Simple closed curves, finite covers of surfaces, and power subgroups of $\mathrm{Out}(F_n)$

Justin Malestein* Andrew Putman†

Abstract

We construct examples of finite covers of punctured surfaces where the first rational homology is not spanned by lifts of simple closed curves. More generally, for any set $\mathcal{O} \subset F_n$ which is contained in the union of finitely many $\mathrm{Aut}(F_n)$-orbits, we construct finite-index normal subgroups of F_n whose first rational homology is not spanned by powers of elements of $\mathcal{O}$. These examples answer questions of Farb–Hensel, Kent, Looijenga, and Marché. We also show that the quotient of $\mathrm{Out}(F_n)$ by the subgroup generated by k^{th} powers of transvections often contains infinite order elements, strengthening a result of Bridson–Vogtmann saying that it is often infinite. Finally, for any set $\mathcal{O} \subset F_n$ which is contained in the union of finitely many $\mathrm{Aut}(F_n)$-orbits, we construct integral linear representations of free groups that have infinite image and map all elements of $\mathcal{O}$ to torsion elements.

1 Introduction

Let $\Sigma_{g,n}$ be a genus g surface with n punctures and let $\mathrm{Mod}_{g,n}$ be its mapping class group. An important classical tool for studying $\mathrm{Mod}_{g,n}$ is its action on $\mathrm{H}_1(\Sigma_{g,n})$. Recently there has been a lot of interest in studying the action of $\mathrm{Mod}_{g,n}$ on the homology of finite covers of $\Sigma_{g,n}$. See, for instance, [4, 5, 9, 10, 11, 12, 13, 17, 18, 19, 21, 22, 26, 27, 32]. These representations encode a lot of subtle information; for instance, work of Putman–Wieland [27] relates them to the virtual first Betti number of $\mathrm{Mod}_{g,n}$.

Simple closed curve homology. Let $\pi\colon \widetilde{\Sigma} \to \Sigma_{g,n}$ be a finite cover. The *simple closed curve homology* of $\widetilde{\Sigma}$, denoted $\mathrm{H}_1^{\text{scc}}(\widetilde{\Sigma})$, is the subspace of $\mathrm{H}_1(\widetilde{\Sigma})$ spanned by the set

$$\{[\widetilde{\gamma}] \in \mathrm{H}_1(\widetilde{\Sigma}) \mid \widetilde{\gamma} \text{ is a component of } \pi^{-1}(\gamma) \text{ for a simple closed curve } \gamma \text{ on } \Sigma_{g,n}\}.$$

Another more algebraic way to describe $\mathrm{H}_1^{\text{scc}}(\widetilde{\Sigma})$ is as follows. Let $R \subset \pi_1(\Sigma_{g,n})$ be the subgroup corresponding to $\widetilde{\Sigma}$. We have $\mathrm{H}_1(\widetilde{\Sigma}) = \mathrm{H}_1(R)$, and $\mathrm{H}_1^{\text{scc}}(\widetilde{\Sigma})$ is the span of the set

$$\{[x^k] \in \mathrm{H}_1(R) \mid x \in \pi_1(\Sigma_{g,n}) \text{ is a simple closed curve and } k \geq 1 \text{ is such that } x^k \in R\}.$$

In a similar way, we can define $\mathrm{H}_1^{\text{scc}}(\widetilde{\Sigma}; A)$ for any commutative ring A.

Equality. A fundamental question about $\mathrm{H}_1(\widetilde{\Sigma}; A)$ is whether $\mathrm{H}_1^{\text{scc}}(\widetilde{\Sigma}; A) = \mathrm{H}_1(\widetilde{\Sigma}; A)$. This seems to have been first asked in print by Marché [24], though Kent has informed us that it also arose in her work on the congruence subgroup property (see Remark 1.5 below). It has since been asked by Farb–Hensel [4] and Looijenga [23], who said that it was a "bit of a scandal" that the answer is not known. The first serious progress on this

*University of Oklahoma, Department of Mathematics, 601 Elm Ave, Norman, OK, 73019, jmalestein@math.ou.edu

†Department of Mathematics, University of Notre Dame, 279 Hurley Hall, Notre Dame, IN 46556, andyp@nd.edu

was work of Koberda–Santharoubane [19], who used TQFT representations of $\mathrm{Mod}_{g,n}$ to construct examples where $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Z}) \neq \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Z})$. However, they were unable to rule out the possibility that $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Z})$ is finite-index in $\mathrm{H}_1(\widetilde{\Sigma};\mathbb{Z})$. In other words, they could not replace $\mathbb{Z}$ with $\mathbb{Q}$. Another partial result is a theorem of Farb–Hensel [4, Proposition 8.4] which says that $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Q}) = \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q})$ when the deck group is abelian. They also constructed examples of finite covers $\widetilde{\Sigma}_{1,2} \to \Sigma_{1,2}$ where $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma}_{1,2};\mathbb{Q}) \neq \mathrm{H}_1(\widetilde{\Sigma}_{1,2};\mathbb{Q})$; however, they indicated that despite an extensive computer search they were unable to find such examples in genus 2.

Inequality. Our first main theorem gives examples of covers of punctured surfaces in all genera where $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Q}) \neq \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q})$.

Theorem A. *For all $g \geq 0$ and $n \geq 1$ such that $\pi_1(\Sigma_{g,n})$ is nonabelian, there is a finite regular cover $\widetilde{\Sigma} \to \Sigma_{g,n}$ with $\mathrm{H}_1^{scc}(\widetilde{\Sigma};\mathbb{Q}) \neq \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q})$.*

Remark 1.1. The degrees of our covers are enormous, so it is not surprising that they could not be found via a computer search. □

Remark 1.2. We do not know how to remove the condition $n \geq 1$ from Theorem A. The issue is that our proof of the key Proposition 2.3 below makes use of delicate results about free restricted Lie algebras. To prove the analogous result in the closed case, we would have to generalize these results to certain 1-relator restricted Lie algebras. □

Branched covers. We can define $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Q})$ for branched covers $\widetilde{\Sigma} \to \Sigma_{g,n}$ exactly like for unbranched covers. Though we are unable to remove the condition $n \geq 1$ from Theorem A, we do want to point out the following consequence for closed genus g surfaces Σ_g.

Theorem B. *For all $g \geq 2$, there exists a finite branched cover $\widetilde{\Sigma} \to \Sigma_g$ with $\mathrm{H}_1^{scc}(\widetilde{\Sigma};\mathbb{Q}) \neq \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q})$.*

This result can be derived from Theorem A as follows. Let $\widetilde{\Sigma}' \to \Sigma_{g,1}$ be the unbranched cover provided by Theorem A. The surface $\widetilde{\Sigma}'$ is a finite-genus surface with punctures $p_1, \ldots, p_k$. A small oriented loop γ surrounding the puncture of $\Sigma_{g,1}$ lifts to a collection of loops $\widetilde{\gamma}_1, \ldots, \widetilde{\gamma}_k$ such that $\widetilde{\gamma}_i$ surrounds p_i. Fill in all the punctures of $\widetilde{\Sigma}'$ to form a closed surface $\widetilde{\Sigma}$. We then have a branched cover $\widetilde{\Sigma} \to \Sigma_g$ whose branch points are precisely the p_i such that the map $\widetilde{\gamma}_i \to \gamma$ is a cover of degree greater than 1. Since the homology classes of the $\widetilde{\gamma}_i$ lie in $\mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma}';\mathbb{Q})$ and generate the kernel of $\mathrm{H}_1(\widetilde{\Sigma}') \to \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q})$, we see that

$$\mathrm{H}_1(\widetilde{\Sigma}';\mathbb{Q}) / \mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma}';\mathbb{Q}) \cong \mathrm{H}_1(\widetilde{\Sigma};\mathbb{Q}) / \mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma};\mathbb{Q}).$$

Since the left hand side is nonzero, so is the right hand side, as desired.

More general result. In fact, we prove a much more general result than Theorem A. To state it, let F_n be the free group on n generators and let $\mathcal{O} \subset F_n$. For a finite-index $R < F_n$ and an abelian group A, define $\mathrm{H}_1^{\mathcal{O}}(R;A)$ to be the span in $\mathrm{H}_1(R;A)$ of the set

$$\{[x^k] \in \mathrm{H}_1(R;A) \mid x \in \mathcal{O} \text{ and } k \geq 1 \text{ is such that } x^k \in R\}.$$

We prove the following theorem.

Theorem C. *Let $n \geq 2$ and let $\mathcal{O} \subset F_n$ be contained in the union of finitely many* $\mathrm{Aut}(F_n)$*-orbits. Then there exists a finite-index $R \lhd F_n$ with $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$.*

We highlight two special cases of Theorem C.

