Algebra & Number Theory

Volume 9
2015
No. 3

Hurwitz monodromy and full number fields

David P. Roberts and Akshay Venkatesh

msp

msp

ALGEBRA AND NUMBER THEORY 9:3 (2015)
dx.doi.org/10.2140/ant.2015.9.511

Hurwitz monodromy and full number fields

David P. Roberts and Akshay Venkatesh

We give conditions for the monodromy group of a Hurwitz space over the configuration space of branch points to be the full alternating or symmetric group on the degree. Specializing the resulting coverings suggests the existence of many number fields with surprisingly little ramification — for example, the existence of infinitely many A_m or S_m number fields unramified away from $\{2, 3, 5\}$.

1. Introduction

1A. ***Overview.*** Hurwitz spaces are defined as moduli spaces of branched covers of the complex projective line P^1 satisfying certain conditions. A given Hurwitz space is canonically presented as a finite-degree covering of the configuration space of possible branching divisors. An important problem is to characterize those Hurwitz spaces for which the monodromy group of this covering is the full alternating or symmetric group on the fiber. Our main result, Theorem 5.1, gives such a characterization in an asymptotic setting when the covers of P^1 being parametrized have suitably many branch points.

Our interest in fullness of Hurwitz monodromy arises from applications to constructing number fields with large Galois group and little ramification, and in particular from an open problem posed in [Malle and Roberts 2005]: Say that a degree-m number field K is *full* if its associated Galois group is either A_m or S_m.

MSC2010: primary 14D05; secondary 20F36, 11R21.
Keywords: number fields, Hurwitz spaces.

For a given fixed set of primes $\mathcal{P}$, are there infinitely many full fields K for which the discriminant of K is divisible only by primes in $\mathcal{P}$? Our Theorem 5.1, together with experimental data to be presented in a sequel paper [Roberts $\geq$ 2015], strongly suggests that the answer to the question is *yes*, whenever $\mathcal{P}$ contains the set of primes dividing the order of a finite nonabelian simple group. This expectation is particularly interesting because the mass heuristic of [Bhargava 2007] predicts *no* for all $\mathcal{P}$.

Sections 2, 3 and 4 provide short summaries of large theories and serve to establish our setting. Section 5 states our main theorem, which we call the full-monodromy theorem. It has the form that two statements, I and II, about data (G, C) defining a multiindexed collection of Hurwitz covers are equivalent. Statement I is an explicit condition on (G, C) and Statement II is an asymptotic statement about the monodromy of the covers in the collection. Sections 6 and 7 prove the theorem by establishing I $\Longrightarrow$ II and II $\Longrightarrow$ I, respectively. Section 8 concludes the paper with a discussion of the application to the construction of full number fields.

1B. ***The full-monodromy theorem.*** This subsection provides an introductory description of the full-monodromy theorem. Define a *Hurwitz parameter* to be a triple $h = (G, C, \nu)$, where G is a finite group, $C = (C_1, \ldots, C_r)$ is a list of conjugacy classes whose union generates G, and $\nu = (\nu_1, \ldots, \nu_r)$ is a list of positive integers, with ν *allowed* in the sense that $\prod [C_i]^{\nu_i} = 1$ in the abelianization G^{ab}. A Hurwitz parameter determines an unramified covering of complex algebraic varieties

$$\pi_h : \mathsf{Hur}_h \to \mathsf{Conf}_\nu. \tag{1-1}$$

Here, the cover Hur_h is a Hurwitz variety parameterizing certain covers of the complex projective line P^1, where the coverings are "of type h". The base Conf_ν is the variety whose points are tuples $(D_1, \ldots, D_r)$ of disjoint divisors D_i of P^1, with $\deg(D_i) = \nu_i$. The map π_h sends a cover to its branch locus.

In complete analogy with the use of the term for number fields, we say that a cover of connected complex algebraic varieties $\mathsf{X} \to \mathsf{Y}$ is *full* if its monodromy group is the entire alternating or symmetric group on the degree. There are two relatively simple obstructions to (1-1) being full. One is associated to G having a nontrivial outer automorphism group, and we deal with it by replacing Hur_h by a quotient variety Hur_h^* also covering Conf_ν. The other is associated to G having a nontrivial Schur multiplier, and we deal with it by a decomposition $\mathsf{Hur}_h^* = \bigsqcup_\ell \mathsf{Hur}_{h,\ell}^*$. Here ℓ runs over the Schur multiplier modulo a certain equivalence relation, and each $\mathsf{Hur}_{h,\ell}^*$ is a union of connected components of Hur_h^*.

The more important direction of the full-monodromy theorem is I $\Longrightarrow$ II. When G is nonabelian and simple, this direction is as follows:

Fix a nonabelian simple group G and a list $C = (C_1, \dots, C_r)$ of conjugacy classes whose union generates G. Consider varying allowed ν and thus varying Hurwitz parameters $h = (G, C, \nu)$. Then as soon as $\min_i \nu_i$ *is sufficiently large, the covers* $\mathsf{Hur}^*_{h,\ell} \to \mathsf{Conf}_\nu$ *are full and pairwise nonisomorphic.*

The complete implication I $\Longrightarrow$ II is similar, but G is allowed to be "pseudo-simple", and therefore groups such as S_d are included. There are considerable complications arising from nontrivial abelianizations G^{ab}, even in the case $|G^{\mathrm{ab}}| = 2$. The extra generality is required for obtaining the natural converse II $\Longrightarrow$ I.

Our proof of I $\Longrightarrow$ II in general starts from the Conway–Parker theorem about connectivity of Hurwitz covers [Conway and Parker 1988; Ellenberg et al. 2013; Fried and Völklein 1991; Malle and Matzat 1999]. We deal with complications from nontrivial G^{ab} in the framework of comparing two Hochschild–Serre five-term exact sequences. We upgrade connectivity to fullness by using a Goursat lemma adapted to our current situation and the explicit classification of finite 2-transitive groups. Our general approach has much in common with the proof of Theorem 7.4 in [Dunfield and Thurston 2006], which is in a different context.

While there is a substantial literature on Hurwitz covers, our topic of asymptotic fullness has not been systematically pursued before. In related directions there are the papers [Eisenbud et al. 1991; Kluitmann 1988; Magaard et al. 2003]. We will indicate relations with some of this literature at various points in the present paper.

2. Hurwitz covers

In this section we summarize the theory of Hurwitz covers, taking the purely algebraic point of view necessary for the application to number field construction. We consider Hurwitz parameters $h = (G, C, \nu)$, with G assumed centerless to avoid technical complications. The central focus is an associated cover $\pi_h : \mathrm{HUR}_h \to \mathrm{CONF}_\nu$ and related objects. A more detailed summary can be found in [Romagny and Wewers 2006], and a comprehensive reference in [Bertin and Romagny 2011]. Note that throughout this paper we use a sans serif font for complex analytic spaces, as in $\mathbb{P}^1(\mathbb{C}) = \mathsf{P}^1$ or $\mathrm{CONF}_\nu(\mathbb{C}) = \mathsf{Conf}_\nu$.

2A. ***Configuration spaces*** $\mathbf{CONF}_\nu$**.** Let $\nu = (\nu_1, \dots, \nu_r)$ be a vector of positive integers; we write $|\nu| = \sum \nu_i$. For k a field, let $\mathrm{CONF}_\nu(k)$ be the set of tuples $(D_1, \dots, D_r)$ of disjoint k-rational divisors on $\mathbb{P}^1_k$ with D_i consisting of ν_i distinct geometric points.

Explicitly, we may regard

$$\mathrm{CONF}_\nu \subseteq \mathbb{P}^{\nu_1} \times \cdots \times \mathbb{P}^{\nu_r},$$

where we regard $\mathbb{P}^{\nu_i}$ as the projectivized space of binary homogeneous forms $q(x, y)$ of degree ν_i, and CONF_ν is then the open subvariety defined by nonvanishing of the discriminant $\mathrm{disc}(q_1 \cdots q_r)$. The divisor D_i associated to an r-tuple $(q_1, \ldots, q_r)$ of such forms is simply the zero locus of q_i.

2B. ***Standard Hurwitz varieties*** $\mathbf{HUR}_h$**.** Let k be an algebraically closed field of characteristic zero. Consider pairs (Σ, f) consisting of a proper smooth connected curve Σ over k together with a Galois covering $f : \Sigma \to \mathbb{P}^1$.

Such a pair has the following associated objects:

- An automorphism group $\mathrm{Aut}(\Sigma/\mathbb{P}^1)$ of size equal to the degree of f.
- A branch locus $Z \subset \mathbb{P}^1(k)$.
- For every $t \in Z$, a local monodromy element $g_t \in \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ defined up to conjugacy. (To define this requires a compatible choice of roots of unity, i.e., an element of $\varprojlim_n \mu_n(k)$; we assume such a choice has been made.)

Consider triples (Σ, f, ι) with $\iota : G \to \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ a given isomorphism. We say that such a triple has type h if $\sum \nu_i = |Z|$ and for each i there are exactly ν_i elements $t \in Z$ such that $g_t \in C_i$. The branch locus Z then defines an element of $\mathrm{CONF}_\nu(k)$ in a natural way.

The theory of Hurwitz varieties implies that there exists a $\overline{\mathbb{Q}}$-variety HUR_h, equipped with an étale map

$$\pi_h : \mathrm{HUR}_h \to \mathrm{CONF}_\nu, \tag{2-1}$$

with the following property holding for all k: For any $u \in \mathrm{CONF}_\nu(k)$, the fiber $\pi_h^{-1}(u)$ is $\mathrm{Aut}(k/\mathbb{Q}(\mu_\infty))$-equivariantly in bijection with the set of isomorphism classes of covers of $\mathbb{P}^1$ of type h, with branch locus equal to u.

2C. ***Quotiented Hurwitz varieties*** $\mathbf{HUR}_h^*$**.** If (Σ, f, ι) is as above, we can modify ι by an element $\alpha \in \mathrm{Aut}(G)$, to obtain a new triple $(\Sigma, f, \iota \circ \alpha^{-1})$. If α is inner, the resulting triple is actually isomorphic to (Σ, f, ι). As a results we obtain actions by groups of outer automorphisms.

Let $\mathrm{Aut}(G, C)$ be the subgroup of $\mathrm{Aut}(G)$ consisting of those elements which fix every C_i. Then $\mathrm{Out}(G, C) = \mathrm{Aut}(G, C)/G$ acts naturally on HUR_h, giving a quotient

$$\mathrm{HUR}_h^* = \mathrm{HUR}_h / \mathrm{Out}(G, C),$$

still lying over CONF_ν. This quotient parameterizes pairs (Σ, f) equipped with an element $(D_1, \ldots, D_r)$ of $\mathrm{CONF}_\nu(k)$ so that the branch locus is precisely $\bigsqcup D_i$, and there exists an isomorphism $\iota : G \to \mathrm{Aut}(\Sigma/\mathbb{P}^1)$ so that the monodromy around each point of D_i is of type $\iota(C_i)$. Our main theorem focuses on HUR_h^* rather than HUR_h.

2D. ***Descent to*** $\mathbb{Q}$**.** The discussion that follows is not used in the body of the paper, but it is relevant to the application to full number fields, sketched in Section 8.

The abelianized absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}} = \widehat{\mathbb{Z}}^\times$ acts on the set of conjugacy classes in any finite group by raising representing elements to powers. In particular, one can talk about rational classes, i.e., conjugacy classes fixed by this action. We say that h is *strongly rational* if all C_i are rational. In this case, (2-1) and its starred version $\pi_h^* : \mathrm{HUR}_h^* \to \mathrm{CONF}_\nu$ canonically descend to covers over $\mathbb{Q}$. This statement can be deduced from the corresponding statement for the "large" Hurwitz space, parameterizing coverings without any restrictions on branch monodromy; for that statement see [Fried and Völklein 1991, Theorem 1] and [Romagny and Wewers 2006, Theorems 2.1 and 4.11]. The rationality of the C_i enters because of the dependence on choice of element of $\varprojlim \mu_n$, as above.

More generally, we say that h is *rational* if conjugate classes appear with equal associated multiplicities. In the main case when all the classes are different, this just means $\nu_i = \nu_j$ whenever C_i and C_j lie in the same Galois orbit. Rationality is a substantially weaker condition than strong rationality. For example, any finite group G has rational h, but only when G^{ab} is trivial or of exponent 2 can G have strongly rational h.

For rational h, there is again canonical descent to $\mathbb{Q}$, although now the maps take the form $\mathrm{HUR}_h \to \mathrm{HUR}_h^* \to \mathrm{CONF}_\nu^\rho$, with ρ indicating a suitable Galois twisting. The subtlety of twisting is not seen in the rest of this paper. Our purpose in briefly discussing twisting here is to make clear that many Hurwitz covers are useful for the construction of full number fields.

3. Braid groups

In this section we switch to a group-theoretic point of view, describing the monodromy of Hurwitz covers $\pi_h : \mathsf{Hur}_h \to \mathsf{Conf}_\nu$ and $\pi_h^* : \mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ in terms of braid groups and their actions on explicit sets. General references for braid groups and their monodromy actions include [Malle and Matzat 1999, Chapter 3] and [Eisenbud et al. 1991, §2].

Our main theorem concerns these monodromy representations only, i.e., it is a theorem in pure group theory. The map of $\mathbb{Q}$-varieties $\mathrm{HUR}_h \to \mathrm{CONF}_\nu$ underlying the map of complex analytic spaces $\mathsf{Hur}_h \to \mathsf{Conf}_\nu$ will return in Section 8.

3A. ***Braid groups*** $\mathbf{Br}_\nu$**.** The Artin braid group on n strands is defined by the generators and relations

$$\mathrm{Br}_n = \left\langle \sigma_1, \dots, \sigma_{n-1} \ : \ \begin{array}{ll} \sigma_i\sigma_j = \sigma_j\sigma_i & \text{if } |i-j| > 1 \\ \sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j & \text{if } |i-j| = 1 \end{array} \right\rangle.$$

The rule $\sigma_i \mapsto (i, i+1)$ extends to a surjection $\mathrm{Br}_n \twoheadrightarrow S_n$. For every subgroup of S_n, one gets a subgroup of Br_n by pullback. In particular, from the last component $\nu = (\nu_1, \ldots, \nu_r)$ of a Hurwitz parameter one gets a subgroup $S_\nu := S_{\nu_1} \times \cdots \times S_{\nu_r}$. We denote its pullback by Br_ν. The extreme Br_n above and the other extreme Br_{1^n} play particularly prominent roles in the literature, the latter often being called the colored or pure braid group.

