, this is compatible with similar statements about $H^n(G, A)$ being determined by statements about the ℓ-Sylows of G (see Rem. 1.25).

LEMMA 1.24. *For any pro-ℓ group, P, of finite rank, its Frattini subgroup is* $\langle [P, P], P^\ell \rangle \stackrel{\text{def}}{=} {}_{\text{fr}}P$. *That is,*

$$P/{}_{\text{fr}}P = (\mathbb{Z}/\ell)^{\mathrm{rk}(P)} \text{ is the smallest quotient of } P$$

presenting P as a Frattini cover [**FrJ86**, Lem. 22.7.4]$_2$.

PROOF. Again, the Sylow theorems: Maximal subgroups of pro-ℓ groups are normal subgroups of index ℓ. Now use that a composition of Frattini covers is Frattini. Therefore, the Frattini quotient $P/\Phi(P)$ must be $(\mathbb{Z}/\ell)^m$, since it will be an ℓ group and the minimal Frattini cover.

The quotient is abelian. So, that puts the commutator subgroup and all ℓ powers in $\Phi(P)$. As $P \to P/\Phi(P)$ is a Frattini cover, the two groups have the same rank. □

REMARK 1.25. [**Br82**, Thm. III. 10.3] notably relates the cohomology of G and restrictions of the cohomology to the ℓ-Sylows of G. For P an ℓ-Sylow of finite group G, restriction to P maps the ℓ-primary part of $H^n(G, A)$ isomorphically to the G *invariant* elements of $H^n(P, A)$. The rub is that saying the conjugation action of G

is invariant is tricky as the chains for $H^n(P, A)$ are defined by functions in $\mathrm{Hom}_{\mathbb{Z}[H]}$, not $\mathrm{Hom}_{\mathbb{Z}[G]}$ (see §1.1.1).

1.4.1. *Characteristic quotient notation.* As usual, ${}_{\mathrm{fr}}P$ is the *closed* subgroup of P *generated by* ℓ powers and commutators of P. Recover a cofinal family of finite quotients of ${}_{\ell}\tilde{G}$ through the Frattini kernel of the natural map

$$1 \to \ker_0 \to {}_{\ell}\tilde{G} \to G \to 1.$$

This produces the *characteristic sequences* of ${}_{\ell}\tilde{G}$:

$$\begin{array}{l}\text{Kernels: } {}_{\ell}\mathcal{K}_G : \ker_0 > {}_{\mathrm{fr}}\ker_0 \stackrel{\mathrm{def}}{=} \ker_1 \geq \cdots \geq {}_{\mathrm{fr}}\ker_{k-1} \stackrel{\mathrm{def}}{=} \ker_k \ldots \\ \text{Frattini Covers: } \{{}_{\ell}\mathcal{G}_G : {}^{k}_{\ell}G \stackrel{\mathrm{def}}{=} {}_{\ell}\tilde{G}/\ker_k \to G\}_{k\geq 0}.\end{array} \tag{1.9}$$

Generally we use the ˜ to indicate a *Frattini tail* is present. The projective limit of the ${}^{k}_{\ell}G$s is ${}_{\ell}\tilde{G}$. Sometimes we denote $\ker_k / \ker_{k'}$ by ${}_{\ell}M_{k,k'}$ or $M_{k,k'}$ for $k' \geq k$.

There is a natural $\mathbb{Z}/\ell[{}^{k}_{\ell}G]$ structure on ${}_{\ell}M_{k,k+1}$. Lift $g \in {}^{k}_{\ell}G$ to

$$\begin{array}{c}\tilde{g} \in {}^{k+1}_{\ell}G \text{ and act by conjugation } m \mapsto \tilde{g}^{-1}m\tilde{g} \text{ for } m \in {}_{\ell}M_{k,k+1}. \\ \text{Especially, } {}_{\ell}M_G \stackrel{\mathrm{def}}{=} {}_{\ell}M_{0,1} \text{ is the characteristic } \mathbb{Z}/\ell[G] \text{ module.}\end{array} \tag{1.10}$$

As ${}_{\ell}M_{k,k+1}$ is a(n abelian) module, the (1.10) action of $\tilde{g}$ is independent of its lift.

Example 1.26 (Prelude to a normal ℓ-Sylow). The easiest cases of (1.9) with an ℓ-perfect G are slight generalizations of D_{ℓ^u}: the *dihedral group* of order $2 \cdot \ell^u$ with ℓ odd. The quotient ${}_{\ell}\tilde{G}/\ker_k$ is $D_{\ell^{k+u}}$, and the commutators $[\ker_k, \ker_k]$ are trivial. They won't be in general.

The obvious generalization is $G = {}^{0}_{\ell}G = \mathbb{Z}/\ell^u \times^s H$, with H an ℓ' group acting faithfully through $(\mathbb{Z}/\ell^u)^*$: the ℓ-Sylow of G is normal and *cyclic*. Then, ${}^{k}_{\ell}G$ is $\mathbb{Z}/\ell^{u+k} \times^s H$ with the H action extending to $\mathbb{Z}/\ell^{u+k}$. △

Terms of ${}_{\ell}\mathcal{K}_G = \{\ker_k\}_{k=0}^{\infty}$ should reference G unless it is understood. For example, they may not be characteristic subgroups of ${}_{\ell}\tilde{G}$, as in the example for $P = {}_{\ell}\tilde{F}_t$ (1.7b). Lem. 1.26 characterizes when they are.

Abelianized quotients: We add the abelianizations of the Frattini tails:

$$\begin{array}{rl}{}_{\ell}\tilde{G}_{\mathrm{ab}(0)} & \stackrel{\mathrm{def}}{=} {}_{\ell}\tilde{G}/[\ker_0, \ker_0], \text{ abelianization from level 0.} \\ {}_{\ell}\tilde{G}_{\mathrm{ab}(k_0)} & \stackrel{\mathrm{def}}{=} {}_{\ell}\tilde{G}/[\ker_{k_0}, \ker_{k_0}], \text{ abelianization from level } k_0.\end{array}$$

So long as there can be no confusion, we will denote ${}_{\ell}\tilde{G}_{\mathrm{ab}(0)}$ as ${}_{\ell}\tilde{G}_{\mathrm{ab}}$,

$$\begin{array}{c}\text{the Universal abelianized } \ell\text{-Frattini cover of } G: \\ V_{G,\ell} \stackrel{\mathrm{def}}{=} (\mathbb{Z}_\ell)^{\nu(G,\ell)} \to {}_{\ell}\tilde{G}_{\mathrm{ab}} \to G, \nu(G,\ell) = \dim_{\mathbb{Z}/\ell}({}_{\ell}M_{0,1}).\end{array} \tag{1.11}$$

It is universal for covers of G with abelian ℓ-group as kernel. Akin to (1.9), consider the sequence

$${}_{\ell,\mathrm{ab}}\mathcal{G}_G : \{ {}_{\ell}\tilde{G}_{\mathrm{ab}}/\ell^k V_{G,\ell} \stackrel{\mathrm{def}}{=} {}^{k}_{\ell}G_{\mathrm{ab}} \to G\}_{k\geq 0}.^{8} \tag{1.12}$$

[8]Here, with $\nu(G, \ell, k_0) = \dim_{\mathbb{Z}/\ell}({}_{\ell}M_{k_0,k_0+1})$, is a variant for abelianization from k_0:

$${}_{\ell,\mathrm{ab}(k_0)}\mathcal{G}_G : \{ {}_{\ell}\tilde{G}_{\mathrm{ab}(k_0)}/\ell^{k-k_0}(\mathbb{Z}_\ell)^{\nu(G,\ell,k_0)} \stackrel{\mathrm{def}}{=} {}^{k}_{\ell}G_{\mathrm{ab}(k_0)} \to G\}_{k\geq k_0}.$$

Sometimes, when G is a semidirect product $P \times^s H$, with P an abelian ℓ-Sylow, we require abelianization *right from the top*, as in $\tilde{P}/[\tilde{P},\tilde{P}] \times^s H$ (notation as in Prop. 1.30). Then we use the notation ${}^k_\ell G_{\mathrm{ab}(-1)}$. In rare cases, P may only be a subgroup of the ℓ-Sylow:

$$\ell \| H| \text{ as in the case } \ell = 2 \text{ in §3.2.}$$

That G module ${}_\ell M_{0,1}$ in (1.11) replicates as

$$\text{the kernel of } {}^{k+1}_\ell \tilde{G}_{\mathrm{ab}} \to {}^k_\ell \tilde{G}_{\mathrm{ab}}.$$

Exchanging $\mathbb{Z}/\ell[G]$ modules for $\mathbb{Z}[G]$ modules changes some crucial details about the modules. Ch. 6 §1.6 gives guidelines in going mod ℓ (*modular representations*) including that the theory of projective modules in characteristic ℓ is different.

REMARK 1.27 (${}_\ell \tilde{G} \neq {}_\ell \tilde{G}_{\mathrm{ab}}$). Unless the rank of $\ker({}_\ell \tilde{G} \to G)$ is $t = 1$, the only case where the pro-free group of rank t is abelian, ${}_\ell \tilde{G}$ can never equal ${}_\ell \tilde{G}_{\mathrm{ab}}$. This follows from (1.7a) because the ℓ-Sylow of ${}_\ell \tilde{G}$ is a pro-free pro-ℓ group. From (1.7b), its finite index subgroup is also.

1.4.2. *${}_\ell \tilde{G}$ vs ${}_\ell \tilde{G}_{\mathrm{ab}}$ and non-perfect primes.* In application to the **RIGP**, accomplishing such regular realizations over certain fields is clearly stronger using the whole Frattini cover ${}_\ell \tilde{G} \to G$, as in §6.2. Yet, an important theme in the book is the pure diophantine difficulty of finding solutions to the **RIGP** as opitomized by the Main Conj. 3.1 of **MT**s, and the cases where that conjecture has been proven.

Here then, understanding the difficulty – as a generalization of results on modular curves – is strengthened using formulations with the cover ${}_\ell \tilde{G}_{\mathrm{ab}} \to G$.[9] Also, using ${}_\ell \tilde{G}_{\mathrm{ab}}$ is the right level to make positive comparisons of the **OIT** generalization with Serre's result.

Denote by G_{abq} the maximal abelian quotient, $G/[G,G]$ of G. The primes ℓ dividing $|G_{\mathrm{abq}}|$ are exactly those for which G is not ℓ-perfect (as in Def. 1.2). Usually, when using ${}_\ell \tilde{G}$, we assume G is ℓ-perfect. Alas, we have these opposing considerations on including $\ell || G_{\mathrm{abq}}|$.

(1.13a) Including such ℓ without modification won't give a canonical tower of Hurwitz spaces from $(G, \mathbf{C}, \ell)$.

(1.13b) Excluding all the ℓ-Frattini extensions associated with $(G, \mathbf{C}, \ell)$ leaves out towers and **RIGP** possibilities with classical consequence.

The point of (1.13a) appears in the proof of Prop. 3.4. Examples of (1.13b) – a process we call *folding under* the Frattini extensions from $\ell || G_{\mathrm{abq}}|$ – are required to extend Serre's **OIT**, for example as explained in Ch. 6 §3.3.3. So, we cannot, quite,

[9]There are, Ch. 6 §1.7, maximal nilpotent and solvable quotients of G.

dismiss non-perfect primes, though pure nilpotent groups don't lend themselves to the moduli space approach.

1.4.3. *Preliminary grasp of ${}_\ell M_G$.* This section is a guide to where we will concentrate on using the universal Frattini cover.

Significant quotients of $\tilde{G} \to G$: Prop. 1.30 gives the first constructive aspects on describing $\tilde{G} \to G$, the case where the ℓ-Sylow of G is normal. These continue as "ℓ pieces Parts 3 and 4" (resp. Ch. 3 Prop. 2.18 and Ch. 6 Prop. 1.28), to describe, more deeply, the universal ℓ-Frattini extensions of an ℓ-perfect G.

DEFINITION 1.28 (Universal elementary ℓ-extension). To understand either the abelianized Universal ℓ-Frattini, or the general ${}_\ell\tilde{G} \to G$, we start with

$$ {}_\ell M_{0,1} = {}_\ell M_G = \ker({}_\ell\tilde{\psi}_{\rm ab})/\ell \ker({}_\ell\tilde{\psi}_{\rm ab}) \text{ as in (1.10).}$$

PROPOSITION 1.29 (ℓ pieces: Part 1). *Fiber products of ${}_\ell\tilde{\psi}_{\rm ab}$, running over $\ell||G|$, give $\tilde{\psi}_{\rm ab} : \tilde{G}/[\ker(\tilde{\psi}), \ker(\tilde{\psi})] \to G$.*

Using conjugation, as in (1.10), $\ker({}_\ell\tilde{\psi}_{\rm ab})$ *is naturally a free $\mathbb{Z}_\ell[G]$ module extending the $\mathbb{Z}/\ell[G]$ module structure on ${}_\ell M_{0,1}$. Then,*

$$\sum_{\ell||G|} \dim_{\mathbb{Z}/\ell}({}_\ell M_G) \le 1 + |G|(\text{rank}(G)-1). \tag{1.14}$$

If $H \le G$ is an ℓ' group, by applying Schur-Zassenhaus, embed H in ${}_\ell\tilde{G}$ (up to conjugacy). Then each of the ${}^k_\ell G$ s inherits a compatible system of coset representations (meaningfully designated by a single symbol T_H).

PROOF. Excluding (c) the proposition pieces have all been proved above (or in their statement). For the exception use (1.7c). This bounds the rank of $\ker({}_\ell\tilde{\psi})/(\ker({}_\ell\tilde{\psi}), \ker({}_\ell\tilde{\psi}))$, which is the same as the rank in the sum in (c). □

Prop. 1.30 gives our first structural statements on $\tilde{G}$.

PROPOSITION 1.30 (ℓ pieces: Part 2). *Any automorphism of G extends to $\tilde{G}$, and for K a characteristic subgroup of $\tilde{G}$, to $\tilde{G}/K$. Denote an ℓ-Sylow of G by P_ℓ.*

(1.15a) *If P_ℓ is normal, then with $H = G/P_\ell$, ${}_\ell\tilde{G} = \tilde{P}_\ell \times^s H$,*

$$\tilde{P}_\ell = {}_\ell\tilde{F}_{\text{rk}(P)}\text{; } \times^s \text{ indicating } H \le \text{Aut}(G) \text{ extends to } \text{Aut}(\tilde{G}).$$

(1.15b) *All such extensions of H to ${}_\ell\tilde{G}$ differ by a conjugation from ${}_\ell\tilde{G}$.*

Characterize ${}_\ell\tilde{G}$ (resp. $\tilde{G}$) as the minimal profinite cover $\tilde{G}^* \to G$ for which the (resp. all) ℓ-Sylow(s) of $\tilde{G}^*$ is (resp. are) ℓ-free.

CONSTRUCTION COMMENTS. Consider the first statement with $\alpha : G \to G$ an automorphism. Then, $\alpha \circ \tilde{\psi}_G : \tilde{G} \to G$ is a Frattini cover of G

$$\text{giving a morphism } \tilde{\alpha} : \tilde{G} \to \tilde{G} \text{ for which } \tilde{\psi}_G \circ \tilde{\alpha} = \alpha \circ \tilde{\psi}_G.$$

The image of $\tilde{\alpha}$ is a subgroup of the Frattini cover $\tilde{G} \to G$ that maps surjectively to G. Therefore $\tilde{\alpha}$ maps surjectively to $\tilde{G}$. Since $\tilde{G}$ is finitely generated, $\tilde{\alpha}$ is an isomorphism [**FrJ86**, Prop. 15.3]$_1$.[10] Then, if K is a characteristic normal subgroup of $\tilde{G}$, by definition the automorphism will preserve it, producing an automorphism of the quotient of $\tilde{G}/K$.

Now consider (1.15a). Under the hypothesis, if we can extend the action of $H = G/P$ to $\tilde{P}$, then we have a Frattini cover with a pro-free pro-ℓ Sylow. So it must be the ℓ-Frattini cover of G. Let $t = \mathrm{rk}(P)$.

From the above, each $h \in H$ extends to an automorphism, $\tilde{h}$, of $\tilde{P} = {}_\ell\tilde{F}_t$, a rank t cover of P. From Lem. 1.26, the group $\tilde{H}$ generated by $\{\tilde{h} \mid h \in H\}$ is profinite. Now apply the profinite Schur-Zassenhaus [**FrJ86**, Lem. 22.10.1]$_2$; extending from finite to profinite is an exercise.

Albeit, we can profitably consider that extension's nature, as in Ex. 1.29, where $P = (\mathbb{Z}/\ell)^t$ in (1.15a). The last paragraph of the proposition generalizes a cohomological statement that a $\mathbb{Z}[G]$ module M is projective if and only if it passes the homological criteria that it is ℓ-projective for each prime $\ell||G|$. Or use [**FrJ86**, §22.4]$_2$ to interpret that directly using elementary abelian ℓ-groups for M. □

Source of algebraic equations: The remaining sections of this chapter introduce the moduli space pieces from which we produce the towers of spaces that apply the Frattini constructions. Monodromy action on various objects, including ℓ-adic representations, comes from a *braid group action* on Nielsen classes, starting in §3.1.3. The beginning objects are tagged by a pair $(G, \mathbf{C})$ with $\mathbf{C}$ the r generating conjugacy classes of G we have discussed in the table of contents, and reintroduced again at the beginning of this chapter.

As previously we simplify by referring to any one of the objects given by, say, an inner equivalence class of covers of $\mathbb{P}^1_z$, by $\mathcal{H}(G, \mathbf{C})$. Suppose we only consider each group G separately and the full collection $I_{G,\mathbb{Q}}$ of conjugacy classes $\mathbf{C}$, that produce spaces $\{\mathcal{H}(G, \mathbf{C})\}_{\mathbf{C}\in I_{G,\mathbb{Q}}}$ each of which – by the Branch Cycle Lemma – has its moduli structure defined over $\mathbb{Q}$, so that $\mathbb{Q}$ points on any one of them gives a regular realization of G. Then, specific inspection of these spaces encapsulates the **RIGP**(as in §1.1) and we make much of this alone in Ch. 4.

A more complete set of mysteries unfolds, though, when we consider for a pair (G, ℓ), with a G that is ℓ-perfect, the possibillity of the **RIGP** applied to the collection $\mathcal{G}_\ell \stackrel{\text{def}}{=} \{{}^k_\ell G\}_{k=0}^\infty$. For example consider this question.

QUESTION 1.31. What prevents, for a given choice of ℓ, finding an integer r_0, such that these hold for $k \geq 0$?

[10] This would be obvious if G is finite. It becomes so for finitely generated profinite groups because the intersection of all subgroups of finite index, say n, both of finite index and characteristic.

(1.16a) There is a collection of classes $\mathbf{C}_k$ in ${}^k_\ell G$ having exactly r_0 classes.

(1.16b) There is a $\boldsymbol{p}_k \in \mathcal{H}({}^k_\ell G, \mathbf{C}_k)(\mathbb{Q})$, giving an **RIGP** realization of ${}^k_\ell G$.

What we find from (1.16) is that for all but a finite number of k, the $\mathbf{C}_k$ s consist only of elements prime ℓ. Therefore, by Schur-Zassenhaus, these can be taken to be given by r_0 classes $\mathbf{C}$ in $G = {}^0_\ell G$ and, without loss, each class in $\mathbf{C}$ lifts uniquely to a conjugacy class in ${}^k_\ell G$ to give $\mathbf{C}_k$.

Now, label each of the $\mathbf{C}_k$ s as $\mathbf{C}$. Then, the spaces $\mathcal{H}({}^k_\ell G, \mathbf{C})$ form a projective sequence of covers of $\mathbb{P}^r \setminus D_r = U_r$. The conclusion of an affirmative answer to Ques.1.31 is then this Ch. 3 §3.1.

COROLLARY 1.32. *For each k there is a natural absolutely irreducible $\mathbb{Q}$ component,*[11] *$\mathcal{H}'_k$ of $\mathcal{H}({}^k_\ell G, \mathbf{C})$ such that the collection forms a projective system. Further, there is $\{\boldsymbol{p}_k \in \mathcal{H}'_k(\mathbb{Q})\}_{k=0}^\infty$.*

There are three points about this.

(1.17a) The Main Conjecture is that the last sentence (about existence of $\mathbb{Q}$ points) is not possible, and for $r_0 = 4$ (or 3), this impossibility is known.

(1.17b) From these $\mathcal{H}'_k$ we get sequences of spaces whose properties – like having no $\mathbb{Q}$ points at high levels – generalize conjectured and proven properties of classical spaces that can be attached to a particular G.

(1.17c) In the proven and conjectured properties above, it appears that everything goes through with ${}^k_\ell G$ replaced by ${}^k_\ell G_{\text{ab}}$.

In (1.17b), the ever present example in this book is of modular curves as attached to the dihedral groups of order 2ℓ. This starts in Ex. 2.7 , continues in Ch. 2 §3.2 and culminates in Ch. 6 §3.2. Directly branching from this are the cases of spaces of hyperelliptic Jacobians (as in [**DFr90**] and Ch. 3 §3.2.1), and slightly more generally, spaces of superelliptic jacobians, as in [**MaSh19**]. At this time we don't know what literature might relate to the spaces for general finite groups G.

Source of ℓ-adic representations: Ultimately, the ℓ-adic representations of the book's title stem from,

the Universal abelianized ℓ-Frattini cover of G.

Here is the general rubric for that. Analogous to (1.11) where ν is $\nu(G, \ell)$, consider any short exact sequence $(\mathbb{Z}_\ell)^\nu \to {}_\ell\tilde{G}^* \to G$ for which ${}_\ell\tilde{G}^* \to G$ is an ℓ-Frattini cover. This defines a sequence of groups ${}^k_\ell G^*_{\text{ab}}$, each a quotient of ${}^k_\ell G^*_{\text{ab}}$, $k \geq 0$.

So long as elements of $\mathbf{C}$ have order prime to ℓ, this gives a projective sequence of covers $\{\mathcal{H}({}^k_\ell G^*_{\text{ab}}, \mathbf{C})\}_{k=0}^\infty$. There are natural conditions for these spaces to be

[11] This includes the moduli properties inherited from $\mathcal{H}({}^k_\ell G, \mathbf{C})$.

nonempty, to compute their (moduli) definition fields, and to have fine moduli, all explained in the upcoming sections.

It is the braid action, §3.1.3, on Nielsen classes that gives the monodromy action on ℓ-adic modules. If $\boldsymbol{p}_0^* \in \mathcal{H}({}_\ell^k G_{\rm ab}^*, \mathbf{C})$ has definition field K, it is the G_K action on projective sequences of points over $\boldsymbol{p}_0^*$ on these spaces that defines the ℓ-adic representations.[12]

Thus, we regard the sequence from (1.11) as *maximal* among those giving ℓ-adic representations that arise from $(G, \ell, \mathbf{C})$. Yet, there may be other choices for ${}_\ell\tilde{G}^* \to G$ with the necessary ℓ-Frattini property to naturally define Hurwitz space sequences. The most conspicuous comes from using, instead of G, the normalizer, N_ℓ, in G, of an ℓ-Sylow of G.

Take the sequence $(\mathbb{Z}_\ell)^{\nu'} \to \tilde{N}_\ell \to N_\ell$ analogous to that for G. The module action induced from N_ℓ to G on $(\mathbb{Z}_\ell)^{\nu'}$ then produces such a G^*. Often, this is a *minimal* – and more computable – ℓ-adic representation attached to $(G, \ell, \mathbf{C})$.

Finally, we don't neglect that all of these groups ${}_\ell^k G^*$ (with and without the ${}_{\rm ab}$ subscript) present challenges to the **RIGP** and its relation to the IGP.

Guidance on mod ℓ *representations:* While the book will gives examples, as guidance, we thankfully don't need a general classification of the representations of G that appear in (1.11). Besides, group theorists and computer scientists consider that – in detail as one understood collection – this is essentially impossible.

Yet, In our applications, we always need to know nontrivial structural data on $\mathbb{Z}/\ell[G]$ quotients of ${}_\ell M_G$. Here we point preliminarily to appropriate results. The classification of representations of finite groups is a starting model for these modular representations. In characteristic 0, a module not a direct sum of two proper submodules (is *indecomposable*) if it has no proper submodules at all.

That is no longer true for $\mathbb{Z}/\ell[G]$ modules. Indeed, a simple first definition is the maximal quotient $M/\mathrm{Rad}(M)$ of M which is a *completely reducible*: A direct sum of irreducible $\mathbb{Z}/\ell[G]$ modules. See Ch. 6 (6.15a) for the names attached to the *Loewy series* resulting from this definition. Also, it is standard (and often necessary), for applying classification theorems of modules, to tensor with an algebraic closure, $\bar{F}$, of the quotient field F of the base ring. We aren't classifying anything. Although all the Frattini extensions of §**??** are significant to all our considerations, we restrict particular examples to more easily recognizable quotients of these.

Ch. 3 Lem. 2.15 and Prop. 2.16 give precise homological characterizations of ${}_\ell M_G$. Ch. 3 Prop. 2.18 says, if G is ℓ-perfect and centerless, then the same is true

[12]The situation without the ${}_{\rm ab}$ subscript makes sense, but for that we would have to decorate these actions as nilpotent, since they come from the nilpotent completion of the fundamental group of the Riemann surface attached to $\boldsymbol{p}_0$, something we aren't quite ready for.

of all the characteristic ℓ-Frattini quotients ${}^k_\ell G$, $k \geq 0$. This is crucial to their use on **MT** levels, giving all those levels *fine moduli space* properties.

Quotients, of say $\ker({}^1_\ell G \to G)$, on which G acts trivially, give *central ℓ-Frattini extensions*. This is a dominant theme in Ch. 3, the book's center, for detecting components of Hurwitz spaces. Also for properties of those spaces on their boundary (cusps). Frattini central extensions have two types, Ext and **Comm** in §2.1 which describes both cohomologically. This is in the service of the *general lift invariant*.

Since the **Comm** type central extensions are so mysterious, explicating them in important cases is an additional reason for investigatng the kernel of, say, ${}^1_\ell G \to G$; Prop. 1.30 is a first result in that direction.

2. Nonsingular sphere covers and Galois closure

The author, here, as in his papers, acts by permutations on the *right* of the symbols of the permutation representation. Most of this section and the next applies to any cover of compact Riemann surfaces. When, however, we start to compute how covers work, we deal primarily with sphere covers: $\varphi : W \to \mathbb{P}^1_z$. These ramify if $\deg(\varphi) > 1$, since the sphere is simply connected.

2.1. Algebraist's Galois closure. One of the techniques that appears in considering sphere covers, especially, when they are used in (Hurwitz) families is to start with covers that aren't Galois. Then go to their *Galois closures*. We give a general construction for the Galois closure of a cover $\varphi : W \to Z$ of *normal*, quasi-projective (locally closed subspaces of some projective space) varieties, with W irreducible, over a field K. T

There is no reason to assume φ, with $\deg(\varphi) = n$, is étale. Let us, however, say that it is finite, flat and separable, and indicate the degree (well-defined from flatness) by $n = n_\varphi$. This is what Grothendieck called a (not necessarily étale) *cover*. §2.1.1 constructs the Galois closure group, G_φ, and natural permutation representation, T_φ, attached to φ, a slight abstraction of [**BFr02**, §3.1.3].

2.1.1. *Fiber product construction.* Take the set theoretic fiber product of the cover φ, n times:

$$W_\varphi^{(n)} = \{(w_1, \dots, w_n) \in W^n \mid \varphi(w_1) = \cdots = \varphi(w_n)\}. \tag{1.18}$$

There are components we don't want: Those where the whole component has n-tuples with two entries (or more) that are equal. That collection, denoted Δ_n, is called the *fat diagonal*.

Now remove Δ_n, referring to the result as W_φ^0. Then, S_n still acts on it by permuting coordinates. Normalization of a projective variety, X, in a finite extension,

F, of its field of functions $K(X)$, is a topic found in [**Mu66**, p. 396-397].[13] We have used it often, say, as in [**Fr77**, p. 36] akin to as in the Comments of Prop. 3.5, to generalize what is below to form families of Galois closures of covers.

For a complex analytic space, X, the main category in this book, there is a natural local definition of normalization. At each $\boldsymbol{p} \in X$, there is ring (integral domain), $R_{\boldsymbol{p}}$, of local holomorphic functions (precisely the meaning of an analytic space) about $\boldsymbol{p}$. That right has a quotient field $K_{\boldsymbol{p}}$, and normal means that at each point the integral closure of $R_{\boldsymbol{p}}$ in $K_{\boldsymbol{p}}$ is just $R_{\boldsymbol{p}}$. With this we can also discuss normalization of X.

Assuming X has a single component, we must consider that its (function) field of meromophic function may actually have no nonconstant meromorphic functions. By contrast, projective algebraic varieties have a function field which determines them up to birational morphism. Here are some other points.

(1.19a) There is a natural algebraic map from the normalization, $\tilde{X}_F$ of X in F to X (defined on geometric points): $\tilde{\psi}_F : \tilde{X}_F \to X$.

(1.19b) We call X normal if $\tilde{\psi}_{K(X)}$ is an isomorphism.

(1.19c) If X is normal and projective, then so is $\tilde{X}_F$.

(1.19d) If X is normal, it is nonsingular in codimension 1.

We start off Ch. 2 explaining precisely why we need normalization and projective varieties, rather than just complex analytic spaces.

Back to W^0_φ, (1.18) with the fat diagonal removed.

(1.20a) Normalize the result, W^0_φ, in the function field of each component. You don't have to do this if φ is étale.

(1.20b) Denote any *irreducible* K-component of W^0_φ, by $\hat{\varphi} : \hat{W} \to Z$ (as a cover). From normalization, (1.19d), all components are disjoint.

See §1.1.1 for the notation we will use for permutation representations. Then, $\hat{\varphi}$ is a Galois closure of φ. (See §1.4.1 for a little categorical glitch if it should turn out that $\hat{W}$ is singular.) §3.2 illustrates Lem. 2.1 in detail in our running example on dihedral groups. For $H' \le H$, denote the normalizer of H' in H by $N_H(H')$.

2.1.2. *The canonical permutation representation.* Classical problems didn't feature the Galois closure of a cover. Simple versions of the Inverse Galois problem emphasized it only. The connection between the two is the canonical permutation representation.

LEMMA 2.1. *The group, $G_\varphi \le S_n$, of $\hat{\varphi}$, appears as the elements of S_n that leave $\hat{W}$ fixed. It is a Galois cover because G_φ acts transitively on each fiber over*

[13] Actually, in either [**H77**] or [**Mu66**], fields of definition are almost always algebraically closed, compatible with the interests of those authors.

Z. By restriction $\hat{W}$ has a projection onto each copy of W in the fiber product. Say, project on the 1st.

That cover is also Galois, with group $G(T_\varphi, 1)$. Then, T_φ is the permutation representation of G_φ on the cosets of $G(T_\varphi, 1)$, where we can take 1 to correspond to the coset of the group element 1.

The collection of components of W_φ^0 with the exact same $G_\varphi \leq S_n$ correspond to the elements of the quotient $N_{S_n}(G_\varphi)/G$.

PROOF. Since S_n is transitive on the fibers of $W_\varphi^0 \to Z$, so too will be G_φ as the elements leaving $\hat{W}$ fixed, showing the $\hat{\varphi}$ is Galois. The rest of the first two paragraphs is already explained from this.

Now suppose $\hat{W}'$ is another component of W_φ^0, and the elements in S_n that leave it fixed form the group G'_φ. From transitivity of S_n on the components, there is $g \in S_n$ that maps $\hat{W}_\varphi \to \hat{W}'_\varphi$. Then, $gG'_\varphi g^{-1}$ also consists of elements in S_n that leave $\hat{W}_\varphi$ fixed (note: we are acting as we mostly do on the right). If we assume that $G'_\varphi = G_\varphi$, then this implies $g \in N_{S_n}(G_\varphi)$, This is reversible and gives the last paragraph of the lemma. □

The attached permutation representation: The significance of the following lemma is that it ties together the fundamental condition called *fine moduli* (see §3) for covers where equivalence is called *absolute* to that for covers where equivalence is called *inner*.

DEFINITION 2.2. For a pair (G, T) where T is transitive and faithful, consider the normalizer, $N_G(G(T,1))$, of $G(T,1)$ in G.

$$\text{Call } (G,T) \textit{ self-normalizing} \text{ if } N_G(G(T,1)) = G(T,1).$$

Consider $\mathrm{Cen}_T(G) = \{h \in S_n \mid hgh^{-1},\ \forall g \in G\}$.

LEMMA 2.3. *Then, $\mathrm{Cen}_T(G) = N_G(G(T,1))/G(T,1)$ is isomorphic to the automorphisms of W that commute with φ. If G is self-normalizing, then φ has no automorphisms (analytic isomorphisms that commute with φ). Further, G is centerless. That the representation is faithful means $\cap_{i=1}^n G(T,i)$ is trivial.*

A decomposition of $\varphi : W \to Z$ into a chain of (normal) covers

$$\varphi_1 : W \to W_2 \xrightarrow{\varphi_2} Z$$

corresponds to a subgroup $G(T,1) \leq H \leq G$, with the degrees of φ_i, $i = 1, 2$, respectively equal to $(G : H)$ and $(H : G(T,1))$.

PROOF. The interpretation of the automorphisms of φ as $N_{G(T,1)}(G)/G(T,1)$ is [**Fr77**, Lem. 2.1]. Then, [**Fr77**, Lem. 2.2] identifies this group with the complete

centralizer of G in S_n. Since we make use of it often, here is the argument that says self-normalizing implies G is centerless.

Suppose $g \in G$ is in the center. Then, $gG(T,1)g^{-1} = G(T,1)$ and so $g \in G(T,1)$. Since T is transitive, for each $i \in \{1,\dots,n\}$, there exists an $h \in G$, for which $(1)T(h) = i$. Then, $h^{-1}gh = g$ takes i to i. Since this holds for all i, and T is faithful, g is trivial.

The correspondence between covers between W and Z with subgroups between $G(T_1,1)$ and G is a special case of the Galois correspondence. □

Reasonably we ask: What is the pair (G_φ, T_φ) given φ? A good answer requires significant labels for such pairs. Considering our limited understanding of finite groups, we must separate such pairs using other concepts. See Ch. 6 §1.1, especially compare the cases when φ does not or does *decompose*, as $\varphi_2 \circ \varphi_1$ with $\deg(\varphi_i) > 1$.

2.1.3. *Group of an equation a la Galois.* Suppose $f(y)$ is a degree n, separable and *irreducible*, polynomial over a field K. For simplicity on a critical point, we will assume – somehow – you have managed to find these roots as particular complex numbers in $\mathbb{C}$. We list them as $\{\alpha_1,\dots,\alpha_n\}$. Then, the sought for Galois group appears as the group of permutations of $\{\alpha_i\}_{i=1}^n$ given as *field automorphisms* of the extension $\hat{K}_f = K(\alpha_1,\dots,\alpha_n)/K$. That, however, leaves a mystery: like, how do you detect field automorphisms?

The vector space $V_k = \{\sum_{j=0}^{n-1} m_j \alpha_k^j\}$ equals the field $K(\alpha_k)$. Further, the substitution map $s_{k,k'} : \alpha_k \mapsto \alpha_{k'}$ gives a natural field isomorphism $V_k \to V_{k'}$. Alas, since $V_{k'}$ is not necessarily equal to V_k, this may not be an automorphism, and V_k is not $\hat{K}_f$. [14]

Our comments below are basic Galois theory, Yet, like a foreign language learned after childhood, they are easily forgotten. Here are reminders.

Apply to $\mathrm{Spec}(K[y]/(f(y)) \to \mathrm{Spec}(K)$ the n-fold fiber product construction of §2.1.1. At the level of taking the tensor product of rings, associate a direct summand of the ring tensor product, to the Galois closure. Since, however, that's not the way it is done in algebra courses, consider one classical construction, of a polynomial $\hat{f}(y)$, for which any *one* of its roots gives K_f.[15] It goes, over K, like this.

Form any linear combination $L_{\boldsymbol{a}} \stackrel{\text{def}}{=} L_{\boldsymbol{a}}(\boldsymbol{\alpha}) \stackrel{\text{def}}{=} \sum_{i=1}^n a_i\alpha_i$ of the roots of $f(y)$, $a_i \in K$. For $\tau \in S_n$ use the notation $L_{\boldsymbol{a}}((\boldsymbol{\alpha})\tau) \stackrel{\text{def}}{=} \sum_{i=1}^n a_i\alpha_{(i)\tau}$.

(1.21a) Choose $\boldsymbol{a}$ so that the $L_{\boldsymbol{a}}((\boldsymbol{\alpha})\tau)$, for $\tau \in S_n$, are distinct.

(1.21b) Choose $\hat{f}$ to be an irreducible factor (over K) of $\prod_{\tau\in S_n}(y - L_{\boldsymbol{a}}((\boldsymbol{\alpha})\tau))$.

Comments on (1.21a)*:* Having f an irreducible polynomial K implies their quotient rings are fields. Since we don't know $\{\alpha_1,\dots,\alpha_n\}$, we cannot a priori pick

[14] Indeed, for $k \neq k'$, $V_k \cap V_{k'} = K$, unless RETURNM

[15] Perhaps due to van der Waerden, but compatible with Galois.

those coefficients $\boldsymbol{a} = a_1, \dots, a_n$, though their existence is assured by avoiding values $\boldsymbol{a} \in K^n$ that lie on the union of the hyperplanes

$$\left\{(x_1, \dots, x_n\} \stackrel{\text{def}}{=} \boldsymbol{x} \in \mathbb{C}^n \mid L_{\boldsymbol{x}}((\boldsymbol{\alpha})\tau) - L_{\boldsymbol{x}}((\boldsymbol{\alpha})\tau'), \tau, \tau' \in S_n, \tau \neq \tau'\right\}.$$

Alas, it is hard to detect when a particular permutation is a field automorphism. So, it is hard to compute G_P. A more positive approach uses the case above:

(1.22) replacing α_1 by $L_{\boldsymbol{a}}$, a single field generator of $K(\alpha_1, \dots, \alpha_n)$.

The effect of an automorphism τ on $K(\alpha_1, \dots, \alpha_n)$, is determined by $L_{\boldsymbol{a}} \mapsto L_{(\boldsymbol{a})\tau}$, one of the conjugates of $L_{\boldsymbol{a}}$: zeros of the irreducible polynomial for $L_{\boldsymbol{a}}$ over K–whose degree we take to be N.

Also, each α_k equals $A_k(L_{\boldsymbol{a}}), k = 1, \dots, n$, with $A_k \in K[y]$, a polynomial of degree $\leq N-1$. The effect of any $L_{\boldsymbol{a}} \mapsto L_{(\boldsymbol{a})\tau}$ is given by this substitution in the A_k s. Thus, the elements in $G_P \leq S_n$ correspond to these substitutions: G_P consists of $\{\tau_1, \dots, \tau_N\}$.

Comments on (1.21b)*:* You can avoid making any choices for $\boldsymbol{a}$ by using the variables $\boldsymbol{x}$ above, and forming the product

$$f^*_{\boldsymbol{x}}(y) = \prod_{\tau \in S_n} \big(y - \sum_{i=1}^{n} \alpha_{((i)\tau} x_i\big) \in K[\boldsymbol{x}].$$

Then, find an irreducible factor, $\hat{f}_{\boldsymbol{x}}(y)$, of it in $K[\boldsymbol{x}]$.

The group G_f of f is $\{\tau \in S_n \mid \hat{f}_{(\boldsymbol{x})\tau}(y)$ identically equals $\hat{F}_{\boldsymbol{x}}(y)\}$.

Any of these definitions work. The geometric one of the previous section – with only one significant choice; picking a connected component or irreducible factor – works especially well for understanding using components of Hurwitz spaces as moduli for variants on the **RIGP**.

REMARK 2.4. In a tasteful, rather nice book, after noting that Galois introduced the word and full concept of (finite) group (quoting [**Gal31**]), [**St10**, p. 391] says:

> Galois produced [the group, G_E, of an equation called E] as the permutation of roots that leave rational functions of the coefficients unaltered ....

A typo or a misunderstanding, by me or by him? Later, [**St10**, p. 413] says

> We may be fairly sure that whatever Galois did was later superceded by Riemann.

Like many I am totally in the thrall of Riemann – as in [**Fr02b**]. Yet, you won't find in Riemann, Galois's intuition about finite groups. Yes, Galois made mistakes. Still, his insight was specific, tasteful and hardly naive, much less for a 20 year old, in his selection of problems.

Still, I found Stillwell's interpretation of Galois' death, especially and thoughtfully included Galois despondency over "the suicide of his father, and Galois's own self-destructive tendencies." I have commented similarly on [**Rig96**], for example in [**Fr90b**, Ch. 2, §10.3], though regarding it as a moment of despondency during the *Republican time* in France that severely depressed many.

2.2. $\mathbb{P}^1_z$ covers and Nielsen classes. We return to $\varphi : W \to \mathbb{P}^1_z$, sphere covers. Call the images, z', of points of φ that ramify *branch points*. Such z' are places on the z-sphere where there are $< n = \deg(\varphi) = n_\varphi$ distinct x's in $\varphi^{-1}(z')$. There are just finitely many such (distinct) points, $\{z'_1, \dots, z'_r\} = \boldsymbol{z'}$. We often use $r = 4$, the first value of r significantly using *braids* (§3.1.1).

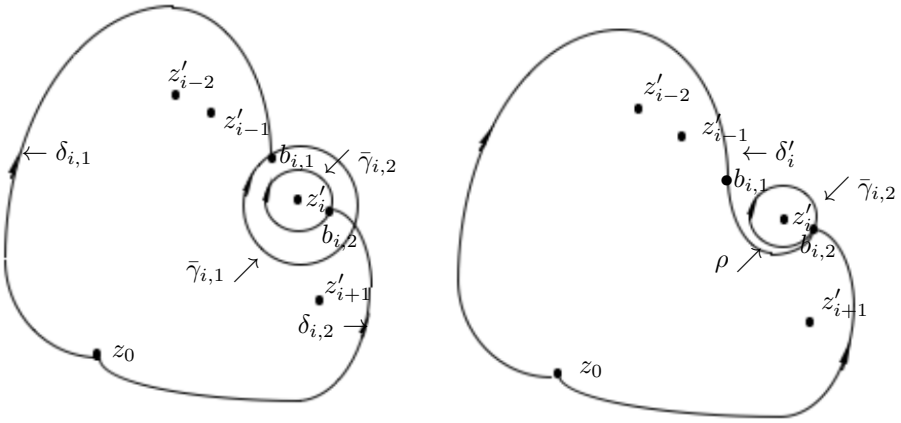
2.2.1. *Using a fundamental group.* Denote the fundamental group of

$$\mathbb{P}^1_z \setminus \boldsymbol{z'} \stackrel{\text{def}}{=} U_{\boldsymbol{z'}} \text{ based at } z_0 \in U_{\boldsymbol{z'}} \text{ by } \pi(U_{\boldsymbol{z'}}, z_0).$$

As always, a (connected) cover, say, the restriction of φ to the points of W over $U_{\boldsymbol{z}}$ of degree n is given by a (transitive) permutation representation – homomorphism of $\pi(U_{\boldsymbol{z'}}, z_0) \to S_n$ by acting on the fiber, $\boldsymbol{w'} = \{w'_1, \dots, w'_n\}$, over z_0 using the unique path-lifting property.

Here, though, we are more explicit and careful about choices. As a preliminary we can profitably use the definition of a z'_i-*loop*: That would be a path based at z_0, that is homotopic to $\delta_i \circ \bar{\gamma}_i \circ \delta_i^{-1}$ on $U_{\boldsymbol{z'}}$ with δ_i a simple path from z_0 to a tiny disk neighborhood D_i of z'_i (on $U_{\boldsymbol{z'}}$) ending at b_i, and $\bar{\gamma}_i$ a (clockwise) circle around D_i starting and ending at b_i. Fig. 1 compares two loops around z'_i.

FIGURE 1. Comparing two loops around $z'_{(i)}$



LEMMA 2.5 (Conjugate loops). *The loop $\delta_{i,j} \circ \bar{\gamma}_{i,j} \circ \delta_{i,j}^{-1}$, $j = 1, 2$, are conjugate in the fundamental group $\pi_1(U_{\boldsymbol{z'}}, z_0)$.*[16]

[16]For those who learned about tame ramification groups of Dedekind domain extensions, it may come as a surprise that Lem. 2.5 picks out a conjugacy class, rather than just a generator. That comes from our choice of a clockwise orientation in our loops.

PROOF. With no loss, up to the homotopy classes of the paths in question, we may assume the disks that $\gamma_{i,j}$, $j = 1, 2$ surround lie one inside the other, with an annulus between them. As in the figure on the right, we have drawn a (simple) path, ρ within that annulus between $b_{i,1}$ and $b_{i,2}$, so that the path δ_i' is $\delta_{i,1} \circ \rho$.

If we conjugate $\delta_{i,1} \circ \bar{\gamma}_{i,1} \circ \delta_{i,1}^{-1}$ by $\delta_{i,1} \circ \rho \circ \delta_{i,2}^{-1}$ the result is

$$\delta_{i,2} \circ \rho \circ \delta_{i,1}^{-1} \circ \delta_{i,1} \circ \bar{\gamma}_{i,1} \circ \delta_{i,1}^{-1} \circ \delta_{i,1} \circ \rho^{-1} \circ \delta_{i,2}^{-1}$$

which is easily seen to be homotopic to $\delta_{i,2} \circ \bar{\gamma}_{i,2} \circ \delta_{i,2}^{-1}$. That proves the lemma. □

Then *Classical generators* for the fundamental group of $\mathbb{P}^1_z \setminus \boldsymbol{z}' \stackrel{\text{def}}{=} U_{\boldsymbol{z}'}$ based at z_0 appear in many places. In words: They are (piecewise simplicial) closed paths, $\{P_1, \dots, P_r\} = \mathcal{P}$, representing, respectively,

$$z_i' - \text{loops}, i = 1, \dots, r, \text{ in } \pi_1(U_{\boldsymbol{z}'}, z_0).$$

Further, other than at z_0 we may assume they pairwise intersect nowhere else. Given $\mathcal{P}$, there is one significant ordering: That these paths emanate from z_0 in going clockwise around a suitably small circle about z_0.

Nielsen classes: For convenience in listing properties of covers with branch points $\boldsymbol{z}'$ relative to these paths, we assume the order of emanation of the z_i'-loops is given by their subscripts $1, \dots, r$. For a cover $\varphi : W \to \mathbb{P}^1_z$ with z_0 and $\boldsymbol{z}'$ as above, label the points on W above z_0 as $\boldsymbol{w}' = \{w_1', \dots, w_n'\}$.[17]

(1.23a) Homotopy classes of $\mathcal{P}$ generate $\pi_1(U_{\boldsymbol{z}'}, z_0)$ freely with one relation: $P_1 \cdots P_r$ is homotopic to 1 (order given above).

(1.23b) *Unique path lifting*: $P_i \mapsto g_i \in S_n$ by the rule, running over w_j', the unique lift of P_i starting at w_j' ends at $w_k' = w_{(j)g_i}'$, $i = 1, \dots, r$.

(1.23c) *branch cycles* $(g_1, \dots, g_r) = \boldsymbol{g}$ satisfy *Nielsen Class* properties:

- *Generation*: the group $\langle g_1, \dots, g_r \rangle = G_\varphi$ is the *geometric monodromy* (Galois closure) group of φ.
- *Product-one*: $g_1 \cdots g_r = 1$.
- *Conjugacy classes*: Independent of $\mathcal{P}$, $\{g_i |\ i = 1, \dots, r\}$ define conjugacy classes $\mathbf{C} = \{\mathrm{C}_1, \dots, \mathrm{C}_r\}$ in G_φ.

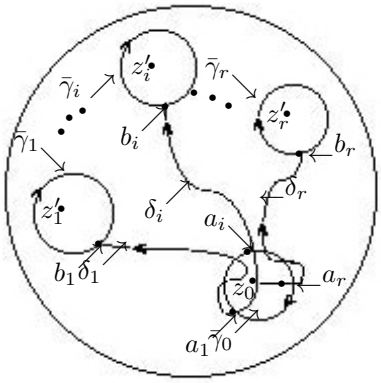
The path notation of Fig. 2 is compatible with that of Fig. 1.

PROBLEM 2.6. Use Ch. 2 Prob. 2.3 to create classical generators from any base point z_0 for any given distinct points $\boldsymbol{z}' \in \mathbb{P}^1_z$.

2.2.2. *First Nielsen class example.* Excluding stipulating the equivalence † we intend to use on covers – several appear – $\mathrm{Ni}(G, \mathbf{C})^\dagger$ is just a listing of the covers of the sphere satisfying the conditions of (1.23c) with attached $(G, \mathbf{C}, T)$ branched

[17](1.23) is done in great detail in [**Fr90b**, Ch. 4] starting from [**Ahl79**, §1.1–1.3]. [**Vo96**] use idealized classical generators, leaving out a crucial point: The braid group is transitive on all possible classical generators, as used in the conclusions of (1.29).

FIGURE 2. Example classical generators based at z_0



precisely at $\boldsymbol{z}'$. Of course, T depends on how we label points in $\boldsymbol{w}'$. In §3 our † will be more explicit about that dependence. RET (Riemann's Existence Theorem) says that giving covers with data attached to $(G, \mathbf{C}, T, \boldsymbol{z}')$ is the *same* as giving r-tuples $\boldsymbol{g}$ as in (1.23c). That is, the sets are the same, though the associations between them depend on the choice of classical generators.

Comments on Prop. 3.5 say more on RET and identifying $\langle g_1, \dots, g_r\rangle$ with the group of the Galois closure of $\varphi : W \to \mathbb{P}^1_z$. We have just shown that the identification requires recognizing that W has a function field.

A cover doesn't include an ordering its branch points. Adding such an ordering would destroy the applications to the **RIGP**. This makes sense of saying *a cover is in the Nielsen class* $\mathrm{Ni}(G, \mathbf{C}, T)$ (or $\mathrm{Ni}(G, \mathbf{C})^\dagger$).

In some ways the dihedral group, $D_{\ell^{k+1}} = \mathbb{Z}/\ell^{k+1} \times^s \{\pm 1\}$, of order $2\cdot\ell^{k+1}$ with ℓ (for now) an odd prime, is an easy group. Still, it will be an extremely important running example for which we consider its elements, and those of related groups, as 2×2 matrices. We have the choice, as in Def. 1.6, to consider $\langle \pm 1\rangle$ as acting on the left (resp. right). For example, with C_2 the conjugacy class of $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, we would regard C_2 as the collection

$$\text{Left action:}\{\left(\begin{smallmatrix} -1 & a \\ 0 & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}/\ell^{k+1}\}$$

$$\text{Right action:}\{\left(\begin{smallmatrix} -1 & 0 \\ a & 1 \end{smallmatrix}\right) \mid a \in \mathbb{Z}/\ell^{k+1}\}.$$

Then, for the standard permutation representation $T : D_{\ell^{k+1}} \to S_{\ell^{k+1}}$, with letters $b \in \mathbb{Z}/\ell^{k+1}$, we would respectively have $g \in D_{\ell^{k+1}}$ act by

$$\text{Left action: } g = \left(\begin{smallmatrix} -1 & a \\ 0 & 1 \end{smallmatrix}\right) : \left(\begin{smallmatrix} b \\ 1 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a-b \\ 1 \end{smallmatrix}\right)$$

$$\text{Right action: } g = \left(\begin{smallmatrix} -1 & 0 \\ a & 1 \end{smallmatrix}\right) : (b\ 1) \mapsto (a-b\ 1),$$

as expected by extending matrix multiplication to vectors.

EXAMPLE 2.7 (An "Elementary" example). As above, using the left action, let N_k be the normalizer in $S_{\ell^{k+1}}$ of $D_{\ell^{k+1}}$ and consider absolute Nielsen classes $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4}, T)^{\mathrm{abs}} = \mathrm{Ni}_k^{\mathrm{abs}}$. Associate

$$\left(\left(\begin{smallmatrix} -1 & a_1 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & a_2 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & a_3 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & a_4 \\ 0 & 1 \end{smallmatrix}\right)\right)$$

to $(a_1, a_2, a_3, a_4) \in (\mathbb{Z}/\ell^{k+1})^4$ modulo N_k.

Count these using representatives with these properties:

(1.24a) $a_1 = 0$, $a_2 - a_3 + a_4 = 0$; and

(1.24b) $a_2 = 1$ or $\ell \,|\, a_2$ and $a_3 = 1$.

Then: $|\mathrm{Ni}_k^{\mathrm{abs}}| = \ell^{k+1} + \ell^k$. Modding out only by $D_{\ell^{k+1}}$ —instead of N_k— gives $|\mathrm{Ni}_k^{\mathrm{in}}| = (\ell^{k+1} + \ell^k)\varphi(\ell^{k+1})/2$ with φ the Euler φ-function.

Renormalize: Use $a_2 - a_3 = a'\ell^u$ with $(a', \ell) = 1$ in place of $a_2 = 1$; conjugate by $\left(\begin{smallmatrix} a' & 0 \\ 0 & 1 \end{smallmatrix}\right)$ to take $a' = 1$. This allows further conjugation with $\alpha \equiv 1 \bmod \ell^{k+1-u}$.

This example continues in Ch. 2 §3.2. Ch. 6 §3.2 identifies spaces of covers (§3) in dihedral Nielsen classes, when $\mathbf{C} = \mathbf{C}_{2^4}$, with *modular curves*. △

2.3. Classical visions of RET**.** Since Riemann died in 1866, there has been a long history of accustoming to RET, much of it evidence of different generations learning it anew, since there is no obvious place in the (especially undergraduate) curriculum where it belongs. In the short subsections §2.3.1 – field theoretic – and §2.3.2 – picture centric – I engage that history. We would never get anywhere if we only concentrated on the elementary questions they raise, though at least the first of these sections deserves more treatment.

2.3.1. *Field version of* RET. Suppose $L/\mathbb{C}(z)$ is a finite extension, given by an irreducible polynomial $F_L(z, w)$, of degree n in w. For each z' (branch point or not), we may find n zeros of F_L in the field of

$$\text{Puiseux expansions } \mathrm{Pu}_{z'} = \cup_{k=1}^{\infty} \mathbb{C}((z - z')^{1/k})).$$

That is, we have an embedding $\psi_{z'} : \hat{L} \to \mathrm{Pu}_{z'}$ of the Galois closure, $\hat{L}$, of $L/\mathbb{C}(z)$ in $\mathrm{Pu}_{z'}$. Such a $\psi_{z'}$ is defined up to composing with elements of $G(\hat{L}/\mathbb{C}(z))$.

Elementary statement of RET*:* Further, there is a canonical automorphism of $\mathrm{Pu}_{z'}$ (fixed on the Laurent series, $\mathbb{C}((z - z'))$ in $z - z'$) given by

$$\sigma_{z'} : (z - z')^{1/k} \mapsto e^{\frac{2\pi i}{k}} (z - z')^{1/k} \text{ for all } k \geq 1.$$

Only for z' among the branch points $\boldsymbol{z}_L$ will the restriction to $\hat{L}$ be nontrivial. For each branch point, z_i, that restriction gives an element g_{z_i} in $G(\hat{L}/\mathbb{C}(z))$, thereby, as previously, defining a conjugacy class C_i in this group.

PROPOSITION 2.8. *The Nielsen class conditions imply for some choices of ψ_{z_i}, $1, \ldots, r$, the $\boldsymbol{g} = \{g_{z_1}, \ldots, g_{z_r}\}$ satisfy product-one and generation.*

Further, they imply the inverse problem. Assume any distinct $\boldsymbol{z}$ *and elements* $\boldsymbol{g}$ *that satisfy product-one that generate a (finite) group* G*, with a transitive permutation representation of degree* n*. Then there is* $L/\mathbb{C}(z)$ *as above producing* $\boldsymbol{g}$*.*

As $\boldsymbol{g}$ defines the genus of the unique Riemann surface associated to L from the RH formula (1.37). So, there is a natural collection of appropriate questions that go under the following heading.

QUESTION 2.9. Is any of this easy, or doable explicitly, or without using the fundamental group of the r-punctured sphere (a la Fig. 2)?

Fiber products of genus 0 covers: For example, consider these questions.

(1.25a) Can we answer Quest. 2.9 affirmatively for genus 0 (given by a rational function in w) extensions?

(1.25b) if the answer is yes, to (1.25a) can we use fiber products of genus 0 extensions to answer yes to all extensions.

Even Riemann relied on fiber products of genus 0 covers – the description of hyperelliptic curves, and finding *nondegenerate odd* half-canonical classes (§1.3 – to conclude one of his most famous theorems. In that he gave a formula for finding all functions on any Riemann surface of genus g as a ratio of translates of a particular θ function formed from that half-canonical class. This generalized Abel's analogous theorem on elliptic curves, the only genus where half-canonical classes could be confused with 2-division points, and where there is a unique odd half-canonical class. This Abel Theorem. not discussed in great detail in [**Fr02b**], though it is the concentration point of most treatises that do mention Abel's Theorems.[18]

PROPOSITION 2.10. *Even if the answer to* (1.25a) *is affirmative, the answer to* (1.25b) *is no.*[19]

PROOF. Suppose a cover $\varphi : W \to \mathbb{P}^1_z$ has monodromy group one of the simple groups that does not appear as a composition factor of a genus 0 cover of $\mathbb{P}^1_z$. Answering (1.25b) affirmatively means that the Galois closure of a given cover, say φ, appears as a quotient of the fiber products of the Galois closures of genus zero covers. In that case, however, the group G_φ would have each composition factor appear as a composition factor of the Galois closure of one of those genus 0 covers.

From, however, the genus 0 problem [**Fr05b**, §7.2.1], only finitely many simple groups – outside of cyclic and alternating groups – appear as composition factors of monodromy of genus 0 covers.[20] Yet, every group appears as the monodromy of

[18]It is in the subjects of [**Fr90b**, §7.2] and [**Fr10**, §6] in a style related to that of Riemann.

[19]see the proof for the meaning of this.

[20]This is the result on the genus 0 problem as originally formulated by the author and J. Thompson, but R. Guralnicks stronger conjectures on the specific monodromy of primitive genus 0 covers, and also general genus, have been proven.

$\mathbb{P}^1_z$ cover from RET, including those simple groups that can't be realized from the genus 0 problem. □

REMARK 2.11. There is a simplification in trying to construct rational function covers, for – by Luroth's Theorem – they are pure transcendental over some coefficient field. In particular cases, they have been so described as covers of $\mathbb{P}^1_z$ following their appearance in families of Hurwitz spaces. For example, as in [**CoCa99**], which constructs the polynomial covers – called Davenport pairs – using a computer program. Still, the group theory and RET as in [**Fr80**] lie behind their solution.

Another example – for regularly realizing Spin_n – is those covers in the Nielsen classes denoted $\mathrm{Ni}(A_n, \mathbf{C}_{3^{n-1}})$, $n \geq 5$ and *odd* in Ch. 3 Ex. 2.9. Here – [**Me90**], with an exposition in [**Se92**, §9.3], and an earlier attempt for $n \equiv 1 \mod 8$ in [**Vi85**] – the construction is only explicit for $\varphi : X \to \mathbb{P}^1_z$ in the Nielsen class when there is $z' \in \mathbb{P}^1_z(\mathbb{Q})$ with $\varphi^{-1}(z')$ consisting of $\mathbb{Q}$ geometric points.

2.3.2. *Cuts and impossible pictures.* There has been a tradition for drawing "3D pictures" – in $\mathbb{R}^3$ – of covers of the sphere, by functions even easier than those given by in Ex. 2.7, for covers with just 3 branch points (or even 2, rather than 3). I have asked two questions:

(1.26a) Are the pictures meaningful, usefully conveying properties of the covers?

(1.26b) Do they turn out to work in more serious examples?

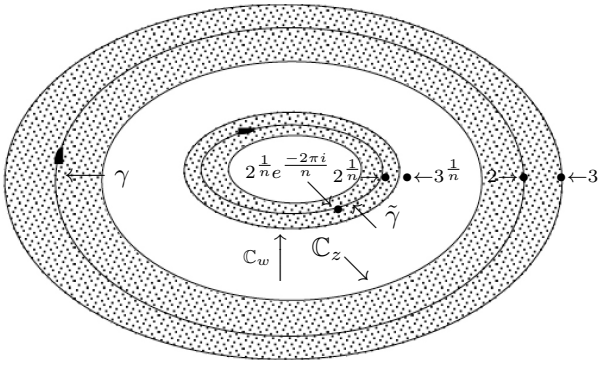
Projecting from $\mathbb{C}^2$ to $\mathbb{R}^3$: Consider the problem of representing covers by pictures in $\mathbb{R}^3$, with an attempt to give a description of the ramified cover $f : U_{w:0,\infty} \to U_{z:0,\infty}$ by $w \mapsto w^n$ in Fig. 3. Points of $U_{w:0,\infty}$ over $z \in U_{z:0,\infty}$ correspond on the graph of f to $\mathbb{C} \times \mathbb{C}$ points on the line with constant second coordinate z.

You can't draw pictures in $\mathbb{C} \times \mathbb{C} = \mathbb{R}^4$. So first year complex variables texts try to represent $U_{w:0,\infty}$ and $U_{z:0,\infty}$ as subsets of $\mathbb{R}^3$. In Fig. 3, a traditional picture representing the nth power map as if it were the projection on a real coordinate. Let (x_1, x_2, x_3) be coordinates for $\mathbb{R}^3$, and let $x_3 = 0$ represent $U_{z:0,\infty}$ sitting in $\mathbb{R}^3 \setminus \{(0,0,0)\}$. Pictures try to represent an annulus around the origin in $U_{w:0,\infty}$ as a set M in $\mathbb{R}^3$ over an annulus D_0 in $U_{z:0,\infty}$. Then, points of M over $(x_1, x_2, 0) \in D_0$ are on the line in $\mathbb{R}^3$ whose points have first coordinates x_1 and x_2. That is, f appears as a coordinate projection.

A lift of γ (a clockwise circle, compatible with choices for classical generators) is $\tilde{\gamma}$ going $\frac{1}{n}$ of the way around a clockwise circle. The associated permutation is an n-cycle of S_n representing that $\tilde{\gamma}$ goes from the lift $y' = 2^{1/n}$ of $\gamma(0) = 2$ to $y'' = 2^{\frac{1}{n}} e^{\frac{-2\pi i}{n}}$, the point on $\tilde{\gamma}$ lying $\frac{1}{n}$ of the way around from y'.

There is, however, no topological subspace M of $\mathbb{R}^3$ that can work! If there were, then a cylinder perpendicular to the plane $x_3 = 0$, with $(0,0,0)$ on its axis,

FIGURE 3. An n-cycle of path liftings



would intersect M in a simple closed path winding n times around the cylinder. Represent such a path by $\gamma : [0,1] \to \mathbb{R}^3$ where $t \in [0,1]$ maps to

$$\gamma(t) = (\cos(2\pi nt), \sin(2\pi nt), x_3(2\pi nt)) \text{ and } x_3(2\pi n) = x_3(0).$$

Conclude: $w(t) = x_3(2\pi nt) - x_3(2\pi nt + 2\pi)$ is 0 for some value of t between 0 and $(n-1)/n$. So, the path isn't simple. The author has never seen such a picture attempt in the literature for any noncyclic cover, much less for more demanding nonsolvable groups.

A word on "cuts": Even the case when the degree n is 2, and we are considering $\varphi : W \to \mathbb{P}^1_z$, where W has a presentation as a sphere with g handles in $\mathbb{R}^3$, presenting the map φ by a picture in $\mathbb{R}^3$ can be confusing. Still, something akin to that appears in many books – for example, [**Con78**, p. 243] – and it is analyzed in [**Fr90b**, Ch. 2, § 2.4.1]. That picture includes all the usual elements, especially the *cuts*. The discussion there, concentrates on the Fig. 7, there: two discs snipped along cuts along their negative real axes, with the left cut on one jointed to the right cut on the other, etc. Then, paths around an origin in the picture jump from one cut disk to the other, in a way that represents continuity symbolically.

From [**Ne81**], we learn that Gauss introduced Riemann to cuts. Their value is that they suggest how a combination of symbols and pictures can justify the topology. This establishes the idea behind the cuts is that "similar" covers – meaning they are in the same Nielsen class – have a locally constant structure. Yet, that symbolic case is a hyperelliptic curve covering $\mathbb{P}^1_z$.

While we don't develop those cuts here in detail, §3.1.1 – under the rubric of "dragging a cover by its branch points" – shows where they get used precisely in the description of the Hurwitz monodromy group, H_r. §3 takes the approach that a Nielsen class representing a space of covers, that deform through changing their branch points, can leap us over an entanglement with impossibly complicated paths on particular Riemann surface covers.

There are so many problems that demand going beyond hyperelliptic covers. One standout, Prob. 3.8 however, dominates the applications in this book.

3. Hurwitz spaces parametrize covers in $\mathrm{Ni}(G,\mathbf{C})^\dagger$

We now discuss the space of all covers in a given Nielsen class. Ch. 5 §3 will explicitly illustrate each of Prop. 3.1, 3.2 and 3.5 on the main example of this paper. That is, we illustrate computing with braids, and Nielsen class elements. That does not mean we will write out equations for the spaces and covers.

3.1. Parameters for covers. A (Hurwitz) space whose points parametrize covers in a particular Nielsen class of r classes appears as a cover of a configuration space. This is r unordered branch points minus the locus where two come together:

(1.27) $\qquad U_r =$ projective r-space $\mathbb{P}^r$, minus its *discriminant locus*, D_r.

Take $\boldsymbol{z}_0$ to be a basepoint of U_r, and

denote $\pi_1(U_r,\boldsymbol{z}_0)$, the *Hurwitz monodromy group*, by H_r.

3.1.1. *Dragging a cover.* Here is how to think of forming Hurwitz spaces, a process we refer to as *dragging a cover by its branch points*.

Start with $\varphi_0 : W_0 \to \mathbb{P}^1_z$, a cover with branch points $\boldsymbol{z}_0$, classical generators $\mathcal{P}_0$ and (branch cycles) $\boldsymbol{g}_0 \in \mathrm{Ni}(G,\mathbf{C})$. Drag the branch points along any path B in U_r, starting at $\boldsymbol{z}_0$ and ending at $\boldsymbol{z}_1$. Then, deform the classical generators along that path to $\mathcal{P}_1$. With no further choices, we may canonically form a cover $\varphi_t : W_t \to \mathbb{P}^1_z$ with respect to the same $\boldsymbol{g}_0$ along the path indicated by the parameter.

Classical generators → identifying branch cycles: This produces a collection of $\mathbb{P}^1_z$ covers of cardinality $|\mathrm{Ni}(G,\mathbf{C})^\dagger|$ over every point of U_r, forcing upon us a decision. Should B be a closed path, representing an element of $\pi(U_r,\boldsymbol{z}_0)$, how do we identify branch cycles $\boldsymbol{g}_1$ for the cover $\varphi_1 : W_1 \to \mathbb{P}^1_z$ lying at the end of the path, relative to the original classical generators $\mathcal{P}_0$?

(1.28) $\qquad$ That is, what will we choose for †?

Here are key points going back to [**Fr77**, §4].

(1.29a) *Endpoint of the Drag*: A cover at the end of B is still in $\mathrm{Ni}(G,\mathbf{C})^\dagger$. It depends only on the homotopy class of B with its ends fixed.

(1.29b) *Branch cycle finale*: For B closed, a *braid*, $q_B \in H_r$ (§2) applied to $\boldsymbol{g}_0$ gives $\boldsymbol{g}_1 = (\boldsymbol{g}_0)q_B$.

(1.29c) *Minimal equivalence*: For each $g \in G$, some braid q_g conjugates entries by g; see Ch. 2 Prob. 2.2: $(\boldsymbol{g}_0)q = g(\boldsymbol{g}_0)g^{-1}$.

(1.29d) *H_r orbits*: (Irreducible) components of spaces of covers in $\mathrm{Ni}(G,\mathbf{C})^\dagger$ correspond to H_r orbits.

Ch. 2 §2.1.2 gives explicit paths on U_r, and their effect as braids. Whatever the problem application, we must be able to identify the Galois closure of the cover. The key ambiguity is in labeling $\boldsymbol{w}' = \{w_1', \dots, w_n'\}$, points lying over z_0. Changing that labeling changes $T : G \to S_n$. A slightly subtler change comes from changing z_0'. There is a distinction between them.

Changing z_0' to z_0^* is affected by rewriting the z_i-loops as

$$\lambda^* \circ \lambda \circ \rho \circ \lambda^{-1} \circ (\lambda^*)^{-1}, \text{ with } \lambda^* \text{ a path from } z_0^* \text{ to } z_0. \tag{1.30}$$

3.1.2. *Absolute vs Inner equivalence.* Assume $\varphi_0 : W_0 \to \mathbb{P}^1_z$ is a cover, branched at $\boldsymbol{z}_0$, with assigned branch cycles using a classical set of generators as above. Applications dictate under what circumstances we will identify covers $\varphi_i : W_i \to \mathbb{P}^1_z$, $i = 0, 1$, branched at $\boldsymbol{z}_0$, obtained from dragging a given cover $\varphi : W \to \mathbb{P}^1_z$ around two (different) closed paths in U_r using the dragging-branch-points principle.

Prop. 3.1 is a first statement on equivalences of covers corresponding to elements in a Nielsen class. Denote the subgroup of the normalizer, $N_{S_n}(G)$, of G in S_n that permutes a given collection, $\mathbf{C}$, of conjugacy classes, by $N_{S_n}(G, \mathbf{C})$.

PROPOSITION 3.1 (Spaces I). *As above, suppose $\mu : W_0 \to W_1$ is a continuous isomorphism with $\mu \circ \varphi_1 = \varphi_0$ (commuting with the projections to $\mathbb{P}^1_z$). Then, μ is automatically analytic. It permutes elements of $\boldsymbol{w}'$ according to $h \in N_{S_n}(G, \mathbf{C})$, inducing $\mu_h^* : g \in G \mapsto hgh^{-1}$; and conversely.*

There are two extremes for the equivalences we allow for such μ s:

(1.31a) *Inner: The effect of running over all $g(\lambda^*)$ s is to change the permutation representation T by conjugating by an element of G.*

(1.31b) *Absolute: Changes of permutation given by conjugating T by any $g \in S_n$ maps $\langle g_1, \dots, g_r \rangle = G$ into itself.*

That is, inner equivalence is minimal to account for not indicating a choice of basepoint, and absolute is maximal (equivalencing the most covers).

COMMENTS. There is a point to be made on (1.30) To keep the loops pairwise non-intersecting except at z_0^* requires only using a fan of λ^* s, one for each i, just slightly varied from each other. It is a minor point (see [**Fr77**, Lem. 1]).

When λ^* is a closed path, using the path lifting property produces a permutation $g(\lambda^*) \in G$ on $\boldsymbol{w}'$, the points lying over z_0. This is the source of why inner equivalence is the minimal equivalence to assure that using a base point in the construction of the Hurwitz spaces does not appear in their final description in §3.1.3. □

3.1.3. *Representations of H_r produce spaces.* Now we show how braids acting on (equivalence classes of) elements in Nielsen classes produce the Hurwitz spaces. Each equivalence class corresponds to an equivalence class of Nielsen classes. Again, we distinguish between the two most used equivalences: *absolute* and *inner*. Then,

assuming the hypothesis of Lem. 2.3, Prop. 3.5 constructs total spaces of covers from the main theorem on fundamental groups applied to the space U_r. We also relate the respective spaces for those two equivalences.

Fundamental group representations give covers: Recall: *unramified* covers of a space, Z, arise from permutation representations $T : \pi_1(Z, z_0) \to S_n$ of the fundamental group of Z. We now apply this to $\pi_1(U_r, \boldsymbol{z}_0) = H_r$.

(1.32) The cover is connected if and only if T is transitive:
For each $i \in \{1, \dots, n\}$, $\exists h \in \pi_1(Z, z_0) \mid (1)T(h) = i$.

PROPOSITION 3.2 (Spaces II). *Applied to* (1.29b)*, equivalences interpret when the final cover, φ_1, after dragging φ_0 along q_B is isomorphic to φ_0. Whatever the equivalence $\dagger$, this defines a parameter space of covers denoted by $\mathcal{H}(G, \mathbf{C})^\dagger$.*

Mapping a cover of $\mathbb{P}^1_z$ to its (unordered) branch points presents $\mathcal{H}(G, \mathbf{C})^\dagger$ as an unramified cover $\Phi^\dagger_{\mathcal{H}} : \mathcal{H}(G, \mathbf{C})^\dagger \to U_r$ of U_r,

Here: $\mathcal{H}(G, \mathbf{C})^\dagger$ arises from a representation of $\pi_1(U_r, \boldsymbol{z}_0)$ acting on $\mathrm{Ni}(G, \mathbf{C})^\dagger$ (made explicit using the rules of §2) [**Fr77**, §4].

(1.33a) *If $\dagger = \mathrm{abs}$ (absolute), then $\mathrm{Ni}(G, \mathbf{C})^\dagger$ is*

$$\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}} = \mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}_T} = \mathrm{Ni}(G, \mathbf{C})/N_{S_n}(G, \mathbf{C}),$$

where we drop the representation T if we know it from context.

(1.33b) *If $\dagger = \mathrm{in}$ (inner) then $\mathrm{Ni}(G, \mathbf{C})^\dagger = \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}} = \mathrm{Ni}(G, \mathbf{C})/G$.*

COMMENTS. We make use of the following comments later. Inner equivalence is understood to be $\mathrm{Ni}(G, \mathbf{C}, T)^{\mathrm{in}} = \mathrm{Ni}(G, \mathbf{C})/G$ where T is the regular representation of G, and each (Galois) cover $\hat{W} \to \mathbb{P}^1_z$ in the Nielsen class includes an isomorphism

(1.34) $\psi : \mathrm{Aut}(\hat{W}/\mathbb{P}^1_z) \to G$, defined up to an inner isomorphism of G.

For each $h \in G$, and $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^\dagger$, there exists $q_B \in H_r$ such that

(1.35) $(\boldsymbol{g})q_B = h\boldsymbol{g}h^{-1}$, with q_B dependent on both h and $\boldsymbol{g}$.

With the operators q_i in §2, the idea comes from

(1.36) $$(\boldsymbol{g})q_1 \cdot q_2 \cdots q_{r-1} \cdot q_{r-1} \cdots q_2 \cdot q_1 = g_1 \boldsymbol{g} g_1^{-1}.$$

This concludes showing that the braid action automatically equivalences Nielsen classes if they are inner conjugate □

Dragging a cover around by its branch points defines an orbit of H_r on a Nielsen class $\mathrm{Ni}(G, \mathbf{C})^\dagger$. Therefore an irreducible cover of U_r (Prop. 3.2). Doing this for each H_r orbit assigns an equivalence class of covers to each point on the cover $\mathcal{H}(G, \mathbf{C})^\dagger$ or even a space of covers in any simply connected neighborhood of any point of $\mathcal{H}(G, \mathbf{C})^\dagger$. The next proposition relates absolute and inner equivalence.

The spaces of Prop. 3.2 are generalizations of the *moduli space of curves of a fixed genus*. That is, all covers $\varphi : W \to \mathbb{P}^1_z$ in a fixed Nielsen class $\mathrm{Ni}(G,\mathbf{C})^\dagger$ have the same genus, $\mathbf{g}_W \stackrel{\text{def}}{=} \mathbf{g}_{G,\mathbf{C}}$. We compute it easily using the notation of the index, $\mathrm{ind}(g) = \deg(T) - k$, of any g in a class C which has precisely k orbits under T. This defines ind(C), and

$$\text{Riemann-Hurwitz: } 2(\deg(T)+\mathbf{g}_{G,\mathbf{C}}-1) = \sum_{i=1}^{r} \mathrm{ind}(\mathrm{C}_i). \tag{1.37}$$

REMARK 3.3. See Def. 3.7 on *braiding inner* vs *outer* automorphisms. This topic is significant for many of our applications.

REMARK 3.4 (Comments on equivalences). Branch cycles give permutation representations of $\Pi_1(U_{\boldsymbol{z}}, z_0)$. We're not done with our basic equivalences yet, as we also have reduced equivalence Ch. 2 §2.1.3. There are others, too, that have been used in applications such as [**DFr90b**]. Further, there is a natural notation for considering when one permutation representation extends another, on the same group or a covering group, and thereby consider chains of covers and the maps induced on Hurwitz spaces from these.

Further, more generally we could add equivalences on permutation representations of $\Pi_1(U_{\boldsymbol{z}}, z_0)$. That would be appropriate for relating the Hurwitz spaces themselves. We haven't considered these systematically as the applications are a different nature than those considered in this book.

3.2. Relating inner and absolute spaces. Given a faithful (transitive) permutation representation $T : G \to S_n$, and a Nielsen class $\mathrm{Ni}(G,\mathbf{C})$, there is automatically a relation between $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ and $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$.

Prop. 3.5 shows the result on the spaces $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$ of the *fine moduli* condition on the group G.

PROPOSITION 3.5 (Spaces III). *Assume (G,T) is self-normalizing as in Lem. 2.3. Then, there is a unique total family, or fine moduli structure,*

$$\Phi^{\mathrm{abs}_T}_{\mathcal{T}} : \mathcal{T}^{\mathrm{abs}_T} \to \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}_T} \times \mathbb{P}^1_z$$

on $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}_T$, so that the pullback over $\boldsymbol{p} \times \mathbb{P}^1_z$ represents the equivalence class of the covers associated to $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}_T}$.

The Galois closure construction of (1.20) *produces a unique total family,*

$$\Phi^{\mathrm{in}}_{\mathcal{T}} : \mathcal{T}^{\mathrm{in}} \to \mathcal{H}(G,\mathbf{C})^{\mathrm{in}} \times \mathbb{P}^1_z$$

on $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ with $\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ over $\boldsymbol{p}$ representing an inner (Galois) cover mapping to an absolute cover. Further, all these spaces are quasi-projective varieties.

For any irreducible component $\mathcal{H}''$ of $\mathcal{H}(G,\mathbf{C})^{\rm in}$, the natural map to its image, $\mathcal{H}'$, in $\mathcal{H}(G,\mathbf{C})^{{\rm abs}_T}$

(1.38) *is Galois with group a subgroup of $N_{S_n}(G,\mathbf{C})/G$.*

The remainder of this subsection consists of background and comments on Prop. 3.5. §3.2.1 emphasizes the main condition on a moduli space that appears in applications: *fine moduli*. It also introduces the idea that RET meshes seamlessly with describing the moduli spaces that put covers in natural families.

Braid orbits on absolute (resp. inner) Nielsen classes give the absolutely irreducible components of absolute (resp. inner) Hurwitz spaces. At the heart of §3.2.2 is how to enumerate the components of the inner Hurwitz space that go to a a single component of the absolute space. A major part of identifying components appears in the topic of braiding outer automorphisms.

3.2.1. *Fine moduli and expanding* RET. In relating the construction of $\mathcal{H}^{\rm in}$ to that of $\mathcal{H}^{\rm abs}$ as a Galois closure construction based on (1.20) we are elaborating on [**BFr02**, §3.1.3]. We give the original argument in [**Fr77**, §4], based on Riemann's work on compact Riemann surfaces and [**GRe57**] as below.

From Lem. 2.3, the self-normalizing condition translates to say covers in the Nielsen class ${\rm Ni}(G,\mathbf{C})^{{\rm abs}_T}$ have no automorphims. Thus, a unique map patches any family of such covers on two overlapping open (simply-connected) sets on $\mathcal{H}(G,\mathbf{C})^{{\rm abs}_T}$. A well-known co-cycle patching puts a total family over the space, giving $\Phi^{{\rm abs}_T}$. We regard the association of elements of Nielsen classes to covers with branch cycles in a Nielsen class, as in (1.23), as part of RET.

Many refer to RET as if its *only* aspect is that any (compact Riemann surface) cover $\varphi: W \to \mathbb{P}^1_z$ has a function field determining it. Or its equivalent, it embeds in a closed subspace of some projective space.

Ch. 2 applications require the generalization of this to which we refer below in these comments. Some need only moduli fields of the components (definition fields as moduli spaces; Def. 4.8). Others require finding points on those same spaces over some specific field (like $\mathbb{Q}$).

Now you can apply the Galois closure construction to $\Phi^{{\rm abs}_T}_{\mathcal{T}} \stackrel{\rm def}{=} \Phi^{\rm abs}$,

$$\text{a degree } n = \deg(T) \text{ cover of } \mathcal{H}(G,\mathbf{C})^{\rm abs} \times \mathbb{P}^1_z.$$

The construction then is to take the n-fold fiber product of $\Phi^{\rm abs}$, remove the appropriate version of the fat diagonal and refer to the result as

$$\Phi': \mathcal{T}' \to \mathcal{H}(G,\mathbf{C})^{\rm abs} \times \mathbb{P}^1_z. \tag{1.39}$$

The Galois closure of the individual covers appears along the fibers over each $\boldsymbol{p} \times \mathbb{P}^1_z$, for $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{\rm abs}$, but usually more times than even in the application of the construction for each individual cover. Now, however, we must figure how

to normalize and what we are getting from taking a component. From the start, we need to know that irreducible components of $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}$ are quasi-projective normal varieties. Initially, we form them analytically, not algebraically.

[**Fr77**] applies a deep theorem – that of Grauert-Remmert [**GRe57**] – to assert that normalization in a function field makes sense. [**H77**, p. 442] references [**GRe58**], which is a more complete writeup of the three short Comptes Rendu papers. This, by itself is an extension of *part* of Riemann's existence theorem.

It says that if W is an irreducible analytic space, covering a Zariski open quasi-projective normal variety Z, then W itself is dominated by a unique quasi-projective normal variety $\tilde{W}$. The major point is that $\tilde{W}$ has a field of functions, obtained by extending the functions of Z by one more function that separates points and tangent directions in general fibers of $W \to Z$.

(1.40a) For the case of $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}_T}$, the quasi-projective normal variety Z is the U_r, (1.27) which is nonsingular, so normal.

(1.40b) Even the case $\varphi : W \to \mathbb{P}^1_z$ in §2 required this.[21]

(1.40c) With self-normalizing for (G,T): $W = \mathcal{T}^{\mathrm{abs}_T}$ and $Z = U_r \times \mathbb{P}^1_z$.

(1.40d) The proof of [**FrV91**, Thm 1] reduces the special cases (1.40a) and (1.40c) to the 1-dimensional case (1.40b).

(1.40e) Besides having a coherent modern treatment, [**Gr71**] has the foundations of ℓ-adic modules from cohomology.

3.2.2. *Identifying fibers of $\mathcal{H}^{\mathrm{in}}$ over a point of $\mathcal{H}^{\mathrm{abs}}$.* Consider a component $\mathcal{H}'$ of $\mathcal{H}(G,\mathbf{C})^{\mathrm{abs}_T}$. For each cover, $W_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$, appearing in in a fiber of Φ^{abs_T} we get a correct count of covers, over this given cover, along each fiber of Φ' from the quotient of the cardinalities of the respective Nielsen classes: $|N_{S_n,\mathbf{C}}(G)/G|$.

Continue (1.39) and take a connected component, $\mathcal{T}^{\mathrm{in}}$, of $\mathcal{T}'$. Normalize $\mathcal{H}'$ in the function field of T^{in}, to get $\mathcal{H}''$, a component of $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$. A subgroup, $G_{\mathcal{H}''/\mathcal{H}'} \le N_{S_n}(G,\mathbf{C})/G$ is transitive on the covers in the fiber of T^{in} lying over $W_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$, for all $\boldsymbol{p} \in \mathcal{H}'$. Thus, $\mathcal{H}'' \to \mathcal{H}'$ is Galois with group $G_{\mathcal{H}''/\mathcal{H}'}$. This completes (1.38).

