Simple closed curves, finite covers of surfaces, and power subgroups of 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 $O \subset F_n$ which is contained in the union of finitely many 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 $O$. These examples answer questions of Farb–Hensel, Kent, Looijenga, and Marché. We also show that the quotient of 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 $O \subset F_n$ which is contained in the union of finitely many Aut($F_n$)-orbits, we construct integral linear representations of free groups that have infinite image and map all elements of $O$ to torsion elements.

1 Introduction
Let $\Sigma_{g,n}$ be a genus $g$ surface with $n$ punctures and let Mod$_{g,n}$ be its mapping class group. An important classical tool for studying Mod$_{g,n}$ is its action on $H_1(\Sigma_{g,n})$. Recently there has been a lot of interest in studying the action of 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 Mod$_{g,n}$.

Simple closed curve homology. Let $\pi: \tilde{\Sigma} \to \Sigma_{g,n}$ be a finite cover. The simple closed curve homology of $\tilde{\Sigma}$, denoted $H_{scc}^1(\tilde{\Sigma})$, is the subspace of $H_1(\tilde{\Sigma})$ spanned by the set

$$\{[\tilde{\gamma}] \in H_1(\tilde{\Sigma}) \mid \tilde{\gamma} \text{ is a component of } \pi^{-1}(\gamma) \text{ for a simple closed curve } \gamma \text{ on } \Sigma_{g,n}\}.$$  

Another more algebraic way to describe $H_{scc}^1(\tilde{\Sigma})$ is as follows. Let $R \subset \pi_1(\Sigma_{g,n})$ be the subgroup corresponding to $\tilde{\Sigma}$. We have $H_1(\tilde{\Sigma}) = H_1(R)$, and $H_{scc}^1(\tilde{\Sigma})$ is the span of the set

$$\{[x^k] \in H_1(R) \mid x \in \pi_1(\Sigma_{g,n}) \text{ is a simple closed curve and } k \geq 1 \text{ is such that } x^k \in R\}.$$  

In a similar way, we can define $H_{scc}^1(\tilde{\Sigma}; A)$ for any commutative ring $A$.

Equality. A fundamental question about $H_1(\tilde{\Sigma}; A)$ is whether $H_{scc}^1(\tilde{\Sigma}; A) = H_1(\tilde{\Sigma}; A)$. 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 \( \text{Mod}_{g,n} \) to construct examples where \( H^1_{\text{cc}}(\Sigma; \mathbb{Z}) \neq H_1(\Sigma; \mathbb{Z}) \). However, they were unable to rule out the possibility that \( H^1_{\text{cc}}(\Sigma; \mathbb{Z}) \) is finite-index in \( H_1(\Sigma; \mathbb{Z}) \). 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 \( H^1_{\text{cc}}(\Sigma; \mathbb{Q}) = H_1(\Sigma; \mathbb{Q}) \) when the deck group is abelian. They also constructed examples of finite covers \( \Sigma_{1,2} \to \Sigma_{1,2} \) where \( H^1_{\text{cc}}(\Sigma_{1,2}; \mathbb{Q}) \neq H_1(\Sigma_{1,2}; \mathbb{Q}) \); 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 \( H^1_{\text{cc}}(\Sigma; \mathbb{Q}) \neq H_1(\Sigma; \mathbb{Q}) \).

**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 \( \tilde{\Sigma} \to \Sigma_{g,n} \) with \( H^1_{\text{cc}}(\tilde{\Sigma}; \mathbb{Q}) \neq H_1(\tilde{\Sigma}; \mathbb{Q}) \).

**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. \( \square \)

**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. \( \square \)

**Branched covers.** We can define \( H^1_{\text{cc}}(\tilde{\Sigma}; \mathbb{Q}) \) for branched covers \( \tilde{\Sigma} \to \Sigma_{g,n} \) 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 \( \Sigma_g \).

**Theorem B.** For all \( g \geq 2 \), there exists a finite branched cover \( \tilde{\Sigma} \to \Sigma_g \) with \( H^1_{\text{cc}}(\tilde{\Sigma}; \mathbb{Q}) \neq H_1(\tilde{\Sigma}; \mathbb{Q}) \).

This result can be derived from Theorem A as follows. Let \( \tilde{\Sigma}' \to \Sigma_{g,1} \) be the unbranched cover provided by Theorem A. The surface \( \tilde{\Sigma}' \) is a finite-genus surface with punctures \( p_1, \ldots, p_k \). A small oriented loop \( \gamma \) surrounding the puncture of \( \Sigma_{g,1} \) lifts to a collection of loops \( \tilde{\gamma}_1, \ldots, \tilde{\gamma}_k \) such that \( \tilde{\gamma}_i \) surrounds \( p_i \). Fill in all the punctures of \( \tilde{\Sigma}' \) to form a closed surface \( \tilde{\Sigma} \). We then have a branched cover \( \tilde{\Sigma} \to \Sigma_g \) whose branch points are precisely the \( p_i \) such that the map \( \tilde{\gamma}_i \to \gamma \) is a cover of degree greater than 1. Since the homology classes of the \( \tilde{\gamma}_i \) lie in \( H^1_{\text{cc}}(\tilde{\Sigma}'; \mathbb{Q}) \) and generate the kernel of \( H_1(\tilde{\Sigma}') \to H_1(\tilde{\Sigma}; \mathbb{Q}) \), we see that