Example 1.3. Let $\mathcal{O}$ be the set of *primitive elements* of F_n, that is, elements that lie in a free basis. The group $\mathrm{Aut}(F_n)$ acts transitively on $\mathcal{O}$. In this case, for finite-index $R \lhd F_n$ the group $\mathrm{H}_1^{\mathcal{O}}(R;A)$ was introduced by Farb–Hensel [4], who called it the *primitive homology* of R and asked whether or not $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) = \mathrm{H}_1(R;\mathbb{Q})$ always holds. They constructed counterexamples to this for $n = 2$. They also proved that there was indeed equality in some situations. For instance they could prove equality when F_n/R is abelian and in some cases when F_n/R is 2-step nilpotent. Theorem C provides a negative answer to their question for all $n \geq 2$. □

Example 1.4. We next explain why Theorem C is a vast generalization of Theorem A. Let $g \geq 0$ and $n \geq 1$ be such that $F = \pi_1(\Sigma_{g,n})$ is nonabelian. Let $\mathcal{O} \subset F$ be the set of simple closed curves. For a finite-index $R \lhd F$, let $\widetilde{\Sigma}_R$ be the associated finite cover of $\Sigma_{g,n}$, so $\mathrm{H}_1(R;\mathbb{Q}) = \mathrm{H}_1(\widetilde{\Sigma}_R;\mathbb{Q})$ and $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) = \mathrm{H}_1^{\mathrm{scc}}(\widetilde{\Sigma}_R;\mathbb{Q})$. The set $\mathcal{O}$ is the union of finitely many mapping class group orbits; see [6, Chapter 1.3]. Since $\mathrm{Aut}(F)$ is larger than the mapping class group, $\mathcal{O}$ is contained in the union of finitely many $\mathrm{Aut}(F)$-orbits. Applying Theorem C, we obtain a finite-index $R \lhd F$ satisfying $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$. Theorem A follows. This can be generalized in a wide variety of ways. For instance, for some fixed $m \geq 0$ we could take $\mathcal{O}$ to be the set of all elements of F that can be represented by a curve with at most m self-intersections. □

Remark 1.5. Let $g \geq 0$ and $n \geq 1$ be such that $F = \pi_1(\Sigma_{g,n})$ is nonabelian. In [16], Kent asked whether the conclusion of Theorem C holds for $\mathcal{O}$ the set of all curves that do not fill $\Sigma_{g,n}$, i.e. curves whose complement contains a non simply connected component. Since these are not contained in finitely many $\mathrm{Aut}(F)$-orbits, this question is not addressed by Theorem C. □

p-primitive homology. We now discuss a variant of Theorem C. Fix a prime p. Say that $x \in F_n$ is *p-primitive* if it maps to a nonzero element of $\mathrm{H}_1(F_n;\mathbb{F}_p)$. We denote the set of p-primitive elements by $\mathfrak{O}_p$. Observe that primitive elements of F_n are p-primitive for all primes p. There are infinitely many $\mathrm{Aut}(F_n)$-orbits of p-primitive element of F_n, so we cannot use Theorem C to construct finite-index $R \lhd F_n$ satisfying $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$. However, the following still holds.

Theorem D. *For all $n \geq 2$ and primes p, there is a finite-index $R \lhd F_n$ with $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$. Moreover, we can choose R such that F_n/R is a p-group.*

Transvections. Using TQFT representations, Funar [7] and Masbaum [25] proved that for $g \geq 2$ and $n \geq 0$ and $k \geq 11$, the subgroup of $\mathrm{Mod}_{g,n}$ generated by k^{th} powers of Dehn twists is an infinite-index subgroup of $\mathrm{Mod}_{g,n}$. In fact, their methods show that the quotient of $\mathrm{Mod}_{g,n}$ by the subgroup generated by k^{th} powers of Dehn twists contains infinite-order elements. Using some of the methods of the proof of Theorem D, we will prove an analogous theorem for $\mathrm{Out}(F_n)$. The analogue in $\mathrm{Out}(F_n)$ of a Dehn twist is a *transvection*, which is defined as follows. Let S be a basis for F_n and let $x, y \in S$ be distinct elements. The transvection $\tau_{S,x,y}$ is then the automorphism $\tau_{S,x,y}\colon F_n \to F_n$ defined via the formula

$$\tau_{S,x,y}(z) = \begin{cases} yz & \text{if } z = x, \\ z & \text{if } z \neq x \end{cases} \qquad (z \in S).$$

All transvections are conjugate to each other, and transvections with S the standard basis for F_n appear in the usual generating sets for $\text{Out}(F_n)$.

For $n \geq 2$ and $k \geq 1$, let $\mathfrak{G}_{n,k}$ be the subgroup of $\text{Out}(F_n)$ generated by k^{th} powers of transvections. Bridson–Vogtmann [2] showed that the quotient $\text{Out}(F_n)/\mathfrak{G}_{n,k}$ contains a copy of the free Burnside group $\mathfrak{B}_{n-1,k}$ obtained by quotienting F_{n-1} by the subgroup generated by all k^{th} powers. In particular, $\text{Out}(F_n)/\mathfrak{G}_{n,k}$ is infinite whenever $\mathfrak{B}_{n-1,k}$ is. We will strengthen this by showing that $\text{Out}(F_n)/\mathfrak{G}_{n,k}$ often contains infinite order elements.

Theorem E. *For all $n \geq 2$, there exists an infinite set of positive numbers $\mathcal{K}_n$ such that $\text{Out}(F_n)/\mathfrak{G}_{n,k}$ contains infinite-order elements for all $k \in \mathcal{K}_n$.*

Remark 1.6. The reader might object that we should also include the transvections $\tau'_{S,x,y}$ defined via the formula

$$\tau'_{S,x,y}(z) = \begin{cases} zy & \text{if } z = x, \\ z & \text{if } z \neq x \end{cases} \qquad (z \in S).$$

But this would be superfluous: letting $S' = (S - \{x\}) \cup \{x^{-1}\}$, we have $\tau'_{S,x,y} = \tau^{-1}_{S',x^{-1},y}$. □

Remark 1.7. Theorem E implies an analogous result for $\text{Aut}(F_n)$. Let $\widetilde{\mathfrak{G}}_{n,k}$ be the subgroup of $\text{Aut}(F_n)$ generated by k^{th} powers of transvections. The surjection $\text{Aut}(F_n) \to \text{Out}(F_n)$ restricts to a surjection from $\widetilde{\mathfrak{G}}_{n,k}$ to $\mathfrak{G}_{n,k}$. Thus $\text{Aut}(F_n)/\widetilde{\mathfrak{G}}_{n,k}$ contains infinite-order elements whenever $\text{Out}(F_n)/\mathfrak{G}_{n,k}$ does. □

Remark 1.8. The proof of Theorem E shows that we can take $\mathcal{K}_n$ to be the set

$$\mathcal{K}_n = \{k \mid \text{there exists a prime power } p^e \text{ dividing } k \text{ such that } p^e > p(p-1)(n-1)\}.$$

We conjecture that there is some uniform $m \geq 2$ such that we can take $\mathcal{K}_n = \{k \mid k \geq m\}$. Precisely explaining what it would take to prove this using the techniques of this paper would require delving into the details of our proof, but roughly speaking one would have to construct for each $k \geq m$ a finite quotient $G = F_n/R$ as in Theorem D such that $x^k = 1$ for all $x \in G$ that are the image of a primitive element of F_n. In our current construction, the orders of such elements are forced to grow with n. □

Infinite quotients of free groups. We conclude with a pair of interesting consequences of Theorems C and D. The first is as follows.

Theorem F. *Let $n \geq 2$ and let $\mathcal{O} \subset F_n$ be contained in the union of finitely many $\text{Aut}(F_n)$-orbits. Then there exists an integral linear representation $\rho\colon F_n \to \text{GL}_d(\mathbb{Z})$ with infinite image such that every element of $\rho(\mathcal{O})$ has finite order.*

For instance, as in Example 1.4 we can use Theorem F to construct for all $g \geq 0$ and $n \geq 1$ with $\pi_1(\Sigma_{g,n})$ nonabelian an integral linear representation $\rho\colon \pi_1(\Sigma_{g,n}) \to \text{GL}_d(\mathbb{Z})$ with infinite image such that for all simple closed curves $x \in \pi_1(\Sigma_{g,n})$, the image $\rho(x)$ has finite order. A slightly weaker version of this with the representation landing in $\text{GL}_d(\mathbb{C})$ instead of $\mathrm{GL}_d(\mathbb{Z})$ was originally proved using TQFT representations by Koberda–Santharoubane [19, Theorem 1.1], who attribute the question of whether such representations exist to Kisin and McMullen. Unlike us, Koberda–Santharoubane could also deal with closed surfaces.

Our second result is the following variant of Theorem F.

Theorem G. *For all $n \geq 2$ and primes p, there exists an integral linear representation $\rho\colon F_n \to \mathrm{GL}_d(\mathbb{Z})$ with infinite image such that every element of $\rho(\mathfrak{O}_p)$ has finite order.*

Remark 1.9. For $n = 2$, this was originally proved by Zelmanov; see [35, p. 140]. □

Remark 1.10. In Theorems F and G, the images of our representations are virtually free abelian. □

Outline. We prove Theorem D in §2, Theorem C in §3, Theorem E in §4, and Theorems F and G in §5. As we indicated above, Theorem A follows from Theorem C and Theorem B follows from Theorem A, so this completes the proofs of all of our main theorems.

Acknowledgments. We wish to thank Khalid Bou-Rabee, Martin Bridson, Mikhail Ershov, Benson Farb, Daniel Groves, Sebastian Hensel, Dawid Kielak, Eduard Looijenga, and Karen Vogtmann for helpful correspondence and conversations. Andrew Putman is supported in part by National Science Foundation grants DMS-1255350 and DMS-1737434.

2 p-primitive homology: Theorem D

This section contains the proof of Theorem D. It has four parts. In §2.1, we give a criterion for certifying that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$ for a finite-index subgroup $R \lhd F_n$. In §2.2, we reduce Theorem D to Proposition 2.3, which asserts that a finite p-group with certain special properties exists. In §2.3, we review some basic material on p-restricted Lie algebras. Finally, in §2.4 we prove Proposition 2.3.

2.1 Certifying the insufficiency of p-primitive homology

This section gives a criterion for certifying that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$ for finite-index subgroups $R \lhd F_n$. This criterion is a variant of one identified by Farb–Hensel [4]. Our main result is as follows.

Theorem 2.1. *For some $n \geq 2$, consider a finite-index $R \lhd F_n$, a field $\mathbf{k}$ of characteristic 0, and a prime p. Letting $G = F_n/R$, assume that there exists a $\mathbf{k}$-representation V of G such that for all p-primitive $x \in F_n$, the action on V of the image of x in G fixes no nonzero vectors. Then $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$.*

The proof of Theorem 2.1 requires one preliminary result. Consider a normal subgroup $R \lhd F_n$ and a field $\mathbf{k}$. The conjugation action of F_n on R induces an action of F_n on $\mathrm{H}_1(R;\mathbf{k})$. The restriction of this action to R is trivial, so we obtain an induced action of $G = F_n/R$ on $\mathrm{H}_1(R;\mathbf{k})$. We then have the following theorem of Gaschütz [8].