3B. ***Fundamental groups.*** Let $\star = (1, \ldots, n) \in \mathsf{Conf}_{1^n}$. We will use it as a basepoint. We use the same notation $\star$ for its image in Conf_ν for any ν. There is a standard surjection $\mathrm{Br}_n \twoheadrightarrow \pi_1(\mathsf{Conf}_n, \star)$, with kernel the smallest normal subgroup containing $\sigma_1 \cdots \sigma_{n-2}\sigma_{n-1}^2\sigma_{n-2} \cdots \sigma_1$ [Malle and Matzat 1999, Theorem III.1.4]. This map identifies σ_i with a small loop in Conf_n that swaps the points i and $i+1$. Because of this very tight connection, the group $\pi_1(\mathsf{Conf}_n, \star)$ is often called the spherical braid group or the Hurwitz braid group.

Similarly, we have surjections

$$\mathrm{Br}_\nu \twoheadrightarrow \pi_1(\mathsf{Conf}_\nu, \star). \tag{3-1}$$

Let $\mathcal{F}_h$ and $\mathcal{F}_h^*$ be the fibers of Hur_h and Hur_h^* over $\star$. To completely translate into group theory, we need group-theoretical descriptions of these fibers as Br_ν-sets. The remainder of this section accomplishes this task.

3C. ***Catch-all actions.*** We use the standard notational convention $g^h = h^{-1}gh$. If G is any group then Br_n acts on G^n by means of a braiding rule, whereby σ_i substitutes $g_i \to g_{i+1}$ and $g_{i+1} \to g_i^{g_{i+1}}$:

$$(\ldots, g_{i-1}, g_i, g_{i+1}, g_{i+2}, \ldots)^{\sigma_i} = (\ldots, g_{i-1}, g_{i+1}, g_i^{g_{i+1}}, g_{i+2}, \ldots). \tag{3-2}$$

Also any $\alpha \in \mathrm{Aut}(G)$ acts on G^n diagonally by

$$(g_1, \ldots, g_n)^\alpha = (g_1^\alpha, \ldots, g_n^\alpha). \tag{3-3}$$

The braiding action and the diagonal action commute, so one has an action of the product group $\mathrm{Br}_n \times \mathrm{Aut}(G)$ on G^n.

3D. ***The*** $\mathbf{Br}_\nu$***-sets*** $\mathcal{F}_h$ ***and*** $\mathcal{F}_h^*$**.** Next we replace G^n by a smaller set appropriate to a given Hurwitz parameter h. This smaller set is

$$\mathcal{G}_h = \big\{(g_1, \ldots, g_n) \in G^n : g_1 \cdots g_n = 1, \langle g_1, \ldots, g_n\rangle = G, \\ \text{first } \nu_1 \text{ of the } g_i \text{ lie in } C_1, \text{ next } \nu_2 \text{ lie in } C_2, \text{ etc.}\big\}. \tag{3-4}$$

The subset $\mathcal{G}_h$ is not preserved by all of $\mathrm{Br}_n \times \mathrm{Aut}(G)$, but it is preserved by $\mathrm{Br}_\nu \times \mathrm{Aut}(G, C)$. The fibers then have the following group-theoretic description:

$$\mathcal{F}_h = \mathcal{G}_h / \operatorname{Inn}(G) \simeq (\text{fiber of } \mathsf{Hur}_h \to \mathsf{Conf}_\nu \text{ above } \star), \tag{3-5}$$

$$\mathcal{F}_h^* = \mathcal{G}_h / \operatorname{Aut}(G, C) \simeq (\text{fiber of } \mathsf{Hur}_h^* \to \mathsf{Conf}_\nu \text{ above } \star). \tag{3-6}$$

Here in both cases the isomorphisms $\simeq$ are isomorphisms of Br_ν-sets. A clear exposition of the relationship of Hurwitz spaces to braiding is given in [Eisenbud et al. 1991, §1], and the isomorphisms (3-5) and (3-6) are a consequence of this relationship; see also [Fried and Völklein 1991, §1]. Note that $\mathcal{F}_h^* = \mathcal{F}_h / \operatorname{Out}(G, C)$.

3E. ***The asymptotic mass formula.*** Character theory gives mass formulas [Serre 2008, Theorem 7.2.1]. These formulas, applied both to G and to subgroups intersecting all the C_i, can be used to exactly determine the degrees $\mathcal{F}_h$ and $\mathcal{F}_h^*$. We need only the asymptotic versions of the mass formulas for G, which are very simple:

$$|\mathcal{F}_h| \sim \frac{\prod_{i=1}^r |C_i|^{\nu_i}}{|G'||\mathrm{Inn}(G)|}, \qquad |\mathcal{F}_h^*| \sim \frac{\prod_{i=1}^r |C_i|^{\nu_i}}{|G'||\mathrm{Aut}(G, C)|}. \tag{3-7}$$

Here the meaning in each case is standard: the left side over the right side tends to 1 for any sequence of allowed ν with $\min_i \nu_i$ tending to ∞. The structure of the products on the right directly reflects the descriptions of the sets in Section 3D.

4. Lifting invariants

In this section we summarize the theory of lifting invariants, which plays a key role in the study of connected components of Hurwitz spaces. Group homology appears prominently, and as a standing convention we abbreviate $H_i(\Gamma, \mathbb{Z})$ by $H_i(\Gamma)$.

In brief summary, the theory being reviewed goes as follows. Let $h = (G, C, \nu)$ be a Hurwitz parameter. The group G determines its Schur multiplier $H_2(G)$. In turn, C determines a quotient group $H_2(G, C)$ of $H_2(G)$, and finally ν determines a certain torsor $H_h = H_2(G, C, \nu)$ over $H_2(G, C)$. The Conway–Parker theorem says that the natural map $\pi_0(\mathsf{Hur}_h) \to H_h$ is bijective whenever $\min_i \nu_i$ is sufficiently large.

4A. ***The Schur multiplier $H_2(G)$.*** A stem extension of G is a central extension G^* such that the kernel of $G^* \to G$ is in the derived group of G^*. A stem extension of maximal order has kernel canonically isomorphic to the cohomology group $H_2(G)$. This kernel is by definition the Schur multiplier. A stem extension of maximal order is called a Schur cover. A given group can have nonisomorphic Schur covers, but this ambiguity never poses problems for us here.

4B. ***The reduced Schur multiplier $H_2(G, C)$.*** If x, y are commuting elements of G, they canonically define an element $\langle x, y\rangle \in H_2(G)$: the commutator of lifts of x, y to a Schur cover. (In the context of this paper, there should be no confusion of this symbol with the group generated by x, y). This pairing is independent of the choice of Schur cover. In fact, a more intrinsic description is that $\langle x, y\rangle$ is the pushforward of the fundamental class of $H_2(\mathbb{Z}^2)$ under the map $\mathbb{Z}^2 \to G$ given by $(m, n) \mapsto x^m y^n$.

Fix a stem extension of maximal order $\widetilde{G} \to G$. For a conjugacy class C_i and a list of conjugacy classes $C = (C_1, \dots, C_r)$ respectively, define subgroups of the Schur multiplier

$$H_2(G)_{C_i} = \{\langle g, z\rangle : g \in C_i \text{ and } z \in Z(g)\}, \tag{4-1}$$

$$H_2(G)_C = \sum H_2(G)_{C_i}. \tag{4-2}$$

Here $Z(g)$ denotes the centralizer of g in G. The reduced Schur multiplier is then the corresponding quotient group $H_2(G, C) = H_2(G)/H_2(G)_C$.

A choice of Schur cover $\widetilde{G}$ determines a reduced Schur cover $\widetilde{G}_C = \widetilde{G}/H_2(G)_C$. The corresponding short exact sequence

$$H_2(G, C) \hookrightarrow \widetilde{G}_C \twoheadrightarrow G$$

plays an essential role in our study.

In a degree-d central extension $\pi : G^* \to G$, the preimage of a conjugacy class D consists of a certain number s of conjugacy classes, all of size $(d/s)|D|$. Always s divides d. If $s = d$ then D is called *split*. By construction, all the C_i are split in $\widetilde{G}_C$, and $\widetilde{G}_C$ is a maximal extension with this property. For more information on reduced Schur multipliers, see [Ellenberg et al. 2013, §7, v1].

4C. ***Torsors $H_2(G, C, \nu)$.*** For $i = 1, \dots, r$, let $H_2(G, C, i)$ be the set of conjugacy classes of $\widetilde{G}_C$ that lie in the preimage of the class C_i. If $\tilde{z}$ and $\tilde{g}$ are lifts to $\widetilde{G}_C$ of the identity $z = 1$ and $g \in C_i$ respectively, then one can multiply $\tilde{z} \in H_2(G, C)$ and $[\tilde{g}] \in H_2(G, C, i)$ to get $[\tilde{z}\tilde{g}] \in H_2(G, C, i)$. This multiplication operator turns each $H_2(G, C, i)$ into a torsor over $H_2(G, C)$.

One can multiply torsors over an abelian group: if T_1 and T_2 are torsors over an abelian group Z, then their product is $(T_1 \times T_2)/Z$, where all $(zt_1, z^{-1}t_2)$ have been identified. In our setting, one has a torsor

$$H_h := H_2(G, C, \nu) = \prod_i H_2(G, C, i)^{\nu_i}. \tag{4-3}$$

Note that H_h is naturally identified with the trivial torsor if all ν_i are multiples of the exponent of $H_2(G, C)$. Namely the product $\prod a_i^{\nu_i}$ is independent of choices $a_i \in H_2(G, C, i)$, and gives a distinguished element of $H_2(G, C, \nu)$. In particular,

this distinguished element is fixed under $\mathrm{Aut}(G, C)$ (see Section 4E for a more detailed discussion of functoriality).

4D. ***The lifting map.*** Suppose we are given $(g_1, \dots, g_n) \in \mathcal{G}_h$. Lift each g_i to an element $\tilde{g}_i \in \widetilde{G}_C$ arbitrarily, subject to the unique condition that the product of the $\tilde{g}_i$ is the identity:

$$\tilde{g}_1 \cdots \tilde{g}_n = 1 \in \widetilde{G}_C.$$

Then each $\tilde{g}_i$ determines an element $[\tilde{g}_i] \in H_2(G, C, i)$. Their product is an element $\prod[\tilde{g}_i] \in H_2(G, C, \nu)$, independent of choices. This product is moreover unchanged if we replaced $(g_1, \dots, g_n)$ by another element in its Br_ν-orbit, or if we replace $(g_1, \dots, g_n)$ by a G-conjugate. Thus, keeping in mind the identification $\pi_0(\mathsf{Hur}_h) = \mathcal{F}_h / \mathrm{Br}_\nu$ from (3-5), we have defined a function

$$\mathrm{inv}_h : \pi_0(\mathsf{Hur}_h) \to H_h. \tag{4-4}$$

We refer to inv_h as the lifting invariant. It has been extensively studied by Fried and Serre; see [Bailey and Fried 2002; Serre 1990]. When a set decomposes according to lifting invariants, we indicate this decomposition by subscripts. Thus, e.g., $\mathcal{F}_h = \bigsqcup \mathcal{F}_{h,\ell}$ and $\mathcal{G}_h = \bigsqcup \mathcal{G}_{h,\ell}$.

The map (4-4) is equivariant with respect to the natural actions of $\mathrm{Out}(G, C)$ and so we can pass to the quotient. Writing $H_h^* = H_h / \mathrm{Out}(G, C)$, we obtain

$$\mathrm{inv}_h^* : \pi_0(\mathsf{Hur}_h^*) \to H_h^*. \tag{4-5}$$

Again we denote lifting invariants by subscripts, so that $\mathcal{F}_{h,\ell}^* = \mathcal{F}_{h,\ell} / \mathrm{Out}(G, C)_\ell$ for example, where $\mathrm{Out}(G, C)_\ell$ is the stabilizer of ℓ inside $\mathrm{Out}(G, C)$.

Note that algebraic structure is typically lost in the process of passing from objects to their corresponding starred objects. Namely, at the unstarred level one has a group $H_2(G, C)$ and its many torsors H_h. At the starred level, $H_2^*(G, C)$ is typically no longer a group, the sets H_h^* are no longer torsors, and the cardinality of H_h^* can depend on ν. Our main theorem makes direct reference only to H_h^*. However in the proof we systematically lift from H_h^* to H_h, to make use of the richer algebraic properties.

We finally note for later use that there are asymptotic mass formulas for $\mathcal{F}_{h,\ell}$ and $\mathcal{F}_{h,\ell}^*$ that are very similar to (3-7). Indeed, they are derived simply by applying (3-7) to $\widetilde{G}_C$ together with liftings of the conjugacy classes C_i:

$$|\mathcal{F}_{h,\ell}| \sim \frac{|\mathcal{F}_h|}{|H_2(G, C)|}, \qquad |\mathcal{F}_{h,\ell}^*| \sim \frac{|\mathcal{F}_{h,\ell}|}{|\mathrm{Out}(G, C)_\ell|}. \tag{4-6}$$

4E. ***Functoriality.*** Suppose we are given a surjection $f : G \to H$ of groups, together with conjugacy classes C_i in G, and set $D_i = f(C_i)$. This clearly induces a map $H_2(G, C) \to H_2(H, D)$. The functoriality of the torsors is less obvious,

because of the lack of uniqueness in a Schur cover. For this, we use a more intrinsic presentation:

Amongst central extensions $\widetilde{G} \to G$ equipped with a lifting $\widetilde{C}_i$ of each C_i, there is a universal one $\widetilde{G}^*$, unique up to unique isomorphism [Ellenberg et al. 2013, Theorem 7.5.1]. Now consider the central extension $G \times \mathbb{Z}^r \to G$, where we lift C_i to $C_i \times e_i$, with e_i the i-th coordinate vector. This gives a canonical map $\alpha : \widetilde{G}^* \to G \times \mathbb{Z}^r$, and we define $H_2(G, C, \nu)_{\text{univ}}$ to be the preimage of $e \times \nu \in G \times \mathbb{Z}^r$.

This is closely related to the previous definition. Note that if we fix lifts $C_i^* \subset \widetilde{G}_C$ of each C_i, we get an induced map $\beta : \widetilde{G}^* \to \widetilde{G}_C$ from the universal property. This induces a bijection of $H_2(G, C, \nu)_{\text{univ}}$ with $H_2(G, C)$; indeed, the canonical map

$$\beta \times_G \alpha : \widetilde{G}^* \to \widetilde{G}_C \times_G (G \times \mathbb{Z}^r) \tag{4-7}$$

is an isomorphism (again, [Ellenberg et al. 2013, Theorem 7.5.1]).