This shows that connected covers $W''_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ over $W_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ in $\mathcal{T}^{\mathrm{in}}$ correspond to composing the identification of their automorphism groups with G (up to conjugation by G) with conjugation by elements of $N_{S_n}(G,\mathbf{C})$. As previously (with S_n action on (1.18)), we get transitivity on those connected covers from explicit elements of $N_{S_n}(G,\mathbf{C})$. See Def. 3.7 for why these may not all lie in one connected component.

[21] Riemann-Roch is stronger, saying for any compact Riemann Surface, it has a field of functions. This is nontrivial even when applied to a genus 0 Riemann surface. There is no general version like that for analytic spaces.

REMARK 3.6. Applications, however, even without the adjective, *fine*, use that $\mathcal{H}(G,\mathbf{C})^\dagger$ has moduli space meaning, with the relation between the equivalence classes inner and absolute (see Rem. 3.10). Ch. 6 §4.3.2 expediently surveys what is now called the *stack structure* for one approach.

Braiding automorphisms: Consider a braid orbit O in $\mathrm{Ni}(G,\mathbf{C})$ and an automorphism α of G that preserves $\mathbf{C}$ (with proper multiplicity).

DEFINITION 3.7 (Braiding automorphisms). If for $\boldsymbol{g}\in O$ and $q\in H_r$,

$$(\boldsymbol{g})q=(\boldsymbol{g})\alpha, \text{ we say } q \textit{ braids } \alpha.$$

Since the α action commutes with any braid $q'\in H_r$ acting, the test for braiding an automorphism is independent of the representative $\boldsymbol{g}\in O$.

More generally, the dominant problem in this book is the following.

PROBLEM 3.8. For a given Nielsen class $\mathrm{Ni}(G,\mathbf{C})^\dagger$, find conditions that identify Hurwitz space components (braid orbits) and their moduli fields.

Our techniques for doing this – especially the **sh**-incidence matrix, and the *lift invariant* – often either reveal a geometric way to separate the distinct orbits, or show them to be conjugate under the action of the absolute Galois group $G_{\mathbb{Q}}$.

A preliminary example on the Nielsen class $\mathrm{Ni}(A_4,\mathbf{C}_{\pm 3^2})^\dagger$ illustrates both techniques. Ch. 2 §3.3.2 for **sh**-incidence and Ch. 2 §3.3.3 for the lift invariant, where precise cusp types, called there **HM** and **DI** separate the components. Then, (1.41) gives geometric interpretation we can recognize as more classical. whereas cuts might not give much of a clue. Label the respective inner Hurwitz space components as $\mathcal{H}_{\mathbf{HM}}$ and $\mathcal{H}_{\mathbf{DI}}$.

(1.41a) Only for $\hat\varphi:\hat W\to\mathbb{P}^1_z$ in $\mathcal{H}_{\mathbf{HM}}$ does there exists a degree 2 unramified cover $\varphi':Y\to W$ for which $\hat\varphi\circ\varphi'$ is Galois with group $\hat A_4$.

(1.41b) Only for $\hat\varphi:\hat W\to\mathbb{P}^1_z$ in $\mathcal{H}_{\mathbf{HM}}$ can we identify a cover on the boundary of the compactification of $\mathcal{H}_{\mathbf{HM}}$ with a totally degenerate cover.

These separations are recognized by $G_{\mathbb{Q}}$, and therefore both $\mathcal{H}_{\mathbf{HM}}$ and $\mathcal{H}_{\mathbf{DI}}$ have moduli field $\mathbb{Q}$. This is an example that uses "cuts," as a theoretical background behind braid orbits, though indirectly an answer for what the questions (1.26) seek.

REMARK 3.9. Expression (1.36) says you can always braid inner automorphisms: conjugations of $\boldsymbol{g}$ by some $g\in G$. This may not apply to $h\in N_{S_n}(G,\mathbf{C})$ or to an outer automorphism not represented by some $g\in S_n$, even if it permutes the conjugacy classes in $\mathbf{C}$. Explaining when you can, or cannot, braid outer automorphisms appears in most applications (say, Thm. 1.7 or in Ch. 5).

REMARK 3.10. We always have the *regular* representation T for considering $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$: the representation of G on the cosets of $\{1_G\}$. Unless, however, G is trivial, that won't satisfy fine moduli.

CHAPTER 2

Fine Moduli and the RIGP

This section starts using what we introduced in Ch. 1. In (1.40), especially in comments to Prop. 3.5, we allude to two oft present extras on families of covers:

(2.1a) quasi-projective coordinates; and

(2.1b) a fine moduli structure.

§1 explains how (2.1) allows us to reliably correspond K points (say, a number field), on certain Hurwitz spaces to encapsulate diophantine problems like the **RIGP**.

Two tools immediately allow serious computing: *Braid action* and the *Branch Cycle Lemma* (**BCL**). §2 starts the former topic, and an equivalence – *reduced*, along with their corresponding Hurwitz spaces – on covers. Then it focuses on the Braid action when the Nielsen classes are of $r = 4$ conjugacy classes.

This case is important as it expands greatly on modular curves in a territory still modular curve-like making our examples accessible. When $r = 4$, reduced spaces are upper half-pane quotient coverings of the j-line. Their cusps on the compactification over $j = \infty \in \mathbb{P}^1_j$ explictly identify with orbits of a subgroup of the Hurwitz monodromy group H_4. That produces an efficient formula for the genus of the reduced Hurwitz spaces.

§3 introduces the first computational tool for identifying Hurwitz space components: *the* **sh**-*incidence matrix*. It applies for all values of r. We show it off on two examples directed at the ultimate goals of the book applying to the **OIT**.

Then, §4 introduces the **BCL**. A corollary gives the moduli field of absolute or inner Hurwitz spaces, the first ingredient for an application, say, to the **RIGP**.

While this can sometimes be sufficient for results, it is subtler to find the precise moduli field of the components of Hurwitz spaces. The main theme of Ch. 3 is an approach to generalizing the **BCL** that often does suffice, based on the second fundamental idea for identifying Hurwitz space components, the *lift-invariant*.

1. Polarizations and fine moduli

Embedding an algebraic variety, V, over a field K in projective space requires having a divisor D, for which the linear system $L(D) \stackrel{\text{def}}{=} \{f \in K(V) | (f) + D \geq 0\}$ contains sufficiently many functions that their values separate points and tangent directions at those points. A polarization starts with having a divisor D', for which

some multiple $D = mD'$ gives such an embedding in projective N-space, $\mathbb{P}^N$:

$$v \in V(\bar{\mathbb{Q}}) \mapsto (f_0(v), \dots f_N(v)), \text{ using some basis } \{f_0, \dots f_N \text{ of } L(D)\}.$$

The author learned it indirectly from the cocycle condition – as applied to abstract varieties – of Andre Weil [**We56**] through [**ShT61**] during his post-doctoral at the *Institute for Advanced Studies* 1967–69. In each case, though, it depends on how the divisor class relates to the moduli problem. §1.1 comments on the cases that arise with Hurwitz spaces where we see the polarization arising from the natural polarization on the configuration space U_r.

Since our Hurwitz spaces are mainly families of curve covers of $\mathbb{P}^1_z$, the canonical divisor class is always at hand. §1.3 adds comments on *canonical classes* as these appear in several different applications.

1.1. Hurwitz space moduli definition field. The Hurwitz space structures we produce are analytic, as in Prop. 3.1.3. Those include the Hurwitz space (unramified) cover $\Phi^{\dagger}_{\mathcal{H}} : \mathcal{H}^{\dagger} \to U_r$, of manifolds (so normal analytic varieties) for $\dagger$ either absolute or inner equivalence.

1.1.1. *Applying Grauert-Remmert.* If, say, fine absolute moduli holds, that gives a unique analytic total space (ramified) cover $\Phi^{\rm abs}_{\mathcal{T}} : \mathcal{T}^{\rm abs} \to \mathcal{H}^{\rm abs} \times \mathbb{P}^1_z$, of manifolds compatible with the projection maps to U_r. Then, in the construction of §3.2, a similar cover $\Phi^{\rm in}_{\mathcal{T}}$ appears, for which fine inner moduli holds (Lem. 2.3) from it holding in the absolute case.

Then, the Grauert-Remmert Theorem (Comments of Ch. 1 Prop. 3.5) produces a function field (for each component) for $\mathcal{H}^{\rm abs}$. Normalization of U_r in that function field gives a unique normal project algebraic variety. Putting the components together this gives $\mathcal{H}^{\rm abs}$ over U_r. A general remark suffices to show that a(n unramfied) cover of U_r is equivalent to a cover with definition field in $\bar{\mathbb{Q}}$ (Rem. 1.2).

Similarly, using that $\mathcal{H}^{\rm abs} \times \mathbb{P}^1_z$ is quasi-projective (from the Segre embedding), we get a unique normal project variety for $\Phi^{\rm abs}_{\mathcal{T}}$. The construction of $\Phi^{\rm in}_{\mathcal{T}}$ is done without Grauert-Remmert, and the projective structure is another application of the Segre embedding applied to the fiber product construction of §2.1.1.

1.1.2. *The moduli field, $\mathbb{Q}_{\mathcal{H}}$.* The goal for a particular Hurwitz space, $\mathcal{H}$, is an explicit (number) field $\mathbb{Q}_{\mathcal{H}}$ for which a K point $\boldsymbol{p} \in \mathcal{H}$ containing $\mathbb{Q}_{\mathcal{H}}$ assures that a representative of the equivalence class will have definition field $K = \mathbb{Q}(\boldsymbol{p})$. The moduli field is well-defined (below). Yet, the conclusion in general – without fine moduli – is only this.

(2.2) A representative of $\boldsymbol{p}$ has definition field $K \implies K \supset \mathbb{Q}_{\mathcal{H}}$.

It is not just a statement about the definition field of the underlying Hurwitz space itself as a quasi-projective variety. If $\mathcal{H}$ has fine moduli then this works as

said here. Without fine moduli, $\mathbb{Q}_{\mathcal{H}}$ still has meaning, though such a K point leads to a weaker conclusion (Rem. 4.9).

Each Hurwitz space, absolute, inner, and reduced versions of each, is defined by an equivalence on a Nielsen class. For each there is a precise criterion for fine moduli, based on that Nielsen class equivalence, $\mathrm{Ni}(G, \mathbf{C})^{\dagger}$. The ingredients appear in the following two lists that address the relation between a given cover $\varphi : X \to \mathbb{P}^1_z$ (2.3) describing how to detect the Nielsen class of the cover.

First: Compatible actions of $\sigma \in G_{\mathbb{Q}}$ on a cover, its branch points and Puiseux expansions above branch points.

(2.3a) Given a cover $\varphi : X \to \mathbb{P}^1_z$ in a Nielsen class, defined over $\bar{\mathbb{Q}}$, $\sigma \in G_{\mathbb{Q}}$ acts on the cover to give $\varphi^{\sigma} : X^{\sigma} \to \mathbb{P}^1_z$.

(2.3b) In all cases, σ acts on the branch points $\boldsymbol{z}$ of φ, sending them to collectively to branch points of φ^{σ}.

(2.3c) (2.3b) induces a compatible action on the Puiseux expansions of functions locally uniformizing φ over those branch points.

Second: Compatible actions of $\sigma \in G_{\mathbb{Q}}$ on the point representing a cover and the moduli space data.

(2.4a) Inner equivalence adds the action of σ on the automorphims of φ.

(2.4b) Adding reduced equivalence won't change the moduli definition field, though fine moduli may no longer hold.

(2.4c) σ acts on φ compatibly with acting on $\mathcal{T} \to \mathcal{H} \times \mathbb{P}^1_z \to U_r$.

The definition fields in each case come from the oft-appearing Branch Cycle Lemma (**BCL**, §4). Even with fine moduli, an absolutely irreducible component $\mathcal{H}'$ of $\mathcal{H}$ (corresponding to a braid orbit on a Nielsen class; we give many examples) may have a nontrivial extension, say $\mathbb{Q}_{\mathcal{H}'}$, of $\mathbb{Q}_{\mathcal{H}}$ as its moduli definition. For that component, $\mathbb{Q}_{\mathcal{H}'}$ is analogous as above for a representative of a point in $\mathcal{H}'$.

The Hurwitz space and its attached moduli structure need – at least – a scheme structure for their K points to have any meaning. We must assure that if someone else has done the same with the same spaces, their K points and ours will be the same. This requires that structure arise from an embedding in projective space, based on the linear system of an equivalence class of divisors compatible with the moduli structure.

Polarization data does exactly that. Usually we expect a natural divisor class, say giving a polarization, to arise from a relation between a space and some convenient projective space. §3.2.1 has already used such on $\mathcal{H}$, its total space $\mathcal{T} \to \mathcal{H} \times \mathbb{P}^1_z$ and the diagram including the map to the configuration space U_r. We track all of these to the projective space $\mathbb{P}^r$ containing U_r.

1.2. Covers over $\bar{\mathbb{Q}}$. Assume the normal quasi-projective variety V (a locally closed subset of projective, normal $\bar{V}$), is defined over a subfield $K \leq \mathbb{C}$. We mean that $\bar{V} \setminus V$ is also defined over K. We only require a little of the topology of quasi-projective algebraic varieties, because the moduli spaces which we define use fundamental groups detailed explicitly in [**Fr90b**]. Nevertheless Rem. 1.2 has references to a relatively modern book, which includes that the (discrete) fundamental group $\pi_(V, v_0)$ of such a variety can be gleaned from its structure as a CW complex using a generic curve on V. In particular, a finite unramified cover $\varphi_H : W_H \to V$ is defined by a subgroup, $H \leq \pi_1(V, v_0)$ of finite index.

LEMMA 1.1. *Then W_H is a equivalent to a cover of V defined over a finite extension of K.*

PROOF. From [**GRe58**] as used in Ch. 1 §3.2.1, W_H is quasi-projective, a locally closed subset in $\mathbb{P}^t$ with its closure $\bar{W}_H$ a normal variety (defined over $\mathbb{C}$). It is therefore defined over a finitely generated extension L of K (contained in $\mathbb{C}$) gleaned from the coefficients of the equations for $\bar{W}_H$. We show it is equivalent to a cover defined over a finite extension of K. Three points establish the Lemma.

- (2.5a) L defines a variety $U_L \stackrel{\text{def}}{=} U$ with function field L, for which $u \in U(\bar{K})$ gives a specialization W_H, u with equations having coefficients in $K(u)$.
- (2.5b) The discriminant of the cover, as a function of u is defined over K. Conclude over a Zariski open subset of U, the discrimiant is constant, and each $\bar{W}_{H,u}$ is a cover of $\bar{V}$, unramified over V.
- (2.5c) In a Zariski neighborhood of $u_\bullet$, all covers $W_{H,u} \to V$ are topologically (and therefore analytically) equivalent.

The conclusion of the lemma then follows, since in any neighborhood of $u_\bullet$ there will be points, algebraic over K, on U, say, by Hilbert's nullstellensatz.

Proof of (2.5a)*:* Since L is finitely generated, it has finite transcendence dimension. Therefore it has a description as a chain of extensions $L/K(\boldsymbol{y})/K$: with $\boldsymbol{y}$ a transcendence basis for L, a maximal set of elements algebraically independent over K; and $L/K(\boldsymbol{y})$ a finite extension [**La71**, p. 254]. Define U_L as the normalization in L of the affine variety defined by the coordinates $\boldsymbol{y}$.

We can use the coefficients of W_H , generating L, as a generic point, $u^\bullet$ of U_L. Then, U_L is quasi-projective, as is $U_L \times \mathbb{P}^t$ from (1.19). Inside $U_L \times \mathbb{P}^t$ we have the union of the $\bar{W}_{H,u}$ s from specializing the coefficients of W_H over $u \in U_L$.

Proof of (2.5b)*:* Suppose $\psi' : W' \to V'$ is finite cover of normal projective varieties. The ramification locus is defined on V' locally by the *discriminant locus* Suppose, locally in the Zariski topology, that ψ' is defined by $\text{Spec}(S) \to \text{Spec}(R)$,

an embedding of integral domains, with $R = S[w']$, and $F(w) = F_{w'}(w)$ the irreducible polynomial for w' over S, with $\deg(F) = m$. The discriminant, $d(F)$ – also known as the *resultant* of F and $\frac{\partial F}{\partial w}$ – then locally defines the discriminant locus of the cover [**La71**, Chap. V, §10].

It is the determinant of a $2m-1 \times 2m-1$ matrix with ith row entries as in (2.6), from $i = 1$ to $m-1$ (top) and $i = m$ to $2m-1$ (bottom):

$$\begin{array}{cccccc} i = 1, \dots, m-1 : 0^{i-1 \text{ times}} & a_0 & a_1 & \dots & a_m & 0^{m-i-1 \text{ times}} \\ i = m, \dots, 2m-1 : 0^{i-m \text{ times}} & ma_0 & (m-1)a_1 & \dots & a_{m-1} & 0^{2m-i-1 \text{ times}} \end{array} \tag{2.6}$$

When S is not generated by a single element w', write S as $R[w'_1, \dots, w'_k]$. Then use the ideal generated by all the $d(F_{w'_i})$s to define the discriminant locus as the ideal they generate. In a Zariski neighborhood of the generic point of U_H, the discriminant is defined by specializing the discriminant at the generic point over K. Since the discriminant at the generic point is defined over K, the discriminant is everywhere the same in this Zariski neighborhood.

Proof of (2.5c)*:* From the above, we have an analytic family $\tilde{W} \to U_L \times V$ with fiber over $u \in U_L$, an unramified cover $\varphi_u : W_{H,u} \to V$, defined in an analytic neighborhood U' of the generic point, $u^\bullet$, of V with the branch locus fixed. Therefore, all covers in this continuous family are defined by using the same generating paths of the finitely generated $\pi_1(V, v_0)$. This final result uses topology. It does not hold in positive characteristic even when $\dim(V) = 1$ (Rem. 1.3). We now show that $W_H \to V$ is analytically isomorphic to $W_{H,u}$ and conclude the lemma as above.

From the implicit function theorem, given a sufficiently small neighborhood U' of $u^\bullet$ and $w'(u^\bullet) \in \varphi_{u^\bullet}^{-1}(v_0)$, there is a continuous section

$$s_{w'(u^\bullet)} : U' \to \tilde{W} \to U_L \times V \text{ through } (u^\bullet, w'(u^\bullet)).$$

This section allows us to identify $w'(u^\bullet)$ with a unique element $w'(u) \in \varphi_u^{-1}(v_0)$. We show there is an isomorphism from W_H to $W_{H,u}$ for u close to $u^\bullet$. In the style of Ch. 1 §3.1.1, let $\mathcal{P}_0$ be generators of $\pi_1(V, v_0)$.

The covers W_H and $W_{H,u}$ are defined by respective permutation representations $\tau_{u^\bullet}, \tau_u : \pi_1(V, v_0) \to S_n$, with the integers $\{1, \dots, n\}$ identified respectively in each representation with $\{w'(u^\bullet) \in \varphi_{u^\bullet}^{-1}\}$ and $\{w'(u) \in \varphi_u^{-1}\}$.

Reminder: The result of $\tau_u(P)$ is the endpoint of the unique path-lift of P to the path starting on $W_{H,u}$ at any $w'(u) \in \varphi_u^{-1}(v_0)$. Denote that unique path lift by $P_{u,w'(u)}$. If for each $P \in \mathcal{P}_0$, the effect of P on the respective fibers is the same, then the two covers are equivalent. Use any convenient metric, D, in $U_L \times \mathbb{P}^t$. Designate a path P in V by $t \in [0,1] \mapsto P(t)$.

Then, $P_{u,w'(u)}(t)$ is a continuous function of (u,t). With $w''(u^\bullet) \in \varphi_{u^\bullet}^{-1}(v_0)$ distinct from $w'(u^\bullet)$, (use the sections $s_{w'(u^\bullet)}$ above) then $P_{u,w''(u)}(t) \neq P_{u',w'(u')}(t)$ for $u, u' \in U'$ and U' small, and any $t \in [0,1]$. Therefore, for $U'' \subset U'$ a small

compact subneighborhood of $u^\bullet$:

$$D(P_{u,w'(u)}(t), P_{u',w'(u')}(t)) < D(w'(u^\bullet), w''(u^\bullet)), \text{ for } (u,u',t) \in U'' \times U'' \times [0,1].$$

In particular, running over all $P \in \mathcal{P}_0$ and $w'(u^\bullet)$, $P_{u,w'(u)}(1) = P_{u^\bullet,w'(u^\bullet)}(1)$. This concludes the argument that the covers W_H and $W_{H,u}$ are equivalent. □

REMARK 1.2 ("Old" topology). Suppose V is an algebraic variety over K, a subfield of $\mathbb{C}$. Then, its fundamental group, $\pi_1(V, v_0)$, with v_0 with coordinates in K, is discrete. The topological properties of a (quasi-projective) algebraic variety over the complexes is an old subject for which one of the last treatments can be found in [**Z71**, Chap. VI] based much on many works of Lefshetz, listed in the volumes bibliography. Although this is very detailed, and theoretically it applies only to a nonsingular projective variety of dimension 2, the idea of a Lefshetz pencil is presented in detail.

As is the relation between the fundamental group of a generic curve and the fundamental group of the algebraic variety, and the homology groups of the variety. This is done through putting a CW complex structure on the variety. The use of resolutions of singularities doesn't affect the fundamental group as we have all of our varieties normalized, so the singularities have codimension 2 and don't affect it. [**Sp66**, p. 147] has the theorem that there is a topological space V for which $\pi_1(V, v_0) = G$ with G any a priori discrete group.

REMARK 1.3 (Lem. 1.1 in positive characteristic). It is wild ramification that causes Lem. 1.1 to be false even when V has dimension 1. [**FrM02**] replaces the configuration space U_r for covers of $\mathbb{P}^1_z$ in positive characteristic by a configuration space (target) for families of sphere covers based on a definition of *ramification data* and *regular ramfication data*, with the latter a generalization of higher ramification groups even when the local ramification is not Galois. Even the Galois closure of the covers in such families is not preserved, though the configuration spaces are of finite type, and locally versal for the finite topology. Grothendieck's famous theorem in the case of curves, when ramification is tame, says Lem. 1.1 then holds, though expected covers in that case might be missing if the prime of the characteristic divides the monodromy group. [**FrM02**] thus produces just one-half of a wildly ramified version of [**Gr71**].

1.3. Polarizations from the canonical class. Since we concentrate on Hurwitz spaces of covers of $\mathbb{P}^1_z$. §1.3 added comments on the *canonical (divisor) class*,

A reasonable model of it starts with a curve. Denote the genus of a compact Riemann surface X by $\mathbf{g}_X$. For this discussion, assume $g > 0$; $g = 0$ is an easier case. Polarizations of curves come from the Riemann-Roch theorem: Take as your

divisor, D', any point. You need, however, a divisor invariant under $G_{\mathbb{Q}}$ for an embedding that presents the curve with equations over $\mathbb{Q}$. See Rem. 1.4

Even, however, for compact, complex, torii, that are algebraic, there can be several different polarizations. So, the subject of abelian varieties includes giving a specific polarization. We later make contact with the following particular case.

For Jacobian varieties, of a projective curve X, there is a canonical polarization. Consider the $\mathbf{g}_X-1$-fold symmetric product, $W = X^{g-1}/S_{g-1}$, of X. These are positive divisors on X of degree $g-1$. Thus, if we translate W by some divisor D_0 of degree $g-1$ on X, the result represents a divisor on the Jacobian J_X of degree 0 divisors on X module linear equivalence.

To make this divisor even more canonical, Riemann took D_0 to be very special, a *half-canonical divisor* ($2D_0$ is in the class of the divisors of holomorphic differentials). He differentiated between the dimensions of the linear systems (even or odd). Eventually he used each type for different purposes in his descriptions of objects – differentials of various kind in particular – on X. [**Fa73**] is an older, still relevant, source for the story of Riemann's – and subsequent – attempts to form such objects. These deal in local coordinates on the moduli of genus g curves. We will deal with coordinates on Hurwitz spaces.

REMARK 1.4. There is a subtlety as to whether a *divisor class* over K with a nonempty linear system $L_{D'} = \{f \in K(X) \mid (f) + D' \geq 0\}$ suffices to give a map of X into a projective space $\mathbb{P}_L$ with image having coordinates over over K. Yes, $\mathbb{P}_L$ is a projective space over $\bar{\mathbb{Q}}$. Yet, unless the space has a point over K, it is just a Brauer-Severi variety – defining an element of the Brauer Group $H^2(G_{\mathbb{Q}}, (\bar{K})^*)$ cite[p. 891-892]Ro02 or [**Se67**].[1] It is not a distinction made in [**H77**] or [**Mu66**] since they predominantly work over an algebraically closed field. The canonical divisor class, though, is defined over the same field as is X.

1.4. Extension of constants. As we intend applications belonging to number theory, we have included the field K, which may be a number field: $[K : \mathbb{Q}] < \infty$ (often $\mathbb{Q}$ itself). We state several goals starting with the **RIGP** for a given G.

PROBLEM 1.5. Find an absolutely irreducible Galois cover $\hat{\varphi} : \hat{W} \to \mathbb{P}^1_z$ with group G defined, with all its automorphisms (commuting with $\hat{\varphi}$), over K.

That is, we seek an inner Nielsen class, $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$, containing a cover, $\hat{\varphi}$, defined over K. Our Main Theorem, followed by the **BCL** (acronym definition in Ch. 1) expands the value of Hurwitz spaces. To state the most useful version of this result we need one general definition.

[1] [**Se67**, Prop. 3] spells out key points about the Brauer group over a number field, including that it is determined by the induced cohomology in the completions of the field where it is locally trivial.

DEFINITION 1.6. Refer to $\varphi : W \to \mathbb{P}^1_z$, a cover in $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}_T}$, as a (G,G^*) regular realization over K, if φ is defined over K, and its Galois closure $\hat{\varphi} : \hat{W} \to \mathbb{P}^1_z$ of φ over K has group G^*. That means (§2.1), $\hat{W}$ has $|G^* : G|$ connected components over $\bar{K}$, all conjugate over K.

THEOREM 1.7. [**FrV91**, Main Thm.] *If G has no center, then the complete set of inequivalent* **RIGP** *realizations of G over K corresponds to this set:*

$$\mathrm{in}_G \stackrel{\mathrm{def}}{=} \cup_{\text{conjugacy class collections } \mathbf{C} \subset G} \{\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}(K)\}. \tag{2.7}$$

That is, for given G, if for even one conjugacy class collection $\mathbf{C}$, there is any K point $\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$, then

this regularly realizes G over K with a Galois cover $\hat{\varphi} : \hat{W}_{\hat{\boldsymbol{p}}} \to \mathbb{P}^1_z$.

Assume (G,T) is self-normalizing, $n = \deg(T)$. Then, $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{abs}}(K)$ corresponds to a (G,G^*) realization with $G^* \le N_{S_n}(G,\mathbf{C})$ (§3). For any $\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ over $\boldsymbol{p}$, as in (1.38)*, $K(\hat{\boldsymbol{p}}) = \hat{K}$ is a definition field of*

(2.8a) *all components of $\hat{W}_{\hat{\boldsymbol{p}}}$ and $\hat{\varphi}$ automorphisms; and*

(2.8b) *$G(\hat{K}/K) = G^*/G$.*

COMMENTS. The ability to set up both the absolute and inner versions (2.7) uniformly – without having to stipulate precise finite groups – to go after the **RIGP** and IGP requires configuration spaces with obvious projective coordinates as natural targets. Here they are the collections $\{U_r\}_{r=3}^{\infty}$.

Referencing these gives meaning to the field generated by the coordinates of $\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ (et. al.) over which the corresponding $\mathbb{P}^1_z$ cover is defined. Abstract schemes, though reasonable as moduli spaces, cannot provide a consistent meaning to giving coefficients of equations over a desired field.

Precise reference to covers by branch cycles in (2.7) does contrast with the more abstract stipulation of (G,G^*) realizations in (2.8). Still, as in Thm. 5.4, it produces very big Galois groups over certain fields K. □

DEFINITION 1.8 (Extension of Constants). Refer to $\hat{K}/K$ in (2.8) as the *extension of constants* for (the Galois closure of the cover of) $\boldsymbol{p}$.

Thm. 1.7 strikes into using the tools of §2 to understand specifics about Hurwitz spaces referenced by $(G,\mathbf{C})$. By attending to the conjugacy classes, $\mathbf{C}$, with G fixed, we open the discussion these issues.

(2.9a) How the **RIGP** for $(G,\mathbf{C})$ for one type of $\mathbf{C}$, can be almost trivial, while it is allied to famous unsolved problems for other $\mathbf{C}$.

(2.9b) How in certain contexts, even if the fine moduli hypotheses don't hold, with no loss we can adjust $(G,\mathbf{C})$ to assure they do.

(2.9c) Where we can use (2.8) to build upon an IGP realization of a group we identify as G^*/G to get an IGP realization of G^*.

(2.9d) What to think of our difficulties, starting with certain conjugacy classes $\mathbf{C}'$, upon allowing each class in $\mathbf{C}'$ to repeat many times.

2. Braid Action for reduced equivalence

[**Fr77**, §4] gives generators and relations for Hurwitz monodromy acting on Nielsen classes. (2.10) lists memorable generating elements. From (1.29d), H_r orbits on a Nielsen class correspond to irreducible components of the Hurwitz space.

2.1. Braids acting on reduced Nielsen classes. §2.1.1 gives the generators and relations of H_r and B_r, while §2.1.2 shows paths on U_r that gives the generators, and compute the most obvious relations. Details on relations that appear in our use of these groups follows in subsequent sections.

2.1.1. *Generators of H_r.* Braids *on Branch cycles* generate the action of H_r, the *Hurwitz monodromy group*, on a Nielsen class element $\boldsymbol{g}$:

$$\begin{array}{rl} q_i: & \boldsymbol{g} \stackrel{\text{def}}{=} (g_1,\dots,g_r) \mapsto (g_1,\dots,g_{i-1},g_ig_{i+1}g_i^{-1},g_i,g_{i+2},\dots,g_r);\\ \mathbf{sh}: & \boldsymbol{g} \mapsto (g_2,g_3,\dots,g_r,g_1) \text{ and } H_r \stackrel{\text{def}}{=} \langle q_2,\mathbf{sh}\rangle \text{ with}\\ & \mathbf{sh}\,q_i\mathbf{sh}^{-1}=q_{i+1},\ i=1,\dots,r{-}1. \end{array} \tag{2.10}$$

We call q_i the ith *twist*. Then, **sh**, sensibly enough is the (left) *shift*. The case $r=4$ is so important in our examples, that when we get to *reduced* Nielsen classes, we conveniently refer to q_2 as the *middle twist*.

Braids lead this subsection, and §3 has detailed examples for using them. We develop this more in the main examples of Ch. 5. It is the **BCL** that starts us into a serious discuss about the spaces. Here are other important points.

(2.11a) From product-one (1.23c) on Nielsen classes $\mathrm{Ni}(G,\mathbf{C})$, **sh** is an r cycle on all such classes.

(2.11b) (2.11a) allows reducing the subscript of q_i modulo r. Easily check this by starting with a given $\boldsymbol{g}$.

(2.11c) Conjugating by **sh**, shows **sh** and q_2 generate H_r.

Braid, B_r, relations: The group H_r is a quotient of the

$$\textit{Artin Braid group, } B_r=\langle Q_1,\dots,Q_{r-1}\rangle,$$

by its (minimal normal) subgroup generated by

$$Q_1Q_2\cdots Q_{r-1}Q_{r-1}\cdots Q_2Q_1,\ r\ge 3. \tag{2.12}$$

These are the standard B_r relations.

(2.13a) $Q_iQ_j=Q_jQ_i$ for $|i{-}j \mod r{-}1|>1$;

(2.13b) $Q_iQ_{i+1}Q_i=Q_{i+1}Q_iQ_{i+1}, i \mod r{-}1$.

The quotient map is given by $Q_i \mapsto q_i, 1 \le i \le r-1$. Calculate the action of (2.12) on $\boldsymbol{g} = (g_1, \dots, g_r)$ in a Nielsen class to see the result is $g_1 \boldsymbol{g} g_1^{-1}$.

REMARK 2.1 (How **sh** works). The operation $q_1 q_2 \cdots q_{r-1}$ on Nielsen classes represents **sh**. Direct calculation on $\boldsymbol{g} = (g_1, \dots, g_r) \in G^r$ shows its effect:

$$\boldsymbol{g} \mapsto (g_1 g_2 g_1^{-1}, \dots, g_1 g_r g_1^{-1}, g_1 g_1 g_1^{-1}) \text{ shift, then conjugate by } g_1.$$

PROBLEM 2.2. Running over all conjugates of (2.12), conclude that the minimal equivalence on $\mathrm{Ni}(G, \mathbf{C})$ that affords an H_r action is $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$.

Hint: Use the generators of (6.35).

2.1.2. *Explicit effect of braiding.* [**Fr77**, p. 49–53] breaks the problem of computing the effect of dragging a cover by its branch points into two parts. First, only branch points restricted to lie on $\mathbb{P}^1_z \setminus \{\infty\} = \mathbb{A}^+$. Here the ith "cut" runs from the initial branch point z_i^0 $\boldsymbol{z}_0$ to $-\infty$ parallel to the (negative) real axis.

This allows taking as a basepoint a simply-defined value: $z_0 = 1 + \max(\Re z_i')_{i=1}^r$. The presentations takes pains how to handle 'cuts" – while dragging branch points – when two or more points happen, at some time t', to lie on a line parallel to the negative x-axis.

PROBLEM 2.3. Given r distinct points $z_1, \dots, z_r$ on $\mathbb{A}^+$, and another point z_0 distinct from them, show there are always smooth pairwise nonintersecting, except at z_0, paths $\gamma_1, \dots, \gamma_r$ starting (respectively) at z_0 and ending at z_i, that emanate from z_0 in clockwise order of their subscripts. Hint: Inductively, assume you have achieved this for i, and use that $\mathbb{A}^+ \setminus \{\gamma_1, \dots, \gamma_i\} \cup \{z_0\}$ is connected by contracting all the paths to z_0.

Use Prob. 2.3 to show with no loss, up to homotopy, we may initially assume $\Im(z_1^0) < \cdots < \Im(z_r^0)$. Let Q_i be the automorphism of $F_r = \pi_1(\mathbb{A}^+, z_0)$ that maps the r-tuple of generators $(\bar{g}_1, \dots, \bar{g}_r)$, in order, to the new r-tuple of generators

$$\bar{\boldsymbol{g}} = (\bar{g}_1, \dots, \bar{g}_{i-1}, \bar{g}_i \bar{g}_{i+1} \bar{g}_i^{-1}, \bar{g}_i, \bar{g}_{i+2}, \dots, \bar{g}_r),\ i = 1, \dots, r-1.$$

Fig. 1 gives a specific path Γ_i on $\mathbb{A}^r$, that has the effect of achieving Q_i, as the acting of dragging branch points and pulling along classical generators lying entirely on $\mathbb{A}^+$ that represent $\bar{\boldsymbol{g}}$. It starts at $\boldsymbol{z}^0$ and ends at

$$(z_1^0, \dots, z_{i-1}^0, z_{i+1}^0, z_i^0, z_{i+2}^0, \dots, z_r^0) = (\boldsymbol{z}^0)\sigma,\ \sigma = (i\, i{+}1).$$

Its coordinates are constant, excluding the ith and $i{+}1$th. The ith coordinate z_i moves from z_i^0 to z_{i+1}^0; the $i{+}1$th coordinate z_{i+1} moves from z_{i+1}^0 to z_i^0.

Consider the bounded component, W, of $\mathbb{A}^1 \setminus \lambda$, where λ is the set of points on the path $\delta_i \bar{\epsilon}_i (\delta_{i+1})^{-1}$. With no loss assume that $\bar{\epsilon}_i'$ is outside W. Finally, let λ_i

FIGURE 1. Traversing $\bar{\Gamma}_i$, z_i and z_{i+1} change places without meeting

(resp., λ'_{i+1}) be the clockwise path from b_i to b'_i (resp., b'_{i+1} to b_{i+1}). It follows automatically (as in Part 3 of the proof of Theorem 2.10) that the paths $\bar{\gamma}_i\bar{\epsilon}_i\bar{\gamma}_{i+1}(\bar{\epsilon}_i)^{-1}$ and $\lambda_i(\bar{\epsilon}'_i)^{-1}\lambda'_{i+1}(\bar{\epsilon}_i)^{-1}$ are homotopic (say, with b_i and b_{i+1} fixed) and that the bounded components of their complement contain z_i^0 and z_{i+1}^0 and exclude z_j^0 for $j \neq i, i+1$. With a judicious choice, however, of $\bar{\epsilon}'_i$ this can be arranged without appeal to previous results. We use the notation of Def. 4.8.

PROPOSITION 2.4. *Let $\bar{\Gamma}_i$ be the path $(z_i^0, \dots, z_{i-1}^0, (\epsilon'_i)^{-1}, \epsilon_i, z_{i+1}^0, \dots, z_r)$. Then, $(\bar{\Gamma}_i)Q^*$ is Q_i, the element of* 4.10, *$i = 1, \dots, r-1$.*

PROOF. Apply a section Φ along Γ (Theorem 4.7). As before, assume that $\bar{\Gamma}_i : [0,1] \to \mathbb{A}^r \setminus \Delta_r$. This is what we must show: that γ_i^1 is homotopic to $\gamma_i^0\gamma_{i+1}^0(\gamma_i^0)^{-1}$; that γ_{i+1}^1 is homotopic to γ_i^0; and that γ_j^1 is homotopic to γ_j^0 for $j \neq i$ or $i+1$. Note that none of the coordinates of $\boldsymbol{z}^0$ can be located in the component W of $\mathbb{P}^1 \setminus \lambda$ (above), or else there would be an a_j on the clockwise path along δ_0 from a_i to a_{i+1}, contrary to Ex. 2.9.

Choose d' as in the proof of Theorem 4.7. There exists $d'' > 0$ such that for $\boldsymbol{\gamma} \in \mathcal{B}(\boldsymbol{z}^0, d'')^+$ we have $\Phi(t)(\boldsymbol{\gamma}) \in \mathcal{B}(\Phi(t)\boldsymbol{z}^0, d')^+$ for all $t \in [0,1]^{[4.4]}$. As in the last paragraph of the proof of Theorem 4.7 conclude:

(2.14a) γ_i^1 is homotopic to $\delta_i\lambda_i(\bar{\epsilon}'_i)^{-1}\lambda'_{i+1}\bar{\gamma}_{i+1}(\lambda'_{i+1})^{-1}\bar{\epsilon}'_i(\lambda_i)^{-1}(\delta_i)^{-1}$;

(2.14b) γ_{i+1}^1 is homotopic to $\delta_{i+1}(\bar{\epsilon}_i)^{-1}\bar{\gamma}_i\bar{\epsilon}_i(\delta_{i+1})^{-1}$; and

(2.14c) γ_j^1 is homotopic to γ_j^0 for $j \neq i, i+1$.

The same argument as in Part 2 of Theorem 2.10 shows that $\delta_i\bar{\epsilon}_i$ is homotopic to δ_{i+1} (with initial and endpoints fixed). From 4.11b this immediately gives γ_{i+1}^1 homotopic to γ_i^0.

Finally, $\bar{\gamma}_i\bar{\epsilon}_i\bar{\gamma}_{i+1}$ and $\lambda_i(\bar{\epsilon}'_i)^{-1}\lambda'_{i+1}$ are homotopic. Therefore 4.11a gives γ_i^1 homotopic to $\delta_i\bar{\gamma}_i\bar{\epsilon}_i\bar{\gamma}_{i+1}(\bar{\epsilon}_i)^{-1}(\bar{\gamma}_i)^{-1}(\delta_i)^{-1}$. This, in turn, is homotopic to

$$\gamma_i^0\delta_{i+1}\bar{\gamma}_{i+1}(\delta_{i+1})^{-1}(\gamma_i^0)^{-1} = \gamma_i^0\gamma_{i+1}^0(\gamma_i^0)^{-1}$$

through an insertion of $(\delta_i)^{-1}\delta_i$ (resp., $\delta_i(\delta_i)^{-1}$) between the terms $\bar{\gamma}_i$ and $\bar{\epsilon}_i$ (resp., $(\bar{\epsilon}_i)^{-1}$ and $(\bar{\gamma}_i)^{-1}$). This concludes the proof of the lemma. □

Thm. 2.5 summarizes what we use of B_r [**ArE25**], [**ArE47**], [**B47**].

THEOREM 2.5. *The natural homomorphism Q^* from dragging branch points maps $\pi_1(\mathbb{A}^r \setminus D_r, \boldsymbol{x}_0)$ onto the conjugacy class preserving automorphisms of F_r that also preserve $\bar{g}_1 \cdots \bar{g}_r$, induces an isomorphism between the former group and $B_r = \langle Q_1, \ldots, Q_{r-1} \rangle$. This gives a presentation of B_r by the normal subgroup generated by the relations in* (2.13).

2.1.3. *Reduced equivalence.* There are other equivalences † than inner or absolute. Yet, in each case we understand many properties of the space of covers through H_r acting on $\mathrm{Ni}(G, \mathbf{C})^\dagger$. For F a field, recall the group (under composition) of *Möbius transformations* on $\mathbb{P}^1_z$:

$$\mathrm{M\ddot{o}b}(F) \stackrel{\mathrm{def}}{=} \left\{ z \mapsto \frac{az+b}{cz+d} \mid ad-bc = 1, a, b, c, d \in F \right\}. \tag{2.15}$$

For $F = \mathbb{C}$ these give the group of automorphisms of $\mathbb{P}^1_z$. Identify these with equivalence classes of matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ satisfying the same conditions, modulo diagonal matrices $\{\left(\begin{smallmatrix} a & 0 \\ 0 & a^{-1} \end{smallmatrix}\right) \mid a \in F^*\}$. This is also denoted $\mathrm{PSL}_2(F)$. §**??** has a list of related affine groups.

DEFINITION 2.6 (Reduced action). A cover $f : W \to \mathbb{P}^1_z$ is *reduced* equivalent to $\alpha \circ f : W \to \mathbb{P}^1_z$ for $\alpha \in \mathrm{PSL}_2(\mathbb{C})$.

Also, α acts on $\boldsymbol{z} \in U_r$ by acting on each entry. That extends to an action on any cover $\Phi^\dagger : \mathcal{H}(G, \mathbf{C})^\dagger \to U_r$ and a reduced Hurwitz space cover:

$$\Phi^{\dagger,\mathrm{rd}} : \mathcal{H}(G, \mathbf{C})^{\dagger,\mathrm{rd}} \to U_r/\mathrm{PSL}_2(\mathbb{C}) \stackrel{\mathrm{def}}{=} J_r. \tag{2.16}$$

Reduced uses: Here are two reasons for its use, each connecting to a different half of the applications in this book. Recall the upper half space

$$\mathbb{H}^{\mathrm{up}} = \{z \in \mathbb{C} \mid \text{the imaginary part of } z > 0\}.$$

(2.17a) If a cover $\hat{\varphi} : \hat{X} \to \mathbb{P}^1_z$ gives an **RIGP** realization of G over $\mathbb{Q}$, then so does $\alpha \circ \hat{\varphi}$ for $\alpha \in \mathrm{PSL}_2(\mathbb{Q})$.

(2.17b) For $r = 4$, reduced Hurwitz spaces are quotients of $\mathbb{H}^{\mathrm{up}}$ (Thm. 2.13).

Comment on (2.17a): We separate the **RIGP** from the IGP. From an **RIGP** realization of G, applying Hilbert's Irreducibility Theorem §6.1.1 by specializing z in $\mathbb{Q}$ immediately produces infinitely many IGP realizations of the given group G. The specializations that work are dense in any particular topology on $\mathbb{P}^1_z(\mathbb{Q})$. Comparing those to IGP realizations not coming from an **RIGP** realization is still nontrivial (as in §6.1).

Whether there are infinitely many **RIGP** realizations of G, or more general parameters for their realizations, is also significant. Using the equivalence of (2.17a) precludes trivial changes in such realizations.

Comment on (2.17b): Not only are the two halves of this book connected, but we can easily use the properties of the spaces on which they rely to see they have analogs of the properties of modular curves. That starts with the *upper half-plane paradigm* below. There, we get to ask questions about the nature of the finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ that defines a reduced Hurwitz space when $r = 4$. Especially about its cusps when it is compactified to a cover of $\mathbb{P}^1_j$, the classical j-line. The comparison comes clearer after we have introduced **M**(odular) **T**(owers).

2.1.4. *The upper half-plane paradigm.* A reduced Hurwitz space of 4 branch point covers is a natural j-line cover – $U_r/\mathrm{PSL}_2(\mathbb{C})$ identifies with $\mathbb{P}^1_j \setminus \{\infty\}$ – that completes to $\overline{\mathcal{H}}(G, \mathbf{C})^{\dagger,\mathrm{rd}} \to \mathbb{P}^1_j$ ramified over $0, 1, \infty$. We refer to this as the

The *upper half plane paradigm* (for $r = 4$),

a consequence of Thm. 2.7. That demonstrates that modding out by $\mathrm{PSL}_2(\mathbb{C})$ on the cover $\mathcal{H}(G, \mathbf{C})^\dagger \to U_4$ produces a natural cover of the classical j-line $\mathbb{P}^1_j \setminus \{\infty\} = U_j = \mathbb{H}^{\mathrm{up}}/\mathrm{SL}_2(\mathbb{Z})$. We have placed the corresponding images of elliptic fixed points on $\mathbb{H}^{\mathrm{up}}$ at 0 and 1.

THEOREM 2.7. *The image, $\mathcal{H}^\dagger/\mathrm{PSL}_2(\mathbb{C}) = \mathcal{H}^{\dagger,\mathrm{rd}}$, of any component, $\mathcal{H}^\dagger$ of $\mathcal{H}(G, \mathbf{C})^\dagger$ is a quotient of the upper half-plane $\mathbb{H}^{\mathrm{up}}$ by a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. That makes $\mathcal{H}^{\dagger,\mathrm{rd}} \to \mathbb{P}^1_j \setminus \{\infty\}$ a cover ramified of order (at most) 3 (resp. 2) over $j = 0$ (resp. 1).*

For $r = 4$, Thm. 2.13 handles the geometric monodromy, and cusps, of reduced Hurwitz space components as covers of the j-line. In particular, it computes the genus of such reduced components.

Then §3 applies that to give example spaces. We have simplified the treatment of [**BFr02**, Prop. 2.3 and its proof, §2.3] in respective proofs of Thm. 2.7 and Thm. 2.14 (a tighter relation between H_4 and B_4, as in (2.13)) in §4. Taking off from the *upper half-plane paradigm*, whereby reduced Hurwitz spaces defined by $r = 4$ conjugacy classes are actually upper half-plane quotients which we may compare with the special case of modular curves, §**??** produces a formula for computing the components and genuses of reduced Hurwitz space components through their being covers of the classical j-line.

2.2. Reduced Hurwitz spaces for $r = 4$. With $\mathcal{Q} = \langle (q_1q_2q_3)^2, q_1q_3^{-1} \rangle$, [**BFr02**, §4.2] contains the formula whose statement in Thm. 2.13 uses

$$\text{reduced Nielsen classes } \mathrm{Ni}(G, \mathbf{C})^{\dagger,\mathrm{rd}} \stackrel{\mathrm{def}}{=} \mathrm{Ni}(G, \mathbf{C})^\dagger/\mathcal{Q}. \tag{2.18}$$

2.2.1. *Universal B_r and H_r actions.* Consider the free group, $\bar{G}_r$, on generators $\bar{g}_1, \dots, \bar{g}_r$, with $\pi(\bar{\boldsymbol{g}}) = \bar{g}_1 \cdots \bar{g}_r$. Denote the conjugacy class of $\bar{g}_i$ by $\mathrm{C}_{\bar{g}_i}$, $i =$

$1,\dots,r$. Now consider a version of a Nielsen class.

$$\bar{\mathrm{Ni}}_r(\bar{G}_r,\mathbf{C}_{\bar{\boldsymbol{g}}})_{\pi(\bar{\boldsymbol{g}})} \stackrel{\text{def}}{=} \{\bar{\boldsymbol{g}}'\in\mathbf{C}_{\bar{\boldsymbol{g}}} \mid \pi(\bar{\boldsymbol{g}}')=\pi(\bar{\boldsymbol{g}}) \text{ and } \langle \boldsymbol{g}'\rangle=\bar{G}_r\}.$$

Use the same actions for the Q_i as for the q_is in (2.13). Then, $\bar{\mathrm{Ni}}_r(\bar{G}_r,\mathbf{C}_{\bar{\boldsymbol{g}}})_{\pi(\bar{\boldsymbol{g}})}$ would be a univeral Nielsen class, except we have replaced product-one with $\pi(\bar{\boldsymbol{g}}')$ – preserved by B_r – being fixed at $\pi(\bar{\boldsymbol{g}})$.

Instead, replace this with the condition $\pi(\bar{\boldsymbol{g}})=1$ and mod out by the inner action of elements of $\bar{G}_r$ ($\bar{\boldsymbol{g}}'$ is equivalent to $\bar{g}\bar{\boldsymbol{g}}'\bar{g}^{-1}$, $\bar{g}\in\bar{G}_r$). Then, we get an object, $\bar{\mathrm{Ni}}_r(\bar{G}_r,\mathbf{C}_{\bar{\boldsymbol{g}}})^{\mathrm{in}}$, that is akin to universal inner Nielsen classes. On it we do have an H_r action as in ((1.29c) or Prob. 2.2). Denote the image group of this action by M_r, the *Mapping Class Group*.

For the rest of this section we assume $r=4$ in §4.2.1. Then, (6.34) gives the extra relations for M_4 (beyond those for B_4):

$$\begin{gathered}\tau_1(4)=(Q_3Q_2)^3=1,\ \tau_2(4)=Q_1^{-2}Q_3^2=1,\\ \tau_3(4)=(Q_2Q_1)^{-3}=1 \text{ and } \tau(4)=(Q_3Q_2Q_1)^4=1.\end{gathered}\tag{2.19}$$

Consider Ch. 6 (6.35) for $r=4$, with $Q_1Q_2Q_3^2Q_2Q_1=R_1(4)$, and

$$\begin{gathered}R_2(4)=Q_1^{-1}R_1(4)Q_1, R_2(4)=Q_2^{-1}R_1(4)Q_2,\\ R_3(4)=Q_3^{-1}R_1(4)Q_3 \text{ and } (Q_1Q_2Q_3)^4.\end{gathered}\tag{2.20}$$

Denote an element of B_4 (resp. H_4) that has the effect of conjugating $\boldsymbol{g}$ by $\pi(\bar{\boldsymbol{g}})$ by $Q(\bar{\boldsymbol{g}})$ (resp. $q(\bar{\boldsymbol{g}})$).

LEMMA 2.8. *Both $(Q_1Q_2Q_3)^4$ and $(Q_3Q_2Q_1)^4$ have the effect of $Q(\bar{\boldsymbol{g}})$.*

Then, B_4 acting on $\bar{G}_4$ induces $\alpha_4: B_4\to\mathrm{Aut}(\bar{G}_4)$ with the center $\langle(Q_1Q_2Q_3)^4\rangle$ of B_4 generating the kernel. This induces $\mu_4: H_4\to M_4$.

The kernel of $B_4\to M_4$ is the direct product of

$$\text{the free group } K_4^*=\langle(Q_3Q_2)^3,Q_1^{-2}Q_3^2,(Q_2Q_1)^{-3}\rangle \text{ and } \langle(Q_1Q_2Q_3)^4\rangle.$$

Above, $Z=i(\bar{\sigma}_1\bar{\sigma}_2\bar{\sigma}_3\bar{\sigma}_4)$ is identical to an element of B_4. Consider the image z of Z in H_4:

$$(q_1q_2q_3)^4z=1=(q_3q_2q_1)^4z=q_1^2q_3^{-2}z \text{ and } z^2=1.$$

In particular, combining this with (2.26) *identifies M_4 with the image of H_4 in $\mathrm{Aut}(G_4)/\mathrm{Inn}(G_4)$. So, the image of z in M_4 is 1.*

PROOF. The map i induces $i: G_4\to\mathrm{Inn}(G_4)$. Action of B_4 preserves $\Pi(\bar{\boldsymbol{\sigma}})$. Thus, it induces a homomorphism of B_4 into $\mathrm{Aut}(G_4)$ where D goes to the automorphism $i(\bar{\sigma}_1^{-1})$, $\bar{\boldsymbol{\sigma}}\mapsto\bar{\sigma}_1\bar{\boldsymbol{\sigma}}\bar{\sigma}_1^{-1}$ (as in (**??**)). Conclude: Modulo inner automorphisms of G_4, D acts trivially, producing the desired homomorphism

$$H_4\to\mathrm{Aut}(G_4)/\mathrm{Inn}(G_4).$$

Now consider the explicit formulas. Most of the calculation is in (**??**): $Q_1Q_2Q_3$ cycles entries of $\bar{\boldsymbol{\sigma}}$ back 1, and conjugates all entries by the first entry's inverse. So

$(Q_1Q_2Q_3)^4$ leaves entries of $\bar{\boldsymbol{\sigma}}$ untouched except for conjugating them by

$$(\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4\bar\sigma_3^{-1}\bar\sigma_2^{-1}\bar\sigma_1^{-1}\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_2^{-1}\bar\sigma_1^{-1}\bar\sigma_1\bar\sigma_2\bar\sigma_1^{-1}\bar\sigma_1)^{-1} = (\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4)^{-1}.$$

Also, $Q_3Q_2Q_1$ cycles the entries of $\bar{\boldsymbol{\sigma}}$ forward 1. The new first entry is the old 4th entry conjugated by the inverse of the product of the old first three entries. Thus, $(Q_1Q_2Q_3)^4$ and $(Q_3Q_2Q_1)^4$ act the same. Add that D maps to 1 in H_4 to see

$$1 = (q_1q_2q_3)^4(q_3q_2q_1)^4 = (q_1q_2q_3)^8 = z^{-2}.$$

Let $Q' = Q_1Q_2Q_3$. Extending the calculation above gives the next list:

$$1 = (Q')^{-1}DQ'(Q_1Q_2)^3 i(\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4);$$
$$1 = (Q'Q_1Q_3^{-1})^2(Q')^{-1}DQ' i(\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4);$$
$$1 = (Q')^4 i(\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4); \text{and}$$
$$1 = (Q_1Q_3^{-1})^2(Q')^{-1}D(Q_1Q_2Q_3)(Q_1Q_2Q_3)^{-2}D(Q_1Q_2Q_3)^2 i(\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4).$$

Add the relation $Q_1Q_3 = Q_3Q_1$ to deduce, in order, these relations in H_4:

$$\begin{array}{llll} \text{a)} & (q_1q_2)^3z = 1; & \text{b)} \quad (q_1q_2q_1)^2z = 1; & \text{c)} \quad (q_1q_2q_3)^4z = 1; \\ \text{d)} & (q_1q_3^{-1})^2z = 1; & \text{e)} \quad q_1q_3 = q_3q_1. & \end{array} \tag{2.21}$$

So, the image of z in M_4 is 1.

The kernel of α_4 contains elements of B_4 inducing inner automorphisms commuting with conjugation by $\bar\sigma_1\bar\sigma_2\bar\sigma_3\bar\sigma_4 = c$. Since c generates conjugations commuting with c, $\langle (Q_1Q_2Q_3)^4\rangle$ generates the kernel of α_4.

Generators of K_4^* act on G_4: Respectively, $(Q_3Q_2)^3, Q_1^{-2}Q_3^2, (Q_2Q_1)^{-3}$ induce conjugation by g_4, g_1g_2, g_1. These conjugations on G_4 form a free group. So K_4^* is a free group on these generators. □

From Lem. 2.8, the direct product of the free group $K_4^* = \langle (Q_3Q_2)^3, Q_1^{-2}Q_3^2, (Q_2Q_1)^{-3}\rangle$ and $\langle (Q_1Q_2Q_3)^4\rangle$ equals $N_4 \stackrel{\text{def}}{=} \ker(B_4 \to M_4)$. Denote $Q_1Q_2Q_3^2Q_2Q_1$ (D in (**??**)) by R_1. The following presentation of N_4 is superior for our purposes. It easily follows from the notation and proof of Lemma 2.8.

The effect of R_i on $\bar{\boldsymbol{g}}$ is conjugation by $\bar g_i$. We consider Prop. 2.9 only for r = 4, though it works for any value of r.

PROPOSITION 2.9. *Elements of* (2.20) *generate* N_4. *Any representative* $\boldsymbol{g}$ *in a Nielsen class* $\mathrm{Ni}(G, \mathbf{C}) = \mathrm{Ni}$ *produces an evaluation homomorphism*

$$\psi_{\boldsymbol{g}} : N_4 \to G/\mathrm{Cen}(G) \text{ mapping } \prod_{i=1}^4 R_i \text{ to } 1.$$

Conversely, any homomorphism $\psi : N_4 \to H$ *mapping* $\prod_{i=1}^4 R_i$ *to 1 produces an associated Nielsen class representative.*

For $Q \in B_4$, *act on* $\psi_{\boldsymbol{g}}$ *by applying evalution of* $Q^{-1}\boldsymbol{R}Q$ *to* $\boldsymbol{g}$. *An orbit on* Ni *is equivalent to a* B_4 *orbit on the homomorphisms* $\psi_{\boldsymbol{g}}$ *(up to conjugation by* G*).*

2.2.2. *The groups $M_4, \bar{M}_4$ and $\mathcal{Q}''$.* Denote the element $q_1q_3^{-1}$ by $\tilde{z}$. Prop. 2.10 shows that $B_4 \to M_r$ factors through H_4 to give $H_4/\langle \tilde{z}^2\rangle = M_4$.

It also shows precisely what relations give the quotient for the H_4 action on reduced equivalence classes of covers; that reduced equivalence kills $\tilde{z}$.

$$\text{Set } \bar{\gamma}_0 = q_1q_2 \text{ and } \bar{\gamma}_1 = q_1q_2q_3.$$

Suppose $\mathcal{P}$ are classical generators of $\pi_1(U_{\boldsymbol{z}}, z_0)$ relative to $(\boldsymbol{z}, z_0)$ (1.23).

Lemma 2.8 shows adding these relations to B_4 is equivalent to adding $q_1^2q_3^{-2} = 1$ to H_4. This produces new equations:

$$q_1q_2q_1^2q_2q_1 = (q_1q_2q_1)^2 = (q_1q_2)^3 = 1. \tag{2.22}$$

Then, $\gamma_0 = q_1q_2$, $\gamma_1 = q_1q_2q_1$ and $\gamma_\infty = q_2$ satisfy

$$\gamma_0\gamma_1\gamma_\infty = 1. \tag{2.23}$$

The relation $q_1q_3^{-1} = 1$ is not automatic from (2.26). Crucial, however, is how M_4 acts on *reduced Nielsen classes*: equivalence of branch cycles $\boldsymbol{g}$ in a Nielsen class equivalenced by the action of $\mathrm{PGL}_2(\mathbb{C})$. This action *does* factor through the relation $q_1q_3^{-1} = 1$ (Prop. 2.10). Therefore it factors through the induced quotient $H_4/\mathcal{Q} = \bar{M}_4$ of Thm. 2.14.

PROPOSITION 2.10. *The center of H_4 contains $\tilde{z}^2$. Both $\mathbf{sh}^4$ and $\tilde{z}^2$ act as the identity on $\bar{\mathrm{Ni}}_r^{\mathrm{in}}$. Thus, $\mathcal{Q}$ acts on $\mathrm{Ni}(\bar{G}_r, \mathbf{C}_{\bar{\boldsymbol{g}}})^{\mathrm{in}}$ through $\mathcal{Q}'' = \mathcal{Q}/\langle\tilde{z}^2\rangle$.*

Further, $\mathcal{Q}''$ is normal in M_4. Let O be a braid orbit in $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$. Then, $\mathcal{Q}''$ acts through representations of the Klein 4-group on O. So, all of its orbits on O have a common length that is 1, 2 or 4.

Assume $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ corresponds to $\varphi_{\boldsymbol{g}} : W_{\boldsymbol{g}} \to \mathbb{P}^1_z$ with respect to $\mathcal{P}$.

Then, for $q \in \mathcal{Q}''$, $\varphi_{(\boldsymbol{g})q} : W_{(\boldsymbol{g})q} \to \mathbb{P}^1_z$ is reduced equivalent to $\varphi_{\boldsymbol{g}}$.

PROOF. Apply $\tilde{z}^2$ to $\bar{\boldsymbol{g}} = (\bar{g}_1, \dots, \bar{g}_4)$:

$$\bar{\boldsymbol{g}} \xrightarrow{\tilde{z}} (\bar{g}_1\bar{g}_2\bar{g}_1^{-1}, \bar{g}_1, \bar{g}_4, \bar{g}_4^{-1}\bar{g}_3\bar{g}_4) \xrightarrow{\tilde{z}}$$
$$((\bar{g}_1\bar{g}_2)\bar{g}_1(\bar{g}_1\bar{g}_2)^{-1}, (\bar{g}_1\bar{g}_2)\bar{g}_2(\bar{g}_1\bar{g}_2)^{-1}, (\bar{g}_3\bar{g}_4)^{-1}\bar{g}_3(\bar{g}_3\bar{g}_4), (\bar{g}_3\bar{g}_4)^{-1}\bar{g}_4(\bar{g}_3\bar{g}_4)).$$

Since $\bar{g}_1 \cdots \bar{g}_4 = 1$, $\bar{g}_1\bar{g}_2 = (\bar{g}_3\bar{g}_4)^{-1}$, the result is conjugation of $\bar{\boldsymbol{g}}$ by $\bar{g}_1\bar{g}_2$. That shows all the statements of the first paragraph, including that $\mathcal{Q}$ acts on Nielsen classes through $\mathcal{Q}''$.

Now we show $\mathcal{Q}''$ is normal in M_4^{in}. From relations (2.13) in B_4:

$$\begin{aligned}\bar{\gamma}_1^2\tilde{z} &= q_1q_2q_3q_1q_2q_1 = q_1(q_2q_3q_2)q_1q_2\\ &= q_1(q_3q_2q_3)q_1q_2 = q_3(q_1q_2q_3)q_1q_2(q_3q_3^{-1}) = q_3\bar{\gamma}_1^2q_3^{-1}.\end{aligned}$$

and $q_3\tilde{z}q_3^{-1} = \tilde{z}$. Thus q_3 normalizes $\mathcal{Q}''$. Since $\tilde{z} = q_1q_3^{-1} \in \mathcal{Q}''$, q_1 also normalizes $\mathcal{Q}$. We now show q_2 does also.

RETURNM Use $(q_1q_2)^3$ *tildez* $= 1$ Apply (2.13a) in the form q?1q?1q?1 = zq q q to get 2 212 121 q?1??1q =q?1q?1q?1q q q =z(q q q)q q q =z?2. 2 2 212232 121323 Also, since z is a central involution, conjugate by q?1 to get q ?2q?1 = z??1.

Compute the action of $\tilde{z}$ on $\boldsymbol{g} = (g_1, \dots, g_4)$:

$$\boldsymbol{g} \xrightarrow{q_1 q_3^{-1}} (g_1 g_2 g_1^{-1}, g_1, g_4, g_4^{-1} g_3 g_4) \xrightarrow{q_1 q_3^{-1}} ((g_1 g_2) g_1 (g_1 g_2)^{-1}, g_1 g_2 g_1^{-1}, g_4^{-1} g_3 g_4, (g_3 g_4)^{-1} g_4 (g_3 g_4)).$$

In the bottom row 2nd term (resp. 3th term) substitute $g_2 g_2 g_2^{-1}$ (resp. $g_3^{-1} g_3 g_3$) for g_2 (resp. g_3). The result is that the first two terms (resp. last two terms) are the corresponding terms of $\boldsymbol{g}$ conjugated by $g_1 g_2$ (resp. $(g_3 g_4)^{-1}$).

From product-one applied to $\mathbf{g}$(????)), $g_1 g_2 = (g_3 g_4)^{-1}$. Therefore, the result is a conjugation by $g_1 g_2$, an inner equivalence occuring in either $\mathrm{Ni}(G, \mathbf{C})^{\dagger}$. That shows the action of $\tilde{z}$ is trivial on Nielsen classes.

With no loss, consider $\mathcal{Q}$ on Nielsen classes as acting through $\mathcal{Q}''$. Since $\mathcal{Q}''$ is normal in M_4, any $\mathcal{Q}''$ orbit, O_m is carried to another $\mathcal{Q}''$ orbit (in O) by any $q \in M_4$. This gives all $\mathcal{Q}''$ orbits in O a common length. Conclude by characterizing the Klein 4-group as the dihedral group D_2.

First, by definition of $\mathcal{Q}''$, $(q_1 q_3^{-1})^2$ is trivial, as is $\mathbf{sh}^2$. As a group generated by two involutions, $\mathcal{Q}''$ in its action on Nielsen classes is the dihedral group D_n, with n the order of the action of the product of $q_1 q_3^{-1}$ and the $\mathbf{sh}$.

The braid relation $q_1 q_2 q_3 q_3 q_2 q_1$ becomes $q_1 q_2 q_1 q_1 q_2 q_1 = 1$. Lemma 2.10 shows adding these relations to B4 is equivalent to adding q2q?2 = 1 to H . This produces new equations: 134 (2.9) q1q2q12q2q1 = (q1q2q1)2 = (q1q2)3 = 1. □

2.2.3. $\bar{M}_4$ *subgroups; reduced fine moduli.* Prop. 2.10 shows how $\mathcal{Q}'' = \mathcal{Q}/\langle \tilde{z} \rangle$ acts on Nielsen classes, an effect critical for what *fine moduli* means for reduced Hurwitz spaces when $r = 4$. The two groups to keep in mind $r = 4$ are these:

$$\begin{aligned} \textit{Moduli Group:} \quad & \mathcal{Q}'' \stackrel{\text{def}}{=} \langle q_1 q_3^{-1}, \mathbf{sh}^2 \rangle / \langle \tilde{z} \rangle \\ \textit{Cusp Group:} \quad & \mathrm{Cu}_4 \stackrel{\text{def}}{=} \langle q_2, \mathcal{Q}'' \rangle / \mathcal{Q}''. \end{aligned} \tag{2.24}$$

(2.25a) *b(irational)-fine moduli*: $\mathcal{Q}''$ must act as a Klein 4-group; and

(2.25b) *e(lliptic)-fine moduli*: neither γ_0 nor γ_1 has fixed points (on O).

We have given in (2.17) reasons for using reduced spaces. Further, in (2.17b) why the case $r = 4$ stands out to make comparisons with modular curves. There are differences between $r = 4$ and $r > 4$ for fine moduli. We illustrate the outcomes when fine moduli doesn't hold in this section using our examples, and specifically the case when we work over the field, $\mathbb{R}$, of real numbers Ch. 3 §6.2.

Remark 2.11 (Fine moduli for $r > 4$). The algorithm for using the $\mathbf{sh}$-incidence matrix works for $r > 4$ as in Lem. 3.6. There are, though these differences. A group like $\mathcal{Q}''$ only appears for $r = 4$, so the first condition of (2.25) is moot. We still, however, have a version of condition (2.25b): existence of elliptic fixed points. These would now would be singular on the reduced Hurwitz space, rather than just ramified in the cover $\mathcal{H}^{\dagger,\mathrm{rd}} \to \mathbb{P}^1_j$.

For these singular points, each can make a contribution to not having fine reduced moduli, a condition that we may calculate from the Nielsen class directly using branch cycles. See §4.3.3.

REMARK 2.12 (Product-one). Product-one, $\gamma_1\gamma_2\gamma_3 = 1$, is now a consequence of the Hurwitz braid relation

$$q_1q_2\cdots q_{r-1}q_{-1}q_{r-2}\cdots q_1 \tag{2.26}$$

combined for $r = 4$ with modding out by $q_1 = q_3$. That immediately gives $\gamma_1^2 = 1$ in its action on reduced Nielsen classes. For $\gamma_0^3 = 1$, use the braid relations

$$q_iq_{i+1}q_i = q_{i+1}q_iq_{i+1} \text{ and for } |i-j| > 1 \mod r-1,\ q_iq_j = q_jq_i. \tag{2.27}$$

The latter says non-contiguous braids commute.

2.2.4. *Genus formula for $r = 4$.* Thm. 2.13 allows computing properties of reduced Hurwitz spaces when $r = 4$ without needing their descriptions as upper half-plane quotients. Except for our running example of covers from dihedral groups, as in §3.2, they aren't modular curves, their defining subgroups are not congruence subgroups. Therefore, they would be both hard to find, and even harder to use.

THEOREM 2.13. *Suppose a component, $\overline{\mathcal{H}}'$, of $\overline{\mathcal{H}}(G,\mathbf{C})^{\dagger,\mathrm{rd}}$ is given by a braid orbit, O, on the corresponding reduced Nielsen classes $\mathrm{Ni}(G,\mathbf{C})^{\dagger,\mathrm{rd}}$. Then, the ramification, respectively over $0,1,\infty$, of $\overline{\mathcal{H}'} \to \mathbb{P}^1_j$ corresponds to the disjoint cycles of $\gamma_0 = q_1q_2$, $\gamma_1 = q_1q_2q_1$, $\gamma_\infty = q_2$ acting on O.*

The genus, $g_{\overline{\mathcal{H}'}}$, of $\overline{\mathcal{H}}(G,\mathbf{C})^{\dagger,\mathrm{rd}}$, a la Riemann-Hurwitz, appears from

$$2(|O| + g_{\bar{\mathcal{H}}'} - 1) = \mathrm{ind}(\gamma_0)+\mathrm{ind}(\gamma_1)+\mathrm{ind}(\gamma_\infty).$$

We recast the proof of [**BFr02**, Thm. 2.9] on Thm. 2.14 combinatorial results on H_4 vs $\bar{M}_4 = H_4/\mathcal{Q}$ in §4.2.

THEOREM 2.14 (Cohomology result for Thm. 2.13).

(2.28a) *The only involution in H_4, $\tilde{z}^2 = (q_1q_3^{-1})^2$, generates its center.*

The quotient $H_4/\langle\tilde{z}^2\rangle$ is M_4.

(2.28b) *$\mathcal{Q} \triangleleft H_4$ with $\mathcal{Q}$ he quaternion group Q_8.*

(2.28c) *$H_4/\mathcal{Q} = \bar{M}_4 \cong \mathrm{PSL}_2(\mathbb{Z})$.*

(2.28d) *Exactly two conjugacy classes of H_4 subgroups $U_1 = \langle q_1, q_2\rangle$ and $U_2 = \langle q_2, q_3\rangle$ (both containing $\langle\tilde{z}\rangle$) are isomorphic to $\mathrm{SL}_2(\mathbb{Z})$.*

From (2.28b), *$\mathcal{Q}$ is the smallest normal subgroup of H_4 containing either $(q_1q_2q_3)^2$ or $q_1q_3^{-1}$. From the braid relation defining H_4 from B_4,* (2.26) *(see Rem. 2.12)*

$$\bar{M}_4 = \langle\gamma_0,\gamma_1\rangle = \langle\gamma_1,\gamma_\infty\rangle \text{ is } M_4 \text{ modulo the relation } q_1 = q_3.$$

3. sh-incidence on reduced Hurwitz spaces

This section gives a tool for treating in detail Hurwitz spaces of reduced Nielsen classes. Property number one for Hurwitz spaces is to detect their components. We give two geometrically interpretable tools for that: the practical **sh**-incidence matrix §3.1, and the theoretical *lift invariant* Ch. 3, which only appears if G has a nontrivial *Schur multiplier*.

We start here two of the main examples in the book. §3.2 has the **MT** description of modular curves (and their cusps). §3.3 does one example based on $G = A_4$, that we can use to reflect on the relation between the **RIGP** and the **OIT**. This relation arises in **MT**s, appearing in all our conjectures, starting with the Main Conjecture (3.1). Especially we use this example to illustrate Thm. 2.13 where the need to identify the braid orbits in the Nielsen class is immediate.

CONJECTURE 3.1 (Main **MT** Conjecture). For K a number field, at high levels there will be no K points on a **MT**.

Also, high levels will be algebraic varieties of general type (high powers of the canonical bundle embed the variety in projective space) [**Fr95**].

3.1. sh-incidence Algorithm. The **sh**-incidence matrix entwines the interaction of the braids and the group G, showing up in invariants of components of Hurwitz spaces by a labeling on cusps.

3.1.1. *Twist orbits.* Def. 3.2 gives us the most easily identified cusp orbits.

DEFINITION 3.2. An element $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ is a *Harbater-Mumford* (**HM**) representative if it has the form $(g_1, g_1^{-1}, \dots, g_s, g_s^{-1})$ (so $2s = r$). A braid orbit O is said to be **HM**, if the orbit contains an **HM** rep.

To initially address Conjecture (3.1), [**Fr95**] inspected the properties of the **MT** for $\mathrm{Ni}(A_5, \mathbf{C}_{3^4}), \ell = 2$ in sufficient detail that any fair observer could see there was something substantive happening in essentially any **MT**. The superficial similarity between that Nielsen class, with one braid orbit, and the A_4 example below (with two braid orbits), is belied by resulting large difference between the two of them. Both have braid orbits with **HM** reps.

Lem. 3.3, for all r, lists q_i orbits. Note though, one index i suffices for the **sh**-incidence matrix. For historical reasons we choose $i = 2$.

LEMMA 3.3. *Let $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ be a Nielsen class representative. With $\mu = g_i g_{i+1}$, the orbit of Q_i on $\boldsymbol{g}$ is the collection*

$$(\boldsymbol{g})q_i^k = \begin{cases} (g_1, \dots, g_{i-1}, \mu^l g_i \mu^{-l}, \mu^l g_{i+1} \mu^{-l}, g_{i+2}, \dots) & \text{for } k=2l \\ (g_1, \dots, g_{i-1}, \mu^l g_i g_{i+1} g_i^{-1} \mu^{-l}, \mu^l g_i \mu^{-l}, g_{i+2}, \dots) & \text{for } k=1+2l. \end{cases}$$

*If $r = 4$, and $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^\dagger$ is an **HM** rep. $(g_1, g_1^{-1}, g_2, g_2^{-1})$, then so are all elements in the $\mathcal{Q}''$ orbit of $\boldsymbol{g}$. Then, the $\mathcal{Q}''$ orbit length on $O_{\boldsymbol{g}}$ is $4/(m+1)$ with m*

the count of conjugacies, in † equivalence, given by

$$hg_1h^{-1} = g_2 \text{ or } g_1 = hg_2^{-1}h^{-1} \text{ with } h^2 = 1\text{; or } h(g_1, g_2)h^{-1} = (g_1^{-1}, g_2^{-1}).$$

If G (resp. $N_{S_n}(G, \mathbf{C})$) has no center (resp. element that centralizes G) for † = in (resp. abs*) then h is determined by these conditions.*

PROOF. The formula of the 1st paragraph comes from the definition of q_i. Similarly, if you apply $q_1q_3^{-1}$ or $\mathbf{sh}^2$ to an **HM** rep, then it is immediate the result is another **HM** rep.

Now consider the $\mathcal{Q}''$ orbit length, which is 4 divided by the number of elements $q \in \mathcal{Q}''$ for which $(\boldsymbol{g})q = h\boldsymbol{g}h^{-1}$ for some $h \in G$ (resp. $h \in N_{S_n}(G, \mathbf{C})$ if † = in (resp. † = abs). The cases are similar, so we will just do the 1st.

If $h^2 = 1$ for which $g_1 = hg_2h^{-1}$, then $g_1^{-1} = hg_2^{-1}h^{-1}$ and

$$h((\boldsymbol{g})\mathbf{sh}^2)h^{-1} = h(g_2, g_2^{-1}, g_1, g_1^{-1})h^{-1} = \boldsymbol{g}.$$

If h_1, h_2 both satisfied these conditions then $h_1h_2^{-1}$ would commute with $\boldsymbol{g}$, contrary to the centralizing assumption. Either one or all three of those conditions are satisfied. Add that number to 1 (for the trivial element in $\mathcal{Q}''$) to get m. □

REMARK 3.4. General expectation from Lem. 3.3 is that Q_2 orbits would have length $2 \cdot \text{ord}(g_ig_{i+1}) \stackrel{\text{def}}{=} 2o$. There is an important exception – Ch. 6 Prop. 2.1 – for which the orbit length (even without concerns about centralizers) is half that expectation. The first condition is that o is odd. It applies to §3.2 and to the cusp labeled ${}_cO^3_{1,3}$ in the Ni_0^+ block of 2.

3.1.2. *Listing cusps for the sh-incidence matrix.* Def. 3.5, the **sh**-incidence matrix, is invaluable to compute braid orbits on specific reduced Nielsen classes.

For, S, a set of representatives in $\text{Ni}(G, \mathbf{C})$ and any equivalence relation $\bullet$ on the Nielsen class, denote by $S^{q_2,\bullet}$ (resp. $S^{\mathbf{sh},\bullet}$) the collection of $\bullet$ equivalence classes of q_2 (resp. **sh**) orbits.

We have been using O for braid orbits on a Nielsen class. For q_2 (cusp) orbits the notation will be ${}_cO$, with the understanding that $\bullet$-equivalence has been specified.

If $r = 4$ and $\bullet$ is one of the reduced equivalences, then **sh** has order 2, thereby producing a symmetric matrix.

DEFINITION 3.5. List $\bullet$-equivalence classes, ${}_cO_1, \ldots, {}_cO_u$, of q_2 (*cusp*) orbits. The **sh**-incidence matrix $A(G, \mathbf{C})$ has (i, j) term $|(O_i)\mathbf{sh} \cap O_j|$.

Denote the transpose of an $n \times n$ matrix by ${}^{\text{tr}}T$. Equivalence $n \times n$ matrices A and $TA^{\text{tr}}T$ running over permutation matrices T associated to elements of S_n. Refer to a matrix A as in *block form* if there are matrices $B_1, \ldots, B_u$, for which A has the form of a $u \times u$ diagonal matrix with diagonal entries $B_1, \ldots, B_u$. The proof of Lem. 3.6 is an algorithm. Rem. 3.8 and Rem. 3.10 have extra comments.

LEMMA 3.6. *For some T, $A(G,\mathbf{C})$ is in block form with the block rows (and columns) labeled by cusp orbits whose union of elements consists of a single braid orbit on* $\mathrm{Ni}(G,\mathbf{C})$ *under $\bullet$-equivalence.*

PROOF. Start with any q_2 orbit and label it ${}_cO_{1,1}$. Then form the sequence

$$ {}_cO_{1,1} \to ({}_cO_{1,1}^{\mathbf{sh},\bullet})^{q_2,\bullet} \to (((({}_cO_{1,1}^{\mathbf{sh},\bullet})^{q_2,\bullet})^{\mathbf{sh},\bullet})^{q_2,\bullet}\dots \tag{2.29}$$

until the sequence stops. The result will be a union of distinct q_2 orbits under $\bullet$-equivalence.

Denote this collection by ${}_c\mathcal{O}_1 = \{{}_cO_{1,1},\dots,{}_cO_{1,b_1}\}$. Since $H_r = \langle q_2, \mathbf{sh}\rangle$, together ${}_c\mathcal{O}_1$ contains all elements – modulo $\bullet$-equivalence – in the Nielsen class that are in the H_r orbit of any element of ${}_cO_{1,1}$.

Label the rows and columns of the first block of your matrix, B_1, by the elements of ${}_c\mathcal{O}_1$. In step 1 of (2.29) you iterate applications of $\mathbf{sh}$ on ${}_cO_{1,1}$ and check for all new q_2 orbits. The (i,j)-entry is $|({}_cO_{1,i})\mathbf{sh}\cap {}_cO_{1,j}|$. Call ${}_cO_i$ and ${}_cO_j$ *neighbors* if $|({}_cO_{1,i})\mathbf{sh}^t\cap {}_cO_{1,j}|$ is nonzero for some t. If the process stops after one step, then all q_2 orbits are neighbors of ${}_cO_{1,1}$. In step 2 you do the same thing to any of the new q_2 orbits, etc., until you stop getting new q_2 orbits. The resulting **sh**-incidence matrix is obtained from a maximal sequence of neighbors.

Therefore, this gives exactly one block, B_1 as described in the opening paragraph of the lemma. If further q_2 orbits in the Nielsen class haven't been used, then start again until you have used them all. Eventually you get blocks $B_1,\dots,B_u$ corresponding to unions of q_2 orbits ${}_c\mathcal{O}_1,\dots,{}_c\mathcal{O}_u$. □

3.1.3. *$r = 4$ and finishing the computation.*

LEMMA 3.7. *Now assume $r = 4$, and $\bullet$-equivalence is one of the reduced equivalences, so q_2 orbits are γ_∞ orbits. Then the sh-incidence matrix is symmetric.*

Replacing $\mathbf{sh}$ *by either γ_0 or γ_1 acting on γ_∞ orbits gives the same blocks in the resulting matrix. Then, fixed points of γ_j, $j = 0$ or 1, on any $\bar{M}_4$ orbit give nonzero entries along the diagonal of the corresponding block. Then,*

$$|({}_cO_{1,t})\mathbf{sh}\cap {}_cO_{1,t'}| = |({}_cO_{1,t})\mathbf{sh}^2\cap ({}_cO_{1,t'})\mathbf{sh}| = |{}_cO_{1,t}\cap ({}_cO_{1,t'})\mathbf{sh}|.$$

That shows the final matrix in block form, has each block symmetric.

PROOF. Take $r = 4$ and for $\bullet$-equivalence one of the reduced equivalences, where $\mathbf{sh}^2$ is the identity on braid orbits.

Use that on reduced classes $q_1 = q_3$, with relation (2.13), $q_1q_2q_1 = q_2q_1q_2$. Now consider what happens if we replace $\mathbf{sh}$ by γ_1 represented by q_1q_2. Since we start with a q_2 orbit, say ${}_cO$, the collection with $\mathbf{sh}$ applied is given by

$$({}_cO)\mathbf{sh} = ({}_cO)q_1q_2q_1 = ({}_cO)q_2q_1q_2 = ({}_cO)q_1q_2.$$

That shows the matrix is the same with γ_0 replacing **sh**. Of course, γ_1 is **sh**. That finishes the proof of the lemma. □

REMARK 3.8 (The algorithm-Part 1). Regard the sequence of expression (2.29) as iterated steps – it shows two steps – in computing one braid orbit on the $\bullet$-equivalence classes on $\mathrm{Ni}(G, \mathbf{C})$. Our examples often have one step.

Notice in our $\mathrm{Ni}(A_4, \mathbf{C}_{+3^2-3^2})$ example §3.3, the seed for each braid orbit – respectively an **HM** rep. Def. 3.2, and a **D**(ouble)**I**(dentity) rep. – end up giving their Hurwitz space components corresponding monikers.

It makes sense to list q_2 orbits, referring to the blocks, as

$$ {}_{\mathrm{c}}O_{1,1}^{w_{1,1}}, \dots, {}_{\mathrm{c}}O_{1,b_1}^{w_{1,b_1}}, {}_{\mathrm{c}}O_{2,1}^{w_{2,1}}, \dots, {}_{\mathrm{c}}O_{2,b_1}^{w_{2,b_2}}, \dots, {}_{\mathrm{c}}O_{u,1}^{w_{u,1}}, \dots {}_{\mathrm{c}}O_{u,b_u}^{w_{u,b_u}}, $$

with the superscript $w_{i,j}$ the cusp width (cusp orbit length). Still, should there be more than one step, labeling within any one block probably should correspond to the step in which it appears. Especially if the seed orbit has been chosen well.

LEMMA 3.9. *For $r = 4$, in the ith block of the* **sh**-*incidence matrix, we can read off the degree of the component $\bar{\mathcal{H}}_i$ over $\mathbb{P}^1_j$ as $\sum_{j=1}^{b_i} w_{i,j}$. Further,*

$$ w_{i,j} = \sum_{k=1}^{b_i} |({}_cO_{i,j})\mathbf{sh} \cap \mathcal{O}_{i,k}|, j = 1, \dots, b_i. $$

PROOF. This follows by recognizing the cusps as the q_2 orbits on the ith braid orbit of the Nielsen classes under reduced equivalence. This is a piece of the proof of Thm. 2.7. The rest is from the combinatorics of the **sh**-incidence matrix. □

REMARK 3.10 (The algorithm-Part 2). Fixed points of γ_0 or γ_1 on a reduced orbit imply that the reduced Hurwitz space component does not have fine moduli. We can almost read that data off directly from the **sh**-incidence matrix. If there are no nonzero diagonal elements corresponding to that block in Lem. 3.6, then for certain γ_0 or γ_1 have no fixed point, and then the only test necessary for fine moduli is that $\mathcal{Q}''$ acts on that orbit as a Klein 4-group.