\[
H_1(\tilde{\Sigma}'; \mathbb{Q}) / H^1_{\text{cc}}(\tilde{\Sigma}'; \mathbb{Q}) \cong H_1(\tilde{\Sigma}; \mathbb{Q}) / H^1_{\text{cc}}(\tilde{\Sigma}; \mathbb{Q}).
\]

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 \( O \subset F_n \). For a finite-index \( R < F_n \) and an abelian group \( A \), define \( H^1_{\text{cc}}(R; A) \) to be the span in \( H_1(R; A) \) of the set

\[
\{ [x^k] \in H_1(R; A) \mid x \in O \text{ and } k \geq 1 \text{ is such that } x^k \in R \}.
\]

We prove the following theorem.
**Theorem C.** Let \( n \geq 2 \) and let \( \emptyset \subset F_n \) be contained in the union of finitely many \( \text{Aut}(F_n) \)-orbits. Then there exists a finite-index \( R \triangleleft F_n \) with \( H_1^{\emptyset}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \).

We highlight two special cases of Theorem C.

**Example 1.3.** Let \( \emptyset \) be the set of primitive elements of \( F_n \), that is, elements that lie in a free basis. The group \( \text{Aut}(F_n) \) acts transitively on \( \emptyset \). In this case, for finite-index \( R \triangleleft F_n \) the group \( H_1^{\emptyset}(R; A) \) was introduced by Farb–Hensel [4], who called it the primitive homology of \( R \) and asked whether or not \( H_1^{\emptyset}(R; \mathbb{Q}) = H_1(R; \mathbb{Q}) \) 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 \( \emptyset \subset F \) be the set of simple closed curves. For a finite-index \( R \triangleleft F \), let \( \Sigma_R \) be the associated finite cover of \( \Sigma_{g,n} \), so \( H_1(R; \mathbb{Q}) = H_1(\Sigma_R; \mathbb{Q}) \) and \( H_1^{\emptyset}(R; \mathbb{Q}) = H_1^{\emptyset}(\Sigma_R; \mathbb{Q}) \). The set \( \emptyset \) is the union of finitely many mapping class group orbits; see [6, Chapter 1.3]. Since \( \text{Aut}(F) \) is larger than the mapping class group, \( \emptyset \) is contained in the union of finitely many \( \text{Aut}(F) \)-orbits. Applying Theorem C, we obtain a finite-index \( R \triangleleft F \) satisfying \( H_1^{\emptyset}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \). Theorem A follows. This can be generalized in a wide variety of ways. For instance, for some fixed \( m \geq 0 \) we could take \( \emptyset \) 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 \( \emptyset \) 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 \( \text{Aut}(F) \)-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 \( H_1(F_n; \mathbb{F}_p) \). We denote the set of \( p \)-primitive elements by \( \mathcal{D}_p \). Observe that primitive elements of \( F_n \) are \( p \)-primitive for all primes \( p \). There are infinitely many \( \text{Aut}(F_n) \)-orbits of \( p \)-primitive element of \( F_n \), so we cannot use Theorem C to construct finite-index \( R \triangleleft F_n \) satisfying \( H_1^{\mathcal{D}_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \). However, the following still holds.

**Theorem D.** For all \( n \geq 2 \) and primes \( p \), there is a finite-index \( R \triangleleft F_n \) with \( H_1^{\mathcal{D}_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \). 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 \( \text{Mod}_{g,n} \) generated by \( k \)-th powers of Dehn twists is an infinite-index subgroup of \( \text{Mod}_{g,n} \). In fact, their methods show that the quotient of \( \text{Mod}_{g,n} \) 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 \( \text{Out}(F_n) \). The analogue in \( \text{Out}(F_n) \) 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 $\tau_{S,x,y}: F_n \to F_n$ defined via the formula

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

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 $\mathbb{B}_{n-1,k}$ 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 $\mathbb{B}_{n-1,k}$ 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