So a choice of lifts C_i^* gives a distinguished element $c_\nu \in H_2(G, C, \nu)_{\text{univ}}$ — the preimage of the identity in $H_2(G, C)$. Moreover, if we replace C_i^* by $z_i C_i^*$, where $z_i \in H_2(G, C)$, then the associated map $\widetilde{G}^* \to \widetilde{G}_C$ is multiplied by the composite map $\widetilde{G}^* \to \mathbb{Z}^r \to \widetilde{G}_C$, where the second map sends $e_i \in \mathbb{Z}^r$ to z_i. Thus, with this replacement, the identification $H_2(G, C, \nu) \xrightarrow{\sim} H_2(G, C)$ has been multiplied by z^{ν_i}; in other words, the distinguished element is replaced by $\prod z_i^{-\nu_i} c_\nu$.

This construction exhibits an identification of torsors

$$H_2(G, C, \nu)_{\text{univ}} \simeq H_2(G, C, \nu)^{-1}, \tag{4-8}$$

where we write $T_1 \simeq T_2^{-1}$ for two A-torsors if there is an identification of T_1 and T_2 transferring the A-action on T_1 to the inverse of the A-action on T_2.

In fact, with respect to the identification (4-8), our lifting invariant corresponds to the lifting invariant of [Ellenberg et al. 2013]: In that paper, the authors take $(g_1, \dots, g_r)$ and associate to it the lifting invariant $\Pi = \prod \tilde{g}_i \in H_2(G, C, \nu)_{\text{univ}}$, where $\tilde{g}$ is the lift to a universal central extensions equipped with lifting. Fix $\widetilde{G}_C$, C_i^* and a morphism $\widetilde{G}^* \to \widetilde{G}_C$ as above. Choose $z_i \in H_2(G, C)$ such that the image of Π in $H_2(G, C)$ coincides with $\prod z_i^{\nu_i}$. Then $\prod \tilde{g}_i$ is carried to $\prod z_i^{\nu_i}$ multiplied by the distinguished element of $H_2(G, C, \nu)_{\text{univ}}$. On the other hand, the lifting invariant as we have defined it above equals $[C_i^* z_i^{-1}] \in H_2(G, C, \nu)$, which equals $\prod z_i^{-\nu_i}$ times the corresponding element of $H_2(G, C, \nu)$.

Now — returning to the surjection $G \to H$ — take a universal extension $\widetilde{H}^* \to H$ equipped with a lifting of the D_i, and consider $G \times_H \widetilde{H}^* \to G$; it's a central extension and it is equipped with a lifting of C_i, namely $C_i \times_H D_i^*$. There is thus a canonical map $\widetilde{G}^* \to \widetilde{H}^*$. Taking fibers above $\nu \in \mathbb{Z}^r$ gives the desired map

$$f_* : H_2(G, C, \nu)_{\text{univ}} \to H_2(H, D, \nu)_{\text{univ}},$$

and by inverting one obtains the desired map $H_2(G, C, \nu) \to H_2(H, D, \nu)$. In particular, one easily verifies that if $H = G$ and $G \to H$ is an inner automorphism, the induced map on $H_2(G, C, \nu)$ is trivial.

Finally, suppose ν is chosen to be simultaneously divisible by the order of $H_2(G, C)$ and $H_2(H, D)$ (i.e., each ν_i is so divisible). Then in fact the map $H_2(G, C, \nu) \to H_2(H, D, \nu)$ respects the natural identifications of both sides with $H_2(G, C)$ and $H_2(H, D)$ (see after (4-3)). In fact, one has natural identifications

$$H_2(G, C, \nu_1 + \nu_2) \simeq H_2(G, C, \nu_1) \times H_2(G, C, \nu_2)/H_2(G, C),$$

where the action of $z \in H_2(G, C)$ on the right is as $z : (t_1, t_2) \mapsto (t_1 z, z^{-1} t_2)$. These identifications are easily seen to be compatible with the map $H_2(G, C, \nu) \to H_2(H, D, \nu)$. Now choose C_i^* and D_i^* as above, giving rise to corresponding elements $c_\nu \in H_2(G, C, \nu)$ and $d_\nu \in H_2(H, D, \nu)$. Write $f_* c_\nu = \gamma_\nu d_\nu$ for some $\gamma_\nu \in H_2(H, D)$; then our comments show that $\gamma_{\nu_1 + \nu_2} = \gamma_{\nu_1} \gamma_{\nu_2}$, and the claim follows: if ν is divisible by the order of $H_2(H, D)$, then γ_ν will be trivial.

4F. ***The Conway–Parker theorem.*** We will use a result due to Conway and Parker [1988] in the important special case where $H_2(G, C)$ is trivial. This result is also described in [Fried and Völklein 1991, Appendix] and [Malle and Matzat 1999, III.6.3]. We need the following generalization to nontrivial $H_2(G, C)$:

Proposition 4.1. *Consider Hurwitz parameters $h = (G, C, \nu)$ for (G, C) fixed and ν varying. Suppose that all the C_i are distinct. For sufficiently large* $\min_i \nu_i$, *the lifting invariant map* $\mathrm{inv}_h : \pi_0(\mathsf{Hur}_h) \to H_h$ *is bijective.*

The generalization is proved in [Ellenberg et al. 2013, §7, Theorem 7.5.1]. Because of the importance of Proposition 4.1 to this paper, we give an overview of the proof here:

Overview of proof of Proposition 4.1. First we reprise, with a few more details, the setting of Section 4E. Consider pairs $(f : G^* \to G, s)$ of a central extension of G together with a section s of f over each C_i, equivariant under conjugation, i.e.,

$$s(f(x) g f(x)^{-1}) = x s(g) x^{-1}$$

for $x \in G^*$, $g \in \bigcup C_i$. There is an initial object $(f^* : \widetilde{G}^* \to G, s^*)$ in the category of such pairs, i.e., a "universal central extension with section over each C_i"; in fact, we describe this initial object explicitly in the penultimate paragraph of this overview.

As discussed before (4-7), there is a natural homomorphism $\widetilde{G}^* \to G \times \mathbb{Z}^r$. Consider the sets $\mathcal{F}_h, \mathcal{G}_h$ described in Section 3D; the map sending g_i to $[g_i]$ gives a well-defined map $\mathcal{G}_h / \mathrm{Br}_\nu \to \widetilde{G}^*$, and in fact

$$\mathcal{F}_h / \mathrm{Br}_\nu \xrightarrow{I} \text{ fiber of } \widetilde{G}^* \text{ above } (e, \nu).$$

As we explained in Section 4E, this map is the lifting invariant, up to the identification discussed around (4-8). We must verify that I is a bijection when all of the ν_i are large enough. The remainder of the argument is close to the argument in the appendix to [Fried and Völklein 1991]:

Consider the monoid given by $S = \bigsqcup_{n\geq 0}\big(\bigcup C_i\big)^n / \operatorname{Br}_n$, with multiplication given by concatenation. For each $g \in C_i$ let $[g]$ be the corresponding element of S (corresponding to $n = 1$). Consider inside this monoid the element

$$U = (\underbrace{x_1, x_1, \ldots, x_1}_{|G|}, \underbrace{x_2, x_2, \ldots, x_2}_{|G|}, x_3, \ldots)$$

given by taking each element of each C_i exactly $|G|$ times in succession, after fixing any ordering of such elements. Then U is central, i.e., commutes with all of S. Therefore, we may formally invert U, i.e., form the group $S[U^{-1}]$. Note that U is "divisible" by each $[g]$, and therefore each $[g]$ is invertible; consequently, $S[U^{-1}]$ is a group. Then $f : [g] \mapsto g$ defines a homomorphism $S[U^{-1}] \to G$ with central kernel; moreover, $s : g \mapsto [g]$ gives a section of this homomorphism over $\bigcup C_i$. Then it is easily verified that $(f : S[U^{-1}] \to G, s)$ is a universal central extension.

Suppose that $a = (g_1, \ldots, g_n)$, $b = (g'_1, \ldots, g'_n) \in \mathcal{F}_h$ have the same image in $\widetilde{G}^*$. The above construction of $\widetilde{G}^*$ shows that $(g_1, \ldots, g_n)\cdot U^k = (g'_1, \ldots, g'_n)\cdot U^k$ inside the semigroup S, i.e., a and b become braid-equivalent after concatenating sufficiently many copies of U. However, an elementary group-theoretic computation (see the appendix of [Fried and Völklein 1991]) shows that this implies — if $\min_i \nu_i$ is large enough — that a and b are themselves braid-equivalent. □

Various comments on Proposition 4.1 are in order. First, the condition that $\min_i \nu_i$ is sufficiently large carries on passively to many of our later considerations. We will repeat it explicitly several times but also refer to it by the word *asymptotically*.

Second, there are a number of equivalent statements. The direct translation of the bijectivity of $\pi_0(\mathsf{Hur}_h) \to H_h$ into group theory is that each fiber of $\mathcal{F}_h \to H_h$ is a single orbit of Br_ν. Alternatively, one could compose the cover $\mathsf{Hur}_h \to \mathsf{Conf}_\nu$ with the cover $\mathsf{Conf}_\nu \to \mathsf{Conf}_n$ and state the result in terms of actions of the full braid group Br_n; this is the viewpoint of both [Fried and Völklein 1991, Appendix] and [Malle and Matzat 1999, III.6.3]

Third, quotienting by $\operatorname{Out}(G, C)$ one gets a similar statement: the resulting map $\mathrm{inv}_h^* : \pi_0(\mathsf{Hur}_h^*) \to H_h^*$ is asymptotically bijective. This is the version that our full-monodromy theorem refines for certain (G, C). Note that a complication not present in Proposition 4.1 itself appears at this level: the cardinality of $H_h^* = H_h/\operatorname{Out}(G, C)$ can be dependent on ν.

5. The full-monodromy theorem

In this section, we state the full-monodromy theorem. Involved in the statement is a homological condition. We clarify the nature of this condition by giving instances when it holds and instances when it fails.

5A. ***Preliminary definitions.*** In this section, we define the notions of *pseudosimple*, *unambiguous*, and *quasifull*. All three of these notions figure prominently in the statement of the full-monodromy theorem.

We say that a centerless finite group G is *pseudosimple* if its derived group G' is a power of a nonabelian simple group and any nontrivial quotient group of G is abelian. Thus, there is an extension

$$G' \to G \to G^{\mathrm{ab}}, \tag{5-1}$$

where $G' \simeq T^w$, with T nonabelian simple, and the action of G^{ab} on T^w is transitive on the w simple factors. (Our terminology is meant to be reminiscent of similar standard terms for groups closely related to a nonabelian simple group T: *almost simple* groups are extensions $T.A$ contained in $\mathrm{Aut}(T)$ and *quasisimple* groups are quotients $M.T$ of the Schur cover $\widetilde{T}$.)

We say that a conjugacy class C_i in a group G is *ambiguous* if the G' action on C_i by conjugation has more than one orbit. If it has exactly one orbit we say that C_i is *unambiguous*. These are standard notions and for many G the division of classes into ambiguous and unambiguous can be read off from an Atlas page [Conway et al. 1985].

Essentially repeating a definition from the introduction, we say that the action of a group Γ on a set X is *full* if the image of Γ in $\mathrm{Sym}(X)$ contains the alternating group $\mathrm{Alt}(X)$. Generalizing now, we say the action is *quasifull* if the image contains $\mathrm{Alt}(X_1) \times \cdots \times \mathrm{Alt}(X_s)$, where the X_i are the orbits of Γ on X. Again we transfer the terminology to a topological setting. Thus a covering X of a connected space Y is quasifull if for any $y \in \mathsf{Y}$, the monodromy action of $\pi_1(\mathsf{Y}, y)$ on the fiber X_y is quasifull.

5B. ***Fiber powers of Hurwitz parameters.*** This subsection describes how a Hurwitz parameter $h = (G, C, \nu)$ and a positive integer k give a triple $h^k = (G^{[k]}, C^k, \nu)$. Part of this notion, in the special case $k = 2$, appears in the statement of the main theorem. The general notion plays a central role in the proof.

In general, if G is a finite group with abelianization G^{ab}, we can consider its k-fold fiber power

$$G^{[k]} = G \times_{G^{\mathrm{ab}}} \cdots \times_{G^{\mathrm{ab}}} G.$$

Note that even when $G = T^w.G^{\mathrm{ab}}$ is pseudosimple, the fiber powers $G^{[k]} = T^{wk}.G^{\mathrm{ab}}$ for $k \geq 2$ are not, because G^{ab} does not act transitively on the factors.

If C_i is a conjugacy class in a group G, we can consider its Cartesian powers $C_i^k \subseteq G^{[k]}$. In general, C_i^k is only a union of conjugacy classes. However, if C_i is unambiguous then C_i^k is a single class.

If $C = (C_1, \dots, C_r)$ is a list of conjugacy classes, we can consider the corresponding list $(C_1^k, \dots, C_r^k)$. Generation of G by the C_i does not imply generation of $G^{[k]}$ by the C_i^k. However, if G is pseudosimple then this implication does hold. (This can be easily deduced, for example, using the Goursat lemma, in the form of Lemma 6.1.) Thus if G is pseudosimple and C consists only of unambiguous classes, the triple h^k is a Hurwitz parameter.

Suppose, then, that G is pseudosimple and C consists of unambiguous classes. The natural map (Section 4E)

$$H_2(G^{[k]}, C^k, \nu) \to H_2(G, C, \nu)^k$$

is surjective. This surjectivity can be seen by interpreting both sides in terms of connected components (in the large ν limit) via the Conway–Parker theorem. Surjectivity can also be seen because the map is equivariant with respect to the natural map $H_2(G^{[k]}, C^k) \to H_2(G, C)^k$, which is surjective by homological algebra, as we explain after (5-2).

5C. ***Statement.*** With our various definitions in place, we can state the main result of this paper:

Theorem 5.1 (full-monodromy theorem). *Let G be a finite centerless nonabelian group, let $C = (C_1, \dots, C_r)$ a list of distinct nonidentity conjugacy classes generating G, and consider Hurwitz parameters $h = (G, C, \nu)$ for varying allowed $\nu \in \mathbb{Z}^r_{\geq 1}$. Then the following two statements are equivalent*:

I: 1. *G is pseudosimple*,
2. *the classes C_i are all unambiguous, and*
3. $|H_2(G^{[2]}, C^2)| = |H_2(G, C)|^2$.

II: *All covers $\mathsf{Hur}^*_h \to \mathsf{Conf}_\nu$ are quasifull whenever $\min_i \nu_i$ is sufficiently large.*

Note that Statement II can equivalently be presented in terms of fullness: *for $\min_i \nu_i$ sufficiently large, the covers $\mathsf{Hur}^*_{h,\ell} \to \mathsf{Conf}_\nu$ are full and pairwise nonisomorphic as ℓ ranges over H_h^*.* Note also that a pseudosimple group G is simple if and only if G^{ab} is trivial. In this case, Conditions 2 and 3 of Statement I are trivially satisfied and the direction I $\Longrightarrow$ II becomes the statement highlighted in Section 1B.