Yet, if there diagonal elements aren't all 0, there may, or not, be γ_0 or γ_1 fixed points. Both cases occur in the $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})$ §3.3. That illustrates many part 3 topics of the book. Before that, though, §3.2 returns to modular curves.

3.2. Dihedral Ex. 2.7 continued. We lay out – extending [**Fr78**, §2] – the cusps on the one braid orbit on $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4}) \stackrel{\mathrm{def}}{=} \mathrm{Ni}_k$.

3.2.1. *Listing the cusps for* $\mathrm{Ni}_k^{\mathrm{in}}$. For a given $\boldsymbol{g} \in \mathrm{Ni}_k^{\mathrm{in}}$, conjugate by $\left(\begin{smallmatrix} 1 & a_1/2 \\ 0 & 1 \end{smallmatrix}\right)$ to assume $g_1 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For $\boldsymbol{g} \in \mathrm{Ni}_k^{\mathrm{abs}}$, conjugate by $\left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $\alpha \in (\mathbb{Z}/\ell^{k+1})^*$ to assume $a_2 - a_3 = \ell^u, u \geq 0$:

$$ \left(\begin{smallmatrix} \alpha & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & a' \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & \alpha a' \\ 0 & 1 \end{smallmatrix}\right). \tag{2.30} $$

(2.31a) Show conjugating by $H_u = \{\alpha \equiv 1 \bmod \ell^{k+1-u}\}$ in (2.30) has no effect on $a_2 - a_3$.

(2.31b) $(a_2, a_3) = (1,1)$ (resp. $(0,1)$) gives a length 1 (resp. ℓ^{k+1}) q_2 orbit on $\mathrm{Ni}_k^{\mathrm{abs,rd}}$, an example of Rem. 3.4.

(2.31c) With $a_2 - a_3 = \ell^u$, $1 \le u \le k$, follow the steps of Prop. 3.11 to count q_2 orbits (cusps), and their widths, on $\mathrm{Ni}_k^{\mathrm{abs,rd}}$.

(2.31d) Use (2.31b) to show Table 1 is the **sh**-incidence matrix for $\mathrm{Ni}_k^{\mathrm{abs,rd}}$. Conclude: $|\mathrm{Ni}_k^{\mathrm{abs,rd}}| = |\mathrm{Ni}_k^{\mathrm{abs}}|$: $\mathcal{Q}''$ action is trivial.

(2.31e) Modify (2.31d) to $\mathrm{Ni}_k^{\mathrm{in,rd}}$: that $|\mathrm{Ni}_k^{\mathrm{in,rd}}| = |\mathrm{Ni}_k^{\mathrm{in}}|$ and we can braid (Rem. 3.9) all the outer automorphisms from $(\mathbb{Z}/\ell^{k+1})^*/\langle \pm 1\rangle$.

Hint for (2.31d): From Table 1 – one component of the **sh**-incidence matrix – you need only test the action of $\mathcal{Q}''$ on an **HM** rep.

Hint for (2.31e): See what happens with the **HM** rep. in (2.31b).

3.2.2. **sh**-*incidence for* $\mathrm{Ni}_k^{\mathrm{abs,rd}}$. Continue notation for (2.31c).

PROPOSITION 3.11. *For $u > 0$, $\langle \boldsymbol{g} \rangle = D_{\ell^{k+1}}$ implies $(a_2, \ell) = 1$. Conjugating by H_u assures ${}_cO_{\boldsymbol{g}}$ has Nielsen class reps. with distinct 2nd entries, $a_2 + m\ell^u \bmod \ell^{k+1-u}$. Denote $(\mathbb{Z}/\ell^{k+1-u})^*$ mod (additive) translate by ℓ^u by $L^{*,+}_{k+1,\ell^u}$.*

Let ${}_u\boldsymbol{g}$ have $a_2 = 1$ and $a_3 = 1 - \ell^u$. Use:

$$({}_u\boldsymbol{g})q_2^l \text{ corresponds to the pair } (a_2, a_3) = (1 + l\ell^u, 1 + (l-1)\ell^u). \tag{2.32}$$

Consider the subgroup $S_u \le H_u$ stabilizing (2.32). Then, $|S_u| = \ell^{\min(u,k+1-u)}$.

This gives a q_2 orbit of length $\ell^{k+1-u}/\ell^{\min(u,k+1-u)}$. Each u, $1 \le u \le k$ contributes $\varphi(\ell^u)/|H_u|$ orbits of q_2 of this length.

(2.33a) *Cusps corresponding to u are ${}_cO_{\ell^{k+1-2u},a}$, $a \in L^{*,+}_{k+1,\ell^u}$.*

(2.33b) *For $0 \le u \le \frac{k-1}{2}$, cusps have widths $k+1-2u$; and*

(2.33c) *for $0 \le \frac{k+1}{2} \le u \le k+1$, cusp have width 1.*

TABLE 1. **sh**-incidence for $\mathrm{Ni}(D_{p^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs,rd}}$ listings for ${}_cO_{\ell^{k+1-2u},a}$

Cusp orbit	$u = 0$	$a \in L^{*,+}_{k+1,\ell^u}$, $1 \le u \le [\frac{k+1}{2}]$	$a \in L^{*,+}_{k+1,\ell^u}$, $[\frac{k+3}{2}] \le u \le k+1$
$u = 0$	$\ell^{k+1} - \ell^k$	ℓ^{k+1-2u}	1
$a \in L^{*,+}_{k+1,\ell^u}$, $1 \le u \le \frac{k+1}{2}$	ℓ^{k+1-2u}	0	0
$a \in L^{*,+}_{k+1,\ell^u}$, $\frac{k+3}{2} \le u \le k+1$	1	0	0

REMARK 3.12. [**Sh94**, p. 25] has the traditional way to compute $X_0(\ell^{k+1})$ cusp data. Note: In (2.31b), an **HM** *rep.* (from $(a_2, a_3) = (0,1)$) gives the longest q_2 orbit. Its shift gives the shortest q_2 orbit.

REMARK 3.13. Above, $\mathcal{Q}''$ acts trivially on inner (and so absolute) Nielsen classes. As these Nielsen classes have modular curves as their reduced spaces, maybe that is why $\mathcal{Q}''$ has not appeared in studies of modular curves. Still, failure of b-fine moduli (as in (2.25)) for both is the same: a Klein 4-group in $\mathrm{PSL}(\mathbb{C})$ stabilizes any four distinct points on $\mathbb{P}^1_z$ as in Thm. 2.7 (especially its proof Ch. 6 §4.1).

3.3. sh-incidence on $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$. We now look at level $k = 0$ for $\ell = 2$ of Ch. 5 (which illustrates generalizing Serre's **OIT**). Let α act on $(\mathbb{Z})^2$ as $\left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix}\right)$ (of order 3). Take the induced action on $(\mathbb{Z}/2)^2$, and regard α as a generator of $\mathbb{Z}/3$, as a multiplicative group. Then,

$$A_4 = (\mathbb{Z}/2)^2 \times^s \mathbb{Z}/3 = \left\{ \left(\begin{smallmatrix} \alpha^j & (x,y) \\ 0 & 1 \end{smallmatrix}\right) \right\} \mid j \in \mathbb{Z}/3, (x,y) \in (\mathbb{Z}/2)^2 \Big\}, \tag{2.34}$$

as in the semi-direct product (left action of α) notation of Ch. 1 Def. 1.6. In that general case, we will be using this matrix notation with $\alpha_0 = \left(\begin{smallmatrix} \alpha & \mathbf{0} \\ 0 & 1 \end{smallmatrix}\right)$.

In, however, §3.3.1, we use permutation notation (right action on {1,2,3,4}), with $\alpha_0 = (1\,2\,3) \in A_4$ the special representative of α. We also have $A_4 \le A_5$, used below, as in Lem. 3.14.[2]

3.3.1. *Describing elements in a particular Nielsen class.* The Nielsen class we want is $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$, where C_{+3} (resp. C_{-3}) is the class of α (resp. α^{-1}) and $\mathbf{C}_{\pm 3^2}$ means the collection repeats each class twice. Therefore, it is a rational union of conjugacy classes. So, it defines Hurwitz spaces over $\mathbb{Q}$ from the **BCL** (Lem. 4.1). Here is what to excect of the example.

(2.35a) The reduced Hurwitz space has two components, labeled $\mathcal{H}_0^{\pm}$, from braid orbits $\mathrm{Ni}_0^{\pm}$ appearing from the **sh**-incidence matrix.

(2.35b) Both Hurwitz space components have fine moduli. The reduced space $\mathcal{H}_0^{+}$ has fine *reduced* moduli (§2.2.3), while $\mathcal{H}_0^{-}$ does not.

(2.35c) The genuses of both $\bar{\mathcal{H}}_0^{\pm}$ are 0.

(2.35d) Neither component is a modular curve, but we can compute their arithmetic and geometric monodromy as j-line covers.

Comment on (2.35b)*:* Fine moduli for inner Hurwitz spaces in this case comes from A_4 having no center Ch. 1 Lem. 2.3. The check for *reduced* fine moduli on a braid orbit O for has two steps [**BFr02**, §4.3.1]: (2.25a), $\mathcal{Q}''$ acts as a Klein 4-group; and (2.25b), neither γ_0 nor γ_1 has fixed points (on O).

Comment on (2.35c)*:* To conclude Main **MT** conj. 3.1 for this **MT** requires going to higher levels to assure component genuses rise beyond 1. Each component has

[2]In Serre's **OIT** the primes $\ell = 2$ and 3 have slightly different behavior than the other primes. That happens, too, in our example. In both, we uniformly compare these with the *lift invariant* and the concept *eventually* ℓ-Frattini.

2-cusps (respectively labeled ${}_cO^4_{1,1}$ and ${}_cO^4_{2,1}$ Table 2. So, it requires more work to establish the explicit rise of genus, but this is the crucial hypothesis of [**Fr06**, §5].

Comment on (2.35d)*:* In Prop. 3.16 we see there is a natural one-one map from $\mathcal{H}_0^{+,\mathrm{in}}$ to $\mathcal{H}_0^{+,\mathrm{abs}}$, though as moduli spaces they are very different, a difference far less subtle than that referred to in Rem. 3.13 as it involves the very large difference between the jacobians of the curves in their respective moduli [**BFr02**, §E.2.2], which we revisit in §1.1.1.

List possible parity sequences from $\mathrm{C}_{\pm 3}$ in $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$:

[1] +-+- [2] ++-- [3] +--+
[4] -+-+ [5] --++ [6] -++-

These are useful observations.

(2.36a) By applying $q \in \mathcal{Q}''$, assume that a reduced representative of an orbit has (1 2 3) as its first entry: Is in $\{[1],[2],[3]\}$.

(2.36b) To check if $(i\,j\,k)$ should be a + or −, conjugate by any $g \in S_4$ that takes it to (1 2 3) and check if g has + or - parity.

3.3.2. *Cusps and the* **sh**-*incidence matrix.* Again, list cusps as ${}_cO^k_{i,j}$: k is the cusp width, and i, j as in Rem. 3.8, corresponds to a labeling of orbit representatives. The following elements are in a Harbater-Mumford component (3.2).

$$\begin{aligned} \textbf{HM} \text{ rep. for } {}_cO^4_{1,1}\text{: } \boldsymbol{g}_{1,1} &= ((1\,2\,3),(1\,3\,2),(1\,3\,4),(1\,4\,3)) \\ \textbf{HM} \text{ rep. for } {}_cO^3_{1,3}\text{: } \boldsymbol{g}_{1,3} &= ((1\,2\,3),(1\,3\,2),(1\,4\,3),(1\,3\,4)) \\ \textbf{sh} \text{ of } \textbf{HM} \text{ rep. for } {}_cO^2_{1,2}\text{: } \boldsymbol{g}_{1,2} &= ((1\,2\,3),(1\,2\,4),(1\,4\,2),(1\,3\,2)). \end{aligned}$$

Consider $g_{2,1} = ((1\,2\,3),(1\,3\,4),(1\,2\,4),(1\,2\,4)) \in [2]$. Its γ_∞ orbit ${}_cO^4_{2,1}$ is what §3.1.2 calls **D**(ouble)**I**(dentity): named for repeated entries in $g_{2,1}$ (positions 3 and 4). The same for the seed of the **DI** cusps ${}_cO^1_{2,2}$ and ${}_cO^1_{2,3}$ (positions 2 and 3).

In Table 2, each cusp orbit has an element with entries (g, g^{-1}) or with entries (g, g): the former in braid orbit Ni_0^+, the latter in braid orbit Ni_0^-.

TABLE 2. The two **sh**-incidence blocks on $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$.

Ni_0^+ Orbit	${}_cO^4_{1,1}$	${}_cO^2_{1,2}$	${}_cO^3_{1,3}$
${}_cO^4_{1,1}$	1	1	2
${}_cO^2_{1,2}$	1	0	1
${}_cO^3_{1,3}$	2	1	0

Ni_0^- Orbit	${}_cO^4_{2,1}$	${}_cO^1_{2,2}$	${}_cO^1_{2,3}$
${}_cO^4_{2,1}$	2	1	1
${}_cO^1_{2,2}$	1	0	0
${}_cO^1_{2,3}$	1	0	0

Prop. 3.16 explains the two blocks – each one step (of (2.29)) – of the **sh**-incidence matrix on $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$. This is our first use of the *lift invariant*. We need the Frattini central extension of A_4, for which the following is convenient:

(2.37) Pullback of $A_4 \le A_5$ to $\mathrm{SL}_2(\mathbb{Z}/5) \to \mathrm{PSL}_2(\mathbb{Z}/5) = A_5$.

For $g \in \mathrm{C}_{\pm 3}$, $\hat{g}$ is the (unique) order 3 lift to $\psi : \hat{A}_4 \to A_4$, for the cover in (2.37). This is a case (for $r = 4$) of Def. 1.4 where we are computing

> The restricted lift invariant relative to ψ of the $O_{\boldsymbol{g}}$ braid orbit of $\boldsymbol{g}$:
> $s_\psi(\boldsymbol{g}) \stackrel{\text{def}}{=} s_\psi(O) = \prod_{i=1}^r \hat{g}_i \stackrel{\text{def}}{=} \prod(\hat{\boldsymbol{g}})$ running over braid components.

3.3.3. *Preliminary on the lift invariant.* Regard $\ker(\psi)$ as $\{\pm 1\}$. If $s_\psi(O_{\boldsymbol{g}}) = +1$, we say it has trivial lift invariant. To compute $s_\psi(O)$, we will compare $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})$ with an auxiliary Nielsen class, $\mathrm{Ni}(A_4, \mathbf{C}_{+3^3})$: 3 repeats of the class C_+. Note: $\mathbf{C}_{+3^3}$ is not a $\mathbb{Q}$ rational union: $\mathrm{C}_{+3}^{-1} = \mathrm{C}_{-3}$.

LEMMA 3.14. *If $\boldsymbol{g} \in \mathrm{Ni}(A_4, \mathbf{C}_{\pm \mathrm{C}^2})$) is an* **HM** *rep., then $s_\psi(O_{\boldsymbol{g}}) = +1$.*

There is a lift invariant preserving correspondence between

$$\begin{aligned} \boldsymbol{g}' = &\quad (g_1', g_2', g_3') \in \mathrm{Ni}(A_4, \mathbf{C}_{+3^3}) \text{ and } \mathbf{DI} \text{ reps.} \\ {}_{1,4}\boldsymbol{g} = &\quad ((g_1')^{-1}, g_2', g_3', (g_1')^{-1}) \in \mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2}). \end{aligned}$$

Then, $s_\psi(O_{\boldsymbol{g}'}) = s_\psi(O_{{}_{1,4}\boldsymbol{g}}) = -1$ and $O_{{}_{1,4}\boldsymbol{g}}$ contains no **HM** *reps.*

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

$${}_{1,2}\boldsymbol{g} = ((g_2')^{-1}, (g_2')^{-1}, g_3', g_1') \text{ or } ({}_{1,3}\boldsymbol{g})q_2^{-1} = ((g_2')^{-1}, (g_2')^{-1} g_3' g_2', (g_2')^{-1}, q_1'),$$

or other variants placing the doubled pair wherever we want.

PROOF. Assume generation, $\langle g_1, g_3 \rangle = A_4$, for $\boldsymbol{g} = (g_1, g_1^{-1}, g_3, g_3^{-1}) \in \mathbf{C}_{\pm 3^2}$. 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 for any **HM** rep.

Now consider $\boldsymbol{g}' = (g_1', g_2', g_3') \in \mathrm{Ni}(G_\ell, \mathbf{C}_{3^3})$. In place of g_3' put

$$((g_3')^{-1}, (g_3')^{-1}) \text{ for the reversible correspondence in the Lemma.}$$

Since $\hat{g}_1$ has order 3, $\hat{g}_1^{-1}\hat{g}_1^{-1} = \hat{g}_1$ is the unique order 3 in $\hat{A}_4$ over g_1 (easy Schur Zassenhaus). So, $s_\psi(\hat{\boldsymbol{g}}') = \hat{g}_1'\hat{g}_2'\hat{g}_3' \in \ker(\psi)$ is the same as

$$(\hat{g}_1')^{-1}\hat{g}_2'(\hat{g}_3')^{-1}(\hat{g}_1')^{-1} = s_\psi({}_{1,4}\boldsymbol{g}).$$

Now we list two different ways to prove this is -1.

(2.38a) *Direct computation*: Find α_1 of order 3 in $\mathrm{SL}_2(\mathbb{Z}/5)$ over (1 2 3). Then, find a conjugate, α_2, of α_1 over (1 3 4) (see Rem. 3.15).

(2.38b) *Fried-Serre formula*: Use that covers in $\mathrm{Ni}(A_4, \mathbf{C}_{+3^3})^{\mathrm{abs}}$ have genus 0. So the lift invariant is $(-1)^3$ (as in Ex. 2.10).

Notice there is no problem with the variants on the **DI** elements; we can braid between them as we did between ${}_{1,2}\boldsymbol{g}$ and ${}_{1,3}\boldsymbol{g}$ in the statement of the lemma. □

REMARK 3.15 (More on s_ψ in Lem. 3.14). Hint on (2.38a): Compute $\alpha_1\alpha_2$ and check its order (it should be 6). Here, where $\ell = 2$, the 2-Sylow in $\hat{A}_4$ is the quaternion group Q_8, not the small Heisenberg group (whose elements for $\ell = 2$ all have order 2) giving the lift invariant in the other cases of Ch. 5 §3 for $\ell > 3$.

3.3.4. *Properties of both H_4 orbits on* $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$). Prop. 3.16 has separated the **HM** and **DI** components, using the notation $\mathcal{H}_0^+$ and $\mathcal{H}_0^-$ for the braid orbits that contain the corresponding cusp types. We treat each separately after stating Prop. 3.16 by referring to the **HM** cusps and the **DI** cusps.

PROPOSITION 3.16. *On* $\mathrm{Ni}(\hat{A}_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$ *(resp.* $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$*) $H_4/\mathcal{Q}''$ has one (resp. two) orbit(s). So, $\mathcal{H}(\hat{A}_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$ (resp. $\mathcal{H}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$) has one (resp. two) component(s), $\hat{\mathcal{H}}_0^+$ (resp. $\mathcal{H}_0^{\pm}$).*

Conclusions on the inner reduced space $\mathcal{H}_0^+ = \mathcal{H}_0^{+,\mathrm{in,rd}}$:

(2.39a) *$\bar{\mathcal{H}}_0^{+,\mathrm{in,rd}} \to \mathbb{P}^1_j$ has degree 9, the space has genus 0, and there are cusps of width 4, 3 and 2 (over ∞).*

(2.39b) *$\Phi^{\mathrm{in,rd}}_{\mathrm{abs,rd}} : \mathcal{H}_0^{+,\mathrm{in,rd}} \to \mathcal{H}_0^{+,\mathrm{abs,rd}}$ is one-one, though the former (resp. latter) is moduli of genus 5 (resp. genus 1) covers.*

(2.39c) *$\mathcal{H}(\hat{A}_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$ maps one-one to $\mathcal{H}_0^+$ (despite the spaces having different moduli).*

(2.39d) *$\mathcal{H}_0^{+,\mathrm{in,rd}}$ fails both tests in* (2.25) *for reduced fine moduli.*

Conclusions on the inner reduced space $\mathcal{H}_0^- = \mathcal{H}_0^{-,\mathrm{in,rd}}$:

(2.40a) *$\bar{\mathcal{H}}_0^{-,\mathrm{in,rd}} \to \mathbb{P}^1_j$ has degree 6, the space has genus 0, and there are 2 cusps of width 1 and one of width 4 (over ∞).*

(2.40b) *$\Phi^{\mathrm{in,rd}}_{\mathrm{abs,rd}} : \mathcal{H}_0^{-,\mathrm{in,rd}} \to \mathcal{H}_0^{-,\mathrm{abs,rd}}$ is two-one.*

(2.40c) *There is nothing on $\mathcal{H}(\hat{A}_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$ over $\mathcal{H}_0^-$.*

(2.40d) *$\mathcal{H}_0^{-,\mathrm{in,rd}}$ fails the b-fine moduli test in* (2.25) *but neither γ_0 or γ_1 have fixed points.*

HM *cusps:* First consider the braid orbit containing all **HM** reps. All 3-cycles in A_4 are conjugate in S_4. Thus, for inner equivalence, assume an **HM** rep. is

$$\boldsymbol{g}_1 = ((1\,2\,3), (1\,3\,2), g, g^{-1}) \text{ or } \boldsymbol{g}_2 = ((1\,3\,2), (1\,2\,3), g', (g')^{-1}).$$

Appying $q_1 q_3^{-1}$ shows $\boldsymbol{g}_1$ is correct up to reduced equivalence. Since g must contain 4, after conjugation by $(1\,2\,3)$ (inner equivalence) it is $(1\,u\,4)$ with $u = 2$ or 3.

So, there are just two reduced inequivalent **HM** reps. whose orbits are represented by $\boldsymbol{g}_{1,1}$ and $\boldsymbol{g}_{1,3}$. Conjugate by $(1\,3)(2\,4)$, as in Lem. 3.3, to see $\mathbf{sh}^2$ fixes $\boldsymbol{g}_{1,1}$, and the $\bar{M}_4$ orbit does not have b-fine reduced moduli.

Here are representatives of the inner reduced q_2 orbits (Lem. 3.3) on the three representatives in **HM** braid orbits we have already selected above Table 2 in the form $((1\,2\,3), \bullet, \bullet, \bullet)$. The display indicates the $\bullet$s in the 2nd and 3rd positions (with the 4th determined by product-one).

${}_{\mathrm{c}}O^4_{1,1} : \boldsymbol{g}_{1,1} = ((1\,3\,2), (1\,3\,4)), ((1\,4\,2), (1\,3\,2)), ((4\,2\,3), (4\,2\,1)), ((4\,1\,3), (4\,2\,3))$
${}_{\mathrm{c}}O^2_{1,2} : \boldsymbol{g}_{1,2} = ((1\,2\,4), (1\,4\,2)), ((1\,4\,2), (1\,2\,4))$
${}_{\mathrm{c}}O^3_{1,3} : \boldsymbol{g}_{1,3} = ((1\,3\,2), (1\,4\,3)), ((2\,4\,1), (1\,3\,2)), ((1\,4\,3), (1\,2\,4))$

We show these representatives give the three q_2 orbits in one (inner) reduced braid orbit, and the Ni^+ block is their **sh**-incidence matrix. Notation for the elements in a q_2 orbit is helpful. For example, starting with $\boldsymbol{g}_{1,1}$ iterates of q_2 on it (Lem. 3.3) give ${}_j\boldsymbol{g}_{1,1}$, $j = 0, 1, 2, 3$ indicating the power of the iterate. With that, connect $cO^2_{1,2}$ and the other two orbits by

$$\begin{aligned}({}_0\boldsymbol{g}_{1,2})\mathbf{sh} &= ((1\,2\,4), (1\,4\,2), (1\,3\,2), (1\,2\,3))\xrightarrow{\mu}\ {}_0\boldsymbol{g}_{1,1}\\ ({}_1\boldsymbol{g}_{1,2})\mathbf{sh} &= ((1\,4\,2)(1\,2\,4), (1\,3\,2), (1\,2\,3))\xrightarrow{\mu'}\ {}_0\boldsymbol{g}_{1,3}.\end{aligned}$$

with μ (resp. μ') given by $q_1q_3^{-1}$ followed by conjugation by $(1\,4)(2\,3)$ (resp. $(3\,2\,1)$). That shows the only possible entries in the 2nd row (and column) of Ni^+_0.

Now look at the entries for $({}_cO^3_{1,3})\mathbf{sh} \cap {}_cO^4_{1,1}$ with $\mu^* = \mathbf{sh}^2q_1^{-1}q_3$:

$$\begin{aligned}({}_1\boldsymbol{g}_{1,3})\mathbf{sh} = &\quad ((2\,4\,1), (1\,3\,2), (1\,3\,4), (1\,2\,3))\xrightarrow{\mu^*}\ {}_1\boldsymbol{g}_{1,1}\\ ({}_2\boldsymbol{g}_{1,3})\mathbf{sh} = &\quad ((1\,4\,3), (1\,2\,4), (1\,3\,4), (1\,2\,3))\xrightarrow{\mu^*}\ {}_2\boldsymbol{g}_{1,1}.\end{aligned}$$

That leaves ${}_3\boldsymbol{g}_{1,1}$ as the only point whose shift is unaccounted, implying it is fixed by γ_1, the shift. That concludes describing the component denoted Ni^+_0.

We read off the cusp widths and sum them for the total degree of the compactified space over $\mathbb{P}^1_j$, thus concluding $\bar{\mathcal{H}}^+$ has degree 9 over $\mathbb{P}^1_j$. From Thm. 2.13, Ex. 3.17 computes from the **sh**-incidence matrix the component genus as 0.

It also shows (2.39d): Ni^+_0 fails both conditions in (2.25) for fine reduced moduli. Since $\mathbf{sh}^2q_1q_3^{-1}$ takes $\boldsymbol{g}_{1,1}$ to $((1\,4\,3), (1\,3\,4), (1\,3\,2), (1\,2\,3))$ which is conjugate to $\boldsymbol{g}_{1,1}$ by $(2\,4)$, two distinct inner **HM** reps are equivalenced by $\mathcal{Q}''$.

This is exactly why $\Phi^{\mathrm{in,abs}}$ has degree 2: from $N_{S_4}(A_4, \mathbf{C}_{\pm 3})/A_4 = \mathbb{Z}/2$ as in Prop. 3.1 and especially in (1.38).

Yet, the reduced version of the map is one-one, concluding (2.39b). It is a simple matter to compute the genuses of the covers in the resp. inner and absolute classes. Refer to the genus for the former as $\mathbf{g}_{A_4,\mathrm{in}}$ and the latter as $\mathbf{g}_{A_4,\mathrm{abs}}$ from the formulas

$$\begin{aligned}2(12+\mathbf{g}_{A_4,\mathrm{in}} - 1) = 4\cdot 4\cdot 2, \mathbf{g}_{A_4,\mathrm{in}} = 5\ \text{vs}\\ 2(4+\mathbf{g}_{A_4,\mathrm{abs}}-1) = 4\cdot 2, \mathbf{g}_{A_4,\mathrm{abs}} = 1.\end{aligned}$$

Lem. 3.14 shows (2.39c) and (2.40c) together once we know Ni^-_0 is the single braid orbit containing all **DI** cusps, which we show below.

DI *cusps:* Now I go to the **DI** orbit to check elements fixed by $\mathcal{Q}''$. We can do what we did above with the **HM** cusps, to assume for, say, (g_1, g_2, g, g) that g is either $(1\,2\,4)$ or $(1\,2\,3)$. We also see clearly representatives of the two width one **DI** orbits by putting $((1\,2\,4), (1\,2\,4))$ and $((1\,2\,3), (1\,2\,3))$ in the 2nd and 3rd positions.

Now we show how quickly we find the full braid orbit in one (2.29) step by forming $\boldsymbol{g}_{2,1}^{q_2;\bullet}$ in the first column (with $\boldsymbol{g}_{2,1}$ at the top), and then, in turn, **sh** to each term to get the second column.

$$\begin{aligned}\boldsymbol{g}_{2,1} &= ((1\,2\,3), (1\,3\,4), (1\,2\,4), (1\,2\,4))\,\mathbf{sh}\to \boldsymbol{g}_{2,3} = ((1\,3\,4), (1\,2\,4), (1\,2\,4), (1\,2\,3))\\ (\boldsymbol{g}_{2,1})q_2 &= ((1\,2\,3), (2\,3\,4), (1\,3\,4), (1\,2\,4))\,\mathbf{sh}\to \quad ((2\,3\,4), (1\,3\,4), (1\,2\,4), (1\,2\,3))\\ (\boldsymbol{g}_{2,1})q_2^2 &= ((1\,2\,3), (1\,2\,3), (2\,3\,4), (1\,2\,4))\,\mathbf{sh}\to \boldsymbol{g}_{2,2} = ((1\,2\,4), (1\,2\,3), (1\,2\,3), (2\,3\,4))\\ (\boldsymbol{g}_{2,1})q_2^3 &= ((1\,2\,3), (1\,2\,4), (1\,2\,3), (1\,2\,4))\,\mathbf{sh}\to \quad ((1\,2\,4), (1\,2\,3), (1\,2\,4), (1\,2\,3))\end{aligned}$$

In the 2nd row, we used $\mathbf{sh}^{-1}$, but that is $\mathbf{sh}$ modulo $\mathcal{Q}''$. Finally, apply $q_1^{-1}q_3 \in \mathcal{Q}''$ to the (4th row, 2nd column) to see we get the (2nd row,1st column).

That is, $\mathbf{sh}$ switches the 2nd and 4th terms of ${}_cO^4_{1,1}$. We have filled in everything in Ni_0^-. This shows there are no fixed points of γ_0 or γ_1 in the Ni_0^- cusp orbits, but you immediately see from computation that $\mathbf{sh}^2q_1q_3^{-1}$ fixes the $\mathbf{DI}$ elements in the length 1 cusps. This shows (2.40d).

To see that we have included all cusp orbits in Ni_0^+ and Ni_0^-, apply elements of $\mathcal{Q}''$ to count elements of shape $++--$. Then, up to inner equivalence count the 4-tuples that start $((1\,2\,3),(1\,2\,3))$ and those that start $((1\,2\,3),(1\,3\,4))$, modulo the action of $q_1q_3^{-1}$ and conjugation by $(1\,2\,3)$).

Example 3.17 (Component genuses). Use $(\gamma_0,\gamma_1,\gamma_\infty)$ from the $\mathbf{sh}$-incidence calculation in Prop. 3.16. Denote their restrictions to lifting invariant +1 (resp. -1) orbit by $(\gamma_0^+,\gamma_1^+,\gamma_\infty^+)$ (resp. $(\gamma_0^-,\gamma_1^-,\gamma_\infty^-)$).

We read indices of the + (resp. −) elements from the Ni_0^+ (resp. Ni_0^-) matrix block. Fixed points of γ_0 and γ_1 appear on the diagonal. Diagonal entries for $O^4_{1,1}$ and $O^4_{2,1}$ are nonzero:

$$\gamma_1 \text{ (resp. } \gamma_0\text{) fixes 1 (resp. no) element of } O_{1,1}.$$
$$\text{Neither of } \gamma_i,\ i=0,1, \text{ fix any element of } O^4_{2,1}.$$

Cusp widths over ∞ add to the degree 9 (resp. 6) to give

$$\mathrm{ind}(\gamma_0^+)=6,\ \mathrm{ind}(\gamma_1^+)=4,\ \mathrm{ind}(\gamma_\infty^+)=6$$
$$\mathrm{ind}(\gamma_0^-)=4,\ \mathrm{ind}(\gamma_1^-)=3,\ \mathrm{ind}(\gamma_\infty^-)=3.$$

From RH, the genus, $\mathbf{g}_\pm$ of $\mathcal{H}^\pm$ is 0: $2(9+g_+-1)=6+4+6=16$ and $2(6+g_--1)=4+3+3=10$. △

4. The Branch Cycle Lemma

At the center of applying Hurwitz spaces to problems in number theory is the definition field for them and their components *as moduli spaces*. That means not just the Hurwitz space, say, $\mathcal{H}(G,\mathbf{C})^\dagger$ (or related), but the natural structure parametrized by the Hurwitz space – giving it its moduli space structure – is defined over that field. Notation will reference a particular component or collection of components of the space.

Example: In Prop. 4.1, $\mathbb{Q}(G,\mathbf{C})^{\mathrm{in}}$ is that definition field for the whole inner Hurwitz space structure of covers in $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$. [**Fr77**, p. 62–64] calls Prop. 4.1 the Branch Cycle Argument. Yet, as exposited here it is a general idea; thus, we refer to its version for $\dagger = \mathrm{in}$ or abs on Hurwitz spaces as

The **B**(ranch)**C**(ycle)**L**(emma).

The organizing principle of [**Fr77**, Thm. 5.1]*:* That is the first formula for finding covers (resp. **RIGP** realizations) over a given field K. It equivalences that to fnding points in $\mathcal{H}^{\rm abs}(K)$ (resp. $\mathcal{H}^{\rm in}(K)$) over K in the corresponding Nielsen class $\mathrm{Ni}(G,\mathbf{C})^{\rm abs}$ (resp. $\mathrm{Ni}(G,\mathbf{C})^{\rm in}$). The condition is that K contains the *moduli field* of the Hurwitz space. Further, if that holds:

$$\begin{array}{c}\text{a } K \text{ point } \boldsymbol{p}\in\mathcal{H}^{\rm abs}(K) \text{ (resp. } \hat{\boldsymbol{p}}\in\mathcal{H}^{\rm in}(K))\\ \text{gives such a cover if the Hurwitz space has } \textit{fine moduli}.\end{array} \tag{2.41}$$

Notation, as in comments on Cor. 4.7, will distinguish the moduli definition fields of Hurwitz spaces components when the Hurwitz space has several components.

Beyond the **BCL***:* §4.2 proves the **BCL**. §4.2.3 addresses Nielsen classes, especially when $r\ge 4$, with several components. It raises issues on extending Nielsen class moduli to component distinguishing moduli, in particular to capture its corresponding moduli definition field.

§4.3 has preliminary examples. In §4.3.1, the Hurwitz space (even with its map to the configuration space) can be defined over $\mathbb{Q}$. Yet, no component total space structure (so no cover in the Nielsen class) has definition field $\mathbb{Q}$. Reference to the Hurwitz space definition field means – unless otherwise said – *as a moduli space*.

4.1. The BCL formula. §4.1.1 gives the cyclotomic fields that will be the definition fields of Hurwitz spaces – as moduli spaces – purely in terms of Nielsen classes. §4.1.2 gives a general context for the moduli definition field attached to a particular equivalence class E for a moduli problem †. We apply it to E, a Nielsen class, under † equal to inner or absolute equivalence in §4.1.3 showing the correct cyclotomic moduli definition fields.

4.1.1. *Absolute and inner cyclotomic fields.* Denote the least common multiple of all elements of $\mathbf{C}$ by $N_{\mathbf{C}}$.

Use this canonical $N_{\mathbf{C}}$th root of 1, $e^{\frac{2\pi i}{N_{\mathbf{C}}}}=\zeta_{\mathbf{C}}$, and denote $K(\zeta_{\mathbf{C}})$ by $\mathrm{Cyc}_{K,\mathbf{C}}$.

Recall: $G(\mathrm{Cyc}_{\mathbb{Q},\mathbf{C}}/\mathbb{Q})=(\mathbb{Z}/N_{\mathbf{C}})^*$, invertible integers mod $N_{\mathbf{C}}$. Then, the subgroup fixed on $K\cap\mathrm{Cyc}_{\mathbb{Q},\mathbf{C}}$ is $G(\mathrm{Cyc}_{K,\mathbf{C}}/K)$. For † = in, define $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}$ to be the fixed (cyclotomic) subfield of $\mathrm{Cyc}_{\mathbb{Q},\mathbf{C}}$ of the following group:

$$\{m\in(\mathbb{Z}/N_{\mathbf{C}})^*\mid\{g^m\mid g\in\mathbf{C}\}\stackrel{\rm def}{=}\mathbf{C}^m=\mathbf{C}\}. \tag{2.42}$$

Note: $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}=\mathbb{Q}$ precisely when $\mathbf{C}$ is a rational union of classes (Ch. 1 Def. 1.4).

Similarly, define $\mathbb{Q}_{G,\mathbf{C},T}\stackrel{\rm def}{=}\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}$ (if T is understood) to be the fixed field of

$$\{m\in(\mathbb{Z}/N_{\mathbf{C}})^*\mid\exists h\in N_{S_n}(G,\mathbf{C}) \text{ with } h\mathbf{C}^mh^{-1}=\mathbf{C}\}. \tag{2.43}$$

Recall fine moduli as in Lem. 2.3 for our equivalences:

for † = abs, (G,T) is self-normalizing; and for † = in, G is centerless.

Write $\mathrm{Ni}(G,\mathbf{C},T)^{\rm abs}\stackrel{\rm def}{=}\mathrm{Ni}(G,\mathbf{C})^{\rm abs}$.

PROPOSITION 4.1. *The field $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}$ (resp. $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}$) is a subfield of any definition field for any cover in* $\mathrm{Ni}(G,\mathbf{C})^{\rm in}$ *(resp.* $\mathrm{Ni}(G,\mathbf{C})^{\rm abs}$*). If fine moduli holds for* $\mathcal{H}(G,\mathbf{C})^{\rm abs}$*, then a representing cover,* $\varphi_{\boldsymbol{p}} : X_{\boldsymbol{p}} \to \mathbb{P}^1_z$ *satisfies* (2.44).

(2.44a) *$\varphi_{\boldsymbol{p}}$ has definition field $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}(\boldsymbol{p})$; any cover equivalent to $\varphi_{\boldsymbol{p}}$ has definition field an extension of $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}(\boldsymbol{p})$; and*

(2.44b) *if $\varphi'_{\boldsymbol{p}}$, defined over $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}(\boldsymbol{p})$, is* abs*-equivalent to $\varphi^{\rm abs}_{\boldsymbol{p}}$, then it is equivalent to it over $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}(\boldsymbol{p})$.*

Similarly, for fine moduli ($\dagger = \mathrm{in}$), except substitute $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}$ for $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}$, and each element of the automorphism group of the Galois extension – with a fixed isomorphism with G, up to conjugacy by G – has $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}(\boldsymbol{p})$ as definition field.

§4.1.2 gives a context for the idea of moduli definition field. Then, §4.1.3 adds fine moduli to it. §4.2 shows the postulates of (2.46) apply to the various moduli of Hurwitz spaces, thereby giving the proof of the **BCL**.

REMARK 4.2. More generally, apply $\sigma \in G_{\bar{\mathbb{Q}}}$ to a specific cover $\varphi : X \to \mathbb{P}^1_z$ over $\bar{\mathbb{Q}}$, with the branch point set $\boldsymbol{z}_\varphi$ fixed by σ. Assume we have two pieces of data:

(2.45a) $n_\sigma \in (\hat{\mathbb{Z}})^*$, the restriction of σ to the cyclotomic closer of $\mathbb{Q}$; and

(2.45b) the permutation by σ of the individual points in $\boldsymbol{z}_\varphi$.

The **BCL** then nails the Nielsen class of the resulting cover $(\varphi^\sigma, X^\sigma)$. For $K = \mathbb{R}$, as in [**DFr90**], it does better: labeling precisely all real and complex points on a given Hurwitz space, as discussed in [**BFr02**, §3.2].

4.1.2. *Context for moduli definition field.* Consider some defining property of equivalence classes of algebraic objects (varieties, diagrams of covers, ...). Call this $\dagger$. For each $\dagger$-equivalence class, E, we assume there is a quasi-projective variety $\mathcal{H}^\dagger_E$ whose points $\boldsymbol{p} \in \mathcal{H}^\dagger_E$ correspond to equivalence classes of objects $O_{\boldsymbol{p}} \in E$. Not only must there be a natural operation of $G_{\mathbb{Q}}$ on $(\dagger, E)$, but we must assure that $G_{\mathbb{Q}}$ respects (the moduli properties of) $(\dagger, E)$.

DEFINITION 4.3. In addition to the $G_{\mathbb{Q}}$ action above, assume for $\sigma \in G_{\mathbb{Q}}$, if $\boldsymbol{p} \in \mathcal{H}^\dagger_E(\bar{\mathbb{Q}})$, those objects $O_{\boldsymbol{p}} \in E$ defined over $\bar{\mathbb{Q}}$ go by σ to objects representing $\boldsymbol{p}^\sigma \in \mathcal{H}^{\dagger^\sigma}_{E^\sigma}$. We then say $G_{\mathbb{Q}}$ *respects* $(\dagger, E)$.

Families of representations objects: Denote the Zariski or étale topology (depending on circumstances) on $\mathcal{H}_E$ by Top_E. Assume we also have the following.

(2.46a) For each $\boldsymbol{p} \in \mathcal{H}^\dagger_E(\bar{\mathbb{Q}})$, some representing object $O_{\boldsymbol{p}}$ is defined over $\bar{\mathbb{Q}}$ (say, by applying Lem. 1.1).

(2.46b) Extending (2.46a), for $\sigma \in G_{\mathbb{Q}}$, $O^\sigma_{\boldsymbol{p}^\sigma}$ is a representing object for $\boldsymbol{p}^\sigma \in \mathcal{H}^{\dagger^\sigma}_{E^\sigma}$.

(2.46c) Each $\boldsymbol{p} \in \mathcal{H}_E^\dagger$ has a neighborhood $U_{\boldsymbol{p}} \in \mathrm{Top}_E$ with nonempty families $\mathcal{F}_U$: Each $F \in \mathcal{F}_U$ comes with a flat quasi-projective map $F \to U$ with fiber at each $\boldsymbol{p}' \in U$ representing the E class of $\boldsymbol{p}'$.

(2.46d) The collections $\{\mathcal{F}_U \mid U \in \mathrm{Top}_E\}$ form a *presheaf* from natural maps $F_U \to F_V$ for $V \to U$.

The maps in (2.46d) come from pullback, say, when V is a cover (or open subset) of U, as explained in §4.3.2. Our families are so explicit, from such tools as §3.1.1, that may use them to approach moduli by nontrivially illustrating their properties. *Fine moduli* means there is an object in $F(\mathcal{H}_E^\dagger)$, unique up to a natural equivalence, that induces a similar object in $F(U)$, $U \in \mathrm{Top}_E$.

Especially important is finding explicitly the following notion of a moduli definition field, $\mathbb{Q}_E^\dagger$, for E.

(2.47) For each $\boldsymbol{p} \in \mathcal{H}_E^\dagger$, any definition field for $O_{\boldsymbol{p}}$ contains $\mathbb{Q}_E^\dagger(\boldsymbol{p})$.
If E has fine moduli, some $O_{\boldsymbol{p}}$ has definition field $\mathbb{Q}_E^\dagger(\boldsymbol{p})$.

Of course, when $\mathbb{Q}_E^\dagger = \mathbb{Q}$, a common target is $\boldsymbol{p} \in \mathcal{H}_E^\dagger(\mathbb{Q})$, thereby realizing $O_{\boldsymbol{p}}$ over $\mathbb{Q}$ when fine moduli holds. Much remains of the **RIGP** precisely because we haven't located for every G, $\mathbf{C}$ with $\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}(\mathbb{Q})$ nonempty. In examples, when $.\mathcal{H}(G,\mathbf{C})^{\mathrm{in}}$ has several components, we sometimes need the following.

(2.48a) For a given $(\dagger, E)$ identify the irreducible components $\mathcal{H}'_1, \dots, \mathcal{H}'_k$ of $\mathcal{H}_E^\dagger(\mathbb{Q})$.

(2.48b) Restrict the presheaf of (2.46d), and for any $G_{\mathbb{Q}_E^\dagger}$ orbit, $\mathcal{H}''$ on $\mathcal{H}'_1, \dots, \mathcal{H}'_k$, identify a(n E extending) moduli characterization E'' for this orbit.

(2.48c) For each orbit $\mathcal{H}''$ in (2.48b), and each component, say, $\mathcal{H}'_j$, find a field extension $L'_j/\mathbb{Q}_E^\dagger$ as an $\mathcal{H}'_j$ replacement for $\mathbb{Q}_E^\dagger$ applied to $\mathcal{H}_E^\dagger$.

REMARK 4.4 (Comment on (2.48)). The L'_js are conjugate fields running over the components of $\mathcal{H}''$ in (2.48c).

The notion of moduli field works: For any $\boldsymbol{p} \in \mathcal{H}_E^\dagger(\bar{\mathbb{Q}})$, consider $O_{\boldsymbol{p}}$, defined over $\bar{\mathbb{Q}}$ using assumption (2.46c), representing $\boldsymbol{p}$. Form the set

$$G_{E,\boldsymbol{p}}^\dagger \stackrel{\mathrm{def}}{=} \{\sigma \in G_{\mathbb{Q}} \mid O_{\boldsymbol{p}}^\sigma \text{ is } \dagger\text{-equivalent over } \bar{\mathbb{Q}} \text{ to } O_{\boldsymbol{p}}\}.$$

LEMMA 4.5. *The set $G_{E,\boldsymbol{p}}^\dagger$ is a group, and its fixed field, $\mathbb{Q}_{E,\boldsymbol{p}}^\dagger$, in $\bar{\mathbb{Q}}$ depends only on $(\dagger, \boldsymbol{p})$, not on the choice of $O_{\boldsymbol{p}}$. Further, if fine moduli holds for $\mathcal{H}_E^\dagger$, then the equivalence class for $\boldsymbol{p}$ contains an object defined over $\mathbb{Q}_{E,\boldsymbol{p}}^\dagger$.*

PROOF. Any $\sigma \in G_{E,\boldsymbol{p}}^\dagger$ leaves $\boldsymbol{p}$ fixed. Otherwise its extension to $O_{\boldsymbol{p}}$ would represent an object in $\boldsymbol{p}^\sigma$, an object not equivalent to $O_{\boldsymbol{p}}$.

Now, suppose two objects, $O_{\boldsymbol{p}}$ and $O'_{\boldsymbol{p}}$, defined over $\bar{\mathbb{Q}}$ represent $\boldsymbol{p}$. Denote the graph of an isomorphism between them, postulated for $G_{E,\boldsymbol{p}}^\dagger$, by Γ. Apply postulate

(2.46a) to assume the graph has definition field in $\bar{\mathbb{Q}}$. Now consider the case $O'_{\boldsymbol{p}} = O^{\sigma}_{\boldsymbol{p}}$ for $\sigma \in G_{\dagger,\boldsymbol{p}}$, denoting Γ by $\Gamma_\sigma : O_{\boldsymbol{p}} \to O^{\sigma}_{\boldsymbol{p}}$. Then, apply $\tau \in G^{\dagger}_{E,\boldsymbol{p}}$ to Γ_σ to get

$$O_{\boldsymbol{p}} \xrightarrow{\Gamma_\sigma} O^{\sigma}_{\boldsymbol{p}} \xrightarrow{(\Gamma_\sigma)^{\tau}} O^{\sigma\cdot\tau}_{\boldsymbol{p}}, \text{ showing } \sigma\cdot\tau \in G^{\dagger}_{E,\boldsymbol{p}} \text{ and } G^{\dagger}_{E,\boldsymbol{p}} \text{ is a group.} \tag{2.49}$$

Denote another object, $O'_{\boldsymbol{p}}$, representing $\boldsymbol{p}$ over $\bar{\mathbb{Q}}$ and Γ the morphism above between them. Temporarily, denote $G^{\dagger}_{E,\boldsymbol{p}}$ using $O'_{\boldsymbol{p}}$ in place of $O_{\boldsymbol{p}}$ by $G'_{E,\boldsymbol{p}}$. In (2.49) substitute $O'_{\boldsymbol{p}}$ for $O^{\sigma}_{\boldsymbol{p}}$ and Γ for Γ_σ. This shows $\tau \in G'_{E,\boldsymbol{p}}$ is also in $G_{E,\boldsymbol{p}}$ establishing that the two groups are the same, and independent of the choice of $O_{\boldsymbol{p}}$.

Now assume fine moduli holds for $(\dagger, E)$). Return to (2.49). Then, the uniqueness of the maps giving isomorphisms for the equivalent objects tells us that we can assure $\Gamma_{\sigma\cdot\tau} = (\Gamma_\sigma)^{\tau} \circ \Gamma_\sigma$ for $(\sigma,\tau) \in G^{\dagger}_{E,\boldsymbol{p}}$. This is the *Weil co-cycle condition* – as in [**We56**] and [**We62**, p. 15, Thm. 3] – that guarantees we can find $O_{\boldsymbol{p}}$ with definition field $\mathbb{Q}^{\dagger}_{E,\boldsymbol{p}}$. Rem. 4.6 adds remarks about relevant to how we use it. □

REMARK 4.6. Saying that there an $O_{\boldsymbol{p}}$ in Lem. 4.5 is defined over the desired field, includes putting natural projective coordinates on that object. Further, we can say that another object defined over $\mathbb{Q}^{\dagger}_{E}(\boldsymbol{p})$ will be †-equivalent over this field. Finally, sometimes we must add a little extra to the use of the cocycle condition; the conditions don't at first appear entirely stated in terms of a quasi-projective structure. We see that in applying the Lemma to fine moduli.

4.1.3. *Definition field of components.* Fine moduli in (2.44) assures there is a representing cover $\varphi_{\boldsymbol{p}}$ over the minimal possible field $\mathbb{Q}^{\dagger}_{G,C}(\boldsymbol{p})$ and that depends only on the coordinates of $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{\dagger}$ and $\mathbb{Q}^{\dagger}_{G,\mathbf{C}}$. Indeed, this arithmetic use of fine moduli is much driven by what we need for the co-cycle condition. Without fine moduli such representing objects may not exist (see Rem. 4.9).

Cor. 4.7 says, in one fell swoop, we can pluck the solution of the moduli problem expressed in (2.44b) by picking a point $\hat{\boldsymbol{p}} \in \mathcal{H}(G,\mathbf{C})^{\rm in}$ (resp. $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{{\rm abs}_T}$), adjoin $\mathbb{Q}^{\in}_{G,\mathbf{C}}$ (resp. $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}$) to it, and take the associated fiber in (2.50). The following is in [**FrV91**, Main Thm.] (an extension of [**Fr77**, Thm. 5.1]).

COROLLARY 4.7 (Global-**BCL**). *Assume fine moduli for* † = in *or* abs *in Thm. 1.7. Then, the minimal definition field of the diagram*

$$\mathcal{T}(G,\mathbf{C})^{\dagger} \to \mathcal{H}(G,\mathbf{C})^{\dagger} \times \mathbb{P}^1_z \xrightarrow{{\rm proj}_{\mathcal{H}^{\dagger}}} \mathcal{H}(G,\mathbf{C})^{\dagger} \to U_r \text{ is } \mathbb{Q}^{\dagger}_{G,\mathbf{C}}. \tag{2.50}$$

Also, minimal definition fields of all covers in ${\rm Ni}(G,\mathbf{C})^{\dagger}$ *intersect in* $\mathbb{Q}^{\dagger}_{G,\mathbf{C}}$.

DEFINITION 4.8 (Definition as a moduli space). Consider the pullback diagram over any component $\mathcal{H}'$ of $\mathcal{H}(G,\mathbf{C})^{\rm abs}$ in Cor. 4.7. Refer to the definition field $\mathbb{Q}_{\mathcal{H}'}$ of that diagram as the definition field of $\mathcal{H}'$ as a *moduli space*.

COMMENTS ON COR. 4.7. §4.2 gives the ingredients of the **BCL**: why the Hurwitz space diagrams are over the 'predicted" fields (here called over $\mathbb{Q}^{\dagger}_{G,\mathbf{C}}$). A rough

statement goes like this. Any $\sigma \in G_{\mathbb{Q}}$ fixed on $\mathbb{Q}^{\dagger}_{G,\mathbf{C}}$ operating on the equation coefficients describing that diagram, or on individual fibers over $\bar{\mathbb{Q}}$, maps them to diagrams and fibers associated with the exact same Nielsen class.

When fine moduli holds, aided by Weil's cocycle condition, the whole diagram has definition field $\mathbb{Q}^{\dagger}_{G,\mathbf{C}}$. With the notation of Def. 4.8, two statements are immediate from the Hurwitz spaces as moduli spaces.

(2.51a) $\mathbb{Q}_{\mathcal{H}''}$ (resp. $\mathbb{Q}_{\mathcal{H}'}$) contains $\mathbb{Q}^{\rm in}_{G,\mathbf{C}}$ (resp. $\mathbb{Q}^{\rm abs}_{G,\mathbf{C}}$ permutes the diagrams running over $\mathcal{H}''$ (resp. $\mathcal{H}'$).

(2.51b) If in (2.51a), $\mathcal{H}''$ lies over $\mathcal{H}'$, then $\mathbb{Q}_{\mathcal{H}''}$ contains $\mathbb{Q}_{\mathcal{H}'}$.

For † equivalence, Hurwitz spaces are algebraic varieties that are complex *manifolds*. That is no longer true for any reduced equivalence. Yet, they are still normal varieties. So their components are disjoint, meaning this.

(2.52) Points in different components represent inequivalent covers.
The definition field of a point contains that of its component.

Nevertheless, here is all that we can say at the outset.

(2.53) Any $\sigma \in G_{\mathbb{Q}_{G,\mathbf{C}}}$ (resp. $G_{\mathbb{Q}_{G,\mathbf{C},T}}$) permutes
$\mathcal{H}(G,\mathbf{C})^{\rm in}$ (resp. $\mathcal{H}(G,\mathbf{C})^{\rm abs}$) components as moduli spaces.

Conclude: if even one cover in the Nielsen class has definition field K, then $\mathbb{Q}^{\dagger}_{G,\mathbf{C}} \subset K$, and the component containing a point corresponding to that cover has moduli field contained in K. See Ex. 4.18. □

Rems. 4.9, 4.10 and 4.11 discuss in general what happens without fine moduli.

REMARK 4.9 (Moduli field without fine moduli). Without a fine moduli property, we don't expect (**??**). That is, a point $\boldsymbol{p} \in \mathcal{H}(G,\mathbf{C})^{\bullet}(\mathbb{Q}_O)$ may not have a representing cover $X_{\boldsymbol{p}} \to \mathbb{P}^1_z$ defined over $\mathbb{Q}(\boldsymbol{p})$. Still, the moduli space, with its structures, will have its definition field determined by the moduli condition.

For example, suppose O is a braid orbit on $\mathrm{Ni}(G,\mathbf{C})^{\dagger}$, corresponding to a component $\mathcal{H}_O$ of $\mathcal{H}(G,\mathbf{C})^{\dagger}$, $\dagger$ = in or abs. Also, that $V \subset \mathcal{H}_O$ is a Zariski or étale open set, defined over $\mathbb{Q}_O$. Then, the following objects will be defined over $\mathbb{Q}_O$:

(2.54a) Maps involved in $\mathcal{H}_O \to U_r \times \mathbb{P}^1_z$ and its projections; and

(2.54b) the collection of families $\mathcal{T}_V \to V \times \mathbb{P}^1_z$ whose fibers $\mathcal{T}_{\boldsymbol{p}} \to \boldsymbol{p} \times \mathbb{P}^1_z$ represent the points $\boldsymbol{p} \in V$.

REMARK 4.10. Even the group $\mathbb{Z}/n$, has something to offer on fine moduli. §3.3.2 notes that there are still realizing covers in this case over $\mathbb{Q}$ when the necessary condition (**??**) holds. It also explains general cases guaranteeing that no cover – even if (**??**) holds – in a Nielsen class will have definition $\mathbb{Q}$. Finally, that there is an explicit bound for the degree of the moduli field/$\mathbb{Q}$ in this case.

REMARK 4.11 (Reduced spaces moduli field). There are similar statements with $\bullet = \{\dagger, \mathrm{rd}\}$ replacing †; adding reduced equivalence and substituting J_r for U_r. The major difference is that the criterion for fine moduli changes, §2.2.3.

For example, Prop. 3.16 gives $(G, \mathbf{C}) = (A_4, \mathbf{C}_{+3^2-3^2})$ with two inner components with $\mathbb{Q}_O = \mathbb{Q}$, for both. Here, the Hurwitz spaces have fine moduli, but reduction of neither of its components has fine moduli. This also shows a refined distinction when $r = 4$: One component has the close condition of b-fine moduli, while the other does not.

4.2. The BCL Proof and Moduli Extension. Here we see how to apply Lem. 4.5 (and Rem. 4.6) to the case where † is one of our equivalences and E is a Nielsen class. Mainly this is checking the hypotheses (2.46). Our proof is a more efficient version of [**Fr77**, p. 33–35]. We start, say, when $\dagger = \mathrm{abs}_T$, with a specific cover $\varphi : X \to \mathbb{P}^1_z$ in $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}_T}$ over K. The essence of [**Fr77**, (5.10)] (or the slower treatment of [**Fr12**, (5.2)]) is to compute the resulting Nielsen class upon applying $\sigma \in \mathcal{G}_K$ to φ. That includes its action on the set of branch points, defined over K, even when individual such points may not be.

4.2.1. *$G_{\mathbb{Q}}$ action on covers in* $\mathrm{Ni}(G, \mathbf{C})^{\dagger}$. Continue the notation of §4.1.1, with $N_{\mathbf{C}}$ the least common multiple of the orders of elements in $\mathbf{C}$, defining the Nielsen class $\mathrm{Ni}(G, \mathbf{C})$. With $\zeta_t = e^{\frac{2\pi i}{t}}$, $t \geq 1$, identify the group $G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ with the multiplicative group $(\mathbb{Z}/N)^*$ of invertible integers modulo N.

As in §4.17, $N_{S_n}(G, \mathbf{C})$ is the normalizer of G that permutes the elements of $\mathbf{C}$. Then, denote the image conjugacy class of C_i under (conjugation by) $\beta \in N_{S_n}(G, \mathbf{C})$ by C_i^{β}. We define two sets:

$$\widehat{M} = \{a \in (\mathbb{Z}/N_{\mathbf{C}})^* | \text{ there exists } \beta \in N_{S_n}(G, \mathbf{C}) \text{ with } \mathrm{C}_i^{\beta} = \mathrm{C}_i^a, i = 1, \ldots, r.$$

$$\begin{gathered} M = \{a \in \big(\mathbf{Z}/(N)\big)^* | \text{ there exists } \gamma \in S_r \text{ and } \beta \in S_r \text{ with} \\ Con\Big(\sigma(i)^a, G(\boldsymbol{g})\Big) = Con\Big(\gamma^{-1} \cdot \sigma\big((i)\beta\big) \cdot \gamma, G(\boldsymbol{g})\Big) \\ \text{for } i = 1, \ldots, r\}. \end{gathered}$$

It is easy to demonstrate the M (and therefore $\widehat{M}$) is a group. Let K_M (resp. $K_{\widehat{M}}$) be the fixed field of M (resp. $\widehat{M}$) in $\mathbf{Q}(\zeta_N)$.

THEOREM 4.1. *We assume that condition* (5.1) *holds. Then the collection* $\mathbb{M}(Y, \varphi; r)$ *has a minimal field of definition which we denote by* $K_{\mathbb{F}}$.

We have $K_M \subset K_{\mathbb{F}}$. *In addition, if the Hurwitz number of* $\big(\sigma(1), \ldots, \sigma(r)\big) = \boldsymbol{g}$ *is* 1 *(see Section* 4.B*), then we have* $K_M = K_{\mathbb{F}}$.

We use the notation of Section 0.C. *The field* $K_{\mathbb{F}}(\mathcal{P})$ *is contained in* $K_{\mathbb{F}}(\mathbb{F}^{\mathrm{symm}})$. *Let* $\widehat{K_{\mathbb{F}}(\mathbb{F}^{\mathrm{symm}})}$ *be the Galois closure of* $K_{\mathbb{F}}(\mathbb{F}^{\mathrm{symm}})/K_{\mathbb{F}}(\mathcal{P} \times \mathbf{P}^1)$, *and let* $\widehat{K_{\mathbb{F}}(\mathcal{P})}$ *be the algebraic closure of* $K_{\mathbb{F}}(\mathcal{P})$ *in* $\widehat{K_{\mathbb{F}}(\mathbb{F}^{\mathrm{symm}})}$. *Then we have* $K_{\widehat{M}} \subset \widehat{K_{\mathbb{F}}(\mathcal{P})}$.

Note:. In the notation at the end of Section 2, $K_{\widehat{M}}$ is a portion of a fixed component of the extension of constants for the family fiber by (5.2). Also, it is an unsolved problem as to whether $K_M = K_{mcF}$ when the Hurwitz number of $\boldsymbol{g}$ is *not* 1.

PROOF. We consider first the collection:

$$\mathbb{M}^0(Y, \varphi; r) = \{\mathbb{F}^{\text{symm}}, \overline{\psi^{\text{symm}}}, \overline{\mathbb{P}^r_1}, \overline{\mathbb{P}^r_2}\}$$

where:

$$\text{a) } \mathbb{F}^{\text{symm}} \xrightarrow{\psi^{\text{symm}}} U_{\mathbf{P}^r} \times \mathbf{P}^1 \xrightarrow{\overline{P^r{}_1}} U_{\mathbf{P}^r} \text{ and;} \tag{2.4}$$

$$\xrightarrow{\overline{P^r{}_2}} \mathbf{P}^1$$

$$\text{b) } \psi^{\text{symm}} = (\psi \circ \overline{P^r{}_1} \circ \Phi^{\text{symm}}, \overline{P^r{}_2} \circ \Phi^{\text{symm}})$$

Our first task is to show that the collection $\mathbb{M}^0(Y, \varphi; r)$ has all the properties attributed to $\mathbb{M}(Y, \varphi; r)$ in the statement of the theorem.

Let $K \subset \mathbf{C}$ be a field of finite type over $\mathbf{Q}$ containing a field of definition for each member of the collection $\mathbb{M}^0(Y, \varphi; r)$. An argument based on the proof of Lemma (**??**)1.2 allows us to assume: $[K : \mathbf{Q}] < \infty$ [nh, i.e., a finite extension]. We also assume that $K/\mathbf{Q}$ is Galois.

For $\gamma \in G(K/\mathbf{Q})$ we define:

$$\mathbb{M}^0(Y, \varphi; r)^\gamma = \{(\mathbb{F}^{\text{symm}})^\gamma, (\psi^{\text{symm}})^\gamma, \overline{P^r{}_1}^\gamma, \overline{P^r{}_2}^\gamma\}$$

to be the transform of the collection $\mathbb{M}^0(Y, \varphi; r)$ under γ. We say that $\mathbb{M}^0(Y, \varphi; r)^\gamma$ is *isomorphic* to $\mathbb{M}^0(Y, \varphi; r)$ if there is an isomorphism $\alpha(\mathbb{F}^{\text{symm}})^\gamma$ rendering commutative the diagram:

$$\begin{array}{ccc} \mathcal{T}^\gamma & \xrightarrow{\Psi^\gamma} & U_r \times \mathbb{P}^1 \\ {\scriptstyle \alpha(\mathcal{T}^\gamma)}\downarrow & \nearrow_{\Psi} & \\ \mathcal{T} & & \end{array} \tag{2.5}$$

nh triangular commutative diagram goes here Let H be the subgroup of $G(K/\mathbf{Q})$ consisting of those γ for which $\mathbb{M}^0(Y, \varphi; r)^\gamma$ is isomorphic to $\mathbb{M}^0(Y, \varphi; r)$. Let $K_{\mathbb{F}}$ be the fixed field in K of H. So far we have not used the fact that $Aut(Y, \varphi) = \{Id.\}$. We call $K_{\mathbb{F}}$ the *field of moduli* of the collection $\mathbb{M}^0(Y, \varphi; r)$, in analogy with ([**?**], pp. 32-35). This concept will be used again in comments in Section 6 (example 8).

Since we assume $Aut(Y, \varphi) = \{Id.\}$, we see that if $\mathbb{M}^0(Y, \varphi; r)^\gamma$ and $\mathbb{M}^0(Y, \varphi; r)$ are isomorphic, there is a unique isomorphism $\alpha\big(\mathbb{F}^{\text{symm}})^\gamma\big)$ making (5.5) commutative. Therefore, from [**?**] we may assume that $K_{\mathbb{F}}$ is a minimal field of definition of $\mathbb{M}^0(Y, \varphi; r)$ (in analogy with the definition preceding the statement of this theorem).

We refer to our next computation as: The Branch Cycle Argument. An approximation to this was used earlier in [**?**].

Let $Z \xrightarrow{\varphi(Z)} \mathbf{P}^1$ be a cover (non-singular and projective) defined over a number field L, with: a description of its branch cycles given by $\sigma(1,Z),\dots,\sigma(r,Z)$, corresponding respectively to branch points $u(1,Z),\dots,u(r,Z)$. In analogy with previous notation consider: $e(1,Z),\dots,e(r,Z); N(Z); L(Z), \widehat{L(Z)}$, and; the algebraic closure of L in $L(Z)$, denoted $\widehat{L}$ if no confusion will occur. Let x be a uniformizing parameter for $\mathbf{P}^1$.

Consider the automorphism $\overline{\sigma}(i)$ of $\overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big)$ [nh seems like unnecessary parentheses) which is the identity on $\overline{\mathbf{Q}}$ and maps $(x-u(i,Z))^{1/e(i,Z)}$ to $\zeta_{e(i,Z)}\cdot(x-u(i,Z))^{1/e(i,Z)}$. We remind that $x-u(i,Z)$ is replaced by $1/x$ when $u(i,Z)=\infty$. We have the embedding, via Puiseux expansions

$$\widehat{L(Z)} \xrightarrow{\widehat{\psi(i,Z)}} \overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big), i=1,\dots,r \tag{2.6}$$

where $\sigma(i,Z)$ is the restriction to $\widehat{L(Z)}$ of $\overline{\sigma}(i)$. For any other embedding (fixed on $L(x)$)

$$\widehat{L(Z)} \xrightarrow{\widehat{\psi'(i,Z)}} \overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big)$$

$\overline{\sigma}(i)$ restricts to some element of $Con\Big(\sigma(i,Z), G\big(\widehat{L(Z)}/L(\mathbf{P}^1)\big)\Big)$. If $\widehat{\psi'(i,Z)}$ is fixed on $\widehat{L}$ then the restriction of $\overline{\sigma}(i)$ is in $Con\Big(\sigma(i,Z), G\big(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1)\big)\Big)$.

Suppose now that $G\big(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1)\big)G\big(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1)\big)$ is isomorphic to $Con\big(\widehat{\mathbf{C}(Y)}\big)/\mathbf{C}(\mathbf{P}^1)\big)$, and suppose also that in the isomorphism $\sigma(i,Z)\in Con\big(\widehat{\mathbf{C}(Y)}\big)/\mathbf{C}(\mathbf{P}^1)\big)$. In particular, from the computations of Section 4, this holds for all covers in the family given by expression (5.2). We now show that $K_M \subset L$ (see statement of the theorem).

Suppose, in fact, that $K_M \not\subseteq L$. Then, there exists $\omega \in G(\overline{\mathbf{Q}}/\mathbf{Q})$ such that ω is fixed on L, but w is not fixed on K_M. Thus, the restriction of ω to $\mathbf{Q}(\zeta_N)$ corresponds to $a(\omega)\in(\mathbf{Z}/(N))^*$ [nh what is a??]such that: there does not exist a $\beta\in S_r$ and a $\gamma\in S_n$ with

$$Con\big(\sigma(i)^{-a(\omega)}, G(\boldsymbol{g})\big) = Con\big(\gamma^{-1}\cdot\sigma((i)\beta)\cdot\gamma, G(\boldsymbol{g})\big) \text{ for all } i=1,\dots,r \tag{2.7}$$

Let ω^* be and element of $G\big(\widehat{L(Z)}/L(\mathbf{P}^1)\big)$ whose restriction to $\widehat{L}$ is equal to ω restricted to $\widehat{L}$. We extend ω to $\overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big)$ by: $\omega(\sum_k a_k(x-u(i,Z))^{1/e(i,Z)}) = \sum_k \omega(a_n)(x-u(i,Z))^{1/e(i,Z)}$ where $\omega(u(i,Z)) = u(j,Z)$. Note that we automatically have $e(i,Z)=e(j,Z)$.

Thus we obtain:

$$\widehat{L(Z)} \xrightarrow{\omega\circ\widehat{\psi(i,Z)}} \overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big). \tag{2.8}$$

For $\alpha\in\widehat{L(Z)}$ we compute the restriction of $\boldsymbol{g}(j)$ to α as:

$$\widehat{\psi(i,Z)}^{-1}\circ\omega^{-1}\circ\boldsymbol{g}(j)\circ\omega\widehat{\psi(i,Z)}.$$

By direct computation on the Puiseux expansion $\widehat{\psi(i,Z)}(\alpha)$ we see that this is the same as:

$$\widehat{\psi(i,Z)}^{-1} \circ \overline{\sigma(i)}^{-a(\omega)} \circ \widehat{\psi(i,Z)},$$

which is $\sigma(i)^{-a(\omega)}$. Since $\widehat{\psi(i,Z)}^{-1} \circ \omega^{-1} \circ \boldsymbol{g}(j) \circ \omega \widehat{\psi(i,Z)}$ is the identity on $\widehat{L}$ (when applied to $\widehat{L(Z)}$), this is in $Con(\sigma(j), G(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1)))$, or

$$Con\Big(\sigma(i)^{-a(\omega)}, G\big(\widehat{L(Z)}/\widehat{L}\mathbf{P}^1)\big)\Big) = Con\Big(\omega^{*-1} \cdot \sigma(j) \cdot \omega^*, G\big(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1)\big)\Big). \tag{2.9}$$

However, with the aforementioned identification of $G(\boldsymbol{g})$ with $G(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1))$, etc., expression (5.9) contradicts (5.7). Therefore $K_M \subset L$.

Now we show that $K_{\widehat{M}} \subseteq \widehat{L}$. If we assume that $K_{\widehat{M}} \not\subseteq \widehat{L}$ and proceed as above, we end up with the expression:

$$Con\Big(\sigma(i)^{-a(\omega)}, G\big(\widehat{L(Z)}/\widehat{L}\mathbf{P}^1)\big)\Big) = Con\Big(\sigma(j) \cdot\ G\big(\widehat{L(Z)}/\widehat{L}\mathbf{P}^1)\big)\Big).$$

where j is defined by $\omega(u(i,Z)) = u(j,Z)$. Again, this is a contradiction (from the definitions of $K_{\widehat{M}}$ and $a(\omega)$).

We need and addition to the brach cycle argument to describe what happens when we apply $\omega \in G(\overline{\mathbf{Q}}/\mathbf{Q})$ to $Z \xrightarrow{\varphi(Z)} \mathbf{P}^1$ when ω is not the identity on L.

Let l^ω be the image of L under ω. Let $Z^\omega \xrightarrow{\varphi(Z)^\omega}$ ($\mathbf{P}^1$ be the transform of $Z \xrightarrow{\varphi(Z)} \mathbf{P}^1$ by ω. By operating on the coefficients of the Puiseux expansions, as above, we obtain:

$$\omega : \overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big) \to \omega : \overline{\mathbf{Q}}\Big(\big((x-u(i,Z))^{1/e(i,Z)}\big)\Big).$$

We define $\widehat{\omega}$ so as to make the following diagram commutative:

nh rectangular commutative diagram goes here

From $\widehat{\omega}$ we obtain an isomorphism between the group $G(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1))$ and $G(\widehat{L^\omega(Z^\omega)}/L^\omega(\mathbf{P}^1))$ given by: $\sigma \to \widehat{\omega} \cdot \sigma \cdot \widehat{\omega}^{-1} \triangleq \sigma^\omega$ for $\sigma \in G(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1))$. Also, if σ is fixed on $\widehat{L}$, then $\widehat{\omega} \cdot \sigma \cdot \widehat{\omega}^{-1}$ is fixed on $\widehat{L}^\omega$, so we have an isomorphism of $G(\widehat{L(Z)}/\widehat{L}(\mathbf{P}^1))$ to $G(\widehat{L^\omega(Z^\omega)}/\widehat{L}^\omega(\mathbf{P}^1))$.

If we identify these two groups by this isomorphism and call the resulting abstract group G, then (by an argument analogous to that above) we see that $Z^\omega \xrightarrow{\varphi(Z)^\omega} \mathbf{P}^1$ has a description of its branch cycles give by $\sigma(i, Z^\omega)$ (the branch cycle cover over $\omega(u(i,Z))$ where:

$$\sigma(i, Z^\omega) \in Con\big(\sigma(i,Z)^{-a(w)}, G\big). \tag{2.10}$$

With this we conclude the computations we need from the branch cycle argument.

4.2.2. *Finish of the proof of Theorem* (4.1) *5.1.* At the beginning of this proof we showed that $\mathbb{M}^0(Y,\varphi;r)$ has a minimal field of definition, designated $K_{\mathbb{F}}$. We finish the proof in three steps.

Step 1. *We show that $K_{\mathbb{F}}$ is a minimal field of definition of the collection $\mathbb{M}(Y,\varphi;r)$.*

Again using the proof of Lemma (**??**) 1.2, we may assume that $\mathbb{M}(Y,\varphi;r)$ is defined over a finite extension of $\mathbf{Q}$ and, for $\gamma \in G(\overline{\mathbf{Q}}/\mathbf{Q})$ we may consider $\mathbb{M}(Y,\varphi;r)^\gamma$ (the transform of the collection $\mathbb{M}(Y,\varphi;r)$. Consider $\gamma \in G(\overline{\mathbf{Q}}/K_{\mathbb{F}})$. Apply γ to:

$$\text{a) } \mathbb{F}^{\text{symm}}(Y,\varphi;r) \xrightarrow{\Phi^{\text{symm}}} \mathbb{P}(Y,\varphi;r)\times\mathbf{P}^1 \xrightarrow{\psi\times Id.} U_{\mathbf{P}^r}\times\mathbf{P}^1 \tag{2.11}$$

to obtain:

$$\text{b) } \mathbb{F}^{\text{symm}}(Y,\varphi;r) \xrightarrow{(\Phi^{\text{symm}})^\gamma} \mathcal{P}(Y,\varphi;r)^\gamma\times\mathbf{P}^1 \xrightarrow{\psi^\gamma\times Id.} U_{\mathbf{P}^r}\times\mathbf{P}^1 \tag{2.11}$$

For $\boldsymbol{p} \in \mathcal{P}(Y,\varphi;r)$, there is a unique point in $\mathcal{P}(Y,\varphi;r)^\gamma$ (denoted $\alpha(\gamma)(\boldsymbol{p}) \in \mathcal{P}(Y,\varphi;r)^\gamma$) over $\psi(\boldsymbol{p})$ such that:

$$\left(\mathbb{F}^{\text{symm}}(Y,\varphi;r)\right)_{(\boldsymbol{p})} \to (\boldsymbol{p})\times\mathbf{P}^1$$

is isomorphic to:

$$\left(\mathbb{F}^{\text{symm}}(Y,\varphi;r)\right)_{\alpha(\gamma)(\boldsymbol{p})} \to \alpha(\gamma)(\boldsymbol{p})\times\mathbf{P}^1$$

From the construction of Hurwitz families in Section 4, the map:

$$\alpha(\gamma) : \mathcal{P}(Y,\varphi;r) \to \mathcal{P}(Y,\varphi;r)^\gamma$$

is easily shown to be an analytic isomorphism. Also the maps:

$$\alpha(\gamma')\circ\alpha(\gamma)^{-1} : \mathcal{P}(Y,\varphi;r)^\gamma \to \mathcal{P}(Y,\varphi;r)^{\gamma'} \text{ for } \gamma,\gamma' \in G(\overline{\mathbf{Q}}/K_{\mathbb{F}}))$$

satisfy Weil's cocycle criteria. Therefore $\mathcal{P}(Y,\varphi;r)$ can be defined over $K_{\mathbb{F}}$. It is a cumbersome, but essentially obvious, calculation to show now that $\mathbb{M}(Y,\varphi;r)$ is defined over $K_{\mathbb{F}}$.

Step 2. *We show $K_M \subset K_{\mathbb{F}}$ and $K_{\widehat{M}} \subset \widehat{K_{\mathbb{F}}(\mathcal{P})}$.*

Suppose K_M is not contained in $K_{\mathbb{F}}$, so that $[K_M\cdot K_{\mathbb{F}} : K_{\mathbb{F}}] > 1$. Then from *Hilbert's Irreducibility Theorem* there exists a point $\boldsymbol{p}\in\mathcal{P}$, algebraic over $K_{\mathbb{F}}$, such that $K_{\mathbb{F}}(\boldsymbol{p})$ is disjoint from $K_M\cdot K_{\mathbb{F}}$ over $K_{\mathbb{F}}$. Therefore:

$$\left(\mathbb{F}^{\text{symm}}(Y,\varphi;r)\right)_{\boldsymbol{p}} \xrightarrow{\text{rest. of} P^r{}_2\circ\Phi^{\text{symm}}} \mathbf{P}^1 \tag{2.12}$$

is a cover defined over $K_{\mathbb{F}}(\boldsymbol{p})$. This contradicts that part of the *Branch Cycle Argument* which showed that any field of definition of (5.12) contains K_M.

A calculation similar to this using Lemma (**??**) 2.3 can be used to show that $K_{\widehat{M}} \subset \widehat{K_{\mathbb{F}}(\mathcal{P})}$.

Step 3. *When the Hurwitz Number is 1, $K_M = K_{\mathbb{F}}$.*

Suppose the Hurwitz Number is 1 and $K_{\mathbb{F}} \not\subseteq K_M$. Then there exists $\gamma \in G(\overline{\mathbf{Q}}, K_M)$ such that γ is *not* fixed on $K_{\mathbb{F}}$. Let $\boldsymbol{p} \in \mathcal{P}(Y, \varphi; r)$ be algebraic over $K_{\mathbb{F}}$. We apply γ to the diagram:

nh rectangular commutative diagram goes here

to obtain:

nh rectangular commutative diagram goes here

However, the last calculation of the *Branch Cycle Argument* tells us that if $\sigma(1), \dots, \sigma(r)$ are a description of the branch cycles over the cover in the left vertical in the diagram (5.13)a), then $\tau(1), \dots, \tau(r)$ is a description of the branch cycles in the cover in the left vertical diagram (5.13)b), where: $\tau(1), \dots, \tau(r)$ generates $G(\boldsymbol{g})$, and, $\tau(i)$ is conjugate to $\sigma(i)$ in $G(\boldsymbol{g})$ for $i = 1, \dots, r$. Since the Hurwitz number is 1, this implies that the cover of the left vertical diagram (5.13)b) actually appears as a fiber in the family

$$\mathbb{F}^{\text{symm}}(Y, \varphi; r) \to \mathcal{P}(Y, \varphi; r) \times \mathbf{P}^1. \tag{2.14}$$

From the uniqueness of the Symmetrized Hurwitz Family containing the cover of the left vertical of diagram (5.13)b) (under condition (5.1)), this implies that the cover:

$$(\mathbb{F}^{\text{symm}}(Y, \varphi; r))^{\gamma} \xrightarrow{(\Phi^{\text{symm}})^{\gamma}} \mathcal{P}(Y, \varphi; r)^{\gamma} \times \mathbf{P}^1$$

is isomorphic to the cover (5.14). Since γ is not fixed on $K_{\mathbb{F}}$ this contradicts the properties we have proven for $K_{\mathbb{F}}$ (it is a field of moduli for $\mathbb{M}(Y, \varphi; r)$). With this contradiction, we conclude the proof of Step 3 and of Theorem (4.1) 5.1. □

Let $Y \xrightarrow{\varphi} \mathbf{P}^1$ be a cover (as in the beginning of this section) with a description of its branch cycles given by $\sigma(1), \dots, \sigma(r)$. We do *not* assume that $Aut(Y, \varphi) = \{Id.\}$.

Corollary 4.12. *Let L be any field of definition of (Y, φ). Then $K_M \subset L$. Let $\widehat{L}$ be the algebraic closure of L in $\widehat{L(Y)}$ (the Galois closure of $L(Y)/L(\mathbf{P}^1)$). Then $K_{\widehat{M}} \subset \widehat{L}$.*

Proof. This was proven in the *Branch Cycle Argument* part of the proof of Theorem (4.1) 5.1. □

As part of Theorem (4.1) 5.1 we immediately obtain:

Corollary 4.13. *Assume in addition to the hypotheses of* Corollary 5.2 *that $Aut(Y, \varphi) = \{Id.\}$ and, the Hurwitz number of $\sigma(1), \dots, \sigma(r)$ is 1. Then the Hurwitz Parameter Space (Hurwitz scheme) $\mathcal{P}(Y, \varphi; r)$ is defined over K_M.*

Note. There are simple examples (e.g., three branch point case) to show that the cover:

$$\mathcal{P}(Y,\varphi;r) \xrightarrow{\psi} U_{\mathbf{P}^r}$$

may be defined over a field strictly contained in K_M. However, since $Aut(\mathcal{P}(Y,\varphi;r),\psi)$ is usually not the identity group, it can be a difficult problem to directly compute the 'correct' field of definition of $\mathcal{P}(Y,\varphi;r),\psi)$.

COROLLARY 4.14. *Assume that* (Y,φ) *satisfies the hypotheses of* Corollary 5.3. *Let* $K(\boldsymbol{g})$ *be the intersection of all fields of definition of all pairs* $(Z,\varphi(Z))$ *where* $Z \xrightarrow{\varphi(Z)} \mathbf{P}^1$ *has a description of its branch cycles given by* $\sigma(1),\dots,\sigma(r)$. *Then* $K(\boldsymbol{g}) = K_M$.

PROOF. For $\boldsymbol{p} \in \mathcal{P}(Y,\varphi;r)$, the cover $\mathbb{F}^{\rm symm}(Y,\varphi;r) \to \boldsymbol{p} \times \mathbf{P}^1$ (obtained from the fiber over $\boldsymbol{p}$ of $\mathbb{F}^{\rm symm}(Y,\varphi;r) \to \mathcal{P}(Y,\varphi;r) \times \mathbf{P}^1$ is defined over $K_M(\boldsymbol{p})$. From Hilbert's irreducibility theorem applied to $\mathcal{P}(Y,\varphi;r) \xrightarrow{\psi} U_{\mathbf{P}r}$ the field:

$$\bigcap_{\boldsymbol{p}\in\mathcal{P}(Y,\varphi;r)} K_M(\boldsymbol{p}) = K_M.$$

□

Let G be a finite group, and let L be a number field. We now discuss some important problems. [nh an important problem?]

PROBLEM 4.15. Show that there exists $Y \xrightarrow{\varphi(Y)} \mathbf{P}^1$ such that: (Y,φ) is defined over a number field K; $G(\widehat{Y}/\widehat{K}\mathbf{P}^1) = G$, and; $\widehat{K}$ is disjoint from L over $\mathbf{Q}$.

Consider a group G with a faithful transitive representation $T : G \to S_n$ with:

(2.15) $\qquad N\big(G(1)\big)/G(1) = \{Id.\}$ (notation of Lemma (**??**) 2.1)

Suppose we could show that:

(2.16) a) even if the Hurwitz number of $(Y,\varphi(Y))$ is *not* 1, then $\mathbb{M}(Y,\varphi;r)$ (see above) is defined over K_M, and;

b) for $\sigma(1),\dots,\sigma(r)$ (a description of the branch cycles of (Y,φ)) including all conjugacy classes of G, then $K_M(\widehat{\mathbb{F}^{\rm symm}(Y,\varphi;r)})$ (Galois closure of the cover $\mathbb{F}^{\rm symm}(Y,\varphi;r) \to \mathcal{P}(Y,\varphi;r) \times \mathbf{P}^1$) has its absolute constants equal to $\widehat{K}_M$.