Theorem 2.2. *For some $n \geq 1$, consider a finite-index $R \lhd F_n$ and a field $\mathbf{k}$ of characteristic 0. Letting $G = F_n/R$, the G-module $\mathrm{H}_1(R;\mathbf{k})$ is isomorphic to $\mathbf{k} \oplus (\mathbf{k}[G])^{n-1}$.*

Proof of Theorem 2.1. Passing to an irreducible subrepresentation of V, we can assume that V is irreducible. Since $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbf{k}) = \mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbf{k}$ and $\mathrm{H}_1(R;\mathbf{k}) = \mathrm{H}_1(R;\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbf{k}$, it is enough to prove that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbf{k}) \neq \mathrm{H}_1(R;\mathbf{k})$. Let $W \subset \mathrm{H}_1(R;\mathbf{k})$ be the V-isotypic component. Theorem 2.2 implies that $W \neq 0$, so it is enough to prove that the projection of $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbf{k})$ to W is 0. Consider a p-primitive element $x \in F_n$ and let $m \geq 1$ be such that $x^m \in R$. We must prove that the projection of $[x^m] \in \mathrm{H}_1(R;\mathbf{k})$ to W is trivial. Let $g \in G$ be the image of x. The fact that x commutes with x^m implies that g acts trivially on $[x^m] \in \mathrm{H}_1(R;\mathbf{k})$. Since x is p-primitive, our assumptions imply that the only vector in V that is fixed by g is 0. We conclude that the projection of $[x^m]$ to W is 0, as desired. □

2.2 Reduction: p-groups with special centers

In this section, we reduce Theorem D to the following proposition, which we will prove in §2.4 below.

Proposition 2.3. *For $n, p \geq 2$ with p prime, there exists a finite p-group G, a central subgroup C of G, and a homomorphism $\Psi\colon C \to \mathbb{Z}/p$ such that the following hold.*

- $\mathrm{H}_1(G;\mathbb{F}_p) = \mathbb{F}_p^n$.
- *For all $g \in G$ whose image in $\mathrm{H}_1(G;\mathbb{F}_p)$ is nontrivial, some power of g is in $C - \ker(\Psi)$.*

Remark 2.4. To give some sense for what is going on in Proposition 2.3, we give some easy examples of groups G that satisfy its conclusion for small values of n and p. In these examples, the central subgroup C satisfies $C \cong \mathbb{Z}/p$ and we can take $\Psi\colon C \to \mathbb{Z}/p$ to be the identity.

1. For any prime p, the cyclic group of order p satisfies the conclusions of Proposition 2.3 for $n = 1$. In this case, the subgroup C is the entire group.
2. The 8-element quaternion group satisfies the conclusions of Proposition 2.3 for $n = 2$ and $p = 2$. In this case, the subgroup C is the center, which is cyclic of order 2.

It is much harder to prove Proposition 2.3 for $n \geq 3$. The issue is that in both of the above examples a stronger conclusion holds: for *every* nontrivial $g \in G$ some power of g lies in $C - \ker(\Psi)$. One can show that there are no examples satisfying this stronger condition for $n \geq 3$. Indeed, given a group G satisfying this stronger condition one can use the construction in the proof of Theorem D below to construct a $\mathbb{C}$-representation V of G such that no nontrivial element of G fixes any nontrivial vector in V. From this, one can deduce that all abelian subgroups of G are cyclic. This implies that $n \leq 2$; see [14, Theorem 6.12]. See [28] for more details. □

Proof of Theorem D, assuming Proposition 2.3. Let us first recall the setup. Let $n \geq 2$ and let p be a prime. Our goal is to construct a finite-index $R \lhd F_n$ such that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$ and such that F_n/R is a p-group.

Let G and C and $\Psi\colon C \to \mathbb{Z}/p$ be as in Proposition 2.3. Since $\mathrm{H}_1(G;\mathbb{F}_p) = \mathbb{F}_p^n$, we can choose a homomorphism $\rho\colon F_n \to G$ taking a basis of F_n to a set S of elements of G that projects to a basis for $\mathrm{H}_1(G;\mathbb{F}_p)$. Equivalently, the induced map $\rho_*\colon \mathrm{H}_1(F_n;\mathbb{F}_p) \to \mathrm{H}_1(G;\mathbb{F}_p)$ is an isomorphism. Note that $\mathrm{H}_1(G;\mathbb{F}_p) = G/D$ with $D = G^p[G,G]$. Since S projects to a basis for $\mathrm{H}_1(G;\mathbb{F}_p)$, the group G is generated by $S \cup D$. Since G is a finite p-group, the group D is the Frattini subgroup of G (see [29, Theorem 5.48]). Since $S \cup D$ generates G and D is the Frattini subgroup of G, we conclude that S generates G, so ρ is surjective.

If $x \in F_n$ is p-primitive, then x projects to a nonzero element of $\mathrm{H}_1(F_n;\mathbb{F}_p)$ and thus $\rho(x) \in G$ also projects to a nontrivial element of $\mathrm{H}_1(G;\mathbb{F}_p)$. Set $R = \ker(\rho)$. By Theorem

2.1, to prove that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$, it is enough to construct a $\mathbb{C}$-representation V of G such that for all $g \in G$ which project to a nonzero element of $\mathrm{H}_1(G;\mathbb{F}_p)$, the action of g on V fixes no nonzero vectors.

By regarding $\mathbb{Z}/p$ as the set of p^{th} roots of unity in $\mathbb{C}$, we can view $\Psi\colon C \to \mathbb{Z}/p$ as a homomorphism from C to $\mathbb{C}^*$. Let W be the 1-dimensional $\mathbb{C}$-representation of C such that $c \in C$ acts on W as multiplication by $\Psi(c) \in \mathbb{C}^*$. Define

$$V = \mathrm{Ind}_C^G W.$$

Consider $g \in G$ that projects to a nonzero element of $\mathrm{H}_1(G;\mathbb{F}_p)$. We wish to prove that g fixes no nonzero vectors in V. By assumption, some power of g equals an element $c \in C - \ker(\Psi)$. It is enough to prove that c fixes no nonzero vectors in V. Choosing a set $\Lambda \subset G$ of coset representatives for G/C, we have

$$V = \bigoplus_{\lambda \in \Lambda} \lambda \cdot W.$$

Moreover, since C is a central subgroup of G it follows that for $w \in W$ and $\lambda \in \Lambda$ we have

$$c \cdot (\lambda \cdot w) = \lambda \cdot (c \cdot w) = \lambda \cdot (\Psi(c) w) = \Psi(c)(\lambda \cdot w).$$

We deduce that c acts on V as multiplication by $\Psi(c)$. Since $c \notin \ker(\Psi)$, we conclude that c fixes no nonzero vectors in V, as desired. □

2.3 Restricted Lie algebras

Before we prove Proposition 2.3, we will need to discuss some preliminary facts about free groups and Lie algebras that can be viewed as "mod-p" analogues of the familiar connection between the lower central series of a free group and the free Lie algebra (see, e.g., [30]).

The starting point is the following definition, which was first made by Zassenhaus [34].

Definition 2.5. Let Γ be a group and let p be a prime. The *Zassenhaus p-central series* of Γ is the fastest descending series

$$\Gamma = \gamma_1^p(\Gamma) \supset \gamma_2^p(\Gamma) \supset \gamma_3^p(\Gamma) \supset \cdots$$

satisfying the following two conditions:

- $[\gamma_i^p(\Gamma), \gamma_j^p(\Gamma)] \subset \gamma_{i+j}^p(\Gamma)$ for all $i, j \geq 1$.
- For all $x \in \gamma_i^p(\Gamma)$, we have $x^p \in \gamma_{ip}^p(\Gamma)$. □

Remark 2.6. Explicitly, one can inductively define $\gamma_i^p(\Gamma)$ as that subgroup generated by

- $[x, y]$ for all $x \in \gamma_j^p(\Gamma), y \in \gamma_k^p(\Gamma)$ with $j, k < i$ and $j + k \geq i$, and
- x^p for all $x \in \gamma_j^p(\Gamma)$ with $j < i$ and $pj \geq i$. □

Given a group Γ, we define

$$\mathcal{L}_i^p(\Gamma) = \gamma_i^p(\Gamma)/\gamma_{i+1}^p(\Gamma) \qquad (i \geq 1).$$

The second condition in the definition of the Zassenhaus p-central series ensures that $\mathcal{L}_i^p(\Gamma)$ is an $\mathbb{F}_p$-vector space. Define

$$\mathcal{L}^p(\Gamma) = \bigoplus_{i \geq 1} \mathcal{L}_i^p(\Gamma).$$

The commutator bracket on Γ descends to an operation on $\mathcal{L}^p(\Gamma)$ that endows it with the structure of a graded Lie algebra over $\mathbb{F}_p$. More precisely, consider $x \in \gamma_i^p(\Gamma)$ and $y \in \gamma_j^p(\Gamma)$. Letting $\overline{x} \in \mathcal{L}_i^p(\Gamma)$ and $\overline{y} \in \mathcal{L}_j^p(\Gamma)$ be their images, the Lie bracket $[\overline{x}, \overline{y}] \in \mathcal{L}_{i+j}^p(\Gamma)$ is the image of the commutator bracket $[x, y] \in \gamma_{i+j}^p(\Gamma)$.

In fact, even more is true: Zassenhaus proved that $\mathcal{L}^p(\Gamma)$ is what is called a p-restricted Lie algebra, the definition of which is as follows ([34]; see [3, §12] for a textbook reference). We recommend that the reader not dwell on the three conditions in this definition – the only one we will explicitly use is the first.