For the more important direction I $\Longrightarrow$ II, the condition that $\min_i \nu_i$ is sufficiently large is simply inherited from the Conway–Parker theorem. Calculations suggest that the covers $\mathsf{Hur}^*_h \to \mathsf{Conf}_\nu$ tend to be quasifull even when all ν_i are small. We are not pursuing the important question of effectivity here, but we note that

effective statements of fullness are obtained for certain classical Hurwitz parameters in [Kluitmann 1988].

Given (G, C), whether or not Conditions 1 and 2 hold is immediately determinable in practice. Evaluating Condition 3 is harder in general, and the next two subsections are devoted to giving an easily checkable reformulation applicable in many cases (Proposition 5.2) and showing (Corollary 5.3) that it sometimes fails.

5D. ***The homological condition for G of split-cyclic type.*** We say that a pseudosimple group G has *split* type if the canonical surjection $\pi : G \to G^{\mathrm{ab}}$ has a homomorphic section $s : G^{\mathrm{ab}} \to G$. Inspecting individual Atlas pages [Conway et al. 1985] shows that this a priori strong condition is actually commonly satisfied. Similarly, we say that a pseudosimple group has *cyclic* type if G^{ab} is cyclic. Again this strong-seeming condition is commonly satisfied, as indeed for a simple group T all of $\mathrm{Out}(T)$ is often cyclic [Conway et al. 1985, Chapter 1, Table 1; Chapter 3, Table 5]. When both of these conditions are satisfied, we say that G is of *split-cyclic* type.

For G of split-cyclic type, the following proposition says that Condition 3 of Theorem 5.1 is equivalent to an apparent strengthening $\hat{3}$. Moreover, these two conditions are both equivalent to a more explicit condition E which makes no reference to either fiber powers or powers. For E, we modify the notions defined in Section 4B as follows:

$$H_2'(G)_{C_i} = \{\langle g, z\rangle : g \in C_i \text{ and } z \in Z(g) \cap G'\},$$
$$H_2'(G)_C = \sum H_2'(G)_{C_i}.$$

These are straightforward variants, as indeed if one removes every $'$ one recovers the definitions (4-1) and (4-2) of the previous notions.

Proposition 5.2. *Let G be a pseudosimple group of split-cyclic type, and let $C = (C_1, \ldots, C_r)$ be a list of distinct unambiguous conjugacy classes. Then the following are equivalent*:

3. $|H_2(G^{[2]}, C^2)| = |H_2(G, C)|^2$.

$\hat{3}$. $|H_2(G^{[k]}, C^k)| = |H_2(G, C)|^k$ *for all positive integers* k.

E. $H_2(G)_C = H_2'(G)_C$.

Moreover, if $|G^{\mathrm{ab}}|$ is relatively prime to $|H_2(G)|$ then all three conditions hold.

Proof. All three conditions involve the list C of conjugacy classes. We begin however with considerations involving G only. The k different coordinate projections $G^{[k]} \to G$ together induce a map $f_k : H_2(G^{[k]}) \to H_2(G)^k$. We first show that the assumption that G has split-cyclic type implies all the f_k are isomorphisms. We present this deduction in some detail because we will return to parts of it in Section 6E.

The map f_k is part of a morphism of five-term exact sequences (see [Eckmann and Stammbach 1970, Theorem 5.2], noting that $H_1(G') = 0$)

$$\begin{array}{ccccccccc} H_3(G^{[k]}) & \xrightarrow{\pi_3^{[k]}} & H_3(G^{\mathrm{ab}}) & \xrightarrow{\delta^{[k]}} & H_2(G'^k)_{G^{\mathrm{ab}}} & \xrightarrow{i_2^{[k]}} & H_2(G^{[k]}) & \xrightarrow{\pi_2^{[k]}} & H_2(G^{\mathrm{ab}}) \\ \downarrow & & \downarrow \Delta_3 & & \downarrow \simeq & & \downarrow f_k & & \downarrow \Delta_2 \\ H_3(G)^k & \xrightarrow{\pi_3^k} & H_3(G^{\mathrm{ab}})^k & \xrightarrow{\delta^k} & H_2(G')^k_{G^{\mathrm{ab}}} & \xrightarrow{i_2^k} & H_2(G)^k & \xrightarrow{\pi_2^k} & H_2(G^{\mathrm{ab}})^k \end{array} \tag{5-2}$$

Each five-term sequence arises from the Hochschild–Serre spectral sequence associated to an exact sequence of groups. The top sequence comes from the k-th fiber power of $G' \overset{i}{\hookrightarrow} G \overset{\pi}{\twoheadrightarrow} G^{\mathrm{ab}}$, while the bottom sequence comes from the k-th ordinary Cartesian power.

We note that (5-2) actually shows that $H_2(G^{[k]}, C^k) \to H_2(G, C)^k$ is surjective whenever G is pseudosimple and C consists of unambiguous classes. The point is that $H_2(G)_C$ surjects onto $H_2(G^{\mathrm{ab}})$. That is because $H_2(G^{\mathrm{ab}})$ is generated by symbols $\langle \alpha, \beta \rangle$. But such a symbol belongs to the image of $H_2(G)_C$, since the $[C_i]$ generate G^{ab} and, for any $g \in C_i$, the centralizer $Z(g)$ surjects to G^{ab} because C_i is unambiguous.

The assumption that $\pi : G \to G^{\mathrm{ab}}$ has a splitting s drastically simplifies (5-2). From $\pi \circ s = \mathrm{Id}_{G^{\mathrm{ab}}}$, one obtains that $\pi_3^{[k]} \circ s_3^{[k]}$ and $\pi_3^k \circ s_3^k$ are the identity on $H_3(G^{\mathrm{ab}})$ and $H_3(G^{\mathrm{ab}})^k$, respectively. Thus $\pi_3^{[k]}$ and π_3^k are both surjective and so the boundary maps $\delta^{[k]}$ and δ^k are both 0. Thus the part of (5-2) relevant for us becomes

$$\begin{array}{ccccc} H_2(G'^k)_{G^{\mathrm{ab}}} & \hookrightarrow & H_2(G^{[k]}) & \twoheadrightarrow & H_2(G^{\mathrm{ab}}) \\ \downarrow \simeq & & \downarrow f_k & & \downarrow \Delta_2 \\ H_2(G')^k_{G^{\mathrm{ab}}} & \hookrightarrow & H_2(G)^k & \twoheadrightarrow & H_2(G^{\mathrm{ab}})^k \end{array} \tag{5-3}$$

We have suppressed some notation, since we have no further use for it.

The assumption that G^{ab} is cyclic is equivalent to the assumption that $H_2(G^{\mathrm{ab}})$ is the zero group. Thus exactly in this situation one gets the independent simplification of (5-2) where the last column becomes the zero map between zero groups. Applied to (5-3) it says that $f_k : H_2(G^{[k]}) \to H_2(G)^k$ is an isomorphism. We henceforth use f_k to identify $H_2(G^{[k]})$ with $H_2(G)^k$.

We now bring in the list C of conjugacy classes. We have a morphism of short exact sequences

$$\begin{array}{ccccc} H_2(G^{[k]})_C & \hookrightarrow & H_2(G^{[k]}) & \twoheadrightarrow & H_2(G^{[k]}, C^k) \\ \downarrow \cap & & \| & & \downarrow \\ H_2(G)^k_C & \hookrightarrow & H_2(G)^k & \twoheadrightarrow & H_2(G, C)^k \end{array} \tag{5-4}$$

Since the map in the right column is surjective, Conditions 3 and $\hat{3}$ become that it is an isomorphism for $k = 2$ and all k respectively. So they are equivalent to the inclusion in the left column being equality, again for $k = 2$ and all k respectively. We work henceforth with these versions of Conditions 3 and $\hat{3}$.

Trivially

$$|H_2(G)_C| = |H_2'(G)_C| \cdot |H_2(G)_C / H_2'(G)_C|. \tag{5-5}$$

But also the image of $H_2(G^{[k]})_{C^k}$ in $(H_2(G)/H_2'(G)_C)^k$ is exactly the diagonal image of $H_2(G)_C/H_2'(G)_C$. To see this, note that $H_2(G^{[k]})_{C^k}$ is generated by

$$(\langle g, z_1\rangle, \dots, \langle g, z_k\rangle),$$

where $g \in \bigcup C_i$, each $z_i \in Z(g)$, and $z_1 \equiv \cdots \equiv z_k$ modulo G'. In particular, it certainly contains the diagonal image of $H_2(G)_C$. On the other hand, the images of $\langle g, z_i\rangle$ inside $H_2(G)_C/H_2'(G)_C$ are equal to each other, since $\langle g, z_i z_j^{-1}\rangle \in H_2'(G)_C$.

Moreover, $H_2'(G)_C^k \subseteq H_2(G^{[k]})_{C^k}$. This inclusion holds because, for any $g \in C_i$ and $z \in Z(g) \cap G'$, we have

$$(\langle g, z\rangle, 0, 0, \dots) \in H_2(G^{[k]})_{C^k},$$

since we can regard the left-hand side as $(\langle g, z\rangle, \langle g, e\rangle, \langle g, e\rangle, \dots)$, and similarly for any other "coordinate". Therefore,

$$|H_2(G^{[k]})_{C^k}| = |H_2'(G)_C|^k \cdot |H_2(G)_C / H_2'(G)_C|. \tag{5-6}$$

Dividing the k-th power of (5-5) by (5-6), one gets

$$\frac{|H_2(G)_C|^k}{|H_2(G^{[k]})_{C^k}|} = |H_2(G)_C/H_2'(G)_C|^{k-1}. \tag{5-7}$$

Condition 3 says the left side is 1 for $k = 2$. Condition $\hat{3}$ says the left side is 1 for all k. Equation (5-7) says that each of these is equivalent to $H_2(G)_C = H_2'(G)_C$, which is exactly Condition E.

For the final statement, $|H_2(G)_{C_i}/H_2'(G)_{C_i}|$ clearly divides $|H_2(G)|$. It also divides $|G^{\mathrm{ab}}|$, because $Z(g)/(Z(g) \cap G')$ surjects onto $H_2(G)_{C_i}/H_2'(G)_{C_i}$ via $z \in Z(g) \mapsto \langle g, z\rangle$, for any fixed $g \in C_i$. So, if $|H_2(G)|$ and $|G^{\mathrm{ab}}|$ are relatively prime then $H_2(G)_{C_i} = H_2'(G)_{C_i}$ always, and so Condition E holds. □

5E. ***The homological condition for G of split-p-p type.*** For p a prime, we say that a pseudosimple group G has *split-p-p* type if $G \to G^{\mathrm{ab}}$ is split and

$$|G^{\mathrm{ab}}| = |H_2(G)| = p.$$

Even this seemingly very special case is common. For example, taking $p = 2$, it includes

- all six extensions $T.A$ of sporadic groups T with A and $H_2(T.A)$ nontrivial,
- all S_d with $d \geq 5$, and
- all $\mathrm{PGL}_2(q)$ for odd $q \geq 5$.

To illustrate the tractability of Condition E of Proposition 5.2, we work it out explicitly for groups G of split-p-p type. Explicating Condition E for the full split-cyclic case would be similar but combinatorially more complicated.

For G of split-p-p type, we divide its unambiguous classes into three types. Let $\widetilde{G}$ be a Schur cover of G. An unambiguous class C is *split* if its preimage $\widetilde{C}$ consists of p conjugacy classes in $\widetilde{G}$. It is *mixed* if $\widetilde{C}$ is p different $\widetilde{G}'$ conjugacy classes but just one $\widetilde{G}$ class. Otherwise a class C is *inert*. Mixed classes are necessarily in the derived group, but split and inert classes can lie above any element of G^{ab}.

Corollary 5.3. *Let G be a pseudosimple group of split-p-p type and let $C = (C_1, \ldots, C_r)$ be a list of unambiguous classes. Then Condition E fails exactly when there are no inert classes and at least one mixed class among the C_i.*

Proof. We are considering subgroups of the p-element Schur multiplier $H_2(G)$. The subgroups have the following form:

C_i	split	mixed	inert
$H_2'(G)_{C_i}$	0	0	$H_2(G)$
$H_2(G)_{C_i}$	0	$H_2(G)$	$H_2(G)$

Thus $H_2'(G)_C = \sum_i H_2'(G)_{C_i}$ is a proper subgroup of $H_2(G)_C = \sum_i H_2(G)_{C_i}$ exactly under the conditions stated in the corollary. □

For a group $T.p$, the types of classes can be determined from an Atlas-style character table, including its lifting row and fusion column. For example, for the six sporadic T mentioned above, the mixed classes in $T.2$ are exactly as follows:

$\mathrm{Mathieu}_{12}$	$\mathrm{Mathieu}_{22}$	Hall–Janko	Higman–Sims	Suzuki	$\mathrm{Fischer}_{22}$
10A	8A	8A	4A, 6A, 12A	12D, 12E, 24A	(15 classes)

In the sequences S_d and $\mathrm{PGL}_2(q)$, the patterns evident from character tables in the first few instances can be proved to hold in general. Namely for S_d, conjugacy classes are indexed by partitions of d. The type of a class C_λ can be read off from two features of the indexing partition λ, the number e of even parts and whether or

not all parts are distinct:

	$e=0$	$e\in\{2,4,6,\dots\}$	$e\in\{1,3,5,\dots\}$
all distinct	ambiguous	mixed	split
not all distinct	split	inert	inert

Thus S_5 has no mixed classes while C_{42} and C_{421} are the unique mixed classes of S_6 and S_7 respectively. For $\mathrm{PGL}_2(q)$ with q odd, the division is even easier: the two classes of order the prime dividing q are ambiguous, the two classes of order 2 are inert, and all other classes are split. Thus for these $\mathrm{PGL}_2(q)$, the homological condition always holds.

6. Proof of I $\Longrightarrow$ II

In this section we prove the implication I $\Longrightarrow$ II of Theorem 5.1. Thus we consider Hurwitz parameters $h=(G,C,\nu)$ for fixed (G,C) satisfying Conditions 1–3 and varying ν. We then prove that the action of Br_ν on $\mathcal{F}_h^*$ is quasifull whenever $\min_i \nu_i$ is sufficiently large.

6A. ***A Goursat lemma.*** The classical Goursat lemma classifies certain subgroups of powers of a simple group. We state and prove a generalized version here. As usual, if one has groups G_1, G_2 endowed with homomorphisms π_1, π_2 to a third group Q, we say that G_1 and G_2 are isomorphic *over* Q if there is an isomorphism $i: G_1\to G_2$ satisfying $\pi_2 i=\pi_1$.