Under these conditions, we can choose $\sigma(1),\dots,\sigma(r)$ so that for each integer a there exists $\beta \in S_r$ such that:

$$Con\big(\sigma(i)^a, G(\boldsymbol{g}\big) = Con\big(\sigma((i)\beta), G(\boldsymbol{g})\big) \text{ for } i = 1, \dots, r$$

(discussion before Theorem (4.1) 5.1).

Then $\widehat{K}_M = \mathbf{Q}$, and by the assumption of (5.16)b) and an application of Hilbert's Irreducibility Theorem (as in the proof of Corollary 5.3), we can affirm a positive solution to Problem 5.5 for (G, T) satisfying (5.15). However, there is no special reason at this time to believe either (5.16)a) or b).

It is an extremely important problem to consider groups G equipped with a faithful representation T for which (5.15) does not hold. In order to consider this problem, it is necessary to consider covers $Y \stackrel{\varphi}{\to} \mathbf{p}^1$ equipped with an extra structure coming from a characteristic subgroup H of $Aut(Y, \varphi)$. Suppose we are give two such structures $(Y_1, \varphi_1), H(Y_1, \varphi_1), S(Y_1))$ and $(Y_2, \varphi_2), H(Y_2, \varphi_2), S(Y_2))$ where: $S(Y_i) : H(Y_i, \varphi_i) \to H$ is an isomorphism of $H(Y_i, \varphi_i)$ with the abstract group H. We say that these two structures are isomorphic if there exists and analytic isomorphism $\alpha : Y_1 \to Y_2$ with:

nh triangular commutative diagram goes here

The construction of moduli schemes and total families analogous to the construction of $\mathcal{P}(Y, \varphi; r)$ and $\mathbb{F}^{\rm symm}(Y, \varphi; r)$ is considered in [**?**]. The search for the fields of definition of these new objects is a contribution to the extension of the results of this section to the more general class. Unfortunately, when the center of $Aut(Y, \varphi)$ is *not* the identity, there are great difficulties which require consideration of still further structure utilizing the Jacobian variety of Y.

4.2.3. *Component distinguishing moduli.* It also discusses that having several Nielsen class components raises issues on extending Nielsen class moduli to a component distinguishing moduli, to capture its corresponding moduli definition field. We have many examples of Nielsen classes having several distinct components. When $r = 3$, this seemingly happens haphazardly. Yet, when $r \geq 4$, and the braid group dominates the nature of Hurwitz spaces, most components – so far – have a natural significance for being separate from the other components. Sometimes, as happens with the Nielsen class $\mathrm{Ni}((\mathbb{Z}/\ell^{k+1})^2\mathbb{Z}/2, \mathbf{C}_{2^4})^{\rm in}$, when the spaces are recognized as modular curves (§**??**), the reason is significant but related to famous classical situations. In that particular case, all the components are conjugate through the action of a cyclotomic Galois group. We say simply, the components are conjugate. There is no chance they are going to contribute **RIGP** solutions, though they certainly contribute meaningfully, as the heart of Serre's **OIT**.

In other cases, though maybe one component separates out as defined over $\mathbb{Q}$ while others are conjugate through a more complicated action of $G_{\mathbb{Q}}$. That's what happens in both Ch. 4 and Ch. 5. In both cases the lift invariant plays a major

role. In the former it provides a result that allows every group to play a role, while the latter is our example of going beyond Serre's **OIT**.

Or perhaps, as in §**??**, where the Nielsen class is $\mathrm{Ni}(A_n, \mathbf{C}_{3^r})$, $r \geq n$, there are exactly two components, both defined over $\mathbb{Q}$, separated by a nonobvious moduli problem detected by the $\mathrm{Spin}_n \to A_n$ cover. If, for all n there are 3-cycle realizations of A_n as an **RIGP** realization, they must/would/could come from any $\mathbb{Q}$ point on one of these spaces. Since, however, there are two spaces, from which would you look? There is a clear choice, for only one of those spaces has attributes like those of the spaces $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{in}}$, extending to $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^{2^s}})^{\mathrm{in}}$, which leads directly to comparing the **RIGP** to famous conjectures on torsion on abelian varieties.

There are other examples, too, that show how the structure on cusps on our Hurwitz spaces, that inspire naming components according to attributes that come in seemingly magical ways from representations of finite groups. So, we do name them, and pose the task of finding if it always happen that there is a convenient way to attribute a moduli problem to these situations. It simplies everything to use the **BCL** and to assume that $\mathbf{C}$ forms a rational union. Then, we ask if we can identify the $G_{\mathbb{Q}}$ orbits of components on a Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$. We know we can starting with our assumption as in Ch. 4 when each conjugacy class in $\mathbf{C}$ appears sufficiently often as in (3.19).

Finding that components $\mathcal{H}''$ have different fields attached to them doesn't change the fact that the **BCL** still applies to them. Yet, if for good reasons, even though $\mathbf{C}$ is a rational, the space has a different moduli definition field $\mathbb{Q}_{\mathcal{H}''}$, it is a contributor to our understanding of where it is that those **RIGP** solutions for G are hiding.

Remark 4.16. [**CmHa85**, Prop 2.5].

4.3. Definition field examples. §4.3.1 gives examples, with fine moduli, in which both the inner and absolute **BCL** can be compared while clarifying subtleties on the meaning of the phrase *as a moduli space*.

While passing to reduced spaces doesn't change the definition field of the Hurwitz space, the fine moduli condition does. §4.3.2 augments slightly the consideration of definition field *as a moduli space*, when fine moduli doesn't hold, especially to include the reduced Hurwitz space cases.

Singular points on the moduli space, $\mathcal{M}_{\mathbf{g}}$, of genus $\mathbf{g}$ correspond to curves with extra automorphisms. For reduced Hurwitz spaces when $r > 4$, §4.3.3 introduces the elliptic fine moduli condition that, as for $r = 4$ in (2.25b), has a Nielsen class interpretation. There is no analog for $r > 4$ of b-fine moduli (2.25a).

4.3.1. *Fine* abs *and* in *examples.* Ex. 4.17 fulfills the remark after [**FrV91**, Thm. 1]. To whit: Assume $(G, \mathbf{C}, T)$ has fine moduli. Let $\mathcal{H}'$ be a component of $\mathcal{H}(G, \mathbf{C})^{\text{abs}_T}$ and $\mathcal{H}''$a component of $\mathcal{H}(G, \mathbf{C})^{\text{in}}$ over it.

Then, we can have $\mathbb{Q}_{\mathcal{H}'} = \mathbb{Q}$, but $\mathbb{Q}_{\mathcal{H}''} \neq \mathbb{Q}$. We intend Ex. 4.18 to clarify distinguishing the definition field of the Hurwitz space cover $\Phi : \mathcal{H}(G, \mathbf{C})^{\dagger} \to U_r$ from its definition as a moduli space (which includes the definition field of Φ together with structure of families of covers).

EXAMPLE 4.17 (Absolute vs Inner **BCL**). All conjugacy classes in S_n are rational. In A_n (T the standard representation), not so. For example, for n odd, there are two conjugacy classes of n cycles: C_n and $\mathrm{C}'_n = (1\,2)\mathrm{C}_n(1\,2)$. For $g \in \mathrm{C}_n$, $g^{-1} \in \mathrm{C}'$ for $n \equiv 3 \mod 4$ (but not if $n \equiv 1 \mod 4$). For n even, the same holds with conjugacy classes C_{n-1} and C'_{n-1} given by $n-1$-cycles, $n-1 \equiv 3 \mod 4$.

Take n even to match the case $\ell = 2$ in Ch. 5 §3 and $\mathbf{C}_{(n-1)^k \cdot (n-1)^{k'}}$ to be $k \geq 1$ repetitions of C_{n-1} and $k' \geq 0$ representations of C'_{n-1}. If $k > k'$, then

$$(\mathbf{C}_{(n-1)^k \cdot (n-1)^{k'}})^{-1} = (\mathbf{C}_{(n-1)^{k'} \cdot (n-1)^k})^{-1}. \tag{2.17}$$

Apply the **BCL** to conclude the diagram of (2.50), with $\dagger = \text{in}$, has definition field

$$\mathbb{Q}(A_n, \mathbf{C}) = \mathbb{Q}(\sqrt{(-1)^{\frac{n-1}{2}} n - 1}) = \mathbb{Q}(\sqrt{-(n-1)}).$$

Yet, if we add $\mod S_n$ to the right side of (2.50), conclude $\mathbb{Q}(A_n, \mathbf{C}, T) = \mathbb{Q}$.

From the extension of the Conway-Fried-Völklein-Parker lemma [**FrV91**, App.] (see §5), for k and k' both *large*, $\mathcal{H}(G, \mathbf{C})^{\text{in}}$ is irreducible. △

EXAMPLE 4.18 (Definition field as a moduli space). Take two Nielsen classes $\mathrm{Ni}(G, \mathbf{C}_i)^{\text{abs}}$, $i = 1, 2$. Suppose they have definition fields $\mathbb{Q}_{G, \mathbf{C}_i, T_i}$, $i = 1, 2$, with $\mathbb{Q}_{G, \mathbf{C}_i, T_1} = \mathbb{Q}_{G, \mathbf{C}, T_2}$ a quadratic extension of $\mathbb{Q}$. Then, it is possible that:

$$\begin{array}{c} \Phi_i : \mathcal{H}(G, \mathbf{C}_i, T_i) \to U_r \text{ are equivalent as covers, defined over } \mathbb{Q}; \\ \text{and they might even have a dense set of } \mathbb{Q} \text{ points.} \end{array} \tag{2.18}$$

Yet, according to Cor. 4.7, none of the covers in those Nielsen classes will have definition field $\mathbb{Q}$.

We will have many examples, includng for inner spaces replacing absolute spaces. Still, this example is done so explicitly in the literature, it is easy to trace any misunderstandings. It is the first discovered (family of) *Davenport polynomial pairs*. These are their specs, with $G = \mathrm{PSL}_3(\mathbb{Z}/2)$.

(2.19a) T_1 (resp. T_2) is its (degree 7) action on points (resp. lines) of $\mathbb{P}^2$.

(2.19b) $\mathbf{C}_i = \{2^3 \cdot \mathrm{C}_i\}$, $i = 1, 2$, with $\{\mathrm{C}_1, \mathrm{C}_2\}$ the two distinct 7-cycle classes in G, 2^3 indicating 3 repetitions of the involution class.

(2.19c) The corresponding Φ_i s in (2.18) are equivalent as covers of U_4.

(2.19d) The reduced Hurwitz spaces are degree 7 genus 0 covers of $\mathbb{P}^1_j$.

(2.19e) $\mathbb{Q}_{G,\mathbf{C}_i,T_i} = \mathbb{Q}(\sqrt{-7})$, the fixed field in $\mathbb{Q}(e^{\frac{2\pi i}{7}})$ of

$$\langle 3\rangle \le (\mathbb{Z}/7)^* = G(\mathbb{Q}(e^{\frac{2\pi i}{7}})/\mathbb{Q}).$$

This started in [**Fr73**]. With improved techniques it went into an exposition on the complete series of Davenport polynomial pairs in [**Fr12**, §1-4] to explain, with little abstraction, how braid monodromy works. [**CoCa99**] uses Magma to explicitly write out the equations for all 21 Davenport-pair families, still using the theory developed in [**Fr73**]. △

4.3.2. *Hurwitz spaces and stacks.* Add comments to start on the moduli structure of Hurwitz spaces even without fine moduli, addending Rem. 4.9 especially to include reduced spaces. Also, do some exposition on [**Fr77**, p. 46-48, Prop. 3] on the criterion for representing families to exist in the Zariski topology.

4.3.3. *Elliptic fine moduli on reduced spaces.* Fill out the Rem. 2.11 in terms of branch cycles as in the first Fried-Gusic etc. paper.

CHAPTER 3

The Lift Invariant and Hurwitz space components

§5 Gives one culmination of the classical period of this subject: The first structure theorem on the absolute Galois group, $\mathcal{G}_{\mathbb{Q}}$, of $\mathbb{Q}$. To show that this work had practical applications, §5.2 explains, as an immediate aftermath, undeniable strides on the **RIGP**. gives two tools – *braid action* and the **BCL**– that help us detect their definition fields and sometimes their irreducible components. §5 uses (2.1) to give precise results about the absolute Galois group, $\mathcal{G}_{\mathbb{Q}}$. §5.2 shows the previous somewhat abstract results, can be explicit in applying to the **RIGP**.

This chapter is a prelude to Part II of the paper. Comparing with the first half is akin to distinguishing monodromy of covers from monodromy of ℓ-adic representations. §2 moves to the second part by introducing (finite) groups that put the **RIGP** in a context with these topics.

(3.1a) The **RIGP** (or IGP) is not nearly done, even were it known for all simple groups (§5.2).

(3.1b) Every finite group, excluding nilpotent (see Shafarevich §5), has associated canonical ℓ-adic representations.

Recall from Cor. 4.7 the first **RIGP** needs for an **RIGP** regular realization over $K \leq \mathbb{C}$ of group G with classes $\mathbf{C}$:

(3.2a) K contains $\mathbb{Q}_{G,\mathbf{C}}$.

(3.2b) $\mathcal{H}(G,\mathbf{C})^{\text{in}}$ has at least one absolutely irreducible K component.

We apply this where $K = \mathbb{Q}$. The immediate **RIGP** application of these:

(3.3a) Conditions (3.2) are *necessary* if the ramification from $\mathbf{C}$ corresponds to even a single **RIGP** realization for G.

(3.3b) (3.2) is sufficient for a $(G,\mathbf{C})$ **RIGP** realization over K. In particular it gives such a realization if K is **PAC**.

Formulas (2.42) and (2.43) are a consequence of a formula useful for considering the definition field of a specific cover in the Nielsen class as noted in the comments of Lem. 4.1. Over $\mathbb{R}$, this gives a compact description of all real points on any Hurwitz space directly from $\mathbf{C}$ and the loci of branch points according to which are real, which fall in complex conjugate pairs [**DFr90**]. This therefore produces other necessary conditions, but again easily decided upon according to properties of $\mathbf{C}$.

1. The restricted lift invariant

First a naive version of how to effectively fulfill the basic needs of (3.2). We restrict here to being over $\mathbb{Q}$, and to inner equivalence, though, as with the **BCL** we can be precise over any (characteristic 0) field and any cover equivalence.

1.1. Commutators and Nielsen classes. Start with a rational union,

$$_*\mathbf{C} = {}_*\mathrm{C}_1, \dots, {}_*\mathrm{C}_{r^*},$$

of distinct conjugacy classes in the group G. For any vector $\boldsymbol{n} \in (\mathbb{Z}^+)^{r^*}$ consider just those *rational* conjugacy class sets of the form $_*\mathbf{C}^{\boldsymbol{n}} = {}_*\mathrm{C}_1^{n_1} \dots {}_*\mathrm{C}_{r^*}^{n_{r^*}}$. These form a semi-group under slotwise multiplication which we denote by $\mathcal{R}_{_*\mathbf{C}}$. From the branch cycle lemma, these are the classes we need to form Hurwitz space components whose points correspond to covers over $\mathbb{Q}$.

For technical reasons we also need classes not restricted to be a rational union but still supported in $_*\mathbf{C}$. Denote these $\mathcal{R}^{\mathrm{un}}_{_*\mathbf{C}}$. Assuming $_*\mathbf{C}$ fixed, regard $\mathcal{R}^{\mathrm{un}}_{_*\mathbf{C}}$ as a subset of $(\mathbb{Z}^+)^{r^*}$.

For nontrivial considerations, assume that $_*\mathbf{C}$ *generates* G.

Lem. 1.7 then guarantees that $\mathrm{Ni}(G, \mathbf{C})$ is nonempty if the multiplicity of the support of all elements in $_*\mathbf{C}$ is sufficiently high. Denote by $N_{_*\mathbf{C}}$ the least common multiple of the orders of the elements in $_*\mathbf{C}$.

Problem 1.1. Running over $\mathcal{R}_{_*\mathbf{C}}$, identify all absolutely irreducible $\mathbb{Q}$ components of $\mathcal{H}(G, {}_*\mathbf{C}^{\boldsymbol{n}})^{\mathrm{in}}$.

Again, components of $\mathcal{H}(G, {}_*\mathbf{C}^{\boldsymbol{n}})^{\mathrm{in}}$ corresponds to orbits of H_r, the Hurwitz monodromy group, on $\mathrm{Ni}(G, {}_*\mathbf{C}^{\boldsymbol{n}})$ with $r = \sum_1^{r^*} n_i$. Our treatment of the topic differs considerably from that in [**FrV91**] and [**FrV92**] to take advantage of Frattini cover insights for two reasons (see Rem. 2.1):

(3.4a) to avoid an overly restrictive topology condition on $H_2(G, \mathbb{Z})$ that G be a perfect group; and

(3.4b) to display the relation between this topic and the Modular Tower topic that is the main goal of this paper.

For $\ell \in D_G \stackrel{\mathrm{def}}{=} \{\ell \mid \ell || G|\}$, there is a *universal ℓ-Frattini cover*

$$\Psi_{G,\ell} : U_{G,\ell} \to G \text{ (§4.4):}$$

$\ker(\Psi_{G,\ell})$ is a pro-free (finitely generated), pro-ℓ group, and $\Psi_{G,\ell}$ factors through any ℓ-Frattini cover of G. The fiber product of the $\Psi_{G,\ell}$s over G, $\Psi_G : U_G \to G$, is versal for factoring (surjectively) through any Frattini cover of G (§1.3). Mod out by the commutator of $\ker(\Psi_{G,\ell})$ to get the universal abelianized ℓ-Frattini cover,

$$\Psi_{G,\ell,\mathrm{ab}} : U_{G,\ell,\mathrm{ab}} = U_{G,\ell}/[\ker(\Psi_{G,\ell}), \ker(\Psi_{G,\ell})] \to G. \tag{3.5}$$

DEFINITION 1.2. A Frattini cover, $\psi : H \to G$, is *central* if $\ker(\psi)$ is nontrivial and in the center of H. Like all Frattini covers it is a fiber product of H_ℓs over G. Denote those ℓ for which $\psi_\ell : H_\ell \to G$ is nontrivial by D^*_ψ.

Notation: The number of classes in $\mathbf{C}$ is $r_{\mathbf{C}}$; and the least common multiple of orders of elements in ${}_*\mathbf{C}$ is $N_{{}_*\mathbf{C}}$.

For $g \in G$, $\ell \in D_G$ and $(\ell, \mathrm{ord}(g)) = 1$, an elementary piece of the *Schur-Zassenhaus lemma* says a unique $\hat{g} \in H_\ell$ over g has $\mathrm{ord}(\hat{g}) = \mathrm{ord}(g)$. As Prop. 1.8 shows, this is a special case of this more general property.

DEFINITION 1.3. Refer to the class, C_g, of $g \in G$ as *liftable* (to ψ) if for $\hat{g} \in H$ over g, $|\mathrm{C}_{\hat{g}}| = |\mathrm{C}_g|$; *unliftable* if not. As ψ is central, liftability depends only on g, not on $\hat{g}$.

That is, there is *no* non-trivial (single) commutator $h\hat{g}h^{-1}\hat{g}^{-1} \in \ker(\psi)$, $h \in H$. Checking this can be nontrivial, even if you know G well.

DEFINITION 1.4. Assume all classes in ${}_*\mathbf{C}$ are liftable to ψ.

$$\text{For } \mathbf{C} \in \mathcal{R}_{{}_*\mathbf{C}} \text{ and } \boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C}), \text{ define } \hat{\boldsymbol{g}} \stackrel{\mathrm{def}}{=} (\hat{g}_1, \ldots, \hat{g}_{r_{\mathbf{C}}}).$$

For $\boldsymbol{g}$ in any braid orbit O on $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$,

$$s_\psi(\boldsymbol{g}) \stackrel{\mathrm{def}}{=} s_\psi(O) = \prod_{i=1}^{r} \hat{g}_i \stackrel{\mathrm{def}}{=} \prod(\hat{\boldsymbol{g}}) \text{ is the } \textit{restricted lift invariant}.$$

For a given $\mathbf{C}$ and $\ell \in D_G$, define

$$\mathcal{S}_{G,\mathbf{C},\psi} \stackrel{\mathrm{def}}{=} \{s_\psi(O) | \text{running over all braid orbits } O \text{ on } \mathrm{Ni}(G, \mathbf{C})\}.$$

We concentrate on a subconcern of Prob. 1.1.

PROBLEM 1.5. Say something definitive about $\mathbf{C} \in \mathcal{R}_{{}_*\mathbf{C}}$ by which we can separate braid orbits on $\mathrm{Ni}(G, \mathbf{C})$ by lift invariants.

§5.2 reminds of examples that cover much territory:

(3.6a) a solved but serious puzzle on simple branched covers;

(3.6b) how Riemann's most famous invention – half-canonical classes – arises with alternating groups; and

(3.6c) unfinished business relating regular realizations of *dihedral groups* with torsion points on hyperelliptic jacobians.

With any central Frattini extension such as ψ we use the subscript ℓ on the kernel, as in $\ker_\ell$, to indicate its ℓ-Sylow. Denote the (generated by) commutator(s) subgroup, $[H, H]$ intersected with $\ker(\psi)$ by $V_H = \prod_{\ell | \ker(\psi)} V_{\psi,\ell}$.

For C a conjugacy class in G, and $g \in \mathrm{C}$, refer to $g_u g g_u^{-1} g^{-1}$, $g_u \in G$, as a C *commutator*. Denote the group they generate, the commutator subgroup of G, by

$[G,G]$; its (maximal abelian) quotient, $G/[G,G]$, by $G_{\rm ab}$; and the canonical map $G \to G_{\rm ab}$ by $\psi_{\rm ab}$ (or if necessary to assure we are aware of G, $\psi_{G,{\rm ab}}$).

There is an analogous definition for $\mathbf{C}$ classes in G: A product of $\mathbf{C}$ commutators. Note: Prop. 1.8 distinguishes between products of commutators in V_H and a single commutator.

DEFINITION 1.6. For any $\mathbf{C}$ supported in ${}_*\mathbf{C}$ consider

$$\prod(\mathbf{C}) \stackrel{\rm def}{=} \{\prod(\boldsymbol{g}) \mid \boldsymbol{g} \in \mathbf{C}\}.$$

Refer to $\mathbf{C}$ as *satisfying product* 1 if $1 \in \prod(\mathbf{C})$. Denote the complete collection of such $\mathbf{C}$ as $\mathbf{Prod}({}_*\mathbf{C})_1$.

Note: $\mathbf{Prod}({}_*\mathbf{C})_1$ includes those $\mathbf{C}$ such that ${\rm Ni}(G,\mathbf{C})$ is a nonempty Nielsen class. Denote the latter set as ${\rm Ni}_{{}_*\mathbf{C}}$.

LEMMA 1.7. *There is a natural semi-group homomorphism, $\pi_{\rm ab}$, from $\mathcal{R}^{un}_{{}_*\mathbf{C}}$ into $G_{\rm ab}$, by $\boldsymbol{g} \in \mathbf{C} \mapsto \prod(\boldsymbol{g})$, for which $\mathbf{C} \in \mathbf{Prod}({}_*\mathbf{C})_1 \mapsto 1$.*

$$\textit{For } \mathbf{C} \in \mathbf{Prod}({}_*\mathbf{C})_1, \textit{ any } g \in \prod(\mathbf{C}) \textit{ is in } [G,G].$$

Suppose $\mathbf{C} \in \mathbf{Prod}({}_*\mathbf{C})_1$ and each class in ${}_*\mathbf{C}$ appears in $\mathbf{C}$ with sufficient multiplicity. Then, running over C' in ${}_*\mathbf{C}$:

(3.7a) $\prod(\mathrm{C}' \cdot \mathbf{C})$ *is the coset of $[G,G]$ represented by $\pi_{\rm ab}(\mathrm{C}')$; and*

(3.7b) $\prod(\mathbf{C})$ *is $[G,G]$ and $\mathbf{C} \in {\rm Ni}_{{}_*\mathbf{C}}$.*

PROOF. The range of $\pi_{\rm ab}$ is $G_{\rm ab}$, the maximal abelian quotient of G. So, the image of $\mathbf{C}$ doesn't depend on the choice of $\boldsymbol{g} \in \mathbf{C}$, or the order of elements in $\boldsymbol{g}$. Thus, it is well defined on the semigroup of elements in $\mathcal{R}_{{}_*\mathbf{C}}$. Therefore, everything in $\mathbf{Prod}({}_*\mathbf{C})_1$ is in $\ker(\pi_{\rm ab})$ and is a products of commutators.

Now, suppose $\mathbf{C} \in \mathbf{Prod}({}_*\mathbf{C})_1$. We have really established (3.7a) above. The rest of the proof is dedicated to (3.7b). Consider the results of the union of the collection $\prod(\mathbf{C})$ running over all $\mathbf{C} \in \mathcal{R}^{\rm un}_{{}_*\mathbf{C}}$ (a subset of G). If $\boldsymbol{g}_i \in \prod(\mathbf{C}_i)$, $i = 1,2$, then $\boldsymbol{g}_1 \cdot \boldsymbol{g}_2 \in \prod(\mathbf{C}_1 \cdot \mathbf{C}_2)$.

(3.8) Use that ${}_*\mathbf{C}$ generates G to conclude the complete collection is G.

Suppose there is a $\mathbf{C}$ for which $\prod(\mathbf{C})$ is $[G,G]$, or a C' in ${}_*\mathbf{C}$ for which $\mathrm{C}' \cdot \mathbf{C}$ is the $g' = \pi_{\rm ab}(\mathrm{C}')$ coset of $[G,G]$. Both cases are similar, so we assume the first. We need an estimate on the multiplicity, $v_1, \dots, v_{r_*}$, of elements in ${}_*\mathbf{C}$ that assures every element of $G_{\rm ab}$ has the form $\sum_{i=1}^{r_*} a_i u_i$, with $1 \le a_i \le v_i$, $u_i = \pi_{\rm ab}({}_*\mathrm{C}_i)$, $i = 1, \dots, r_*$. (Clearly, $v_i \le |G_{\rm ab}|$ works, but in practice you might want much better than that.)

For any $g' \in G$, $\{g' \cdot g\}_{g \in \prod \mathbf{C}}$ is a coset of $[G,G]$. Consider the multiplicity, $w_1, \dots, w_{r_*}$, of appearance of classes in ${}_*\mathbf{C}$ in $\mathbf{C}$. Then, an appropriate bound for

the multiplicities of appearance of the classes in ${}_*\mathbf{C}$ for the conclusion of in (3.7b) is given by $(w_1+v_1,\dots,w_{r_*}+v_{r_*})$. Finally, if there is no such $\mathbf{C}$ we get a contradiction to (3.8). □

Prop. 1.8 works for classical applications with G a group, as in Ex. 2.9, of which most have heard. Prop. 5.9 is general – though similar – in handling all finite groups. That forces an adjustment on the lift invariant. When we know $|V_H|$ a priori, (3.10d) is very helpful:

(3.9) that $(N_{*\mathbf{C}},|V_H|)=1$ implies ${}_*\mathbf{C}$ is liftable.

PROPOSITION 1.8. *Suppose all elements of ${}_*\mathbf{C}$ are liftable to ψ. This allows identifying the classes of ${}_*\mathbf{C}$ with classes in H. If O is a braid orbit on* $\mathrm{Ni}(G,\mathbf{C})$*, then the following hold.*

(3.10a) *The restricted lift invariant in* $\ker(\psi)$ *is independent of $\boldsymbol{g}\in O$ and distinct values in $s_{G,\mathbf{C},\psi}$ correspond to distinct braid orbits.*

(3.10b) *For $g_1',g_2'\in\prod(\mathbf{C})$, (resp. $s_1,s_2\in\mathcal{S}_{G,\mathbf{C},\psi}$), $g_1'(g_2')^{-1}$ (resp. $s_1s_2^{-1}$) is an explicit product of $\mathbf{C}$ commutators in G (resp. in H).*

(3.10c) *If* (3.9) *holds, then, all elements of ${}_*\mathbf{C}$ are liftable to ψ.*

(3.10d) *If* $\mathrm{Ni}(G,\mathbf{C})$ *is a nonempty Nielsen class (resp. $1\in\mathcal{S}_{G,\mathbf{C},\psi}$), then each $g\in\prod(\mathbf{C})$ (resp. $s\in\mathcal{S}_{G,\mathbf{C},\psi}$) is an explicit product of $\mathbf{C}$ commutators in G (resp. in H).*

(3.10e) *If all ${}_*\mathrm{C}$ in ${}_*\mathbf{C}$ appear in $\mathbf{C}$ with high multiplicity, then each $v\in\ker(\psi)$ is a product of $\mathbf{C}$ commutators and* $\ker(\psi)=S_{G,\mathbf{C}',\psi}$.

Denote the collection of orbits of $\boldsymbol{g}\in\mathrm{Ni}(G,\mathbf{C})$ for which $s_\psi(\boldsymbol{g})=1$ by Ni_1. *Then, if $\mathbf{C}$ is a rational union, $G_{\mathbb{Q}}$ permutes their corresponding components (as inner or absolute moduli spaces, Def. 4.8).*

§1.3 has the proof of Prop. 1.8, several of whose pieces will be used elsewhere. It also aids in distinctions with Prop. 5.9. It is preceeded by §1.2 on a universal construction of Frattini central extensions based on the Universal Frattini cover.

REMARK 1.9 (Lem. 1.7 explicitness). Points of explicitness start in Lem. 1.7. We can write $\prod(\boldsymbol{g})$, $\boldsymbol{g}\in\mathbf{C}$, for $\mathbf{C}$ in $\mathbf{Prod}({}_*\mathbf{C})_1$, explicitly as a product of $\mathbf{C}$ commutators (3.10d). Being explicit on the multiplicity in $\mathbf{C}$ of the classes in ${}_*\mathbf{C}$ is harder. Example: Specifically comparing production of $w_1,\dots,w_{r_*}$ with (3.8) requires producing the coset representation expressing G_{ab}. The *Todd-Coxeter* (a la Shreier's) *algorithm* suffices [**Ar91**, Chp. 6, §9], because combining branch cycles with the commutator expressions is a quotient of the free group presentation required of the algorithm.

Even more involved is how to deal, for $\mathbf{C} \in \mathrm{Ni}_{*\mathbf{C}}$, with the number and nature of braid orbits. Prop. 1.8 and Prop. 5.9 show that involves computational statements about central Frattini extensions (see §2.1).

1.2. Central Frattini covers. Recall the universal abelian ℓ-Frattini cover $\Psi_{G,\ell,\mathrm{ab}} : U_{G,\ell,\mathrm{ab}} \to G$ (from (3.5)). We use it to locate the Frattini *central* extensions of G by which we construct the lift invariant.

Form a versal central extension $R_{G,\ell}$ for Frattini central covers of G with kernel an abelian ℓ-group as follows.

(3.11a) For a maximal quotient of $\ker(\Psi_{G,\ell,\mathrm{ab}})$ with trivial G action, mod out by $W_{G,\ell} = [U_{G,\ell,\mathrm{ab}}, \ker(\Psi_{G,\ell,\mathrm{ab}})]$ on $\ker(\Psi_{G,\ell,\mathrm{ab}})$.

(3.11b) Prop. 1.8 shows elements in $W_{G,\ell}$ that are lift invariant differences come from products of commutators:

$$V_{G,\ell} = \ker(\Psi_{G,\ell,\mathrm{ab}}) \cap [U_{G,\ell,\mathrm{ab}}, U_{G,\ell,\mathrm{ab}}]/W_{G,\ell}.$$

Similarly there is a V_G. Notice that the map $\Psi_{G,\ell,\mathrm{ab}}$ restricts to send the product of all the $V_{G,\ell}$ s surjectively to V_H. The lift invariant is a tool for investigating Hurwitz space components, via ℓ-Frattini central extensions of G, to see the effect of those components for a given $\mathbf{C}$.

Definition 1.10 (Representation covers). There is a central Frattini cover $\psi_{G,\ell} : R_{G,\ell} \to G$ (resp. $\psi_G : R_G \to G$) – an ℓ-representation cover – in which $V_{G,\ell}$ (resp. V_G) is the exact kernel. Prop. 2.3 shows its existence, et. al.

Schur first showed the existence of V_G (the *Schur multiplier* of G). We see it as a maximal possible $\ker(\psi)$, ψ a central Frattini cover with commutator kernel as in Cor. 2.6. While R – a *representation cover* – does not uniquely present it unless G is perfect, Cor. 2.6 locates representation covers among all central Frattini covers.

[**Is94**, p. 118] expostulates,"We shall not attempt to expain why anyone would be interested in such a thing." We have been giving motivation for this: It immediately produces and explains many distinct Hurwitz space components, though as in §3.1.2 §3.2, not all, once we get into the territory of Serre's OIT. We have two goals for the remainder of this subsection.

Ex. 1.11 and Prop. 5.9 handle differently the mysterious, but finite (in many cases, trivial), group V_G. There are three disparate applications in which we ask about components related to lift invariants.

(3.12a) Draw precise conclusions about a natural family of (related) pairs $(G, {}_*\mathbf{C})$ running over all $\mathbf{C} \in \mathcal{R}_{*\mathbf{C}}$.

(3.12b) For each G, include all its nontrivial classes in ${}_*\mathbf{C}$.

(3.12c) Instead of changing $\mathbf{C}$, in **MT**s it makes sense to consider a natural series of groups $\{G_k\}_{k=0}^{\infty}$ covering one fixed group, $G = G_0$.

In (3.12c) we make sense of $\mathbf{C}$ not changing, though G does. In these applications the goal remains to identify components of Nielsen classes defined (as moduli spaces) over $\mathbb{Q}$. In §1.1, as with the other applications, we take a natural family of groups in (3.12c), but even there we fix $\mathbf{C}$. For the application to Thm. 5.4 and its like, given by (3.12b), it suffices to draw conclusions about components for a cofinal family of finite groups as is stated in Prop. 5.9. That is because once G is realized regularly, so is every quotient of G.

1.3. Proof of Prop. 1.8. Generating braids are in (2.10). Write $g \in \prod(\mathbf{C})$ as a product of elements in the respective conjugacy classes. Then, any braid applied to the $r_{\mathbf{C}}$ tuple, preserves the product of the entries, as we now illustrate by example. That the lift invariant is a braid invariant only needs that in H, replacing, say

$$\hat{g}_k\hat{g}_{k+1} \text{ by } \widehat{g_k g_{k+1} g_k^{-1}}\hat{g}_k$$

gives the same lift invariant. That is, $\widehat{g_k g_{k+1} g_k^{-1}} = \hat{g}_k\hat{g}_{k+1}\hat{g}_k^{-1}$: both are the same element over $g_k g_{k+1} g_k^{-1}$, the left side given by conjugating a representative of that conjugacy class through the formula $|\mathrm{C}_{\hat{g}}| = |\mathrm{C}_g|$.

There are two statements in (3.10b) acceding to similar arguments. So we just show the difference of the lift invariants of $\boldsymbol{g}, \boldsymbol{g}' \in \mathrm{Ni}(G, \mathbf{C})$ is an explicit product of $\mathbf{C}$ commutators. With no loss, as above, apply a braid to $\boldsymbol{g}'$ to assure that g_i' is conjugate to g_i, $i = 1, \dots, r$. Then, with $\mathbf{C}^{-1}$ the conjugacy classes of the inverse of the classes of $\mathbf{C}$, express their difference as the lift invariant of the juxtaposition $(\boldsymbol{g}, (\boldsymbol{g}')^{-1})$ in $\mathrm{Ni}(G, \mathbf{C}\cdot\mathbf{C}^{-1})$.

With $\hat{\boldsymbol{g}}' = (h_1\hat{g}_1h_1^{-1}, \dots, h_r\hat{g}_rh_r^{-1}), h_1, \dots, h_r \in H_\ell$, apply a sequence of braids to express the invariant differences as $\prod_{i=1}^r \hat{g}_i \cdot \prod_{i=r}^1 h_i\hat{g}_i^{-1}h_i^{-1} =$

$$\begin{array}{c}\prod_{i=1}^r \hat{g}_1h_1'\hat{g}_1^{-1}(h_1')^{-1}\cdots\hat{g}_ih_i'\hat{g}_i^{-1}(h_i')^{-1}\cdots\hat{g}_rh_r'\hat{g}_r^{-1}(h_r')^{-1}: \\ \text{a product of } \mathbf{C} \text{ commutators in } \ker(\psi).\end{array} \tag{3.13}$$

For example, $h_r = h_r'$, $h_{r-1}' = g_rh_{r-1}g_r^{-1}h_{r-1}g_rh_{r-1}^{-1}g_r^{-1}$, …, tedious, but fairly obvious. The result, in $\ker_\ell$, is a product of commutators in H_ℓ. Conversely, given (3.13), we can reverse the braids to express it as the lift invariant of two distinct braid orbits in $\mathrm{Ni}(G, \mathbf{C})$.

That finishes (3.10a) and (3.10b). For each case of (3.10d), apply (3.10b) using the hypothesized expression of 1 as $\prod(\boldsymbol{g}')$ (resp. $\prod(\hat{\boldsymbol{g}}')$) for $\boldsymbol{g}' \in \mathbf{C}$.

Now assume (3.9). Since $(|\ker(\psi)|, N_{*\mathbf{C}}) = 1$, Schur Zassenhaus says there is a unique same-order lift $g \in \mathrm{C}$ to $\hat{g} \in H$. If $h\hat{g}h^{-1}$ also lies over g, then it is the unique same order lift. So it equals $\hat{g}$, finishing (3.10c).

Now apply Lem. 1.7 to get (3.10d). Then, once we know $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$, from the Frattini property it follows that $\hat{\boldsymbol{g}} \in \mathrm{Ni}(H, \mathbf{C})$, and (3.10e) follows.

Now suppose the subset of $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ with $s_\psi(\boldsymbol{g}) = 1$ is nonempty. Relative to any classical generators, take a cover, $\hat{\varphi} : \hat{X} \to \mathbb{P}^1_z$ that represents an element in

$\mathrm{Ni}(G,\mathbf{C})_1$. Then, there is a cover $\hat{\varphi}_H : \hat{X}_H \to \mathbb{P}^1_z$ with group H that factors through $\hat{\varphi}$ and is unramified from $\hat{X}_H \to \hat{X}$. Indeed, branch cycles for $\hat{\varphi}_H$ are given by $\hat{\boldsymbol{g}}$, the lift of $\boldsymbol{g}$. The no-ramification property is a consequence of what Grothendieck called Abhyankar's Lemma. We will refer to $\hat{\varphi}_H$ later as the *Trivial Invariant lift* (of $\hat{\varphi}$).

We assumed $\mathbf{C}$ is rational union of conjugacy classes. We show, therefore, that covers having trivial lift invariant will be recognized by $G_{\mathbb{Q}}$. From the **BCL**, $\sigma \in G_{\mathbb{Q}}$ will send $\hat{\varphi}$ to an element in the same Nielsen class. That action will extend to $\hat{\varphi}_H$, including to any local parameters for ramification, preserving those ramification indices. Thus, covers in $\mathcal{H}'$ are mapped by σ into covers in $\mathcal{H}'$. A single cover in a moduli space component determines the lift (braid) invariant. That concludes the statement that the components of $\mathcal{H}'$ are mapped among themselves by $G_{\mathbb{Q}}$.

Prop. 1.8 says, assuming high multiplicity of all the support conjugacy classes from ${}_*\mathbf{C}$, we achieve all lift invariants as products of $\mathbf{C}$ commutators if and only $\pi_{\mathrm{ab}}(\mathbf{C}) = 1$. Ex. 1.11 does a special case that simplifies most of the explicitness complications of Rem. 1.9. In this example, the remaining mystery is how to directly know central Frattini covers, a problem finessed by the general lift invariant in Prop. 5.9. It also emphasizes the value for rational unions of classes to satisfy the last paragraph of Prop. 1.8.

EXAMPLE 1.11. Assume ${}_*\mathbf{C}$ is a single rational (generating) conjugacy class C of odd, d, order elements, with $(|V_G|, d) = 1$. First let $\psi_R : R \to G$ be a representation cover of G. It is a Frattini cover, and so C lifts to a generating conjugacy class in R. Therefore, for any $m \in \ker(\psi_R)$, If $r \geq r'$ by noting that we can write any integer exceeding d in the form $2a_2 + da_d$ with a_2, a_d nonnegative integers.

Indeed, take m as above, and let g be any representative of C. Write $r - r_m$ as $2a_2 + da_d$. With $(g, \ldots, g)$ the juxtaposition of g taken d times, take as a representative with lift invariant r_m the Nielsen class element

$$({}_m\boldsymbol{g}, (g, g^{-1})_{a_2}, (g, \ldots, g)_{a_d})$$

with subscripts a_2 and a_d indicating repetition. △

2. The general lift invariant

Prop. 1.8 used the restricted lift invariant, for which the assumption was that ${}_*\mathbf{C}$ is liftable. Ex. 2.9, satisfying the special case where $(N_{*\mathbf{C}}, \ker(\psi)) = 1$ for any central Frattini extension ψ of G, guided the author (see Serre's reference to our interchange in the footnote in [**Se90a**, p. 480 and Ref. 4], or [**Fr10**, Inv. Cor. 2.3]).

The difference between Prop. 1.8 and Prop. 5.9 is the removal of the liftable condition. That came through John Thompson from Conway and Parker. Völklein thought to reduce the problem to the case of one braid orbit. That, however, is

neither necessary (from the last paragraph of Prop. 1.8) nor always wise, since it removes the classical connections and applications now feasible to 1-dimensional reduced Hurwitz spaces. Even those well-acquinted with this area should be surprised at the relevance in Ex. 2.11 of the oldest example: simple branched covers of the sphere.

2.1. Commutator kernels and Schur multipliers. To define the lift invariant start with g in one of the conjugacy classes ${}_*\mathrm{C}$ in ${}_*\mathbf{C}$. Define $\hat{g}$ to be *any* lift of g to a representation cover $\psi_R : R \to G$ (or one prime at a time to $\psi_\ell : R_\ell \to G$). The big difference is that condition (3.10a) no longer holds: a difference of achieved lift invariants can be a single commutator in a representation cover $\psi_R : R \to G$ Frattini central extension. The case A_4, $\ell = 2$ starts two very different series of examples: Ex. 2.9 or Ex. 4.8.

This confounds that the lift invariant for $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ is a braid invariant. That results from $\widehat{g_k g_{k+1} g_k^{-1}} = \hat{g}_k \hat{g}_{k+1} \hat{g}_k^{-1}$ as in the proof of Prop. 1.8. To restore this formula we have only to mod out V_G or $V_{G,\ell}$ by the subgroup, $\mathrm{SC}_{*\mathbf{C}}$, generated by single commutators from ${}_*\mathbf{C}$. Since $R/\mathrm{SC}_{*\mathbf{C}} \to G$ is still a central Frattini extension, this changes almost nothing in the natural extension of Prop. 1.8 to Prop. 5.9.

Definition 2.1 (General lift invariant). Extend the lift invariant from Def. 1.4 by putting its value in $V_G/\mathrm{SC}_{*\mathbf{C}}$. We await Prop. 5.9 to find, for *each* G, a rational union $\mathbf{C}$ having

(3.14) a braid component $\mathcal{H}'$ of $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$ defined over $\mathbb{Q}$.

It is by dealing with each prime $\ell || G|$ one-at-a-time that we affect (3.4a). The Universal ℓ-Frattini cover of G in §1.2 applied in § 1.3 to see the important Frattini central extensions that give us the lift invariant. This replaced a Hopf use of a free group and a presentation of G to define $H_2(G, \mathbb{Z})$ with its motivation as a definition of a particular (group) homology group (discussion [**Br82**, p. 2]). We conclude this subsection by relating the ingredients of a long story in group theory to our considerations.

Definition 2.2. Refer to a central cover $\psi : R \to G$ as having *commutator kernel* if $\ker(\psi)$ consists of elements in $[R, R]$.

The restricted lift invariant condition applied to ψ says that $\ker(\psi)$ is not only a product of commutators, it is a product of $\mathbf{C}$ commutators, so long as these necessary conditions hold (3.10e):

(3.15a) elements of ${}_*\mathbf{C}$ appear suitably often in $\mathbf{C}$; and

(3.15b) the image of $\mathbf{C}$ in the commutator quotient of G is trivial.

That leaves us two goals for the remainder of this subsection.

(3.16a) Prop. 2.3 comments: Find a good route to explaining the Schur multiplier, in the generality required in applications.

(3.16b) Cor. 2.6 and Cor. 1.6: Exploit the universal ℓ-Frattini cover as a sometimes effective computation of lift invariants.

We apply (3.17) when G acts trivially on A in our search for central Frattini extensions of G, though it holds for any abelian G module A.

The comments explain terms, including Ext and h. Cor. 2.6 connects to primes for which G is not perfect using $H_1(G,\mathbb{Z}) = G/[G,G] \stackrel{\text{def}}{=} G_{\text{ab}}$. As in §1.1 denote the canonical map $G \to G_{\text{ab}}$ by ψ_{ab}. Ch. 6 §1.4 puts Ext in a context.

PROPOSITION 2.3. [**Sp66**, Thm. 3, Chap. 5, §5] *calls the split exact sequence* (3.17) *a universal-coefficient theorem for cohomology:*

$$0 \to \text{Ext}(H_{q-1}(G,\mathbb{Z}),A) \to H^q(G,A) \xrightarrow{h} \text{Hom}(H_q(G,\mathbb{Z}),A) \to 0. \tag{3.17}$$

Take $q = 2$ in (3.17). *Apply h to the class of an extension of G by A to produce the element of* $\text{Hom}(H_2(G,\mathbb{Z}),A)$ *that derives from it.*

The image of an extension $\psi_E : E \to G_{\text{ab}}$ realizing an element of $\text{Ext}(H_1(G,\mathbb{Z}),A)$ *defines the extension $\psi_{\text{ab}}^* : E^* \to G$ by pullback, giving the image of ψ_E in $H^2(G,A)$. Expression* (3.18) *gives this map at the cocycle level defining the cohomology classes.*

COMMENTS. Denote the q-chains over $\mathbb{Z}[G]$ by which we compute cohomology by C_q. Compute h in (3.17) by recognizing that an element of $H^q(G,A)$ is given by f in the kernel of the derivative operator applied to $\text{Hom}(C_q,A)$. Use the same chains to compute homology. Elements of $H_q(G,A')$, in the kernel of the derivative operator, have the form $\sum_i c_i \otimes a_i'$, with the c_is in C_q. Then, $\sum_i f(c_i) \otimes a_i'$ makes sense upon checking independence of f (resp. $\sum_i c_i \otimes a_i'$) modulo respective boundaries. That defines h.

While [**Br82**, p. 306] refers to the *universal coefficient theorem*, the spots those references appear – based on spectral sequences – don't use the phrase. I eventually found it buried in exercises [**Br82**, p. 60, #3]. By contrast, [**Br82**, p. 97, #7] has a long exercise on *Universal Central Extensions*.

Alas, it assumes G is *perfect* – we can't – concluding then that

$$H^2(G,A) = \text{Hom}(H_2(G,\mathbb{Z}),A) \text{ (A with trivial G action).}$$

Here the *universal coefficient* is $H_2(G,\mathbb{Z})$; or $H_2(G,\mathbb{Z})$ *represents* $H^2(G,A)$ (a functor of A). Even then, it uses another telegraphic exercise, *Yoneda's Lemma*. [**Sp66**] is about topological spaces; though [**Br82**] stresses that group cohomology extends compatibly singular cohomology of topological spaces. Cor. 2.6 refers to [**Br82**]'s, often clever, exercises.

In Brown or Spanier, Ext refers to $\text{Ext}^1_{\mathbb{Z}}$, the first Ext functor for which $\text{Ext}^1_R(M,A)$, with R modules M and A, representing classes of abelian extensions $0 \to A \to$

$E\xrightarrow{\nu}M\to 0$ with A a submodule of E. Another extension $E'\xrightarrow{\nu'}M$, with $A\le E'$, is equivalent to ν, if there is a module homomorphism $\mu: E\to E'$ with $\nu'\circ\mu=\nu$. Here we extend $G_{\rm ab}$ by A.

Now consider a cocycle $(u_1,u_2)\in G_{\rm ab}\mapsto c(u_1,u_2)\in A$ defined by an element in $\mathrm{Ext}(G_{\rm ab},A)$. It creates a new multiplication on $A\times G_{\rm ab}$:

$$(a_1,u_1)+^*(a_2,u_2)=(a_1{+}a_2+c(u_1,u_2)(a_1,a_2)\mid u_1,u_2\in G_{\rm ab},a_1,a_2\in A.$$

The key condition in defining a cocycle is that the law of addition, $+^*$ be associative. The natural map that sends the cocycle representative to a cocycle representative, $c^*(g_1,g_2)$ in $H^2(G,A)$ is given by the formula

$$c^*(g_1,g_2)(a_1,a_2)=c(\psi_{\rm ab}(g_1),\psi_{\rm ab}(g_2))(a_1,a_2). \tag{3.18}$$

Now, easily trace that the multiplication on $c^*(g_1,g_2)$ is defining the pullback. This concludes the proof. □

For M an abelian group, denote by $\Phi_{M,{\rm ab}}:\hat M_{\rm ab}\to M$ the natural profree abelian group of the same rank that covers M. The composition into ℓ components is given by $\hat M_{\rm ab}=\prod_{\ell||M|}\hat M_{\ell,{\rm ab}}$ where $\hat M_{\ell,{\rm ab}}$ is the pro-ℓ abelian group of the same rank as the ℓ component, M_ℓ, of M.

Corollary 2.4. *With M and A abelian groups, elements of $\mathrm{Ext}(M,A)$ giving abelian (so central) Frattini covers of M are quotients $\psi:E\to M$ of $\hat M_{\rm ab}\to M$ with kernel A.*

For $M=G_{\rm ab}$, and E above, the pullback of $\psi^*_{\rm ab}(E)$ of E over G (as in Prop. 2.3) is a central Frattini cover. Then, the fiber product $G\times_{G_{\rm ab}}E$ is also a central Frattini cover of G (see Rem. 2.8).

Proof. The elementary divisor theorem allows us to write M as a sum of its (cyclic) ℓ-primary parts. Since $\mathrm{Ext}(M,A)$ is an additive functor in each variable, and since Frattini covers are given by fiber products of their ℓ parts, it suffices to take $M=\mathbb{Z}/\ell^t$. Then, the abelian Frattini covers of M are $\mathbb{Z}/\ell^u$ for any $u\ge t$. Combine these over all the primary parts of M.

Now take $M=G_{\rm ab}$, and consider a nontrivial abelian Frattini cover $\psi:E\to G_{\rm ab}$ from above. The kernel of $\psi^*_{\rm ab}:G_E\stackrel{\rm def}{=}G\times_{G_{\rm ab}}E\to G$ has the form $\{(1,e)\mid e\in\ker(E\to G_{\rm ab})$. Clearly that is in the center of G_E.

Suppose G_E is not a Frattini cover of G (by projection onto the first factor). Then, some $H<G_E$ projects onto G: $\mathrm{pr}_H:H\to G$ is a cover. Then, $\ker(\mathrm{pr}_H)$ is isomorphic to $\mathbb{Z}/\ell^v$ with $v<u{-}t$. Assume E has cocycle $c:G_{\rm ab}\times G_{\rm ab}\to A$ as at the end of the proof of Prop. 2.3.

Then $\ell^v\cdot c:(u_1,u_2)\in G\mapsto\ell^v c(u_1,u_2)$ defines a nontrivial element of

$$\mathrm{Ext}(G_{\rm ab},\mathbb{Z}/\ell^{u-t-v})\text{ whose image in }H^2(G,\mathbb{Z}/\ell^{u-t-v})\text{ is trivial.}$$

Apply (3.17) with A above replaced by $A' = \mathbb{Z}/\ell^{u-t-v}$.

That says $\mathrm{Ext}(G_{\mathrm{ab}}, A') \to H^2(G, A')$ is an embedding. Here, though, the trivial element of $\mathrm{Ext}(G_{\mathrm{ab}}, A')$ and the element defined by $\ell^v \cdot c$ both go to the trivial element. Thus, $v = u-t$, and $H = G_E$ is a Frattini cover of G. That concludes the proof of the lemma. □

DEFINITION 2.5. According to (3.17), the middle term is a direct sum its left and right sides (see Rem. 2.7). Our main case is $q = 2$. It is convenient to refer to the left (resp. right) as the Ext (resp. Comm) side.

Cor. 2.6 differentiates the central *Frattini* extensions from Ext side from those from the **Comm** side. While the latter are significant in the description of the lift invariant, both play serious roles in the **OIT**. As previously, use $\psi_\ell : R_{G,\ell} \to G$ to be an ℓ-representation cover of G. Also, denote the ℓ part of G_{ab} by $G_{\mathrm{ab},\ell}$.

COROLLARY 2.6. *A central cover $\psi : H \to G$ from the* **Comm** *side is a Frattini cover. In particular, for any finite group G (resp. prime $\ell||G|$) there is a representation (resp. ℓ-representation) cover*

$$\psi_G : R_G \to G \text{ (resp. } \psi_{G,\ell} : R_{G,\ell} \to G).$$

Assume the natural cover, $\psi_{\mathrm{ab},\ell} : G \to G_{\mathrm{ab},\ell}$, splits. Further, for a choice of splitting, $\mu : G_{\mathrm{ab},\ell} \to G$, the commutation action of $\mu(G_{\mathrm{ab},\ell})$ extends to the ℓ part of a representation cover $\psi' : R_{\ker(\psi_{\mathrm{ab},\ell})} \to \ker(\psi_{\mathrm{ab},\ell})$, centralizing $\ker(\psi')$. Then the restriction of $\psi_{G,\ell}$ over $\ker(\psi_{\mathrm{ab},\ell})$ is ψ'.

PROOF. Suppose ψ is a central cover with commutator kernel, but it is not a Frattini cover. Then, their exists $H_1 < H$ for which the restriction of ψ is surjective to G. Then $H = \cup_{i=1}^t H_1 c_i$ with $t > 1$, with the c_is coset reps that centralize H_1. Thus, commutators in H have the form

$$ch_1c'h_1'(ch_1)^{-1}(c'h_1')^{-1} = h_1h_1'(h_1)^{-1}(h_1')^{-1} \text{ with } c, c' \in \ker(\psi), h_1, h_1' \in H_1.$$

This is, all commutators reside in H_1, and ψ does not have commutator kernel.

A representation cover arises by taking $A = H_2(G, \mathbb{Z})$ and the identity map in $\mathrm{Hom}(H_2(G, \mathbb{Z}), A)$. The fiber of h lying over this element then includes an element identified with 0. Once we have one representation cover, $\psi_G : R_G \to G$, and we know it is Frattini, then it has a representation as the fiber product over G of $\psi_{G,\ell} : R_{G,\ell} \to G$ where $\ker(\psi_{G,\ell})$ is the ℓ part of $\ker(\psi_G)$. Then, $\psi_{G,\ell}$ is an ℓ-representation cover of G. □

REMARK 2.7 (Direct sum in (3.17)). That the Ext and **Comm** sides are direct summands of the middle term in (3.17) is based in the proof on the choice of (coefficient) chains used. For $q = 2$ see this directly. Everything on the Ext side

is a sum of quotients from $\hat{M}_{\rm ab} \to M$. Everything on the **Comm** side is a sum of quotients of the finite representation cover.

There is no overlap between the summands on the two sides as the kernel of extensions of G, because the Ext side is a quotient of a free abelian group. A free abelian subgroup of a finitely generated abelian group automatically splits off by the *elementary divisor theorem*.

REMARK 2.8 (Fiber products vs Frattini covers). Forming a universal Frattini cover (Lem. 1.16) uses subgroups of a fiber product of two Frattini covers, H_i, $i = 1, 2$, of G. Then, a subgroup of $H_1 \times_G H_2$ that is a Frattini cover of G automatically factors surjectively through *both* H_is.

2.2. Example lift invariants vs Hurwitz components. We know $\mathbf{C}$ commutators – represented in the quotient $V_G = \prod_{\ell||G|} V_{G,\ell}$ by $\mathrm{SC}_{*\mathbf{C}}$ of Def. 2.1 – correspond to distinct braid orbits in $\mathrm{Ni}(G, \mathbf{C})$. Those modules have a description, as a quotient of $H_2(G, \mathbb{Z})$ (resp. $H_2(G, \mathbb{Z}_\ell)$) – a second *homology* group, where G has trivial action on $\mathbb{Z}$ (resp. $\mathbb{Z}_\ell$) [**Br82**, p. 2].

We achieve all such $\mathbf{C}$ commutators, given the necessary conditions, (3.15), on $\mathbf{C}$ given the following ubiquitous condition:

(3.19) Each element of ${}_*\mathbf{C}$ appears in $\mathbf{C}$ with "high" multiplicity.

The condition in this case comes from Lem. 1.7. Finite group homology and cohomology are finite groups, annihilated by $|G|$ [**Br82**, III. Cor. 10.2]. So the kernels of representation covers, and the quotients above, are bounded by invariants dependent only on G, giving a lower bound on the cardinality of braid orbits on $\mathrm{Ni}(G, \mathbf{C})$ assuming (3.19).

Further reminder: We need the definition field of Hurwitz space components corresponding to braid orbits for all applications of this paper. That leaves these goals for given G and ${}_*\mathbf{C}$.

(3.20a) When is there a $\mathbf{C}$ with support precisely in ${}_*\mathbf{C}$ with just one braid orbit on $\mathrm{Ni}(G, \mathbf{C})$ with general lift invariant 1?

(3.20b) Effectiveness 1: Assume (3.19) holds, components correspond to the general lift invariant, and we know their definition fields?

(3.20c) Effectiveness 2: Same as (3.20b) except we are either effective on (3.19) or we may drop it altogether?

2.2.1. *Examples with liftable conjugacy classes.* Theoretically, from the last paragraph of Prop. 1.8, all we need to finish Prop. 5.9 is the conclusion (3.20a) (for all G). That gives us a component of $\mathcal{H}(G, \mathbf{C})^{\rm in}$ over $\mathbb{Q}$ from the component associated with a trivial (general) lift invariant. Our examples require knowing

something about the following.

(3.21) Which elements of ${}_*\mathbf{C}$ are liftable. What is $V_G/\mathrm{SC}_{*\mathbf{C}}$?

The *spin cover*, $\psi : \mathrm{Spin}_n \to O_n(\mathbb{R})$, $n \geq 3$, of the orthogonal group – the most famous central Frattini extension – arises in quantum mechanics to the hermitian observable: *spins* of electrons around atoms. Regard $\ker(\psi)$ as $\{\pm 1\}$. The natural permutation embedding of A_n in O_n induces

$$\psi : \mathrm{Spin}_n \stackrel{\mathrm{def}}{=} \hat{A}_n \to A_n, \text{ abusing notation a little.}$$

All this section's examples, of A_n and S_n, involve the spin cover. Ex. 1.33 has more perspective using the Universal Frattini cover of A_n.

Two conjugacy classes in A_n stand out: C_3 of 3-cycles, and C_{2^2} of products of two disjoint 2-cycles. Exs. 2.9 has the case where ${}_*\mathbf{C} = \{\mathrm{C}_3\}$, a definitive answer in this case to Prob. 1.1, identifying all components by values of the restricted lift invariant. It also notes that if ${}_*\mathbf{C}$ contains C_{2^2}, then the general lift invariant (in $V_G/\mathrm{SC}_{*\mathbf{C}} = \{1\}$) must be trivial, even if $\mathbf{C}$ contains C_{2^2} only once. Exs. 2.10 notes recent results for A_n, for low values of n, allowing ${}_*\mathbf{C}$ to be arbitrary.

Example 2.9 (A_n Examples I). With the spin cover as above, [**BFr02**, Prop. 5.10] uses the Clifford algebra to conclude this. For $g \in \mathrm{C}_{2^{2s}}$ (products of $2s$ disjoint 2-cycles), any lift $\hat{g} \in \hat{A}_n$ of g has order 4 if s is odd and 2 if s is even. If $s = 1$, then, there is an $h \in \hat{A}_n$ such that $h\hat{g}h^{-1}\hat{g}^{-1}$ is the nontrivial element in $\hat{A}_n$. This follows by direct computation in A_4 using the notation of $M(x, y, z)$ from (5.5):

$$M(1,0,0)M(0,1,0)M(1,0,0)^{-1}M(0,1,0)^{-1} = M(0,0,1).$$

Use $A_4 \leq A_n$ acting on $\{1, 2, 3, 4\}$ in A_n to see this applies to C_{2^2} in any A_n. Here's what that means. Let $\mathbf{C} = \mathbf{C}_{3^{r_1}\cdot(2^2)^{r_2}}$ refer to the repetition of r_1 (resp. r_2) of C_3s (resp. C_{2^2}s) in A_n. For $r_2 \geq 1$, the general lift invariant (Def. 2) can only take the value 1 even under assumption (3.19).

If, however, $r_2 = 0$, then [**Fr10**, Main Thm.] shows the lift invariant is $(-1)^{n-1}$ starting with -1 at $n = 4$ for $r = n-1$ (covers of genus $\mathbf{g} = 0$). It assumes both values for $r \geq n$ ($\mathbf{g} > 0$), precisely distinguishing braid orbits (Hurwitz space components) of *all components* when $r_2 = 0$. One hard point:

(3.22) You can braid the outer automorphism (Rem. 3.9) from S_n.

Thus, in $\mathcal{H}(A_n, \mathbf{C}_{3^r})^{\mathrm{in}} \to \mathcal{H}(A_n, \mathbf{C}_{3^r})^{\mathrm{abs}}$, for all $r \geq n-1$, each image component has only one preimage. △

Again, under assumption (3.19), (3.22) can be applied to all finite groups in Prop. 5.9, if ${}_*\mathbf{C}$ contains all classes of G.

Alternating group examples distinguish between Hurwitz spaces of genus $\mathbf{g} = 0$ and $\mathbf{g} > 0$ covers (as in Ex.2.10). §2 compares this computation with new cases of a computable lift invariant.

EXAMPLE 2.10 (A_n Examples II). Refer to $g \in A_n$ as *pure-cycle* if it has but one disjoint cycle of length exceeding 1. When that length, l is odd, define $\omega(g) = \frac{(l-1)^2}{8}$. For a general odd order $g \in A_n$ define $\omega(g)$ as the sum over its disjoint cycle. There is a precise formula for the lift invariant in $\mathrm{Ni}(A_n, \mathbf{C})$ – in ± 1 – when $\mathbf{C}$ consists of odd order classes, and $\mathbf{g} = 0$ (absolute Hurwitz spaces) extending the case $\mathbf{C} = \mathbf{C}_{3^{n-1}}$ in Ex. 2.9:

$$s_{A_n,\mathbf{C}} = (-1)^{\sum \omega(g_i)},\ \boldsymbol{g} \in \mathrm{Ni}(A_n, \mathbf{C})\ [\mathbf{Se90a}] \text{ or } [\mathbf{Fr10}, \text{Cor. 2.3}]. \tag{3.23}$$

Def. 1.4 references a braid orbit, and a particular central Frattini cover. We assume the Spin cover. More significantly the result is independent of the braid orbit. Reference #2 in (3.23) inducts using only $\mathbf{C}_{3^{n-1}}$ modulo one case: Computing the lift invariant of $((1...k)^{-1}, (1\,2\,3), (1\,4\,5...k))$ for odd $k \geq 5$, where reference #1 uses the Clifford algebra.

[**LO08**] considered]*absolute* Hurwitz spaces with covers in $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{abs}}$ having genus 0, and pure-cycle classes: They conclude transitive braid action on Nielsen classes. That overlaps with part of the 1 braid orbit (Ex. 2.9) result for genus zero when ${}_*\mathbf{C} = \{\mathrm{C}_3\}$. [**LO08**, §5] suggests that all these Hurwitz spaces are without significant distinguishing properties.

[**Fr09**, §9], however, dispels that by considering the inner (rather than absolute) Hurwitz spaces. [**Fr09**, Prop. 5.15] uses the sh-incidence matrix to display cusps, elliptic fixed points, and genuses of the inner Hurwitz spaces in two infinite lists of [**LO08**] examples. In one there are two level 0 components (conjugate over a quadratic extension of $\mathbb{Q}$). For the other just one. These examples have seriously diverging behaviors in their associated Modular Towers, at their level 1 cusps.

Similarly, going beyond one conjugacy class, [**JMS15**] treated just A_5, but possible conjugacy class collections, $\mathbf{C}$, in that group. After an initial step of listing the nonempty Nielsen classes – mostly from checking non-negative genus from Riemann-Hurwitz – they find in each case, the lift invariant determines the orbits. They concentrated on inner Nielsen classes, the harder case, and noted (as in Ex. 2.9), the lift invariant is trivial if C_{2^2} is contained in the collection.

Respectively, Firkin and James, students of Shpectorov, did $G = A_4$ and $G = A_6$ for Nielsen classes of genus $\mathbf{g} = 0$). For genus $\mathbf{g} > 0$, but ${}_*\mathrm{C} = \{\mathrm{C}_3\}$, A_6 was a tough case in [**Fr10**] requiring special techniques. △

2.2.2. *Examples with non-liftable classes.* In S_n the standout class is C_2 of 2-cycles. Ex. 2.11, with ${}_*\mathbf{C} = \{\mathrm{C}_2\}$ reappears constantly in the literature, since its

contribution to Prob. 1.1 is so definitive: one Hurwitz space component, a generalization of the connectedness of the moduli of curves of genus g. Alas, it is totally misleading about general expectations for complicated reasons.

Despite the extremely short proof ([**Vo96**, Lem. 10.15], repeated essentially from [**BiFr86**]), this finesses that there are nontrivial central Frattini extensions. That is, it is not obvious that $V_{S_n}/\mathrm{SC}_{*\mathbf{C}} = \{1\}$. So, it must be that the class of 2-cycles, C_2 in S_n is unliftable in any nontrivial quotient of V_{S_n}. Otherwise, as in Prop. 1.8, consider $\mathbf{C}_{2^{2t}}$ denoting $2t$ repetitions of C_2. Then, for t large, a central 2-Frattini extension of S_n with commutator kernel (of order 2) would give at least two braid orbits on $\mathrm{Ni}(S_n, \mathbf{C}_{2^{2t}})$.

Prop. 5.9, (3.64a) has a general case when $V_G/\mathrm{SC}_{*\mathbf{C}} = \{1\}$, showing that every group has a finite cover, and corresponding rational classes, where this applies. Finally, Cor. 1.6 carries out, in more detail, a special case of Cor. 2.6, the start for the part of this paper that explains its title.

EXAMPLE 2.11 (Simple branching). [**Se92**, p. 97–98] lists three separate copies of $\mathbb{Z}/2$ that realize the inequivalent extensions given by $H^2(S_n, \mathbb{Z}/2)$ (2nd *cohomology* with $A = \mathbb{Z}/2$ in (3.17)), as kernels of central Frattini extensions. (Said differently.) This presentation was early in the topic of lift invariants. Its purpose there – close to the end of [**Se92**] was toward quadratic forms. I now show directly $V_{S_n}/\mathrm{SC}_{*\mathbf{C}} = \{1\}$ when ${}_*\mathbf{C} = \{\mathrm{C}_2\}$. Reason: either only single commutators appear (Def. 1.4), so C_2 is unliftable, or the lift invariant is constant on the Nielsen class.

In writing $H^2(S_n, \mathbb{Z}/2) = (\mathbb{Z}/2)^2$, there is a contribution from the Ext (left) side of (3.17), since $S_n/[S_n, S_n] = \mathbb{Z}/2$. We have already shown we don't have to deal with that for separating braid orbits. Still, this shows $(S_n, \{\mathrm{C}_2\})$ gives a mixing of the two types of central Frattini extensions. The $H_2(G, \mathbb{Z}/2)$ (right) side of (3.17) is another matter. Serre notes (from the [**Atlas**]?) that this extension is related to that we used above by restriction. By accepting facts about A_n, we can get that from just the case $n = 4$, where we also see that C_2 is not liftable.

Use the $M(x, y, z)$ matrix notation in §3. Indeed, we only need that the small Heisenberg presentation for $A_4 = (\mathbb{Z}/2)^2 \times^s \mathbb{Z}^3$ extends (as a central Frattini cover) to $S_4 = (\mathbb{Z}/2)^2 \times^s S_3$. Our action of $\mathbb{Z}/3$ on $M(x, y, z)$ leaves z untouched, and it regards (x, y) as the first two coordinates of $\mathbb{Z}^3$, acting as a cycle $(x, y, t) \mapsto (t, x, y)$ by the 3-cycle α. Then, mod out by the subspace generated by $(1, 1, 1)$. Now extend the natural permutation representation from A_4 to S_4. In this extension, an element of C_2 lifts to an element of order 2. This is an explicit description of the one case Serre doesn't do (it is useful to solve his exercise [**Se92**, 2 c), p. 98]).

We show C_2 is unliftable. Liftability means that, for $g_1 \in \mathrm{C}_2$, $|\mathrm{C}_{g_1}| = \mathrm{C}_{\hat{g}_1}$ for $g_1 \in \hat{S}_n$ over g_1. Take any $g_2 \in \mathrm{C}_2$ with support disjoint from that of g_1. It, too, will

have a well defined lift, $\hat{g}_2$. Then, $\hat{g}_1\hat{g}_2$ is a lift of g_1g_2 to $\hat{S}_n$. Consider, for $\hat{h} \in \hat{A}_n$,

$$\hat{h}\hat{g}_1\hat{h}^{-1}\hat{h}\hat{g}_2\hat{h}^{-1} \stackrel{\text{def}}{=} (\hat{g}_1\hat{g}_2)^{\hat{h}}.$$

Then, C_{2^2} would be liftable if, when $(\hat{g}_1\hat{g}_2)^{\hat{h}}$ lies over $\hat{g}_1\hat{g}_2$, then $\hat{h}\hat{g}_1\hat{h}^{-1} = \hat{g}_j$, for $j = 1$ or 2. Since this expression is true in S_n (without the ˆs), and the elements with the ˆs on them are uniquely defined, the result follows. Since the conjugacy class C_{2^2} is the same in A_n and in S_n, this gives g_1g_2 a unique lift in $\hat{S}_n$, so certainly in $\hat{A}_n$, contrary to Ex. 2.9. △

Assume G is a group for which we know the primes $\ell||G_{\text{ab}}|$ (for which G is not ℓ-perfect). As previously, we may deal one ℓ at a time for they recombine using the fiber product over G. Therefore, we also fix ℓ. In case you haven't guessed by now, the biggest mystery is what values of A, an abelian ℓ group, are sufficient to pick up ℓ-representation covers (Def. 1.10).

(3.24a) Since (3.17) is split, every ℓ central Frattini cover of G has a canonical **Comm** (which may be trivial) cover attached to it.

(3.24b) For any **Comm** cover $\psi : H \to G$, $|\ker(\psi)| = \ell^u$ is maximal value when ψ is an ℓ-representation cover.

(3.24c) As with the fundamental Frattini cover property (Lem. 1.16), the fiber product of any two central ℓ-Frattini covers $\psi_i : H_i \to G$, $i = 1, 2$, has a subcover $\psi : H \to G$ that is (central) ℓ-Frattini.

(3.24d) If ψ_1 (resp. ψ_2) is an Ext (resp. **Comm**) cover in (3.24c), both nontrivial, then H is a proper subgroup of the fiber product.

We are not likely to have a priori knowledge of u in (3.24b). So, it makes sense to take $A = \mathbb{Z}/\ell$, and deal with fiber products of the Ext and **Comm** covers associated with that choice in $H^2(G, \mathbb{Z}/\ell)$, if warranted going to higher values of u. Inside $H^2(G, \mathbb{Z}/\ell)$ any extensions (covers) would have associated factor sets, and those have an abelian group structure – can be added, another way to combine them.

§2.3 reviews an effective computation of the 1st level of the universal ℓ-Frattini cover of G in [**Fr02**, Prop. 2.8]. That can classify *Schur quotients*: central ℓ-Frattini covers of $\psi : H \to G$ with $\mathbb{Z}/\ell$ kernels. [**Fr02**, §4] generalizes Serre's example ($G = S_n$, $\ell = 2$) alluded to in Ex. 2.11 by using what happens to the order of lifts of ℓ order elements going from G to H to distinguish these Schur quotients.

2.3. Properties of ${}_\ell M_G$. Ch. 6 §1.6 shows how, in practice, properties (and proofs) in Prop. 2.18 work. It is a primer on *Loewy displays*, and how they tie irreducible representations together into (sometimes very) long chains. It also should dissuade anyone from thinking that production of characteristic ℓ-Frattini covers of, say a simple group, follows from elementary principles.

The proof of Prop. 2.18 uses Prop. 1.30, when an ℓ-Sylow of G is a normal to explicitly construct the characteristic module ${}_\ell M_G$ in all cases. To a modular representation theorist we haven't described such modules unless we have written out the Loewy display of this indecomposable module completely, as described by, say, the Heller description Prop. 2.16. Our needs are often much less. Example: Rem. 1.2 notes our concern with the appearance of $\mathbf{1}_G$ in ${}_\ell M_G$.

Recall, ${}_\ell\tilde{F}_t$ is pro-free pro-ℓ group of rank t. *Explicate* means to give the module in terms of its *Loewy decomposition* into *simple* $\mathbb{Z}/\ell[G]$ modules. Here we run into the big difference between *irreducible* (or *simple* $\mathbb{Z}/\ell[G]$ modules – no proper submodules – and indecomposable modules – no proper direct summands. Those are the same when $\ell \not| |G|$, a condition that never applies with ℓ-Frattini covers and their characteristic modules.

2.3.1. *Submodules of projective modules.* A good part of homological algebra is built on the construction of submodules of projective modules. Within that, we must distinguish when a submodule of a projective is a direct summand.

LEMMA 2.12. *A direct summand, P^*, of a project module P is projective. Consider a surjective map from a projective module $\alpha_i : P_i \to M$, $i = 1, 2$. Then:*

(3.25) *the fiber product $P_1 \times_M P_2$ is isomorphic to $P_1 \oplus \ker(\alpha_2) \equiv P_2 \oplus \ker(\alpha_1)$.*

PROOF. Consider the first sentence. Given $\alpha_{P^*} : P^* \to M$ and $\beta : N \to M$ onto morphisms, extend P^* to $\alpha_P : P \to M$ just be mapping the complement to P^* to 0. Then use projectivity of P to construct $\beta_P : P \to N$ for which $\beta \circ \beta_P = \alpha_P$. Form $\beta_{P^*} : P^* \to N$ by restricting β_P to P^* to conclude P^* is projective.

Now consider the fiber product. Since P_1 is projective, its projection to P_1 splits. The kernel of that projection is $\ker(\alpha_2)$. Combining that with the result of projection to P_2, that proves (3.25). □

Any $\mathbb{Z}/\ell[G]$ module M has a *smallest* projective cover $P \to M$. That means, for no direct summand P^* of P does its map to M go to 0. This defines

$$0 \to \Omega(M) \to P \to M \to 0. \tag{3.26}$$

Benson [**Be91**] calls this Heller's construction [**He61**]. Lem. 2.13 shows the uniqueness of $\Omega(M)$. Inductively, for $i \geq 1$, define $\Omega^i(M) \stackrel{\text{def}}{=} \Omega(\Omega^{i-1}(M))$.

All modules are finitely generated $\mathbb{Z}/\ell[G]$ modules. As already appeared in Prop. 2.3, $\mathrm{Ext}^i_G(M, N)$ and $H^{i+1}(G, N)$, even when computing the latter is the main goal, often appear together. They do so in Prop. 2.16. This follows [**Se88**] and is based on [**Fr95**, Lem. 2.3], but with many more details.

We use this to describe ${}_\ell M_G \stackrel{\text{def}}{=} {}_\ell M_{0,1}$, the characteristic $\mathbb{Z}/\ell[G]$ module, (1.10). Ch. 6 §1.4 reminds of the following topics.

(3.27a) $H^i(G,N)$ is just $\mathrm{Ext}^i(\mathbf{1},N) = \mathrm{Ext}^i_G(\mathbf{1},N)$ [**Nor62**, p. 223, Thm. 4].

(3.27b) $\mathrm{Ext}^1(M,N)$ is equivalence classes of extensions of M by N [**Nor62**, p. 129].

(3.27c) Projective and injective $\mathbb{Z}/\ell[G]$ modules are the same; a maximal simple quotient determines an indecomposable projective [**Be91**, p. 10, §1.6].

(3.27d) Resulting exact sequences of "cohomology" from applying $\mathrm{Ext}^\bullet$ (or $H^\bullet$) to a short exact sequence of modules in either slot (see (3.30)).

LEMMA 2.13. *Extension* (3.26) *canonically defines* $\alpha_M \in \mathrm{Ext}^1(M,\Omega(M))$*, uniquely up to equivalence for extensions. Similarly, there is the operator* $\Omega^{-1}(M)$*: the cokernel of the embedding of* M *in a minimal injective module. Here,* P *is a minimal injective module containing* $\Omega(M)$*.*

PROOF. Suppose P' is another projective module with the same properties. Then, their projectivity gives maps

$$\nu_{P',P} : P \to P' \text{ and } \nu_{P,P'} : P' \to P$$

each commuting with the surjective maps from P and P' to M.

Define $f = \nu_{P,P'} \circ \nu_{P',P}$ (acting on the left), and the composition of f, n times, by $f^{\circ n}$. Since $K_n \stackrel{\mathrm{def}}{=} \ker(f^{\circ n})$ is increasing with n, it stabilizes for large n.

$$\text{For such an } n \ f^{\circ n} \stackrel{\mathrm{def}}{=} F : P_n \stackrel{\mathrm{def}}{=} \mathrm{im}(f^{\circ n}) \to P_n$$

is an isomorphism. Thus,

$$P = K_n \oplus P_n : \text{ direct sum decomposition into kernel and image}$$

(as vector spaces, that happen to be G modules). As K_n – a projective summand of a projective module – goes to 0 under the map from P to M, from the minimality of P, it must be trivial. That proves f is an isomorphism defing $\Omega(M)$ uniquely.

Now apply (3.27c) to conclude P above is both the minimal projective covering M and the minimal injective containing $\Omega(M)$. □

2.3.2. *Homological characterizations of* ${}_\ell M_G$. Lem. 2.15 gives a simply-stated characterization of a Frattini cover $\psi : H \to G$ as an element $\alpha_\psi \in H^2(G,\ker(\psi))$. We put that to use in Prop. 2.16 based on the fundamental objects of modular representation theory, projective indecomposable $\mathbb{Z}/\ell[G]$ modules.

DEFINITION 2.14. An $\alpha \in \mathrm{Ext}^i(M,N)$ is *supported on* a submodule $N' < N$ if α is the image of some $\alpha' \in \mathrm{Ext}^i(M,N')$ from the natural map to $\mathrm{Ext}^i(M,N)$.[1]

The word *universal* in (3.28c) means each $\alpha \in H^2(G,N)$, not supported on a submodule of N is the image of $\alpha_{\ell\psi}$ from a homomorphism $\ker({}_\ell\psi) \to N$.

[1]The special case , for $M = \mathbf{1}_G$: $\alpha \in H^i(G,N)$: α is *supported* by $\mathbb{Z}/\ell[G]$ module $N' \subset N$ if α is the image of $\alpha' \in H^i(G,N')$ (from inclusion).

LEMMA 2.15. *As above, denote by $\alpha_\psi \in H^2(G, \ker(\psi))$ the equivalence class of the cover $\psi : H \to G$. Then ψ is a Frattini cover if and only if α_ψ is not supported on a (proper) submodule, N', of $\ker(\psi)$. This is equivalent to α_ψ does not go to 0 in $H^2(G, \ker(\psi)/N')$.*

Here are three properties of the extension ${}^1_\ell\psi : E = {}^1_\ell G \to G$.

(3.28a) *${}^1_\ell\psi$ is not supported on a submodule of $\ker({}^1_\ell\psi)$.*

(3.28b) *${}^1_\ell\psi$ is minimal among ℓ-projective covers of G with $\mathbb{Z}/\ell[G]$ kernel.*

(3.28c) *$(\ker({}^1_\ell\psi), \alpha_{{}^1_\ell\psi})$ is universal among pairs (N, α) with $\alpha \in H^2(G, N)$ not supported on a submodule of N.*

PROOF. We will use the following principle. Given a $\mathbb{Z}/\ell[G]$ module homomorphism $\mu : N' \to N$, an extension $\psi' : E' \to G$ defined by $\alpha' \in H^2(G, N')$ naturally maps to the extension defined by the image, α, of α' in $H^2(G, N)$. See this directly from the factor set $c'_e(g_1, g_2), g_1, g_2 \in G$ defined by α', Ch. 1 §1.2.2.

Recall: if $s' : G \to E'$ is a section, then with $s(g_i) = n'_i$, $i = 1, 2$,

$$s'(g_1)s'(g_2) = c'_e(g_1, g_2)s'(g_1g_2), \text{ defines } c'_e : G \times G \to N'.$$

Regard ψ' as giving a group structure on $N' \times G$ (with right action) by

$$\begin{pmatrix} g_1 & 0 \\ n'_1 & 1 \end{pmatrix}\begin{pmatrix} g_2 & 0 \\ n'_2 & 1 \end{pmatrix} = \begin{pmatrix} g_1g_2 & 0 \\ n'_1 \cdot g_2 + n'_2 + c'_e(g_1, g_2) & 1 \end{pmatrix}.$$

Then the image α is defined by the factor set

$$G \times G \to N : (g_1, g_2) \mapsto \mu(c'_e(g_1, g_2)).$$

Substitute any $(n_1, n_2) \in N \times N$ into this formula to get $\psi : E \to G$, defined by α, giving the homorphism from $E' \to E$ commuting with the maps to G.

Suppose $\psi : H \to G$ is supported on a submodule $N' < N$, by $\alpha' \in H^2(G, N')$. Then, from the above, the image of the extension, E', given by α' is a proper subgroup of H, that maps surjectively to G by ψ. Thus, ψ is not a Frattini cover.

Finally, consider the part of the exact sequence of cohomology in (3.27d) by applying $H^2(G, \cdot)$ to $0 \to N' \to N \to N/N' \to 0$. Then,

$$\alpha' \in H^2(G, N') \mapsto \alpha_\psi \in H^2(G, N) \mapsto 0 \in H^2(G, N/N'). \tag{3.29}$$

That is, the cover $E'' \to G$ with kernel N/N', from the image of α_ψ, splits the cover ψ; again a contradiction to ψ being a Frattini cover.

For (3.28b) use that ${}_\ell\tilde{\psi} : {}_\ell\tilde{G} \to G$ is universal for covers of G with profinite pro-ℓ kernel. Consider any cover $\psi_H : H \to G$ with $\mathbb{Z}/\ell[G]$ kernel. Then there is a cover $\mu : {}_\ell\tilde{G} \to H$ for which $\psi_H \circ \mu = {}_\ell\tilde{\psi}$, and μ factors through ${}^1_\ell\psi : {}^1_\ell G \to G$.

This shows ${}^1_\ell\psi$ is projective for covers to G with $\mathbb{Z}/\ell[G]$ kernel. To show it is minimal among such projective covers, assume ψ_H is projective. Then, there is $\mu' : H \to {}^1_\ell G$ that commutes with the maps to G. Again use that ${}^1_\ell G$ is Frattini to conclude μ' is surjective. So, ${}^1_\ell\psi$ is minimal in the sense of (3.28b).

The arguments above have already shown (3.28c) from the universality of $\frac{1}{\ell}\psi$ when it is combined with the characterization of Frattini covers above. □

Dimension shifting to comfort: The proof of Prop. 2.16 uses *dimension shifting* to take advantage of computing $\mathrm{Ext}^i(M,N)$ from a projective projective cover of M. We know from Lem. 2.15 that the universal $\mathbb{Z}/\ell[G]$ module N having $\alpha \in \mathrm{Ext}^2(\mathbf{1},N)$ not supported on a submodule $N' < N$ is ${}_\ell M_G$.