Definition 2.7. Fix a prime p. A *p-restricted Lie algebra* over $\mathbb{F}_p$ is a Lie algebra A over $\mathbb{F}_p$ equipped with a p^{th} power operation that takes $x \in A$ to $x^{[p]} \in A$. This operation must satisfy the following three conditions:

1. For $c \in \mathbb{F}_p$ and $x \in A$, we have $(cx)^{[p]} = c^p x^{[p]}$.
2. For all $x \in A$, we have $\text{Ad}(x^{[p]}) = (\text{Ad}\,(x))^p$, where the right hand side indicates that we are taking the p^{th} iterate of $\text{Ad}(x)\colon A \to A$.
3. For $x, y \in A$, we have

$$(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_i(x, y),$$

where $s_i(x, y)$ is the coefficient of t^{i-1} in the polynomial $(\text{Ad}\,(tx+y))^{p-1}\,(x)$. □

Remark 2.8. If A is a p-restricted Lie algebra, then for $x \in A$ and $k \geq 1$ we can define $x^{[p^k]}$ by iterating the p^{th} power operation k times. □

The p^{th}-power operation on $\mathcal{L}^p(\Gamma)$ is induced by the operation of taking p^{th} powers in Γ. More precisely, consider $x \in \gamma_i^p(\Gamma)$. Letting $\overline{x} \in \mathcal{L}_i^p(\Gamma)$ be its image, the element $\overline{x}^{[p]} \in \mathcal{L}_{ip}^p(\Gamma)$ is the image of $x^p \in \gamma_{ip}^p(\Gamma)$. In particular, the p^{th} power operation on $\mathcal{L}^p(\Gamma)$ takes $\mathcal{L}_i^p(\Gamma)$ to $\mathcal{L}_{ip}^p(\Gamma)$.

We now make the following definition.

Definition 2.9. The *free p-restricted Lie algebra* on a set S is a p-restricted Lie algebra $\mathcal{FL}^p(S)$ generated by S such that for all p-restricted Lie algebras L, we have

$$\text{Hom}_{\text{Set}}(S, L) = \text{Hom}_{\text{pLie}}(\mathcal{FL}^p(S), L).$$

Here the right hand side is the set of morphisms of p-restricted Lie algebras. □

Remark 2.10. See [1, §2.7] for a textbook reference about $\mathcal{FL}^p(S)$ that in particular proves that it exists. □

The free p-restricted Lie algebra $\mathcal{FL}^p(S)$ has a natural grading that is respected by the Lie bracket and the p^{th} power operation. Denoting the i^{th} graded piece by $\mathcal{FL}_i^p(S)$, the degree 1 piece $\mathcal{FL}_1^p(S)$ is an $\mathbb{F}_p$-vector space with basis S. The p-restricted Lie algebra $\mathcal{FL}^p(S)$ is generated by $\mathcal{FL}_1^p(S)$ in the sense that its higher degree pieces are spanned by the result of repeatedly applying the Lie bracket operation and the p^{th} power operation to elements of $\mathcal{FL}_1^p(S)$.

Lazard proved the following theorem connecting the free group and the free p-restricted Lie algebra; see [20, Theorem 6.5].

Theorem 2.11. *If F is the free group on a set S and p is a prime, then $\mathcal{L}^p(F) \cong \mathcal{FL}^p(S)$ as graded p-restricted Lie algebras.*

2.4 The proof of Proposition 2.3

In this section, we prove Proposition 2.3 and thus complete the proof of Theorem D. We first recall the statement. Consider $n, p \geq 2$ with p prime. We must construct a finite p-group G, a central subgroup C of G, and a homomorphism $\Psi \colon C \to \mathbb{Z}/p$ such that the following two conditions hold.

- $\mathrm{H}_1(G; \mathbb{F}_p) = \mathbb{F}_p^n$.
- For all $g \in G$ whose image in $\mathrm{H}_1(G; \mathbb{F}_p)$ is nontrivial, some power of g lies in $C - \ker(\Psi)$.

Let S be an n-element set and let F be the free group on S. Pick $k \geq 1$ such that $p^k > (p-1)(n-1)$. (The reason for this assumption on k will become clear later). Set $G = F/\gamma^p_{p^k+1}(F)$, so

$$\mathrm{H}_1(G; \mathbb{F}_p) \cong G/\gamma^p_2(G) \cong F/\gamma^p_2(F) \cong \mathbb{F}_p^n.$$

By Theorem 2.11, we have

$$\mathcal{L}^p(G) = \bigoplus_{i=1}^{p^k} \mathcal{FL}^p_i(S).$$

Letting

$$C = \gamma^p_{p^k}(G) \cong \gamma^p_{p^k}(F)/\gamma^p_{p^k+1}(F) \cong \mathcal{FL}^p_{p^k}(S),$$

the fact that $\gamma^p_{p^k+1}(G) = 1$ implies that C is central in G. The needed homomorphism $\Psi \colon C \to \mathbb{Z}/p$ is now provided by Proposition 2.12 below.

Proposition 2.12. *Let $n \geq 2$, let p be a prime, and let S be an n-element set. Pick $k \geq 1$ such that $p^k > (p-1)(n-1)$. Then there exists an $\mathbb{F}_p$-linear map $\Psi \colon \mathcal{FL}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ such that $\Psi(v^{[p^k]}) \neq 0$ for all nonzero $v \in \mathcal{FL}^p_1(S)$.*

Proof. We begin with some preliminary observations. Let $\mathcal{A}^p(S)$ be the free associative $\mathbb{F}_p$-algebra on S. The algebra $\mathcal{A}^p(S)$ can be viewed as consisting of polynomials over $\mathbb{F}_p$ in the noncommuting variables S, and thus has a natural grading by degree. Let $\mathcal{A}^p_i(S)$ be its i^{th} graded piece, so

$$\mathcal{A}^p(S) = \bigoplus_{i=0}^{\infty} \mathcal{A}^p_i(S).$$

The associative algebra $\mathcal{A}^p(S)$ can be endowed with the structure of a p-restricted Lie algebra via the bracket

$$[x, y] = xy - yx \qquad (x, y \in \mathcal{A}^p(S))$$

and the ordinary p^{th} power operation

$$x^{[p]} = x^p \qquad (x \in \mathcal{A}^p(S)).$$

The inclusion $S \hookrightarrow \mathcal{A}^p(S)$ thus induces a homomorphism $\iota \colon \mathcal{FL}^p(S) \to \mathcal{A}^p(S)$ of graded p-restricted Lie algebras. Though we will not need this, we remark that ι is injective; see [1, Proposition 2.7.14].

We have a commutative diagram

$$\begin{array}{ccc} \mathcal{FL}^p_1(S) & \xrightarrow{\cong} & \mathcal{A}^p_1(S) \\ \downarrow & & \downarrow \\ \mathcal{FL}^p_{p^k}(S) & \longrightarrow & \mathcal{A}^p_{p^k}(S) \end{array}$$

whose horizontal arrows are ι and whose vertical arrows are the p^{th}-power operations. To construct a linear map $\Psi\colon \mathcal{FL}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ such that $\Psi(v^{[p^k]}) \neq 0$ for all nonzero $v \in \mathcal{FL}^p_1(S)$, it is thus enough to construct a linear map $\Phi\colon \mathcal{A}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ such that $\Phi(w^{p^k}) \neq 0$ for all nonzero $w \in \mathcal{A}^p_1(S)$.

Enumerate S as $S = \{x_1, \ldots, x_n\}$. For a linear map $\Phi\colon \mathcal{A}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$, define $f_\Phi\colon \mathbb{F}_p^n \to \mathbb{F}_p$ via the formula

$$f_\Phi(a_1, \ldots, a_n) = \Phi\left((a_1x_1 + \cdots + a_nx_n)^{p^k}\right) \qquad (a_1, \ldots, a_n \in \mathbb{F}_p).$$

We must find some linear map $\Phi\colon \mathcal{A}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ such that $f_\Phi(a_1, \ldots, a_n) \neq 0$ for all nonzero $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$.

Claim. *For any homogeneous polynomial $g \in \mathbb{F}_p[t_1, \ldots, t_n]$ of degree p^k, there exists a linear map $\Phi\colon \mathcal{A}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ such that $f_\Phi(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$.*

Proof of claim. Set $\mathcal{E} = \{(e_1, \ldots, e_n) \in \mathbb{Z}^n_{\geq 0} \mid e_1 + \cdots + e_n = p^k\}$. For $\mathbf{e} = (e_1, \ldots, e_n) \in \mathcal{E}$, define $\mathbf{t}^{\mathbf{e}} = t_1^{e_1} \cdots t_n^{e_n} \in \mathbb{F}_p[t_1, \ldots, t_n]$. Also, for $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$ define $\mathbf{a}^{\mathbf{e}} = a_1^{e_1} \cdots a_n^{e_n} \in \mathbb{F}_p$. Write $g = \sum_{\mathbf{e} \in \mathcal{E}} c_{\mathbf{e}} \mathbf{t}^{\mathbf{e}}$ with $c_{\mathbf{e}} \in \mathbb{F}_p$ for all $\mathbf{e} \in \mathcal{E}$. The vector space $\mathcal{A}_{p^k}(S)$ has a basis

$$\mathcal{B} = \{x_{i_1}^{e_{i_1}} x_{i_2}^{e_{i_2}} \cdots x_{i_m}^{e_{i_m}} \mid 1 \leq i_1, \ldots, i_m \leq n \text{ and } e_{i_1} + \cdots + e_{i_m} = p^k\}$$

For $b \in \mathcal{B}$, write $\mathbf{d}(b) = (d_1(b), \ldots, d_n(b))$, where $d_i(b)$ is the number of x_i factors that occur in b. For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$, we have

$$(a_1x_1 + \cdots + a_nx_n)^{p^k} = \sum_{b \in \mathcal{B}} \mathbf{a}^{\mathbf{d}(b)} b.$$

Define $\Phi\colon \mathcal{A}^p_{p^k}(S) \longrightarrow \mathbb{F}_p$ via the formula

$$\Phi(b) = \begin{cases} c_{\mathbf{e}} & \text{if } b = x_1^{e_1} \cdots x_n^{e_n} \text{ for some } \mathbf{e} = (e_1, \ldots, e_n) \in \mathcal{E}, \\ 0 & \text{otherwise} \end{cases} \qquad (b \in \mathcal{B}).$$

For $\mathbf{a} = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$, we then have

$$\begin{aligned} f_\Phi(a_1, \ldots, a_n) &= \Phi\left((a_1x_1 + \cdots + a_nx_n)^{p^k}\right) = \Phi\left(\sum_{b \in \mathcal{B}} \mathbf{a}^{\mathbf{d}(b)} b\right) \\ &= \sum_{\mathbf{e} \in \mathcal{E}} c_{\mathbf{e}} \mathbf{a}^{\mathbf{e}} = g(a_1, \ldots, a_n). \end{aligned}$$ □

We must therefore construct a homogeneous polynomial $g \in \mathbb{F}_p[t_1, \ldots, t_n]$ of degree p^k such that $g(a_1, \ldots, a_n) \neq 0$ for all nonzero $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$. For this, it will be helpful to be able to use a wider class of not necessarily homogeneous polynomials. For $g, g' \in \mathbb{F}_p[t_1, \ldots, t_n]$, write $g \sim g'$ if $g(a_1, \ldots, a_n) = g'(a_1, \ldots, a_n)$ for all $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$. If $g = t_1^{e_1} \cdots t_n^{e_n}$ and $g' = t_1^{e'_1} \cdots t_n^{e'_n}$ for some $e_1, \ldots, e_n, e'_1, \ldots, e'_n \geq 0$, we have $g \sim g'$ precisely when the following two conditions hold for all $1 \leq i \leq n$:

- $e_i \equiv e'_i \pmod{p-1}$, and
- $e_i = 0$ if and only if $e'_i = 0$.