Lemma 6.1 (generalized Goursat lemma). *Suppose that G is pseudosimpleand $H\subseteq G^{[k]}$ is a "Goursat subgroup" in the sense that it surjects onto each coordinate factor. Then*:

(1) *H is itself isomorphic over G^{ab} to $G^{[w]}$ for some $w\le k$.*

(2) *There is a surjection $f:[1,k]\to[1,w]$ and automorphisms $\varphi_1,\dots,\varphi_k$ of G over G^{ab} such that H is the image of $G^{[w]}$ under*

$$(g_1,\dots,g_w)\mapsto(\varphi_1(g_{f(1)}),\dots,\varphi_k(g_{f(k)})).$$

Proof. We first prove (1) by induction, the base case $k=1$ being trivial. Note that the projection $\overline{H}=\pi_2(H)$ of H to the second factor in

$$G^{[k]}=G\times_{G^{\mathrm{ab}}}G^{[k-1]}$$

is also a Goursat subgroup. By induction, it is G^{ab}-isomorphic to $G^{[v]}$ for suitable v. The kernel $K=\ker(\pi_2)$ of the projection $H\to\overline{H}$ maps, under the first projection π_1, to a subgroup $\overline{K}\subseteq G'$ that is invariant under conjugation by G. In particular, either $\overline{K}$ is trivial, and we're done by induction, or $\overline{K}=G'$. In the latter case, we will show that $H=G\times_{G^{\mathrm{ab}}}\overline{H}$: Take any element $(m^*,\mu)\in G\times_{G^{\mathrm{ab}}}\overline{H}$. By

assumption, there exists m in G such that $(m, \mu) \in H$, but then m and m^* have the same projection to G^{ab}, and so

$$(m^*, \mu) = (m^* m^{-1}, 1) \cdot (m, \mu)$$

lies in H also. This concludes the proof of the first assertion: H is isomorphic to $G^{[w]}$ over G^{ab} for some w.

Now we deduce (2) from (1). Let $\Theta = G^{[w]} \to H$ be any isomorphism and write $\Theta(g) = (\theta_1(g), \dots, \theta_k(g))$. We need to show that, for each i, one can express $\theta_i(g)$ in the form $\varphi_i(g_{f(i)})$ as in (2). In other words, letting $\pi_j : G^{[w]} \to G$ be the j-th projection, we need to show that any surjective morphism $\theta : G^{[w]} \to G$ over G^{ab} factors as $\varphi\pi_j$ for some $j \in \{1, \dots, w\}$ and some automorphism $\varphi : G \to G$ over G^{ab}.

So let $\theta : G^{[w]} \to G$ be any surjective morphism over G^{ab}. Its kernel K is a normal subgroup of $(G')^w$, invariant under $G^{[w]}$, and with index $|G'|$. Now, via the isomorphism $G' \simeq T^u$ for some nonabelian simple group T, the normal subgroups of $(G')^w \simeq T^{uw}$ are of the form $T_I = \prod_{(i,j)\in I} T_{(i,j)}$, where I is a subset of $P = \{1, \dots, u\} \times \{1, \dots, w\}$. The normal subgroups which are invariant under G^w are those for which the indexing set I is invariant under the natural action of G^{ab}. The orbits of G^{ab} on P are the sets $P_j = \{1, \dots, u\} \times \{j\}$. So the kernel K of θ necessarily has the form T_{P-P_j} for some j. Thus K is also the kernel of the coordinate projection π_j. The unique bijection $\varphi : G \to G$ satisfying $\theta = \varphi\pi_j$ is then an automorphism of G over G^{ab}. □

6B. ***Identifying braid orbits.*** For F a set and k a positive integer we let

$$F^{\underline{k}} = \{(x_1, \dots, x_k) : \text{all } x_i \text{ are different}\}.$$

If F has cardinality N then $F^{\underline{k}}$ has cardinality $N^{\underline{k}} := N(N-1)\cdots(N-k+1)$. In this subsection we assume Conditions 1 and 2 of Statement I in Theorem 5.1 and identify the quotient set $(\mathcal{F}_h^*)^{\underline{k}}/\operatorname{Br}_v$ asymptotically.

Begin with $x_1, \dots, x_k \in \mathcal{F}_h^*$. Choose a set of representatives $\underline{g}_1, \dots, \underline{g}_k \in \mathcal{G}_h$. Writing each $\underline{g}_i$ as a column vector, we get a matrix

$$(\underline{g}_1, \dots, \underline{g}_k) = \begin{pmatrix} g_{11} & g_{21} & \cdots & g_{k1} \\ g_{12} & g_{22} & \cdots & g_{k2} \\ g_{13} & g_{23} & \cdots & g_{k3} \\ \vdots & \vdots & \ddots & \vdots \\ g_{1n} & g_{2n} & \cdots & g_{kn} \end{pmatrix}. \tag{6-1}$$

So, simply recalling our context:

- All the g_{ij} in a given row are in the same conjugacy class of G.
- These conjugacy classes are

$$\underbrace{C_1, \ldots, C_1}_{\nu_1}; \ \ldots \ ; \underbrace{C_r, \ldots, C_r}_{\nu_r}$$

  as one goes down the rows, so that a given row is in some C_i^k.
- Each column in its given order multiplies to 1.
- Each column generates all of G.

All entries in a given row certainly have the same projection to G^{ab}, and so each row defines an element of $G^{[k]}$. Consider now the subgroup H of $G^{[k]}$ generated by the rows of this matrix. We are going to show that

$$H = G^{[k]} \iff \text{all } x_i \text{ are different.} \tag{6-2}$$

First of all, note that the condition that $H = G^{[k]}$ is independent of the choice of lifting from $\mathcal{F}_h^*$ to $\mathcal{G}_h$. For example, if we modify $\underline{g}_1$, the first column of (6-1), by an element $\alpha \in \mathrm{Aut}(G, C)$, then the subgroup generated by the rows simply changes by the automorphism $(\alpha, 1, 1, 1 \ldots, 1)$ of $G^{[k]}$. Note that α is automatically an isomorphism of G over G^{ab} because it preserves each C_i and they generate G^{ab}.

Now the $\Longrightarrow$ direction of (6-2) is easy: if $x_i = x_j$ for some $i \neq j$, then we could lift so that $\underline{g}_i = \underline{g}_j$, and then certainly $H \subsetneq G^{[k]}$.

Now suppose that $x_i \neq x_j$ for all $i \neq j$; we'll show that $H = G^{[k]}$. Since each column generates G, the subgroup H is a Goursat subgroup of $G^{[k]}$. Accordingly we may apply Lemma 6.1, and see that H can be constructed from a surjective function $f : [1, k] \to [1, w]$ together with a system of isomorphisms $\varphi_j : G \to G$ over G^{ab}, for $1 \leq j \leq k$. In particular, we may find $(y_1, \ldots, y_w) \in G^{[w]}$ which maps to the first row $(g_{11}, g_{21}, \ldots, g_{k1})$, so that

$$\varphi_j(y_{f(j)}) = g_{j1}, \quad 1 \leq j \leq k.$$

In particular, whenever $f(j) = f(j')$, the map

$$\varphi_{j'} \varphi_j^{-1}$$

carries g_{j1} to $g_{j'1}$ and so preserves C_1. By similar reasoning, applied to the second row, third row and so on, this map preserves *every* conjugacy class, so

$$\varphi_{j'} \varphi_j^{-1} \in \mathrm{Aut}(G, C)$$

whenever $f(j) = f(j')$. But $\varphi_{j'} \varphi_j^{-1}$ carries g_{ji} to $g_{j'i}$; that means that actually $x_j = x_j'$, and so $j = j'$. In other words, f is injective, and so $H \simeq G^{[k]}$, as desired.

Each matrix of the form (6-1) with H all of $G^{[k]}$ defines an element of $\mathcal{G}_{h^k}$. Now, the group $\mathrm{Aut}(G,C)^k$ acts on $G^{[k]}$; its image in the outer automorphism group will be called $\mathrm{Out}(G,C)^{[k]}$. This latter group maps onto $\mathrm{Out}(G,C)^k$, with kernel isomorphic to $(G^{\mathrm{ab}})^{k-1}$. These considerations give a bijective map

$$\mathcal{F}_{h^k}/\mathrm{Out}(G,C)^{[k]} \xrightarrow{\sim} \mathcal{F}_h^{*\underline{k}}. \tag{6-3}$$

This bijection is purely algebraic in nature and is valid for all ν.

Lifting invariants give a map $\mathcal{F}_{h^k}/\mathrm{Br}_\nu \to H_2(G^{[k]}, C^k, \nu)$. For any fixed k, the Conway–Parker theorem says that this map is asymptotically a bijection. Taking the quotient by $\mathrm{Out}(G,C)^{[k]}$ and incorporating the Goursat conclusion (6-3), we get the desired description of braid orbits:

$$\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \underset{a}{\xrightarrow{\sim}} H_2(G^{[k]}, C^k, \nu)/\mathrm{Out}(G,C)^{[k]}. \tag{6-4}$$

The map of (6-4) is defined for all allowed ν and, as indicated by the notation $\underset{a}{\xrightarrow{\sim}}$, is asymptotically a bijection.

There is, of course, a map $\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \to (\mathcal{F}_h^*/\mathrm{Br}_\nu)^k$; on the right-hand side of (6-4), this corresponds to the natural map

$$H_2(G^{[k]}, C^k, \nu)/\mathrm{Out}(G,C)^{[k]} \to (H_2(G,C,\nu)/\mathrm{Out}(G,C))^k. \tag{6-5}$$

Note that the action of $\mathrm{Out}(G,C)^{[k]}$ on $H_2(G^{[k]}, C^k, \nu)$ factors, under the coordinate projection $H_2(G^{[k]}, C^k, \nu) \to H_2(G,C,\nu)$, through the corresponding coordinate projection $\mathrm{Out}(G,C)^{[k]} \to \mathrm{Out}(G,C)$.

6C. ***End of the proof of I $\Longrightarrow$ II in the split-cyclic case.*** We now assume not only Conditions 1 and 2 of I, but also Condition 3. In this subsection, we complete the proof of I $\Longrightarrow$ II under the auxiliary assumption that the surjection $G \to G^{\mathrm{ab}}$ is split and G^{ab} is cyclic. Some of the notions introduced here are used again in Section 6E, where we complete the proof without auxiliary assumptions.

Consider the canonical surjections $H_2(G^{[k]}, C^k, \nu) \twoheadrightarrow H_2(G,C,\nu)^k$. Under our auxiliary assumption that G has split-cyclic type, Condition 3 and Proposition 5.2 show that

$$|H_2(G^{[k]}, C^k)| = |H_2(G,C)|^k$$

for all k. Thus, since cardinality does not change when one passes from groups to torsors, the surjections are bijections. Moreover, because inner automorphisms act trivially on $H_2(G,C,\nu)$, the action of $\mathrm{Out}(G,C)^{[k]}$ on $H_2(G,C,\nu)^k$ actually factors through $\mathrm{Out}(G,C)^k$.

Taking the quotient by $\mathrm{Out}(G,C)^{[k]}$, we can rewrite (6-4) as

$$\mathcal{F}_h^{*\underline{k}}/\mathrm{Br}_\nu \underset{a}{\xrightarrow{\sim}} H_2^*(G,C,\nu)^k. \tag{6-6}$$

Then standard group theory shows that the action of Br_ν on $\mathcal{F}_h^*$ is quasifull for sufficiently large $\min_i \nu_i$:

In general, consider a permutation group $B \subseteq \mathrm{Sym}(F)$ with orbit decomposition $F = \bigsqcup_{i=1}^{s} F_i$. Suppose each orbit F_i has size at least k. Then the induced action of B on $F^{\underline{k}}$ has at least s^k orbits. If equality holds, then the images $B_i \subseteq \mathrm{Sym}(F_i)$ of B are each individually k-transitive. If $k \geq 6$, then the classification of finite simple groups says that B_i contains $\mathrm{Alt}(F_i)$. Still assuming that B has exactly s^k orbits on $F^{\underline{k}}$, it is then elementary that B contains $\mathrm{Alt}(F_1) \times \cdots \times \mathrm{Alt}(F_s)$. In other words, B is quasifull, as desired.

6D. ***A lemma on 2-transitive groups.*** For the general case, Condition 3 gives us control over Br_ν-orbits only on pairs (x_1, x_2) of distinct elements in $\mathcal{F}_h^*$, not tuples of larger length. To deal with this problem, we replace the classification of multiply transitive groups by a statement derived from the classification of 2-transitive groups. The exact formulation of our lemma is inessential; its import is that full groups are clearly separated out from other 2-transitive groups in a way sufficient for our purpose.

Lemma 6.2. *Fix an odd integer $j \geq 5$ and a finite set X. Suppose a 2-transitive group $\Gamma \subseteq \mathrm{Sym}(X)$ satisfies $|X^{\underline{2j}}/\Gamma| \leq 2^{j^2-4j}$. If $|X|$ is sufficiently large, then Γ is full.*

Proof. To prove the statement, we use the classification of nonfull 2-transitive groups, as presented in [Dixon and Mortimer 1996, §7.7], thereby breaking our argument into a finite number of cases. For fixed j, we discard in each case a finite number of Γ and establish $|X^{\underline{2j}}/\Gamma| > 2^{j^2-4j}$ for all other Γ.

It suffices to restrict attention to maximal nonfull 2-transitive groups Γ. Besides a small number of examples involving seven of the sporadic groups [Dixon and Mortimer 1996, pp. 252–253], every such maximal Γ occurs in the following table:

#	type	Γ	degree $N := \lvert X\rvert$	order $\lvert\Gamma\rvert$
1	affine	$\mathrm{AGL}_d(p)$	p^d	
2	projective	$\mathrm{P\Gamma L}_d(q)$	$(q^d-1)/(q-1)$	
3	OS2	$O_{2d+1}(2)$	$2^d(2^d \pm 1)/2$	
4	unitary	$U_3(q)$	q^3+1	$q^3(q^2-1)(q^3+1)$
5	Suzuki	$Sz(q)$	q^2+1	$(q^2+1)q^2(q-1)$
6	Ree	$R(q)$	q^3+1	$(q^3+1)q^3(q-1)$

The six series are listed in the order they are treated in [Dixon and Mortimer 1996, pp. 244–252], with $d \geq 1$ and $d \geq 2$ in Cases 1 and 2 respectively. Throughout, p is a prime number and $q = p^e$ is a prime power. These numbers are arbitrary, except in Cases 5 and 6, where the base is $p = 2$ and $p = 3$ respectively and the

exponent e is odd. The orders $|\Gamma|$ in Cases 1–3 are not needed in our argument and so are omitted from the table.