We now generalize this property, for a given $\mathbb{Z}/\ell[G]$ module M, to find a universal pair $(\cdot,\alpha_\cdot)$, $\alpha_\cdot \in \mathrm{Ext}^i(M,\cdot)$ when the module N put in the place holder $\cdot$ is *not* supported on a submodule. Recall (3.26):

$$\begin{array}{c} 0 \to \Omega(M) \to P \to M \to 0 \text{ defines } \alpha_{M,1} \in \mathrm{Ext}^1(M,\Omega(M)). \\ \text{Dimension shift in the } M \text{ position: } \mathrm{Ext}^i(M,N) = \mathrm{Ext}^{i-1}(\Omega(M),N). \end{array} \tag{3.30}$$ [2]

Prop. 2.16 uses both the contravariant (M) slot of $\mathrm{Ext}^\bullet(M,N)$ (here); then, in assiduously applying the definition of 'not supported" on a submodule, the covariant slot (N). We very much need both slots when we end up at the same place in a particular value $E^2(M,N)$.

PROPOSITION 2.16. *Consider the pair $(\Omega^i(M),\alpha_{M,i})$, defined from dimension shifting in* (3.30) *from $(\Omega(M),\alpha_{M,1})$ for $i \geq 1$. It has these properties.*

(3.31a) *$\alpha_{M,i}$ is not supported on a submodule of $\Omega^i(M)$ $\Leftrightarrow$ it doesn't go to 0 in a nontrivial quotient of $\Omega^i(M)$.*

(3.31b) *It is universal for elements of $\alpha \in \mathrm{Ext}^i(M,N)$ with α not defined on a submodule of N.*

In particular, identify ${}_\ell M_G$ as $\Omega^2(\mathbf{1}_G)$. It is an indecomposable module.

Iterate this to see it applies with $(G_k, M_{k,k+1})$ replacing $(G, {}_\ell M_G)$, $k \geq 0$.

PROOF. We do an induction first assuming (3.31) holds for $i = 1$:

$(\Omega(M),\alpha_{M,1})$ is not supported on a submodule, and universal.

For the induction step from $i-1$ to i, assume – for all M – that $(\Omega^{i-1}(M),\alpha_{M,i-1})$ is universal for $\alpha \in \mathrm{Ext}^{i-1}(M,N)$, for α not supported on a submodule of N.

Not-supported on a submodule hypothesis: Assume (N,α), $\alpha \in \mathrm{Ext}^i(M,N)$ is not supported on a submodule. Then, $\alpha' \in \mathrm{Ext}^{i-1}(\Omega(M),N) = \mathrm{Ext}^i(M,N)$, the image of α, is also not supported on a submodule $N' < N$. Otherwise

$$\alpha'' \in \mathrm{Ext}^i(M,N') = \mathrm{Ext}^{i-1}(\Omega(M),N')$$

would have image α in $\mathrm{Ext}^i(M,N)$, contrary to our assumption. By the induction hypothesis, $\alpha_{M,i-1} \in \mathrm{Ext}^{i-1}(\Omega(M),\Omega^i(M))$ maps to α' from some homomorphism

[2] This is the exact sequence of cohomology result whereby

$$\dots Ext^{i-1}(P,N) \to \mathrm{Ext}^{i-1}(\Omega(M),N) \to \mathrm{Ext}^i(M,N) \to \mathrm{Ext}^i(P,N) \dots$$

is exact and P is projective.

$\mu : \Omega^i(M) \to N$. Everything pulls back to Ext^i, including the homomorphism effect of μ on $\mathrm{Ext}^i(M, \Omega^i(M)) \to \mathrm{Ext}^i(M, N)$.

Conclude the universal property for i. The equivalence of the statements in (3.31a) is the exact Ext analog of the cohomology observation in (3.29).

Proof for the case $i = 1$: For the initial induction step we show $\alpha_{M,1}$:

(3.32a) $\not\mapsto 0$ in $\mathrm{Ext}^1(M, N)$ with N a nontrivial quotient of $\Omega(M)$; and

(3.32b) it is universal for $\alpha \in \mathrm{Ext}^1(M, N)$ for N unsupported on a submodule.

Suppose (3.32a) is false for $N = \Omega^1(M)/O'$. Then, if $O' \le O'' < \Omega^1(M)$, from the analog argument of (3.29), conclude $\alpha_{M,1} \mapsto 0$ in $\mathrm{Ext}(M, \Omega^1(M)/O'')$. Therefore, with no loss we may assume $\Omega^1(M)/O'' = B$ is a nontrivial simple quotient of a direct summand P' of P in the definition of $\Omega(M)$, and $P \to B$ splits. That splitting contradicts that B uniquely determines P', (3.27c).

Finally, return to $\alpha \in \mathrm{Ext}^1(M, N)$ not supported on a submodule of N, with α corresponding to the short exact sequence $N \to W \to M$. Since P is projective, the morphism $P \to M$ induces the short exact sequence $\Omega(M) \to P \xrightarrow{\tau} W$ that gives a natural diagram:

$$\begin{array}{ccccc} \Omega(M) & \longrightarrow & P & \xrightarrow{\psi} & M \\ \downarrow & & {\scriptstyle\tau}\downarrow & & || \\ N & \longrightarrow & W & \longrightarrow & M \end{array} \tag{3.33}$$

From [**Nor62**, p. 129], the exact sequence of cohomology on the covariant 2nd slot produces $\mathrm{Ext}^1(M, \Omega(M)) \to \mathrm{Ext}^1(M, N)$. The element of $\mathrm{Ext}^1(M, \Omega(M))$ defining the upper row of (3.33) maps to the element of $\mathrm{Ext}^1(M, N)$ defining the lower row of (3.33). This shows universality of the upper row extension.

Indecomposability of ${}_\ell M_G$: Take $M = \mathbf{1}_G$. In (3.28c), we have established that $\alpha_{\mathbf{1}_G,2} \in H^2(G, {}_\ell M_G)$, the universal Frattini cover with $\mathbb{Z}/\ell[G]$ kernel, is the universal object for $\mathrm{Ext}^2(\mathbf{1}_G, N) = H^2(G, N)$, the formula given by (3.27a). Therefore the above shows ${}_\ell M_G = \Omega^2(\mathbf{1}_G)$. We give two arguments for its indecomposability.

Here is a version of the argument in [**Be91**, p. 11, Exec. 1]. Up to a direct summand by a projective module, $\Omega^{-1}(\Omega(M)) = M$. Assuming M has no projective summands, since the powers of Ω are all additive operators, M is indecomposable if and only if $\Omega^1(M)$ is. Now use that, from (3.26), the operators Ω give objects minimal in the sense of having no additional projective summands. Therefore, since $\mathbf{1}_G$ is indecomposable and $\Omega^2(\mathbf{1}_G)$ has no projective summands, it is too. □

REMARK 2.17 (Significance of ${}_\ell M_G$ indecomposability). Knowing from Prop. 2.16 that ${}_\ell M_G$ is indecomposable allows displaying explicitly some of the territory that

has yet to be touched by the **RIGP**, and further, to bound and make connection to classical situations. In, however, considering its relation to the **OIT**, we do use ℓ-Frattini extensions $\psi : H \to G$ where $\ker(\psi)$ is significantly decomposable. The standout example is where we go from a sequence of ℓ-Frattini Nielsen classes $\{\mathrm{Ni}({}^{k+1}_{\ell}G, \mathbf{C})\}_{k=0}^{\infty}$ to *Jacobian* Nielsen classes (formed canonically) denoted $\{\mathrm{Ni}({}^{k+1}_{\ell}G_{jac}, \mathbf{C})\}_{k=0}^{\infty}$. This, for example, occurs in both Serre's case Ch. 6 §3.3 and in our illustrating case Ch. 5 §4, wherein the $\mathbb{Z}/\ell^k[G]$ modules in the kernel of ${}^{k+1}_{\ell}G_{jac} \to G$ are decomposable.

2.3.3. *ℓ and ℓ' elements in ${}^{k}_{\ell}G$.* There are several explicitness questions on the construction(s) in Prop. 2.16, should they be necessary to determine appropriate properties of **MT** levels. Use the notaton of Ch. 1 (1.9).

(3.34a) Can you seriously construct the modules ${}_{\ell}M_{k,k+1}(G)$, inductively?

(3.34b) Ditto for the groups ${}^{k}_{\ell}G$, at least to determine appropriate properties?

Ch. 6 Prop. 1.27 and Prop. 1.28 combined with §1.6 – to show it works – demonstrate a reasonably positive answer to both these questions. The context, though, of this book isn't to push on in this direction without a guide from the arithmetic geometry questions about Hurwitz spaces.

That is, the problem we emphasize isn't to classify the ℓ-Frattini modules. Rather, where they arise for any pair (G, ℓ), especially for G that is ℓ-perfect, they pose simply stated problems, interpreted on **MT** levels, that relate the **RIGP** and the**OIT**. These problems take advantage of the attention brought, and value adhering, to modular curves. Prop. 2.18 is the archetype of a problem that translates to group theory properties immediately applicable to **MT** levels.

Proposition 2.18 (ℓ pieces: Part 3). *The ℓ' elements generate G, if and only if, G is ℓ-perfect. If G is centerless, and ℓ-perfect, then so are ${}^{k}_{\ell}G$, and ${}^{k}_{\ell}G_{\mathrm{ab}}$, for $k \geq 0$. Further, for $g \in G$:*

(3.35a) *if $(\mathrm{ord}(g), \ell) = 1$, then g has an ℓ' lift all the way to ${}_{\ell}\tilde{G}$;*

(3.35b) *if $(\mathrm{ord}(g), \ell) = \ell$ and ${}_{k}g \in {}^{k}_{\ell}G$, (or in ${}^{k}_{\ell}G_{\mathrm{ab}}$), $k \geq 0$, lies over g, then* $\mathrm{ord}({}_{k}g) = \ell^k \cdot \mathrm{ord}(g)$

Proof. [**BFr02**, Lem. 3.19] shows that the collection of ℓ' elements generate G if and only if it is ℓ-perfect. The argument is quite simple, for ℓ' elements generate a normal subgroup of G. Then, the quotient by that subgroup must be an ℓ-group, that therefore has a $\mathbb{Z}/\ell$ quotient. Further, if G has a $\mathbb{Z}/\ell$ quotient, some lift of an order ℓ element in it is necessary to generate G.

[**BFr02**, Prop. 3.21] does the inductive argument that if ${}^{0}_{\ell}G = G$ is centerless and ℓ-perfect, then so is ${}^{k}_{\ell}G$ for all k. Assume, for our inductive hypothesis that ${}^{k}_{\ell}G$ is centerless and ℓ-perfect. Suppose $\alpha : {}^{k+1}_{\ell}G \to \mathbb{Z}/\ell$ is a cover. Then, $\ker(\alpha) \to {}^{k}_{\ell}G$

induced by the canonical map ${}^{k+1}_{\ell}G \to {}^{k}_{\ell}G$ – a Frattini cover – implies $\ker(\alpha)$, a proper subgroup of ${}^{k+1}_{\ell}G$ is not onto ${}^{k}_{\ell}G$.

Thus, $\ker(\alpha)$ has image an index ℓ normal subgroup of ${}^{k}_{\ell}G$. That gives ${}^{k}_{\ell}G$ a $\mathbb{Z}/\ell$ quotient, contrary to our assumptions. Therefore ${}^{k}_{\ell}G$ is ℓ-perfect.

Now we show ${}^{k+1}_{\ell}G$ has no center. Consider the simple module $\mathbf{1}_G = \mathbf{1}$. [**Fr95**, Lem. 5.6] characterizes that ${}^{k+1}_{\ell}G$ is centerless if (and only if):

(3.36a) ${}^{k}_{\ell}G$ has no center; and with notation of (**??**),

(3.36b) ${}_{\ell}M_{k,k+1}$ has no ${}^{k}_{\ell}G$ subquotient of Loewy type $\mathbf{1} \to \mathbf{1}$.

If a G module has Loewy type $\mathbf{1} \to \mathbf{1}$ (distinct from $\mathbf{1} \oplus \mathbf{1}$), this gives a representation of G of form $g \mapsto \left(\begin{smallmatrix} 1 & a_g \\ 0 & 1 \end{smallmatrix}\right)$. If such exists, then this gives a homomorphism, $G \mapsto \mathbb{Z}/\ell$, from $g \in G \mapsto a_g$. Apply this to ${}^{k}_{\ell}G$, which, from above, is ℓ-perfect. So (3.36b) holds. This concludes the proof of the proposition's first part.

From [**Be91**, Prop. 3.1.2], an irreducible module at the far right of the Loewy display of a principle indecomposable is also at the far left of the Loewy display. Thus **1** can't appear at the far left of the Loewy display of P either. Prop 2.7, however, says $\Omega_2(\mathbf{1}) = ker_n/ker_{n+1}$ is some part on the left of the P Loewy display. Thus **1**is not a submodule of ker_n/ker_{n+1}. Thus, the Center Hypothesis holds for ${}_1\tilde{G}$.

Assume G [**Fr95**, Lem. 3.6] has the argument that if ${}^{k}_{\ell}G = G_k$ is centerless, then so is G_{k+1}, and $\ker_k / \ker_{k+1}$ has no subquotient of Loewy type $\mathbf{1} \to \mathbf{1}$. Inductively use that if G_k is centerless, then the only way G_{k+1} can have a center is if $\mathbf{1}_{G_k}$ appears at the far left of the Loewy display of M_k.

[**FrK97**, Rem. 2.5] Gives an example of a Frattini kernel that decomposes. Frattini covers $\psi_i : H_i \to G$, $i = 1, 2$ where the H_is are simple nonisomorphic modules. Then the fiber product is still Frattini and has $\ker(\psi_1) \oplus \ker(\psi_2)$ as kernel.

Two series of simple groups agree when n = 8: A8 ?= SL(4,Z/2). Let M4 be the standard 4 dimensional representation of SL(4, Z/2). [Be] shows H 2 (A8 , M4) has dimension 1. This gives a Frattini extension of A8 not factoring through the universal central extension of A8. It is an example of the above.

This is in [Be] D. J. Benson, The Loewy structures for the projective indecomposable modules for A8 and A9 in characteristic 2, Comm. in Alg. 11 (1983), 13951451. [**FrK97**] says [Be2], the wrong reference.

Lem. 2.6 there is a one-one correspondence between simple G modules and simple ${}^{k}_{\ell}G$ modules. Also for M simple, the principle indecomposable for M as a G module is a quotient of the principle indecomposable for M as a ${}^{k}_{\ell}G$ module. Therefore expression (2.10) shows how to construct ${}^{k}_{\ell}G$ inductively as given in Prop. 2.7. Section II.E actually constructs $\tilde{A}_5$ 1 2 and this gives a posing of the questions about it, that are essentially answered in [**BFr02**].

We need to compare $\tilde{P}\times^s N_P/P$ with $\psi^{-1}(N_P)$ and $\tilde{\psi}:\ {}_\ell\tilde{G}\to G$, and to see that indecomposable for ${}_\ell M_G$, detemines it as a component of the induced from ${}_\ell M_{N_P}$. Then, for any $\mathbb{C}$ that are ℓ' classes (assume generating) then the inner Hurwitz spaces are all fine moduli. Part of it appeals to Fr95, Lem. 3.6]: G_{k+1} is centerless if G_k has no center, and $\ker_k/\ker_{k+1}$ has no subquotient of Loewy type $\mathbf{1}\to\mathbf{1}$. That module is distinct from $\mathbf{1}\oplus\mathbf{1}$ and it comes from a nontrivial representation of G_k of form $g\mapsto \left(\begin{smallmatrix}1 & a_g\\ 0 & 1\end{smallmatrix}\right)$ giving the map By hypothesis this doesn't exist. (see the rest)

RETURNM

2.4. Lift invariant effect on Definition fields. Given $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$ we compare the definition fields of the components of Hurwitz spaces with those of $\mathrm{Ni}(\hat{G},\mathbf{C})^{\mathrm{in}}$ with $\hat{G}\to G$ a central Frattini cover from the **Comm** side, as in Prop. 2.6. RETURNM

Proposition 2.19.

3. MTs and the RIGP

Most groups are neither simple nor solvable. For example, starting with any one (finite) G, ℓ-perfect and centerless, we can *canonically* create infinitely many ℓ-perfect and centerless covers of it.

All those covers give opportunities to relate the **RIGP** and the **OIT** that enhance classical results, while simultaneously posing novel problems with good prospects for technical progress.

§3.1 explains this, starting with an elementary **RIGP** success, followed by a listing of progress barriers. Modulo being ℓ-perfect and centerless, no G escapes being entwined with some of the most honored classical unsolved problems we know. §3.3 explains the main conjectures, and puts them in a context with classical diophantine conjectures.

We use the extension (3.37) to formulate a context for what is seriously unknown about the **RIGP**. That moves us away from questions that are without structure, say, about what isn't known about realizing simple groups, even in §4.2.1 where explicit Nielsen classes is the theme.

3.1. RIGP unknowns. From Ch. 1 (1.12), there is $\nu(G,\ell)>0$ and

$$\text{an extension } 1\to(\mathbb{Z}_\ell)^{\nu(G,\ell)}\to {}_\ell\tilde{G}_{\mathrm{ab}}\xrightarrow{{}_\ell\tilde{\psi}_{\mathrm{ab}}}G\to 1, \tag{3.37}$$

universal for covers of G with abelian ℓ-group kernel. Further, $\nu(G,\ell)>1$, unless G has a rank 1 normal ℓ-Sylow (Rem. 3.10).

Consider a centerless group G, a prime ℓ for which G is ℓ-perfect, and a rational union (Def. 1.4) of distinct ℓ' (generating) conjugacy classes ${}_*\mathbf{C}$. There has as yet arisen no obstruction to the following conjecture

CONJECTURE 3.1. For infinitely many $\mathbf{C}$ supported in ${}_*\mathbf{C}$ – they must be rational unions of classes from the **BCL**, Lem. 4.1 – $\mathcal{H}(G,\mathbf{C})^{\rm in}(\mathbb{Q}) \neq \emptyset$.

Generally, with K a number field containing $\mathbb{Q}_{G,{}_*\mathbf{C}}$ (from the **BCL**), the conclusion would replace $\mathbb{Q}$ in $\mathcal{H}(G,\mathbf{C})^{\rm in}(\mathbb{Q}) \neq \emptyset$ by K.

DEFINITION 3.2. From Cor. 4.7, the conclusion of Conj. 3.1 is phrased as G has infinitely many regular realizatiions supported in ${}_*\mathbf{C}$ over $\mathbb{Q}_{G,{}_*\mathbf{C}}$

Now consider the sequence of groups in (1.12):

$$ {}_\ell\tilde{G}_{\rm ab}/\ell^k V_{G,\ell} \stackrel{\rm def}{=} {}^k_\ell G_{\rm ab} \to G, k \geq 0. \tag{3.38}$$

Since ${}_*\mathbf{C}$ are ℓ' classes, Schur-Zassenhaus lifts these uniquely to ${}_\ell\tilde{G}_{\rm ab}$.

This makes sense of ${}_\ell\mathbb{H}(G,\mathbf{C})^{\rm in,rd} \stackrel{\rm def}{=} \{\mathcal{H}({}^k_\ell G_{\rm ab},\mathbf{C})^{\rm in,rd}\}_{k=0}^\infty$, a projective sequence of Hurwitz spaces. The maps between the corresponding Nielsen classes induce the Hurwitz space maps.

DEFINITION 3.3. A **M**(odular)**T**(ower) is a projective sequence of (absolutely irreducible) components $\mathbb{H}' \stackrel{\rm def}{=} \{\mathcal{H}'_k\}_{k=0}^\infty$ on ${}_\ell\mathbb{H}(G,\mathbf{C})^{\rm in,rd}$.

Actually, that is an *abelianized* **MT**. We occasionally adjust this to consider the **MT** construction under these adjustments:

(3.39a) replacing ${}^k_\ell G_{\rm ab}$ by ${}^k_\ell G$, a *full* **MT**; or

(3.39b) replacing inner classes by absolute classes, when appropriate, as under the ℓ' condition on $H \leq G$ in Prop. 1.29; or

(3.39c) dropping the extra equivalence of rd, and just considering inner or absolute **MT**s; or

(3.39d) dropping the ℓ-perfect condition on G in a special way.

Statements (3.40) combine Conj. 3.1 and the collection (3.38), toward question (3.40) about $(G,{}_*\mathbf{C})$. Use $r_{\mathbf{C}}$ as the number of classes in $\mathbf{C}$.

(3.40a) As a function of k, where might you find $\mathbf{C}_k$ supported in ${}_*\mathbf{C}$ with $\mathcal{H}({}^k_\ell G_{\rm ab},\mathbf{C}_k)^{\rm in,rd}(\mathbb{Q}) \neq \emptyset$, $k \geq 0$?

(3.40b) In (3.40a) is it possible that there might be an r_0 for which a positive conclusion holds with $r_{\mathbf{C}_k} \leq r_0$ for all k.

It seems easier to solve the **RIGP** for the collection (3.38) if the only restriction on ${}_*\mathbf{C}$ is that it be ℓ'. Even easier if we drop reference to $\mathbf{C}_k$ being, as in (3.40a), supported in ${}_*\mathbf{C}$.

Implications of (3.40)*:* Prop. 3.4 shows – with the r_0 constraint of (3.40b), but without reference to ${}_*\mathbf{C}$ – a single **MT** will have **RIGP** solutions land on each of its levels.

Again, G is centerless and ℓ-perfect, and K is a number field. We use the following with G_k either ${}^k_\ell G$ or ${}^k_\ell G_{\rm ab}$ and $\bullet$ any Nielsen class equivalence.

(3.41) Going Down: If $\mathcal{H}(G_k,\mathbf{C}_k)^\bullet(K)\neq\emptyset$. Then, the same is true of $\mathcal{H}(G_{k'},\mathbf{C}_{k'})^\bullet(K)$ with $k'\le k$ and $\mathbf{C}_{k'}$ the image classes in $G_{k'}$.

In the proofs of Prop. 3.4 and its corollaries $\hat{\boldsymbol{p}}_k$ denotes a point of $\mathcal{H}'_k(K)$, $k\ge 0$.

PROPOSITION 3.4. *Consider whether there can be any bound, r_0, for which each ${}^k_\ell G_{\rm ab}$ has a K regular realization with no more than r_0 branch points.*

If so, then there exists $\mathbf{C}$, ℓ' *classes of* G *($r_{\mathbf{C}}\le r_0$), and a* **MT**

$$\mathbb{H}'=\{\mathcal{H}'_k\}_{k=0}^\infty\subset {}_\ell\mathbb{H}(G,\mathbf{C})^{\rm in,rd} \text{ for which } \mathcal{H}'_k(K)\neq\emptyset, k\ge 0. \tag{3.42}$$

PROOF. There are only finitely many Nielsen classes $\mathrm{Ni}(G,\mathbf{C})$ with $r_{\mathbf{C}}\le r_0$. The **RIGP** realization assumption implies there are infinitely many pairs $({}^k_\ell G_{\rm ab},\mathbf{C}_k)$ for which: $\mathcal{H}({}^k_\ell G_{\rm ab},\mathbf{C}_k)^{\rm in}(K)\neq 0$, $r_{\mathbf{C}_k}\le r_0$, and a component $\mathcal{H}'_k$ of $\mathcal{H}({}^k_\ell G_{\rm ab},\mathbf{C}_k)^{\rm in}$ with a K point, also defined over K (the comments (2.52) and (2.53)). There are two possible cases:

(3.43) $\mathrm{S}_{\ell'}$: Infinitely many $\mathbf{C}_k$ consist of ℓ' classes; or S_ℓ: Not $\mathrm{S}_{\ell'}$.

First assume $\mathrm{S}_{\ell'}$, and restrict consideration to just those cases where $\mathbf{C}_k$ is ℓ'. Then (from Schur-Zassenhaus as previously), we may assume $\mathbf{C}_k$ is the canonical lift of some $\mathbf{C}'_k$ collection of ℓ' classes in G. There are only finitely many such. Without loss, there exists infinitely many ℓ' collections $\mathbf{C}_k$, $k\in I$, all lying over the same $\mathbf{C}'$ collection of classes in G.

So, $\{\mathcal{H}'_k\}_{k\in I}$ is a cofinal collection of K components of $\{\mathcal{H}(G_k,\mathbf{C}')^{\rm in}\}_{k=0}^\infty$ containing K points. Apply (3.41) to replace $k\in I$ by $k\ge 0$. Such components form a system, finite but nonempty at each level. By the Tychonov Theorem, that implies there is a projective system of such components.

That gives an inner **MT**. To get a **MT** of reduced spaces, just apply reduced equivalence, whereby K components and points are mapped (resp.) to K components and points. To complete the proof of (3.42), we have only to show that S_ℓ is not possible. The original argument is [**FrK97**, Lem. 4.1 combined with Thm. 4.4]. We give a variant on this.

Whatever are the realizations of ${}^k_\ell G_{\rm ab}$, as a function of k, there must be infinitely many that accumulate over a particular Nielsen class $\mathrm{Ni}(G,\mathbf{C})$ using (3.41). Each such realization, say of ${}^k_\ell G_{\rm ab}$ – for which, compatible with previous notation, we use the symbol $\hat{\boldsymbol{p}}_k$ – lies on a Hurwitz space component of a Nielsen class $\mathrm{Ni}({}^k_\ell G_{\rm ab},\mathbf{C}_{\hat{\boldsymbol{p}}_k})^{\rm in}$ with at most r_0 classes in $\mathbf{C}_{\hat{\boldsymbol{p}}_k}$.

We are assuming $S_{\ell'}$ doesn't hold. So, again conclude from (3.41), with no loss, there is a k_0 with none of $\mathbf{C}_{\hat{\boldsymbol{p}}_k}$ or its images in ${}^{k'}_{\ell}G_{\rm ab}$ being ℓ' for $k \geq k' \geq k_0$. Again applying the Tychonov Theorem, we find a projective sequence of conjugacy classes, $\{\mathbf{C}'_k \stackrel{\rm def}{=} \mathbf{C}'_{\hat{\boldsymbol{p}}_k}\}_{k=k_0}^{\infty}$, with these properties:

(3.44a) one of the $\mathbf{C}'_k$, say, C'_k has elements of order divisible by ℓ;

(3.44b) giving a projective sequence of $\mathfrak{g}= \{g'_k \in \mathrm{C}'_k\}_{k=k_0}^{\infty}$ with $\ell|\mathrm{ord}(g_k)$.

The proof of the proposition will follow if we show (3.45b).

(3.45a) For $k \geq k_0$, $\mathrm{ord}(g'_{k+1}) = \ell \cdot \mathrm{ord}(g'_k)$.

(3.45b) The definition field of a component containing $\hat{\boldsymbol{p}}_k$ grows with k.

Apply (3.35b) to conclude (3.45a). Now we use that by applying the **BCL** Cor. 4.7 to show (3.45b). A cover, $\hat{\boldsymbol{p}}_k \in \mathrm{Ni}({}^{k}_{\ell}G, \mathbf{C}_k)$, to be defined over K requires $K \geq \mathbb{Q}_{{}^{k}_{\ell}G, \mathbf{C}_k}$. So, $[\mathbb{Q}_{{}^{k}_{\ell}G, \mathbf{C}_k} : \mathbb{Q}] \leq [K : \mathbb{Q}]$. Also, $\mathbf{C}_k^m = \mathbf{C}_k$ if and only if $m \in (\mathbb{Z}/N_{\mathbf{C}_k})^*$ is fixed on $\mathbb{Q}_{{}^{k}_{\ell}G, \mathbf{C}_k}$.

Yet, elements $g'_k \in \mathrm{C}'_k$ have order $\mathrm{ord}(g'_{k_0}) \cdot \ell^{k-k_0}$. Since $\ker({}^{k}_{\ell}G_{\rm ab} \to G)$ is abelian, The number of conjugates of g'_k cannot exceed those of its image, g'_0, in G_0. RETURNM

Therefore, the number of distinct classes among the powers of $(g'_k)^m$ with m running over a finite set of cosets grows with k, eventually exceeding the bound r_0 on the total allowable conjugacy classes in $\mathbf{C}_k$. This concludes the proof of (3.45b), and thereby the proposition. □

Corollary 3.5. *Continue the notation of Prop. 3.4 and consider the* **MT** $\{\mathcal{H}'_k\}_{k=0}^{\infty}$ *produced there.*

(3.46a) *There is no projective system* $\{\hat{\boldsymbol{p}}_k\}_{k=0}^{\infty}$ *of* K *points on* $\{\mathcal{H}'_k\}_{k=0}^{\infty}$.

(3.46b) *Further, there can be no* k_0 *for which* $|\mathcal{H}'_{k_0}(K)| < \infty$.

In particular, if $r_{\mathbf{C}} \leq 4$, *high levels of* ${}_{\ell}\mathbb{H}(G, \mathbf{C})^{\rm in,rd}$ *have no* K *points.*

§3.2 starts with two, simply-stated, classically motivated, examples that show what Prop. 3.4 is about. More than that, we find essentially every ℓ-perfect finite group has a version of this.

In the proof of Prop. 3.4, we considered one prime ℓ for which G is ℓ-perfect, and found if we had a prayer to bound number of branch points of the collection of extensions, then eventually we could deal with one ℓ' collection of classes $\mathbf{C}$ for all k, and the corresponding $\mathbb{Q}$ points would fall on the levels of one **MT** for $(G, \mathbf{C})$. Immediately that raises a bunch of issues.

Remark 3.6 (Two primes ℓ_1, ℓ_2). Suppose G is ℓ_i-perfect, $i = 1, 2$. Then, the version of Prop. 3.4 for both primes would ask how to simultaneously locate one such $\mathbf{C}$ with which we could find ${}^{k_1}_{\ell_1}G \times_G {}^{k_2}_{\ell_2}G$, for all (k_1, k_2). RETURNM

REMARK 3.7 (Bounded def. fields on **MT**s). Let K be a number field. For a(n abelianized) **MT** to have K points at all levels, there must be a uniform bound on the definition fields of all levels of the **MT** $\mathbb{H}'$. We know how to find a cyclotomic field that includes the definition field of all levels of ${}_\ell\mathbb{H}(G,\mathbf{C})^{\mathrm{in,rd}}$. The problem is we need a **MT** whose (absolutely irreducible) component levels have a number field definition bound. Yet, as we see clearly later, many **MT**s have no such bounding definition field. So, it is valuable to know that for a given (G,ℓ) we can explicitly find many $(G,\mathbf{C},\ell)$ for which there are such **MT**s. RETURNM

3.2. Context for Prop. 3.4. Conj. 3.8, the Main **MT** conjecture says (3.42) is impossible. Subex.: Even for $G = A_5$, where $\nu(G,2) = 5$, for no $k > 0$ has

$$ {}_2\tilde{A}_{5,\mathrm{ab}}/2^k \ker({}_\ell\tilde{\psi}_{\mathrm{ab}}) = {}^k_2A_{5.\mathrm{ab}} $$

been realized (regularly or not) over $\mathbb{Q}$.

Assume r conjugacy classes, $\mathbf{C}$ of G; all containing elements of order ℓ'. Also, do the dihedral group example, and turn back to the previously dihedral examples to figure out what you want to say about the characteristic ℓ-Frattini you care about.

3.2.1. *The Main Conjecture.*

CONJECTURE 3.8. High **MT** tower levels have *general type* and no $\mathbb{Q}$ points. A special case (joint with Pierre Debes) is $G = D_\ell$, ℓ an odd prime. That interprets as existence of ℓ^{k+1} cyclotomic points for each k, on hyperelliptic jacobians of a fixed dimension d (independent of k, but the Jacobian may change with k).

Thm:[Outlined in [**Fr06**]] The Main Conjecture is true for $r = 4$, based on the genus formula and methods for distinguishing different types of cusps. It suffices to show the genus rises with the **MT** levels.

[**CaTa09**] proved the disappearance of rational points at high levels, without engaging the reduced Hurwitz spaces or their cusps. [**CaD09**] showed the Torsion Conjecture on abelian varieties $\implies$ $\mathbb{Q}$ statement of the Main Conjecture in general.

We state Lem. 3.9 with the universal Frattini covers of G and H, but the same results hold by replacing them by their abelianized versions (for example, ${}^k_\ell G$ by ${}^k_\ell G_{\mathrm{ab}}$, and ${}^\ell_k H$ by ${}^\ell_k H_{\mathrm{ab}}$). Let P_ℓ be an ℓ-Sylow of G, and $M_{0,1}(G) = M(G)$ the characteristic ℓ-Frattini module.

LEMMA 3.9. *For $H \le G$, ${}_\ell\tilde{H}$ embeds in ${}_\ell\tilde{G}$. Further, for each $k \ge 0$, ${}^k_\ell H$ naturally embeds in ${}^k_\ell G$. If $\mathrm{rk}(M_{1,0}(W)) = \mathrm{rk}(M_{1,0}(G))$, then ${}_\ell\tilde{W}$ appears from the universal ℓ-Frattini cover $\tilde{\varphi} : {}_\ell\tilde{G} \to G$ as $\tilde{\varphi}^{-1}(W)$.*

For $H = N_G(P_\ell)$ this applies if $\mathrm{rk}(P_\ell) = \mathrm{rk}(M(G))$.

PROOF. The Sylow Theorems say an ℓ-Sylow of ${}_\ell\tilde{G}$ contains an ℓ-Sylow of $\tilde{\varphi}^{-1}(W)$. So, the latter is profree, which is now a closed subgroup of a profree

group of finite index, so profree. Prop. 1.30 characterizes ${}_\ell\tilde{W}$ as the minimal cover of W with pro-free ℓ-Sylow.

That implies there is a natural map $\gamma_W : \tilde{\varphi}^{-1}(W) \to {}_\ell\tilde{W}$ commuting with the map to W. As ${}_\ell\tilde{W}$ is an ℓ-Frattini cover of W, the map must be surjective. Since the natural map $\tilde{\varphi}^{-1}(W) \to W$ has a pro-ℓ group as kernel, the natural map ${}_\ell\tilde{W} \to W$ produces $\psi_W : {}_\ell\tilde{W} \to \tilde{\varphi}^{-1}(W)$ commuting with the projections to W.

The composition $\gamma_W \circ \psi_W$ (commuting with the projections to W) is an endomorphism of ${}_\ell\tilde{W}$. The image of $\gamma_W \circ \psi_W$ is a closed subgroup of ${}_\ell\tilde{W}$ mapping surjectively to W. Again, from the Frattini property, $\gamma_W \circ \psi_W$ is onto. An onto endomorphism of finitely generated profinite groups is an isomorphism [**FrJ86**, Prop. 15.3]$_1$. In particular, ψ_W is an injection.

The characteristic quotients have maps between them induced by ψ_W, and W_k injects into G_k, inducing an injection of

$$\ker_k(W)/\ker_{k+1}(W) \to \ker_k(G)/\ker_{k+1}(G).$$

If (for $k = 0$), $M(W)$ and $M(G)$ have the same dimension, they are isomorphic. These groups characterize $\ker_0(W)$ and $\ker_0(G)$. That implies they are equal, giving an isomorphism of $\ker_0(H)$ and $\ker_0(G)$ in the special case. □

Let $O_{\ell'}(G)$ be the maximal ℓ' normal subgroup of any finite group G. Prop. 3.10, uses the following designations: an ℓ-Sylow of G is P_ℓ; its universal ℓ-Frattini is $\tilde{P}_\ell$, and the rank of either is $\mathrm{rk}_\ell \stackrel{\text{def}}{=} \mathrm{rk}_{G,\ell}$. It characterizes when the characteristic ℓ-Frattini module of G has rank 1; at its core it is a rather clear generalization of our beginning case, where $G = \mathbb{Z}/\ell^{k+1} \times^s \mathbb{Z}/2$.

Assume, as often, that G is ℓ-perfect, but see Rem. 3.13.

PROPOSITION 3.10 ($\nu(G,\ell) = 1$). *Schreier's formula* (1.7b) *implies the rank of* $\ker(\tilde{P}_\ell \to P_\ell)$ *is* $1+|P_\ell|(\mathrm{rk}_\ell - 1)$.

If P_ℓ is normal then, this is the correct rank of $\ker({}_\ell\tilde{G} \to G)$ *(Prop. 1.30), and therefore of* $\ker({}_\ell\tilde{G}_{\mathrm{ab}} \to G)$*, say, from Lem. 3.9. That leaves* $\mathrm{rk}_\ell = 1$ *(cyclic ℓ-Sylow) as the only possibility that $\nu(G,\ell) = 1$. Then, $\nu(G,\ell) = 1$ if and only if:*

$$P_\ell = \mathbb{Z}/\ell^t \text{ is normal; and } G/O_{\ell'}(G) \le \mathbb{Z}/\ell^t \times^s (\mathbb{Z}/\ell)^*. \tag{3.47}$$

In analogy to $O_{\ell'}(G)$, denote the maximal normal ℓ-subgroup of G by $O_\ell(G)$. That is, $G/O_\ell(G/O_{\ell'}(G)) \stackrel{\text{def}}{=} G_{\text{ mod } \ell', \text{ mod } \ell}$ results from: mod out G by a maximal normal ℓ' part; then, mod out by the maximal normal ℓ part.

DEFINITION 3.11. We say G is ℓ-supersolvable if $G_{\text{ mod } \ell', \text{ mod } \ell}$ is abelian of exponent dividing $\ell-1$.[3]

[3] G is *supersolvable* if a chain of subgroups

$$G = G_u > G_1 > \cdots > G_1 > 1 = G_0 \text{ has } G_i \text{ normal in } G$$
$$\text{with } [G_{i+1} : G_i] \text{ prime, } 0 \le i \le u-1 \text{ [**Is94**, p. 102].}$$

EXAMPLE 3.12. Consider ${}_\ell G = (\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/3$, with prime $\ell \neq 3$ as in Ch. 5 Def. 3.1. Then, ${}_\ell G$ is ℓ-supersingular if and only if $3|\ell-1$ which is the exact condition that $(\mathbb{Z}/\ell)^2$ is a direct sum of two distinct $\mathbb{Z}/\ell$ modules. $\triangle$

REMARK 3.13 (Continue Prop. 3.10). Without assuming G is ℓ-perfect, [**GS78**] characterizes $\nu(G,\ell) = 1$. Then, G is ℓ-supersolvable with a cyclic ℓ-Sylow. We used that the ℓ-Frattini extension captures the characteristic module, when it need not contend with the Ext side of the Universal Coefficient Theorem, Def. 2.5.

REMARK 3.14. Cyclic ℓ-Sylow itself is far from giving $\dim(M_{0,1}) = 1$. For example, A_5 has a cyclic 5-Sylow, though, ${}_5M_{0,1}(A_5)$ has dimension 6 (Ch. 6 §1.6 or [**Fr95**, Prop. 2.4]). Its Loewy display has one copy of the adjoint representation of $\mathrm{PSL}_2(\mathbb{Z}/5) = A_5$ on top of another. Each A_n, $n \geq 5$, has a cyclic ℓ-Sylow (say, $\ell > n/2$ a prime) with $\nu(G,\ell) > 1$.

REMARK 3.15 (Addendum to Dihedral Ex. Ch. 2 §3.2). We excluded, for the moment, $\ell = 2$ in considering ${}_\ell M_G$ with $G = D_{\ell^{k+1}}$. §3.3.3, however, includes it.

3.3. Including both G and C in the RIGP. Much of the **RIGP** treatment in [**FrJ86**] is dedicated to showing how far elementary considerations about groups can extend. Here we introduce just how close are two situations:

(3.48a) Elmentary group situations that do allow **RIGP** solutions; and

(3.48b) situations that face unsolved problems in classical arithmetic situations.

§3.3.1 includes some principles that have general use in dealing with Galois group realizations. §3.3.2 compares and enhances observations made in $[\mathbf{FrJ86}]_2$ and in [**Se92**]. Then, §3.3.3 puts those easy dihedral group regular realizations in a generalizing context, producing affine group regular realizations more advanced than first year graduate algebra Galois realizations of dihedral groups. It concludes with general classical unsolved problems that don't seem **RIGP** related at all.

3.3.1. *Using wreath products.* We simplify the proof of $[\mathbf{FrJ86}, \text{Prop. } 16.4.4]_2$, mostly due to [**Ik**], in Prop. 3.17.

DEFINITION 3.16. Suppose H is the Galois group of an extension M_1/N over a field K. We say this realization *extends* to a cover $\psi : G \to H$ – not necessarily a semidirect product – if we realize G as the group of an extension M_2/N that identifies M_1 as the fixed field of $\ker(\psi)$.

We may qualify realizations and extensions with adjectives, as we choose. For example, by saying the realizations are regular, or the extensions are split (or Frattini) as we do in Prop. 3.17. §3.3.2 says considerable about the techniques in (3.50) and the significance of their conclusions. Below assume K is an Hilbertian field.

PROPOSITION 3.17. *Suppose there is a K regular realization of H, with H acting on a finite abelian group A. Then the regular realization of H extends to a K regular realization of $A \times^s H$.*

PROOF. The wreath product – Ch. 6 §1.2.1 – explains this with these changes in notation for a right-hand action: $H \mapsto A$, $G \mapsto H$, and $n \mapsto |H|$ for the regular representation. We deal with the subgroup $A \wr H = A^n \times^s H$ of $A^n \times^s S_n$ with $h \in H$ acting on the letters $\{h_1, \dots, h_n\}$ of S_n by multiplication on the right: $h_i \mapsto h_i h$. With $(a_{h_1} \dots, a_{h_n}) \stackrel{\text{def}}{=} \boldsymbol{a} \in A^n$ denote elements of $A \wr H$ as $\left(\begin{smallmatrix} h & 0 \\ (a_{h_1}, \dots, a_{h_n}) & 1 \end{smallmatrix}\right)$.

Use the matrix multiplication of §1.2, as in Ch. 6 §1.2.1. For $h' \in H$ and $h_j = h_i h'$, then the h_j coordinate of $\boldsymbol{a} * h'$ is a_{h_i}.

Getting an $A \times^s H$ quotient: Now we show $A \times^s H$ is a quotient of $A \wr H$ given by

$$\left(\begin{smallmatrix} h & 0 \\ \boldsymbol{a} & 1 \end{smallmatrix}\right) \xrightarrow{\alpha} \left(\begin{smallmatrix} h & 0 \\ \sum_i (a_{h_i}) h_i \stackrel{\text{def}}{=} \alpha(\boldsymbol{a}) & 1 \end{smallmatrix}\right), \tag{3.49}$$

with the lower left term – as A is abelian – written additively. From the matrix multiplication, α is a homomorphism if for $h, h' \in H$ and $\boldsymbol{a}, \boldsymbol{a}' \in A^n$:

$$(\alpha(\boldsymbol{a}))h' + \alpha(\boldsymbol{a}') = \alpha((\boldsymbol{a}) * h' + \boldsymbol{a}'), \text{ or } (\alpha(\boldsymbol{a}))h' = \alpha((\boldsymbol{a}) * h'.$$

In terms of its coordinates the check has the left side as $\sum_i ((a_{h_i})h_i)h'$. Summing the right side over j gives exactly the same.

Use the principle that a quotient of a K regular realization is also a K regular realization. Thus, we will conclude the whole proposition by applying α to a K regular realization of $A \wr H$. For this there are two steps:

(3.50a) There is a regular realization of A over K [**FrJ86**, Prop. 16.3.5]$_2$.

(3.50b) Combine regular realizations of H and $A^{|H|}$ to give one of $A \wr H$.

(3.50a) follows, by the elementary divisor theorem,[4] from the case where A is a cyclic prime power. §3.3.2 gives details on both parts of (3.50). □

3.3.2. *Comments on* (3.50). It must be a surprise that a K regular realization of a cyclic group (below) seems to require so much extra attention. Rem. 3.20 on fine moduli explains why.

The **BCL** *and* (3.50a)*:* Suppose W is a variety over L with $[L : K] = d$. Denote the Galois closure of L/K by $\hat{L}$. The following formalism produces a variety called the *Weil trace* (or restriction of scalars) of W from L to K. Choose a primitive element $\alpha = \alpha_1$ for L/K with $\alpha_1, \dots, \alpha_d$ the complete list of conjugates of α_1 over K. Each conjugate α_i gives a conjugate variety W_i, defined over $K(\alpha_i)$.[5]

[4] That a finitely generated module over a principal ideal domain R is a direct sum of cyclic modules (each of form $R/(r)$, $r \in R$).

[5] Replace L/K by any finite perfect extension to affect the same construction.

Then, $G = G(\hat{L}/K)$ acts on $W^\star = W_1 \times \cdots W_d$, permutating the coordinates according to its natural permutation representation of degree d. For $\sigma \in G$, indicate this action by $T(\sigma)$, acting on the left.

Now regard σ, by its action on the coefficients of the equations for $W^\star$ as giving a conjugate of $W^\star$. Denote this by $W^{\star,\sigma}$. Thus, for each $\sigma \in G$,

$$\text{the sets } T(\sigma^{-1})(W^{\star,\sigma}) \text{ and } W^\star \text{ are identical.}$$

PROPOSITION 3.18. *There is a variety $R_{L/K}(W)$ over K for which extending scalars by L gives $W^\star$. In this correspondence $W(L) \leftrightarrow R_{L/\mathbb{Q}}(W)(K)$: L points of W correspond to the K points of the Weil restriction.*[6]

PROOF. [**Se92**, p. 21] alludes to Weil's restriction of scalars [**We61**].[7] Intuitively, points of the variety $R_{L/\mathbb{Q}}(W)$ consist of the collections $\{T(\sigma)(w \in V^*)\}_{\sigma\in G}$. Assume with no loss that W is affine, and embedded in a copy of $\mathbb{A}^n$, also defined over L for this universal approach.

There is a linear map $\mathcal{L} = (\mathcal{L}_1, \ldots, \mathcal{L}_d) : \mathbb{A}^{nd} \to (\mathbb{A}^n)^d$ defined over L with the following property. For any subvariety $W = W_1 \subset \mathbb{A}^n$ defined L, there is a subvariety $R_{L/K}(W) \subset \mathbb{A}^{nd}$ defined over K such that

$$\text{restriction of } \mathcal{L} \text{ maps } R_{L/K}(W) \text{ isomorphically to } W_1 \times \cdots \times W_d. \tag{3.51}$$

Here the $\mathcal{L}_i$ s are the conjugates of $\mathcal{L}_1$; see the notation of Ex. 3.19, which reminds of the classical case $n = 1$.

Thus, we can apply this to the L subvarieties in W. This produces a K subvariety of $R_{L/K}(W)$ corresponding to the product of the conjugates of W. So, $\boldsymbol{p} \in W(L)$ produces $R_{L/K}(\boldsymbol{p}) \in R_{L/K}(W)(K)$. □

Now we discuss two proofs of the regular realization of $\mathbb{Z}/n$. [**FrJ86**, Lem. 16.3.1]$_2$ presents a regular realization of $\mathbb{Z}/n$ over $\mathbb{Q}$ in detail by constructing $g_n(w, z) \in \mathbb{Q}[w, z]$ with Galois group over $\mathbb{Q}$ equal to $\mathbb{Z}/n$, having a zero in $\mathbb{Q}((z^{1/n}))$. As expected, it uses the extension $\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q}$ by adjoining $z^{\frac{1}{n}}$. Still, it is a complicated construction to get this. Though its coefficients aren't enlightening, we use the case $n = \ell^e$, ℓ a prime in (3.52).

[**Se92**, p. 36–37] has an equation free proof regularly realizing $\mathbb{Z}/n$. Only problem is, this calls for a seriously educated reader on *tori*. [**Se68**, Chap. II] (or less brief, [**O61**]) is helpful background. It starts off with the requisite tori definitions. Instead of $\mathbb{A}^1$, use $\mathcal{G}_m$, the multiplicative group of nonzero elements.

Define a dimension d torus, $\mathcal{G}$, over a field K, to be an algebraic group in $\mathbb{A}^d$ whose $\bar{K}$ points is isomorphic to the d-fold product of the multiplicative group

[6] More generally: K morphisms from a K variety U to $R_{L/\mathbb{Q}}(W)$ correspond to L morphisms from $U \otimes L$ to W.

[7] The pubication date in this bibliography is 1982; the [**Se68**] bibliography has the date 1961.

$(\bar{K})^* \stackrel{\text{def}}{=} \mathcal{G}_m(\bar{K})$. Indicate field image of the distinct embeddings $\sigma_i : L^* \to \bar{K}$ by L_j^*, $j = 1, \dots, d$.

Forming $\mathcal{G}_{L/K} \stackrel{\text{def}}{=} R_{L/K}(\mathcal{G}_m)$ from Ex. 3.19 makes sense. The result is an algebraic group whose K points – Prop. 3.18 – identify with L^*, and whose extension of scalars to L (resp. to $\bar{K}$) identifies, as a group, with $\prod_{j=1}^d L_j^*$ (resp. the extension to the d-fold product of $\bar{K}^*$).

The *character group* of $\mathcal{G}$ is $\mathrm{Hom}_{\bar{K}}(\mathcal{G}\otimes\bar{K}, \mathcal{G}_m(\bar{K}))$; its elements are only sensitive to the field embeddings listed above. List them in this multiplicative notation by $\prod_{i=1}^j \sigma^{n_\sigma}$ following Serre's notation. For $\sigma \in G_{\bar{K}}$, $\sigma^{-1}\sigma_i\sigma^{-1}$, is also an embedding, giving a permutation action of G_K on these embeddings, and a $\mathbb{Z}$ basis for the characters, stable under G_K.

EXAMPLE 3.19 (Weil restriction: $n = 1$). For $n = 1$, here is how $\mathcal{L}$ in (3.51) works. Use $y_1, \dots, y_d$ as domain variables, and the linear map $\mathcal{L}_1(\boldsymbol{y}) = \sum_{i=1}^d \alpha_1^i y_i$. Then, an L subvariety of $\mathbb{A}^1$ is just $\sum_{i=1}^d \alpha_1^i y_i'$; the y_i's are in K, and the $\mathcal{L}_j(\boldsymbol{y})$s are the conjugates $\sum_{i=1}^d \alpha_j^i y_i$, $j = 1, \dots, d$.

Finish by showing how to get $R_{L/K}(\boldsymbol{p})$ with $\boldsymbol{p} = \boldsymbol{p}_1 = \sum_{i=1}^d \alpha_1^i t_i'$ as above. Conjugates of $\boldsymbol{p}_1$ over K are then $\boldsymbol{p}_1, \dots, \boldsymbol{p}_d$ by substituting: $\alpha_1 \mapsto \alpha_j$, $j = 1, \dots, d$. Apply Cramer's rule [**Ar91**, p. 31] to

$$\mathcal{L} = \begin{pmatrix} 1 & \alpha_1 & \cdots & \alpha_1^{d-1} \\ \dots & \dots & \cdots & \dots \\ 1 & \alpha_d & \cdots & \alpha_d^{d-1} \end{pmatrix} \text{ with } |\mathrm{Det}(\mathcal{L})| = |\prod_{j<j'} (\alpha_j - \alpha_j')| \neq 0.$$

That is, $\mathcal{L}$ has an inverse, $\mathcal{L}^{-1}$, with $\mathcal{L}^{-1}(\boldsymbol{p}_1, \dots, \boldsymbol{p}_d) = (y_1', \dots, y_d') \in K^d$. △

This is essentially a field crossing argument in [**FrJ86**, Lem. 13.8.1]$_2$, whereby independent variables $\{t_1, \dots, t_n\}$ for a regular realization for each copy of A in $A^{|H|}$ are entwined with a basis $\{c_1, \dots, c_n\}$ for an extension L/K with group G in the form of a system of linear equations $S = \{\sum_{i=1}^n c_i^\sigma t_i\}_{\sigma \in G(L/K)}$.

Then, combine $M/K(u)$ and $L(S)/K(t_1, \dots, t_n)$ into the extension $M{\cdot}L(S)/K(u, t_1, \dots, t_n)$ with its group $G \times G$ and take the fixed field of the diagonal action of G to RETURNM p. 259 FrJ.

Consider the projective nonsingular completion, W, of $\{(w, z) \mid g_n(w, z)\}$. Then take the corresponding cover:

$$(w, z) \mapsto z, \text{ giving } \varphi : W \to \mathbb{P}^1_z.$$

In the notation of the **BCL** Prop. 4.1, denote the branch cycle classes of φ in $G_{g_n} = \mathbb{Z}/n$ by $\mathbf{C}$. Indicate each by the unique $u \in \mathbb{Z}/n$ in the class; still denote it C_u and the union, $\{C_u \mid (u, p) = 1, u \in \mathbb{Z}/p^e\}$ by $\mathbf{C}(p')$. The **BCL** is precise on what would be the minimal cardinality of the classes in $\mathbf{C}$ for a Nielsen class $\mathrm{Ni}(\mathbb{Z}/n, \mathbf{C})$ supporting a regular realization like φ.

(3.52a) **C** must contain $\mathbf{C}(p')$: the minimal possible number of branch points of φ is $p^{e-1}(p-1)$.

(3.52b) We can't expect a regular realization in $\mathrm{Ni}(\mathbb{Z}/n, \mathbf{C}(p'))$, which hasn't got fine moduli, for $\mathbb{Z}/n$ has a center. Yet, the explicit g_n is in this class.

Comments on (3.52a)*:*

REMARK 3.20 (Fine moduli failure).

3.3.3. *Two sequence paradigm.* While this goes beyond generalizing our running dihedral group example, it has a number of elements in common with that, that eventually get us back to classical spaces. Cyclic groups and dihedral groups require little understanding of group theory.[8] Yet, they are irresistible to many who have considered the **RIGP** template – with an eye to techniques – in a personal conception of what the land of groups is about.

Starting with any centerless finite group G_0 and prime ℓ for which G_0 is ℓ-perfect, there is a $\mathbb{Z}_\ell[G_0]$ module $L_{G,\ell}$ of dimension[9] ≥ 1 giving rise to *two* extensions:

$$(G,\ell)\text{-tower sequences: } L_{G,\ell} \to {}_\ell\tilde{G}_s \to G \text{ and } L_{G,\ell} \to {}_\ell\tilde{G}_f \to G.^{10}$$

These sequences have these properties (explained further below).

(3.53a) *Split:* ${}_\ell\tilde{G}_s$ is split, equal to $L_{G,\ell} \times^s G_0$. If G_0 is regularly realized over K, then so is ${}^u_\ell\tilde{G}_s \stackrel{\text{def}}{=} L_{G,\ell}/\ell^u L_{G,\ell} \times^s G_0$, $u \geq 1$.[11]

(3.53b) *Frattini:* ${}^u_\ell\tilde{G}_f \stackrel{\text{def}}{=} {}_\ell\tilde{G}_f/\ell^u L_{G,\ell} \to G_0$ is Frattini.[12] Even for $G_0 = A_5$, $\ell = 2, 3$ or 5, $u \geq 1$, there have been no $\mathbb{Q}$ realizations of ${}^u_\ell G_f$.

3.4. Two RIGP statements. With The **RIGP** realization result of (3.53a) – with $A_u \stackrel{\text{def}}{=} L_{G,\ell}/\ell^u L_{G,\ell}$ applying to the semi-direct product ${}^u_\ell\tilde{G}_s = A_u \times^s G_0$ – is a corollary of the following with $H = G_0$ and $A = A_u$.

An explicit (resp. abstract) proof of these pieces is in [**FrJ86**, Prop. 16.3.5]$_2$ (resp. [**Se92**, §4.2]). For (3.50a) it suffices to consider the case $A = \mathbb{Z}/\ell^u$, and though it is overkill, the Branch Cycle Lemma (**BCL**; [**Fr77**, Thm. 5] and, among other places, a key ingredient in [**FrV91**, Main Thm]) says – for ℓ odd – the minimal number of possible branch points for such a realizing cover is $\ell^{u-1}(\ell-1)$. Conclude:

LEMMA 3.21. *Consider any sequence of regular realizations of* $\{A_u\}_{u=1}^\infty$ *over* $\mathbb{Q}$*, with corresponding count of the branch points as* $\{r_u\}_{u=1}^\infty$*. Then,* $r_u \mapsto \infty$*.*

[8] As we will see the same cannot be said for, say, alternating groups, though they give the first simple – nonabelian – groups in a graduate algebra course.

[9] Necessarily ≥ 2 unless G_0 is the ℓ-supersolvable generalization of dihedral.

[10] There may be more than one $L_{G,\ell}$ but among them is a maximal such with a characteristic dimension dependent on (G,ℓ).

[11] There is an explicit degree bound for such a K, dependent only on (G,ℓ).

[12] $H \to G_0$, a group cover, is Frattini if $H_1 \leq H$ maps surjectively to G_0, then $H_1 = H$.

Yet, the conclusion of Prop. 3.22 – referring to Hurwitz spaces $\mathcal{H}(G,\mathbf{C})^\dagger$ of sphere covers corresponding to a Nielsen class $\mathrm{Ni}(G,\mathbf{C})^\dagger$ as if a reader knows about them – is still a possibility.

$\Diamond$: This conference would include many, some giving expositions, knowledgable on the arithmetic of Hurwitz spaces and their literature.

With K a number field, suppose the sequence $\{{}^u_\ell\tilde{G}_f\}_{u=1}^\infty$ has a sequence of respective K regular realizations $\mathcal{W}_{f,G_0} \stackrel{\text{def}}{=} \{\varphi_{u,f} : W_{u,f} \to \mathbb{P}^1_z\}_{u=1}^\infty$. Denote the number of branch points of $\varphi_{u,f}$ by $r_{u,f}$.

Proposition 3.22. *If there is any uniform bound B_{f,G_0} on all of the $r_{u,f}$ s, then, there exist r conjugacy classes $\mathbf{C}_f$ of G_0,*

$$r \stackrel{\text{def}}{=} r_{\mathbf{C}_f} \le B_{f,G_0}, \text{ each class of elements of order prime to } \ell \ (\ell').$$

From Schur-Zassenhaus, these $\mathbf{C}_f$ lift canonically to classes – still denoted $\mathbf{C}_f$ – in each ${}^u_\ell\tilde{G}_f$. With $\dagger$ = inner, this gives a projective sequence of Hurwitz spaces $\mathbb{H}_{G_f,\mathbf{C}_f,\ell} \stackrel{\text{def}}{=} \{\mathcal{H}^{\text{in}}_{f,u} \stackrel{\text{def}}{=} \mathcal{H}({}^u_\ell\tilde{G}_f,\mathbf{C})^{\text{in}}\}_{u=0}^\infty$.

Diophantine addition: $\mathcal{H}^{\text{in}}_{f,u}$ has an absolutely irreducible K component, $\mathcal{H}'_{u,\mathbf{C}_f}$ with a K point $\boldsymbol{p}_{f,u}$ from a K regular realization of ${}^u_\ell\tilde{G}_f$, $u \ge 1$.

With no loss, you may assume the sequence $\mathbb{H}'_{\mathbf{C}_f} \stackrel{\text{def}}{=} \{\mathcal{H}'_{u,\mathbf{C}_f}\}_{u=1}^\infty$ is a projective sequence. In a natural way, induced from ${}^{u+1}_\ell\tilde{G}_f \to {}^u_\ell\tilde{G}_f$, points of $\mathcal{H}'_{u+1,\mathbf{C}_f}$ lie over points of $\mathcal{H}'_{u,\mathbf{C}_f}$.

Given $r = r_{\mathbf{C}_f}$-tuple $\boldsymbol{g}_{u+1} \in ({}^{u+1}_\ell\tilde{G}_f)^r$ in $\mathbf{C}_f$ lying over $\boldsymbol{g}_u \in \mathrm{Ni}({}^{u+1}_\ell\tilde{G}_f,\mathbf{C}_f)$. From the Frattini cover property they generate ${}^{u+1}_\ell\tilde{G}_f$. So,

(3.54) $\qquad \boldsymbol{g}_{u+1} \in \mathrm{Ni}({}^{u+1}_\ell\tilde{G}_f,\mathbf{C}_f)$ precisely when product-one (**??**) holds.

In (3.57), denote the rank of P_ℓ by $\nu(\ell)$, $\tilde{\psi}_{\ell,\text{ab}} : \tilde{P}_{\ell,\text{ab}} = (\mathbb{Z}_\ell)^{\nu(\ell)} \to P_\ell$ the universal free-abelian ℓ-extension of P_ℓ (as in Cor. 2.4), and G/P_ℓ by H. We will use comments on the ℓ contribution to **RIGP** realization of ${}_\ell\tilde{G}_{\text{ab}}$ from the Prop. 3.23 proof.

Corollary 3.23. *The G action on P_ℓ extends to $\tilde{P}_\ell$, inducing an H action on $\tilde{P}_{\ell,\text{ab}}$ extending that on P_ℓ.*

If G/P_ℓ has a regular realization over an Hilbertian field K, then so does each of the quotient groups $\tilde{P}_\ell/\ell^{k+1}\ker(\tilde{\psi}_{\ell,\text{ab}}) \times^s H, k \ge 0$.

Proof. From Prop. 1.30, the H action on P_ℓ extends to ${}_\ell\tilde{G}$. That action preserves $[P_\ell,P_\ell]$, giving the 1st paragraph. It also preserves $\ell^{k+1}\tilde{\psi}_{\ell,\text{ab}}$ giving an H action on the quotient by that group. □

If, as above, P_ℓ is not normal in G, say when G is simple, then for no $k > 0$ has any ${}^k_\ell G$ been regularly realized (A_5, and $\ell = 2$, worthy on its own).

The **R**(egular)**I**(nverse)**G**(alois)**P**(roblem)
and **M**(odular) **T**(ower)s RETURNM

(3.55a) *Frattini cover*: $\psi : H \to G$; if $H^* \le H$ and $\psi(H^*) = G \Longrightarrow H^* = H$.

ℓ-perfect: $\ell || G|$, but G has no $\mathbb{Z}/\ell$ quotient.

(3.55b) Problem: Most groups are not like simple or solvable.

(3.55c) Example: Take G, ℓ-perfect and centerless: $\exists \nu(G,\ell) > 0$ (> 1, outside supersolvable) and an extension

$$1 \to (\mathbb{Z}_\ell)^{\nu(G,\ell)} \to {}_\ell\tilde{G}_{\rm ab} \xrightarrow{{}_\ell\tilde{\psi}_{\rm ab}} G \to 1 : {}^{8}$$

${}_\ell\tilde{G}_{\rm ab}$ universal for ℓ-Frattini covers of G with abelian kernel.

(3.55d) ¡4-¿ Subex.: Even for $G = A_5$, and where $v(G,2) = 5$, for no $k > 0$

has ${}_2\tilde{A}_{5,{\rm ab}}/2^k \ker({}_\ell\tilde{\psi}_{\rm ab}) = {}^k_2A_5$ been realized over $\mathbb{Q}$.[9]

Which is more *important/serious/...*?:
Cases similar to $(G,\ell) = (D_\ell, \ell = \ell)$ or to $(A_5, \ell = 2)$.
MT definition

(3.56a) Assume r conjugacy classes, $\mathbf{C}$ of G; elements of order ℓ'.

Schur-Zassenhaus lifts these classes uniquely to ${}_\ell\tilde{G}_{\rm ab}$.

(3.56b) Makes sense of ${}_\ell\mathbb{H}(G,\mathbf{C})^{\rm in,rd} \stackrel{\rm def}{=} \{\mathcal{H}({}^k_\ell G, \mathbf{C})^{\rm in,rd}\}_{k=0}^\infty$.

MT: Projective sequence of components on ${}_\ell\mathbb{H}(G,\mathbf{C})^{\rm in,rd}$.[9]

(3.56c) ${}_\ell\mathbb{H}(D_\ell, \mathbf{C}_{2^4})^{\rm in,rd} = \{X_1(\ell^{k+1})\}_{k=0}^\infty$ for ℓ odd.

(3.56d) Example: ${}_2\tilde{A}_4$ is the pullback of $A_4 \le A_5$ to ${}_2\tilde{A}_5$.
$(\mathbb{Z}_2)^5$: As A_4(but not A_5) module has $(\mathbb{Z}_2)^2$ as a quotient.

$\mathcal{H}(A_5, \mathbf{C}_{3^4})^{\rm in,rd}$ has one genus 0 component.[10]

REMARK 3.24 (Conj. 3.1). Indeed, we make the conjecture with ${}^k_\ell G \to G$ replacing ${}^k_\ell G_{\rm ab} \to G$. Our point in making it in the latter case was to show an edge closeto examples of regular realizations that update common knowledge about the **RIGP**. Further, we can treat the conjecture as defining ${}_*\mathbf{C}$ regular realizations of G over a field K: it corresponds to a K point on a Hurwitz space defined by $\mathbf{C}$ with support in ${}_*\mathbf{C}$, and it is absolutey necessary that such a point lies of on Hurwitz space component defined over K, with the **BCL** merely giving the minimal definition field of the whole Hurwitz space.

(3.57) Assume G has an ℓ-Sylow, P_ℓ, that is abelian and normal.

4. Moduli interpretation of the (G,ℓ)-tower sequences

We start with production the module $L_{G,\ell}$. Then, we go to simple **RIGP** questions that produce the moduli spaces whose properties generalize those usually associated with moduli of abelian varieties.

4.1. Source of $L_{G,\ell}$. The following statements start from [**FrJ86**, §22.4]$_2$ with supplements in [**BFr02**] and related. Especially [**?**] which includes a 4-Parted series called *Frattini ℓ pieces*.

Given (G,ℓ) as above, there is a universal ℓ-Frattini cover ${}_\ell\psi : {}_\ell\tilde{G} \to G$: any Frattini cover $H \to G$ with ℓ-group kernel is a quotient from ${}_\ell\psi$.

A fiber product construction produces a universal (profinite) Frattini cover $\tilde{\psi} : \tilde{G} \to G$ from which come these ℓ-Frattini covers and the abelianizations of their kernels as a quotient. This shows $\ker({}_\ell\psi)$ is a pro-ℓ pro-free group of rank bounded computable – from the rank of G and the index of an ℓ-Sylow. By modding out by the commutator of the kernel, $\ker({}_\ell\psi) = \ker_\ell$, there is a universal abelianized version ${}_\ell\psi_{\rm ab} : {}_\ell\tilde{G}/(\ker_\ell, \ker_\ell)/ \to G$.

That gives the Frattini sequence (3.53b). It also identifies $\ker({}_\ell\psi_{\rm ab})$ with the maximal possible $L_{G,\ell}$ that can appear in this sequence. To understand the abelianized Universal ℓ-Frattini, consider

$$ {}_\ell M_G = \ker({}_\ell\tilde{\psi}_{\rm ab})/\ell\ker({}_\ell\tilde{\psi}_{\rm ab}).$$

4.2. A taste of the Frattini ℓ pieces. For example, Part 1 of the Frattini ℓ-pieces is [**?**, Ch. 1, Prop. 1.14] includes these statements.

(3.58a) Fiber products of ${}_\ell\tilde{\psi}_{\rm ab}$, $\ell||G|$, give $\tilde{\psi}_{\rm ab} : \tilde{G}/[\ker(\tilde{\psi}), \ker(\tilde{\psi})] \to G$.

(3.58b) Conjugating by lifts of elements in G, makes $\ker({}_\ell\tilde{\psi}_{\rm ab})$ a free $\mathbb{Z}_\ell[G]$ module extending the $\mathbb{Z}/\ell[G]$ module structure on ${}_\ell M_G$.

(3.58c) $\sum_{\ell||G|} \dim_{\mathbb{Z}/\ell}({}_\ell M_G) \le 1 + |G|(\text{rank}(G)-1)$.

Other possible G lattices that serve as $L_{G,\ell}$ are quotients of $\ker({}_\ell\psi_{\rm ab})$. Ordinarily modular representations have somewhat *scary* aspects called *wild*. Yet, Parts 1 to 4 of the Frattini ℓ pieces gives illuminating examples of the moduli space towers that appear below. For accessibility, results compare them with the special case of *towers of modular curves*.

4.2.1. *Explicit Nielsen classes.*

(3.59a) Thompson and Völklein produced large series of Chevalley groups, G, rank > 1, as $\mathbb{Q}$ regular realizations (3 total such groups had been achieved previously) by finding $\mathbf{C}$ so the Hurwitz space, $\mathcal{H}(G,\mathbf{C})$, corresponding to $(G,\mathbf{C})$ has $\mathbb{Q}$ points.

(3.59b) Appying the Branch cycle Lemma, the Fried-Serre Lift Invariant, the Conway-Fried-Parker-Völklein component bound, for each G, gave infinitely many explicit $\mathbf{C}$ with $\mathcal{H}(G,\mathbf{C})$ *nonempty* and *having a* $\mathbb{Q}$ *component.*

(3.59c) Fried produced infinitely many explicit $\mathbf{C}$ (called *Harbater-Mumford*) for which the canonical projective system of Hurwitz spaces $\{\mathcal{H}(G_u,\mathbf{C})\}_{u=0}^{\infty}$ contains a subsystem, $\{\mathcal{H}'_u\}$, of nonempty (absolutely irreducible) components over $\mathbb{Q}$.

Found explicit connected Hurwitz spaces $\mathcal{H}(G,\mathbf{C})$ with:

- $\mathcal{H}(G,\mathbf{C})$ transcendental parametrizing parameters;
- $\mathbf{C}$ as a collection rational over $\mathbb{Q}$.
- Guarantees **RIGP** for those groups over $\mathbb{Q}$.

For any subset, S, of a group G, refer to it as ℓ' if all elements in S have order prime to ℓ. The Hurwitz space objects as explicit encoders of all regular realizations raise myriad questions. The following projects responded to that.

5. PAC fields; A presentation of $\mathcal{G}_{\mathbb{Q}}$

This section continues §3 through consequences to the **RIGP** through using the field analogy to finite fields called **PAC** fields (Def. 5.1). It features a place of success, whereby non-classical subfields of $\bar{\mathbb{Q}}$ have benefitted the **RIGP**, Thm. 5.4.

§5.2 joins both versions of the **BCL** – for inner and absolute equivalence – to investigate $\mathcal{G}_{\mathbb{Q}}$ by a paradigm new in [**FrV92**]. §5.2 does this by guaranteeing there exist $\mathbb{Q}$ Hurwitz space components indexed by $(G,\mathbf{C})$ for infinitely many $\mathbf{C}$, a particular case of the theme of §3.3. §5.3 completes Thm.. 5.4 by combining techniques in this **PAC** context that allow us to deal with *all* groups.

Definition 5.1 (PAC). Refer to a field $L\subset\bar{\mathbb{Q}}$ as

$$\mathbf{P}(\text{seudo})\mathbf{A}(\text{lgebraically})\mathbf{C}(\text{losed}) \text{ if } V(L)\neq\emptyset,$$

for each absolutely irreducible (quasi-projective) variety V over L.

Using Weil's restriction of scalers, and the Bertini-Noether theorem, the test for **PAC** reduces to checking on just those V that are absolutely irreducible curves over $\mathbb{Q}$: [**FrJ86**, Thm. 10.4]$_1$ or [**FrJ86**, Thm. 11.2.3]$_2$. Note also, that allowing V to be quasi–projective means there are L points lying off any particular proper algebraic subset of V.

Remark 5.2. If L [**?**, Thm. 2] is not **PAC**, then there is an absolutely irreducible curve in $\mathbb{P}^1$ over L with no L points. That is, the test of plane projective curves fo L points suffices to separate **PAC** fields from non-**PAC** fields.

5.1. Absolute Galois groups of PAC, Hilbertian fields.

DEFINITION 5.3. Denote the profree group on a countable set of generators by F_ω. We call a field L ω-free if $\mathcal{G}_L \equiv F_\omega$. So, $\mathcal{G}_L$ has every finite group as a quotient : it satisfies the IGP for every finite group G. Such a field is also Hilbertian (see §6.1.1 for the definition) as we discuss below. Similarly, denote the group that is profree on a countable set of involutions to be F_{2^∞}, and refer to any field having it as absolute Galois group as Inv-free.

THEOREM 5.4 ($\mathcal{G}_\mathbb{Q}$ structure). *A* **PAC** *field L is Hilbertian if and only if L is ω-free. For K a number field, then $K \le L$, with L Galois over K and* **PAC**. *Further, we may choose L so that $\mathcal{G}_K$ has a presentation*

$$1 \to F_\omega = \mathcal{G}_L \to \mathcal{G}_K \to \Pi_{n=2}^\infty S_n \stackrel{\text{def}}{=} \mathcal{S}_\infty \to 1 \tag{3.60}$$

The left side of (3.60) is a corollary of the first sentence. The heart of

$$\text{“ } \mathbf{PAC}\text{+ Hilbertian } \implies \omega\text{-free ”}$$

comes from choosing **C** (as in answers to (2.9b)) for convenience and tying together the abs and in spaces (as in (2.9c)), to build large IGP realizations over Hilbertian **PAC** fields (Prop. 5.9). The right side of (3.60), was created with this thought: Our technique for constructing it was based on a simple principle about presenting curves over $\mathbb{Q}$ as covers, and from that we wanted a (relatively small) group, $\mathcal{S}_\infty$, recognizable by most mathematicians. Rems. 6.8 and 6.9 give the subtleties of that choice.

We say a **PAC** field K is *Frobenius* if $\mathcal{G}_K = \mathcal{G}$ has the following property.

DEFINITION 5.5 (Embedding Property). For any group covers $\psi : \mathcal{G} \to A$ and $\psi' : B \to A$, with B a quotient of $\mathcal{G}$, there exists a cover $\gamma : \mathcal{G} \to B$ for which $\psi' \circ \gamma = \psi$ [**FrJ86**, Defs. 24.1.2 and 24.1.3]$_2$.

Frobenius fields include the case of e-free fields where $1 \le e \le \infty$, with ∞-free the same as ω-free, our case here. The 1-free fields arose as the exact **PAC** analog of finite fields (Rem. 6.7). Lem. 5.6, implying the Hilbertian property for **PAC** fields that are ω-free, comes from a trick

$$\text{– the } \mathbf{F}\textit{(ield)}\mathbf{C}\textit{(rossing)}\mathbf{A}\textit{(rgument)} \text{ –}$$

that goes back to Chebotarev's proof of his renown *Density Theorem*. §6.1.1 reminds of the history of that Chebotarev-HIT connection from [**Fr74**, §2–3].

In extending the ideas of [**FrS76**], aimed at solving an Ax-Kochen problem about finite fields, the **PAC** condition replaces the so-called Lang-Weil argument: an absolutely irreducible variety over a suitably *large* finite field $\mathbb{F}_q$ has a $\mathbb{F}_q$ point. The length and complication of the proof in [**FrJ86**, §24.1]$_2$ (or [**FrJ86**, §23.1]$_1$)

comes from passing back and forth between covers and fields, instead of, say, the treatment in [**FrS76**] which used covers, their fibers and fiber products directly.

The material of the **FCA** in this application starts with two finite extensions of our base field L, $E_1 = \hat{L}/L$ which is Galois and $E_2 = F/L(z)$, which is regular, with Galois closure $E_2^* = \hat{F}/L(z)$. They have these properties.

(3.61a) E_1 and E_2^* both have group identified with G; and

(3.61b) $E_3 = \hat{M}/F$, with group H, is the extension of constants of $\hat{F}/L(z)$ through which E_1 factors.

Now form the covers $\mathbb{P}^1_{z,\hat{L}} \stackrel{\text{def}}{=} \mathbb{P}^1_z \times \text{Spec}(\hat{L}) \to \mathbb{P}^1_z$ and $\hat{\varphi} : \hat{X} \to \mathbb{P}^1_z$ with $\hat{X}$ the projective, normalization in the function field $\hat{F}$. Then the fiber product

(3.62) $\hat{\varphi}_{\hat{L}} = \mathbb{P}^1_{\hat{L}} \times_{\mathbb{P}^1_z} \hat{X} \to \mathbb{P}^1_z$ has group identified with $G \times_H G$.[13]

LEMMA 5.6. *Assume L is* **PAC** *and ω-free. Then, L is Hilbertian.*

COMMENTS. Use the notation of (3.62). To show that L is Hilbertian, we use the Galois version of the Hilbertian property (**HIT**; §**??**) and show it applies to $\hat{\varphi}$. [**FrJ86**, p. 230]$_2$ has a short summary of the various results (Weissauer's and the Diamond Theorem; that are proved after that) that give infinite extensions of $\mathbb{Q}$ that are Hilbertian. The basic one we use is Weissauer's, restated in §**??** with relevant examples to our discussion.

Construct the field extension $\hat{L}$ immediately by using that L is ω-free. Rem. 6.7 explains why, even though $\mathcal{G}_L$ is automatically projective, that is insufficient for such a conclusion.

Now take the diagonal $\Delta(G)$ on $G \times_H G$. Quotient out by $\Delta(G)$ acting on $\mathbb{P}^1_{\hat{L}} \times_{\mathbb{P}^1_z} \hat{X}$ to get $\varphi_Y : Y \to \mathbb{P}^1_z$ an absolutely irreducible cover over L. Running over the infinitely $\boldsymbol{y} \in Y$ given by the **PAC** property, allows us to assure $\varphi_Y(\boldsymbol{y})$ avoids any branch points of $\hat{\varphi}$. It is now automatic from the construction that the decomposition group of $\varphi_Y(\boldsymbol{y})$ in $\hat{\varphi}$ is G. That establishes Hilbertianity. □

Prop. 5.9 gives the other direction that proves (3.60), based on the relation between inner and absolute spaces. It also opens the topic, for a given finite group G, of which classes, **C**, suit a specific application. We continue here with lessons on what we have learned from **PAC** fields.

Conj. 5.7 replaces the hypothesis that L is **PAC** with the projective property that **PAC** implies. There are projective fields that aren't **PAC**, but are Hilbertian. Example: The cyclotomic closure, K^{cyc}, with a K a number field for which there are elliptic curves over K^{cyc} with rational points. This simultaneously generalizes a Conjecture of Shafarevich, and Thm. 5.4.

[13]The conditions in (3.61) that the fields are extensions of $L(z)$ and that E_1 and E_2 have the same groups, rather than the group of E_1 being a subgroup of that of E_2, are expedients to move the argument along more quickly.

CONJECTURE 5.7. [**FrV92**,] Any Hilbertian field $L \subset \bar{\mathbb{Q}}$ is ω-free if and only if $\mathcal{G}_L$ is *projective*.

This raises three aspects of **PAC** fields which we take up in the remarks.

(3.63a) Are they Serious?: Rem. 6.7 clarifies why they can't be dismissed.

(3.63b) Are they useful?: For **PAC** fields such properties as Hilbertian and RG-Hilbertian are group-theoretic (Rem. 6.10).

(3.63c) Are they apparent?: Do **PAC** fields appear in serious applications? What about projective fields (Rem. 6.8 and Rem. 6.9)?

5.2. Completion of presenting $\mathcal{G}_{\mathbb{Q}}$. We now complete the hard half of Thm. 5.4. To do so required coming to grips with aspects of the effect, for a fixed G, of different choices of $\mathbf{C}$. The essence of it is to construct covers $\varphi : X \to \mathbb{P}^1_z$, over any **PAC** Hilbertian subfield of $\mathbb{C}$, that achieve (G, G^*) realizations (Def. 1.6) using the diagram of Thm. 1.7. That will also be a model for what to expect in achieving such results over number fields, where the problem arises naturally in specific cases (§6.1.3). We must do this in the generality required to consider the problem for all pairs (G, G^*).

As in §1.1, assume ${}_*\mathbf{C}$ is a rational union of conjugacy classes. Prop. 5.9 lists sufficient conditions for $(G, {}_*\mathbf{C})$ that guarantee $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ has $\mathbb{Q}$ components for infinitely many $\mathbf{C} \in \mathcal{R}_{{}_*\mathbf{C}}$ (rational unions of classes containing each class of, and supported in, ${}_*\mathbf{C}$). It further shows that every finite group is a quotient of some G that occurs among these pairs, for some extending classes ${}_*\mathbf{C}$.

These appeared in [**FrV91**] to give sufficient absolutely irreducible $\mathbb{Q}$-components from the desired list of Prob. 1.1 so as to finish the proposition. By 1988, Ex. 2.9 guided me in simplifying what was going on with braid orbits, so long as high multiplicity condition (3.19) holds.

DEFINITION 5.8. An extreme opposite to all classes in ${}_*\mathbf{C}$ being liftable (Def. 1.4) to a central Frattini cover $\psi : H \to G$, is that the generalized lift invariant is trivial. It is equivalent that single commutators from ${}_*\mathbf{C}$ generate $\ker(\psi)$ (as in Ex. 2.11). We say $(\ker(\psi), {}_*\mathbf{C})$ has trivial lift invariant.

If $(\ker(\psi), {}_*\mathbf{C})$ has trivial lift invariant, then for any $\mathbf{C} \in \mathcal{R}_{{}_*\mathbf{C}}$, the lift invariant of any $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ is trivial. When ${}_*\mathbf{C}$ consists of all nontrivial classes in G, [**FrV91**] refers to Def. 5.8 as $\ker(\psi)$ is generated by commutators. If G has no center, then the group of automorphisms, $\mathrm{Aut}(G)$, extends the action of G as conjugations on G.

PROPOSITION 5.9. *By replacing G by a finite cover of G, with no loss we may assume the following.*

(3.64a) *For a representation cover, $\psi_G : R \to G$, single commutators generate* $\ker(\psi)$.

(3.64b) *In addition to* (3.64a)*, G is centerless and, if ${}_*\mathbf{C}$ contains all nontrivial classes of G, then* $(\ker(\psi_G), {}_*\mathbf{C})$ *has trivial lift invariant.*

Consider G^* the cover of G for which G^*/G consists of all outer automorphisms of G. Assume RETURN , if (3.19) *holds, for $\mathbf{C} \in \mathcal{R}_{{}_*\mathbf{C}}$, from the diagram $\mathcal{H}^{\rm in} \to \mathcal{H}^{\rm abs}$ there is a $\mathbb{Q}$ component (as a moduli space) of $\mathcal{H}^{\rm in}$ from which we can achieve (G, G^*) over every* **PAC** *field, $L \le \bar{\mathbb{Q}}$.*

(3.65a) *with L^*/L Galois with group G^*/G we may achieve the realization of* (3.64b)*, from a regular cover $\varphi : X \to \mathbb{P}^1_z$ whose constant field extension is L^*/L.*

In particular, G_L is profree on a countable number of generators.

The next three subsections prove and comment on the pieces of Prop. 5.9.

5.3. Producing the cover of (3.64)**.** We produce a centerless cover of G whose representation cover has trivial lift invariant. Choose $\psi_G : R_G \to G$, a representation cover of G (Def. 1.10). Then, consider a representation cover $\psi_{G.2} : R_{G,2} \to R_G$. As a composition of Frattini covers,

$$\psi \stackrel{\rm def}{=} \psi_G \circ \psi_{G,2} : R_{G,2} \to G \text{ is a Frattini cover,}$$

but it may not be central.

Now, let $T \stackrel{\rm def}{=} \psi_{G,2}^{-1}(\ker(\psi_G))$. Then, $Z \stackrel{\rm def}{=} [R_{G,2}, T] \le \ker(\psi_{G,2})$ is a subgroup generated by single commutators. Thus, $\psi/Z : R_{G,2}/Z \to G$, with $\ker(\psi/Z) = T/Z$, is a central Frattini cover with commutator kernel (Def. 1.10). As ψ_G is a maximal central Frattini cover of G with commutator kernel, and ψ/Z factors through it, conclude that $R_{G,2}/Z = R_G$.

(3.66) So, $Z = \ker(\psi_{G,2})$: Single commutators generate $\ker(\psi_{G,2})$.

Suppose we replace G by R_G. Then, we have a cover of G with a representation cover whose kernel is generated by single commutators. Therefore, no matter what is ${}_*\mathbf{C}$, the lift invariant for any Nielsen class will be trivial. That still leaves a problem.