We then have the following. We remark that this claim is where we use our assumption that $p^k > (p-1)(n-1)$.

Claim. *Consider a monomial $t_1^{e_1} \cdots t_n^{e_n}$ whose degree equals 1 modulo $p-1$. Then there exists a monomial $t_1^{e_1'} \cdots t_n^{e_n'}$ of degree p^k such that $t_1^{e_1} \cdots t_n^{e_n} \sim t_1^{e_1'} \cdots t_n^{e_n'}$.*

Proof of claim. One of the e_i must be nonzero. Reordering the variables if necessary, we can assume that $e_1 \neq 0$. Pick $e_1', \ldots, e_n'$ as follows. For $2 \leq i \leq n$, let $e_i' = 0$ if $e_i = 0$, and otherwise let e_i' be the unique number satisfying $0 < e_i' < p$ and $e_i' \equiv e_i \pmod{p-1}$. Next, let $e_1' = p^k - (e_2' + \cdots + e_n')$. Since $p^k > (p-1)(n-1) \geq e_2' + \cdots + e_n'$, the number e_1' is positive.

It is clear that $e_1' + \cdots + e_n' = p^k$ and that $e_i' = 0$ if and only if $e_i = 0$ for all $1 \leq i \leq n$. We must prove that $e_i \equiv e_i' \pmod{p-1}$ for all $1 \leq i \leq n$. The only nontrivial case is $i = 1$. For this, observe that modulo $p-1$ we have

$$\begin{aligned} e_1' &= p^k - (e_2' + \cdots + e_n') \equiv p^k - (e_2 + \cdots + e_n) = p^k + e_1 - (e_1 + \cdots + e_n) \\ &\equiv p^k + e_1 - 1 \equiv e_1, \end{aligned}$$

where the next to last $\equiv$ follows from the fact that $e_1 + \cdots + e_n \equiv 1 \pmod{p-1}$. □

By the above two claims, we see that the following claim implies the proposition.

Claim. *For all $n \geq 1$, there exists a polynomial $f_n \in \mathbb{F}_p[t_1, \ldots, t_n]$ with the following properties.*

- *The degree of each monomial appearing in f_n equals 1 modulo $p-1$.*
- *$f_n(a_1, \ldots, a_n) \neq 0$ for all nonzero $(a_1, \ldots, a_n) \in \mathbb{F}_p^n$.*

Proof of claim. For $f \in \mathbb{F}_p[t_1, \ldots, t_n]$, define $Z(f) = \{\mathbf{a} \in \mathbb{F}_p^n \mid f(\mathbf{a}) = 0\}$. Set $F(t_1, t_2) = t_1 - t_1 t_2^{p-1} + t_2$. We claim that for $g, h \in \mathbb{F}_p[t_1, \ldots, t_n]$ we have

$$Z(F(g,h)) = Z(g) \cap Z(h). \tag{2.1}$$

It is clear that $Z(g) \cap Z(h) \subset Z(F(g,h))$, so we only need to prove the other inclusion. Consider $\mathbf{a} \in Z(F(g,h))$. If $\mathbf{a} \notin Z(h)$, then

$$0 = F(g(\mathbf{a}), h(\mathbf{a})) = g(\mathbf{a}) - g(\mathbf{a})h(\mathbf{a})^{p-1} + h(\mathbf{a}) = g(\mathbf{a}) - g(\mathbf{a}) + h(\mathbf{a}) = h(\mathbf{a}) \neq 0,$$

a contradiction. We thus have $\mathbf{a} \in Z(h)$, which implies that

$$0 = F(g(\mathbf{a}), h(\mathbf{a})) = g(\mathbf{a}) - g(\mathbf{a})h(\mathbf{a})^{p-1} + h(\mathbf{a}) = g(\mathbf{a}),$$

so $\mathbf{a} \in Z(g)$ and thus $\mathbf{a} \in Z(g) \cap Z(h)$, as desired.

We now construct f_n by induction on n. For the base case $n = 1$, we simply set $f_1 = t_1$. Now assume that $n > 1$ and that f_{n-1} has been constructed. Define $f_n = F(f_{n-1}, t_n)$. The first conclusion of the claim is clearly satisfied, and the second follows from (2.1). □

This completes the proof of the proposition. □

3 The proof of Theorem C

In this section, we prove Theorem C. We first recall the setup. Let $n \geq 2$ and let $\mathcal{O} \subset F_n$ be contained in the union of finitely many $\text{Aut}(F_n)$-orbits. Our goal is to construct a finite-index $R \lhd F_n$ with $\text{H}_1^{\mathcal{O}}(R; \mathbb{Q}) \neq \text{H}_1(R; \mathbb{Q})$. If $\mathcal{O}' \subset F_n$ satisfies $\mathcal{O} \subset \mathcal{O}'$, then $\text{H}_1^{\mathcal{O}}(R; \mathbb{Q}) \subset \text{H}_1^{\mathcal{O}'}(R; \mathbb{Q})$. From this, we see that without loss of generality we can enlarge $\mathcal{O}$ and assume that $\mathcal{O}$ is actually equal to the union of finitely many $\text{Aut}(F_n)$-orbits. Let $\mathfrak{S} \subset F_n$ be the finite set such that $\mathcal{O} = \text{Aut}(F_n) \cdot \mathfrak{S}$. Without loss of generality, we can assume that $1 \notin \mathfrak{S}$.

The construction will have three steps. Recall that a subgroup of F_n is characteristic if it is preserved by all elements of $\text{Aut}(F_n)$.

Step 1. *For all $s \in \mathfrak{S}$, we construct a finite-index characteristic subgroup $R_1^s \lhd F_n$ with the following property. Consider an element $x \in F_n$ that is in the* $\text{Aut}(F_n)$*-orbit of s. Pick $m \geq 1$ such that $x^m \in R_1^s$. Then $[x^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero.*

By Marshall Hall's Theorem ([15]; see [31] for a simple proof), there exists a finite-index $T < F_n$ such that $s \in T$ and such that s is a primitive element of T. Define

$$R_1^s = \bigcap_{\phi \in \text{Aut}(F_n)} \phi(T),$$

so R_1^s is a finite-index subgroup of F_n that is contained in T and is characteristic. Consider some $x \in F_n$ such that there exists $\phi \in \text{Aut}(F_n)$ with $\phi(x) = s$. Pick $m \geq 1$ such that $x^m \in R_1^s$. Our goal is to prove that $[x^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero. Since R_1^s is a characteristic subgroup of F_n, the group $\text{Aut}(F_n)$ acts on R_1^s and thus on $\text{H}_1(R_1^s; \mathbb{Q})$. Observe that

$$\phi([x^m]) = [\phi(x)^m] = [s^m] \in \text{H}_1(R_1^s; \mathbb{Q}).$$

To prove that $[x^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero, it is thus enough to prove that $[s^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero. The inclusion map $R_1^s \hookrightarrow T$ takes s^m to s^m, and thus the induced map $\text{H}_1(R_1^s; \mathbb{Q}) \to \text{H}_1(T; \mathbb{Q})$ takes $[s^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ to $[s^m] \in \text{H}_1(T; \mathbb{Q})$. Since s is a primitive element of T, it follows that $[s] \in \text{H}_1(T; \mathbb{Q})$ is nonzero and hence that $[s^m] \in \text{H}_1(T; \mathbb{Q})$ is nonzero. We conclude that $[s^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero, as desired.

Step 2. *We construct a finite-index characteristic subgroup $R_1 \lhd F_n$ with the following property. Consider $x \in \mathcal{O}$. Pick $m \geq 1$ such that $x^m \in R_1$. Then, $[x^m] \in \text{H}_1(R_1; \mathbb{Q})$ is nonzero.*

Define

$$R_1 = \bigcap_{s \in \mathfrak{S}} R_1^s.$$

Since R_1 is a finite intersection of finite-index characteristic subgroups of F_n, it is also a finite-index characteristic subgroup. Consider $x \in \mathcal{O}$ and some $m \geq 1$ such that $x^m \in R_1$. We must prove that $[x^m] \in \text{H}_1(R_1; \mathbb{Q})$ is nonzero. Let $s \in \mathfrak{S}$ be such that x is in the $\text{Aut}(F_n)$-orbit of s. We have $x^m \in R_1^s$, and by the previous step the element $[x^m] \in \text{H}_1(R_1^s; \mathbb{Q})$ is nonzero. An argument like in the previous step now implies that $[x^m] \in \text{H}_1(R_1; \mathbb{Q})$ is nonzero, as desired.