Cases 4–6. In these cases, the order $|\Gamma|$ grows only polynomially in the degree N, with $|\Gamma| < N^3$ holding always. One has

$$|X^{\underline{2j}}/\Gamma| \geq N^{\underline{2j}}/|\Gamma| > N^{\underline{2j}}/N^3.$$

For $j \geq 5$ fixed and $N \to \infty$, the right side tends to ∞. So, with finitely many exceptions, $|X^{\underline{2j}}/\Gamma| > 2^{j^2-4j}$.

Case 1. In this case, the affine general linear group $\mathrm{AGL}_d(\mathbb{F}_p)$ acts on the affine space $\mathbb{F}_p^d$. Let $w = \min(j, d+1)$. Fix $x_1, \ldots, x_w$ in $\mathbb{F}_p^d$ spanning an affine subspace A of dimension $w-1$. The set $A - \{x_1, \ldots, x_w\}$ has $p^{w-1} - w$ elements. There are $(p^{w-1}-w)^{\underline{2j-w}}$ ways to successively choose $x_{w+1}, \ldots, x_{2j}$ in A so that all the x_i are distinct. The tuples $(x_1, \ldots, x_{2j}) \in (\mathbb{F}_p^d)^{\underline{2j}}$ so obtained are in different $\mathrm{AGL}_d(\mathbb{F}_p)$-orbits. Thus

$$|(\mathbb{F}_p^d)^{\underline{2j}}/\mathrm{AGL}_d(\mathbb{F}_p)| \geq (p^{w-1}-w)^{\underline{2j-w}}.$$

For fixed $d < j$, so that $w = d+1$, the right side tends to ∞ with p, and so with finitely many exceptions $|(\mathbb{F}_p^d)^{\underline{2j}}/\mathrm{AGL}_d(\mathbb{F}_p)| > 2^{j^2-4j}$. For $d \geq j$, so that $w = j$, one gets no exceptions, as

$$(p^{w-1}-w)^{\underline{2j-w}} = (p^{j-1}-j)^{\underline{j}} \geq (2^{j-1}-j)^{\underline{j}} \geq (2^{j-1}-2j+1)^j > 2^{j^2-4j}.$$

(Case 1 is the only case where there is a complicated list of nonmaximal 2-transitive groups. Some large ones are $\mathrm{AGL}_{d/e}(\mathbb{F}_{p^e}) \subset \mathrm{A\Gamma L}_{d/e}(\mathbb{F}_{p^e}) \subset \mathrm{AGL}_d(p)$, for any e properly dividing d.)

Cases 2 and 3 are very similar to Case 1, but are sufficiently different to require separate treatments.

Case 2. Here $\Gamma = \mathrm{P\Gamma L}_d(\mathbb{F}_q) = \mathrm{PGL}_d(\mathbb{F}_q).\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ acts on the projective space $X = \mathbb{P}^{d-1}(\mathbb{F}_q)$. Again let $w = \min(j, d+1)$. Fix $x_1, \ldots, x_w$ in $\mathbb{P}^{d-1}(\mathbb{F}_q)$ spanning a projective subspace P of dimension $w-1$. Similarly to Case 1, there are $((q^w-1)/(q-1)-w)^{\underline{2j-w}}$ ways to successively choose $x_{w+1}, \ldots, x_{2j}$ in P so that all the x_i are distinct. The tuples $(x_1, \ldots, x_{2j}) \in \mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}$ so obtained are in different $\mathrm{PGL}_d(\mathbb{F}_q)$-orbits. However one $\mathrm{P\Gamma L}_d(\mathbb{F}_q)$-orbit can consist of up to e different $\mathrm{PGL}_d(\mathbb{F}_q)$-orbits. Thus our lower bound in this case is

$$|\mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}/\mathrm{P\Gamma L}_d(\mathbb{F}_q)| \geq \frac{1}{e}\left(\frac{q^w-1}{q-1} - w\right)^{\underline{2j-w}}.$$

Again, the subcase $d < j$, where $w = d + 1$, is simple: the right side tends to ∞ with q and so $|\mathbb{P}^{d-1}(\mathbb{F}_q)^{\underline{2j}}/\mathrm{P\Gamma L}_d(\mathbb{F}_q)| > 2^{j^2-4j}$ holds with only finitely many exceptions. For $d \geq j$, so that $w = j$ again, one has no further exceptions since

$$\frac{1}{e}\left(\frac{q^w - 1}{q-1} - w\right)^{\underline{2j-w}} > \frac{1}{e}(q^{j-1} - 2j + 1)^j > (2^{j-1} - 2j + 1)^j > 2^{j^2-4j}.$$

Case 3. Here the group in question, in its most familiar guise, is $\Gamma = \mathrm{Sp}_{2d}(\mathbb{F}_2)$ for $d \geq 2$. It is better in our context to view $\Gamma = O_{2d+1}(\mathbb{F}_2)$, as from this point of view the 2-transitive actions appear most naturally. In fact, the orbit decomposition of the natural action of $O_{2d+1}(\mathbb{F}_2)$ is

$$\mathbb{F}_2^{2d+1} - \{0\} = X_{-1} \sqcup X_1 \sqcup X_0.$$

Here X_0 is the set of isotropic vectors. The pair $(O_{2d+1}(\mathbb{F}_2), X_0)$ is a copy of the more standard pair $(\mathrm{Sp}_{2d}(\mathbb{F}_2), \mathbb{F}_2^{2d} - \{0\})$, and so in particular $|X_0| = 2^{2d} - 1$. A nonisotropic vector is in X_1 if its stabilizer is the split orthogonal group $O^+_{2d}(\mathbb{F}_2)$ and is in X_{-1} if its stabilizer is the nonsplit orthogonal group $O^-_{2d}(\mathbb{F}_2)$. From the order of the stabilizers, one gets that $|X_\epsilon| = 2^{d-1}(2^d + \epsilon)$. While the action of Γ on $X_0^{\underline{2}}$ has two orbits, the actions on the other two X_ϵ are 2-transitive. (Familiar examples for $O_{2d+1}(\mathbb{F}_2) = \mathrm{Sp}_{2d}(\mathbb{F}_2)$ come from $d = 2$ and $d = 3$. Here the groups are S_6 and $W(E_7)$, respectively. The orbit sizes on (X_{-1}, X_1, X_0) are $(6, 10, 15)$ and $(28, 36, 63)$ respectively.)

By discarding a finite number of Γ, we can assume $d \geq j$. For $\epsilon \in \{\pm 1\}$, fix $x_1, \ldots, x_j$ in X_ϵ spanning a j-dimensional vector space $V \subset \mathbb{F}_2^{2d+1}$ on which the quadratic form remains nondegenerate and with each x_i having type ϵ in this smaller space. Let $V_\epsilon = V \cap X_\epsilon$. Writing $j = 2u + 1$, one has $|V_\epsilon| = 2^{u-1}(2^u + \epsilon)$. There are $(|V_\epsilon| - j)^{\underline{j}}$ ways to successively choose $x_{j+1}, \ldots, x_{2j}$ in V_ϵ so that all the x_i are distinct. One has

$$|X_\epsilon^{\underline{2j}}/O_{2d+1}(\mathbb{F}_2)| \geq (2^{u-1}(2^u + \epsilon) - j)^{\underline{j}} \geq (2^{u-1}(2^u + \epsilon) - 2j + 1)^j > 2^{j^2-4j}.$$

Thus there are no further exceptional Γ from this case. □

6E. ***End of the proof of I ⟹ II in general.*** We now end the proof without the split-cyclicity assumption, by modifying the standard argument of Section 6C.

Consider again the diagram (5-2) relating two five-term exact sequences. The last three terms of the top sequence and the last four terms of the bottom sequence give respectively

$$|H_2(G^{[k]})| \leq |H_2(G')_{G^{\mathrm{ab}}}|^k |H_2(G^{\mathrm{ab}})|,$$

$$|H_2(G')_{G^{\mathrm{ab}}}|^k \leq \frac{|H_3(G^{\mathrm{ab}})|^k |H_2(G)|^k}{|H_2(G^{\mathrm{ab}})|^k}.$$

Combining these inequalities and replacing $H_2(G^{[k]})$ by its quotient $H_2(G^{[k]}, C^k)$ yields

$$|H_2(G^{[k]}, C^k)| \leq |H_2(G) \times H_3(G^{\mathrm{ab}})|^k. \tag{6-7}$$

As described in Section 6C, Condition 3 implies that for $\min \nu_i$ sufficiently large, the action of Br_ν on $\mathcal{F}_h^*$ is 2-transitive when restricted to each orbit. We will use this 2-transitivity and the exponential bound (6-7) to conclude that the action of Br_ν on $\mathcal{F}_h^*$ is asymptotically quasifull.

Consider S_m in its standard full action on $Y_m = \{1, \dots, m\}$. The induced action on $X_m = Y_m \sqcup Y_m$ is not quasifull. Let $a_{k,m}$ be the number of orbits of S_m on $Y_m^{\underline{k}}$. As m increases, the sequence $a_{k,m}$ stabilizes at a number a_k. The sequence a_k appears in [Sloane 1991] as A000898. There are several explicit formulas and combinatorial interpretations. The only important thing for us is that a_k grows superexponentially, as indeed $a_k/a_{k-1} \sim \sqrt{2k}$.

From (6-7) we know that there exists an odd number j with

$$|H_2(G^{[2j]}, C^{2j}, \nu)/\operatorname{Out}(G, C)^{[2j]}| \leq |H_2(G^{[2j]}, C^{2j})| < \min(2^{j^2-4j}, a_{2j}).$$

By (6-4), the left-hand set is identified with $|\mathcal{F}_h^{*\underline{2j}} / \mathrm{Br}_\nu|$ for sufficiently large $\min_i \nu_i$. Lemma 6.2 above says that, at the possible expense of making $\min_i \nu_i$ even larger, each orbit of the action of Br_ν on $\mathcal{F}_h^*$ is full. Our discussion of the action of S_m on Y_m says that the constituents are pairwise nonisomorphic, again for sufficiently large $\min_i \nu_i$. The classical Goursat lemma then says the action is quasifull. □

A consequence of the results of this section is that in fact the equivalence $3 \iff \hat{3}$ of Proposition 5.2 holds without the assumption of split-cyclicity. Condition E is also meaningful in general, and it would be interesting to identify the class of (G, C) for which the equivalence extends to include E.

7. Proof of II $\Longrightarrow$ I

In this section, we complete the proof of Theorem 5.1 by proving that (not I) implies (not II). Accordingly, we fix a centerless group G and a list $C = (C_1, \dots, C_r)$ of conjugacy classes, and consider consequences of the failure of Conditions 1, 2, and 3 in turn. In all three cases, we show more than is needed for Theorem 5.1.

7A. ***Failure of Condition 1.*** The failure of the first condition requires a somewhat lengthy analysis, because it breaks into two quite different cases. The conclusion of the following lemma shows more than that asymptotic quasifullness of $\mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ fails; it shows that asymptotically each individual component $\mathsf{Hur}_{h,\ell}^* \to \mathsf{Conf}_\nu$ fails to be full.

Lemma 7.1. *Let G be a centerless group which is not pseudosimple. Let $C = (C_1, \dots, C_r)$ be a list of conjugacy classes. Consider varying allowed $\nu \in \mathbb{Z}^r_{\geq 1}$ and thus varying Hurwitz parameters $h = (G, C, \nu)$. Then for $\min_i \nu_i$ sufficiently large and any $\ell \in H_h^*$, the action of Br_ν on $\mathcal{F}^*_{h,\ell}$ is not full.*

Proof. A group is pseudosimple exactly when it satisfies two conditions: (A), it has no proper nonabelian quotients, or (B), its derived group is nonabelian. We assume first that (A) fails. Then we assume that (A) holds but (B) fails.

Assume (A) fails. Let $\overline{G}$ be a proper nonabelian quotient and $\overline{h} = (\overline{G}, (\overline{C}_1, \dots, \overline{C}_r), \nu)$ the corresponding quotient Hurwitz parameter. Consider the natural map $H_h \to H_{\overline{h}}$ from Section 4E, and let $\bar{\ell}$ be the image of ℓ.

By the definition of Hurwitz parameters, the classes C_i generate G. At least one of the surjections $C_i \to \overline{C}_i$ has to be noninjective, as otherwise the kernel of $G \to \overline{G}$ would be central in G and G is centerless. So $|C_i| \geq 2|\overline{C}_i|$ for at least one i. Similarly, since $\overline{G}$ is nonabelian and generated by the $\overline{C}_i$, one has $|\overline{C}_i| \geq 2$ for at least one i.

We now examine the induced map $\mathcal{G}_{h,\ell} \to \mathcal{G}_{\overline{h},\bar{\ell}}$. Let $\mathcal{I}_{h,\ell}$ be its image and $\phi_{h,\ell}$ the size of its largest fiber. We will use the two inequalities of the previous paragraph to show that both $\phi_{h,\ell}$ and $|\mathcal{I}_{h,\ell}|$ grow without bound with $\min_i \nu_i$.

From $|C_i| \geq 2|\overline{C}_i|$ and two applications of the asymptotic mass formula (3-7), one gets $|\mathcal{G}_{h,\ell}| \geq 1.5^{\min_i \nu_i} |\mathcal{G}_{\overline{h},\bar{\ell}}|$, and hence $\phi_{h,\ell} \geq 1.5^{\min_i \nu_i}$.

To show the growth of $|\mathcal{I}_{h,\ell}|$, we assume without loss of generality that $|\overline{C}_1| \geq 2$, and choose $y_1 \neq y_2 \in \overline{C}_1$. Let M be the exponent of a reduced Schur cover $\widetilde{G}_C$ of G. Let k be a positive integer and let $a_1, \dots, a_k$ be a sequence with $a_i \in \{1, 2\}$. Then for $\min_i \nu_i$ large enough, we claim that $\mathcal{I}_{h,\ell}$ contains an element of the form

$$(\underbrace{y_{a_1}, \dots, y_{a_1}}_{M}, \dots, \underbrace{y_{a_k}, \dots, y_{a_k}}_{M}, \underbrace{x_1, \dots, x_{\nu_1 - Mk}}_{\text{all in } \overline{C}_1}, \dots, \underbrace{x_{n-kM-\nu_r+1}, \dots, x_{n-kM}}_{\text{all in } \overline{C}_r}). \tag{7-1}$$

To see the existence of such an element, fix a lift C_i^* of the conjugacy class C_i to $\widetilde{G}_C$ and choose $\tilde{y}_1, \tilde{y}_2 \in C_1^*$ mapping (under $\widetilde{G}_C \to G \to \overline{G}$) to $y_1, y_2 \in \overline{C}_1$ respectively.