Even if G has no center, R_G does if it is a nontrivial cover of G. [**FrV91**, Lem. 2] produces a cover of G that adds property (3.64b) to (3.64a). RETURN

Remark 5.10 (Explicitness in Prop. 5.9). §3.64 produces the group satisfying (3.64), replacing the original group, in two steps. First: By forming a representation cover $R_G \to G$. Second: By forming a wreath product of R_G with an explicit group. Thus, the resulting group is explicit if there is an explicit construction of R_G. As with all things Frattini, consider the construction one $\ell||G|$ at a time. The module

$M_{G,\ell}$ appears as the ℓ-part of $H_2(G,\mathbb{Z})$, an abelian group killed by multiplying by $|G|$, [**Br82**, III. Cor. 10.2] from the restriction-corestriction sequence.

RETURN That bounds the power of ℓ dividing M_G. In particular, that bounds the ℓ-Frattini level in which M_G, with trivial G action can appear, as a split summand of kernel of $\to G$. Therefore, the explicitness results from the explicit construction of the 1st ℓ-Frattini cover level, as in Prop. 2.18.

6. The meaning of "Field Arithmetic"

"Field Arithmetic," the title of $[\mathbf{FrJ86}]_1$ comes from these ideas.

(3.67a) Measure the dependence between diophantine properties by the nature of the fields for which they simultaneously hold.

(3.67b) Expand on using, for a projective algebraic set V over $\mathbb{Q}$, the nature of those residue classes $\mathbb{Z}/\ell$ for which $V(\mathbb{Z}/\ell) \neq \emptyset$.

This section is mostly expositional, tying together historical subjects to our topics. The absolute Galois group of $\mathbb{Q}$, $G_{\mathbb{Q}}$, and the collection, $\mathbb{B} = \{B_r\}_{r=3}^{\infty}$, of braid groups are the heart of many of the great disciplines of mathematics.

The former starts with forms of the IGP, giving explicit descriptions of various quotients of $\mathbb{Q}$, especially the maximal abelian (commutator) and then attempts at the maximal nilpotent quotient of $\mathbb{Q}$. Here are two milestones:

(3.68a) Ihara's description of the 2nd commutator quotient of $G_{\mathbb{Q}}$; and

(3.68b) Shafarevich's proof that all nilpotent groups are quotients of $G_{\mathbb{Q}}$.

The study of $\mathbb{B}$ drives descriptions of various spaces through fundamental groups. Also, we relate it and $G_{\mathbb{Q}}$, by producing spaces whose points and definition fields over specific fields reflect on the **RIGP** and the **OIT**. Concentrating on properties of particular Hurwitz spaces, often with classical connections, is our focus.

General too is the connection of the **RIGP** and **OIT** to a sometimes dismissed element in this discussion: **H**(ilbert's)**I**(rreducibility)**T**(heorem). Hilbert introduced it to connect the **RIGP** and the IGP. It became an adjective *Hilbertian*, a property of fields. §6 describes how it illustrated the goals of [**FrJ86**] using **PAC** fields.

Somewhat confusing – in the classical literature – is with what weight should we emphasize fields vs algebraic sets. To whit: What algebraic sets – say, complete intersections of various degrees, or abelian varieties – were assured of having rational points over which fields. §6.2 reminds of this. In particular that special result called Chevalley's Theorem §6.4 – that culminated in a **PAC** avatar conjectured by Ax and proved by Kollár.

Then, there are the various results and conjectures of Ax, Jarden, Shafarevich §6.2.2 that motivated so much of what lay behind [**FrJ86**] and the result (with

its natural conjecture) of the Fried-Voelklein Conj. 5.7 on Hilbertian fields with projective absolute Galois group.

Extending those concerns to Hurwitz spaces, where describing properties of components of Hurwitz spaces defined by various groups and their conjugacy classes gets us to the most modern considerations §6.2.3. The properties in question are *birational*. Then, extracting such properties from $\mathbb{B}$ opens a new subject, *birational algebraic geometry*, for which *homotopy theory* is a requisite tool.

Finally, we can't avoid connecting to two of Grothendieck's famous topics, dessins d'enfant and his Teichmüller group §6.3, especially because of his comment relating correspondences on curves to the **OIT**.

6.1. IGP **and RIGP comparison.** §6.1.1 reviews the nature of the hilbertian property, comparing the IGP, the **RIGP** and hilbertianity and its surprising behavior on the lattice of subfields of $\bar{\mathbb{Q}}$ in the spirit of Field Arithmetic.

There is an ongoing project that delves into the role of **HIT** the relation between the **RIGP** and the IGP. §6.1.2 does an exposition on it comparing over a field F, for a given group G, realizations of G as a Galois extension of F, $\mathcal{F}_{G,\mathrm{IGP}}$ and $\mathcal{F}_{G,\mathbf{RIGP}}$: The specializations of **RIGP** realizations of G using **HIT**. At this stage, with both problems still so unsolved, the comparison is often qualitative, comparing densities of elements of $\mathcal{F}_{G,\mathbf{RIGP}}$ resulting from specific **RIGP** realizations of G with those of $\mathcal{F}_{G,\mathrm{IGP}}$.

Finally, §6.1.3 notes the ubiquitous appearance in absolute Hurwitz families of covers $X \to \mathbb{P}^1_z$ that are absolutely irreducible, but whose Galois closures in the related inner Hurwitz spaces may not be regular. Prevalence of such families are precisely what motivated much of this book, as they include and generalize so many classical diophantine problems, starting with problems from *modular curves*.

6.1.1. *Hilbertian fields and universal Hilbert subsets.* The simplest statement of the Hilbertian property for a field K is this: for $f(x,y) \in K[x,y]$, irreducible (over K), then $f(x_0,y)$ remains irreducible as a polynomial in one variable over K for infinitely many $x_0 \in K$. This statement leaves open many ways we might indicate some properties of the *Hilbertian set*

$$H_f(K) = \{x_0 \in K \mid f(x_0,y) \text{ is irreducible over } K.$$

For example, we might consider finding an infinite set $H \subset \mathbb{Q}$, a *universal Hilbert subset*, for which up to finite sets $H \subset H_f(K)$ for every irreducible $f \in \mathbb{Q}[x,y]$. [**FrJ86**, p. 289]$_2$ which lists results on this from [**Fr85**]. Specifically, it notes, to our knowledge, that the first explicit version of such is $H = \{[e^{\sqrt{\log(\log(m))}}]+m!2^{m^2}\}_{m-1}^{\infty}$ in [**Spr81**]. More arithmetically enlightening is the example of [**DZ98**, Thm. 1], $\{2^n+n\}$, a special case where you can replace 2 by b ($|b|>2$) and n by $p(n)$ where $p \in \mathbb{Z}[z]$ is any nonconstant polynomial.

Still, there is the question of effectiveness, as all these results rely on Siegel's Theorem that a function $f(w)$ on an affine curve in (z, w) will have at most finitely many $\mathbb{Z}[1/a]$ values at rational points of the curve, unless $f(w)$ has at most two poles, and a special form at that. Then, that taking on the special values listed in these papers is possible only finitely many times. Siegel's result though is (still) ineffective. Another approach is that of [**D96**, Cor. 3.7]. This effectively bounds the elements appearing in a given H_f, indeed, it allows any finite collection of polyomials in two variables. [**D96**, Express. (23)] makes no assumption on absolute irreducibility. It givies an explicit bounding expression depending on bounds d on the total degrees and heights h of the polynomials. This is explicit, and a polynomial in h. Whether such a bound is possible that is polynomial in both d and h appears not yet to be known.

The historical roots of the relation between the Chebotarev density theorem, especially its non-reregular analog [**Fr74**, §2] and its relation to [**FrS76**], where it was assiduously applied, and a proof of the **HIT** as given in [**Fr74**, §3]. The more general Field Crossing argument as in [**FrV92**, Lem. 1] appears entirely field theoretically in [**FrJ86**, §23.1]$_1$.

Finally, there is Weissauer's result for which one immediate conclusion is that the Hilbertianity property for fields can jump around a lot.

THEOREM 6.1 (Weissauer). *We assume $K \subset \bar{\mathbb{Q}}$. If K is Hilbertian, and L/K is Galois, then any extension K^*/L is Hilbertian if the inequalities $\infty > [K^* : L] > 1$ hold* [**FrJ86**, Thm. 13.9.1]$_2$.

Independence of **RIGP**, IGP *and Hilbertianity:* Now that we know there exist many **PAC** fields that lie deep in the algebraic numbers, we use them to consider what holds for all **PAC** fields. Rem. 6.3 gives one hint at the independence of the **RIGP** and the IGP. The **RIGP** holds for $\bar{\mathbb{Q}}$ from RET, but clearly the IGP does not. The following property is relevant to connecting the **RIGP** and hilbertianity.

DEFINITION 6.2. If, for a field L, each regular Galois cover $\hat{\varphi} : \hat{Y} \to \mathbb{P}^1_z$ over L has infinitely many irreducible fibers $\hat{Y}_{z_0}$, $z_0 \in \mathbb{P}^1_z$, we say L is **RG**-Hilbertian.

REMARK 6.3. The IGP can hold for a **PAC** field that is not Hilbertian, giving an independence statement of the relation between the two properties **HIT** and IGP. [**FrV92**, p. 480] constructs such as an overfield of a **PAC**, Hilbertian, field P defined as the fixed field of a subgroup $\tilde{H} \leq F_\omega$ that happens to be the Universal Frattini cover of the following *small* group: $\prod_{i=2}^{\infty} G_i$ where each finite group appears in $\{G_i\}_{i=2}^{\infty}$ exactly once.

6.1.2. *Relating $\mathcal{F}_{G,\mathrm{IGP}}$ and $\mathcal{F}_{G,\mathbf{RIGP}}$.*

6.1.3. *Diophantine problems calling for (G, G^*) realizations.*

6.2. Finite fields, $\mathbb{R}$ and p-adic fields. From the viewpoint of this book, [**FrJ86**, Chap. 19]$_1$ (resp. [**FrJ86**, Chap. 21]$_2$) barely scratches the surface of the historical motivation around the problems of arithmetic geometry. Each edition of the book emphasizes model theory of fields more than the previous. Yet, the p. 268 (resp. p. 452) statement

> Each of these concrete problems focuses our attention on rich historically motivated concepts that could be overlooked in an abstract model theoretic viewpoint.

Overlooked, because model theory tries to encompass any possible problem, while arithmetic geometry aims to develop new tools to handle bottlenecks previously blocking progress in understanding fields which provide solutions to various structured sets of algebraic equations. This subsection emphasizes the history, starting with Chevalley's Theorem §6.4. It certainly motivated the formulation of results about **PAC** fields, instigated by James Ax.

6.2.1. *Chevalley's and Kollár's Theorems.* Chevalley's Theorem drove diophantine considerations in many directions primarily by distinguishing for fields – among a collection $\mathcal{V}$ of varieties – between a member $V \in \mathcal{V}$ having an absolutely irreducible component defined over the field and having a rational point in the field.

There was nothing diophantine in the work of Abel, Galois or Riemann. Their work recognizes the mystery in relating all zeros of an irreducible polynomial over a field, and the role of the Galois group of the polynomial to it. Yet, earlier than these, was the work of Gauss (quadratic reciprocity specifically), Lagrange (Pell's equation and the values of forms), the great body of work on the nature of primes (say, Dirichlet's proof of primes in arithmetic progressions and L-functions attached to number field extensions), the attempt to solve Fermat's last theorem by so many (Dedekind's codifying results on algebraic number fields).

Still, if you had to take one theorem that had inordinate influence to its proof and sweep, it had to beThm. 6.4.[14] Use these notations for fields: a finite field of order q is $\mathbb{F}_q$; a completion of a number field K at a prime $\boldsymbol{p}$ is $K_{\boldsymbol{p}}$; and the formal power series in a variable t over $\mathbb{F}_q$ is $\mathbb{F}_q[[t]]$.

THEOREM 6.4 (Chevalley). *A form F of degree d in $\mathbb{P}^d$ over a finite field $\mathbb{F}_q$ has a point in $\mathbb{F}_q$. So, that form, over $\mathbb{F}_q$ contains an absolutely irreducible $\mathbb{F}_q$ variety.*

E. Artin, its formulator, also apparently suggested the next step up:

(3.69) A degree d form in $\mathbb{P}^{d^2}$ over a p-adic field K_p should have a point in K_p.

[14] [**BvSh66**, p. 5] reproduces the proof after an introduction to polynomials modulo p. It does the proof over $\mathbb{Z}/p$, but says it works over any finite field. The main replacement is $a^{p-1} \mapsto a^{q-1}$ in Euler's Theorem on the multiplicative group of nonzero elements in $\mathbb{F}_q$.

Lang [**La52**] suggested this might be true by proving it held for $\mathbb{F}_q[[t]]$. Ax and Kochen showed that any nontrivial ultaproduct of $\{\mathbb{Q}_p \mid \text{ primes } p\}$ is isomorphic to the same ultraproduct of the fields with $\mathbb{F}_p[[t]]$ replacing $\mathbb{Q}_p$. So, any arithmetic geometry statement quantifying algebraic sets that could be interpreted in this set for either ultraproduct would be *true* for almost all p in one if and only if in the other. Thus this Artin Conjecture, followed in this form from Lang's Theorem.

These are statements (not pure existential) in the first order predicate theory of finite fields. That means – given d – there are collections of variables quantified by $\forall$ (for all) and by $\exists$ (there exists). Here: $\forall$ set of coefficients of a hypersurface of degree d, $\exists$ values of the variables in $\mathbb{F}$ (placeholder for a finite field).

Question Q_d: is this statement true for all, or all but infinitely many, or infinitely many q, with $\mathbb{F}_q = \mathbb{F}$? It is those problems that drove Ax, and for which he and Simon Kochen won their Cole Prize. [15]

The major shock, in a way, was that unlike Chevalley's Theorem, the Artin Conjecture was true only for almost all p: For each fixed d there were usually a host (but finite) of primes p for which there were hypersurfaces of degree d in $\mathbb{P}^{d^2}$ that had no $\mathbb{Q}_p$ points.[16]

Ax knew the algebraic numbers for *certain* ultraproducts aren't **PAC**, for essentially the same reason that p-adic fields aren't. Yet, he still conjectured that Chevalley's Theorem held for any perfect **PAC** field. In particular for any case where the algebraic numbers in an ultraproduct were **PAC**. Indeed, the case when a **PAC**field had abelian absolute Galois group followed from Chevalley's Theorem. Such a field could not be Galois over $\mathbb{Q}$, and perhaps that constrained his thinking about **PAC**field. He even conjectured that being both **PAC** and Galois over $\mathbb{Q}$ was not possible, except for $\bar{\mathbb{Q}}$. That was shown wrong in [**FrJ78**]. That negative comes out in a positive way in Ch. 4.

CONJECTURE 6.5 (Ax). A hypersurface of degree d in $\mathbb{P}^d$ over a perfect **PAC** field K, contains an absolutely irreducible K subspace.

[**Ko07b**] starts out immediately by using an intrinsic, rather than the hypersurface equation (extrinsic), form of such a hypersurface V. It is a *Fano variety*: Its canonical class κ_V has the property that its *negative* is *ample*.

REMARK 6.6 (Hypersurface intersections). Following [**DeJL83**] the actual result in [**Ko07b**, Thm. 2] extends to the intersections of hypersurfaces in $\mathbb{P}^d$ whose degrees sum to at most d.

[15][**BvSh66**, p. 58–59] includes many comments on this, without reference to Ax-Kochen, including its truth for $d = 2$ and 3, and with d^2 replaced by an explicit, but large, $N(d)$ its truth without reservation in [**Bra45**].

[16]Nor is there an obvious rational for the exceptional primes for a given value of d, [**Sch84**].

6.2.2. *The Conjectures: Ax, Shafarevich, Fried-Völklein.* Prop. 5.9 plays on finding Hurwitz spaces $\mathcal{H}(G,\mathbf{C})^*$ with a single absolutely irreducible component. Given G, but allowing $\mathbf{C}$ to vary, we know one component is very common, if all classes in $\mathbf{C}$ appear suitably often. That hypothesis, however, doesn't hold if – for good reason – we restrict to the case $r = 4$, by which we can compare with classical situations, especially with modular curves, as we do in Ch. 5.

REMARK 6.7 (**HIT** vs Chebotarev). Ax found the algebraic closure of $\mathbb{Q}$ isn't the only **PAC** subfield, L, of $\bar{\mathbb{Q}}$. Almost (but not all) fields of algebraic numbers of a non-trivial *ultraproduct of finite fields* are **PAC**. Based on *Chevalley's Theorem* and the *Lang-Weil result*, Ax made conjectures:

(3.70a) A $\mathbb{Q}$ form of degree d in projective d space has an L point; and

(3.70b) The only **PAC** field L that is Galois over $\mathbb{Q}$ is $\bar{\mathbb{Q}}$.

He was significantly right about (3.70a) as Kollár [**Ko07b**] showed (§ refchevalley). He was significantly wrong about (3.70b). Not only could be it Galois, it could also be Hilbertian, as [**FrJ78**] shows by presenting every projective curve X over $\mathbb{Q}$ as $\varphi : X \to \mathbb{P}^1_z$ with *simple branching* (branch cycles are 2-cycles) with an arbitrarily high number of branch points. Thus, the Galois closure cover $\hat{\varphi}$ is regular with group $S_{\deg(\varphi)}$ (Rem. 6.8).

REMARK 6.8 (Canonical Fields I). The source of **PAC**, Hilbertian fields is from an arithmetic form of a Lefschetz argument, as in Rem. 6.7. Nonsingular projective curves project birationally over $\mathbb{Q}$ to give a plane (in $\mathbb{P}^2$) curve, X, of degree $\deg(X) = n_X$, with only ordinary double point singularities. Take a suitably general $\mathbb{Q}$ point $u \in \mathbb{P}^2 \setminus X$, so that any lines L through u meets X at at most one point with multiplicity 2. With $\tilde{X}$ the projective normalization of X, this produces:

(3.71a) A natural map: $x \in X \mapsto L_{x,u} = \varphi_{X,u}(x)$ the line through x;

(3.71b) by extension to $\tilde{X}$, $\tilde{\varphi}_{X,u} : \tilde{X} \to \mathbb{P}^1$ is a simple-branched (branch cycles are 2-cycles) regular cover; and

(3.71c) the monodromy group of $\tilde{\varphi}_{X,u}$ is S_{n_X}.

Applying **HIT** to $\tilde{\varphi}_{X,u}$ produces ∞-ly many $z' \in \mathbb{P}^1_z(\mathbb{Q})$ giving decomposition fields $K'_z/\mathbb{Q}$ with group S_{n_X} disjoint from any a' priori given finite extension of $\mathbb{Q}$. By compositing infinitely many of these z's, we easily get a field over which X has infinitely many points.

Alas, we want for any one integer n, just *one copy* of S_{n_X} to appear in the final composite L_{fin}, and yet X has infinitely many L_{fin} points. Here is how they come from other distinct copies of $S_{n'}$ with n' varying.

List infinitely many copies of X as $\{(X,j)\}_{j=1}^{\infty}$. Now, induct on j to produce a field $M_{X,j}/\mathbb{Q}$ with group $S_{n_{X,j}}$ over which there is a guaranteed new point $m_{X,j} \in$

X with coordinates not in a field $M_{X,j-1}$ indicated inductively below. Here is our device for this. Let $n_{X,j} = n_X \cdot n'_{X,j}$ where $n'_{X,j}$ has been selected so that $n_{X,j} > n_{X,j-1}$. Consider among all the degree $n'_{X,j}$ maps $f : \mathbb{P}^2 \to \mathbb{P}^2$ over $\mathbb{Q}$ one for which the pullback, $f^*(X)$, of X still satisfies the Lefshetz singular point condition.

Now, with a choice of $\mathbb{Q}$ point $u_{f^*(X)}$ as above, apply **HIT** to produce the desired $S_{n_{X,j}}$ extension over $\mathbb{Q}$ from a point m' that generates an extension over $\mathbb{Q}$ disjoint from $M_{X,j-1}$ and for which $m_{X,j} \stackrel{\text{def}}{=} f^*(m') \notin M_{X,j-1}$. Define $M_{X,j}$ as the composite of this field with $M_{X,j-1}$. [17]

REMARK 6.9 (Canonical Fields II). Shafarevich's case of Conj. 5.7 replaces $\prod_{n=2}^{\infty} G_i$ with a canonical group (and field) $(\mathbb{Z})^* = G(\mathbb{Q}^{\text{cyc}}/\mathbb{Q})$. Mightn't we form a canonical field based on symmetric groups from the field of composites, $\mathbb{Q}^{S_\infty}$, of all extensions of $\mathbb{Q}$ having S_n, for some n as Galois group?

It is a canonical, Galois over $\mathbb{Q}$, projective extension of $\mathbb{Q}$ that contains the intersection of all the **PAC** fields that could appear in Thm. 5.4. Yet, it is not Hilbertian. No regular extension of $\mathbb{Q}$ with any group S_n would have nontrivial specializations over $\mathbb{Q}^{S_\infty}$: $\mathcal{G}_{\mathbb{Q}^{S_\infty}}$ is not (isomorphic to) F_ω.

Other canonical fields appear for which these questions, especially their relation to Hilbertianity, are valuable. One is the totally real algebraic numbers, $\mathbb{Q}^{\text{tr}}$, consisting of algebraic numbers all of whose conjugates are real (see §6.1.1). We comment here on the solvable closure, $\mathbb{Q}^{\text{sol}}$, of $\mathbb{Q}$. Is this a **PAC** field [**FrJ86**, Prob. 1 a, p. 748]$_1$? It is projective (as a subfield of a projective field $\mathbb{Q}^{\text{cyc}}$). It isn't Hilbertian or even RG-Hilbertian: No regular solvable group extension has a nontrivial specialization over $\mathbb{Q}^{\text{sol}}$. Iwasawa conjectured $\mathcal{G}_{\mathbb{Q}^{\text{cyc}}} = F_\omega$ [**FrJ86**, p. 754]$_2$. Alas, they can't *both* be correct: **PAC** + ω-free implies Hilbertian (Lem. 5.6). [18]

REMARK 6.10 (Hilbertian-like Properties). The RG-Hilbertian for a field L considers the specialization property – infinitely many fibers over $z' \in \mathbb{P}^1_z(L)$ have the whole group as decomposition group – only for *regular* Galois covers $\hat{\varphi} : \hat{X} \to \mathbb{P}^1_z$. The argument of Lem. 5.6 shows, if L is **PAC**, then it is RG-Hilbertian if and only if the IGP holds [**FrV91**, Thm. B]. A general construction produces RG-Hilbertian **PAC** fields that are not Hilbertian [**FrV92**, p. 479] in the following way. List all finite groups, each just once (up to isomorphism), as $G_1, G_2, \ldots$ with

[17] We considered only one X. By, however, ordering $\{(X,j)\}_{\text{appropriate } X, 1 \le j < \infty}$, the above works by changing $M_{X,j}/\mathbb{Q}$ to include the composite of all the fields associated with those (X', j') that come before (X, j). Further, when you get to $S_{n_{X,j}}$, add any missing $S_{n'}$ s with with $n' < n_{X,j}$ by taking any regular $S_{n'}$ cover and applying **HIT** to it, keeping it disjoint from extensions appearing previously in the construction.

[18] Galois died so long ago. Yet $\mathbb{Q}^{\text{sol}}$ remains such a mystery. I'd bet that $\mathbb{Q}^{\text{sol}}$ is not **PAC**. Yet, ... G. Frey showed the nilpotent closure of $\mathbb{Q}$ isn't **PAC**, by giving genus 1 curves over $\mathbb{Q}$ without such points. [**CW06b**, p. 222] exposits on conditions on genus 1 curves that guarantees they do have $\mathbb{Q}^{\text{sol}}$ points using the Weil-Chatalet group of the Jacobian of the curve.

$|G_1| = 2$. Since $\mathcal{H} = \prod_{i=1}^{\infty} G_i$ has countable rank, it is a quotient of F_ω, represented as $\mathcal{G}_L$ with L a **PAC** field. The projective group formed from the Universal Frattini cover, $\tilde{\mathcal{H}}$ of $\mathcal{H}$ (§1.3), therefore embeds as a subgroup of $\mathcal{G}_L$.

Now denote the fixed field of $\tilde{\mathcal{H}}$ by L^*, which by Thm. B (loc. sit.) is RG-Hilbertian. If L^* were Hilbertian, then $\mathcal{G}_{L^*}$ would also be F_ω and every finite embedding problem over L^* would be solvable. Consider, however, the covers $\tilde{\mathcal{H}} \to G_1$ (factorization through $\mathcal{H}$) and $\tilde{\mathcal{H}} \to S_5$ (from F_ω being profree. There is no way to solve this embedding problem as that would give A_5 as a subgroup of the kernal of the pullback of G_1 in $\tilde{\mathcal{H}}$. That kernel, however, is pronilpotent [**FrJ86**, Lem. 20.2]$_1$ (§1.3), certainly not simple.

6.2.3. *Getting to their applications.* [**?**, §6] explains enough of the Cohen-Lenstra problem to remark on the relevance of (6.21d). Let $C(d)$ count the number of square-free monic polynomials $f \in \mathbb{F}_q[t]$ of degree $2d+1$, and let $N(d)$ be the sum, over f, of $h-1$, where h is the number of ℓ-torsion elements in the class group of $\mathbb{F}_q(t; , \sqrt{f})$. They necessarily assume q, a prime power (order of a finite field) is large as a function of ℓ and $\ell \not| q(q-1)$. Here they are trying to show $C(d)/N(d)$ approaches 1 as $d \mapsto \infty$. The ingredients of this result get to the heart of the paper.

(3.72a) The Jacobian of a curve interprets statements about abelian unramified covers of a curve, and so questions about ℓ-torsion of class numbers. You then see that counting $\mathbb{F}_q$ points on the Hurwitz space for $G = D_\ell$ (dihedral group of degree ℓ) is what you are after.

(3.72b) [**?**, Cor. 5.8.2] is the stable homology result, essentially saying that if the jth $\mathbb{Q}$ homology is stable along a system of Hurwitz space components as d gets large, then the jth homology is the same for those Hurwitz space components as it is for the *configuration space* which the Hurwitz space covers.

(3.72c) [**?**] shows a corresponding isomorphism of the ith étale cohomology of the Hurwitz space components and of the configuration space assuming d exceeds some function of i.

(3.72d) Now you need a bound on the (count of points contribution of the) cohomology outside the range of values of i for which their stability result holds. They say the argument is exactly as in the proof of [**?**, Thm. 8.7].

Comment on (3.72d). See (**????**) and (**????**) for taking advantage of the nice arguments in [**?**].

6.2.4. *Points on Hurwitz spaces.* Actually, Pierre and Michel Emsalem have facility with a version of the Deligne Mumford compactification of the Hurwitz space, as does Wewers, which Wewers did at the same time Mochuzuki did it, possibly influenced (Wewers certainly was, I was in Essen at the time; and I was in

contact with Ihara at the time) by my 1995 (first) paper on Modular Towers. I gave a compactification in the paper, based on iterated normalization on the boundary, very non-DM. The application there was to giving examples of projective systems of Modular Tower components uniformly defined over $\mathbb{Q}$.

Pierre and Michel aimed at giving ℓ-adic points on the (full) Modular Tower of any finite group, for a Nielsen class with sufficiently many Harbater-Mumford representatives (there is a precise quantitative statement). That now seems like a long time ago, and I have not looked back at this topic since that time.

I went in the Modular Tower direction because, as I told Ellenberg when I gave lectures at Wisconsin, I didn't know enough homotopy theory to go after the specific problem that I wanted, for which one result in that direction was exactly the stable homotopy result that Ellenberg-Venkatesh-Westerland were going after. Conway-Fried-Parker-Voelklein was the stable H^0 result. So, for me that problem goes back to, essentially 1993, the beginning formulation of the Modular Tower program, which had a preliminary paper with Pierre. That was the result quoted in the abstract below. The certain types of torsion points being cyclotomic torsion points. This still, as far as I know, unsolved problem – about regular realizations of dihedral groups – was generalized by Modular Towers to (essentially) all finite groups.

29. with P. Debes, Nonrigid situations in constructive Galois theory, Pacific Journal 163 (1994), 81122. This uses the results of "Rigidity and Real Residue Classes" on several problems among which are these.

Show every finite group is realized regularly over the totally real (all conjugates real) numbers. How to construct Sn covers with four branch points with the covers also having real points (can't be done with three branch points). Based on Mazur's Theorem on torsion points on elliptic curves over the rationals, if m is a prime larger than 7, then the dihedral group of order 2m isn't regularly realized over the rationals with fewer than 6 branch points. #3 amounts to the formulation of the M(odular) T(ower) program just for dihedral groups (see the html file for URLs to the MT Time Line), a statement equivalent to finding certain types of torsion points on hyperelliptic Jacobians. NonRigidGT.html

6.3. Correspondences and other Grothendieck topics.

CHAPTER 4

Spaces test the RIGP

We assiduously use ℓ as a prime involved in the construction of Frattini covers, of a given (finite) group G and the moduli spaces associated to it. While p is reserved for primes that appear for separate purposes, say, reduction of those moduli spaces modulo p. §5.2, in particular, has gone through the story of how advantage was made of translating the regular version of the Inverse Galois Problem (at least in characteristic 0) to the story of rational points on Hurwitz spaces.

Here we start the formation of natural towers of moduli spaces: **M**(odular) **T**(ower)s (**MT**s). For simplicity we start with the assumption that G is ℓ-perfect. In, however, §3, we remove that assumption, by avoiding the Ext-Frattini covers that appear in Cor. 2.6, without removing any significant Frattini covers from consideration. **MT**s generalize modular curves in precise ways (as in §3.2), while we can use finite group theory to exert control over from.

Further, towers from essentially *any* pair (G, ℓ), with G a finite group that is ℓ-perfect, have revealed much on how to compare them with modular curve towers. In particular, how their properties, proven and conjectural generalize modular curve properties, especially around properties of cusps.

§1 constructs the towers, including being precise on when they are nonempty. It also explains why our structural statements concentrate on ℓ-Frattini covers. For example, Ch. 3 Prop. 5.9 dealt with all finite groups of necessity. §2 lists the main **MT** conjectures, and the progress on them. Here, in using the Branch Cycle Lemma (**BCL**) as characterized in Ch. 2 Prop. 4.1, we distinguish between two cases.

(4.1a) When all components of a tower have definition field a finite extension of $\mathbb{Q}$ (possibly just $\mathbb{Q}$ itself).

(4.1b) When the definition fields of the tower levels grow with the level, and how much we can figure what they are.

Even modular curve towers display both phenomena.

§4.2 reexamines Serre's **O**(pen)**I**(mage)**T**(heorem), pointing to the book's conclusion.

When reduced Hurwitz spaces are one dimensional, parametrizing covers with 4 branch points, they are upper half plane quotients ramified at the expected 3 points of the j-line (Ch. 2 Prop. 2.7).

Ch. 5 has **MT**s whose levels are all such j-line covers. This illustrates with one example that displays phenomena generalizing the **OIT** subject to them being akin to modular curve towers – which we also regard as one example. Yet, nowhere among its tower levels are there any modular curves.

1. Constructing MTs

Any particular tower has levels indexed by a parameter $0 \le k < \infty$. All levels are Hurwitz space components defined by Nielsen classes, with level 0 defined by a Nielsen class $\mathrm{Ni}(G, \mathbf{C})$, with $\mathbf{C}$ a collection of $r \ge 3$ conjugacy classes in G. Typically in our main applications, as does Ch. 3, this starts with a rational union, ${}_*\mathbf{C} = {}_*\mathrm{C}_1, \dots, {}_*\mathrm{C}_{r^*}$, of distinct conjugacy classes in G. As previously, denote the gcd of the orders of elements in ${}_*\mathbf{C}$ by $N_{{}_*\mathbf{C}}$.

For a fixed, centerless, G, the $\mathbb{Q}$ points on the corresponding Hurwitz space $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$ correspond to the complete collection of regular extensons $L/\mathbb{Q}(z)$ realizing G as a Galois group over $\mathbb{Q}$ with $\mathbf{C}$ as branch cycles.

Our basic assumption for forming **MT**s is the following.

(4.2) ℓ'-*condition*: $(\ell, N_{{}_*\mathbf{C}}) = 1$; that is, ${}_*\mathbf{C}$ consists of ℓ' classes.

From (4.2), §3.1 canonically produces **MT**s based on the Ch. 3 Prop. 2.18 construction of the centerless, ℓ-perfect groups ${}^k_\ell G_{\mathrm{ab}}$ that give the Hurwitz spaces $\mathcal{H}({}^k_\ell G_{\mathrm{ab}}, \mathbf{C})^{\mathrm{in}}$ on which the **MT** levels fall.

1.1. Constructing Frattini modules. We now outline the proof of [**Fr02**, §2.2.1-2.2.2, culminating in Thm. 2.8] adding comments on explicitness. First step: Replace G by the normalizer, $N_G(P) \stackrel{\mathrm{def}}{=} N$, in G, to consider the case P is normal in G, as in (1.15a). To avoid confusion about the characteristics kernels, refer to them as $\mathcal{K}_N = \{\ker_k(N)\}$. So, start by constructing ${}_\ell M_N$.

As in Ch. 3 Rem. 1.9, the *Todd-Coxeter* (a la Shreier's) *algorithm* suffices to form generators of M_P since we explicit relations from $\ker_1$ as required. Lem. 1.26 assures that the action of N/P extends to ${}_\ell N/\ker_1 = {}_\ell{}^1 N$.

[**Fr02**, Thm. 2.10] I SHOULD PUT THIS IN THE PAPER PROPER Suppose p divides the order of g ? Gk. Then, any lift g ? Gk+1 has order p ord(g). Assume g ? Gk is a p? element. A unique p? conjugacy class of Gk+1 lifts g. If G0 is centerless and p-perfect, so is Gk for all k. The action of H extends to it by applying Prop. 1.30, but now we need some additional information. For (6.19b), this is essentially a special case of (1.15a). Then, except for noting that the rank of $(\mathbb{Z}_\ell)^t$ as a $\mathbb{Z}_\ell$ module is the same as the dimension t of the vector space $(\mathbb{Z}/\ell)t$, we get to the real issue: Constructing ${}_\ell M_G$. We will use pieces of this in the body of the book. We regard Fp[G0] as ? G0 ? a left Fp[G0] module and as a right Fp[G0] module. The induced module indG?0 (M0) is the G0 module M0? ?Fp[G?0] Fp[G0] = M0? ?Fp

Fp[G0/G?0]. The notation Fp[G0/G?0] is for the right G0 module written as the vector space ? G0? generated by right cosets of G0 in G0. Then, indG?0 (M0) is a right G0 module. Suppose N is a right G0 module. Any Z/p[G?0] homomorphism ? : M ? N G0 g extends to a Z/p[G0] module homomorphism IndG?0 (M) ? M by m ? g ? ?(m) . Recall that M0 is an indecomposable G0 module ([Ben91, p. 11, Exec. 1] or [FK97, Indecom. Lem. 2.4]). To characterize M0 as the versal module for exponent p extensions of G0, we use this result [Fri95, Prop. 2.7]. Proposition 2.5. The cohomology group H2(G0, M0) has dimension one over Fp. The 2-cocycle for the short exact sequence 1?M0 ?G1 ?G0 ?1 represents a generator. We define any nontrivial ? ? H2(G0,M0) as G1 up to an automorphism fixed on the G0 quotient and multiplying M0 by a scalar. □

Then, a particular **MT**, formed from $(G, \ell, {}_*\mathbf{C})$ starts from a Nielsen class $\mathrm{Ni}(G, \mathbf{C})$ with each class of ${}_*\mathbf{C}$, and no others, appearing in $\mathbf{C}$. Since we have diophantine considerations based on the appearance of groups as Galois groups over $\mathbb{Q}$ as a primary goal, eventually those $\mathbf{C}$ considered for level 0 will fall among *rational* conjugacy class sets of the form ${}_*\mathbf{C}^{\boldsymbol{n}} = {}_*\mathrm{C}_1^{n_1} \dots {}_*\mathrm{C}_{r^*}^{n_{r^*}}$ from a vector $\boldsymbol{n} \in (\mathbb{Z}^+)^{r^*}$. Again: These form a semi-group under slotwise multiplication which, denoted $\mathcal{R}_{{}_*\mathbf{C}}$.

Now we give the data, based on notation from §**??**, for the level k Nielsen class from which level k of a particular tower from $\mathrm{Ni}(G, \mathbf{C})$ will appear. This subsection concludes with an if and only if condition that there are nonempty **MT**s from this data.

As in §**??**, RETURN We list places of increasing difficulty for computing $\tilde{G}$, given G, including using the idea of lifting orders of ℓ elements to Schur quotients.

(4.3a)

[**Fr02**, Prop. 2.8] gives a reasonably effective computation of the kernel of $G_1 \to G$. Remind of this.

Prop.

Remark 1.1 (Central Frattini vs Universal Frattini covers). A representation cover $\psi : R \to G$ has finite kernel, and it is a Frattini cover. By contrast, $\tilde{\psi}_G \to G$, being a projective group, has no points of finite order. Yet, ψ_G factors through ψ. Yet, that central Frattini cover plays a signficant role in almost every aspect of **MT**s.

(4.4a) Starting with Prop. **??** which, in particular, characterizes when a **MT** is nonempty.

(4.4b) Continuing with the characterization of particular types of cusps in the case when level 0 of a **MT** is given by $\mathrm{Ni}(G, \mathbf{C})$ where $\mathbf{C}$ consists of 4 classes.

§1.7 continues this discussion.

REMARK 1.2 (Loewy display need).

2. ℓ-perfect and centerless

[**BFr02**, Prop. 3.21] has the ℓ-perfect and centerless result that says this replicates up the **MT**. We went where the motivating problems (the **OIT** included) led us. They weren't handpicked to have general ideas apply to make them comprehensible. We discover their definition fields through extensions of the **BCL** that connect to properties that sometimes – but not always – trace to topics arising with the moduli of curves of genus g. For spaces of 3 branch point covers, I suppose popularly called *dessin d' enfant*, there do seem to be inexplicable accidents. In our experience, they disappear when $r \geq 4$.

RETURN Here we will list what we know about the appearance of irreducible $\mathbb{Q}$ components in inner Hurwitz spaces.

3. Ext-free ℓ-Frattini covers

Cor. 2.6 refers to ℓ-Frattini central extensions of the type Ext-Frattini. They appear from an abelian cover of $G_{\rm ab}$, the commutator quotient of G. For a prime ℓ that divides $G_{\rm ab}$, they are the natural generalization of the ℓ-Frattini cover $\mathbb{Z}/\ell^2 \to \mathbb{Z}/\ell$. If we allow such extensions for a prime ℓ, then even if G is centerless, then the 1st characteristic ℓ-Frattini cover, ${}^1_\ell G \to G$ of G, would have a nontrivial center, contrary to the conclusion of Prop. 2.18.

On the other hand, if we just remove ℓ from consideration, then we could be leaving out significant ℓ-Frattini extensions of G. For example, $G = S_n, n \geq 4$, and the prime $\ell = 2$ as in Ex. 2.11, and the case $\ell = 2$ of Serre's **OIT** as in §3.2 or the case $\ell = 3$ of our main example, §3.

3.1. M(odular)T(ower)s from ℓ' conjugacy classes C.

CONJECTURE 3.1. There is a $\mathbf{C} \in \mathcal{R}_{*\mathbf{C}}$ for which $\mathcal{H}(G, \mathbf{C})^{\rm in}$, as a moduli space, has a rational point. In particular, that point would give a regular realization of G over $\mathbb{Q}$.

LEMMA 3.2. *Assume* (3.1) *and also assume the Main Modular Tower conjecture. Then, the* $\mathbf{C}$ *for which there are* $(G, \mathbf{C})$ *regular realizations over* $\mathbb{Q}$ *RETURN*

So, here are natural questions assuming the **RIGP** is true.

(4.5a) If there are any $\mathbb{Q}$ points among them, for what $\mathbf{C}$ would they appear?

Hurwitz space types depend on cover equivalences.

Use *inner, reduced*: appropriate for **RIGP**. §**??** has brief reminders of elementary, but key, definitions we will use. For example, the meanings of the following

phrases for a group G: nilpotent; an ℓ' subset; being ℓ-perfect; ℓ-Frattini cover; and Schur multiplier and its relation to Frattini central extensions.

PROPOSITION 3.3. *Simple groups: Inadequate for the Inverse Galois Problem (set $S \subset G$ is p' if its elements are prime to p.)*

-
- $(G,p) \implies \exists$ *sequence* $G = G_0 \leftarrow G_1 \leftarrow G_2 \leftarrow \dots$ *of group covers and integer* $\nu(G,p)$ *with these properties:*
- $M_k = \ker(G_{k+1} \to G_0) = (\mathbb{Z}/p^{k+1})^{\nu(G,p)}$, $k \geq 0$ *the level.*
- *If G is centerless, then so are all the G_k s.*
- $\psi_k : G_{k+1} \to G_0$ *is a p-Frattini cover.*[*3]
- *There is a maximal* $\nu(G,p)$, $\nu(G,p)_{\max}$ *(> 1 unless G is $\mathbb{Z}/p^t \times^s H$, $(|H|,p) = 1$).*[*4]

[**BFr02**, §2] *cleans up some delicate points related to the action on reduced Nielsen classes.*

CONSTRUCTION COMMENTS. □

DEFINITION 3.4.

- Schur-Zassenhaus $\implies \exists \{\mathcal{H}(G_k, \mathbf{C})^{\text{in,rd}}\}_{k=0}^{\infty} \stackrel{\text{def}}{=} \mathcal{H}_{G,\mathbf{C},p}$.[*5]
- Reduced: Equivalence $\varphi : X \to \mathbb{P}^1_z$ and $\alpha \circ \varphi$, $\alpha \in \mathrm{PSL}_2(\mathbb{C})$.[*6]
-

  DEFINITION 3.5 (abelianized inner, reduced **MT**). *Nonempty* projective sequence $\{\mathcal{H}'_k\}_{k=0}^{\infty}$ of components on $\mathcal{H}_{G,p}$.

  $$\mathcal{H}'_k \to S_r \backslash (\mathbb{P}^1)^r \setminus \Delta / \mathrm{PSL}_2(\mathbb{C}) \stackrel{\text{def}}{=} J_r; J_4 = \mathbb{P}^1_j \setminus \{\infty\}$$

- $M(G,p,\mathbf{C})$ *Main conj.*: Number field $K, \mathcal{H}'_k(K) = \emptyset, k >> 0$.
  - Generalizes $\{X_1(p^{k+1})(K) = \emptyset \text{ off cusps}\}_{k>>0}^{\infty}$.

Any projective sequence $\{\mathcal{H}'_u\}$ of components of $\{\mathcal{H}(G_u, \mathbf{C})\}_{u=0}^{\infty}$ is a(n abelianized) Modular Tower; *over K* if all are defined over K. This generalizes the tower of modular curves $\{X_1(\ell^u)\}_{u \in \mathbb{N}}$, off their cusps, associated to the dihedral group D_ℓ, ℓ odd. For p a prime, $\mathbb{Q}_{p,\text{unr}}$ is the maximal unramified extension of $\mathbb{Q}_p$, the p-adic numbers.

(4.6a) Dèbes and Emsalem, separately Wewers, used a Deligne-Mumford compactification for Fried's result showing $G_{\mathbb{Q}}$ permutes Harbater-Mumford components.

(4.6b) A Modular Tower in (3.59c) over $\mathbb{Q}$ is subject to the *Main Modular Tower conjecture*: For any number field K, high tower levels should have no K points. Else, one fell-swoop would give **RIGP**realizations of the mysterious sequence $\{G_u\}_{u=0}^{\infty}$.

(4.6c) For each allowable pair (G, ℓ), Dèbes and Emsalem applied (3.59c) to a fixed Harbater-Mumford $(G, \mathbf{C})$ to regularly realize the whole uniform sequence of groups $\{(G_u)\}_{u=0}^{\infty}$ over $\mathbb{Q}_{p,\mathrm{unr}}$, for each p not dividing $|G|$.

Fried formulated the likely generalization of Harbater-Mumford triples $(G, \mathbf{C}, \ell)$, under the Modular Tower assumptions, referring to $\mathbf{C}$ as g-ℓ'. For such $\mathbf{C}$, we can explicitly label the components of $\mathcal{H}(G, \mathbf{C})$ as being g-ℓ' components. Again, in the search for where regular realizations might be hiding, and, in light of the Fundamental Conjecture, where they likely could not be hiding, the following conjectures/results came about.

(4.7a) Fried showed the Fried-Serre lift invariant is trivial for g-ℓ' components, and so above such a component there is a nonempty Modular Tower.

(4.7b) Fried conjectured the only Modular Towers with a projective sequence of $\mathbb{Q}_p$ points must be g-ℓ'. Emsalem proved a close approximation to this conjecture, and showed the conclusion of (4.6c) holds for these Modular Towers, too.

(4.7c) For $\mathbf{C}$ consisting of $r = 4$ (or less) elements, Fried gave an explicit proof of the Fundamental conjecture (2005; no K points at high levels), assuming at any level a p-cusp. Cadoret and Tamagawa (2008) gave a general inexplicit proof.

Explicit in (4.7c) means Fried developed a formula for the genus of reduced Hurwitz spaces (which for $r = 4$ are upper half-plane quotients). His computations showed, under the p-cusp condition – expected at high levels of a g-ℓ Modular Tower, the genus of tower levels rises with u, giving the conjecture as an application of Faltings. Cadoret-Tamagawa is a statement on 1-dimensional families of abelian varieties, without explicit spaces attached to them, but also an application of Faltings. Indeed the two proofs relate to the natural ℓ-adic representations hidden in abelianized Modular Towers stemming from (motivic) components of jacobians from level 0. This led to the natural next step.

Going beyond the case $\mathbf{C}$ has $r = 4$ four classes leads to tower levels of dimension $r - 3$, and so beyond a use of any present version of Falting's Theorem. So, for the fundamental theorem, any use even of Lang-Type conjectures requires an intermediate step that supercedes (4.7c).

The following gives the latest material coming from all involved schools.

(4.8a) Development of cases to test if for $r > 4$, high Modular Towers levels have *general type*: Have sufficiently many holomorphic differentials. For certain cases, Fried has developed half-canonical differential forms that can be used for this.

(4.8b) Fried, and Cadoret and Tamagawa, have separate approaches and progress giving a *Serre Open Image Theorem*. In Fried's formulation this relates the Galois action on the attached ℓ-adic representations to the arithmetic monodromy group of a Modular Tower, whether over a number field or not.

(4.8c) Dèbes has expanded on the Beckmann-Black conjectures on regular realization based on asking if there could be for each G a finite number of Nielsen classes corresponding to $(G, \mathbf{C}_1, \dots, \mathbf{C}_v)$ so that each regular realization of G is obtained from pullback of a cover $\mathbb{P}^1 \to \mathbb{P}^1$ of a cover from $(G, \mathbf{C}_i)$ for some $i \in \{1, \dots, v\}$.

Dèbes and Legrand have produced an invariant that gives a minimal value of v (dependent on G). They have computed that invariant in several cases, thereby showing that one Nielsen class ($v_G = 1$) will not suffice for most groups G. Whether some finite v_G will always work is still unknown, but it does in some known cases.

4. Arithmetic/Geometric monodromy in a MT

§4.1 starts with the key definition – *eventually Frattini* – that leads quickly to the conjectures that guide us to formulating a generalization of Serre's **OIT**.

As defined in Ch. 1 (1.12), the sequences ${}^{k}_{\ell}G_{\rm ab} \to G$ that define **MT**s are ℓ-Frattini covers of ${}^{0}_{\ell}G = G$. A general case of what we are after would start with $\mathbf{C}$, ℓ' conjugacy classes in G, $r = r_{\mathbf{C}}$, for which we investigate Question 4.1.

Question 4.1. Do the monodromy groups over J_r of levels of a **MT** from $\{\mathcal{H}({}^{k}_{\ell}G_{\rm ab}, \mathbf{C})^{\rm in,rd}\}_{k=0}^{\infty}$ inherit eventually ℓ-Frattini properties from the defining covers in their Nielsen class definition.

A paraphrase of the full conjectures is that **MT**s are sequences of moduli spaces whose monodromy groups over the configuration space J_r, and even all their decomposition groups, inherit this eventually ℓ-Frattini property from the moduli problem that defines them.

That moduli problem starts from the **RIGP**. A case that keeps us close to both problems, where the ℓ-Sylow of G is both normal and abelian starts in Ch. 3 (3.57).

4.1. Eventually Frattini sequences. Prop. 4.3 gives a first consequence of the eventually Frattini property that suffices as a weak **OIT**, and thereby **OIT**-Conj$_1$ (Conj. 4.5) for **MT**s that they will satisfy this property. **OIT**-Conj$_2$ is much stronger; even in Serre's **OIT** there are still unsolved aspects of it.

Definition 4.2. Refer to a sequence of covers of finite groups

$$\cdots \to H_{k+1} \to H_k \to \cdots \to H_1 \to H_0 = G$$

as *eventually Frattini* (resp. eventually ℓ-Frattini) if for some k_0, $H_{k_0+l} \to H_{k_0}$ is a Frattini (resp. ℓ-Frattini) cover for $l \geq 0$.

Suppose the projective limit of the H_k s is $\tilde{H}$. We say $\tilde{H}$ is eventually Frattini since the same property will hold for any cofinal sequence of quotients.

Notation for the extension of the **OIT** uses Serre's case in §4.2. In our main example, as we do in Serre's case, we use the relation between two systems of Nielsen classes: $\{\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})\}_{k=0}^{\infty}$ and $\{\mathrm{Ni}(\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/2, \mathbf{C}_{2^4})\}_{k=0}^{\infty}$. We generalize that relation below before applying it to our case. A reader will benefit from seeing that relation in detail on Serre's case in Ch. 6 §3.3.

Assume $\mathbb{H}_{G,\mathbf{C}} \stackrel{\text{def}}{=} \{\mathcal{H}({}^{k}_{\ell}G_{\mathrm{ab}}, \mathbf{C})^{\dagger,\mathrm{rd}}\}_{k=0}^{\infty}$, with, say, $\dagger$ either inner or absolute equivalence, is a tower of Hurwitz spaces defined by the universal abelianized Frattini cover of a group G, with conjugacy classes $\mathbf{C}$ for which $(N_{\mathbf{C}}, \ell) = 1$.

Consider a **MT**: $\mathbb{H}' \stackrel{\text{def}}{=} \{\mathcal{H}'_k\}_{k=0} \subset \mathbb{H}_{G,\mathbf{C}}$. The levels of $\mathbb{H}'$ have definite fields as moduli spaces (as in Def. 4.8). Then, consider the collection of geometric covers $\{\Phi_k : \mathcal{H}'_k \to J_r\}_{k=0}^{\infty}$ and their corresponding geometric (resp. arithmetic) monodromy groups $\{G_{\Phi_k}\}_{k=0}^{\infty}$ (resp. $\{\hat{G}_{\Phi_k}\}_{k=0}^{\infty}$.

Even if, for a given k, it is possible to take a lower definition field of the cover, say, as in Ex. 4.18, that won't be the right definition field for the **RIGP** and **OIT** applications. Denote the projective limit of this sequence by $G_{\mathbb{H}'}$ (resp. $\hat{G}_{\mathbb{H}'}$).

Here is the first property necessary to generalizing the **OIT** to a **MT**,

PROPOSITION 4.3 (Weak **OIT**). *Assume G_{Φ_∞} is eventually ℓ-Frattini. Then, for a general point $j' \in J_r(\bar{\mathbb{Q}})$, the decomposition group of a projective sequence of points $\{\boldsymbol{p}_k^{j'}\}_{k=0}^{\infty}$ lying over j' is $\hat{G}_{\varphi_\infty}$.*

More generally, suppose for $j' \in J_r(\bar{\mathbb{Q}})$, the (arithmetic) decomposition group $D_{j'}$ of a projective sequence of points $\{\boldsymbol{p}_k^{j'}\}_{k=0}^{\infty}$ on $\mathbb{H}'$ lying over j' intersects $G_{\mathbb{H}'}$ in an eventually ℓ-Frattini subgroup $D_{j'}^{\geq}$. Then, $D_{j'}$ is RETURNM

PROOF. RETURNM

□

DEFINITION 4.4. If If each **MT** on $\mathbb{H}_{G,\mathbf{C}}$ satisfies the hypothesis of Prop. 4.3, we say $\mathbb{H}_{G,\mathbf{C}}$ has the Weak **OIT** property.

CONJECTURE 4.5 (**OIT**-Conj$_1$). Each **MT** has the weak **OIT** property.

CONJECTURE 4.6 (**OIT**-Conj$_2$). Each **MT** has the strong **OIT** property.

REMARK 4.7. Any open subgroup of $\tilde{H}$ will also be eventually Frattini (resp. ℓ-Frattini). Further, if $G^* \to G$ is a Frattini cover of finite groups, then the pullback sequence consisting of $H_{k_0} \times_G G^*, k \geq 0$ will be eventually Frattini over G^*. RETURNM

4.2. Monodromy of $X_0(\ell^{k+1}) \to \mathbb{P}^1_j$. Here is a reminder of the eventually ℓ-Frattini properties and their application to Hilbert's Irreducibility Theorem from Serre's **OIT**.

(4.9a) For $\ell > 3$, $k_0 = 0$ (resp. $\ell = 3$, $k_0 = 1$; $\ell = 2$, $k_0 = 2$) and $k \geq k_0$:

$$\mathrm{SL}_2(\mathbb{Z}/\ell^{k+l+1})/\langle \pm I_2\rangle \to \mathrm{SL}_2(\mathbb{Z}/\ell^{k_0+1})/\langle \pm I_2\rangle \text{ is } \ell\text{-Frattini, } l \geq 0.$$

(4.9b) (a) says for this case (${}^0_\ell G = D_\ell$, $\mathbf{C} = \mathbf{C}_{2^4}$): $M({}^0_\ell G, \ell, \mathbf{C}_{3^4})$ is *eventually* ℓ-Frattini; ℓ-Frattini for almost all ℓ.

(4.9c) Take $x^\bullet_\ell \stackrel{\text{def}}{=} \{\boldsymbol{x}_{\ell,k+1} \in X_0(\ell^{k+1})\}_{k\geq k_0}^{\infty}$, a projective sequence over $j' \in U_j(K)$; and $H(x^\bullet_\ell)_K$ its arithmetic monodromy.

(4.9d) If $H(x_{\ell,k_0+1}) = \mathrm{GL}_2(\mathbb{Z}/\ell^{k_0+1})/\langle \pm I_2\rangle$, then

$$H(x^\bullet_\ell) = \mathrm{GL}_2(\mathbb{Z}_\ell)/\langle \pm I_2\rangle.$$

[Se68, IV-23, Lem. 3 and IV-28, exer. 3] [FrH14, Lem. 3.4]

4.3. Jacobian Nielsen class. Consider an inner Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ with $G < G^*$ for which the natural extension of $\mathbf{C}$ to G^* gives nonempty Nielsen classes, $\mathrm{Ni}(G^*, \mathbf{C})$. An example we have been using is $G = A_4$, $G^* = A_5$, and $\mathbf{C} = \mathbf{C}_{\pm 3^2}$ extended to A_5 where the proper notation – in the latter where there is only one class of 3-cycles – is $\mathbf{C}_{3^4}$. This example alone shows that the results can be quite different, as there are two braid orbits on $\mathrm{Ni}(A_4, \mathbf{C}_{\pm 3^2})^{\mathrm{in,rd}}$, but just one on $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{in,rd}}$, though for both their compactified components give genus 0 covers of $\mathbb{P}^1_j$ (Prop. 3.16). Here we consider the process of going from $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ to RETURNM

4.4. Computing Schur multipliers and lift Invariants.

REMARK 4.8. Note the difference with the lift invariant if you include a conjugacy class of order divisible by ℓ.

Denote the conjugacy class of $g \in G$ by $\mathrm{C}_g = \mathrm{C}_{G,g}$.

(4.10a) *Frattini cover* $G^* \to G$: Group cover with restriction to any proper subgroup of G^* not a cover.

(4.10b) *Schur-Zassenhaus*: If $g \in G$ and $(|g|, |\ker(G^*/G)|) = 1$, then C_g lifts uniquely to $\mathrm{C}_{\hat g}$, $\hat g \in G^* \mapsto g \in G$ with $|g| = |\hat g|$.

(4.10c) *Central Frattini extension*: $\psi : R \to G$: $\ker(R \to G)$ is a quotient of the Schur multiplier, SM_G, of G.

(4.10d) *Lift invariant* if $\mathbf{C}$ is (p' for p dividing) $\ker(\psi)$: *10

$$\text{For } \boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C}), s_{R/G}(\boldsymbol{g}) = \prod_{i=1}^{r} \hat g_i \in \ker(R/G).$$

4.5. $M(G, p, \mathbf{C})$ **monodromy statement.**

- *Rank 0 Conj.*: Any Modular Tower has geometric monodromy (over J_r; over $\mathbb{P}^1_j$ when $r = 4$) eventually p-Frattini.
- $r = 4 \Rightarrow$ **MT** levels are upper half-plane quotients.
- *Rank* $t \geq 0$ *Conj.*: Start with $(\mathbb{Z})^t \times^s H$. Take $G_p = (\mathbb{Z}/p)^t \times^s H$ and $\mathbf{C}$ appropriate.

  Then, for a. a. p the Modular Tower is p-Frattini:

  the p-Frattini conclusion for modular curves holds here, too.[*12]

CHAPTER 5

Comparing general MTs with Serre's case

G_K orbits on generators of ℓ-adic lines (with a $\mathbb{Z}/2$-action) on elliptic curve ℓ-adic 1st cohomology.

1. The Comparison Framework

1.1. Analog to $X_0(\ell^{k+1})$ and $X_1(\ell^{k+1})$ Modular Curves.

(5.1a) All *modular curves* came from a rank 1 ($D = \mathbb{Z} \times^s \mathbb{Z}/2, \mathbf{C}_{2^4}$), or a rank 2 ($2D = (\mathbb{Z})^2 \times^s \mathbb{Z}/2, \mathbf{C}_{2^4}$) **MT**.

(5.1b) To illustrate general ideas:

$$D, 2D \Rightarrow G = (\mathbb{Z})^2 \times^s \mathbb{Z}/3, 2G = (\mathbb{Z})^4 \times^s \mathbb{Z}/3.$$

(5.1c) $\mathbb{Z}/3 = H = \langle \alpha \rangle$ action on $(\mathbb{Z})^2$: Through $\alpha = \left(\begin{smallmatrix} 0 & 1 \\ -1 & -1 \end{smallmatrix} \right)$, induced on $V_{p^{k+1}} = (\mathbb{Z}/p^{k+1})^2$, and on $2V_{p^{k+1}} = (\mathbb{Z}/p^{k+1})^4$.
$\mathbf{C} = \mathbf{C}_{\pm 3^2}$ – two copies each of α and α^{-1}.

1.1.1. *Reduced spaces for $\ell = 2$.* Return to Comment on (2.35d).

(5.2a) Our case: ℓ-adic H^1 of genus 2 curves with $\mathbb{Z}/3$ (faithful) action. Compare G_K orbits of 2-dimensional p-adic subspaces preserved by $\mathbb{Z}/3$ with **MT** arithmetic monodromy.

(5.2b) Last slides: Defy mysterious correspondences –Grothendieck (late '60s): Detect $G_{\mathbb{Q}}$ non-conjugate **MT** s. Cusp geometry $\Rightarrow$ definition fields of level k **MT** components.

- *Branch-Cycle Lemma*;
- *Fried-Serre Lift invariant* on a small *Heisenberg group*; and
- *Weil pairing* from a large Heisenberg group.

2. Computation of the Lift Invariant

Michael Fried ¡michaeldavidfried@gmail.com¿ Subject: I thought to add something that I could not include in my one page on what was accomplished on the Open Image Theorem case at Chern Institute Date: January 27, 2017 at 8:44:22 PM MST To: Pierre Dbes ¡Pierre.Debes@univ-lille1.fr¿, Benjamin Collas ¡benjamin.collas@gmail.com¿

Why my first attempt to write the one page failed is explained by my trying to include something of what is below. It just wasn't possible.

In my writeup I used the term K-bound, meaning a Modular Tower had all levels defined over a specific field K (number field usually). The basic result for an **OIT** is a comparison of what happens in the Decomposition group of a Modular Tower to the Arithmetic monodromy group of the tower. There is a hard, NECESSARY initial step: You must show that the geometric tower monodromy is almost ℓ-Frattini (ℓ-Frattini from some point on) and ℓ-Frattini for almost all ℓ.

Part of the structure that works with Modular Towers is that the monodromy action of the base on the fibers of the tower is through (a subgroup of) the braid group. The family of Hurwitz spaces I took at Chern had a full set of primes, and four repetitions of a particular conjugacy class, so I could fully compare with modular curve towers. (As always, when there are four conjugacy classes, the reduced Hurwitz space levels are upper-half plane quotients ramified at the expected three points. Of course, these aren't modular curves, and they aren't defined by congruence subgroups, or I wouldn't have taken them.

Unlike modular curves there are several types of Modular Towers. Recall, a(n abelian) Modular Tower is a projective sequence of irreducible components on a sequence of Hurwitz spaces defined by the ℓ-Frattini (abelianized) characteristic quotients given by a finite group.

These distinct Modular Towers for a given prime ℓ are separated by their lift invariants for the appropriate group. Here that comes, for each ℓ, from the small Heisenberg group for the prime ℓ. (Recall: For alternating groups it was their spin cover.)

1. Type 1 have Fried-Serre lift invariant that is ℓ', falling in $(\mathbb{Z}_\ell)^*$ (it makes sense to take a projective limit of the lift invariants of the levels). At each level the components are all conjugate over $\mathbb{Q}$. There is formula for the lift invariant, different (of course) than the formula for the Alternating groups as given by Fried-Serre. Finding that formula is the hardest result in the paper. The definition field result is a special case of a general theorem never in print previously.

2. Type 2 modular towers have lift invariant in $\ker(\mathbb{Z}_\ell \to \mathbb{Z}/\ell)$. Mod ℓ these are Harbater-Mumford components. There are several of them – a precise number dependent on ℓ – for each $\ell > 6$. I describe these Modular Towers explicitly.

For Type #2, I still have unanswered questions about component definition fields. For example, for the pure Harbater-Mumford types, I don't know if they are $\mathbb{Q}$-bound, since their lift invariants are 0. This is the best test case I have found for guessing precisely between Towers that have or do not have a $\mathbb{Q}$-bound. I have decided to publish the paper leaving this a puzzle.

3. Our main example, and the Small Heisenberg group

In our examples, we will be illustrating Propositions 3.1, 3.2 and 3.5 of Ch. 1. Denote $(\mathbb{Z}/\ell^{k+1})^2$ by ${}^{k+1}_{\ell}V$ and ${}^{k+1}_{\ell}V\times^s\mathbb{Z}/3$ by ${}^{k}_{\ell}G$. In §3.1 we start with the analog of $X_1(\mathbb{Z}/\ell^{k+1})$ (for which there is a natural analog also of $X_0(\mathbb{Z}/\ell^{k+1})$).

Then, as in the modular curve case Ch. 6 §3.3.1, we go to a Jacobian version in §4. Here the group will change from ${}^{k}_{\ell}G$ to

$$ {}^{k+1}_{\ell}G_{jac} \stackrel{\text{def}}{=} ({}^{k+1}_{\ell}V)^2\times^s\mathbb{Z}/3 \ (\mathbf{C}=\mathbf{C}_{\pm 3^2} \text{ remains the same}). \tag{5.3}$$

Analogous to the dihedral case with $\ell=2$, until §3.3.1, we avoid $\ell=3$. Then:

$$\begin{array}{c} {}^{k+1}_{\ell}V \mod \ell \text{ has a 1-dimensional } \alpha\text{-eigenspace} \\ \text{if and only if } \alpha^2+\alpha+1\equiv 0 \mod \ell \text{ has a solution} \Leftrightarrow \ell\equiv 2 \mod 3. \end{array} \tag{5.4}$$

Definition 3.1 (α-span). For ${}^{k+1}_{\ell}G$ (resp. ${}^{k+1}_{\ell}G_{jac}$ in (5.3)) a subset U of ${}^{k+1}_{\ell}V$ (resp. $({}^{k+1}_{\ell}V)^2$) is said to α-span if $\langle U, {}^{\alpha}U\rangle = {}^{k+1}_{\ell}V$ (resp. $({}^{k+1}_{\ell}V)^2$).

3.1. The Small Heisenberg group. The key group in this section is the *Small Heisenberg group* for $\ell>3$:

$$\mathbb{H}(\mathbb{Z}/\ell^{k+1}) = \left\{ M(x,y,z) \stackrel{\text{def}}{=} \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix}, x,y,z\in\mathbb{Z}/\ell^{k+1} \right\}. \tag{5.5}$$

So, there is a natural map

$$\psi_{\mathbb{H}} : \mathbb{H}(\mathbb{Z}/\ell^{k+1}) \to {}^{k+1}_{\ell}V : M(x,y,z)\mapsto (x,y)=\boldsymbol{v}\in {}^{k+1}_{\ell}V,$$

for which $\ker(\psi_{\mathbb{H}})=\mathbb{Z}/\ell^{k+1}$. As in Ex. 2.7 we use the left action (here of $\mathbb{Z}/3$) to describe the extension of $\mathbb{Z}/3=\langle\alpha\rangle$ to the group of (5.5).

Lemma 3.2. *For $\ell>2$ each element in $\mathbb{H}(\mathbb{Z}/\ell^{k+1})$ has order ℓ^{k+1}. By contrast, $\mathbb{H}(\mathbb{Z}/2^{k+1})$ has elements of order 2^{k+2}, and for $k=0$ it is D_4, dihedral of order 8.*

Proof. Write $M(x,y,z)$ as I_3+A and put it to the ℓ^{k+1} power. Since A^u is the 0 matrix for $u>2$, the expansion gives

$$\mathrm{I}_3+\ell^{k+1}A+\frac{\ell^{k+1}(\ell^{k+1}-1)}{2}A^2$$

which is I_3 unless, $\ell=2$ and $\frac{\ell^{k+1}(\ell^{k+1}-1)}{2}\cdot(xy)$ is nonzero $\mod \ell^{k+1}$, or $xy \mod 2$ is nonzero. Therefore, for $k=0$, the group is nonabelian and has two classes of elements of order 2. So is dihedral. □

3.1.1. *Conjugacy classes.* Use $\psi_{\mathbb{H}}$ (with ℓ and its power understood) even with the $\mathbb{Z}/3$ action. The conjugacy class lift of $\alpha_0=\left(\begin{smallmatrix}\alpha & \mathbf{0}\\ 0 & 1\end{smallmatrix}\right)$ to ${}^{k+1}_{\ell}G$ is

$$\left\{ \left(\begin{smallmatrix}1 & \boldsymbol{v}\\ 0 & 1\end{smallmatrix}\right)\alpha_0\left(\begin{smallmatrix}1 & -\boldsymbol{v}\\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix}\alpha & \boldsymbol{v}-{}^{\alpha}\boldsymbol{v}\\ 0 & 1\end{smallmatrix}\right) \stackrel{\text{def}}{=} \alpha_{\boldsymbol{v}} \mid \boldsymbol{v}\in {}^{k+1}_{\ell}V \right\}. \tag{5.6}$$

We often use ${}^{1-\alpha}\boldsymbol{v}$ for $\boldsymbol{v}-{}^{\alpha}\boldsymbol{v}$. Similarly, $\alpha_{\boldsymbol{v}}^{-1}=\left(\begin{smallmatrix}\alpha^{-1} & {}^{1-\alpha^{-1}}\boldsymbol{v}\\ 0 & 1\end{smallmatrix}\right)$.

Denote the $n \times n$ identity matrix by I_n. For example, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{I}_2$.

The action of α comes is from the permutation action of S_n on $(\mathbb{Z})^n$ (here $n = 3$). Then, mod out by the S_n stable module $\langle (1, \dots, 1) \rangle$, to get $\mathbb{Z}^{n-1}$.

Elements in $\mathrm{Ni}({}^{k+1}_{\ell}G, \mathbf{C}_{\pm 3^2})^{\mathrm{in}}$ will be 4-tuples with entries denoted either $\alpha_{\boldsymbol{v}}$ or $\alpha_{\boldsymbol{v}}^{-1}$. Each element in the Nielsen class is inner equivalent to an element in

$$T_{\pm\pm} \stackrel{\mathrm{def}}{=} \{\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} = (\alpha_0, \alpha_{\boldsymbol{v}_2}^{-1}, \alpha_{\boldsymbol{v}_3}, \alpha_{\boldsymbol{v}_4}^{-1})\}. \tag{5.7}$$

with the correct extra notation, say ℓ^{k+1}, understood.

LEMMA 3.3. *Since ${}^{k+1}_{\ell}V \to {}^{1}_{\ell}V$ is a Frattini cover, $\boldsymbol{v} \in {}^{k+1}_{\ell}V$ α-spans if and only if $\boldsymbol{v} \mod \ell$ is in no α eigenspace. By Def. 3.2, an* **HM** *rep. in $T_{\pm\pm}$ has $\boldsymbol{v}_2 = \mathbf{0}$, with $\boldsymbol{v}_3 \mod \ell$ in no α eigenspace. From product-one,*

$$\alpha_{\boldsymbol{v}_3}\alpha_{\boldsymbol{v}_4}^{-1} = \left(\begin{smallmatrix} \alpha & {}^{1-\alpha}\boldsymbol{v}_3 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \alpha^{-1} & {}^{1-\alpha^{-1}}\boldsymbol{v}_4 \\ 0 & 1 \end{smallmatrix}\right) = \mathrm{I}_2; \text{ or } {}^{1-\alpha}(\boldsymbol{v}_3 - \boldsymbol{v}_4) = \mathbf{0}. \tag{5.8}$$

That is, $\boldsymbol{v}_3 = \boldsymbol{v}_4$ since $\ker(1-\alpha) = 0$.

PROOF. For generation to apply, $\langle \alpha_0, \alpha_{\boldsymbol{v}_3} \rangle = {}^{k}_{\ell}G$. Since ${}^{k+1}_{\ell}G \to {}^{0}_{\ell}G$ is a Frattini cover, we need only consider when

$$\langle \alpha_0, \alpha_{\boldsymbol{v}_3} \mod \ell \rangle = \langle \alpha_0, \alpha_0^{-1}\alpha_{\boldsymbol{v}_3} \mod \ell \rangle = {}^{0}_{\ell}G.$$

That happens if and only if ${}^{1-\alpha}\boldsymbol{v}_3$ α-spans. If ${}^{\alpha}\boldsymbol{v}_3 = \mu\boldsymbol{v}_3$, $\mu \in \mathbb{Z}/\ell^{k+1}$, then ${}^{1-\alpha}\boldsymbol{v}_3 = (1-\mu)\boldsymbol{v}_3$, an invertible relation. This shows $\boldsymbol{v}_3$ α-spans, and it does α-span if and only if it defines an **HM** rep. by the formula above. □

3.1.2. *The lift invariant and* **DI** *elements.* We already saw the definition of **DI** elements in the case of $G = A_4$ for the conjugacy classes $\mathbf{C} = \mathbf{C}_{\pm 3^2}$.

DEFINITION 3.4 (**D**(ouble)**I**(dentity)). **DI** elements in $T_{\pm\pm}$ are those for which either $\boldsymbol{v}_3 = \mathbf{0}$, or $\boldsymbol{v}_2 = \boldsymbol{v}_4$.

Prop. 3.5 expands on the exercises [**Br82**, p. 97, Ex. 8 and p. 127, Exs. 4-5] to describe the **Comm** part of the universal coefficient theorem for $q = 2$ when G is abelian. Cor. 3.6 concludes that the small Heisenberg group is the universal central extension of ${}^{k}_{\ell}G$.

PROPOSITION 3.5. *Given a central extension $A \to E \to B$ with B abelian, denote the factor set associated to it in* Ch. 1 §1.2.2 by c_e. Define $\tilde{c}_e : B \times B \to A$ by $(b_1, b_2) \mapsto c_e(b_1, b_2) - c_e(b_2, b_1)$. With $\Lambda^2(B)$ the second exterior product of B,[1] this gives a map of $H^2(B, A)$ to $\mathrm{Hom}(\Lambda^2(B), A)$, with the Ext extensions in the kernel. This produces an exact sequence:

$$0 \to \mathrm{Ext}(B, A) \to H^2(B, A) \xrightarrow{\tilde{c}_e} \mathrm{Hom}(\Lambda^2(B), A) \to 0 \tag{5.9}$$

[1] $\Lambda^2(B) = B \otimes B / \langle b_1 \otimes b_2 - b_2 \otimes b_1 \mid b_1, b_2 \in B \rangle$

that is (3.17) in disguise with $\Lambda^2(B)$ identifying with the Schur module $H_2(B,\mathbb{Z})$, for B.

PROOF. Consider a central ℓ-Frattini extension $\psi : H \to B$ defined by a factor set $c_e : B \times B \to A$ as in Ch. 1 §1.2.2. With $A = \ker(\psi)$, that gives an element of $H^2(B,A)$. From Cor. 2.6, commutators of H that lie in $\ker(\psi)$ determine the lift invariant to ψ. With, however, B abelian, any commutator $h_1h_2h_1^{-1}h_2^{-1}$ is in $\ker(\psi)$. Further, using the factor set, in the description of this extension, we may write this commutator as

$$\begin{aligned}&\left(\left(\begin{smallmatrix} b_1 & a_1 \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} b_2 & a_2 \\ 0 & 1\end{smallmatrix}\right)\right)\left(\left(\begin{smallmatrix} b_2 & a_2 \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} b_1 & a_1 \\ 0 & 1\end{smallmatrix}\right)\right)^{-1} = \\ &\left(\begin{smallmatrix} b_1b_2 & b_1*a_2+a_1+c_e(b_1,b_2) \\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix} b_2b_1 & b_2*a_1+a_2+c_e(b_2,b_1) \\ 0 & 1\end{smallmatrix}\right)^{-1}.\end{aligned} \tag{5.10}$$

Now apply that $b_1b_2 = b_2b_1$ (B abelian) and $b_2 * a_1 = a_1$ (central extension) etc. to conclude the result is $\tilde{c}_e(b_1,b_2)$ as given in the statement of the lemma.

This shows that the **Comm** part of $H^2(B,A)$ maps through $\mathrm{Hom}(\Lambda^2(B),A)$, as in Def. 2.2 or Def. 2.5 and Rem. 2.7, with kernel the Ext part. The resemblance of this sequence to the universal coefficient theorem (3.17) suggests that $\Lambda^2(B)$ identifies with the Schur module $H_2(B,\mathbb{Z})$, for B.

Indeed, [**Br82**, V. Thm. (6.4) (iii)] (with $k = \mathbb{Z}$) says exactly that. Then, with the substitution of $\Lambda^2(B)$ for $H_2(G,\mathbb{Z})$ in (3.17) for $q = 2$, [**Br82**, Exs. 4. (a) and 5] says the sequences may be identified through the map $\tilde{c}_e$ above. Ch. 6 §**??**

□

COROLLARY 3.6. *Extend $\mathbb{Z}/3$ on $B = {}^{k+1}_{\ell}V$ to $\mathbb{H}(\mathbb{Z}/\ell^{k+1})$ by acting trivially on $\ker(\psi_{\mathbb{H}(\mathbb{Z}/\ell^{k+1})})$. Thus, $\mathbb{H}(\mathbb{Z}/\ell^{k+1}) \times^s \mathbb{Z}/3$ is the universal central extension of ${}^{k+1}_{\ell}G$ for $\ell > 3$. For $\ell = 2$, it is*

PROOF. In the case at hand, $B = {}^{k+1}_{\ell}V$. Then, $\Lambda^2(B)$ is a 1-dimensional $\mathbb{Z}/\ell^{k+1}[B]$ module. We show $\mathbb{Z}/3$ acts trivially on it. The action of α is through $(\mathbb{Z}/\ell^{k+1})^*$, of order $(\ell-1)\ell^k$, if the action for $k = 0$ is trivial then, on the kernel the action is an element of order ℓ contrary to the order of α. So, it suffices to see the action is trivial for $k = 0$.

If $\ell \equiv 2 \mod 3$ then α acts irreducibly on B. So, it has no eigenvectors in $\mathbb{Z}/\ell$, and it must act trivially. if, however, $\ell \equiv 1 \mod 3$, then α has two distinct eigenvalues a_1, a_2, for vectors $\boldsymbol{v}_1, \boldsymbol{v}_2 \in B$ with product 1 (the constant coefficient of $\frac{x^3-1}{x-1}$). Then, $\Lambda^2(B)$ is generated by $\boldsymbol{v}_1 \wedge \boldsymbol{v}_2$ on which α acts as

$$\boldsymbol{v}_1 \wedge \boldsymbol{v}_2 \mapsto \alpha(\boldsymbol{v}_1) \wedge \alpha(\boldsymbol{v}_2) = a_1a_2\boldsymbol{v}_1 \wedge \boldsymbol{v}_2 = \boldsymbol{v}_1 \wedge \boldsymbol{v}_2.$$

This proves the claim. □

In the next proposition denote $\mathrm{Ni}({}^{k+1}_{\ell}G, \mathbf{C}_{+3^3})^{\mathrm{in}}$ (resp. $\mathrm{Ni}({}^{k+1}_{\ell}G, \mathbf{C}_{\pm 3^2})^{\mathrm{in}}$) by $\mathrm{Ni}_{\ell^{k+1},3^3}$ (resp. $\mathrm{Ni}_{\ell^{k+1},\pm 3^2}$).

PROPOSITION 3.7. *Elements of* $\mathrm{Ni}_{\ell^{k+1},3^3}$ *have representatives of form*

$$\boldsymbol{g}_{\boldsymbol{w}} = (\alpha_0, \alpha_{\boldsymbol{w}_2}, \alpha_{\boldsymbol{w}_3}) \text{ with } \boldsymbol{w}_3 = -\boldsymbol{w}_2^{\alpha}.$$

All $\boldsymbol{g}^* \in \mathrm{Ni}_{\ell^{k+1},3^3}$ *have lift invariant* $s_{3^3}(\boldsymbol{g}^*) \in (\mathbb{Z}/\ell^{k+1})^* \subset \ker(\psi_{\mathbb{H}})$.

If for some some $\boldsymbol{g}^* \in \mathrm{Ni}_{\ell^{k+1},3^3}$ $s_{3^3}(\boldsymbol{g}^*) = \mu$, *then* $\mu = s_{\pm 3^2}(\boldsymbol{g})$ *for* $\boldsymbol{g} \in \mathrm{Ni}_{\ell^{k+1},\pm 3^2}$ *a* **DI** *element* [**FrH15**, Prop. 4.18].

Elements with ℓ*-divisible lift invariant and* **DI** *reps. have distinct braid orbits.*

Main orbit result on $\mathrm{Ni}({}^0_{\ell}G, \mathbf{C}_{+3^2-3^2})^{\mathrm{in,rd}}$ uses this quantity for $\ell > 3$:

$$K_\ell = \frac{\ell \pm 1}{6}, \ell \equiv \mp 1 \mod 3.$$

We have already done the result for $\ell = 2$ (and $k = 0$) in Ch. 2 §3.16, where there is one **HM** and one **DI** orbit. That case is different in ways from the case of general ℓ, but mostly because the maximal ℓ-central Frattini cover is of a different nature for $\ell = 2$, than for $\ell > 3$.

COROLLARY 3.8 (Level 0 Main Result). *For* $\ell > 3$ *prime and* $k = 0$*:*

(5.11a) *Classes with trivial lift invariant fall in* K_p **HM** *braid orbits. Each intersects* $T_{\ell,\pm\pm,1-\deg}$ *in* $\ell(\ell-1)$ *elements.*

(5.11b) *Orbits have nontrivial lift invariant if and only if they are double identity, and that distinguishes the orbits.*

(5.11c) *Each* **DI** *orbit intersects* $T_{\ell,\pm\pm,1-\deg}$ *in* $K_\ell(\ell-1)$ *elements.*

§3.1.3 gives the proof of Prop. 3.7 and its corollary, starting from a general idea of computing the universal ℓ-Frattini extension. §3.1.4 gives a complete description of the braid orbits on these Nielsen classes at all levels. This is an example of where we are able to gives succinct labels to braid orbits based on the types of cusps they contain. That is, at the end of this subsection we precisely know all the braid orbits. on $\mathrm{Ni}_{\ell^{k+1},\pm 3^2}$ for all ℓ, $(\ell, 3) = 1$, and all k.

REMARK 3.9. Notation of (5.6) is compatible with Ch. 6 §3.3 for an entry in $\boldsymbol{g} \in \mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})$ is $\left(\begin{smallmatrix} -1 & a \\ 0 & 1 \end{smallmatrix}\right)$. A more precise analog would be the conjugate

$$\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 2a \\ 0 & 1 \end{smallmatrix}\right).$$

Still, with $(\ell, 2) = 1$, there was no loss – and improved notation – in replacing $2a$ by a, and regarding $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as the analog of α_0.[2]

3.1.3. *Proof of Prop. 3.7.*

3.1.4. *Proof of Cor. 3.8.*

[2]Ch. 6 §3.3.3 makes the large adjustments in Serre's case for preserving the rubric even when $\ell = 2$, as we will do for this case with $\ell = 3$.

3.2. 1-degenerates in $\mathrm{Ni}(G_{p^{k+1}}, \mathbf{C}_{+3^2-3^2})^{\mathrm{in}}$**.**

- $\boldsymbol{g}_{\boldsymbol{v}_2,\boldsymbol{v}_3} \in T_{\pm\pm}$: *product-one* $\leftrightarrow \boldsymbol{v}_2 - \boldsymbol{v}_3 + \boldsymbol{v}_4 = \mathbf{0}$.
- *Generation* $\leftrightarrow \langle \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\rangle$ contains an α-gen. of $V_{p^{k+1}}$.
- 1-*degeneracy*: $\langle \boldsymbol{v}_2, \boldsymbol{v}_3, \boldsymbol{v}_4\rangle \simeq \mathbb{Z}/p^{k+1}$. Since $p \neq 2$ this is equivalent $\boldsymbol{v}_j = m_j\boldsymbol{v}$ with $\boldsymbol{v} = \boldsymbol{v}_i$ for some i, $j = 1, 2, 3$.
- $K^* = \langle q_2^2, q_3^2, \mathbf{sh}\rangle$ is the stabilizer of the collection $T_{\pm\pm} \mod \mathcal{Q}''$ with $[K^* : \langle q_2^2, q_3^2\rangle] = 2$.

3.3. Braid orbits $\leftrightarrow$ 1-degenerates, $T_{\pm\pm,1-\mathrm{deg}}$**, in** $T_{\pm\pm}$**.**

3.3.1. *The case* $\ell = 3$.

4. The Jacobian case, (5.1b)

As above, denote $(\mathbb{Z}/\ell^{k+1})^2$ by ${}^{k+1}_{\ell}V$ and $({}^{k+1}_{\ell}V)^2 \times^s \mathbb{Z}/3$ by ${}^{k}_{\ell}G_{jac}$. Then, the Hurwitz spaces on which we form our **MT**s is given by the Nielsen class $\mathrm{Ni}({}^{k}_{\ell}G_{jac}, \mathbf{C}_{\pm 3^2}) \stackrel{\mathrm{def}}{=} \mathrm{Ni}_{\ell^{k+1},\pm 3^2\, jac}$. This is an analog of the modular curve (Jacobian) case given by the notation of Ch. 6§3.3.1.

Below we refer to the 1st (resp. 2nd) copy of ${}^{k+1}_{\ell}V$ in $({}^{k+1}_{\ell}V)^2$ as the 1st (resp. 2nd) $\frac{1}{2}$-space. As in Rem. 2.17, there are good reasons for dealing with decomposable ℓ-Frattini kernels for all ℓ in the Jacobian cases.