Step 3. *We construct a finite-index $R \lhd F_n$ with $\text{H}_1^{\mathcal{O}}(R; \mathbb{Q}) \neq \text{H}_1(R; \mathbb{Q})$.*

For each $s \in \mathfrak{S}$, pick $m_s \geq 1$ such that $s^{m_s} \in R_1$. Since each $[s^{m_s}] \in \mathrm{H}_1(R_1;\mathbb{Q})$ is nonzero, there exists some large prime p such that each s^{m_s} projects to a nonzero element of $\mathrm{H}_1(R_1;\mathbb{F}_p)$. Applying Theorem D to R_1, we can find a finite-index subgroup $R \lhd R_1$ such that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$, where here $\mathfrak{O}_p$ refers to the p-primitive elements of R_1, *not* of F_n. We claim that $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$, where by $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q})$ we are considering R as a subgroup of F_n. To prove this, it is enough to prove that $\mathrm{H}_1^{\mathcal{O}}(R;\mathbb{Q}) \subset \mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q})$. Consider some $x \in \mathcal{O}$. Pick $\phi \in \mathrm{Aut}(F_n)$ and $s \in \mathfrak{S}$ such that $\phi(x) = s$. Since R_1 is a characteristic subgroup of F_n, the group $\mathrm{Aut}(F_n)$ acts on R_1 and thus on $\mathrm{H}_1(R_1;\mathbb{F}_p)$. We have

$$\phi([x^{m_s}]) = [\phi(x)^{m_s}] = [s^{m_s}] \in \mathrm{H}_1(R_1;\mathbb{F}_p).$$

Since $[s^{m_s}] \in \mathrm{H}_1(R_1;\mathbb{F}_p)$ is nonzero, so is $[x^{m_s}] \in \mathrm{H}_1(R_1;\mathbb{F}_p)$. Pick $m \geq 1$ such that $(x^{m_s})^m \in R$. We then have $[(x^{m_s})^m] \in \mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q})$, as desired.

4 Transvections: Theorem E

In this section, we prove Theorem E, which concerns the subgroup of $\mathrm{Out}(F_n)$ generated by powers of transvections. There are two sections. In §4.1, we discuss the chain action, which will play a key role in our proof. The proof itself is in §4.2.

4.1 The action of $\mathrm{Aut}(F_n)$ on chains

In this section, we construct a family of linear representations $\mathcal{M}_R$ of subgroups of $\mathrm{Aut}(F_n)$ that are indexed by subgroups $R \lhd F_n$. Our construction generalizes Suzuki's geometric construction of the classical Magnus representation [33], which corresponds to the case $R = [F_n, F_n]$. Since we allow F_n/R to be nonabelian, one can consider $\mathcal{M}_R$ as a kind of "nonabelian Magnus representation".

Setup. Fix a subgroup $R \lhd F_n$ and a field $\mathbf{k}$. Set $G = F_n/R$. The conjugation action of F_n on R induces an action of G on $\mathrm{H}_1(R;\mathbf{k})$. When R is finite-index and $\mathbf{k}$ has characteristic 0, this G-module is described by Theorem 2.2 above. Define

$$\mathrm{Aut}(F_n, R) = \{\phi \in \mathrm{Aut}(F_n) \mid \phi(R) = R\}.$$

The group $\mathrm{Aut}(F_n, R)$ acts on $\mathrm{H}_1(R;\mathbf{k})$; however, this action can be very complicated. To help us understand it, we embed $\mathrm{H}_1(R;\mathbf{k})$ into a larger vector space. This requires some topological preliminaries.

Graph homotopy-equivalences. Fix a free basis $S = \{x_1, \ldots, x_n\}$ for F_n. Let X_n be an oriented graph with a single vertex $*$ and with edges $\{e_1, \ldots, e_n\}$. For $1 \leq i \leq n$, the edge e_i is an oriented loop based at $*$, and we identify F_n with $\pi_1(X_n, *)$ in such a way as to identify x_i with the homotopy class of the loop e_i. The group $\mathrm{Aut}(F_n)$ can be identified with the group of homotopy classes of homotopy equivalences of X_n that fix $*$.

Lifting homotopy-equivalences. Let $\pi\colon (\widetilde{X}_n, \widetilde{*}) \to (X_n, *)$ be the based cover corresponding to $R \subset F_n$, so $\mathrm{H}_1(\widetilde{X}_n;\mathbf{k}) = \mathrm{H}_1(R;\mathbf{k})$. For a continuous map $f\colon (X_n, *) \to (X_n, *)$, we know from covering space theory that f can be lifted to a map $\widetilde{f}\colon (\widetilde{X}_n, \widetilde{*}) \to (\widetilde{X}_n, \widetilde{*})$ if and only if $f_*(R) \subset R$. From this, we see that the group $\mathrm{Aut}(F_n, R)$ acts on $\widetilde{X}_n$ by homotopy equivalences that fix $\widetilde{*}$. The resulting action of $\mathrm{Aut}(F_n, R)$ on $\mathrm{H}_1(\widetilde{X}_n;\mathbf{k}) = \mathrm{H}_1(R;\mathbf{k})$ is precisely the action arising from the restriction of the action of $\mathrm{Aut}(F_n, R)$ to R.

Action on chains. Since $\widetilde{X}_n$ is a 1-dimensional cell complex, the vector space $\mathrm{H}_1(\widetilde{X}_n;\mathbf{k})$ is a subspace of the cellular chain group $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$. Namely,

$$\mathrm{H}_1(\widetilde{X}_n;\mathbf{k}) = \ker(\mathrm{C}_1(\widetilde{X}_n;\mathbf{k}) \xrightarrow{\partial} \mathrm{C}_0(\widetilde{X}_n;\mathbf{k})).$$

The action of $\mathrm{Aut}(F_n, R)$ on $\widetilde{X}_n$ by homotopy equivalences induces an action of $\mathrm{Aut}(F_n, R)$ on $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ that restricts to the above action on $\mathrm{H}_1(\widetilde{X}_n;\mathbf{k})$. It turns out that $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ is far easier to understand than $\mathrm{H}_1(\widetilde{X}_n;\mathbf{k})$. Note that this action on 1-chains was also studied in [11, 12, 13].

The G-module structure. Observe that the action of the deck group $G = F_n/R$ on $\widetilde{X}_n$ endows each cellular chain group $\mathrm{C}_k(\widetilde{X}_n;\mathbf{k})$ with the structure of a G-module. It is easy to understand these G-modules:

- We can identify the vertices of $\widetilde{X}_n$ with G via the bijection taking $g \in G$ to $g(\widetilde{*})$. Using this identification, we obtain a G-equivariant isomorphism $\mathrm{C}_0(\widetilde{X}_n;\mathbf{k}) \cong \mathbf{k}[G]$.
- For $1 \leq i \leq n$, let $\widetilde{e}_i$ be the oriented edge of $\widetilde{X}_n$ that starts at $\widetilde{*}$ and projects to $e_i \subset S_n$. The edges of $\widetilde{X}_n$ are precisely $\{g(\widetilde{e}_i) \mid g \in G,\, 1 \leq i \leq n\}$. Using this, we obtain a G-equivariant isomorphism $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k}) \cong (\mathbf{k}[G])^n$.

The boundary map $\partial\colon \mathrm{C}_1(\widetilde{X}_n;\mathbf{k}) \to \mathrm{C}_0(\widetilde{X}_n;\mathbf{k})$ is G-equivariant, so $\mathrm{H}_1(R;\mathbf{k}) \subset \mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ is a G-submodule. This G-action agrees with the action of G on $\mathrm{H}_1(R;\mathbf{k})$ induced by the conjugation action of F_n on R via the surjection $F_n \to G$.

The representation. Combining the above action of $\mathrm{Aut}(F_n, R)$ on $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ with the above identification of $\mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ with $(\mathbf{k}[G])^n$, we obtain a homomorphism

$$\widehat{\mathcal{M}}_R\colon \mathrm{Aut}(F_n, R) \longrightarrow \mathrm{Aut}_{\mathbf{k}}\left((\mathbf{k}[G])^n\right).$$

Unfortunately, the image of $\widehat{\mathcal{M}}_R$ does *not* preserve the G-module structure on $(\mathbf{k}[G])^n$. Instead, we have

$$\widehat{\mathcal{M}}_R(\phi)(g \cdot v) = \phi_*(g) \cdot \widehat{\mathcal{M}}_R(\phi)(v) \qquad \left(\phi \in \mathrm{Aut}\left(F_n, R\right), g \in G, v \in (\mathbf{k}[G])^n\right),$$

where $\phi_* \in \mathrm{Aut}(G)$ is the induced action of $\phi \in \mathrm{Aut}(F_n, R)$ on $G = F_n/R$. To fix this, define

$$\mathrm{Aut}_R(F_n) = \{\phi \in \mathrm{Aut}(F_n, R) \mid \phi \text{ acts trivially on } G\}.$$

We then obtain a homomorphism

$$\mathcal{M}_R\colon \mathrm{Aut}_R(F_n) \longrightarrow \mathrm{Aut}_G\left((\mathbf{k}[G])^n\right).$$

Note that since the action on 1-chains induces the action on homology, this representation $\mathcal{M}_R$ is an extension of the action on $\mathrm{H}_1(R;\mathbf{k}) \subset \mathrm{C}_1(\widetilde{X}_n;\mathbf{k}) \cong (\mathbf{k}[G])^n$. For computations in coordinates with $\mathcal{M}_R$, we will need to use a basis. The *standard basis* for $(\mathbf{k}[G])^n$ is the set $\{\overline{e}_1, \ldots, \overline{e}_n\}$, where $\overline{e}_i \in (\mathbf{k}[g])^n \cong \mathrm{C}_1(\widetilde{X}_n;\mathbf{k})$ is the chain corresponding to the oriented edge $\widetilde{e}_i$ of $\widetilde{X}_n$.