Let $z \in H_2(G, C)$ be chosen so that $z^{-1} \cdot \prod_i [C_i]^{\nu_i} = \ell$ inside $H_2(G, C, \nu)$. Consider the equation

$$(\tilde{y}_{a_1}^M \cdots \tilde{y}_{a_k}^M) \underbrace{\tilde{x}_1 \cdots \tilde{x}_{\nu_1 - kM}}_{\text{all in } C_1^*} \cdots \underbrace{\tilde{x}_{n-kM-\nu_r+1} \cdots \tilde{x}_{n-kM}}_{\text{all in } C_r^*} = z, \tag{7-2}$$

where $\tilde{x}_i \in C_i^*$. By our choice of M, the powers $\tilde{y}_{a_i}^M$ are all the identity in $\widetilde{G}_C$. One has $[C_1^*]^{\nu_1 - kM} \cdots [C_r^*]^{\nu_r} = [z]$ in $\widetilde{G}_C^{\mathrm{ab}} = G^{\mathrm{ab}}$, both sides being the identity. The asymptotic mass formula then applies to say that (7-2) in fact has

many solutions $(\tilde{x}_1, \ldots, \tilde{x}_{n-kM})$ where moreover the $\tilde{x}_i$ generate $\widetilde{G}_C$. Now, the image of $(\tilde{y}_{a_1}, \ldots, \tilde{y}_{a_k}, \tilde{x}_1, \ldots, \tilde{x}_{n-kM})$ actually defines an element of $\mathcal{G}_{h,\ell}$, and its image in $\overline{G}$ is an element of $\mathcal{I}_{h,\ell}$ of the form (7-1). Varying $(a_1, \ldots, a_k)$ now, always taking $\min_i \nu_i$ sufficiently large, we conclude $|\mathcal{I}_{h,\ell}| \geq 2^k$.

For large enough $\min_i \nu_i$, the action of Br_ν on $\mathcal{G}_{h,\ell}$ is transitive, by the Conway–Parker theorem. This action preserves a partition of $\mathcal{G}_{h,\ell}$ into $b = |\mathcal{I}_{h,\ell}|$ blocks, each of size $f = \phi_{h,\ell}$. Thus the image of Br_ν on $\mathcal{G}_{h,\ell}$ is contained in the wreath product $S_f \wr S_b$. Hence the image of Br_ν on $\mathcal{F}^*_{h,\ell}$ is contained in a subquotient of $S_f \wr S_b$. But we have established that f and b increase indefinitely with $\min_i \nu_i$. Let $a = |\mathrm{Aut}(G, C)_\ell|$ and $m = |\mathcal{F}^*_{h,\ell}|$, so that $|\mathcal{G}_{h,\ell}| = ma = fb$. As soon as $\min(f, b) > a$, one has $m > \max(f, b)$ and the alternating group A_m is not a subquotient of $S_f \wr S_b$. So the action of Br_ν on $\mathcal{F}^*_{h,\ell}$ is not full.

Assume (A) holds but (B) fails. The assumptions force G' to be isomorphic to the additive group of $\mathbb{F}_p^w$ for some prime p and some power w. Moreover, consider the action of G^{ab} on G'. Now G', considered as an $\mathbb{F}_p$-vector space, is an irreducible representation of $\mathbb{F}_p[G^{\mathrm{ab}}]$. The order of G^{ab} must be coprime to p, as otherwise the fixed subspace for the p-primary part of G^{ab} would be a proper subrepresentation. So $\mathbb{F}_p[G^{\mathrm{ab}}]$ is isomorphic to a sum of finite fields and the action on $G' = \mathbb{F}_p^w$ is through a single summand $\mathbb{F}_q$. We can thus identify G' with the additive group of a finite field $\mathbb{F}_q$ and G^{ab} with a subgroup of $\mathbb{F}_q^\times$ in such a way that G itself is a subgroup of the affine group $\mathbb{F}_q.\mathbb{F}_q^\times$. Moreover, $G^{\mathrm{ab}} \subseteq \mathbb{F}_q^\times$ acts irreducibly on $\mathbb{F}_q$ as an $\mathbb{F}_p$-vector space.

We think of elements of G as affine transformations $x \mapsto mx + b$. Since braid groups act on the right in (3-2), we compose these affine transformation from left to right, so that the group law is

$$\binom{m_1}{b_1}\binom{m_2}{b_2} = \binom{m_1 m_2}{m_2 b_1 + b_2}.$$

We think of elements $(g_1, \ldots, g_n) \in \mathcal{G}_h$ with $g_i = \binom{m_i}{b_i}$ in terms of the matrix

$$\begin{pmatrix} m_1 & \ldots & m_i & m_{i+1} & \ldots & m_n \\ b_1 & \ldots & b_i & b_{i+1} & \ldots & b_n \end{pmatrix}. \tag{7-3}$$

The top row is determined by C, via $m_i = [C_i]$. Thus, via the bottom row, we have realized $\mathcal{G}_h$ as a subset of $\mathbb{F}_q^n$. We can assume without loss of generality that none of the C_i are the identity class. Then the requirement $g_i \in C_i$ for membership in $\mathcal{G}_h$ gives $|G^{\mathrm{ab}}|$ choices for b_i if $m_i = 1$. If $m_i \neq 1$ then $g_i \in C_i$ allows all q choices for b_i.

Now briefly view $(g_1, \ldots, g_n)$ as part of the larger catch-all set G^n of Section 3C, on which the standard braid operators σ_i act. The braiding rule (3-2) in our current

setting becomes

$$\left(\ldots,\binom{m_i}{b_i},\binom{m_{i+1}}{b_{i+1}},\ldots\right)^{\sigma_i}=\left(\ldots,\binom{m_{i+1}}{b_{i+1}},\binom{m_i}{b_{i+1}+m_{i+1}b_i-m_ib_{i+1}},\ldots\right).$$

Thus the action of σ_i corresponds to the bottom row of (7-3), viewed as row vector of length n, being multiplied on the right by an n-by-n matrix in $GL_n(\mathbb{F}_q)$.

Returning now to the set $\mathcal{G}_h$ itself, any element of Br_ν can be written as a product of the σ_i and their inverses. Accordingly, image of Br_ν in $\mathrm{Sym}(\mathcal{G}_h)$ lies in $GL_n(\mathbb{F}_q)$.

To prove nonfullness, it suffices to bound the sizes of groups. On the one hand,

$$|\text{image of } \mathrm{Br}_\nu \text{ in } \mathrm{Sym}(\mathcal{F}^*_{h,\ell})| \le |\text{image of } \mathrm{Br}_\nu \text{ in } \mathrm{Sym}(\mathcal{G}_h)| \le |\,\mathrm{GL}_n(\mathbb{F}_q)| < q^{n^2}.$$

On the other hand, let $b = |H_2(G,C)||\mathrm{Out}(G,C)|+1$. Then, using (3-7), (4-6) and the fact that $|C_i| \in \{|G^{\mathrm{ab}}|, q\}$, one has

$$|\mathcal{F}^*_{h,\ell}| > \frac{\prod_i |C_i|^{\nu_i}}{|G||G'|b} \ge \frac{|G^{\mathrm{ab}}|^{n-3}}{q^2 b}$$

for all sufficiently large n. Certainly $q^{n^2} < \frac{1}{2}((a^{n-3})/(q^2b))!$ for any fixed a, b, $q>1$ and sufficiently large n. Thus the image of Br_ν in $\mathrm{Sym}(\mathcal{F}^*_{h,\ell})$ cannot contain $\mathrm{Alt}(\mathcal{F}^*_{h,\ell})$. □

The paper [Eisenbud et al. 1991] calculates monodromy in cases with $G = S_3$ and $G = S_4$, providing worked-out examples. Another illustration of the case with affine monodromy is [Malle and Matzat 1999, Proposition 10.4].

7B. ***Failure of Condition 2.*** Our next lemma has the same conclusion as the previous lemma:

Lemma 7.2. *Let G be a centerless group. Let $C = (C_1,\ldots,C_r)$ be a list of conjugacy classes with at least one C_i ambiguous. Consider varying allowed $\nu \in \mathbb{Z}^r_{\ge 1}$ and thus varying Hurwitz parameters $h = (G,C,\nu)$. Then for $\min_i \nu_i$ sufficiently large and any $\ell \in H_h^*$, the action of Br_ν on $\mathcal{F}^*_{h,\ell}$ is not full.*

Proof. Introduce indexing sets B_i by writing

$$C_i = \textstyle\bigsqcup_{b\in B_i} C_{ib},$$

where each C_{ib} is a single G'-orbit. Our hypothesis says that at least one of the B_i — without loss of generality, B_1 — has size larger than 1. On the other hand, at least one of the B_i has size strictly less than C_i; otherwise G' would centralize each element of each C_i, and then all of G, which is impossible for G center-free.

Define

$$\mathcal{G}_h^{\mathrm{amb}} = \underbrace{B_1\times\cdots\times B_1}_{\nu_1}\times\cdots\times\underbrace{B_r\times\cdots\times B_r}_{\nu_r}.$$

The group G acts transitively through its abelianization G^{ab} on each B_i. For a lifting invariant $\ell \in H_h$, consider the natural map $\mathcal{G}_{h,\ell} \to \mathcal{G}_h^{\mathrm{amb}}$. The action of the braid group Br_ν on $\mathcal{G}_{h,\ell}$ descends to an action on $\mathcal{G}_h^{\mathrm{amb}}$.

Now we let $\min_i \nu_i \to \infty$ and get the following consequences, by arguments very closely paralleling those for the first case of Lemma 7.1. First, the image of the map $\mathcal{G}_{h,\ell} \to \mathcal{G}_h^{\mathrm{amb}}$ has size that goes to ∞. Second, the mass formula again shows that $|\mathcal{G}_{h,\ell}|/|\mathcal{G}_h^{\mathrm{amb}}| \to \infty$ with $\min_i \nu_i$. By the last paragraph of the first case of the proof of Lemma 7.1, the action of Br_ν on each orbit of $\mathcal{F}_{h,\ell}^*$ is forced to be imprimitive, and hence not full. □

For a contrasting pair of examples, consider $h = (S_5, (C_{2111}, C_{311}, C_5), \nu)$ for $\nu = (2, 2, 1)$ and $\nu = (2, 1, 2)$. The monodromy group for the former is all of S_{125}, despite the presence of the ambiguous class C_5. The monodromy group for the latter is $S_{85} \wr S_2$ and represents the asymptotically forced nonfullness.

7C. ***Failure of Condition 3.*** The last lemma of this section is different in structure from the previous two, and its proof is essentially a collection of some of our previous arguments. From the discussion of surjectivity after (5-2), one always has

$$|H_2(G^{[2]}, C^2)| = a|H_2(G, C)|^2 \tag{7-4}$$

for some positive integer a. Condition 3 is that $a = 1$. The number a reappears as the cardinality of every fiber of the map of torsors

$$H_2(G^{[2]}, C^2, \nu) \overset{\pi}{\twoheadrightarrow} H_2(G, C, \nu)^2$$

considered in Section 4E.

Now suppose that ν is such that all ν_i are divisible by both the exponent of $H_2(G, C)$ and the exponent of $H_2(G^{[2]}, C^2)$. In that case, we have identifications

$$\begin{array}{ccc} H_2(G^{[2]}, C^2, \nu)_f & \xrightarrow{\pi} & H_2(G, C, \nu)_g^2 \\ \downarrow & & \downarrow \\ H_2(G^{[2]}, C^2) & \longrightarrow & H_2(G, C)^2 \end{array} \tag{7-5}$$

where the vertical bijections f, g come from Section 4C, and the fact that the diagram commutes is also explained there. The set $E := \pi^{-1} g^{-1}(0) \subseteq H_2(G^{[2]}, C^2, \nu)$ is a fiber of π. It has size ≥ 2 and $f(E) \subseteq H_2(G^{[2]}, C^2)$ is a subgroup.

The group $\mathrm{Out}(G, C)^{[2]}$, defined before (6-3), acts on $H_2(G^{[2]}, C^2, \nu)$ and also (compatibly) on $H_2(G^{[2]}, C^2)$. It preserves E and acts on it with at least two orbits, because it fixes the zero element of $f(E)$. Under the bijection (6-4), these two orbits correspond to two different braid orbits O, O' on $(\mathcal{F}_h^*)^{\underline{2}}$ which project (in both coordinates) to the same braid orbit on $\mathcal{F}_h^*$.

Summarizing, we have proved:

Lemma 7.3. *Let G be a pseudosimple group, let $C = (C_1, \dots, C_r)$ be a list of unambiguous conjugacy classes, and suppose $a > 1$ in* (7-4). *Consider ν with each ν_i a multiple of the exponent of both $H_2(G, C)$ and $H_2(G^{[2]}, C^2)$ so that $H_h^* = H_2(G, C, \nu)$ contains a trivial lifting invariant* 0 *via f from* (7-5). *Then for* $\min_i \nu_i$ *sufficiently large, the action of* Br_ν *on $\mathcal{F}_{h,0}^*$ is not* 2*-transitive and hence not full.*

8. Full number fields

The full-monodromy theorem gives us confidence in the following conjecture:

Conjecture 8.1. Suppose $\mathcal{P}$ contains the set of prime divisors of the order of a nonabelian finite simple group. Then there exist infinitely many full fields unramified outside $\mathcal{P}$.

In this final section we briefly discuss this conjecture. In particular we give a heuristic justification based on our results here. The sequel paper [Roberts $\geq$ 2015] will present a more comprehensive treatment.

8A. ***Specialization to number fields.*** Let $h = (G, C, \nu)$ be a Hurwitz parameter with each C_i rational for simplicity. Then one has (see Section 2D) the cover $\pi : \mathrm{HUR}_h^* \to \mathrm{CONF}_\nu$ of $\mathbb{Q}$-varieties. For every $u \in \mathrm{CONF}_\nu(\mathbb{Q})$, the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the fiber $\pi^{-1}(u) \subset \mathrm{HUR}_h^*(\overline{\mathbb{Q}})$. Let $K_{h,u}^*$ be the corresponding $\mathbb{Q}$-algebra, so that $K_{h,u}^*$ factors into fields indexed by the orbits of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $\pi^{-1}(u)$.

Controlling Galois groups. The Hilbert irreducibility theorem says that the Galois groups associated to $K_{h,u}^*$ coincide with the generic Galois group of the cover for u outside a thin set. Thus, to take the example most relevant for us, if the cover is full then one has many full specializations $K_{h,u}^*$.