4.1. Jacobian Nielsen classes. An analog of $T_{\pm\pm}$ represents braid orbits of $\mathrm{Ni}({}^{k+1}_{\ell}G_{jac}, \mathbf{C}_{\pm 3^2}) \stackrel{\mathrm{def}}{=} \mathrm{Ni}_{\ell^{k+1},\pm 3^2\, jac}$ as in Prop. 3.7:

$$T_{\pm\pm\, jac} \stackrel{\mathrm{def}}{=} \{(\alpha_0, \alpha^{-1}_{(\boldsymbol{v}_2,\boldsymbol{v}_2')}, \alpha_{(\boldsymbol{v}_3,\boldsymbol{v}_3')}, \alpha^{-1}_{(\boldsymbol{v}_4,\boldsymbol{v}_4')}) \stackrel{\mathrm{def}}{=} \boldsymbol{g}_{\boldsymbol{v},\boldsymbol{v}'}\}_{(\boldsymbol{v}_2,\boldsymbol{v}_2'),(\boldsymbol{v}_3,\boldsymbol{v}_3')\in({}^{k+1}_{\ell}V)^2} \tag{5.12}$$

where we understand that $(\boldsymbol{v}_2, \boldsymbol{v}_2'), (\boldsymbol{v}_3, \boldsymbol{v}_3')$ determine $(\boldsymbol{v}_4, \boldsymbol{v}_4')$ (from product-one) and they α-span $({}^{k+1}_{\ell}V)^2$. Lem. 4.1 says we may take an element $\boldsymbol{g}_{\boldsymbol{v},\boldsymbol{v}'} \in T_{\pm\pm\, jac}$ so that $\boldsymbol{v}$ is in one of the normal forms – **HM** or **DI** – given by Cor. 3.8.

From product-one,

$$\begin{aligned} {}^{k+1}_{\ell}G &= \langle \alpha_0, \alpha_0\alpha^{-1}_{(\boldsymbol{v}_2,\boldsymbol{v}_2')}, \alpha_{(\boldsymbol{v}_3,\boldsymbol{v}_3')}\alpha_0^{-1}\rangle \\ &= \langle \alpha_0, \left(\begin{smallmatrix} 1 & 1-\alpha(\boldsymbol{v}_2,\boldsymbol{v}_2') \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 1-\alpha(\boldsymbol{v}_3,\boldsymbol{v}_3') \\ 0 & 1 \end{smallmatrix}\right)\rangle. \end{aligned} \tag{5.13}$$

LEMMA 4.1. *Take* $k = 0$. *With no loss for braid orbit lists assume of* $\boldsymbol{g}_{\boldsymbol{v},\boldsymbol{v}'}$*:*

(5.14a) $\boldsymbol{g}_{\boldsymbol{v}}$ *and* $\boldsymbol{g}_{\boldsymbol{v}'}$ *are in* $\mathrm{Ni}_{\ell,\pm 3^2}$*; and either*

(5.14b) $\boldsymbol{v} = (\mathbf{0}, \mathbf{0}, \boldsymbol{v}_3, \boldsymbol{v}_3)$, (5.8), *an* **HM** *orbit case; or*

(5.14c) $\boldsymbol{v} = (\mathbf{0}, \boldsymbol{v}_2, \mathbf{0}, -\boldsymbol{v}_2)$, *a* **DI** *orbit case.*

Then, $\boldsymbol{g}_{\boldsymbol{v},\boldsymbol{v}'}$ *satisfying* (5.12) *is equivalent, in case* (5.14b) *(resp.* (5.14c)*) to* $\boldsymbol{v}_3$ *(resp.* $\boldsymbol{v}_2$*)* α*-spans and then that* $\langle \boldsymbol{v}_2', \boldsymbol{v}_3'\rangle = {}^{k+1}_{\ell}V$.

PROOF. The natural map ${}^{k+1}_{\ell}G_{jac} \to {}^{k+1}_{\ell}G$ extends to the Nielsen classes and is compatible with the braid action. Therefore, with no loss for representatives of

braid orbits, assume for $\boldsymbol{g}_{\boldsymbol{v},\boldsymbol{v}'}$ that $\boldsymbol{g}_{\boldsymbol{v}}$ is one of the normal forms for the orbits. To see that the 4th entry gives product-one in (5.14c), check:

$$\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha^{-1} & {}^{1-\alpha^{-1}}\boldsymbol{v}_2\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}\alpha^{-1} & -^{1-\alpha^{-1}}\boldsymbol{v}_2\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1 & {}^{\alpha-1}\boldsymbol{v}_2\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & -^{\alpha-1}\boldsymbol{v}_2\\ 0 & 1\end{smallmatrix}\right).$$

For (5.12) to hold requires in case (5.14b) (resp. (5.14c)) that $\boldsymbol{v}_3$ (resp. $\boldsymbol{v}_2$) α-spans ${}^{k+1}_{\ell}V$. For (5.14b), apply (5.13). Then,

$$^{1-\alpha}(\boldsymbol{0},\boldsymbol{v}_2') \text{ and } {}^{1-\alpha}(\boldsymbol{v}_3,\boldsymbol{v}_3') \ \alpha\text{-span } ({}^{1}_{\ell}V)^2. \tag{5.15}$$

We know that $\boldsymbol{v}_3$ α-spans ${}^{1}_{\ell}V$, but assume $\boldsymbol{v}_2',\boldsymbol{v}_3'$ do not span ${}^{1}_{\ell}V$, but lie in a 1-dim subspace. Then, RETURNM $\square$

CHAPTER 6

Historical Resources and Perspectives

As usual ℓ refers to a key prime of consideration. We could have regarded this chapter as "Appendices," since the sections are independent, though they are surely more than that. For example, §3 inspects, in revisiting Serre's version of the **OIT** to connect to our main definitions, the following topics:

- *eventually ℓ-Frattini* for the primes 2 and 3;
- visualizing of Weil's pairing on $H^1(X, \mathbb{Z}_\ell)$ as a *lift invariant*, with X an elliptic curve;
- connecting the Jacobian Nielsen class $\mathrm{Ni}((\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/2, \mathbf{C}_{2^4})$ and the Nielsen class $\mathrm{Ni}(\mathbb{Z}/\ell \times^s \mathbb{Z}/2, \mathbf{C}_{2^4})$; and
- passing from specific Nielsen classes to modular curves.

We treated it so as a resource for what we do almost everywhere in the book, enhancing our connection to modular curves, though we have gone into territory controlled by curves that replace elliptic curves as the driver of our problems.

We treated it thus, so the reader unacquinted with Serre's **OIT**, or perhaps even having forgotten about it, would not have that dominate the mathematical stories featuring the connection between the **RIGP** and the expanded **OIT**.

Or quite differently, how in §1.4 – to augment the treatment of the cohomology of extensions starting in Ch. 1 §1.2.2 – we make a path through the huge topics of cohomology of groups and modular representations. We base this on what we learned/used partly from [**Nor62**], [**Br82**] and [**Be91**], and the many appearances of "small" cohomology arguments in both of Serre's books [**Se68**] and [**Se92**].

In a paraphrase here, of a paraphrase of a statement of Serre's about the **RIGP** with which I concluded [**Fr94**],

> it is astonishing what one can learn of cohomological topics
> from confronting significant extensions of groups.

1. Group, group covers and homological algebra

For a group the word *rank* usually means the number of elements required to generate the group. If the group is projective, it refers to topological generation, meaning number of elements required to give a subgroup whose closure is the whole

group. In special cases, it can refer to the rank, not of the group, but of a particularly important subgroup. For a group H, we will denote its (topological) rank by $\mathrm{rk}(H)$.

Isomorphism is the criterion for two groups to be alike. Some groups are sufficiently similar that they will likely collect together in descriptions for the rest of time. Like (finite) abelian or nilpotent groups (Ch. 1 §1.3), with their rank and the primes dividing their order, standing out as invariants. §1.3 introduces those groups this book uses to put the Inverse Galois Problem in a context with other classical problems of arithmetic geometry.

Mathematicians now accept the classification of *finite simple groups* as a milestone. We don't expect a reader to know it in any detail; the author is no expert on it, either. Our goals use as a starting point only examples that most readers would have had in a first course in graduate algebra.

1.1. Finite groups and their algebras. §1.1.1 reminds of the topic of pairs (G, T), a group and an attached *faithful* permutation representation. When regarding group elements as functions or operators we apply the elements in the order in which they are written from left to right.

We give a much slower path to group algebras, starting with reminders of *Jordan canonical form*. The easiest way for mathematicians, raised on linear algebra, to see groups is through representations of their elements as matrices acting on the left of elements of a vector space. Therefore, §1.3 uses a left action for the traditional look of Jordan canonical form. Yet, in many chapters of this book most groups will act from the right.

We use this – based on Jordan canonical form – to introduce the simplest algebras with these essential ingredients: *central, orthogonal, idempotents*, aided by the *Jacobson radical*, and a recognizable version of Loewy display for illustrating irreducible constituents of a module this isn't completely reducible.

§1.3.1 then introduces these ingredients in generality sufficient to get to form the cuminating objects of this book. Starting from a group G, and an ℓ-perfect prime of G,[1] our basic group theoretic object is the the universal ℓ-Frattini cover ${}^1_\ell G \to G$ of G, §1.4.1. In many ways, the characteristic ℓ-Frattini module ${}^1_\ell M = {}_\ell M_G$ of (1.10) for the group algebra, $\mathbb{F}_\ell[G]$ is essentially equivalent to it.

Recall the Universal abelianized ℓ-Frattini cover of G (1.11):

$$V_{G,\ell} \stackrel{\mathrm{def}}{=} (\mathbb{Z}_\ell)^{\nu(G,\ell)} \to {}_\ell\tilde{G}_{\mathrm{ab}} \to G, \nu(G,\ell) = \dim_{\mathbb{Z}/\ell}({}_\ell M_G). \tag{6.1}$$

This consists, for the G action of a series of ${}_\ell M_G$ modules for which the kernel of the map is the source of the main ℓ-adic representations in the title of the book. This more tractible object sits perfectly between considerations of the **RIGP** or **OIT** the **MT**s attached to it already have conjectures and results about them.

[1] We will explain how to drop the ℓ-perfect condition for our goals.

There can, however, be other such extensions, in (6.20) and related to (6.1), from which we may form canonical sequences of moduli spaces for which the conjectures and already established results are also expected.

1.1.1. *Notation for group actions.* There is a major difference between them on how they act naturally on elements as functions. Our major computations are with Nielsen classes (§2.2). These are r-tuples of elements from groups, usually often understood to be permutation groups, though they could be elements of some algebraic, even affine, group.

Right vs Left Action: Computations often appear as a series of actions formed from a string of group elements, say, written as $g_1g_2g_3\cdots g_r$, acting. That is the multiplication is read as

$$\text{“}g_1\text{, times } g_2\text{, times } g_3\text{, } \ldots\text{”}.$$

Here we will mean that g_1 acts first, then g_2, etc. Nielsen classes consist of arrays, say, $\boldsymbol{g}$, of such elements on which act elements q_i (called braids) from the Hurwitz monodromy group H_r. Here, two, we sometimes show that action as a series, as in this notation:

$$(\boldsymbol{g}) \mapsto (\boldsymbol{g})q' \mapsto ((\boldsymbol{g})q')q'' \mapsto (((\boldsymbol{g})q')q'')q''$$

read as q' acts, then q'' acts on the result, etc. All of this is compatible with reading multiplication from left to right, and so acting from left to right.

When we must make an exception to regard elements of a group as matrices, acting as functions from linear algebra, we do our best to forwarn the reader; noting how someone could switch to our left-right notation if they wanted. Example: In regarding elements of $\mathrm{PGL}_2(\mathbb{C})$ (linear fractional transformations) as acting from matrices we might have,

$$\text{from the left} \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} z \\ 1 \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} az+b \\ cz+d \end{smallmatrix}\right) \text{ versus}$$

$$\text{from the right} \quad (z\ 1)\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \mapsto (az+b\ cz+d).$$

Permutation representations: We give a permutation representation (of degree n) as a pair (G, T) with $T : G \to S_n$ a homorphism of groups. Usually we assume T is *transitive*: for $i, j \in \{1, \ldots, n\}$ there exists $g \in G$ for which $(i)T(g) = j$. If it is transitive, then giving (G, T) is equivalent to giving (G, H) with H a subgroup of *index* $(G : H) = n$.

A *right* coset of H in G is a subset $Hm = \{hm \mid h \in H\}$. That means, G is a disjoint union of precisely n distinct (we usually take *right*, but if you are consistent, then you can take *left*) cosets $\dot{\cup}_{i=1}^{n} Hm_i = G$.

Then the right action of G on these cosets is well-defined and equivalent to the permutation representation whereby we take

$$H = \{g \in G \mid (1)T(g) = 1\} \stackrel{\text{def}}{=} G(T, 1).$$

Usually, we also assume G is *faithful*, or its kernel $\ker(T)$ is $\{1\}$ (trivial). A permutation representation is primitive if between G and $G(T, 1)$ there are no proper subgroups. In constructing covers in §2, these correspond to covers without *decomposition*: composition as two covers of degree exceeding 1 as in Lem. 2.3.

There is a classification of groups with a primitive permutation representation. Excluding those related to sporadic simple groups, this divides into two types: those based on the series of finite simple groups, and those related to affine groups [**AsS**] with the latter not considered classifiable at this time. This result is called the *Aschbacher–O'nan–Scott Theorem*.

There are well-known problems that reduce to looking at primitive groups, then solved by a combination of arithmetic geometry interpreting a property about ramification groups theoretically (see §1.4.1). Then, group theorists – who knew the classification well – weeded out those primitive groups for which the ramification groups appear appropriately. These problems usually had precise phrasings on the Arithmetic/Geometric monodromy of a (usually sphere) cover. Thus, they were not pure **RIGP** problems. [**FrGS**] may be the first that required having on the team members who know the classification well, to complete an analysis in this style.

I know of no one in print who has undertaken to provide the tools to enhance this classification precisely to general (G, T), because one must be intrepid with these more sophisticated tools to try it. Still, the tools are there, using wreath products and Frattini covers. That suggests that one can treat finite groups that arise from covers in a way that will one day allow names for covers – through the use of their Galois closures (and permutation representations). I think it enhances this book and the idea of a Galois closure to say that.

1.2. Special collections of groups. While our moduli space considerations play so much on Frattini covers, we always have considerations involving semi-direct products. Wreath products §1.2.1 and affine groups §1.2.2 being two such.

1.2.1. *Wreath products.* For any group H and integer n, denote the associated wreath product by $H \wr S_n \stackrel{\text{def}}{=} H^n \times^s S_n$. We give the (right) action of σ on $(h_1, \ldots, h_n)$ by $\sigma : (h_1, \ldots, h_n) \mapsto (h_{(1)\sigma}, \ldots, h_{(n)\sigma}) \stackrel{\text{def}}{=} \boldsymbol{h}^\sigma$. If, in the notation of Ch. 1 §1.2, we write its elements as $\left(\begin{smallmatrix} \sigma & 0 \\ \boldsymbol{h} & 1 \end{smallmatrix}\right)$, then the (symbolic) multiplication gives this:

$$\left(\begin{smallmatrix} \sigma & 0 \\ \boldsymbol{h} & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \sigma' & 0 \\ \boldsymbol{h}' & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} \sigma\sigma' & 0 \\ \boldsymbol{h}^{\sigma'}\cdot\boldsymbol{h}' & 1 \end{smallmatrix}\right).$$

A group $G \geq H$ with $(G : H) = n$: Then, explicate the degree n permutation representation $T_H : G \in S_n$ by choosing (right) coset representatives $g_1^*, \ldots, g_n^*$. This gives, $g_j^* g = h_j g_{(j)\sigma}^*$, $j = 1, \ldots, n$, defining $g \xrightarrow{\psi_{\boldsymbol{g}^*}} \left(\begin{smallmatrix} \sigma & 0 \\ (h_1,\ldots,h_n) & 1 \end{smallmatrix}\right) \in H \wr S_n$.

Now suppose, for k a field, that $k[H]$ acts on a module M, Then, $H \wr S_n$ acts on $\boldsymbol{m} \in M^n$ by the formula used in §1.1.1 (from the right) for linear fractional transformations: $\left(\boldsymbol{m} \quad 1\right)\left(\begin{smallmatrix} \sigma & 0 \\ \boldsymbol{h} & 1 \end{smallmatrix}\right) = \left(\boldsymbol{m}^\sigma \cdot \boldsymbol{h} \quad 1\right)$.

PROBLEM 1.1. Check that $\psi_{\boldsymbol{g}^*}$ is a homomorphism given by the expected multiplication. If you change $\boldsymbol{g}^*$ to $\boldsymbol{g}^{**}$ then $\boldsymbol{g}^{**} = \boldsymbol{h}' \cdot \boldsymbol{g}^*$ for some $\boldsymbol{h}' \in H^n$.

$$\text{Show that } \psi_{\boldsymbol{g}^{**}} = \left(\begin{smallmatrix} 1 & 0 \\ \boldsymbol{h}' & 1 \end{smallmatrix}\right)\psi_{\boldsymbol{g}^*}\left(\begin{smallmatrix} 1 & 0 \\ (\boldsymbol{h}')^{-1} & 1 \end{smallmatrix}\right).$$

Prob. 1.24 uses this to interpret the G module $M^{\uparrow G}$ induced from M.

Monodromy group of a cover composite: Suppose $W \xrightarrow{\psi_X} X \xrightarrow{\psi_Z} Z$ is a sequence of covers of irreducible algebraic varieties, say as in Ch. 1 §2.1. For simplicity, assume they are defined over $\mathbb{C}$.

We wish to compute the Galois closure group, $G_{W/Z}$, of the function field extension, $\mathbb{C}(W)/\mathbb{C}(Z)$, from our knowledge of the Galois closure group, $G_{W/X} \leq S_n$ ($n = \deg(\psi_X)$) and $G_{X/Z} \leq S_m$ ($m = \deg(\psi_Z)$) of resp. ψ_X and ψ_Z.

Use the *primitive element theorem* to write the respective field extensions $\mathbb{C}(W)/\mathbb{C}(Z), \mathbb{C}(X)/\mathbb{C}(Z), \mathbb{C}(W)/\mathbb{C}(X)$ using variables $u_{X/Z}, u_{W/X}$ so that

$$\mathbb{C}(X) = \mathbb{C}(Z)(u_{X/Z}) \text{ and } \mathbb{C}(W) = \mathbb{C}(Z)(u_{X/Z}, u_{W/X}).$$

In referring to conjugates in the next discussion we mean elements in an algebraic closure of $\mathbb{C}(Z)$. Denote the polynomial in the variable u^* for $u_{W,X}$ over $\mathbb{C}(Z)(u_{X,Z})$ by $P(u^*) \in \mathbb{C}(Z)(u_{X,Z})[u^*]$.

This gives polynomial equations for conjugates $u_{X/Z}^1, \ldots, u_{X/Z}^m$ of $u_{X/Z}^1 = u_{X/Z}$ over $\mathbb{C}(Z)$. Substituting in the coefficients of $P(u^*)$ for the conjugates of $u_{X/Z}^1$ gives polynomials $P_k(u^*) \in \mathbb{C}(Z)(u_{X/Z}^k)[u^*]$, for $k = 1, \ldots, m$. For each k, this gives conjugates $u_{W/X}^{k,j}$, $j = 1, \ldots, n$, for the solutions of $P_k(u_{W/X})$.

Each Galois extension of $\mathbb{C}(X)$ obtained by adjoining $\{u_{W/X}^{k,j}, j = 1, \ldots, n\}$ to $\mathbb{C}(Z)(u_{X/Z})$ has group identified with $G_{W/X} \leq S_n$. This identifies $G_{W/Z}$ with a subgroup of the wreath product $G_{W/X} \wr G_{X/Z}$ where the semi-direct product action of $G_{X/Z}$ on $G_{W/X}^n$ is given by our discussion of the conjugates of $u_{X/Z}^1$.

REMARK 1.2. The simplest example of computing the composite Galois closure above occurs where $W = \mathbb{P}_w^1$, $X = \mathbb{P}_x^1$ and $Z = \mathbb{P}_z^1$, using Luroth's Theorem that says that we may choose w so that x and z are rational functions in w, and you detect the composite as given by $f(w) = z = g(h(w))$ with $h(w) = x$ and h, g are rational functions in one variable. Additionally, we have RET and branch cycles to aid in the computation.

In many situations, however, the starting data is branch cycles for $f(w)$ and $g(x)$, where branch cycles for h must be surmized from these. The best situation is when – on general principles – you get the whole wreath product above for $G_{W/Z}$. In, however, many problems that isn't the case that attracts attention.

1.2.2. *Affine, nilpotent and other groups.* Let R be an integral domain. We will deal with $\mathbb{M}_n(R)$, the ring of matrices under the usual addition and multiplication, over R and the corresponding *general linear group* $\mathrm{GL}_n(R)$ – elements multiplicatively invertible. The natural action of $\mathrm{GL}_n(R)$ on $(R)^n$ gives the affine group $(R)^n \times^s \mathrm{GL}_n(R)$.

More generally, if we have a subgroup $H \leq \mathrm{GL}_n(R)$, regard its restriction to $(R)^n$ also as an affine group as giving an affine group $(R)^n \times^s H$. The multiplication can be represented as matrix multiplication – as is done in Ch. 1 §1.2 –

$$\left(\begin{smallmatrix} h_1 & 0 \\ r_1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} h_2 & 0 \\ r_2 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} h_1h_2 & 0 \\ r_1*h_2+r_2 & 1 \end{smallmatrix}\right).$$

Nilpotent: A profinite group G is nilpotent if it is a product of its ℓ-Sylows. Each such ℓ-Sylow is a quotient of the free pro-ℓ group of rank (minimal number of generators) the same as the ℓ-Sylow.

1.3. Linear algebra basics. Denote the $n \times n$ identity matrix by I_n. There are various vector spaces, V, over K on which we may regard Λ as acting, either on the right or left usually given by matrix multiplication. Most typically, by its action on $\mathbb{M}_{n,m}(\bar{K})$ (resp. $\mathbb{M}_{m,n}$) of matrices with n rows (resp. m rows) and m (resp. n) columns by multiplication on the left (resp. right).

We refer to V as a (left) *module*. Proper Λ modules are *irreducible* (also simple) modules if they have no proper submodules. Any such V is therefore generated – as a Λ module – by a single element, say $\boldsymbol{v} \in V$, denoted ${}_\Lambda\langle \boldsymbol{v}\rangle$. This module is irreducible if and only if the (annihilator) ideal $\mathrm{An}_{\boldsymbol{v}} = \{\lambda \in \Lambda \mid \lambda \boldsymbol{v} = 0\}$ is a maximal left ideal.

Our archetype is the endomorphism ring (Def. 1.7) of homomorphisms of V that commute with a matrix $A \in \mathbb{M}_n(K)$ acting on the left of $\boldsymbol{v} \in \mathbb{M}(n,1)(\bar{K}) = \bar{K}^n$. This gives $A(\boldsymbol{v})$ by dotting the vector $\boldsymbol{v}$ into the rows of A. For example for $n = 3$:

$$\text{Left Action: } A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \text{ and } \boldsymbol{v} = \begin{pmatrix} 1 \\ -1 \\ 2 \end{pmatrix} \text{ gives } A(\boldsymbol{v}) = \begin{pmatrix} 5 \\ 11 \\ 17 \end{pmatrix}.$$

If we had chosen the right action of A on $\boldsymbol{v} \in \mathbb{M}(1,3)$ the result would be

$$(\boldsymbol{v})A = \begin{pmatrix} 11 & 13 & 15 \end{pmatrix} \text{ akin to the above for } \boldsymbol{v} = \begin{pmatrix} 1 & -1 & 2 \end{pmatrix}.$$

As a preliminary algebra we take $\Lambda^0 = \Lambda^0_A \stackrel{\text{def}}{=} K[A]$ (acting on the left). Then the Λ^0 module generated by $\boldsymbol{v}$ is

$$\{P(A)(\boldsymbol{v}) \mid P \in K[x]\} \text{ or the span of } \{A^k(\boldsymbol{v}) \mid 0 \le k \le n-1\}.^2$$

The vector space dimension of any such Λ is a submodule of the finite dimensional space $\mathbb{M}_n(K)$which has finite dimension. Each ideal in Λ is also a vector space. Therefore any chain of descending ideals is bounded by the dimension of Λ. This gives Lem. 1.3 under what will be our basic assumptions:

$$\begin{array}{c}\Lambda \text{ is a Noetherian and } \textit{Artinian ring};\\ \text{that is also associative and has an identity.}\end{array} \tag{6.2}$$

LEMMA 1.3. *For any proper subalgebra Λ of $\mathbb{M}_n(K)$, and any finite dimensional module V, V has a (proper) minimal, and so simple, submodule. In particular, any left (or right) ideal I of Λ, contains a minimal left (or right) ideal I^*.*

Jordan canonical form as a guide: For the following discussion on Jordan canonical form assume $K = \bar{K}$ is algebraically closed. Recall: an *eigenvector* of A is a vector, $\boldsymbol{v} \neq \boldsymbol{0}$, that generates a 1-dimensional A-invariant subspace of $V = K^n$: $A(\boldsymbol{v}) = \lambda\boldsymbol{v}$, with *eigenvalue* λ (possibly 0). Eigenvalues those values $\lambda \in K$ for which $N_\lambda = A - \lambda \mathrm{I}_n$ is *not* invertible.

Equivalently, N_λ has a nontrivial *null* space, an eigenvector with eigenvalue 0.

The last line of Lem. 1.4 continues into our discussion of an example giving Jordan canonical form as an explicit conjugate DAD^{-1},

LEMMA 1.4. *If N_λ is not invertible, then there is an integer $0 < t \le n$ with these properties:*

(6.3a) *$V_\lambda \stackrel{\text{def}}{=} \ker(N_\lambda^t)$ is a nontrivial invariant subspace;*

(6.3b) *N_λ acts without kernel on R_λ the range of N_λ^t; and*

(6.3c) *V is a direct sum of V_λ and R_λ.*

Inductively, A acting on V is a direct sum of the N_λ modules running over all A eigenvalues. Then, each V_λ is a direct sum of indecomposable $K[A]$ modules, $V_{\lambda,1}, \dots, V_{\lambda,s}$. If $V_{\lambda,k}$ has dimension t_k, it has a basis $\{\boldsymbol{v}_0, \dots \boldsymbol{v}_{t_k-1}\}$ for which the irreducible modules for the action of A on $V_{\lambda,k}$ are in this series:

$$\langle \boldsymbol{v}_0\rangle < \langle \boldsymbol{v}_0, \boldsymbol{v}_1\rangle < \cdots < \langle \boldsymbol{v}_0, \dots \boldsymbol{v}_{t_k-1}\rangle. \tag{6.4}$$

In particular, each $V_{\lambda,k}$ contains precisely one eigenspace.

This gives a complete accounting of the irreducible and indecomposable invariant module constituents for the action of $\Lambda^0_A = K[A]$ on K^n.

[2]Since $A = \lambda$ is a zero of its degree n *characteristic polynomial* $\det(A - \lambda I_n)$.

PROOF. Since N_λ is not invertible, its range, an invariant subspace for N_λ, has dimension less than n, and its kernel is nontrivial. By induction, there is a minimal integer $t \leq n$ so that N_λ^{t+1} has exactly the same range as N_λ^t, and this defines V_λ in the statement of the lemma as the set of vectors killed by some power of N_λ.

This gives an algorithm for finding the eigenvalues of A on V_λ by corresponding to $\boldsymbol{v} \in V_\lambda$ the minimal integer k with $N_\lambda^k(\boldsymbol{v}) = \mathbf{0}$. Then, $N_\lambda^{k-1}(\boldsymbol{v})$ is an eigenvector of N_λ. A basis of R_λ and a basis of V_λ together have cardinality n. So it suffices to show $R_\lambda \cap V_\lambda = \{\mathbf{0}\}$. But the overlap would be a nonzero vector $\boldsymbol{v}$ killed by N_λ^t and in an invariant space with no vector is killed by N_λ. Thus, there is an integer u for which $N_\lambda^{u-1}(\boldsymbol{v}) \in R_\lambda$ is nonzero, fwith $N_\lambda^{u-1}(\boldsymbol{v}) = \mathbf{0}$; a contradiction.

The first sentence of the second paragraph results from an induction by restricting A to R_λ. Cramer's rule gives the eigevalues of A as the zeros of $\det(A - \lambda I_n)$.[3] The second sentence is most relevant for the sequel on Loewy display. Start by considering the eigenvectors for powers of N_λ^{t-1} on V_λ, starting with a basis of eigenvectors of N_λ^{t-1}. Each such eigenvector, say $\boldsymbol{v}$, then produces a basis of an indecomposable subspace for A on V_λ by considering a chain of antecedents:

$$\begin{gathered} \mathcal{B}_{\boldsymbol{v}} = \{\boldsymbol{v} = \boldsymbol{v}_0, \boldsymbol{v}_1, \ldots, \boldsymbol{v}_{t-1}\}, \text{ so that} \\ N_\lambda(\boldsymbol{v}_{t-1}) = \boldsymbol{v}_{t-2}, N_\lambda(\boldsymbol{v}_{t-2}) = \boldsymbol{v}_{t-3}, \ldots, N_\lambda(\boldsymbol{v}_1) = \boldsymbol{v}_0. \end{gathered} \tag{6.5}$$

We see that the vectors in $\mathcal{B}_{\boldsymbol{v}}$ are linearly independent by taking a supposed linear dependence relation of the form $\boldsymbol{v}_k + a_{k-1}\boldsymbol{v}_{k-1} + \cdots + a_0\boldsymbol{v}_0 = \mathbf{0}$ with the starting term indexed by $k \leq n$ as small as possible. But there must be at least one $a_u \neq 0$, $u \leq k-1$. Apply N_λ to this expression to get a contradition.

If this gives a basis for V_λ we are done. If not, take another basis element from the eigenvectors of N_λ^{t-1}, and repeat the construction of a new set of basis vectors for another indecomposable module. Then, juxtapose the basis of this new module with the set $\mathcal{B}_{\boldsymbol{v}}$. When you are done with those go to a basis of eigenvectors of N_λ^{t-2}, etc. We do that explicitly for a particular set of As in Lem. 1.6 below. That shows the result as blocks along diagonal of a matrix similar to A from which the invariant indecomposables and irreducibles appear. □

The relevant equivalence on matrices is Def. 1.5.

DEFINITION 1.5. Two elements $A, A' \in \mathbb{M}_n(K)$ are *similar* (denoted $A \sim A'$) if there is an element $D \in \mathrm{GL}_n(K)$ such that $DAD^{-1} = A'$. Equivalently, A' is the matrix of A given by changing the standard basis $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ to the columns of D.

The minimal value $t = t_{\mathrm{nil}}$ given in the statement of Lem. 1.4 is the nilpotency of N_λ. The matrix A has as its ith column $A(\boldsymbol{e}_i)$, with $\boldsymbol{e}_i$ with all entries 0, except the ith, which is 1. The essential case is to find a basis, $\mathcal{B} = \boldsymbol{v}_1, \ldots, \boldsymbol{v}_n$, of V for

[3] There are more elementary approaches, using elementary row operations (say, [**Axl15**, §8.D]; I would have preferred "... done well.") Yet, Cramer's rule is so elegant, I hate to leave it out.

which A is canonical with expressed in terms of $\mathcal{B}$ (see the example in the proof of Lem. 1.6), when the only eigenvalues of N_λ are 0. Here is an example of the canonical form when $n = 9$ where $N'_\lambda = DN_\lambda D^{-1}$ or $A' = DAD^{-1}$:

$$N'_\lambda = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix} \text{ and } A' = \lambda \mathrm{I}_n + N'_\lambda \tag{6.6}$$

This is a case where $k_{\text{nil}} = 3$. It is easy to turn the proof of Lem. 1.6 – whose notation we use below – into a proof of of Jordan canonical form for any matrix over the algebraic closure of any perfect field. It also has a reminder of what is meant by computing the matrix relative to a basis. Suppose $A^* : \mathbb{R}^9 \to \mathbb{R}^9$ has a unique eigenvalue λ, and $N^*_\lambda = A^* - \lambda I_9$.

LEMMA 1.6. *Assume also: $k_{\text{nil}} = 3$; the range, R_2, of $(N^*_\lambda)^2$ has dimension 2; and the range, R_1, of N^*_λ has dimension 5. Conclusion: A^* is A' in* (6.6) *relative to some basis $\mathcal{B}^* = \boldsymbol{v}^*_1, \dots, \boldsymbol{v}^*_9$.*

PROOF. Take a basis $\boldsymbol{w}_1, \boldsymbol{w}_2$ of R_2. For each, form $\boldsymbol{v}_{i,2}, \boldsymbol{v}_{i,1}, \boldsymbol{v}_{i,0} = \boldsymbol{w}_i$, $i = 1, 2$, so that $N_\lambda(\boldsymbol{v}_{i,2}) = \boldsymbol{v}_{i,1}, N_\lambda(\boldsymbol{v}_{i,1}) = \boldsymbol{v}_{i,0}, i = 1, 2$. Then, this list,

$$\mathcal{B}_1 = \{\boldsymbol{v}_{1,0}, \boldsymbol{v}_{1,1}, \boldsymbol{v}_{1,2}, \boldsymbol{v}_{2,0}, \boldsymbol{v}_{2,1}, \boldsymbol{v}_{2,1}\}, \text{consists of linearly independent vectors.}^4$$

So, in the range of N^*_λ, of dimension 5, there is another vector – which we take as $\boldsymbol{v}_{3,0}$ – that must go to $\mathbf{0}$ under N^*_λ. It too has an N^*_λ preimage $\boldsymbol{v}_{3,1}$. Adjoining $\mathcal{B}_2 = \{\boldsymbol{v}_{3,0}, \boldsymbol{v}_{3,1}\}$ to $\mathcal{B}_1$ gives 8 linearly independent vectors in V.

There must be one more vector, $\boldsymbol{v}_{4,0}$, that goes to $\mathbf{0}$ under N^*_λ,. We have a basis for V by adjoining $\boldsymbol{v}_{4,0}$ to $\mathcal{B}_1 \cup \mathcal{B}_2$. Just rename them, as $\boldsymbol{v}^*_, \dots, \boldsymbol{v}^*_9$ in this order:

$$\boldsymbol{v}_{1,0}, \boldsymbol{v}_{1,1}, \boldsymbol{v}_{1,2}, \boldsymbol{v}_{2,0}, \boldsymbol{v}_{2,1}, \boldsymbol{v}_{2,2}, \boldsymbol{v}_{3,0}, \boldsymbol{v}_{3,1}, \boldsymbol{v}_{4,0}.$$

Indeed, compute A^* relative to this basis by applying N^*_λ to each vector in order. Then rewrite the result as a linear combination of the $\boldsymbol{v}^*$s. For example, $N^*(\boldsymbol{v}_{1,0}) = \mathbf{0}, N^*(\boldsymbol{v}_{1,1}) = \boldsymbol{v}_{1,0}, N^*(\boldsymbol{v}_{1,2}) = \boldsymbol{v}_{1,1}$. This gives us the 3×3 block in the upper left corner of N'_λ. Etc. □

Matrix A' in Lem. 1.6 has 4 blocks along its diagonal. Each corresponds to an invariant, indecomposable subspace, for A^* acting on V; each such subspace having precisely one eigenspace. For example, $V_1 = \langle \boldsymbol{v}_{1,0}, \boldsymbol{v}_{1,1}, \boldsymbol{v}_{1,2} \rangle$ is invariant under A^*,

[4]The Lem. 1.4 proof shows the 1st 3 and 2nd 3 are linearly independent. Write a minimal relation among them; the 1st 3 on one side, the last 3 on the other; apply N_λ for a contradiction.

for which $\langle \boldsymbol{v}_{1,0}\rangle$ is its only eigenspace. There is no direct sum decomposition of $V_1 = V_{1,0}$ into proper invariant subspaces.[5] Similarly, A^* has $V_2 = \langle \boldsymbol{v}_{2,0}, \boldsymbol{v}_{2,1}, \boldsymbol{v}_{2,1}\rangle$, $V_3 = \langle \boldsymbol{v}_{3,0}, \boldsymbol{v}_{3,1}\rangle$ and $V_4 = \langle \boldsymbol{v}_{4,0}\rangle$ as indecomposable invariant subspaces. This is the complete list of invariant indecomposable subspaces for A^* action on K^9.

Algebra form of submodules of M: We now use Jordan canonical form as a guide to general definitions about an algebra (satisfying (6.2)) acting on a module M by first extending Λ_A^0 to a larger algebra.

DEFINITION 1.7. For an algebra Λ acting on a left (or right) Λ module M write $\mathrm{End}_\Lambda(M) = \mathrm{Hom}_\Lambda(M, M)$ for the homomorphisms from M to M that commute with the action of Λ. This, too, is an associative algebra.

Write $\Lambda_A \stackrel{\text{def}}{=} \mathrm{End}_{\bar K[A]}(M)$ for the $\bar K$ algebra of homomorphisms of M that commute with the action of Λ_A^0. Assume M is finite dimensional Λ module and write M as a direct sum, $\oplus_{i=1}^u M_i$, of Λ invariant modules.

Lem. 1.8 is immediate from the definitions.

LEMMA 1.8. *If E_i is the homomorphism of M that is the identity on M_i, and 0 on M_j, $j \neq i$, then $E_i, I_n - E_i \in \mathrm{End}_{\Lambda_A^0}(M)$, $I_n = \sum_{i=1}^u E_i$ and:*

$$E_i^2 = E_i, (I_n - E_i)^2 = I_n - E_i, \text{ and for } i \neq j, E_i \cdot E_j = \mathbf{0}_n. \tag{6.7}$$

Further, if M_i is indecomposable, then E_i cannot be decomposed as $E_i' + E_i''$ with E_i', E_i'' satisfying (6.7).

DEFINITION 1.9. Suppose an algebra Λ has elements $E_1, \dots, E_u$ satisfying the properties of (6.7). We call them orthogonal idempotents. Refer to them as *primitive* if the modules M_i are indecomposable.[6]

Consider matrices that centralize an $n \times n$ matrix $E_{n,j}$ whose entries are all 0, except those – all 1 s – along the j+1th diagonal given by the entries

$$\{(k, j+k) \mid 1 \leq k \leq n-j\}, 0 \leq j \leq n-1.$$

For example, N_λ' in (6.6) has $E_{3,1}, E_{3,1}, E_{2,1}, E_{1,1}$ as blocks along its diagonal. Lem. 1.10 considers $\mathrm{Cen}_{E_{n,1}}$, the matrices that centralize $E_{n,1}$.

LEMMA 1.10. *In the notation above, the following hold.*

(6.8a) $\mathrm{Cen}_{E_{n,1}} = \{\sum_{j=0}^{n-1} a_j E_{n,j} \mid a_j \in \mathbb{C}\}$*; and for* $1 \leq s \leq n$,

(6.8b) $\langle \boldsymbol{e}_1, \dots, \boldsymbol{e}_s\rangle$ *is the unique $E_{n,1}$ invariant subspace of dimension s.*

[5] Hint: If there were, restriction of A^* to each would have its own eigenspace, contrary to A^* having just one eigenspace on V_1.

[6] We can get away with the basics, say, from [**Be91**, p. 7–8], but future projects following the lead of this book will require further education.

More generally, suppose N has 0 s everywhere, except it has Jordan form blocks consisting of the matrices $E_{n_1,1},\dots,E_{n_u,1}$ along its diagonal. Then, the centralizer C_N contains $\mathrm{Cen}_{E_{n_1,1}}\times\cdots\times\mathrm{Cen}_{E_{n_u,1}}$.[7]

In particular, Cen_N *contains the matrices $E_{n_j,0}=E_j$ that are 0 everywhere, except at the position of the jth block, it is I_{n_j}, with*

(6.9) $E_1,\dots,E_u$ *satisfying the conditions of Lem. 1.8.*

Finally, replace N by $A\in\mathbb{M}_n$; with 0 s everywhere, except – a kin to N – blocks $\lambda_jE_j+E_{n_j,1}$, along the diagonal. Then, the E_j s are in Cen_A, $j=1,\dots,u$.

Proof. Use that $E_{n,1}^m=E_{n,1+m-1}$, $1\le m\le n-1$. Claim, the terms to the left (and below) the main diagonal of an $A\in\mathrm{Cen}_{E_{n,1}}$ are all zeros. For example, look at the $(n-j,1)$ term of $AE_{n,1}=E_{n,1}A$, $1\le j\le n-1$: From the left side it is 0; from the right it is $a_{n-j+1,1}$. The first column entries of A below the first are 0.

Similarly, dotting the kth column of $E_{n,1}$ (resp. A) into the $n-j$th row of A (resp. $E_{n,1}$) gives equality of the $(n-j,k)$ terms as

$$a_{n-j,k-1}=a_{n-j+1,k},0\le j\le n-k,\ \text{and proceed inductively.}$$

2nd claim: A has all terms along the kth diagonal equal. For example, look at the term $(j,j+1)$ of both sides of $AE_{n,1}=E_{n,1}A$. On the left is $a_{j,j}$ and on the right $a_{j+1,j+1},1\le j\le n-1$. So all the terms along the (1st) diagonal are equal.

Similarly, dotting the $j+k$th column of $E_{n,1}$ (resp. A) into the jth row of A (resp. $E_{n,1}$) gives the $(j,j+k)$ term equality as

$$a_{j,j+k-1}=a_{j+1,j+k}\text{ for }2\le j+1\le n,1\le k\le n-j.$$

Consider the properties (6.8). If $\boldsymbol{x}=(x_1,\dots,x_n)$ is an eigenvector (so nonzero) of $E_{n,1}$, since $E_{n,2}(\boldsymbol{x})=(x_2,x_3,\dots,x_n,0)$, there is a value λ such that $\lambda x_i=x_{i+1}$, $i=1,\dots,n-1$. Conclude, $\lambda=0$, and x_1 is the only nonzero entry. That shows (6.8a). Further, in imitation of the example of degree 9, (6.6), $E_{n,1}$ maps $\boldsymbol{e}_s$ to $\boldsymbol{e}_{s-1}$, and V_s generates by $\{E_{n,1}^j(\boldsymbol{e}_s),j=1,\dots,s\}$ is the invariant dimension s subspace naturally associated to $E_{n,1}$.

The last line of the lemma is essentially already in Lem. 1.8. □

Corollary 1.11. *In the notation of Lem. 1.10, with $\Lambda_A=\mathrm{End}_{\bar K[A]}(M)$, each maximal submodule of M is of the form $E'M$ for some element $E'\in\Lambda_A$. Therefore we can write every submodule of M in such a form.*

Proof. If we write M as a direct sum of indecomposable modules, $\oplus_{i=1}^u M_i$, then the maximal submodules are of the form

$M_1\oplus\cdots\oplus M_{i-1}\oplus M'\oplus M_{i+1}\oplus\cdots\oplus M_u$ with M' the maximal submodule of M_i.

[7] If, for example, $u=2$ and $n_1=n_2$, the centralizer of N is larger, for it also contains the matrix that switches the last n_1 columns with the first n_1 columns. The whole centralizer of N is now clear in Lem. 1.10 from this principle.

In this case take

$$E' = E_1 \oplus \cdots \oplus E_{i-1} \oplus E_{n_i,1} \oplus E_{i+1} \oplus \cdots \oplus E_u.$$

We know every submodule of M explicitly, and can continue inductively in this style in the general case. □

1.3.1. *Loewy layers of a* Λ *module.* This section introduces *Loewy* displays of the simple modules that compose general modular representations. The opening section of [**Be91**] treats this as elementary material, run through quickly with few details. We have structural properties in §1.5.4 and examples in §1.6 sufficient to avoid having to characterize them.[8] This extension is more abstract, for finite dimensional modules M over an algebra Λ satisfying (6.2).

DEFINITION 1.12. The *socle*, $\mathrm{Soc}(M) \stackrel{\mathrm{def}}{=} \mathrm{Soc}^1(M)$ ($\mathrm{Soc}^0(M) = \{0\}$), of M is generated by all irreducible submodules of M. The Socle layers are defined by successive application of the Soc operator to a previous socle quotient:

$$\mathrm{Soc}^2(M) = \mathrm{Soc}(M/\mathrm{Soc}^1(M)), \mathrm{Soc}^3(M) = \mathrm{Soc}(M/\mathrm{Soc}^2(M)), \ldots$$

Then, M is *completely reducible* if $M = \mathrm{Soc}(M)$.

DEFINITION 1.13. The *radical*, $\mathrm{Rad}(M) \stackrel{\mathrm{def}}{=} \mathrm{Rad}^1(M)$ of M is the intersection of all maximal submodules of M. Radicals are defined by successive application of the Rad operator: $\mathrm{Rad}^0(M) = M$, $\mathrm{Rad}^2(M) = \mathrm{Rad}(\mathrm{Rad}^1(M))$, ... Successive radical quotients define the *Loewy series*:

$$\mathrm{Rad}^0(M)/\mathrm{Rad}^1(M) \text{ the } \textit{head}, \mathrm{Rad}^1(M)/\mathrm{Rad}^2(M), \ldots.$$

In displaying the Loewy series for group rings $K[G]$ we put the head to the far right, the rest of the layers to the left of it (as in §1.6).

EXAMPLE 1.14 (Lem. 1.6 Socle series and Loewy series). For a matrix A acting on K^n and having precisely one eigenvalue, say λ, the socle of $K[A]$ is the direct sum of the eigenspaces of A. That is, one for each block along the diagonal of its Jordan canonical form. That means for the matrix A' of (6.6), its socle has dimension 4, generated by the eigenspaces $\langle \boldsymbol{v}_{j,0} \rangle, j = 1, 2, 3, 4$.

Here is a prescription for the $K[A]$ maximal submodules. They are given by considering a block A_i, running from the r_i to the $r_{i+1}-1$ row in the canonical form. Then, its corresponding submodule is M_i spanned by $\mathcal{B}_i = \{\boldsymbol{e}_{r_i}, \ldots, \boldsymbol{e}_{r_{i+np1}-1}\}$. Its submodules form a uniserial series.[9] Therefore a maximal submodule corresponding to it is given by removing $\boldsymbol{e}_{r_{i+np1}-1}$ from the standard basis.

[8] That anyway, would be beyond our expertise.

[9] In (6.6), the module corresponding to the 2nd block is spanned by $\mathcal{B}_2 = \{\boldsymbol{e}_4, \boldsymbol{e}_5, \boldsymbol{e}_6\}$, and its other two invariant submodules, respectively by $\{\boldsymbol{e}_5, \boldsymbol{e}_6\}$ and $\{\boldsymbol{e}_6\}$.

Conclude: Rad(A) of $K[A]$ is the subspace generated by standard basis vectors, with the vectors $\{\boldsymbol{e}_{r_i-1} \mid i$ running over the blocks of $A\}$ removed. So, in (6.6), the images of $\{\boldsymbol{v}_{1,3}, \boldsymbol{v}_{2,3}, \boldsymbol{v}_{3,1}, \boldsymbol{v}_{4,0}\}$ generate the 1st Loewy layer of $K[A']$. △

The Jacobson radical:

For finitely generated modules over a Noetherian Λ, there are (maximal) composition series of submodules of a Λ module M: A chain

$$\{0\} < M_1 < \cdots < M_t = M$$

of submodules (composition factors or constituents) with no possible further refinements. The Jordan-Hölder theorem [**Be91**, Thm. 1.1.4] says that any two such maximal chains have the same lengths, and the (simple) quotients M_i/M_{i+1} (*constituents*) are uniquely defined up to reordering.

For M a left Λ module, $\varphi_\lambda : m \to \lambda m, m \in M$ is a module homomorphism. The annihilator, Ann(M), of M is $\{\lambda \in \Lambda \mid \varphi_\lambda$ is $0\}$: a 2-sided ideal.

Call a module M *semisimple* or *completely reducible* if it is the direct sum of irreducible (or *simple*) Λ modules. A module M is semisimple if and only its component series is a direct sum $\oplus_{i=1}^t M_i$ with the M_i s simple.

Then, among the maximal submodules of M are the sums $N_j = \oplus_{i,i\neq j} M_i$. So, $\cap_{j=1}^t N_j = 0$, and Rad(M) $= 0$. Conversely, if Rad(M) $= 0$, consider any collection $\{N_i\}_{i\in I}$ of maximal submodules, and the sum $M_I^* = \oplus_{i\in I} M/N_i$. There is a natural map, $\psi_I : M \to M_I^*$, with $\ker(\psi_I) = \cap_{i\in I} N_i$. From DCC on submodules, there is a finite subset I such that $\ker(\psi_I) =$ Rad(M). For any chain of such I s, select I minimal so that this holds

Reminder: If I is a left ideal then the Λ module Λ/I is a (natural) ring if and only if I is a 2-sided ideal. Define $J_L(\Lambda)$ (resp. $J_R(\Lambda)$) to be the intersection of maximal left (resp. right) ideals of Λ). The following treatment benefitted from [**Ro02**, p. 544–5, p. 547–8].

LEMMA 1.15. *These statements are equivalent to $x \in J_L(\Lambda)$.*

(6.10a) *The elements* $1 - \Lambda x \stackrel{\text{def}}{=} \{1 - \lambda x \mid \lambda \in \Lambda\}$ *each have a left inverse.*

(6.10b) $x \cdot \Lambda/I = \{\mathbf{0}\}$ *for every maximal left ideal I.*

From (6.10b)*, $J_L(\Lambda)$ is the intersection of* Ann(Λ/I) *running over maximal left ideals I. So, it is a 2-sided ideal. Further:*

(6.11a) *J_L of the ring $\Lambda/J_L(\Lambda) = \bar{\Lambda}$ is trivial; and*

(6.11b) *for any finitely generated Λ module M, $M/J_L(\Lambda)M$ is completely reducible. Equivalently, $J_L(\Lambda)M =$* Rad(M).

PROOF. A module M is irreducible if and only if any nonzero element in M igenerates it as a Λ module. Also, the two sided ideal $\mathrm{Ann}(M)$ is maximal if and only if every nonzero element of $\Lambda/\mathrm{Ann}(M)$ is invertible: It is a division algebra.

Consider $x \in J_L(\Lambda)$, $\lambda \in \Lambda$ for which $1-\lambda x$ has no left inverse, Then some maximal left ideal I contains $1-\lambda x$. So, $1-\lambda x+\lambda x = 1 \in I$, contrary to I being a proper ideal: (6.10a) holds.

Now we show (6.10a) implies (6.10b). Consider a maximal left ideal I, and $\bar{m} \in \Lambda/I$ for which $x\bar{m} \neq \mathbf{0}$. Since Λ/I is simple, $\Lambda x\bar{m} = \Lambda/I$. There must be $\lambda' \in \Lambda$ with $\lambda' x\bar{m} = \bar{m}$. That means $(1-\lambda' x)$ has no left inverse contrary to (6.10a).

Expression (6.11a) follows from $J_L(\Lambda/J_L(\Lambda)) = J_L(\Lambda)/J_L(\Lambda) = \{1\}$.[10]

Another way to write (6.11a) is to say, that Λ as a left Λ module – say, denoted ${}_\Lambda\Lambda$ – is completely reducible. By choosing generators of M, we can write M as a quotient of a direct sum of copies of Λ. That implies M is also completely irreducible, concluding the lemma. □

Lem. 1.15 equally holds for defining $J_R(\Lambda)$ using maximal right ideals. That uses right units in place of (6.10a). Now use the collection of 2-sided units, U in Λ:

$$\{u \in \Lambda \mid \exists u', u'' \in \Lambda, uu' = 1 = u''u\}.^{11}$$

PROPOSITION 1.16. *The following equality gives the symmetric version of the Jacobson radical, $J(\Lambda)$:*

$$J' \stackrel{\mathrm{def}}{=} \{x \in \Lambda \mid 1+\Lambda x\Lambda \textit{ consists of 2-sides units}\} = J_L(\Lambda) = J_R(\Lambda).$$

For any finitely generated module M, $J(\Lambda)M = \mathrm{Rad}(M)$.

PROOF. From (6.10a), $J' \subset J_L(\Lambda)$.

Consider $x \in J_L(\Lambda)$, a 2-sided ideal, so $x\Lambda \subset J_L(\Lambda)$, and any $1-\lambda' x\lambda$ has a left inverse u: $u(1-\lambda' x\lambda) = 1$. This shows u has a right inverse. It also has the form $1+v$ with $v \in J_L(\Lambda)$, so it has a left inverse. As already noted, this makes u a 2-sided unit and $1-\lambda' x\lambda \in J'(\Lambda)$. The same result holds for $J_R(\Lambda)$.

With the last line following from Lem. 1.15 and the equality of $J(\Lambda)$ and $J_L(\Lambda)$, conclude the proof of the proposition. □

Central idempotents and blocks: Recall Def. 1.9: primitive, orthogonal idempotents. There is a 1-1 association between primitive orthogonal decompositions

$$1 = \sum_{u=1}^{t} E_u \text{ and direct sum decompositions, } \sum_{u=1}^{t} \Lambda_u$$

[10] [**Ro02**, p. 320] has this for $I = J_L(\Lambda)$ of a correspondence principle for rings. It states this for Λ commutative, a one-one correspondence for ideals between I and Λ and quotients of these by I. It should be between two-sided ideals in this range and the quotients.

[11] So, $u'(uu'') = (u'u)u'' = u' = u''$ from associativity of multiplication.

into indecomposable modules of the (left) regular representation of Λ: $E_i\Lambda = \Lambda_i$ [**Be91**, p. 11]. Even more useful is [**Be91**, p. 14].

LEMMA 1.17. *If in addition to the above, the idempotents are central, then the decomposition is into 2-sided ideals. This decomposition – up to order – is unique.*[12]

PROOF. Because the idempotents are central, the ideals $E_i\Lambda$ are 2-sided. If $1 = \sum_{u=1}^{t'} E'_u$ is another such decomposition. Then, if $E_uE'_{u'}$ is not 0, then it is another central idempotent. Thus, $E_u = E_uE'_1 + \cdots + E_uE'_{t'}$, and therefore, from primitivity, $E_u = E_uE'_{u'} = E'_{u'}$, for a unique u'. □

The decomposition above is often written $\Lambda = \sum_{u=1}^{t} B_u$ with the B_us called the *blocks* of Λ. If a Λ module M is indecomposable, then $M = \sum_{u=1}^{t} E_uM$ and for a unique u, $E_uM = M$: M belongs to the uth block. The *principal block* is the block of the trivial module $\mathbf{1}_G$. The idea is general. We apply it generally to any indecomposable module M of a Noetherian algebra Λ over a field K or $\mathbb{Z}$ or its p-adic completion.

COROLLARY 1.18. *All simple constituents in any indecomposable module belong to the same block.*

This applies to any projective indecomposable. For $\Lambda = \mathbb{Z}/\ell[G]$, the simple modules of the characteristic module $\frac{1}{\ell}M_G$ all belong to the principal block.

PROOF. Suppose E is a primitive central idempotent that corresponds to block B, and M is indecomposable. Assume M' is a simple constituent of M given as a submodule of M/M^* for some submodule of M^* of M. Then, $EM^* = M^*$ inducing $EM/M^* = M/M^*$, and E acts as the identify on M'.

That completes the first sentence. Now consider $\Lambda = \mathbb{Z}/\ell[G]$, and the characteristic module $\frac{1}{\ell}M_G$. From Chp. 2 Prop. 2.16, $\frac{1}{\ell}M_G$ is an indecomposable Λ module each of whose constituents can be described as a constituent formed from a length two chain: from the projective indecomposable $P_{\mathbf{1}_G}$, then to a projective indecomposable P_M where M is a constituent at the head of the kernel of $P_{\mathbf{1}_G} \to \mathbf{1}_G$. The first step implies M is in the principal block, and the corollary now follows from the first sentence applied to P_M. □

Relating the Loewy layers:

REMARK 1.19. Given an idempotent E of Λ then $E\Lambda E$ is clearly an algebra under multiplication. So, are both $\mathrm{End}_\Lambda(\Lambda E)$ and $\mathrm{End}_\Lambda(E\Lambda)$) (resp. regarding ΛE, $E\Lambda$ as a left, right Λ module). The latter (resp. former) is isomorphic (resp. isomorphic with the opposed multiplication) to $E\Lambda E$. Here is the argument for a natural

[12] Λ_A in Lem. 1.10, for $A \in \mathbb{M}_n(\bar{K})$, has only central idempotents.

isomorphism $\psi : E\Lambda E \to \mathrm{End}_\Lambda(\Lambda E)$ for the opposed multiplication statement: For $E\lambda E \in E\Lambda E$, and $\lambda' E \in \Lambda E$,

$$\psi(E\lambda E)(\lambda' E) \mapsto \lambda' E(E\lambda E) = (\lambda' E\lambda)E \in \Lambda E.$$

The left Λ action commutes with this map as the action of $E\lambda E$ is on the right; it is the opposed multiplication because $\varphi(E\lambda_2 E)\varphi(E\lambda_1 E) = \varphi(E\lambda_1\lambda_2 E)$.

1.4. Homological reminders. The short [**Br82**, Ch. 1 §0] contains many definitions. We will try to be expedient in imitating it by concentrating on what we require for comfort with cohomology of $R[G]$ modules in computing, say, $H^2(G, M)$ or $\mathrm{Ext}^r_G(M, N)$ where $R = \mathbb{Z}$ or $\mathbb{Z}/\ell$ or closely related.

As a guide, consider these general comments. In homological algebra, group cohomology, homotopy theory, etc. there are two different objects that get conjoined in treatments. These are sequences of objects – *chain complex* – in some category,

$$\mathcal{C} \stackrel{\mathrm{def}}{=} \cdots C_{i+1} \xrightarrow{d_{i+1}} \to C_i \xrightarrow{d_i} \cdots,$$

ostensibly infinite in both directions but usually 0 from some point on to the right, with $d_{i+1} \circ d_i = 0, i \geq 0$. Notationally, we say $\boldsymbol{d} = \{d_i\}_{i\in\mathbb{Z}}$ has square-zero *differential*: $\boldsymbol{d} \circ \boldsymbol{d} = \mathbf{0}$. The expectation is that the construction of such sequences is categorical. The reason d' etre for them is that, as in Def. 1.7 and Def. 1.8, the quotient of the kernel of d_i by the image of d_{i+1}, $H_i(\mathcal{C})$ will meanfully interpret and compute properties of the object(s) M (and N) which gave rise to the sequence.

[**Br82**] takes an historical approach, starting from simplicial complexes, based on topological CW complexes, and the fundamental group $\pi_1(X)$ of X, a topological space. From that defines the group cohomology of an arbitrary discrete group (from which we can go to a profinite group easily), as given by forming a $\mathbb{Z}[G]$ *projective resolution* of $\mathbb{Z}$ as a trivial G module. The particular projective resolution is formed from the CW structure (with a G action on it) with C_i the chains of dimension i, and a map $C_0 \to \mathbb{Z}$ by $\sum_k u_i p_i \mapsto \sum_i u_i$ where the sum is over a finite set of points. The last is called the *augmentation map* . Then, remove the augmentation map to get a complex whose cohomology is independent of the CW complex structure.

To generalize to group (including finite) homology, with coefficients in a G module M, the replacement is to take any projective resolution of M, generalizing the augmentation map. Then prove it doesn't matter which projective resolution you take. The reason is that any one complex $\mathcal{C}' \to M$ will have a chain map, $\boldsymbol{f} : \mathcal{C}' \to \mathcal{C}$, of degree 0 (preserving the subscripts) to any other such complex $\mathcal{C} \to M$, preserving the respective maps to M, and commuting with the differentials: $\boldsymbol{f} \circ \boldsymbol{d}' = \boldsymbol{d} \circ \boldsymbol{f}$ from using projective modules.

Further, the homology groups will be the same [**Br82**, Ch. I Thm. 7.5]. There are three specifics to this that lead to general definitions. First: the idea of a *homotopy*,

$\boldsymbol{h} : \mathcal{C}' \to \mathcal{C}$, $h_i : C'_i \to C_{i+1}$, $i \geq 0$ between chain maps ${}_k\boldsymbol{f}$, $k = 1, 2$.

$$\boldsymbol{h} \circ \boldsymbol{d}' + \boldsymbol{d} \circ \boldsymbol{h} = {}_1\boldsymbol{f} - {}_2\boldsymbol{f}. \tag{6.12}$$

The key in [**Br82**, Ch. I Thm. 7.5] is that the augmentation preserving chain maps from two different projective resolutions are unique up to homotopy, and therefore the automatic map $\boldsymbol{f}' : \mathcal{C} \to \mathcal{C}'$ from the same argument, will induce $\boldsymbol{f} \circ \boldsymbol{f}'$ and $\boldsymbol{f}' \circ \boldsymbol{f}$ to both be homotopic to the identity. Clearly, then the homotopy groups are the same.

If you have an explicit chain complex, then you might be able to explicitly interpret/calculate the homology. Certainly that is what happens in Def. 1.8 to interpret $H^2(G, M)$ via the bar resolution. The H^1 and H^2 interpretations should suffice to indicate what that resolution is in general.

Comments on $\mathrm{Ext}^r_G(M, N)$*:*

RETURNM Put the right diagram here.

$$\begin{array}{ccc} E_{j'} & \xrightarrow{\text{degree } \ell \text{ isogeny}} & E_{j'}/C_{\ell^{k+1}} \\ {\scriptstyle \bmod \langle \pm 1 \rangle}\downarrow & & {\scriptstyle \bmod \langle \pm 1 \rangle}\downarrow \\ \mathbb{P}^1_w & \xrightarrow{\text{degree } \ell \text{ rational function } f} & \mathbb{P}^1_z \end{array} \tag{6.13}$$

Since this seems to general, it might seem that *mere* extensions are just a small part of the topic of cohomology groups. Maybe, but maybe not, since actual computation comes down to explicit cases, and even these (as in Prop. 2.16) entangle group cohomology and Ext. Therefore we comment on the properties of (3.27). Also, in the category that interests us most, that of $\mathbb{Z}/\ell[G]$ modules, how unlike the category of $\mathbb{Z}$ modules in having projectives and injectives the same.

Restriction and corestriction: Suppose $H \leq G$, a finite group and A is a (left) G module, compatible with the notation around Def. 1.8. We add to the properties of $H^n(G, A)$ and $H^n(H, A)$ an action of G induced by conjugation, comparing them just enough to define the operators res^G_H and cor^G_H.

At the level of cocycle functions, if ${}_Hc \in \mathrm{Hom}_{\mathbb{Z}[H]} : \mathbb{Z}[G]^n \to A$, we want to act with $g \in G$ by the diagonal action that maps

$$(g_1, \ldots, g_n) \mapsto g * {}_Hc(g^{-1}g_1, \ldots, g^{-1}g_n).$$

For $g \in H$, the result is

$$g(g^{-1}) * {}_Hc(g_1, \ldots, g_n) = {}_Hc(g_1, \ldots, g_n).$$

That is ${}_Hc$ is invariant by g.

More generally, if ${}_Hc$ is the restriction of ${}_Gc \in \mathrm{Hom}_{\mathbb{Z}[G]} : \mathbb{Z}[G]^n \to A$ to H, then the resulting element is invariant by $g \in G$. To generalize the action of $g \in G$, we can just map elements in (H, A) to (gHg^{-1}, A) by $(h, a) \mapsto (ghg^{-2}, g * a)$. Call this

map Con_g, and trace through that it gives an isomorphism between $H^n(H, A)$ and $H^n(gHg^{-1}, A)$. Again, tracing through the action to cohomology, this gives.

LEMMA 1.20. *If $H \triangleleft G$, then $\mathrm{Con}_g, g \in G$ induces an action of G/H on $H^n(G, A)$.*

1.4.1. *Including ramification.* Allowing ramification includes using ramification groups (stabilizers of the primes defining crucial points). These appeared in class field theory in the case given by number fields; Riemann's existence theorem in the case of compact Riemann surfaces. Those join together in the study of curve covers over finite fields.

Those cases are were the idea of normalization arose, and normalization guarantees a unique Galois closure. This has also worked very well in problems where you can guarantee that the maps appearing as $\varphi : X \to Z$ are finite and X and Z are both nonsingular. In that case, the map is automatically flat, a Grothendieck cover, and the fiber dimensions have locally constant degree.

Normal varieties are always nonsingular in codimension 1 (singularity may have codimension as small as 2). The one problem appears in the normalization in the function field of the fiber product components, which may actually be singular. Fiber products of φ with itself will be singular if there is ramification, but normalization often removes that.

1.5. Modular representations. Following some literature comments, §1.5.1, on why modular representations are hard, we exposit on their classical theory, §**??**, especially Loewy layers and projectives. Ch. 1 §1.3 started our series of statements on ℓ-Frattini covers (of finite groups), and their relation to *nilpotent* groups. §1.5.3 describes when our characteristic ℓ-Frattini covers of G are truly characteristic in the sense of being preserved by automophisms that might not come from their actual construction.

Finally, §1.5.4 concludes with our best shot at two explicit constructions of ${}_\ell M_G$: recognizing it from its homological definition (Prop. 1.27), and taking advantage of its indecomposability (Prop. 1.28).

1.5.1. *Modular representations are hard, but ...* Classifying the $\mod \ell$ representations (up to equivalence) is "wild" in the formal technical sense, whenever the ℓ-Sylow is not cyclic and, when $\ell = 2$, not dihedral, semi-dihedral, nor generalized quaternion. [**BoDr77**] and [**Ri75**].

The technical sense of wild used here implies that a classification of the $\mod \ell$ representations of any *one* such group would provide a classification of the $\mod \ell$ representations of *any* finitely generated algebra over $\mathbb{F}_\ell$. Hence such problems are often referred to as *hopeless*. We resist thinking this on the basis of two aspects relevant to their appearance in our considerations.

Approach 1: As characteristic modules for ℓ-perfect groups: Our seed group G, which we fix here, is either ℓ-perfect, or when we must go beyond that case, we *fold under* the ℓ-Frattini covers that come from the Ext-Frattini part of the ℓ-Frattini cover of G as in §3.3.3. For simplicity, consider just the former case here.

Ch. 1 (1.11) already separates considerations from the characteristic quotients of the full ℓ-Frattini cover of G from the abelianized extension ${}_\ell\tilde{G}_{\rm ab} \to G$ that define **MT**s. We also know these facts.

(6.14a) With N_ℓ the normalization in G of an ℓ-Sylow P_ℓ, extension ${}^1_\ell G \to G$ factors through an extension $N^*_\ell \to G$ with kernel $\mathrm{ind}^G_{N_\ell}({}_\ell M_{N_\ell})$ (from Lem. **??**) from the extension ${}^1_\ell N_\ell \to N_\ell$.

(6.14b)

Look at p. 174 Cor. 1.4 to see if I have the quote of Shapiro's lemma correctly.

Approach 2: No need for a "perfect" display: There is a great quote by Mumford in a footnote criticizing the "hopeless" aspect here:

The classification of [two] non-commuting maps $f, g\colon V \to V \mod \mathrm{GL}(V)$ is sometimes referred to as an impossible problem. It is not clear to me why this is said. If $\dim V = n$, then for each n, there might be a finite number of explicitly describable algebraic varieties $W_i^{(n)}$ whose points are in natural 1-1 correspondence with suitable strata $S_i^{(n)}$ in the full set S_n of pairs $(f, g)\colon k^n \to k^n \mod \mathrm{GL}(n)$ [**MuFo82**, App. C, Ch. 4, footnote p. 167].

2) Over any field L, the theory of finite-dimensional $L\langle < X, Y > \rangle$-modules (non-commutative polynomial ring in 2 variables) is undecidable [**Ba75**] and [**KoMa73**].

1.5.2. *Loewy layers and projective modules.* Despite the above we can wend our way through accessible information about the characteristic $\mathbb{Z}/\ell[G]$ modules, ${}_\ell M_G$, by which we define and divine properties of the moduli spaces at the center of this book. First we consider topics mentioned in (3.27c) and which are necessary to gain some understanding of what possible modules can arise. The author learned these from [**Be91**], which – unlike here – treats the definitions in far greater generality.

(6.15a) Loewy layers: Defining successive maximal quotients of completely reducible modules.

(6.15b) Frobenius duality: Concluding the regular representation of $\mathbb{Z}/\ell[G]$ (which is automatically projective) is also injective.

(6.15c) A simple quotient determines any projective indecomposable module.

These topics come alive in examples of §1.6.

Comments on (6.15a)*:* Define the *radical*, $\mathrm{Rad}(M) = \mathrm{Rad}^1(M)$, of a $\mathbb{Z}/\ell[G]$ module M to be the intersection of its maximal proper submodules. Then, $M/\mathrm{Rad}(M)$ is the maximal completely reducible quotient of M. This lends itself to an inductive

definition, $\mathrm{Rad}(\mathrm{Rad}^u(M)) = \mathrm{Rad}^{u+1}(M)$, and its successive sequence – finite in our case – of *Loewy layer quotients*,

$$\{\mathrm{Rad}^{u-1}/\mathrm{Rad}^u(M)\}_{u=1}^{\infty} \text{ with it convenient to define } \mathrm{Rad}^0(M) = M. \tag{6.16}$$

The complication is how these layers fit together. From Prop. 2.16, ${}_\ell M_G$ is indecomposable. Therefore, significant examples of nontrivial Loewy layers arise immediately from the case of normal ℓ sylows in G that aren't cyclic; and then from (non-cyclic) simple groups, even when an ℓ-Sylow is cyclic. §1.6 gives explicit examples, uses $G = A_5$ for $\ell = 2, 3, 5$.

§1.5.4 gives a procedure, often more effective than finding the Loewy display of ${}_\ell M_G$, that gives the basic structure needed for properties of the reduced Hurwitz spaces that are the levels of a **MT** at the core of this book.

Comments on (6.15b)*:* [**Be91**, Prop. 1.6.2] is a telegraphic treatment of the equivalence of projective and injective modules in the category of $\mathbb{Z}/\ell[G]$ modules. For our case it starts with the augmentation map:

$$\lambda : \mathbb{Z}/\ell[G] \to \mathbb{Z}/\ell \text{ by } \sum_{g\in G} a_g g \mapsto \sum_{g\in G} a_g,$$

and the left and right regular representation modules ${}_L\mathbb{Z}/\ell[G]$ and $\mathbb{Z}/\ell[G]_R$. This gives a linear map that turns out ot be a module homomorphism

$$\varphi_\lambda : {}_L\mathbb{Z}/\ell[G] \to \mathrm{Hom}(\mathbb{Z}/\ell[G]_R, \mathbb{Z}/\ell) \stackrel{\mathrm{def}}{=} \mathbb{Z}/\ell[G]_R^* :$$
$$\varphi_\lambda(x) : y \in \mathbb{Z}/\ell[G]_R \mapsto \lambda(yx).$$

LEMMA 1.21. *Define φ_λ as a module homomorphism using, for $g \in G$,*

$$g\varphi_\lambda(x)(y) \mapsto \varphi_\lambda(x)(yg) = \lambda(xgy) = \varphi_\lambda(gx)(y).$$

The equalities are the result of $\lambda(xy) = \lambda(yx)$. Further, φ_λ is injective, and since the range has the same dimension as the image, it is an isomorphism.

Applying the definition of projective to a (finite dimensional) module M shows that $\mathrm{Hom}(M, \mathbb{Z}/\ell) = M^*$ is also projective. Ditto for injective. For finite dimensional modules dualizing take injectives to projectives, and vice-versa.

PROOF. From linearity of λ, to show $\lambda(xy) = \lambda(yx)$ it suffices to take $y = g'$, $g' \in G$. In that case $\sum a_g g'g$ clearly has the same coefficients as $\sum a_g gg'$, just in a different order.

Apply this symmetry to see the equalities in the formula of the lemma. The rest of the observations to give (6.15b) are in the statement of the lemma. □

Comments on (6.15c), *Projective indecomposables:* Denote the algebraic closure of $\mathbb{Z}/\ell = \mathbb{F}_\ell$ by K_ℓ. We list ingredients from the theory of *modular representations* [**A86**, Chaps. 1-3]. Brauer's Theorem (below) on simple G modules forces

considering, at times, $\dot{\mathcal{G}} = K_\ell[G]$ modules instead of $\mathbb{F}_\ell[G] = \mathcal{G}$ modules. Translation between statements about $\mathcal{G}$ modules to $\dot{\mathcal{G}}$ modules is usually straightforward. A $\dot{}$-over notation for a $\mathcal{G}$ module means we've tensored with K_ℓ to make it a $\dot{\mathcal{G}}$ module. In contrast to an *indecomposable* $\dot{\mathcal{G}}$ module – one without a nontrivial direct summand – is a *simple* (or *irreducible*) $\dot{\mathcal{G}}$ module – one with no proper submodules.

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

(6.17a) *Brauer's theorem*: The collection of $\dot{\mathcal{G}}$ modules has the same cardinality as G conjugacy classes whose elements have order prime to ℓ [**A86**, p. 14].

(6.17b) Indecomposable projectives M correspond to simple $\dot{\mathcal{G}}$ modules via the map $M \to M/\mathrm{rad}(M)$ [**A86**, p. 31].

(6.17c) M is a projective $\dot{\mathcal{G}}$ module if and only if M_{P_ℓ}, P_ℓ an ℓ-Sylow of G, is a free $K_\ell[P_\ell]$ module [**A86**, p. 33 and 66].

Induced modules and Shapiro's Lemma: For a $\mathbb{Z}/\ell[G]$ module N^G, and $H \le G$, denote the module given by restriction of the G action to $\mathbb{Z}/\ell[H]$ by $N^G_{\downarrow H}$. Denote an ℓ-Sylow of G by P_ℓ, and its normalizer in G by $N_G(P_\ell) \stackrel{\text{def}}{=} N_\ell$. Then, consider the characteristic ℓ-Frattini module (for N_ℓ) ${}_\ell M(N_\ell)$.

It may not be a natural G module. For $H \le G$, consider a $\mathbb{Z}/\ell[H]$ module M_H.

$$\text{Then, the module } M_H^{\uparrow G} \stackrel{\text{def}}{=} \mathrm{ind}_H^G(M_H) \stackrel{\text{def}}{=} M_H \otimes_{\mathbb{Z}/\ell[H]} \mathbb{Z}/\ell[G]$$

induced from M_H is a $\mathbb{Z}/\ell[G]$ module. Define the right action of G akin to how G acts on right cosets of H in G, say as listed by $Hg_1, \ldots, Hg_r$:

$$\text{For } m \otimes g_i \in M_H \otimes g_i, \text{ if } g_i g = h g_j, h \in H, \text{ then } (m \otimes g_i)g \mapsto (m)h \otimes g_j.$$

[**Br82**, p. 63] inspired the universal property in Lem. 1.22.

LEMMA 1.22. *For any $\mathbb{Z}/\ell[G]$ module N^G, $\mathrm{Hom}_{\mathbb{Z}/\ell[G]}(M_H^{\uparrow G}, N^G)$ is naturally isomorphic to $\mathrm{Hom}_{\mathbb{Z}/\ell[H]}(M_H, N^G_{\downarrow H})$.*

Also, in all of this we may replace $\mathbb{Z}/\ell$ by $\mathbb{Z}_\ell$.

PROOF. Given a $\mathbb{Z}/\ell[H]$ module homomorphism, $\mu : M_H \to N^G_{\downarrow H}$, we are forced to associate to it

$$\mu^{\uparrow G} : M_H^{\uparrow G} \to N^G \text{ by } m \otimes g_i \in M_H \otimes g_i \mapsto ((m)\mu)g_i.$$

Assuming, for $g \in G$, with $g_i g = h g_j$, showing this is a $\mathbb{Z}/\ell[G]$ homomorphism requires checking if $(((m)\mu)g_i)g = (((m)\mu)h)g_j$. That it does, since the action of $h \in H$ commutes with μ. □

Cor. 1.23 applies Lem. 1.22 when $H = N_\ell$, $M_H = {}_\ell M_H$ and $N^G = {}_\ell M_G$.

COROLLARY 1.23. *With notation as above, there is a $\mathbb{Z}/\ell[G]$ module homomorphism of ${}_\ell M_H^{\uparrow G}$ into ${}_\ell M_G$.*

From Shapiro's Lemma: $H^2(G, {}_\ell M_H^{\uparrow G}) = H^2(N_\ell, {}_\ell M_H)$. If this natural generating extension is a Frattini cover, then ${}_\ell M_H^{\uparrow G}$ identifies with ${}_\ell M_G$.

PROOF. Restrict the characteristic cover ${}^1_\ell G$ to N_ℓ. The universal ℓ-Frattini property induces a map ${}^1_\ell N_\ell \to {}^1_\ell G$ that gives a $\mathbb{Z}/\ell[N_\ell$ homomorphism embedding of ${}_\ell M_H \to {}_\ell M_G$. From Lem. 1.22 that produces a $\mathbb{Z}/\ell[G]$ embedding ${}_\ell M_H^{\uparrow G} \to {}_\ell M_G$, completing the first line of the corollary.

□

PROBLEM 1.24. As in Prob. 1.1 show, with $n = (G : H)$, that regarding G as a subgroup of $H \wr S_n$ and the action there of the wreath product on M_H^n, then $M_H^{\uparrow G}$ is the restriction of this action to G.

REMARK 1.25. Prob. 1.24 is from [**Be91**, p. 89]. By replacing M^n by the n-fold tensor $M^{\otimes n}$, that applies to a construction called *tensor induction*.

1.5.3. *Characteristic subgroups of ${}_\ell\tilde{G}$.* Use the notation of Lem. 1.29

If P is an ℓ-group, then as in Lem. 1.24, its Frattini subgroup is (the closure of) ${}_{\rm fr}P \stackrel{\rm def}{=} P^\ell[P, P]$ and $P \to P/{}_{\rm fr}P$ is a Frattini cover.

Recover a cofinal family of finite quotients of ${}_\ell\tilde{G}$ through the Frattini kernel of the natural map $1 \to \ker_0 \to {}_\ell\tilde{G} \to G \to 1$ as in (1.9).

Terms of $\mathcal{K}_G = \{\ker_k\}_{k=0}^\infty$ should reference G unless it is understood. For example, they may not be characteristic subgroups of ${}_\ell\tilde{G}$, as easily seen by example for $P = {}_\ell\tilde{F}_t$ (as in (1.7b)). Still, Lem. 1.26 extends [**BFr02**, Lem. 3.10].

LEMMA 1.26. *If $\ker_0$ is a characteristic subgroup of ${}_\ell\tilde{G}$, then so are all terms of $\mathcal{K}_G$. Since the intersection of the ℓ-Sylows of ${}_\ell\tilde{G}$ is a characteristic subgroup of ${}_\ell\tilde{G}$ (containing $\ker_0$), $\ker_0$ is characteristic if the ℓ-Sylows of G intersect in $\langle 1_G\rangle$, as when G is simple.*

In general, $\mathcal{K}_G$ is cofinal in the closed subgroups in the profinite topology. In particular, the automorphisms, $\mathrm{Aut}({}_\ell\tilde{G})_G$ of ${}_\ell\tilde{G}$ that extend those of G define a profinite group.

PROOF. The first statement follows because $\ker_1$ is a characteristic subgroup of $\ker_0$: Every automorphism of ${}_\ell\tilde{G}$ recognizes ℓth powers and commutators. Any automorphism of ${}_\ell\tilde{G}$ will take $\ker_0$ into itself by hypothesis. So it will induce an automorphism on the characteristic subgroup $\ker_1$, making that a characteristic subgroup of ${}_\ell\tilde{G}$. Proceed by induction to conclude this holds for all the $\ker_k$ s.

As with finite groups, all ℓ-Sylows of ${}_\ell\tilde{G}$ are conjugate [**FrJ86**, Prop. 22.9.1]$_2$. Therefore their intersection is a characteristic subgroup, containing $\ker_0$. If the ℓ-Sylows of G intersect in $\langle 1\rangle$, then the intersection of the ℓ-Sylows of ${}_\ell\tilde{G}$ is $\ker_0$, proving it is characteristic.

From (1.7b), $\ker_0$ is pro-free, and $\{\ker_i\}_{i=1}^\infty$ is a neighborhood base of the origin consisting of characteristic subgroups of $\ker_0$. Thus, automorphisms of ${}_\ell\tilde{G}$ that extend those of G (so mapping $\ker_0$ into itself) also act on each of $\{\ker_i\}_{i=1}^\infty$, and on the quotients ${}^k_\ell G$. This means, with the natural notation, $\mathrm{Aut}({}_\ell\tilde{G})_G$ is the projective limit of the finite groups $\mathrm{Aut}({}^k_\ell G)_G$, concluding the proof. □

1.5.4. *Constructing ${}_\ell M_G$.* Ch. 1 Prop. 1.30 gives structural statements about the Universal Frattini cover of $\tilde{G}$. Ch. 3 Prop. 2.16 gave a description of ${}_\ell M_{k,k+1}$ given ${}^k_\ell G$. Prop. 1.27 extends this to ${}^{k+1}_\ell G$ given solid information on the following short exact sequences of ${}^k_\ell G$ modules with $P_{\mathbf{1}}$ the projective indecomposable for $\mathbf{1} = \mathbf{1}_{{}^k_\ell G}$, and P the minimal projective ${}^k_\ell G$ module covering $\Omega^1(\mathbf{1})$.

(6.18a) $1 \to \Omega^1(\mathbf{1}) \to P_{\mathbf{1}} \to \mathbf{1} \to 1.$

(6.18b) $1 \to \Omega^2(\mathbf{1}) \to P \to \Omega^1(\mathbf{1}) \to 1.$

Compute boundary maps from the standard exact sequences of cohomology:

$$H^0({}^k_\ell G, \mathbf{1}) \xrightarrow{\delta_0} H^1({}^k_\ell G, \Omega^1(\mathbf{1})) \xrightarrow{\delta_1} H^2({}^k_\ell G, \Omega^2(\mathbf{1})).$$

Denote a vector space generator of $\mathbf{1}$ by $1_{\mathbf{1}}$.

PROPOSITION 1.27. *The element $\delta_1 \circ \delta_0(1_{\mathbf{1}}) \in H^2({}^k_\ell G, \Omega^2(\mathbf{1}))$ represents the group extension ${}^{k+1}_\ell G$ whose class generates $H^2({}^k_\ell G, \Omega^2(\mathbf{1}))$, as in Prop. 2.16.*

To be explicit, consider the semi-direct product $\Omega^1(\mathbf{1}) \times^s {}^k_\ell G$. Choose $m \in P_{\mathbf{1}}$ lying over $1_{\mathbf{1}}$. The cocycle $g \mapsto g(m) - m$ for $g \in G$ represents $\delta_0(1_{\mathbf{1}})$. This cocycle defines a splitting $\psi : {}^k_\ell G \to \Omega^1(\mathbf{1}) \times^s {}^k_\ell G$ by $g \mapsto (g(m) - m, g)$. Then, ${}^{k+1}_\ell G$ is the preimage in $P \times^s {}^k_\ell G$ of $\psi({}^k_\ell G)$ in $\Omega^1(\mathbf{1}) \times^s {}^k_\ell G$ from sequence (6.18a).

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

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

The essence of identifying ${}^{k+1}_\ell G$ is to show that pullback of $\psi({}^k_\ell G)$, as an extension of ${}^k_\ell G$, has the correct 2-cocycle. Suppose α represents a 1-cocycle. Then, $g \mapsto (\alpha(g), g)$ gives a splitting of ${}^k_\ell G$ in $\Omega^1(\mathbf{1}) \times^s {}^k_\ell G$. For each $g \in {}^k_\ell G$ let $\bar{\alpha}(g)$ be an element of P lying over $\alpha(g) \in \Omega^1(\mathbf{1})$.

The boundary map *differentiates* the 1-cycle $g \mapsto \alpha(g)$ to give

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

[**Nor62**, p. 241] shows this 2-cocycle is the factor system for the associative multiplication on the pullback group. □

§1.6 puts Prop. 1.27 into action with the primes dividing A_5, using Prop. 1.28, an alternate way to trying construct the Loewy decomposition of ${}_\ell M_G$.

1.5.5. *Small ℓ-Frattini quotients of ${}_\ell\tilde{G}$.* Ch. 3 Prop. 2.16 shows that the characteristic module ${}_\ell M_G$ is indecomposable. Prop. 1.27 gives an inductive construction of all of the groups ${}^k_\ell G$. That, however, is dependent on finding two projective modules, for ${}^k_\ell G$, one of them the projective indecomposable for $\mathbf{1}_{{}^k_\ell G}$.