Remark 4.1. The precise representation $\mathrm{Aut}_R(F_n) \longrightarrow \mathrm{Aut}_G\left((\mathbf{k}[G])^n\right)$ depends on the choice of basis S of F_n, but it is always an extension of the action on $\mathrm{H}_1(R;\mathbf{k})$. □

Image of a transvection. Recall that $S = \{x_1, \ldots, x_n\}$. In the introduction we defined the transvection $\tau_{S,x_1,x_2} \in \mathrm{Aut}(F_n)$ via the formula

$$\tau_{S,x_1,x_2}(x_i) = \begin{cases} x_2 x_i & \text{if } i = 1, \\ x_i & \text{if } i \neq 1 \end{cases} \qquad (1 \leq i \leq n).$$

Assume that $x_2^m \in R$ for some $m \geq 1$. Examining our definitions, we see that $\tau_{S,x_1,x_2}^m \in \mathrm{Aut}_R(F_n)$. The following lemma calculates the image of τ_{S,x_1,x_2} under $\mathcal{M}_R$.

Lemma 4.2. *For some $n \geq 1$, let $R \lhd F_n$ be finite-index, let $\mathbf{k}$ be a field, and let $\{x_1, \ldots, x_n\}$ be a basis for F_n. Let $G = F_n/R$, and for $1 \leq i \leq n$ let $g_i \in G$ be the image of $x_i \in F_n$. Finally, let $\{\overline{e}_1, \ldots, \overline{e}_n\}$ be the standard basis for $(\mathbf{k}[G])^n$. If $m \geq 1$ is such that $x_1^m \in R$, then*

$$\mathcal{M}_R(\tau_{S,x_1,x_2}^m)(\overline{e}_i) = \begin{cases} \overline{e}_i + \overline{e}_2 + g_2 \cdot \overline{e}_2 + g_2^2 \cdot \overline{e}_2 + \cdots + g_2^{m-1} \cdot \overline{e}_2 & \text{if } i = 1, \\ \overline{e}_i & \text{if } i \neq 1 \end{cases} \qquad (1 \leq i \leq n).$$

Proof. The indicated calculation is only nontrivial for $i = 1$. For that case, observe that $\tau_{S,x_1,x_2}^m(x_1) = x_2^m x_1$. Using the concatenation product for paths, the loop in X_n corresponding to $x_2^m x_1$ is $e_2^m e_1$. The lift of this to $\widetilde{X}_n$ is the path

$$(\widetilde{e}_2)(g_2 \cdot \widetilde{e}_2)(g_2^2 \cdot \widetilde{e}_2) \cdots (g_2^{m-1} \cdot \widetilde{e}_2)(g_2^m \cdot \widetilde{e}_1) = (\widetilde{e}_2)(g_2 \cdot \widetilde{e}_2)(g_2^2 \cdot \widetilde{e}_2) \cdots (g_2^{m-1} \cdot \widetilde{e}_2)(\widetilde{e}_1).$$

The lemma follows. □

4.2 Theorem E

We now give the proof of Theorem E. The heart of our argument is the following more precise result for $\mathrm{Aut}(F_n)$. For its statement, observe that if G is a finite group, $\pi\colon F_n \to G$ is a surjection with kernel R, and V is an irreducible representation of G over a field $\mathbf{k}$ of characteristic 0, then the action of $\mathrm{Aut}_R(F_n)$ on $\mathrm{H}_1(R; \mathbf{k})$ preserves the V-isotypic component.

Proposition 4.3. *For some $n \geq 2$, let G be a finite group and let $\pi\colon F_n \to G$ be a surjection. Assume that there exists an irreducible $\mathbb{Q}$-representation V of G such that for all primitive $x \in F_n$, the action of $\pi(x)$ on V fixes no nonzero vectors. Let $R = \ker(\pi)$, let $W \subset \mathrm{H}_1(R; \mathbb{Q})$ be the V-isotypic component, and let $\Phi\colon \mathrm{Aut}_R(F_n) \to \mathrm{GL}(W)$ be the restriction to W of the action of $\mathrm{Aut}_R(F_n)$ on $\mathrm{H}_1(R; \mathbb{Q})$. Then the following hold.*

- *The image of Φ has infinite order elements.*
- *Let $m \geq 1$ be divisible by the orders in G of all elements of $\{\pi(x) \mid x \in F_n \text{ primitive}\}$. Then the m^{th} power of any transvection lies in $\ker(\Phi)$.*

Proof. Farb–Hensel [5, Theorem 1.1] proved that the $\mathrm{Aut}_R(F_n)$-orbit of a nonzero vector in $\mathrm{H}_1(R; \mathbb{Q})$ is infinite. Moreover, they showed that for any nonzero $v \in \mathrm{H}_1(R; \mathbb{Q})$, there is a $\phi \in \mathrm{Aut}_R(F_n)$ such that $\{\phi^k(v) \mid k \in \mathbb{Z}\}$ is infinite. Since the action of $\mathrm{Aut}_R(F_n)$ on $\mathrm{H}_1(R; \mathbb{Q})$ preserves W (which is nonzero by Theorem 2.2), we deduce that the image of Φ has infinite order elements.

Now consider any basis $S = \{x_1, \ldots, x_n\}$ for F_n. We must prove that $\tau_{S,x_1,x_2}^m \in \ker(\Phi)$. Consider the representation $\mathcal{M}_R\colon \mathrm{Aut}_R(F_n) \to \mathrm{Aut}_G((\mathbb{Q}[G])^n)$ defined in §4.1.

Let $\{\overline{e}_1, \ldots, \overline{e}_n\}$ be the standard basis for $(\mathbb{Q}[G])^n$ and for $1 \leq i \leq n$ define $g_i = \pi(x_i) \in G$. By Lemma 4.2, we have

$$\mathcal{M}_R(\tau^m_{S,x_1,x_2})(\overline{e}_i) = \begin{cases} \overline{e}_i + \overline{e}_2 + g_2 \cdot \overline{e}_2 + g_2^2 \cdot \overline{e}_2 + \cdots + g_2^{m-1} \cdot \overline{e}_2 & \text{if } i = 1, \\ \overline{e}_i & \text{if } i \neq 1 \end{cases} \qquad (1 \leq i \leq n).$$

The element $\overline{e}_2 + g_2 \cdot \overline{e}_2 + g_2^2 \cdot \overline{e}_2 + \cdots + g_2^{m-1} \cdot \overline{e}_2$ of $(\mathbb{Q}[G])^n$ is fixed by g_2, and thus projects to 0 in the V-isotypic component of $(\mathbb{Q}[G])^n$. We conclude that $\mathcal{M}_R(\tau^m_{S,x_1,x_2})$ acts as the identity on the V-isotypic component of $(\mathbb{Q}[G])^n$, which implies that $\tau^m_{S,x_1,x_2} \in \ker(\Phi)$, as desired. □

In Proposition 4.3, we restrict ourselves to representations over $\mathbb{Q}$ since those are required in [5, Theorem 1.1]. The following lemma produces an appropriate representation over $\mathbb{Q}$ from one over an arbitrary field of characteristic 0.

Lemma 4.4. *For some $n \geq 2$, let G be a finite group and let $\pi \colon F_n \to G$ be a surjection. Assume that for some field $\mathbf{k}$ of characteristic 0, there exists a $\mathbf{k}$-representation V of G such that for all primitive $x \in F_n$, the action of $\pi(x)$ on V fixes no nonzero vectors. Then there exists an irreducible $\mathbb{Q}$-representation V' of G such that for all primitive $x \in F_n$, the action of $\pi(x)$ on V' fixes no nonzero vectors.*

Proof. Let $v \in V$ be a nonzero vector. Since $\mathbf{k}$ contains $\mathbb{Q}$ as a subfield, we can let V'' be the $\mathbb{Q}$-span in V of the G-orbit of v. The group G acts on the $\mathbb{Q}$-vector space V'', and any irreducible subrepresentation V' of V'' satisfies the conclusion of the lemma. □

Proof of Theorem E. We first recall the statement. Fix some $n \geq 2$, and for $k \geq 1$ let $\mathfrak{G}_{n,k} \subset \mathrm{Out}(F_n)$ be the subgroup generated by k^{th} powers of transvections. We must prove that there exists an infinite set of positive numbers $\mathcal{K}_n$ such that $\mathrm{Out}(F_n)/\mathfrak{G}_{n,k}$ contains infinite-order elements for all $k \in \mathcal{K}_n$.

Define

$$\mathcal{K}_n = \{k \mid \text{there exists a prime power } p^e \text{ dividing } k \text{ such that } p^e > p(p-1)(n-1)\}.$$

To prove that $\mathcal{K}_n$ satisfies the conclusion of the theorem, it is enough to prove that if p^e is a prime power satisfying $p^e > p(p-1)(n-1)$, then $\mathrm{Out}(F_n)/\mathfrak{G}_{n,p^e}$ contains infinite-order elements. Lemma 4.4 and the proof of Theorem D gives the following:

- A surjection $\pi \colon F_n \to G$ to a finite group such that for all p-primitive $x \in F_n$, the order of $\pi(x)$ is p^e.
- An irreducible $\mathbb{Q}$-representation V of G such that for all p-primitive $x \in F_n$, the action of $\pi(x)$ on V fixes no nonzero vectors.

We remark that these two bullet points hold in particular for each primitive $x \in F_n$. Let W be the V-isotypic component of $\mathrm{H}_1(R; \mathbb{Q})$ and let $\Phi \colon \mathrm{Aut}_R(F_n) \to \mathrm{Aut}_G(W)$ be the resulting action. Define $\Gamma = \mathrm{Im}(\Phi)$. Proposition 4.3 implies that Γ contains infinite-order elements and that $(p^e)^{\text{th}}$ powers of transvections lie in $\ker(\Phi)$. This implies that the quotient of $\mathrm{Aut}(F_n)$ by the subgroup generated by $(p^e)^{\text{th}}$ powers of transvections contains infinite-order elements.