Controlling ramification. For $\mathcal{P}$ a set of primes, let $\mathbb{Z}[1/\mathcal{P}] = \mathbb{Z}[\{1/p\}_{p\in\mathcal{P}}]$. The variety CONF_ν comes from a scheme over $\mathbb{Z}$ and so the set of $\mathcal{P}$-integral points $\mathrm{CONF}_\nu(\mathbb{Z}[1/\mathcal{P}])$ is defined. Suppose now that $\mathcal{P}$ contains all primes dividing $|G|$. Then the cover $\mathrm{HUR}_h^* \to \mathrm{CONF}_\nu$ has bad reduction within $\mathcal{P}$. The theory of algebraic fundamental groups then implies that $K_{h,u}^*$ is ramified within $\mathcal{P}$ whenever $u \in \mathrm{CONF}_\nu(\mathbb{Z}[1/\mathcal{P}])$.

8B. ***Heuristic argument for Conjecture 8.1.*** Let $\mathcal{P}$ be as in the statement of the conjecture. Let G be a simple group with all primes dividing $|G|$ in $\mathcal{P}$. Let $C_1 \subset G$ be a class of involutions. Then $(G, (C_1))$ satisfies Statement I of the full-monodromy theorem. By Statement II, there are infinitely many Hurwitz

parameters $h = (G, (C_1), (\nu_1))$ such that $\mathsf{Hur}_h^* \to \mathsf{Conf}_\nu$ has quasifull monodromy with connected components indexed by the finite set H_h^*.

There is a natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$ on H_h^*. When ν_1 is divisible by the exponent of $H_{G,(C_1)}$, there is an identity element $0 \in H_h^*$ fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})^{\mathrm{ab}}$. Thus one gets infinitely many full covers $\mathrm{HUR}_{h,0}^* \to \mathrm{CONF}_\nu$ defined over $\mathbb{Q}$ and ramified within $\mathcal{P}$. It is proved in [Roberts 2014, §7] that the number $N(\nu_1)$ of $\mathrm{PGL}_2(\mathbb{Q})$-orbits represented by points in $\mathrm{CONF}_{(\nu_1)}(\mathbb{Z}[1/\mathcal{P}])$ tends to ∞ with ν_1.

Thus, for each ν_1 in an infinite arithmetic progression, one has $N(\nu_1)$ algebras $K_{h,u}^*$ ramified within $\mathcal{P}$. To prove Conjecture 8.1, one not only has to control Galois groups and ramification as in Section 8A, one has to control them simultaneously, a difficult task. However if the thin set from Hilbert irreducibility intersects the $\mathcal{P}$-integral points at random, the $K_{h,u}^*$ should have a strong tendency to be full fields. On similar grounds, one would expect the $K_{h,u}^*$ to be nonisomorphic. Direct calculations, like those summarized in the next two subsections, confirm these expectations very strongly. For Conjecture 8.1 to hold for $\mathcal{P}$, there would just have to be a subsequence of ν_1 for which one of the $N(\nu_1)$ subalgebras was full.

8C. ***Specializing a sample cover.*** To illustrate concretely how Hurwitz covers naturally lead to full number fields with controlled ramification, we summarize here the introductory example of [Roberts $\geq$ 2015]. In this example, let $h = (S_5, (C_{2111}, C_5), (4, 1))$, with C_{2111} and C_5 the class of involutions and 5-cycles respectively. Then $\mathsf{Hur}_h^* = \mathsf{Hur}_h$ is a full cover of $\mathsf{Conf}_{4,1}$ of degree 25. The fiber of $\mathsf{Hur}_h \to \mathsf{Conf}_{4,1}$ over the configuration $u = (D_1, D_2) = (\{a_1, a_2, a_3, a_4\}, \{\infty\})$ consists of all equivalence classes of quintic polynomials

$$g(y) = y^5 + by^3 + cy^2 + dy + e \tag{8-1}$$

whose critical values are a_1, a_2, a_3, a_4. Here the equivalence class of $g(y)$ consists of the five polynomials $g(\zeta y)$, where ζ runs over fifth roots of unity.

Explicitly, consider the resultant $r(t)$ of $g(y) - t$ and $g'(y)$. Then $r(t)$ equals

$$\begin{aligned}
&3125t^4 + 1250(3bc - 10e)t^3 \\
&+ (108b^5 - 900b^3d + 825b^2c^2 - 11250bce + 2000bd^2 + 2250c^2d + 18750e^2)t^2 \\
&- 2\big(108b^5e - 36b^4cd + 8b^3c^3 - 900b^3de + 825b^2c^2e + 280b^2cd^2 - 315bc^3d \\
&\qquad - 5625bce^2 + 2000bd^2e + 54c^5 + 2250c^2de - 800cd^3 + 6250e^3\big)t \\
&+ \big(108b^5e^2 - 72b^4cde + 16b^4d^3 + 16b^3c^3e - 4b^3c^2d^2 - 900b^3de^2 + 825b^2c^2e^2 \\
&\qquad + 560b^2cd^2e - 128b^2d^4 - 630bc^3de + 144bc^2d^3 - 3750bce^3 + 2000bd^2e^2 \\
&\qquad + 108c^5e - 27c^4d^2 + 2250c^2de^2 - 1600cd^3e + 256d^5 + 3125e^4\big).
\end{aligned}$$

For fixed $\{a_1, a_2, a_3, a_4\}$, there are generically 125 different solutions (b, c, d, e) to the equation $r(t) = 3125(t - a_1) \cdots (t - a_4)$. Two solutions are equivalent exactly if

they have the same e. Whenever D_1 is rational, i.e., $\prod(t-a_i) \in \mathbb{Q}[t]$, the resulting set of e forms the set of roots of a degree-25 polynomial with rational coefficients. By taking $u \in \mathrm{CONF}_{4,1}(\mathbb{Z}[1/30])$, one gets more than 10000 different fields with Galois group A_{25} or S_{25} and discriminant of the form $\pm 2^a 3^b 5^c$.

8D. ***Comparison with the mass heuristic.*** Let $F_{\mathcal{P}}(m)$ be the number of full fields ramified within $\mathcal{P}$ of degree m. The mass heuristic [Bhargava 2007, (3.3)] gives an expected value $\mu_{\mathcal{P}}(m)$ for $F_{\mathcal{P}}(m)$ as an easily computed product of local masses. This heuristic has had clear success in the setting of fixed degree and large discriminant, being for example exactly right on average for $m = 5$ [Bhargava 2010]. In [Roberts 2007, §11], we considered the opposite regime of fixed ramifying primes and increasing degree. We proved there that for any $\mathcal{P}$ the sequence $\mu_{\mathcal{P}}(m)$ ultimately decreases superexponentially with m.

The convergence of $\sum_{m=1}^{\infty} \mu_{\mathcal{P}}(m)$ for any $\mathcal{P}$ argues against Conjecture 8.1. However, our calculations confirming genericity of specialization make it clear that the $K_{h,u}^*$ we are considering here simply escape the influence of the mass heuristic. For instance, one of many examples in [Roberts $\geq$ 2015] comes from the Hurwitz parameter $h = (S_6, (C_{21111}, C_{321}, C_{3111}, C_{411}), (2,1,1,1))$. The covering $\mathrm{HUR}_h \to \mathrm{CONF}_{2,1,1,1}$ is full of degree 202. The specialization set $\mathrm{CONF}_{2,1,1,1}(\mathbb{Z}[1/30])$ intersects exactly 2947 different $\mathrm{PGL}_2(\mathbb{Q})$-orbits on the set $\mathrm{CONF}_{2,1,1,1}(\mathbb{Q})$ [Roberts 2014, §9.2]. The mass heuristic predicts

$$\sum_{m=202}^{\infty} \mu_{\{2,3,5\}}(m) < 10^{-16}$$

full fields in degree ≥ 202. However specialization is as generic as it could be, as the 2947 algebras $K_{h,u}$ are pairwise nonisomorphic and all full.

8E. ***Concluding discussion.*** There are other aspects of the sequences $F_{\mathcal{P}}(m)$ that are not addressed by Conjecture 8.1. For example, our belief is that Conjecture 8.1 still holds with the conclusion strengthened to $F_{\mathcal{P}}(m)$ being unbounded. Also notable is that fields arising from full fibers of Hurwitz covers occur only in degrees for which there is a cover. By the mass formula, these degrees form a sequence of density zero. A fundamental question is thus the support of the sequences $F_{\mathcal{P}}(m)$, meaning the set of degrees m for which $F_{\mathcal{P}}(m)$ is positive.

One extreme possibility, giving as much credence to the mass heuristic as is still reasonable, is that $F_{\mathcal{P}}(m)$ has support on a sequence of density zero in general and is eventually zero unless $\mathcal{P}$ contains the set of prime divisors of the order of a finite simple group. This would imply that the classification of finite simple groups has an unexpected governing influence on a part of algebraic number theory seemingly quite removed from general group theory. If this extreme possibility does not hold,

then there would have to be a broad and as yet unknown class of number fields which is also exceptional from the point of view of the mass heuristic.

Acknowledgements

We thank Simon Rubinstein-Salzedo and John Voight for helpful comments on earlier drafts of this paper. We also thank two anonymous referees for their helpful corrections and suggestions.

Roberts was supported by grant #209472 from the Simons Foundation. Venkatesh was supported by grants from the NSF and from the Packard Foundation.

References

[Bailey and Fried 2002] P. Bailey and M. D. Fried, "Hurwitz monodromy, spin separation and higher levels of a modular tower", pp. 79–220 in *Arithmetic fundamental groups and noncommutative algebra* (Berkeley, CA, 1999), edited by M. D. Fried and Y. Ihara, Proc. Sympos. Pure Math. **70**, Amer. Math. Soc., Providence, RI, 2002. MR 2005b:14044 Zbl 1072.14026

[Bertin and Romagny 2011] J. Bertin and M. Romagny, *Champs de Hurwitz*, Mém. Soc. Math. Fr. (N.S.) **125–126**, 2011. MR 2920693 Zbl 1242.14025

[Bhargava 2007] M. Bhargava, "Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants", *Int. Math. Res. Not.* **2007**:17 (2007), Art. ID rnm052. MR 2009e:11220 Zbl 1145.11080

[Bhargava 2010] M. Bhargava, "The density of discriminants of quintic rings and fields", *Ann. of Math.* (2) **172**:3 (2010), 1559–1591. MR 2011k:11152 Zbl 1220.11139

[Conway and Parker 1988] J. H. Conway and R. A. Parker, "On the Hurwitz number of arrays of group elements", unpublished preprint, 1988.

[Conway et al. 1985] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. MR 88g:20025 Zbl 0568.20001

[Dixon and Mortimer 1996] J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics **163**, Springer, New York, 1996. MR 98m:20003 Zbl 0951.20001

[Dunfield and Thurston 2006] N. M. Dunfield and W. P. Thurston, "Finite covers of random 3-manifolds", *Invent. Math.* **166**:3 (2006), 457–521. MR 2007f:57039 Zbl 1111.57013

[Eckmann and Stammbach 1970] B. Eckmann and U. Stammbach, "On exact sequences in the homology of groups and algebras", *Illinois J. Math.* **14** (1970), 205–215. MR 42 #4615 Zbl 0195.03402

[Eisenbud et al. 1991] D. Eisenbud, N. Elkies, J. Harris, and R. Speiser, "On the Hurwitz scheme and its monodromy", *Compositio Math.* **77**:1 (1991), 95–117. MR 92c:14019 Zbl 0726.14022

[Ellenberg et al. 2013] J. Ellenberg, A. Venkatesh, and C. Westerland, "Homological stability for Hurwitz spaces and the Cohen–Lenstra conjecture over function fields, II", preprint, 2013. arXiv 1212.0923

[Fried and Völklein 1991] M. D. Fried and H. Völklein, "The inverse Galois problem and rational points on moduli spaces", *Math. Ann.* **290**:4 (1991), 771–800. MR 93a:12004 Zbl 0763.12004

[Kluitmann 1988] P. Kluitmann, "Hurwitz action and finite quotients of braid groups", pp. 299–325 in *Braids* (Santa Cruz, CA, 1986), edited by J. S. Birman and A. Libgober, Contemp. Math. **78**, Amer. Math. Soc., Providence, RI, 1988. MR 90d:20071 Zbl 0701.20019

[Magaard et al. 2003] K. Magaard, S. Shpectorov, and H. Völklein, "A GAP package for braid orbit computation and applications", *Experiment. Math.* **12**:4 (2003), 385–393. MR 2005e:12007 Zbl 1068.12002

[Malle and Matzat 1999] G. Malle and B. H. Matzat, *Inverse Galois theory*, Springer, Berlin, 1999. MR 2000k:12004 Zbl 0940.12001

[Malle and Roberts 2005] G. Malle and D. P. Roberts, "Number fields with discriminant $\pm 2^a 3^b$ and Galois group A_n or S_n", *LMS J. Comput. Math.* **8** (2005), 80–101. MR 2006a:11137 Zbl 1119.11064

[Roberts 2007] D. P. Roberts, "Wild partitions and number theory", *J. Integer Seq.* **10**:6 (2007), Article 07.6.6, 34. MR 2009b:11206 Zbl 1174.11094

[Roberts 2014] D. P. Roberts, "Polynomials with prescribed bad primes", *Int. J. Number Theory* (online publication December 2014).

[Roberts $\geq$ 2015] D. P. Roberts, "Hurwitz number fields", in preparation.

[Romagny and Wewers 2006] M. Romagny and S. Wewers, "Hurwitz spaces", pp. 313–341 in *Groupes de Galois arithmétiques et différentiels*, edited by D. Bertrand and P. Dèbes, Sémin. Congr. **13**, Soc. Math. France, Paris, 2006. MR 2008e:14040 Zbl 1156.14314

[Serre 1990] J.-P. Serre, "Relèvements dans $\tilde{\mathfrak{A}}_n$", *C. R. Acad. Sci. Paris Sér. I Math.* **311**:8 (1990), 477–482. MR 91m:20010 Zbl 0714.20003

[Serre 2008] J.-P. Serre, *Topics in Galois theory*, 2nd ed., Research Notes in Mathematics **1**, A K Peters, Wellesley, MA, 2008. MR 2008i:12010 Zbl 1128.12001

[Sloane 1991] N. Sloane, "$a(n) = 2(a(n-1) + (n-1)a(n-2))$, $a(0) = 1$", sequence A000898 in *The online encyclopedia of integer sequences* (oeis.org), 1991.

Communicated by Barry Mazur
Received 2014-01-28 Revised 2015-01-08 Accepted 2015-02-18

roberts@morris.umn.edu *Division of Science and Mathematics, University of Minnesota, Morris, MN 56267, United States*

akshay@math.stanford.edu *Department of Mathematics, Building 380, Stanford University, Stanford, CA 94305, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2015 is US $255/year for the electronic version, and $440/year (+$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 9 No. 3 2015

1937-0652(2015)9:3;1-6