This is illuminating, precisely clarifying the homological algebra in forming the characteristic ℓ-Frattini modules going up the universal ℓ-Frattini cover. Still, it fails in practice to show how to approach these towers. We set our sights on a much more practical use of **MT**s, though retaining the idea that it is the moduli spaces that count the most, and we have some insight on the modular curve case.

The small quotients we have in mind all support our previous topics and conjectures. We know some properties of the characteristic module ${}_\ell M_G$. For example, it is an indecomposable G module whose irreducible subquotients all belong to the principle block. In most cases, however, the module is difficult to compute, and only on general abstract principles – at this time – can we draw conclusions about the corresponding **MT** levels.

Rubric for the arithmetic of covers: More naively, assume someone has a group G of interest to them, and a cover, defined over, say, $\mathbb{Q}$, $\varphi : X \to \mathbb{P}^1_z$, whose geometric monodromy group is G. They are particularly interested in the branch cycles, $\mathbf{C}$, of this cover, and how Hilbert's irreducibility theorem is producing this group as a Galois group.[13] You suggest one cover at a time is a pain and that you can show them a serious **HIT** situation using **MT**s.

You propose forming extensions of G like that of (6.1) (or (1.11)), and putting the whole families of covers with similar branch cycles together, akin to forming the groups ${}^k_\ell G_{\rm ab}$ based on Nielsen classes $\mathrm{Ni}({}^k_\ell G_{\rm ab}, \mathbf{C})$ with $(\ell, N_{\mathbf{C}}) = 1$.

Induction from an ℓ-Sylow: Here we give another extension construction of **MT** objects for (G, ℓ) as used in the constructions above. They can be easier to put in the context of known modular group results. For our given situation starting with (G, p) such quotients $\psi : H \to G$ will have $\ker(\psi)$ a $\mathbb{Z}_\ell[G]$ module constructed in a general way from our previous results.

PROPOSITION 1.28 (ℓ pieces: Part 4). *Denote an ℓ-Sylow of G by P_ℓ, and its normalizer in G by $N_G(P_\ell)$.*

(6.19a) *There is an explicit lower bound on* $\mathrm{rk}(\ker(\tilde{\varphi}))$ *and* $\mathrm{rk}(\ker({}_\ell\tilde{\varphi}))$*, with the latter* $\geq 1 + |P|(\mathrm{rk}(P)-1)$.

[13] We have already given the collections of groups D_ℓ with involutions, $\ell \neq 2$, and A_n with 3-cycles and $\ell \not\mid 3$, of such situations that are in the mathematics literature.

(6.19b) $\mathrm{rk}(\ker({}_\ell\tilde{\varphi}))$ *in* (6.19a) *is the rank of*

$$ {}_\ell\tilde{M}_G \stackrel{\text{def}}{=} \ker({}_\ell\tilde{\psi}_G)/[\ker({}_\ell\tilde{\psi}_G), \ker({}_\ell\tilde{\psi}_G)] \text{ as a } \mathbb{Z}_\ell \text{ module.} $$

(6.19c) *The rank* (6.19b) *is the* $\mathbb{Z}/\ell$ *vector space dimension of* ${}_\ell M_G$.

PROOF. Now consider (6.19). Bound any ranks given there by bounding the corresponding ranks of its ℓ-Frattini constituents. To get a bound on the rank ${}_\ell M_G$, apply that $\ker_0$ RETURN is an index $|P|$ subgroup of any ℓ-Sylow, $\tilde{P}$, of ${}_\ell\tilde{G}$. Also, from (1.15a), $\tilde{P} = {}_\ell\tilde{F}_{\mathrm{rk}(P)}$. Therefore, from (1.7b), the rank of $\ker_0$ is $1 + |P|(\mathrm{rk}(P)-1)$, the same as that of ${}_\ell M_G$.

Check back on Rem. 3.13 related to how this applies to [**GS78**]. □

EXAMPLE 1.29 (P elementary abelian in (1.15a)). △

Other extensions giving **MT** s based on

(6.20a)

(6.20b) **MT** *s*.

DEFINITION 1.30.

1.6. Characteristic A_5 ℓ-Frattini covers. Notice our examples in this section, where we do discuss the Loewy displays of the projective indecomposables, is restricted to the cases at the start of §1.5.1 that are not considered "wild."

Let $\mathbb{M}_n(R)$ be the $n \times n$ matrices over an integral domain R. It is valuable to have an "elementary" model for the key definitions for algebras that work on group rings over finite fields and related. So §**??** reminds of how a slight enhancement of Jordan canonical form of a matrix $A \in \mathbb{M}_n(\mathbb{C})$ can be such.

1.6.1. *The case* $\ell = 5$. A 5-Sylow, P_5, is $\mathbb{Z}/5$, and the normalizer N_{P_5} in A_5 is a D_5 isomorphic to $\langle (1\,2\,3\,4\,5), (2\,3)(4\,5)\rangle$. Therefore, intuition might suggest it is – contrary to Prop. 3.10 – a candidate for the possibility that ${}_5M_G$ has rank 1.

If it did, restricting the characteristic 5-Frattini cover $\frac{1}{5}D_5 = D_{5^2}$ to ${}_5M_G$ would assure a nontrivial action. Therefore it could not be the trivial module. Nor could the trivial module be a quotient of ${}_5M_G$. Also, the Loewy display could not have a quotient with kernel $\mathbf{1}_{A_5}$ since that would give $\frac{1}{5}A_5$ with a nontrivial center contrary to Ch. 3 Prop. 2.18. Apply Prop. 1.28 showing that ${}_5M_G$ is indecomposable. Do the iterated construction from Prop. 2.16. If the projective indecomposable for $\mathbf{1}_G$ has V_4 at the head of $\Omega^1(\mathbf{1}_G)$, then – in computing $\Omega^2(G)$, the kernel, $\mathbf{1}_G$ would appear at its head because the projective indecompasable of V_4 is the degree 5 permutation representation of A_5, which has $\mathbf{1}_G$ as the kernel of its map to V_4.

Work in $\mathrm{PSL}_2(\mathbb{Z}/5)$*:* We want to check what is the module ${}_\ell M'_5 \stackrel{\text{def}}{=} \mathrm{ind}_{D_5}^{A_5}({}_5M_{D_5})$, which has dimension 6. Its irreducible subquotients have dimensions that sum to $\leq$

6, and don't contain $\mathbf{1}_{A_5}$. The only possibilities for the *indecomposable* subquotients are therefore the adjoint representation, or two copies of the adjoint representation, one on top of the other. We work within the identification of A_5 and $\mathrm{PSL}_2(\mathbb{Z}/5)$.

LEMMA 1.31. *Show how the case $\ell = 5$ applies to $\mathrm{PSL}_2(\mathbb{Z}/\ell)$ that ${}_\ell M_G$ is not the adjoint representation.*

PROOF. First we pick a copy of D_5 in $\mathrm{SL}_2(\mathbb{Z}/5) = G$, by selecting any two of its distinct involutions. Say

$$g_1 = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \text{ and } g_2 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & -1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & 2 \\ -1 & 1 \end{smallmatrix}\right).$$

We find $g' = g_1 g_2$ is $\left(\begin{smallmatrix} -1 & 1 \\ 1 & -2 \end{smallmatrix}\right)$ and $(g')^2 g'(g')^2 = 2\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & 1 \\ 1 & -2 \end{smallmatrix}\right)2\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) = \mathrm{I}_5$. Therefore $\langle g_1, g_2\rangle = H$ is a copy of D_5 in G. The module ${}_5 M_{D_5}$ now identifies with the conjugation action of H on its own 5-Sylow $P_5 \stackrel{\text{def}}{=} \langle g'\rangle$.

Now we investigate ${}_\ell M'_5$, which we write as

$$\oplus_{i=1}^{6} P_5 \otimes u_i \text{ with } u_1, \dots, u_6 \text{ cosets representatives of } H \text{ in } G.$$

Consider first the adjoint representation of G, as conjugation on the trace 0 matrices of $\mathbb{M}(\mathbb{Z}/5)$. Denote these by $\mathbb{M}_0(\mathbb{Z}/5)$.

□

1.6.2. *The case $\ell = 2$.* As in Ch. 1 Lem. 1.19, denote the pro-ℓ completion of the profree group $\tilde{F}_t$ on t generators by ${}_\ell\tilde{F}_t$.

PROPOSITION 1.32. *Let $H = A_4 = K_4 \times^s \mathbb{Z}/3$. Then, $M(H)$ identifies with the $\mathbb{Z}/2[H]$ module generated by the six cosets of a $\mathbb{Z}/2$ in A_4, modulo the module generated by the sum of the cosets. Any D_5 in A_5 has a unique $\mathbb{Z}/2$ lying in A_4. So, the action of A_4 on $\mathbb{Z}/2$ cosets extends to an A_5 action on cosets of a dihedral group. Thus,* Prop. **??** *gives ${}_2^1\tilde{A}_5$ as an extension of A_5 by $\ker_0(H)$.*

PROOF. Let $\psi : {}_\ell\tilde{F}_t \to P_\ell$ be a surjective homomorphism, with P_ℓ any (finite) ℓ group. Schreier's construction (1.7b) gives explicit generators of the kernel of ψ Apply this with $t = 2$, $\ell = 2$ and $P_2 = K_4$, the Klein 4-group and $\ker_0 = \ker(\psi)$. Let $\bar{\alpha}$ be a generator of $\mathbb{Z}/3$. With u and v generators of ${}_2\tilde{F}_2$ let $\bar{\alpha}$ act on ${}_2\tilde{F}_2$ by mapping (u, v) to $(v^{-1}, v^{-1}u)$.

Use $S = \{1, u, v^{-1}, u^{-1}v\}$ as coset representatives for $\ker_0$ in ${}_2\tilde{F}_2$. Form the set V of elements in $\ker_0$ having the form tus^{-1} or tvs^{-1} with $s, t \in S$. Toss from V those equal to 1. Now consider the images of $\bar{\alpha}$ and $\bar{\alpha}^2$ on $uu = u^2 = m_1 \in V$. This produces $v^{-1}v^{-1} = m_2$ and $u^{-1}vu^{-1}v = m_3$.

Consider $\bar{\alpha}$ on $m_6 = u(v^{-1})^2u^{-1}$. Recall: Modulo $\ker_1$ any two elements in $\ker_0$ commute. Apply this to get

$$v^{-1}(u^{-1}v)^2v = (v^{-1}u^{-1}v)(u^{-1})v^2 \mod \ker_1 = vu^{-1}vu^{-1} = m_5.$$

Apply $\bar{\alpha}$ again to get $v^{-1}u^2v = m_4$. The action of $K_4 \times^s \mathbb{Z}/3 = A_4$ on the m_is is the same as the action on the six cosets of an element of order 2.

Denote a commutator of two elements w_1, w_2 by (w_1, w_2). Modulo $\ker_1$ there are relations among the m_is: $m_1m_2m_3 = (u, v) \mod \ker_1$; and $m_4m_5m_6 = (u, v)^{-1} \mod \ker_1$. So, the product of the m_is is 1. The proof follows from associating a $\mathbb{Z}/2$ in A_4 with a dihedral in A_5 as in the statement of the proposition. □

1.7. Central extensions vs $\tilde{G} \to G$. The case $G = \mathrm{PSL}_2(\mathbb{Z}/\ell)$ is important, though somewhat misleading.

At its inception, the formulation of the conjectures on **MT**s were about the whole extension, $\tilde{\psi} : \tilde{G} \to G$, and its whole ℓ-Frattini quotients ${}_\ell\tilde{\psi} : \tilde{G}_\ell \to G$, rather than just about their abelianized versions. The arithmetic list of problems (**??**) makes a distinction between them, based on the idea that we eventually consider, say, a k quotient, $\tilde{G}_{\ell,k}$ of $\tilde{G}_\ell$. Then, we consider the ker ker ker ker ker ker kern kern kern kern RETURN As usual we understand kerpn kern kern to b e the closed subgroup of p G with generators from the elements of this set Though Lem. **??** is quite simple, we differentiate a structural group theory statement, say, about the ranks of the kernel of, say, from technical group theory in that Still, the pieces of ψ_G are technically constructive.

Example 1.33 (A most prestigious example). Ex. 2.9 and 2.11 both engage the universal central extension of A_n.

△

Every finite group has a maximal solvable quotient. Form it by considering the successive commutator subroups,

$$G \geq [G, G] \stackrel{\text{def}}{=} G_{1,c} \geq [G_{1,c}, G_{1,c}] \stackrel{\text{def}}{=} G_{2,c} \cdots \text{ until this sequence stops at } G_{u,c}.$$

Then, $G/G_{u,c}$ is the maximal solvable quotient of G.

Similarly, there is a maximal nilpotent quotient, G_{niq}, of G:

$$\text{replace } [G_{j-1,c}, G_{j-1,c}] = G_{j,c} \text{ by } G_{1,c} \stackrel{\text{def}}{=} G_{1,n}, [G, G_{1,n}] \stackrel{\text{def}}{=} G_{2,n} \cdots$$

until this sequence stops at $G_{t,n}$. Then, $G/G_{t,n}$ is G_{niq}.

2. Braid orbits

You want the components of the Hurwitz spaces, and you know the subsets with different lift invariants are in different braid orbits. Also, if a collection of generating conjugacy classes repeat often enough, the braid orbits correspond one-one to lift invariants. Here are examples that appear in the author's paper.

Groups they take, some others, and the lift invariant values.

(6.21a) p. 31: G is the dihedral group, $\mathbb{Z}/\ell \times^s \{\pm 1\}$ of order 2ℓ, ℓ odd, and c is the conjugacy class of involutions.

(6.21b) also p. 31: $G = V_\ell \times^s S_3$, where $\ell > 3$ is a prime, V_ℓ is the 2-dimensional reduced permutation representation of S_3, and c is again the conjugacy class of involutions.

(6.21c) In §12, Cohen-Lenstra Heuristics, they take what they call a generalized dihedral group $A \times^s \{\pm\}$ with A a finite abelian group of odd order with -1 acting as -1.

(6.21d) Akin to (6.21b), but much harder: $G = V_\ell \times^s \mathbb{Z}/3$, $\ell \neq 3$; c consists of the two nontrivial conjugacy classes in $\mathbb{Z}/3$, each repeated with the same, d', multiplicity: $c_{d',d'}$.

Comments on (6.21a): Prop. 6.0.3 shows how their results have gone beyond their previous paper in their bound on the Cohen-Lenstra class numbers. See (**????**).

I use example (6.21d) in §**??**.

2.1. Other braid orbit computations. The length of a q_i orbit on $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})^\bullet$ with $\bullet$ an equivalence relation is crucial to most explicit calculations of braid orbits, and so Hurwitz space components. Typically, we expect that to be $2\mathrm{ord}(g_i g_{i-1})$. Yet, there is an important exception when it is half that length. That occurred, for example, in the orbit labeled $\mathcal{H}^{+,\mathrm{in,rd}}$ in Table 2 for the shift of an **HM** cusp. Prop. 2.1 [**BFr02**, Prop. 2.17] explains that.

The structure constant formula (§**??**) calculates $|S(\mathbf{C}')|$ using complex representations of G. Calculations in §**??** compute the length of γ orbits on $S(\mathbf{C}')_{g_3}$. For g_1, g_2 in a group, denote the centralizer of $\langle g_1, g_2\rangle$ by $Z(g_1, g_2)$.

Let $g_1 g_2 = g_3$, and $g_2 g_1 = g_3'$. Let $o(g_1, g_2) = o$ (resp. $o'(g_1, g_2) = o'$ be the length of the orbit of γ^2 (resp. γ) on (g_1, g_2). If $g_1 = g_2$, then $o = o' = 1$.

Proposition 2.1. *Assume $g_1 \neq g_2$. The orbit of γ^2 containing (g_1, g_2) is $(g_3^j g_1 g_3^{-j}, g_3^j g_2 g_3^{-j})$, $j = 0, \dots, \mathrm{ord}(g_3)-1$. So,*

$$o = \mathrm{ord}(g_3)/|\langle g_3\rangle \cap Z(g_1, g_2)| \stackrel{\mathrm{def}}{=} o(g_1, g_2).$$

Then, $o' = 2 \cdot o$, unless o is odd, and with $x = (g_3)^{(o-1)/2}$ and $y = (g_3')^{(o-1)/2}$

(6.22) *(so $g_1 y = x g_1$ and $y g_2 = g_2 x$), $y g_2$ has order 2 and $o' = o$.*

Proof. For t an integer,

$$(g_1, g_2)\gamma^{2t} = (g_3^t g_1 g_3^{-t}, g_3^t g_2 g_3^{-t}) \text{ and } (g_1, g_2)\gamma^{2t+1} = (g_3^t g_1 g_2 g_1^{-1} g_3^{-t}, g_3^t g_1 g_1 g_1^{-1} g_3^{-t}).$$

The minimal t with $(g_1, g_2)\gamma^{2t} = (g_1, g_2)$ is $o(g_1, g_2)$. Further, the minimal j with $(g_1, g_2)\gamma^j = (g_1, g_2)$ divides any other integer with this property. So $j | 2o(g_1, g_2)$ and if j is odd, $j | o(g_1, g_2)$.

From the above, if the orbit of γ does not have length $2o(g_1, g_2)$, it has length $o(g_1, g_2)$. Use the notation around (6.22). The expressions $g_1y = xg_1$ and $yg_2 = g_2x$ are tautologies. If o is odd, then $(g_1, g_2)q_2^o = x(g_1, g_2)q_2x^{-1}$. Assume this equals (g_1, g_2), which is true if and only if $xg_1 = g_2x = yg_2$. The expression $(g_1g_2)^o = 1$ and $xg_1yg_2 = 1$ are equivalent. Conclude $(yg_2)^2 = 1$. So long as the order of yg_2 is not 1, this shows (6.22) holds. If, however, $yg_2 = xg_1 = g_2x = g_1y = 1$, then $g_1 = g_2$, contrary to hypothesis.

This reversible argument shows the converse: $(g_1, g_2)q_2^o = (g_1, g_2)$ follows from (6.22). This concludes the proof. □

2.2. Covers of higher genus curves. We easily extend the restricted and general lift invariants from §1 and §2 to consider ramified covers, $\varphi : W \to Z$, of compact Riemann surfaces, without assuming $Z = \mathbb{P}^1_z$. This is brief. Excluding that the fundamental group of Z is no longer trivial, this is fairly obvious.

With $\mathbf{g}_Z = \mathbf{g}$, the genus of Z, ramified at points $z_1, \dots, z_r$. Go to the Galois closure $\hat{\varphi} : \hat{W} \to Z$. Denote the automorphism group by G_φ, and let $\psi_G : R \to G$ be a *representation cover* of G: a *central* Frattini cover of G whose kernel – contained in the commutator subgroup in R – is isomorphic to the Schur multiplier of G. Denote $|\ker(\varphi_R)|$ by M_G. We are now in shape to imitate Cor. 2.6.

Suppose we have classical generators ,

$$(a_1^*, b_1^*, \dots, a_{\mathbf{g}}^*, b_{\mathbf{g}}^*, g_1^*, \dots, g_n^*) \stackrel{\text{def}}{=} P_{\boldsymbol{a}^*, \boldsymbol{b}^*, \boldsymbol{g}^*},$$

for the fundamental group, π_1, of $Z \setminus \{z_1, \dots, z_r\}$. Then φ determines a cover $\pi_1 \to G$ that sends the entries of $P_{\boldsymbol{a}^*, \boldsymbol{b}^*, \boldsymbol{g}^*}$ to elements of G, which we denote by $P_{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{g}}$. There is a natural product constructed from the entries of $P_{\boldsymbol{a}^*, \boldsymbol{b}^*, \boldsymbol{g}^*}$. Denote a commutator $(a_k^*)(b_k^*)(a_k^*)^{-1}((b_k^*))^{-1}$ by $[a_k^*, b_k^*]$. Form

$$\Pi_{k=1}^{\mathbf{g}}[a_k^*, b_k^*]\Pi_{i=1}^r g_i^*, \text{ referring to the result as } \Pi(\boldsymbol{a}^*, \boldsymbol{b}^*, \boldsymbol{g}^*).$$

Since $P_{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{g}}$ are classical generators, we have a product-one condition: $\Pi(\boldsymbol{a}^*, \boldsymbol{b}^*, \boldsymbol{g}^*) = 1$. Thus, so do the corresponding entries of $P_{\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{g}}$ satisfy product-one. As previously, the g_is define conjugacy classes $\mathrm{C}_1, \dots, \mathrm{C}_r$ in G for which, as previously, use the notation $N_{\mathbf{C}}$ for the least common multiple of the orders of their elements. Here are some facts about this.

(6.23a) If $(N_{\mathbf{C}}, M_G) = 1$, then (mini-Schur-Zassenhaus), we can lift the entries of $\boldsymbol{g}$ to R retaining the prime to N_G condition.

(6.23b) Denote the (6.23a) lifted entries by $P_{\hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \hat{\boldsymbol{g}}}$ and their product by $s_{R/G}(\hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \hat{\boldsymbol{g}}) \in \ker(R/G)$.

Directly compute that the value of the commutator $[\hat{a}_i, \hat{b}_i]$ won't depend on the choice of lifts for a_i and b_i to the central extension $R \to G$. Therefore the value of $s_{R/G}(\hat{\boldsymbol{a}}, \hat{\boldsymbol{b}}, \hat{\boldsymbol{g}})$ is well defined. Further, the argument of §1.3 shows that it is

an invariant of the deformation of $Z \setminus z_1, \dots, z_r$. Explanation: The most obvious meaning of that is, we deform Z in the space of genus **g** compact surfaces while continuously deforming the distinct points $z_1, \dots, z_r$. While that might look like it calls for a whole new proof, it seriously does not; you can move the complex structure leaving the branch points fixed, and you can get the effect of deforming the branch points by the generalization of braids to a genus *geng* surface.

Then, the formula for the general lift invariant, should the assumption of (6.23a) not hold, lies exactly in the quotient of Def. 2.1 as for $Z = \mathbb{P}^1_z$.

3. Serre's OIT

We have put here comments on Serre's version of his **OIT**. These are examples illustrating the concepts we use to generalize it. §3.1 starts with the notion of eventually (ℓ-)Frattini and how it is appropriate for what we are calling the *weak* **OIT**. That using **MT**s does generalize the **OIT** is in §3.2. This starts with the observation from [**Fr95**, §1.A], expanding on [**Fr77**, §2] that all the standard collections of modular curves,

$$\mathcal{X}_{0,\ell} \stackrel{\text{def}}{=} \{X_0(\ell^{k+1})\}_{k=0}^{\infty}, \mathcal{X}_{1,\ell} \stackrel{\text{def}}{=} \{X_1(\ell^{k+1})\}_{k=0}^{\infty} \text{ and } \mathcal{Y}_\ell \stackrel{\text{def}}{=} \{Y(\ell^{k+1})\}_{k=0}^{\infty},$$

as covers of $\mathbb{P}^1_j$, are compactified one-one (and onto) images of the reduced Hurwitz spaces listed on the left in (1).

3.1. Eventually ℓ-Frattini and Serre's OIT.

The first Prop. 3.2 statement might well be the most well-known piece from [**Se68**]. It is *the* examplar of the ℓ-Frattini property. We emphasize the eventually ℓ-Frattini property (Ch. 4 Def. 4.2). §3.1.1 does preliminaries relevant to our whole approach on SL_2 vs PSL_2. §3.1.2 is the proof of Prop. 3.2.

3.1.1. SL_2 *vs* PSL_2. Consider ${}_\ell\psi' : \mathrm{PSL}_2(\mathbb{Z}_\ell) \to \mathrm{PSL}(\mathbb{Z}/\ell)$ (or of $\mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{SL}(\mathbb{Z}/\ell)$). Then, $\ker({}_\ell\psi') = \mathrm{Ad}_3(\mathbb{Z}_\ell)$, 2×2 trace 0 matrices with coefficients in $\mathbb{Z}_\ell$, is abelian. Though Prop. 3.2 says they are ℓ-Frattini covers for $\ell > 3$, $\mathrm{PSL}_2(\mathbb{Z}_\ell)$ is far from the universal ℓ-Frattini cover of $\mathrm{PSL}_2(\mathbb{Z}/\ell)$.

Indeed, it is a proper quotient of ${}_\ell\tilde{G}_{\mathrm{ab}}$ with $G = \mathrm{PSL}_2(\mathbb{Z}/\ell)$ since the characteristic module $\mathrm{Ad}_3(\mathbb{Z}/\ell)$ is a proper quotient of ${}_\ell M_G$ (Rem. 1.31), even though, here, that proper quotient is indecomposable (even irreducible) as a $\mathbb{Z}/\ell[G]$ module.

The geometric monodromy of modular curves over the j-line, or of our dihedral group related reduced Hurwitz spaces in §3.2, are directly related to $\mathrm{PSL}_2(\mathbb{Z}_\ell)$ rather than $\mathrm{SL}_2(\mathbb{Z}_\ell)$. It is the Frattini properties of the geometric monodromy for general **MT**s that are the subject of topics such as Ch. 4 Conj. 4.5.

LEMMA 3.1. *For all ℓ, ${}_\ell\alpha : \mathrm{SL}_2(\mathbb{Z}/\ell) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$ is a Frattini cover.*

PROOF. A proper subgroup $G^* \le \mathrm{SL}_2(\mathbb{Z}/\ell)$, for which ${}_\ell\alpha$ restricted to G^* is onto, has index 2 in $\mathrm{SL}_2(\mathbb{Z}/\ell)$. Thus, G^* contains all the elements of order ℓ in $\mathrm{SL}_2(\mathbb{Z}/\ell)$. In particular it contains

$$A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \text{ and } B = \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right). \tag{6.24}$$

The effect of multiplying by A^a (resp. B^b) on any matrix C in $\mathrm{SL}_2(\mathbb{Z}/\ell)$ is to do row operations (of determinant 1) on C. If either the upper right corner or lower left corner of C is nonzero – say the latter – then multiplying on left by A^a for some a, then B^b for some b, can change C to a matrix with the upper left corner 1, and the lower left corner 0.

Since the resulting C is in $\mathrm{SL}_2(\mathbb{Z}/\ell)$, it has the form $\left(\begin{smallmatrix} 1 & b' \\ 0 & 1 \end{smallmatrix}\right) = B^{b'}$. That still leaves the case that C has diagonal form $C_{a'} = \left(\begin{smallmatrix} a' & 0 \\ 0 & (a')^{-1} \end{smallmatrix}\right)$. The remedy is to multiply C on the left by B to get a nonzero entry in the lower left corner, and proceed as above. □

PROPOSITION 3.2. *The natural cover* $\mathrm{SL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{SL}_2(\mathbb{Z}/\ell)$ *is a Frattini cover for all* k *if* $\ell > 3$.

For $\ell = 3$ *(resp. 2),* $\mathrm{SL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{SL}_2(\mathbb{Z}/\ell^{k_0+1})$, $k \ge k_0$ *where* $k_0 = 1$ *(resp. 2), is the minimal value for which these are Frattini covers.*

That is, for all ℓ, $\{\mathrm{SL}_2(\mathbb{Z}/\ell^{k+1})\}_{k=0}^{\infty}$ *is eventually Frattini.*

Then, ${}_\ell\tilde{\alpha} : \mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{SL}_2(\mathbb{Z}/\ell)$ *and* ${}_\ell\alpha \circ {}_\ell\tilde{\alpha} : \mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$ *are* ℓ*-Frattini for* $\ell > 3$*, and eventually* ℓ*-Frattini for all* ℓ.

In particular, the same statements apply to $\mathrm{PSL}_2(\mathbb{Z}_\ell) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$.

3.1.2. *Proof of Prop. 3.2.* The first sentence is [**FrJ86**, Cor. 22.13.4]$_2$, form [**Se68**, Lem. 3, IV-23] which also has as an exercise that the same statement and proof applies to $\mathrm{SL}_d(\mathbb{Z}/\ell)$. Below we augment those exercises for $\ell = 2$ and 3.

The induction for $\ell > 3$*:* First, we trim the treatment of [**FrJ86**, Cor. 22.13.4]$_2$. As in the proof of Lem. 3.1, use A and B from (6.24). Following [**FrJ86**, p. 532]$_2$, add $C = \left(\begin{smallmatrix} 1 & -1 \\ 1 & -1 \end{smallmatrix}\right)$ to give three independent generators of $\mathrm{Ad}_3(\mathbb{Z}/\ell)$, all with square 0: every $u \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$ is a sum of square 0 elements.

Our induction hypothesis is that $H \le \mathrm{SL}_2(\mathbb{Z}/\ell^{k+1}) \to \mathrm{SL}_2(\mathbb{Z}/\ell^k)$ maps surjectively. We have only to show, for $u \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$, there is $h \in H$ of form $1+\ell^k u$. For getting this, the induction assumption gives $h_0 \in H$ and $v \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$ with $h_0 = 1+u\ell^{k-1}+v\ell^k$ for some $v \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$. Here are the remaining steps.

(6.25a) Binomially expand $h = (h_0)^\ell$ to see it is $1+u\ell^k \mod \ell^{k+1}$ unless $k = 1$ when it is $1+u\ell+\ell(u+v\ell)^2(\bullet)+(u+v\ell)^\ell$ with $\bullet \in \mathbb{Z}$.

(6.25b) If $u^2 = 0$ (and $k = 1$), the result is $1+\ell u \mod \ell^2$, if $(u+v\ell)^\ell \equiv 0 \mod \ell^2$. For $\ell > 3$ this is clearly so (see Rem. 3.3).

(6.25c) Write $u \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$ as a sum of squares $u = \sum_{i=1}^t u_i$. From (6.25b) find $h_i \in H$ with $h_i = 1+u_i\ell$, so that $\prod_{i=1}^t h_i = 1+u\ell \mod \ell^2$.

Then, (6.25c) concludes the induction argument, for the first sentence.

The cohomology for $\ell = 3$: 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. Then, $\mu \in H^2(\mathrm{SL}_2(\mathbb{Z}/3), \mathrm{Ad}_3(\mathbb{Z}/3))$ defines the cohomology class of this extension ([**Nor62**, p. 241] as in (3.27)).

For any cohomology group, $H^*(G, M)$, with M a $\mathbb{Z}/\ell[G]$ module, restrict to an ℓ-Sylow $P_\ell \le G$. This gives an isomorphism onto the G invariant elements of $H^*(P_\ell, M)$ [**Br82**, III. Prop. 10.4]: see Rem 1.25. So, 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 $A = \left(\begin{smallmatrix} 1 & -3 \\ 1 & -2 \end{smallmatrix}\right)$ – generates a 3-Sylow. (In Ch. 5 §3 we have reason to use a different element, $A^* = \left(\begin{smallmatrix} 0 & -1 \\ 1 & -1 \end{smallmatrix}\right)$.)

Conclude that 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

$$\ker(\mathrm{SL}_2(\mathbb{Z}/3^2) \to \mathrm{SL}_2(\mathbb{Z}/3)) = \mathrm{Ad}_3(\mathbb{Z}/3)$$

is an element of order 3^2 in the Frattini cover

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

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 $\mathrm{SL}_2(\mathbb{Z}/3^{k+2}) \to \mathrm{SL}_2(\mathbb{Z}/3^2)$, $k \ge 0$, is Frattini. Take $v \in \ker(\mathrm{SL}_2(\mathbb{Z}/3^2) \to \mathrm{SL}_2(\mathbb{Z}/3))$.

For $\tilde{v} \in \ker(\mathrm{SL}_2(\mathbb{Z}/3^3) \to \mathrm{SL}_2(\mathbb{Z}/3))$ lifting v, $\tilde{v}^3$ identifies with v, but in $\ker(\mathrm{SL}_2(\mathbb{Z}/3^3) \to \mathrm{SL}_2(\mathbb{Z}/3^2))$. 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 higher level to exploit the free-abelianness of $\ker(\mathrm{SL}_2(\mathbb{Z}/2^k) \to \mathrm{SL}_2(\mathbb{Z}/2^3))$, $k \ge 3$. [**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.

Using $\mathrm{SL}_2(\mathbb{Z}_\ell) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$ is Frattini: As the composite of two Frattini covers, ${}_\ell\alpha \circ {}_\ell\tilde{\alpha}$ is also a Frattini cover. Finally, at least for $\ell > 3$, the Frattininess of $\mathrm{PSL}_2(\mathbb{Z}_\ell) \to \mathrm{PSL}_2(\mathbb{Z}/\ell)$ is the converse statement: If $\psi : H \to G$ is Frattini, and ψ factors through H_1, then both $H \to H_1$ and $H_1 \to G$ are Frattini.

The eventually Frattini comment follows from Rem. 4.7. The last sentence follows from Rem. 1.27.

Remark 3.3 (Simpleness vs Frattininess for $\mathrm{SL}_2(\mathbb{Z}_\ell)$). It is well-known that the values of $\ell > 3$ used in Prop. 3.2 coincide with the values for which $\mathrm{PSL}_2(\mathbb{Z}/\ell)$

is simple, say, [**Ar91**, p. 296].[14] In (6.25b), the condition $\ell > 3$ arises from the necessity of the equation

$$(u+v\ell)^\ell \equiv ((u+v\ell)^2)^2(u+v\ell)^{\ell-4} \equiv 0 \mod \ell^2,$$

for $u \in \mathrm{Ad}_3(\mathbb{Z}/\ell)$ whose square is 0. Simpleness is not directly related.

3.2. Modular curves vs MTs. Starting with the case ℓ is odd, we follow the braid action in going from

$$\{\mathrm{Ni}^\dagger_{\ell^{k+1},1} \stackrel{\mathrm{def}}{=} \mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\dagger,\mathrm{rd}}\}_{k=0}^\infty \text{ to}$$
$$\{\mathrm{Ni}^\dagger_{\ell^{k+1},2} \stackrel{\mathrm{def}}{=} \mathrm{Ni}(\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/2, \mathbf{C}_{2^4})^{\dagger,\mathrm{rd}}\}_{k=0}^\infty$$

with a † superscript indicating inner or absolute classes.

§3.3.3 has the case $\ell = 2$, the type-2 special case of the general idea of how we handle the primes ℓ that aren't perfect. Again, this is an example of the **MT** approach to the **OIT**, taking on, in this case, the hardest special prime.

$\mu^{\mathrm{abs,rd}}_{\ell,1}$ and $\mu^{\mathrm{in,rd}}_{\ell,1}$ for ℓ odd: In each case of Table 1, the left system maps to the right as a system of moduli spaces; each term is given by a one-one map on the underlying covers of $\mathbb{P}^1_j$, whose points represent moduli. This is compatible with the corresponding maps on their respective stack structures (as in §4.3.2; the reduced spaces don't have fine moduli).

TABLE 1. Dihedral Nielsen classes $\Longrightarrow$ Modular Curves

$$\{\overline{\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})}^{\,\mathrm{abs,rd}}\}_{k\ge 0} \to \mathbb{P}^1_j \quad \stackrel{\mu^{\mathrm{abs,rd}}_{\ell,1}}{\Longrightarrow} \quad \mathcal{X}_{0,\ell} \to \mathbb{P}^1_j$$

$$\{\overline{\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})}^{\,\mathrm{in,rd}}\}_{k\ge 0} \to \mathbb{P}^1_j \quad \stackrel{\mu^{\mathrm{in,rd}}_{\ell,1}}{\Longrightarrow} \quad \mathcal{X}_{1,\ell} \to \mathbb{P}^1_j$$

$$\{\overline{\mathcal{H}((\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/2, \mathbf{C}_{2^4})}^{\,\mathrm{in,rd}}\}_{k\ge 0} \to \mathbb{P}^1_j \quad \stackrel{\mu^{\mathrm{in,rd}}_{\ell,2}}{\Longrightarrow} \quad \mathcal{Y}_\ell \to \mathbb{P}^1_j$$

We attend to $\mu^{\mathrm{abs,rd}}_{\ell,1}$ and $\mu^{\mathrm{in,rd}}_{\ell,1}$ with ℓ odd here, to $\ell = 2$ in §3.3.3 and to the more intricate $\mu^{\mathrm{in,rd}}_{\ell,2}$ in Table 1 – Jacobian Nielsen class – in §3.3.

3.2.1. *The absolute case.* The permutation representation of $D_{\ell^{k+1}}$ is given by the action on $\langle \left(\begin{smallmatrix} -1 & 0 \\ 1 & 0 \end{smallmatrix}\right) \rangle \stackrel{\mathrm{def}}{=} H$ cosets. A conjugate $m^{-1}\left(\begin{smallmatrix} -1 & 0 \\ 1 & 0 \end{smallmatrix}\right)m$ fixes only the coset Hm. Given the four branch points $\boldsymbol{z}_f$, and a set of classical generators (as in §2.2), a cover $f : W \to \mathbb{P}^1_z$ in the Nielsen class $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\mathrm{abs}}$ gets assigned particular branch cycles in $S_{\ell^{k+1}}$

$$\text{having cycle type } (2)\cdots(2)(1)\text{: (2) repeats } \frac{\ell^{k+1}-1}{2} \text{ times.}$$

Its genus, $\mathbf{g}_f$ is given by

$$2(\ell^{k+1}+\mathbf{g}_f-1) = 4(\frac{\ell^{k+1}-1}{2}), \text{ or } \mathbf{g}_f = 0.$$

[14]For reasons unknown [**Ar91**, Thm. 8.3] left out $\ell = 5$, for which we have the well-known equality $\mathrm{PSL}_2(\mathbb{Z}/5) = A_5$ used, say, in §1.6.

Similarly, compute the genus of the Galois closure cover $\mathbf{g}_{\hat{f}}$ from

$$2(2\ell^{k+1}+\mathbf{g}_{\hat{f}}-1) = 4(\ell^{k+1}) \text{ or } \mathbf{g}_{\hat{f}} = 1.$$

Such a cover represents $\boldsymbol{p}_f \in \mathcal{H}(D_\ell, \mathbf{C}_{2^4})^{\rm abs}$. As in, §3.2, we can braid all those outer automorphisms; both Hurwitz spaces are irreducible.

The Galois closure of f corresponds to a point $\hat{\boldsymbol{p}}_f \in \mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm in}$ lying over $\boldsymbol{p}_f$. Then, a cover $\hat{f} : \hat{W} \to \mathbb{P}^1_z$, identified with any component of the fiber product ℓ^{k+1}-times of f – as constructed in §2.1, represents $\hat{\boldsymbol{p}}_f$. A copy of $D_{\ell^{k+1}}$ identifies with its automorphism group, up to conjugation by $D_{\ell^{k+1}}$. The normalizer, $N_{S_{\ell^{k+1}}}(D_{\ell^{k|np1}})$ of $D_{\ell^{k+1}}$ in $S_{\ell^{k+1}}$, gives a listing of points of $\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm in}$ over $\boldsymbol{p}_f$. Here is why.

Pick a component $\hat{W}$ (in notation of (1.20)). You find $D_{\ell^{k+1}}$, as a subgroup of the symmetric group, preserves it. Any other component is given by conjugation of this one by some $g \in S_{\ell^{k+1}}$. As in Lem. 2.1, that component is the same as $\hat{W}$, if and only if g conjugates the copy of $D_{\ell^{k+1}}$ into itself; equivalently, $g \in N_{S_{\ell^{k+1}}}(D_{\ell^{k+1}}$.

Further, this component represents an element of $\mathrm{Ni}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm in}$ if and only if $g \in D_{\ell^{k+1}}$. That is why the natural map from the inner to the absolute space, $\mathcal{H}^{\rm in}_{\ell^{k+1}} \to \mathcal{H}^{\rm abs}_{\ell^{k+1}}$, over any one component, $\mathcal{H}'$ of the absolute space, consists of a union of Galois covers $\mathcal{H}'' \to \mathcal{H}'$, with the group of this cover identified with a subgroup of the quotient $N_{S_{\ell^{k+1}}}(D_{\ell^{k+1}})/D_{\ell^{k+1}}$: as in Spaces III Prop. 3.5. In this example, though, there is only one inner component, again according to §3.2.

3.2.2. *The traditional* $X_0(\ell^{k+1})$. Denote $X_0(\ell^{k+1})$ minus its cusps (points over $j = \infty$) by $X_0(\ell^{k+1})'$. A point of it is an equivalence class of an elliptic curve $E_{j'}$, together with a subgroup $C_{\ell^{k+1}}$ isomorphic to $\mathbb{Z}/\ell^{k+1}$ on $E_{j'}$. Here j' will be the equivalence class modulo $\mathrm{PSL}_2(\mathbb{C})$ of the collection $\boldsymbol{z}_f$. Take $E_{j'}$ to be the Picard group, $\mathrm{Pic}(\tilde{W}_f)_0$, of degree 0 divisor classes on $\tilde{W}_f$. Then, $D_{\ell^{k+1}}$ acts on $E_{j'}$.

The normalizer, $N_{S_\ell}(D_\ell) = \mathbb{Z}/\ell^{k+1} \times^s (\mathbb{Z}/\ell^{k+1})^*$ has the same ℓ-Sylow as does $D_{\ell^{k+1}}$. Take $C_{\ell^{k+1}}$ to be the group generated by translations of the origin induced by the ℓ-Sylow. Then, $\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm abs} \to X_0'(\ell^{k+1})$

$$\text{is given by } f : W \to \mathbb{P}^1_z \mapsto (E_{j'}, C_{\ell^{k+1}}). \tag{6.26}$$

This map factors through the action of $\mathrm{PSL}_2(\mathbb{C})$ on the Hurwitz space since that action doesn't affect the Galois closure cover.

To see this induced map is one-one from $\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm abs,rd}$ to $X_0(\ell^{k+1})'$, complete the map to $\mathbb{P}^1_j$, from the projective normalization of $\mathcal{H}(D_{\ell^{k+1}}, \mathbf{C}_{2^4})^{\rm abs,rd}$. Then use (1.24) for the cover degree. Or, we can reverse

$$\boldsymbol{p}_f \in \mathcal{H}(D_\ell, \mathbf{C}_{2^4})^{\rm abs,rd} \mapsto (E_{j'}, C_{\ell^{k+1}}) \text{ in (6.26) by forming the diagram}$$

$$\begin{array}{ccc} E_{j'} & \xrightarrow{\text{degree } \ell \text{ isogeny}} & E_{j'}/C_{\ell^{k+1}} \\ \mod\langle\pm1\rangle \big\downarrow & & \mod\langle\pm1\rangle \big\downarrow \\ \mathbb{P}^1_w & \xrightarrow{\text{degree } \ell \text{ rational function } f} & \mathbb{P}^1_z \end{array} \tag{6.27}$$

REMARK 3.4. Using the degree of the covers over the j-line can also be done by summing the cusp widths cusps (over $j=\infty$) as in Thm. 2.13, from (2.31b). For example: with $k=0$, the degree of $\overline{\mathcal{H}(D_\ell, \mathbf{C}_{2^4})}^{\,\text{abs,rd}} \to \mathbb{P}^1_j$ is ℓ+1: the sum of the widths of an **HM** cusp and its shift (resp. ℓ and 1). In that counting, these are the q_2 orbits on reduced Nielsen classes of

$$\begin{aligned} \boldsymbol{g}_{\mathbf{HM}} &= (\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a\\ 0 & 1\end{smallmatrix}\right)), \text{ and} \\ (\boldsymbol{g}_{\mathbf{HM}})\mathbf{sh} &= (\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)). \end{aligned}$$

One problem, though, for general k, is that the cusp widths are not a well-known computation for $X_0(\mathbb{Z}/\ell^{k+1})$.

3.2.3. *Adjustment from absolute to inner.* The adjustment to handle $\mu^{\text{in,rd}}_{\ell,1}$ requires only replacing the subgroup C_ℓ on the elliptic curve $E_{j'}$, with a generator e' of C_ℓ in the classical description of $X_1(\mathbb{Z}/\ell^{k+1})$. Then, the natural map $\mathcal{H}(D_\ell, \mathbf{C}_{2^4})^{\text{in}} \to X_1'(\ell)$ is given by $\hat{f}: \hat{W} \to \mathbb{P}^1_z \mapsto (E_{j'}, e')$.

The equivalence on the right $(E_{j'}, e') \sim (E_{j'}, -e')$ is matched by inner equivalence on the left, conjugation by $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$. As in (2.31e), the whole inner Nielsen class is the braid orbit of an **HM** rep.

REMARK 3.5 (Fine moduli to not fine *reduced* moduli). The center of $D_{\ell^{k+1}}$ is trivial, as in Thm. 1.7. So, the inner and absolute D_ℓ Hurwitz spaces have fine moduli. Over $z' \in \boldsymbol{z}_f$, there is a unique unramified point $w_{z'} \in W_f$. The Klein 4-group, $K_{\boldsymbol{z}_f} < \mathrm{PSL}_2(\mathbb{C})$ preserving $\boldsymbol{z}_f$, gives an absolute equivalence of f with itself, as a cover of $\mathbb{P}^1_z$. Since $\mathcal{Q}''$ acts trivially on inner Nielsen classes, each $q \in \mathcal{Q}''$ extends to an equivalence of $\hat{f}$ with itself. That is, $\mathcal{Q}''$ acting trivially on Nielsen classes in §3.2. Those equivalences are transitive on the collection $\{w_{z'}\}_{z' \in \boldsymbol{z}_f}$.

3.3. Modular curves and MTs: Jacobian case.

3.3.1. *Jacobian Nielsen class in Serre's case.* We now find the lift invariant is a replacement for the traditional role of the *Weil pairing*, following Ch. 4 §4.3 in considering the braid action on $\mathrm{Ni}_{\ell^{k+1},2}$.

ℓ is odd: Consider these 4-tuples

$$A_{\ell^{k+1}} \stackrel{\text{def}}{=} \{\boldsymbol{a} = (a_1, \dots, a_4) \in (\mathbb{Z}/\ell^{k+1})^4 \mid$$
$$a_1 - a_2 + a_3 + a_4 \equiv 0 \mod \ell^{k+1}, \langle a_i - a_j, 1 \le i < j \le 4\rangle = \mathbb{Z}/\ell^{k+1}\}.$$

Associate to $\boldsymbol{g}_{\boldsymbol{a}} \in \mathrm{Ni}_{\ell^{k+1},1}$ the element $\boldsymbol{a} = (a_1, \dots, a_4)$ given by

$$\left(\left(\begin{smallmatrix}-1 & a_1\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a_2\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a_3\\ 0 & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}-1 & a_4\\ 0 & 1\end{smallmatrix}\right)\right) \text{ as in Ex. 2.7.} \tag{6.28}$$

Then, it makes sense to denote elements in $\mathrm{Ni}_{\ell^{k+1},2}$ by $\boldsymbol{g}_{\boldsymbol{a},\boldsymbol{a}'}$ by substituting (a_i, a_i') for a_i, $i = 1, \dots, 4$, in (6.28).

The Nielsen class $\mathrm{Ni}_{\ell^{k+1},1}$ has one braid orbit (§3.2). The action of H_4 on $\mathrm{Ni}_{\ell^{k+1},2}$ extends its action on $\mathrm{Ni}_{\ell^{k+1},1}$, to compute braid orbits on $\mathrm{Ni}_{\ell^{k+1},2}$ we may choose any one allowable $\boldsymbol{a}$, and check possibilities for $\boldsymbol{a}'$ that go with it. Start where $\boldsymbol{a}$ corresponds to the shift of an **HM** rep. $\boldsymbol{a}_{\mathbf{sh}} = (0, a, a, 0)$ with $a \in (\mathbb{Z}/\ell^{k+1})^*$. The only condition not obviously satisfied is generation.

LEMMA 3.6. *Substitute $\boldsymbol{g}_{\boldsymbol{a},\boldsymbol{a}'}$ in $\boldsymbol{g}_{\boldsymbol{a}}$, or (a_i, a_i') for a_i, $1 \le i \le 4$, to represent a class in $\mathrm{Ni}^{\mathrm{in}}_{\ell^{k+1},2}$ modulo these conditions:*

(6.29a) $(a_1, a_1') = \mathbf{0}$ *and* $\sum_{i=2}^{4}(-1)^i(a_i, a_i') \equiv \mathbf{0} \mod \ell^{k+1}$;

(6.29b) $\{(a_i, a_i') \mod \ell \mid 2 \le i \le 4\}$ *aren't all on a line through* $\mathbf{0}$.

Starting with $\boldsymbol{a}_{\mathbf{sh}}$, the allowable $\boldsymbol{a}'$, up to inner equivalence, have the form

$$\{(0, a_2', a_3', a_3' - a_2')\} \text{ with } a_3' - a_2' \not\equiv 0 \mod \ell.$$

PROOF. For the 1st item of (6.29a), replace the original element by the inner equivalent representative by conjugating by $\left(\begin{smallmatrix} 1 & (a_1/2, a_1'/2) \\ 0 & 1 \end{smallmatrix}\right)$. Since

$$\left(\begin{smallmatrix} 1 & -(a_1/2, a_1'/2) \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} -1 & (a, a') \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & (a_1/2, a_1'/2) \\ 0 & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} -1 & (a - a_1, a' - a_1') \\ 0 & 1 \end{smallmatrix}\right)$$

we may assume $(a_1, a_1') = \mathbf{0}$. Complete (6.29a) from product-one (1.23c).

Recognize (6.29b) as equivalent to entries of $\boldsymbol{g}_{\boldsymbol{a},\boldsymbol{a}'}$ generate $(\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/2$. Given that the first entry is now $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, this says

$$\langle (a_i, a_i'), i = 2, 3, 4 \rangle = (\mathbb{Z}/\ell^{k+1})^2 \stackrel{\mathrm{def}}{=} E_k.$$

Since E_k is a Frattini cover of E_1, this is equivalent to showing that the image of $\langle (a_i, a_i'), i = 2, 3, 4 \rangle$ is all of E_1. For this it suffices in the two dimensional space E_1 that the hoped for generators aren't all on one line (through the origin).

Now consider the allowable $\boldsymbol{a}'$ that go with $\boldsymbol{a}_{\mathbf{sh}}$. Having the 4th entry nonzero mod ℓ is necessary and sufficient for the second line condition of (6.29), while the first line is automatic from its form. □

3.3.2. *Values of the lift invariant.* Now we show values of the lift invariant to the small Heisenberg group separate braid orbits on $\mathrm{Ni}_{\ell^{k+1},2}$. Indirectly, this accounts for the constants that come from $\mathbb{Q}(e^{2\pi i/\ell^{k+1}})$ traditionally arising from the *Weil pairing*. These now interpret as values of a Nielsen class lift invariant.

There is no lift invariant for the Nielsen classes with $D_{\ell^{k+1}}$ and ℓ odd. Yet, there is one for $G_{\ell^{k+1}} = (\mathbb{Z}/\ell^{k+1})^2 \times^s \mathbb{Z}/2, k \ge 0$. It comes from the small Heisenberg group, as in Ch. 5 §3, except the external semidirect product comes from $\mathbb{Z}/2$ rather than $\mathbb{Z}/3$ (as in Ch. 5).

So, $\mathrm{Ni}(\mathbb{H}(\mathbb{Z}/\ell)\times^s\mathbb{Z}/2,\mathbf{C}_{2^4})$ elements are 4-tuples with entries of form

$$\left(\begin{smallmatrix}-1 & M(a,a',z)\\ 0 & 1\end{smallmatrix}\right) \text{ with } \left\{M(x,y,z)\stackrel{\text{def}}{=}\begin{pmatrix}1 & a & z\\ 0 & 1 & a'\\ 0 & 0 & 1\end{pmatrix}, a,a',z\in\mathbb{Z}/\ell^{k+1}\right\}.$$

Precisely, following Lem. 3.6, $\boldsymbol{a}_{\mathbf{sh}}=\boldsymbol{a}$ as above,

$$\text{with } \boldsymbol{a}' \text{ given by } (0,a_2',a_3',a_3'-a_2'), \text{ with } a_3'-a_2'\neq 0.$$

Write the action of the $\mathbb{Z}/2$ on $M(a,a',z)$ as $-1*M(a,a',z)=M(-a,-a',z)$; trivial action on z comporting with

$$\mathbb{H}(\mathbb{Z}/\ell)\times^s\mathbb{Z}/2\to(\mathbb{Z}/\ell)^2\times^s\mathbb{Z}/2 \text{ is a central extension.}$$

PROPOSITION 3.7. *An element* $\left(\begin{smallmatrix}-1 & M(x,x',z)\\ 0 & 1\end{smallmatrix}\right)$ *in* $\mathbb{H}(\mathbb{Z}/\ell^{k+1})\times^s\mathbb{Z}/2$ *has order 2 if and only if* $z=\frac{xx'}{2}$.

The lift invariant of $\boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'}$ *(as above) is* $\frac{a(a_3'-a_2')}{2}\neq 0$. *It has* $|(\mathbb{Z}/\ell^{k+1})^*|$ *values , running over all elements in* $\mathrm{Ni}_{\ell^{k+1},2}$. *In particular:*

(6.30a) *all braid orbits are separated by their lift invariant values;*

(6.30b) *their corresponding inner Hurwitz space components are conjugate by the action of* $G(\mathbb{Q}(e^{2\pi i/\ell^{k+1}})/\mathbb{Q})$*;*

(6.30c) *The normalizer of* G_{ℓ^k+1} *in* S_{ℓ^2}, $N_{S_{\ell^2}}(G_{\ell^k+1})$ *is* $\mathrm{GL}_2(\mathbb{Z}/\ell)$*;*

(6.30d) *the geometric (resp. arithmetic) monodromy group of any* $\mathrm{Ni}^{\mathrm{in}}_{\ell^{k+1},2}$ *component over* $\mathbb{P}^1_j$ *is* $\mathrm{SL}_2(\mathbb{Z}/\ell^{k+1})/\langle\pm1\rangle$ *(resp.* $\mathrm{GL}_2(\mathbb{Z}/\ell^{k+1})/\langle\pm1\rangle$*).*

PROOF. An order 2 lift of $\left(\begin{smallmatrix}-1 & (x,x')\\ 0 & 1\end{smallmatrix}\right)$ to $\mathbb{H}(\mathbb{Z}/\ell^{k+1})\times^s\mathbb{Z}/2$ satisfies

$$\left(\begin{smallmatrix}-1 & M(x,x',z)\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & M(x,x',z)\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1 & (-1)*M(x,x',z)M(x,x',z)\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix}1 & M(0,0,0)\\ 0 & 1\end{smallmatrix}\right).$$

Directly calculate that $(-1)*M(x,x',z)M(x,x',z)$ has upper right entry $2z-xx'$, or $z=\frac{xx'}{2}$ as stated in the lemma.

Now compute the lift invariant of $\boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'}$, by taking the product of the order 2 lifts of its entries to $\mathbb{H}(\mathbb{Z}/\ell^{k+1})\times^s\mathbb{Z}/2$. That calculation amounts to checking the upper right entry of the following product:

$$\left(\begin{smallmatrix}-1 & M(0,0,0)\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & M(a,a_2',\frac{aa_2'}{2})\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & M(a,a_3',\frac{aa_3'}{2})\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}-1 & M(0,a_3'-a_2',0\\ 0 & 1\end{smallmatrix}\right).$$

Multiply the first two matrices, then and the last two matrices, to get

$$\left(\begin{smallmatrix}1 & M(-a,-a_2',\frac{aa_2'}{2})\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & M(a,a_2'\frac{aa_3'}{2})\\ 0 & 1\end{smallmatrix}\right).$$

Conclude the upper right entry of $M(a,a_2',\frac{aa_3'}{2})M(-a,-a_2',\frac{aa_2'}{2})$, the lift invariant value, is $\frac{a(a_3'-a_2')}{2}\neq 0$, an element in $(\mathbb{Z}/\ell^{k+1})^*$ according to the conditions of Lem. 3.6. From (3.10a), the lift invariant is a braid invariant, preserved by the action of H_4 on $\boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'}$.

Regard $V_k=(\mathbb{Z}/\ell^{k+1})^2$ as both the letters of a permutation representation and as a subgroup of $S_{(\mathbb{Z}/\ell^{k+1})^2}$ The automorphisms of V_k are given by $\mathrm{GL}_2(\mathbb{Z}/\ell^{k+1})$

which we can now regard as a subgroup of the symmetric group. The copy of $\mathbb{Z}/2$ in $V_k \times^s \mathbb{Z}/2$ is in its center, generated by minus the identity matrix.

An element of $\mathrm{GL}_2(\mathbb{Z}/\ell^{k+1})$ acting by conjugation on Nielsen classes is therefore determined by what it does to $(\boldsymbol{a}, \boldsymbol{a}')$. By the conditions, this is determined by what it does to the pair $(a, a'_2), (a, a'_3)$ since that linearly determines what it does to $(0, a'_3 - a'_2)$. The same holds for any braid q acting on reduced inner Nielsen classes. Therefore, all braid element actions are given by conjugations by $\mathrm{GL}_2(\mathbb{Z}/\ell^{k+1})$.

It remains to braid conjugation by elements of $\mathrm{SL}_2(\mathbb{Z}/\ell)$ (as in Def. 3.7). To see that action, there are two calculations figured by what the generators of H_4 do to the 2nd and 3rd entries of $\boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'}$, after the result has been normalized to have $\left(\begin{smallmatrix} -1 & (0,0) \\ 0 & 1 \end{smallmatrix}\right)$ in the first entry, and product one determining the 4th entry:

$$
\begin{aligned}
\mathbf{sh} : \boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'} \to \quad & \left(\bullet, \left(\begin{smallmatrix} -1 & (0,a'_3-a'_2) \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & (-a,a'_3-2a'_2) \\ 0 & 1 \end{smallmatrix}\right), \bullet\right) \\
q_2 : \boldsymbol{g}_{\boldsymbol{a}_{\mathbf{sh}},\boldsymbol{a}'} \to \quad & \left(\bullet, \left(\begin{smallmatrix} -1 & 2(a,a'_2)-(-a,-a'_3) \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} -1 & (a,a'_2) \\ 0 & 1 \end{smallmatrix}\right), \bullet\right).
\end{aligned} \tag{6.31}
$$

That is, $\mathbf{sh}$ is represented by $\left(\begin{smallmatrix} -1 & -2 \\ 1 & 1 \end{smallmatrix}\right)$ and q_2 is represented by $\left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. The square of $\left(\begin{smallmatrix} -1 & -2 \\ 1 & 1 \end{smallmatrix}\right)$ is $-I_2$, whose effect is inner equivalent to I_2 by conjugating $\boldsymbol{g}_{\boldsymbol{a},\boldsymbol{a}'}$ by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Multiply $q_1 q_2 q_1 = q_2 q_1 q_2$ by q_2^{-1} to get $q_1 q_2$. That acts as

$$
\left(\begin{smallmatrix} -1 & -2 \\ 1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 2 & 1 \\ -1 & 0 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} -2 & -3 \\ 1 & 1 \end{smallmatrix}\right).
$$

Check this has order 3. Therefore elements of respective order 3 and 2, independent of ℓ, represent the actions of γ_0 and $\mathbf{sh}$.

So, they give generators for $\mathrm{PSL}_2(\mathbb{Z})$, as expected. Now, combine the PSL_2 action with conjugations on the inner braid components from the action of (6.30b) from the lift invariant. Ch. 3 Prop. 2.19 then gives the full action of $\mathrm{GL}_2(\mathbb{Z}/\ell)/\langle \pm 1 \rangle$. That concludes the proof. □

3.3.3. *What happens if $\ell = 2$.* The phrasing, say of [**BFr02**, §1.1], only referred to D_ℓ (or $(\mathbb{Z}/\ell)^2 \times^s \mathbb{Z}/2$), for ℓ odd, because we assumed G is ℓ-perfect. We amend this to include all ℓ, a special case of our *folding under* the Ext-Frattini covers of Prop. 2.6. By not having considered the prime 2 divisor of D_ℓ, when ℓ is odd, we are following the type-1 paradigm in case RETURNM. Now we are following the type-2 paradigm.

At level $k = 0$ for $\ell = 2$, there are these tiny groups:

(6.32a) For $X_0(\mathbb{Z}/2)$, D_2 (a Klein 4-group); and

(6.32b) for $X(\mathbb{Z}/2)$, $(\mathbb{Z}/2)^2 \times^s \mathbb{Z}/2$.

4. Proof of the Upper half-plane Paradigm

4.1. Proof of Thm. 2.7.

4.2. Proof of Thm. 2.14. [**BFr02**, §2.6] takes a completely cohomological approach to the properties listed in (2.28). We give an example.

[**BFr02**, §2.6.4] works on the complements of $\mathcal{Q}''$ (a Klein 4-group, and therefore abelian according to Prop. 2.10) in M_4. This starts with seeing directly one splitting by the group $\Gamma_1' = \langle q_1\langle\tilde{z}\rangle, q_2\langle\tilde{z}\rangle\rangle$. As in Def. 1.7, splittings correspond to elements of $H^1(\Gamma_1', \mathcal{Q}'')$. Conclude (2.28d) if this cohomology group has order 2.

Let B be the largest elementary abelian 2-group quotient of the rank 2 free group $\mathrm{Cen}_{\Gamma_1'}(\mathcal{Q}'')$. Then B and $\mathcal{Q}''$ are isomorphic as $\mathbb{F}_2\left[\Gamma_1'\right]$ modules. For any group G with normal subgroup H acting on a module M, there is an exact sequence [**AW67**, p. 100]:

$$0 \to H^1(G/H, M^H) \xrightarrow{\inf} H^1(G, M) \xrightarrow{\mathrm{res}} H^1(H, M)^G \to H^2(G/H, M^H). \tag{6.33}$$

Apply this with $M = \mathcal{Q}''$, $G = \Gamma_1'$ and $H = \mathrm{Cen}_{\Gamma_1'}(\mathcal{Q}'')$, so $G/H = S_3$. Restrict to a 2-Sylow P_2 of S_3. Restriction of an element from $H^*(G, A)$ to $H^*(P, A)$ is injective if P is the p-Sylow of G [**AW67**, p. 105] (more precisely in the footnote near the beginning of §1.4). Therefore, if $H^*(P_2, M^H)$ is trivial, so is $H^*(G/H, M^H)$.

The action of P_2 on $\mathcal{Q}''$ is the regular representation on two copies of P_2, so $\mathcal{Q}''$ is a free P_2 module and the cohomology groups $H^1(G, M)$ and $H^2(G, M)$ are trivial. Conclude: $H^1(\Gamma_1', \mathcal{Q}'') = \mathrm{Hom}(B, \mathcal{Q}'')^{S_3} = \mathbb{Z}/2$.

Those two conjugacy classes of subgroups of M_4 that are isomorphic to PSL2($\mathbb{Z}$) are joined by the relation $q_1 q_3^{-1} = 1$.

4.2.1. *A presentation of M_r.* §2.2 defines the mapping class group M_r as the image group of H_r acting on the Nielsen class $\mathrm{Ni}(\bar{G}_r, \mathbf{C}_{\bar{\boldsymbol{g}}})^{\mathrm{in}}$. This is given by the action by the braids $Q_1, \ldots, Q_{r-1}$ modulo the action by inner automorphisms, $\mathrm{Inn}(\bar{G}_r)$, of $\bar{G}_r$. mapping $\bar{g}_1, \ldots, \bar{g}_r$ to permutations of their conjugates. This maps B_r (relations given by (2.13)) to M_r factoring through H_r.

Further, M_r is the quotient of B_r by the relations (6.34):

$$\begin{array}{l} \tau_1(r) = (Q_{r-1}Q_{r-2}\cdots Q_2)^{r-1}, \tau_2(r) = Q_1^{-2}(Q_{r-1}\cdots Q_3)^{r-2}, \ldots, \\ \tau_{\ell+1}(r) = (Q_\ell \cdots Q_1)^{-\ell-1}(Q_{r-1}\cdots Q_{\ell+2})^{r-\ell-1}, \ldots, \\ \tau_{r-1}(r) = (Q_{r-2}\cdots Q_1)^{1-r}, \text{and } \tau(r) = (Q_{r-1}\cdots Q_1)^r. \end{array} \tag{6.34}$$

This complicated presentation, from [**KMS66**, §3.7] or [**Ma34**], is oblivious to the map $H_r \to M_r$ dominating this paper. Using it conceptualizes $N_r = \ker(B_r \to M_r)$. The switch of emphasis shows in Prop. 2.9.

With $Q_1Q_2\cdots Q_{r-1}^2\cdots Q_2Q_1 = R_1$, consider these additional elements:

$$R_2 = Q_1^{-1}R_1Q_1, \ldots, R_r = Q_{r-1}^{-1}R_1Q_{r-1} \text{ and } (Q_1Q_2\cdots Q_{r-1})^r. \tag{6.35}$$

The relation between the maps $B_r \to H_r$ and $B_r \to M_r$ amounts to a comparison of (6.34) with (6.35). Thm. 2.14 presents both M_4 and N_4 memorably. Here our remarks comment on what the argument does for the case of general r.

Bibliography

[Ahl79] L. Ahlfors, *Introduction to the Theory of Analytic Functions of One Variable*, 3rd edition, Inter. Series in Pure and Applied Math., McGraw-Hill Complex Variable, 1979.

[A86] J.L. Alperin, *Local representation theory*, Cambridge Univ. Press, Cambridge studies in advanced mathematics **11**, 1986.

[ArE25] E. Artin, *Theorie der Zopfe*, Abh. Math. Sem. Hamburg **4** (1925), 47–72.

[ArE47] E. Artin, *Theory of braids*, Annals of Math. **48** (1947), 101–126.

[Ar91] M. Artin, *Algebra*, Prentice Hall, 1991.

[ArP03] M. Artebani and G.P. Pirola, **Algebraic functions with even monodromy**, preprint Feb. 2003.

[AsS] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Algebra **92** (1985), 44–80.

[Atlas] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups.* New York: Clarendon press, 1985.

[AW67] M.F. Atiyah and C.T.C. Wall, *Cohomology of groups*, article in Algebraic Number Theory, pp. 94–115, Thompson Book Co. and Academic Press, 1967, Editor J. W. S. Cassels.

[Ax68] J. Ax, *The elementary theory of finite field*, Annals of Math. (2) **88** (1968), 239–271.

[Axl15] S. Axler, *Linear Algebra Done Right*, Spring Undergraduate Texts in Mathematics, 3rd Edition.

[Ba75] W. Baur, *Decidability and undecidability of theories of abelian groups with predicates for subgroups*, Compositio Math. **31** (1975), 23–30.

[Be91] D. J. Benson, *Representations and cohomology, I: Basic representation theory of finite groups and associative algebras*, Cambridge studies in Advanced Mathematics, Camb. Univ. Press **30** (1991).

[BFr02] P. Bailey and M. D. Fried, *Hurwitz monodromy, spin separation and higher levels of a Modular Tower*, Arithmetic fundamental groups and noncommutative algebra, PSPUM vol. **7**0 of AMS (2002), 79–220. arXiv:math.NT/0104289 v2 16 Jun 2005.

[BiFr86] R. Biggers and ———, *Irreducibility of moduli spaces of cyclic unramified covers of genus g curves*, TAMS **295**, 59–70.

[BoDr77] V.M. Bondarenko and Yu.A. Drozd, *Representation type of finite groups*, Zap. Naucn. Sem. Leningrad (LOMI) **57** (1977), 24–41.

[B47] P. Bohnenblust, *The algebraical braid group*, Annals of Math. **48** (1947), 127–136.

[BvSh66] Z.I. Borevich and I.R. Shafarevich, *Number Theory*, Translated by N. Greenleaf, Academic Press, NY and London (1966).

[Bra45] R. Brauer, *A note on systems of homogeneous algebraic equations*, BAMS **51** (1945) 749–755.

[Br82] K.S. Brown, *Cohomology of Groups*, Graduate texts in Mathematics, Springer-Verlag, New York, Berlin, . . . , (1982).

[CaD09] A. Cadoret and P. Dèbes, *Abelian obstructions in inverse Galois theory*, Manuscripta Mathematica, 128/3 (2009), 329341.

[CasF67] *Algebraic Number Theory*, Proceedings of a conference organized by the London Math. Soc. edited by J.W.S. Cassels and A. Fröhlich 1967, Thompson Book Co.

[CaTa09] A. Cadoret and A. Tamagawa, *Uniform boundedness of p-primary torsion of Abelian Schemes*, preprint as of June 2008.

[Ch36] C. Chevalley, *Demonstration d'une hypothèse de E. Artin*, Abhundlungen aus dem Mathematischen Seminar Hamburg, **11** (1936), 73–75.

[CW06a] M. Ciperiani, *Solvable Points on Genus One Curves*, Notices AMS, **64** no. 3 (2017), 221–223.

[CW06b] ——— and A. Wiles, *Solvable Points on Genus One Curves*, Duke Math. J. **142** (2008), 381–464. MR2412044.

[Con78] J.B. Conway, *Functions of One Complex Variable*, 2nd ed., Grad. Texts in Math. **11** Springer-Verlag, NY, Heidelberg, Berlin, 1978.

[CmHa85] K. Coombes, D. Harbater. *Hurwitz families and arithmetic Galois groups*, Duke Mathematical Journal, 52 (1985), 821–839.

[CoCa99] J.-M. Couveignes and P. Cassou-Nogus, *Factorisations explicites de $g(y)?h(z)$*, Acta Arith. **87** (1999), no. 4, 291–317.

[D96] P. Dèbes, *Hilbert subsets and s-integral points*, Manuscripta Mathematica, vol. **89**, 1996, 107–137.

[DZ98] P. Dèbes and U. Zannier, *Universal Hilbert subsets*, Math. Proc. Cambridge Phi. Soc., vol. **124**, 1998, 127–134.

[DFr90] P. Dèbes and M.D. Fried, *Rigidity and real residue class fields*, Acta. Arith. **56** (1990), 13–45.

[DFr90b] ——— and ———, *Arithmetic variation of fibers in families: Hurwitz monodromy criteria for rational points on all members of the family*, Crelles J. **409** (1990), 106–137.

[CaD09] A. Cadoret and P. Dèbes, *Abelian obstructions in inverse Galois theory*, Manuscripta Mathematica, 128/3 (2009), 329341.

[CaTa09] A. Cadoret and A. Tamagawa, *Uniform boundedness of p-primary torsion of Abelian Schemes*, preprint as of June 2008.

[DFr94] P. Dèbes and M.D. Fried, *Nonrigid situations in constructive Galois theory*, Pacific Journal **163** (1994), 81–122.

[DeJL83] J. Denef, M. Jarden and D.J. Lewis, *On Ax-fields which are C_1*, The Quarterly Journal of Mathematics, Oxford, 2nd Series **34** (1983), 21–36.

[DDo97] P. Dèbes and JC Douai, *Algebraic covers: field of moduli versus field of definition*, Annales scientifiques de l'É.N.S. 4^e série, tome **30**, n^0 3 (1997), 303–338.

[DeJaL83] J. Denef, M. Jarden and D.J. Lewis, *On Ax-fields which are C_1*, The Quarterly J. of Math. Oxford. Second Series **34** (1983), 21–36.

[Fa73] J. Fay, *Theta Functions on Riemann Surfaces*, Lecture notes in Mathematics **352**, Springer Verlag, Heidelberg, 1973.

[Fr73] M.D. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Ill. J. Math. **17** (1973), 128–146.

[Fr74] M.D. Fried, *On Hilbert's irreducibility theorem*, Journal of No. Theory **6** (1974), 211–232.

[FrS76] M.D. Fried and G. Sacerdote, *Solving diophantine problems over all residue class fields of a number field ...*, Annals Math. **104** (1976), 203–233.

[Fr77] M.D. Fried, *Fields of Definition of Function Fields and Hurwitz Families and; Groups as Galois Groups*, Communications in Algebra **5** (1977), 1782.

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

[Fr80] ———, *Exposition on an Arithmetic-Group Theoretic Connection via Riemanns Existence Theorem*, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups, A.M.S. Publications **37** (1980), 571601.

[Fr85] ———, *On the Sprindzuk-Weissauer approach to universal Hilbert subsets*, Israel J. of Math. **51** (1985), 347–363.

[Fr90] , ———, *Arithmetic of 3 and 4 branch point covers: a bridge provided by noncongruence subgroups of* $\mathrm{SL}_2(\mathbb{Z})$, Progress in Math. Birkhauser **81** (1990), 77–117.

[Fr90b] M.D. Fried, *Riemanns Existence Theorem: An elementary approach to moduli*, http://www.math.uci.edu/ mfried/booklist-ret.html takes you to an introduction to the whole topic, and to each of the chapters, separately, each with its own succinct abstract. The differences: Chap. 1 is a separate description of the whole book, Chap. 4 is more complete – parts written later – in the complete manuscript; Chapters 2 and 3 have their separate html files (after chapter abstracts) giving ways to approach the chapters.

[Fr94] ———, *Enhanced review of J.-P. Serres Topics in Galois Theory, with examples illustrating braid rigidity*, Recent Developments in the Galois Problem, Cont. Math., proceedings of AMS-NSF Summer Conference, Seattle **186** (1995), 15–32. Briefer reviewTopics in Galois Theory, J.-P. Serre, 1992, Bartlett and Jones Publishers, BAMS **30** #1 (1994), 124–135. ISBN 0-86720-210-6.

[DFr94] P. Dèbes and M.D. Fried, *Nonrigid situations in constructive Galois theory*, Pacific Journal **163** (1994), 81–122.

[Fr95] ———, *Introduction to Modular Towers: Generalizing dihedral groupmodular curve connections*, Recent Developments in the Inverse Galois Problem, Cont. Math., proceedings of AMS-NSF Summer Conference 1994, Seattle **186** (1995), 111–171.

[Fr02] ———, *Moduli of relatively nilpotent extensions*, Inst. of Math. Science Analysis **1267**, June 2002, Communications in Arithmetic Fundamental Groups, 70–94. Developed from three lectures I gave at RIMS, Spring 2001.

[Fr02b] ———, *What Gauss Told Riemann about Abel's Theorem,* up on the Abel Website at the *Danish National Academy of Sciences*: presented in the Florida Mathematics History Seminar, Spring 2002, as part of John Thompson's 70th birthday celebration.

[Fr05] ———, *The place of exceptional covers among all diophantine relations*, J. Finite Fields **11** (2005) 367–433.

[Fr05b] ———, *Relating two genus 0 problems of John Thompson*, Volume for John Thompson's 70th birthday, in Progress in Galois Theory, H. Voelklein and T. Shaska editors 2005 Springer Science, 51–85.

[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. Debes), Sem. et Congres, Vol. **13** (2006), 165–233.

[Fr09] ———, *Connectedness of families of sphere covers of A_n-type*, Preprint as of June 2008.

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

[Fr12] ———, *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**, January 2012, 1–72

[Fr17] ———, *Introduction to moduli, l-adic representations and the Regular Version of the Inverse Galois Problem*, To Appear in the volume for the Chern Institute Conference on Moduli spaces and the Grothendieck Teichmuller group.

[FrGS] ———, R. Guralnick and J. Saxl, *Schur Covers and Carlitz's Conjecture*, Israel J.; Thompson Volume **82** (1993), 157–225.

[FrH15] ——— and M. van Hoeij, *The small Heisenberg group and ℓ-adic representations from Hurwitz spaces.*

[FrJ78] ——— and M. Jarden, *Diophantine properties of subfields of $\bar{\mathbb{Q}}$* Amer. J. Math. **100** (1978), 653–666.

[FrJ86] ——— and ———, *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 dEnfants, Mapping Class Groups and Moduli, vol. **243**, Cambridge U. Press, 1997, London Math. Soc. Lecture Notes, pp. 172–197.

[FrM02] ——— and A. Mezard, *Configuration spaces for wildly ramified covers*, Arithmetic fundamental groups and noncommutative algebra, PSPUM vol. of the American Math. Society (2002), 223–247.

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

[FrV92] ——— and ———, *The embedding problem over an Hilbertian-PAC field*, Annals of Math 135 (1992), 469–481.

[Gal31] E. Galois, *Mémoire sur les conditions de résolution algbrique des équations*, in Bourgne and Azra (1962), pp. 163-165,

[GRe57] H. Grauert and R. Remmert, *3 papers in Comptes Rendus de L'Academie des Science*, Paris Band **245** (1957), 819–822, 822–825, 918–921.

[GRe58] ———, *Komplex Räume*, Math. Ann. **136** (1958), 245–318.

[GS78] R. Griess and P. Schmid, *The Frattini module*, Archiv. Math. **30** (1978), 256–266.

[Gr71] A. Grothendieck, *Revêtements étale et groupes fondamental*, Lect. Notes Math., vol. **224**, Berline Heidelberg New York, Springer 1971.

[GuMS03] R. Guralnick, P. Müller and J. Saxl, *The rational function analoque of a question of Schur and exceptionality of permutations representations*, Memoirs of the AMS 162–773 (2003), **ISBN** 0065-9266.

[Ha84] D. Harbater, *Mock covers and Galois extensions*, J. Algebra **91** (1984), 281-293.

[He61] A. Heller and I. Reiner, *Indecomposable representations*, Ill. J. Math. **5** (1961), 314–323.

[H77] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Math. **52**, Springer-Verlag, 1977.

[Ih90] Y. Ihara, *Briads, Galois Groups, and some Arithmetic Functions*, Proceedings of the Int. Cong. Math., Kyoto 1990, Springer-Verlag Tokyo, 1991, 99–120.

[Ik] Ikeda, the reference is missing from $[\mathbf{FrJ86}]_2$

[JMS15] A. James, K. Magaard, and S. Shpectorov, *The lift invariant distinguishes components of Hurwitz spaces for A_5*, PAMS **143** (2015), 1377–1390.

[Is94] M. Isaacs, *Algebra, a graduate course*, Brooks/Cole (1994).

[KMS66] A. Karrass, W. Magnus and D. Solitar, *Combinatorial group theory*, Interscience Publishers, J. Wiley and Sons, 1966.

[KoMa73] A.I. Kokorin and V. I. Mart'yanov, **Universal extended theories**, Algebra, Ikutsk (1973), 107–114.

[Ko07a] J. Kollár, *Algebraic varieties over PAC fields*, Israel Journal of Mathematics, 2007, Volume **161**, Issue 1, 89–101.

[Ko07b] ———, *A conjecture of Ax and degenerations of Fano varieties*, Israel Journal of Mathematics, 2007, Volume **162**, Issue 1, 235–251.

[La52] S. Lang, *On quasi algebraic closure*, Annals of Math. **55** (1952), 373-390.

[La71] S. Lang, *Algebra*, 2nd edition, Addison-Wesley, Reading 1971.

[LO08] F. Liu and B. Osserman. *The irreducibility of certain pure-cycle Hurwtiz spaces*, American journal Math., 2008 **130** (6), 1687–1708.

[Ma34] W. Magnus, *Über Automorphismen von Fundamentalgruppen berandeter Flächen*, Math. Ann. 109, 1934, 617–646.

[MaSh19] A. Malmendier and T. Shaska, *From hyperelliptic to superelliptic curves*, preprint May 2019.

[MM99] G.Malle and B.H. Matzat, *Inverse Galois Theory*, Springer Monographs in Math., 3-540-62890-8, Springer, Berlin, 1999: My review is at BLMS 34 (2002), 109–112.

[Me90] J.F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$*, J. of Algebra **131** (1990), 483–495.

[Mu66] D. Mumford, *Introduction to Algebraic Geometry; The Red Book*, Harvard Lecture Notes, 1966.

[Mu72] ———, *An analytic construction of degenerating curves over complete local rings*, Comp. Math. **24** (1972), 129–174.

[MuFo82] ——— and J. Fogarty, *Geometric Invariant Theory*, 2nd enlarged edition, Spring-Verlag, Ergebnisse der Mathematik.

[Ne81] E. Neuenschwanden, *Studies in the history of complex function theory II: Interactions among the French school, Riemann and Weierstrass*, BAMS **5** (1981), 87–105.

[Nor62] D.G. Northcott *An introduction to homological algebra*, Cambridge Univ. Press, Great Britain, 1962.

[O61] T. Ono, *Arithmetic of algebraic tori*, Ann. Math., **74**, 1961, p. 101–139.

[Pa04] A. Pál, *Solvable points on projective algebraic curves*, Canad. J. Math. Vol. **56** (3) 612–637.

[Ri75] C.M. Ringel, *The representation type of local algebras*, Representations of algebra, Ottawa 1974. Lecture Notes in Mathematics 488, Springer, 1975.

[Rig96] L.T. Rigatelli, *Evariste Galois, 1811-1832*, Vita mathematica, **11**, Birkhuser, ISBN 3-7643-5410-0.

[Ro02] J. Rotman, *Advanced Modern Algebra*, (2002) by Pearson Education.

[Se67] J.P. Serre, *Local Class Field Theory*, 128–161 in [**CasF67**].

[Se68] J.P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill Univ. Lecture Notes, Benjamin, New York, Amsterdam, 1968, notes of W. Kuyk and J. Labute; 2nd corrected ed. (substantially the same) by A. K. Peters, Wellesley, MA, 1998.

[Se88] ———, *Letter on* Ext, Private Correspondence.

[Se90a] ———, *Relêvements dans A_n*, C. R. Acad. Sci. Paris 311 (1990), 477–482.

[Se90b] ———, *Revêtements a ramification impaire et thêta-caractèristiques*, C. R. Acad. Sci. Paris 311 (1990), 547–552.

[Se92] ———, *Topics in Galois theory*, no. ISBN #0-86720-210-6, Bartlett and Jones Publishers, notes of H. Darmon, 1992.

[Se97] ———, *Unpublished notes on an attempt to get a generic version of the* **OIT** *result for higher dimension Jacobians*, sent by Serre to Fried after Serre's 1997 Caltech lectures.

[Sch84] W. Schmidt, *The solubility of certain p-adic equations*, JNoTh **19** (1984), 63–80.

[ShT61] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its Applications in Number Theory*, Math. Soc. of Japan, 1961.

[Sh94] G. Shimura, *Introduction to the arithmetic of automorphic functions*, Publications of Math. Soc. Japan, Princeton U. Press, 2nd ed., first printing 1971 (1994).

[Sp66] E. Spanier, *Algebraic Topology*, McGraw-Hill, Higher Mathematics (1966).

[Spr81] V.G. Sprindzuk, *Diophantine equations involving unknown primes*, TRudy NIAN SSR **158** (1981), 180-196.

[Sp57] G. Springer, *Introduction to Riemann Surfaces*, 1st ed., Addison-Wesley Mathematics Series, vol. **11**, Addison-Wesley, Reading, Mass. (1957).

[St10] J. Stillwell, *Mathematics and its History*, 3rd ed., Springer Undergraduate texts in mathematics, Springer 2010.

[Th90] J.G. Thompson, $\mathrm{GL}_n(q)$*, rigidity and the braid group*, Bull. Soc. Math. Belg. **17** (1990), 723-733.

[Vi85] N. Vila, *Central extensions of A_n as Galois groups over $\mathbb{Q}$*, Arch. Math. **44** (1985), 424–437.

[Vo92] H. Völklein, $\mathrm{GL}_n(q)$ *as Galois group over the rationals*, Math. Annalen **293**, 163–76.

[Vo94] H. Völklein, *Braid group action, embedding problems and the groups* $\mathrm{PGL}(n,q)$, $\mathrm{PU}(n,q^2)$, Forum Math. **6** (1994), 513–35.

[Vo96] ———, *Groups as Galois Groups*, Cambridge Studies in Adv. Math. **53**, 1996.

[We56] A. Weil, *The field of definition of a variety*, Amer. J. Math., **78** (1956), 509–524.

[We62] ———, *Foundations of Algebraic Geometry*, A.M.S. Colloquium Publications, Vol. **XXIX**, Providence, RI, 1962.

[We61] ———, *Adeles and algebraic groups*, notes by M. Damazure and T. Ono, Birkhäuser-Boston, 1961.

[Wo64] K. Wohlfahrt, *An extension of F. Kleins level concept*, Ill. J. Math. **8** (1964), 529–535.

[Z71] O. Zariski, *Algebraic Surfaces*, 2nd Supplemented Ed. with appendices by S.S. Abhyankar, J. Lipman, D. Mumford, Spring Verlag (1971).