We will upgrade this to $\mathrm{Out}(F_n)$ as follows. Define $\mathrm{Out}_R(F_n)$ to be the image of $\mathrm{Aut}_R(F_n)$ in $\mathrm{Out}(F_n)$. Unfortunately, it is not quite true that Φ factors through $\mathrm{Out}_R(F_n)$, but this almost holds. Let $\mathrm{Inn}(F_n) \cong F_n$ be the group of inner automorphisms and let $\mathrm{Inn}_R(F_n) = \mathrm{Inn}(F_n) \cap \mathrm{Aut}_R(F_n)$. By definition, we have

$$\mathrm{Inn}_R(F_n) = \{x \in F_n \mid \pi(x) \in G \text{ is central}\}.$$

The image $\Phi(\mathrm{Inn}_R(F_n)) \subset \Gamma$ is a finite subgroup of the center of Γ. Letting

$$\overline{\Gamma} = \Gamma/\Phi(\mathrm{Inn}_R(F_n)),$$

we obtain a surjective homomorphism $\overline{\Phi}\colon \mathrm{Out}_R(F_n) \to \overline{\Gamma}$. Since $\overline{\Gamma}$ contains infinite-order elements and $\mathfrak{G}_{n,p^e} \subset \ker(\overline{\Phi})$, the theorem follows. □

5 Integral representations: the proofs of Theorems F and G

We now prove Theorems F and G via an argument of Koberda–Santharoubane [19]. We will give the details for Theorem G; the proof of Theorem F is similar. We start by recalling the statement of Theorem G. Fix some $n \geq 2$ and some prime p. We must construct an integral linear representation $\rho\colon F_n \to \mathrm{GL}_d(\mathbb{Z})$ with the following two properties.

- The image of ρ is infinite.
- For all p-primitive $x \in F_n$, the image $\rho(x)$ has finite order.

Use Theorem D to find a finite-index $R \lhd F_n$ such that $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q}) \neq \mathrm{H}_1(R;\mathbb{Q})$. Define $G = F_n/R$ and $\widehat{\Gamma} = F_n/[R,R]$. We thus have a short exact sequence

$$1 \longrightarrow \mathrm{H}_1(R;\mathbb{Z}) \longrightarrow \widehat{\Gamma} \longrightarrow G \longrightarrow 1.$$

The action of G on $\mathrm{H}_1(R;\mathbb{Z})$ preserves the subgroup $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Z})$, and hence $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Z})$ is a normal subgroup of $\widehat{\Gamma}$. Define $\Gamma = \widehat{\Gamma}/\,\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Z})$. Setting $A = \mathrm{H}_1(R;\mathbb{Z})/\,\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Z})$, we thus have a short exact sequence

$$1 \longrightarrow A \longrightarrow \Gamma \longrightarrow G \longrightarrow 1.$$

Since $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Q})$ is a proper subspace of $\mathrm{H}_1(R;\mathbb{Q})$, the group A is infinite. Let $\pi\colon F_n \to \Gamma$ be the projection, and consider some p-primitive $x \in F_n$. Let m be the order of the image of x in $G = F_n/R$. It follows from the definition of $\mathrm{H}_1^{\mathfrak{O}_p}(R;\mathbb{Z})$ that $\pi(x^m) = 1$, and thus that $\pi(x)$ has finite order.

Since A is a finitely generated abelian group, there is a faithful integral linear representation $A \hookrightarrow \mathrm{GL}_{d'}(\mathbb{Z})$ for some $d' \geq 1$. Since A is a finite-index subgroup of Γ, we can induce this representation up to Γ to get a faithful integral linear representation $\Gamma \hookrightarrow \mathrm{GL}_d(\mathbb{Z})$ for some $d \geq 1$. The desired integral linear representation of F_n is then the composition

$$F_n \xrightarrow{\pi} \Gamma \hookrightarrow \mathrm{GL}_d(\mathbb{Z}).$$

References

[1] Yu. A. Bahturin, *Identical relations in Lie algebras*, translated from the Russian by Bahturin, VNU Science Press, b.v., Utrecht, 1987.

[2] M. R. Bridson and K. Vogtmann, Homomorphisms from automorphism groups of free groups, Bull. London Math. Soc. 35 (2003), no. 6, 785–792.

[3] J. D. Dixon, M. Du Sautoy, A. Mann, and D. Segal, *Analytic pro-p groups*, second edition, Cambridge Studies in Advanced Mathematics, 61, Cambridge University Press, Cambridge, 1999.

[4] B. Farb and S. Hensel, Finite covers of graphs, their primitive homology, and representation theory, New York J. Math. 22 (2016), 1365–1391.

[5] B. Farb and S. Hensel, Moving homology classes in finite covers of graphs, Israel J. Math. 220 (2017), no. 2, 605–615.

[6] B. Farb and D. Margalit, *A primer on mapping class groups*, Princeton Mathematical Series, 49, Princeton University Press, Princeton, NJ, 2012.

[7] L. Funar, On the TQFT representations of the mapping class groups, Pacific J. Math. 188 (1999), no. 2, 251–274.

[8] W. Gaschütz, Über modulare Darstellungen endlicher Gruppend, die von freien Gruppen induziert werden, Math. Z. 60 (1954), 274–286.

[9] F. Grunewald, M. Larsen, A. Lubotzky, and J. Malestein, Arithmetic quotients of the mapping class group, Geom. Funct. Anal. 25 (2015), no. 5, 1493–1542.

[10] F. Grunewald and A. Lubotzky, Linear representations of the automorphism group of a free group, Geom. Funct. Anal. 18 (2009), no. 5, 1564–1608.

[11] A. Hadari, Every Infinite order mapping class has an infinite order action on the homology of some finite cover, preprint, arxiv.org/abs/1508.01555

[12] A. Hadari, Homological eigenvalues of lifts of pseudo-Anosov mapping classes to finite covers, preprint, arxiv.org/abs/1712.01416

[13] A. Hadari, Non virtually solvable subgroups of mapping class groups have non virtually solvable representations, preprint, arxiv.org/abs/1805.01527

[14] M. Isaacs, *Finite group theory*, Graduate Studies in Mathematics, 92, American Mathematical Society, Providence, RI, 2008.

[15] M. Hall, Jr., Coset representations in free groups, Trans. Amer. Math. Soc. 67 (1949), 421–432.

[16] A. Kent (`https://mathoverflow.net/users/1335/autumn-kent`), Homology generated by lifts of simple curves, URL (version: 2012-01-29): `https://mathoverflow.net/q/86938`

[17] T. Koberda, Asymptotic linearity of the mapping class group and a homological version of the Nielsen-Thurston classification, Geom. Dedicata 156 (2012), 13–30.

[18] T. Koberda, Alexander varieties and largeness of finitely presented groups, J. Homotopy Relat. Struct. 9 (2014), no. 2, 513–531.

[19] T. Koberda and R. Santharoubane, Quotients of surface groups and homology of finite covers via quantum representations, Invent. Math. 206 (2016), no. 2, 269–292.

[20] M. Lazard, Sur les groupes nilpotents et les anneaux de Lie, Ann. Sci. Ecole Norm. Sup. (3) 71 (1954), 101–190.

[21] Y. Liu, Virtual homological spectral radii for automorphisms of surfaces, preprint, arxiv.org/abs/1710.05039.

[22] E. Looijenga, Prym representations of mapping class groups, Geom. Dedicata 64 (1997), no. 1, 69–83.

[23] E. Looijenga, Some algebraic geometry related to the mapping class group, abstract of talk at June 2015 Oberwolfach workshop “New Perspectives on the Interplay between Discrete Groups in Low-Dimensional Topology and Arithmetic Lattice”, available at `https://www.staff.science.uu.nl/ looij101/eduardlooijengaOWjuni2015.pdf`

[24] J. Marché (`https://mathoverflow.net/users/14547/julien-marche`), Homology generated by lifts of simple curves, URL (version: 2012-01-28): `https://mathoverflow.net/q/86894`

[25] G. Masbaum, An element of infinite order in TQFT-representations of mapping class groups, in *Low-dimensional topology (Funchal, 1998)*, 137–139, Contemp. Math., 233, Amer. Math. Soc., Providence, RI.

[26] C. McMullen, Entropy on Riemann surfaces and the Jacobians of finite covers, Comment. Math. Helv. 88 (2013), no. 4, 953–964.

[27] A. Putman and B. Wieland, Abelian quotients of subgroups of the mappings class group and higher Prym representations, J. Lond. Math. Soc. (2) 88 (2013), no. 1, 79–96.

[28] Representations of p-groups where 1 is never an eigenvalue, URL (version: 2016-02-26): `https://mathoverflow.net/q/232227`

[29] J. J. Rotman, *An introduction to the theory of groups*, fourth edition, Graduate Texts in Mathematics, 148, Springer-Verlag, New York, 1995.

[30] J.-P. Serre, *Lie algebras and Lie groups*, Lectures given at Harvard University, 1964, W. A. Benjamin, Inc., New York, 1965.

[31] J. R. Stallings, Topology of finite graphs, Invent. Math. 71 (1983), no. 3, 551–565.

[32] H. Sun, Virtual homological spectral radius and mapping torus of pseudo-Anosov maps, Proc. Amer. Math. Soc. 145 (2017), no. 10, 4551–4560.

[33] M. Suzuki, Geometric interpretation of the Magnus representation of the mapping class group, Kobe J. Math. 22 (2005), no. 1-2, 39–47.

[34] H. Zassenhaus, Ein Verfahren, jeder endlichenp-Gruppe einen Lie-Ring mit der Charakteristik p zuzuordnen, Abh. Math. Sem. Univ. Hamburg 13 (1939), no. 1, 200–207.

[35] E. Zelmanov, On some open problems related to the restricted Burnside problem, in *Recent progress in algebra (Taejon/Seoul, 1997)*, 237–243, Contemp. Math., 224, Amer. Math. Soc., Providence, RI.

Justin Malestein
University of Oklahoma
Department of Mathematics
601 Elm Ave
Norman, OK 73019
`jmalestein@math.ou.edu`

Andrew Putman
Department of Mathematics
University of Notre Dame
279 Hurley Hall
Notre Dame, IN 46556
`andyp@nd.edu`