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

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 $\mathfrak{G}_{n,k}$ 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 $\mathfrak{G}_{n,k}$ to $\mathfrak{G}_{n,k}$. Thus $\text{Aut}(F_n)/\mathfrak{G}_{n,k}$ 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 $\emptyset \subset F_n$ be contained in the union of finitely many $\text{Aut}(F_n)$-orbits. Then there exists an integral linear representation $\rho: F_n \to \text{GL}_d(\mathbb{Z})$ with infinite image such that every element of $\rho(\emptyset)$ 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 $\rho: \pi_1(\Sigma_{g,n}) \to \text{GL}_d(\mathbb{Z})$ 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 $\text{GL}_d(\mathbb{Z})$ 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 $\rho: F_n \to \text{GL}_d(\mathbb{Z})$ with infinite image such that every element of $\rho(O_p)$ 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 $H^1_{O_p}(R; \mathbb{Q}) \neq H^1(R; \mathbb{Q})$ for a finite-index subgroup $R \triangleleft F_n$. 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 $H^1_{O_p}(R; \mathbb{Q}) \neq H^1(R; \mathbb{Q})$ for finite-index subgroups $R \triangleleft F_n$. 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 $R \triangleleft F_n$, a field $k$ of characteristic 0, and a prime $p$. Letting $G = F_n/R$, assume that there exists a $k$-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 $H^1_{O_p}(R; \mathbb{Q}) \neq H^1(R; \mathbb{Q})$.

The proof of Theorem 2.1 requires one preliminary result. Consider a normal subgroup $R \triangleleft F_n$ and a field $k$. The conjugation action of $F_n$ on $R$ induces an action of $F_n$ on $H^1(R; k)$. The restriction of this action to $R$ is trivial, so we obtain an induced action of $G = F_n/R$ on $H^1(R; k)$. We then have the following theorem of Gaschütz [8].

**Theorem 2.2.** For some $n \geq 1$, consider a finite-index $R \triangleleft F_n$ and a field $k$ of characteristic 0. Letting $G = F_n/R$, the $G$-module $H^1(R; k)$ is isomorphic to $k \oplus (k[G])^{n-1}$. 
Proof of Theorem 2.1. Passing to an irreducible subrepresentation of $V$, we can assume that $V$ is irreducible. Since $H_1^{O_p}(R; k) = H_1^{O_p}(R; \mathbb{Q}) \otimes \mathbb{Q} k$ and $H_1(R; k) = H_1(R; \mathbb{Q}) \otimes \mathbb{Q} k$, it is enough to prove that $H_1^{O_p}(R; k) \neq H_1(R; k)$. Let $W \subset H_1(R; k)$ be the $V$-isotypic component. Theorem 2.2 implies that $W \neq 0$, so it is enough to prove that the projection of $H_1^{O_p}(R; k)$ 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 $[x^m] \in H_1(R; k)$ 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 $[x^m] \in H_1(R; k)$. 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. \qed

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 $\Psi: C \to \mathbb{Z}/p$ such that the following hold.

- $H_1(G/F_p) = \mathbb{F}_p^n$.
- For all $g \in G$ whose image in $H_1(G/F_p)$ 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 $\Psi: C \to \mathbb{Z}/p$ 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 $C$-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. \qed

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 $H_1^{O_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q})$ and such that $F_n/R$ is a $p$-group.

Let $G$ and $C$ and $\Psi: C \to \mathbb{Z}/p$ be as in Proposition 2.3. Since $H_1(G/F_p) = \mathbb{F}_p^n$, we can choose a homomorphism $\rho: F_n \to G$ taking a basis of $F_n$ to a set $S$ of elements of $G$ that projects to a basis for $H_1(G/F_p)$. Equivalently, the induced map $\rho_*: H_1(F_n/F_p) \to H_1(G/F_p)$ is an isomorphism. Note that $H_1(G/F_p) = G/D$ with $D = G^{p}|[G, G]$. Since $S$ projects to a basis for $H_1(G/F_p)$, 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 $\rho$ is surjective.

If $x \in F_n$ is $p$-primitive, then $x$ projects to a nonzero element of $H_1(F_n/F_p)$ and thus $\rho(x) \in G$ also projects to a nontrivial element of $H_1(G/F_p)$. Set $R = \ker(\rho)$. By Theorem
2.1, to prove that $H^1_p(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q})$, 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 $H_1(G; \mathbb{F}_p)$, 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 $\Psi : C \to \mathbb{Z}/p$ 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 

$$V = \text{Ind}^G_C W.$$ 

Consider $g \in G$ that projects to a nonzero element of $H_1(G; \mathbb{F}_p)$. 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 $\Gamma$ be a group and let $p$ be a prime. The **Zassenhaus $p$-central series** of $\Gamma$ 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 $\Gamma$, we define 

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

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 \( \Gamma \) 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 \( \overline{x} \in \mathcal{L}^p_i(\Gamma) \) and \( \overline{y} \in \mathcal{L}^p_j(\Gamma) \) be their images, the Lie bracket \( [\overline{x}, \overline{y}] \in \mathcal{L}^p_{i+j}(\Gamma) \) 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 \( (cx)^{[p]} = c^px^{[p]} \).
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 \( \text{Ad}(x) \): \( A \to A \).
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 \( \Gamma \). More precisely, consider \( x \in \gamma_i^p(\Gamma) \). Letting \( \overline{x} \in \mathcal{L}^p_i(\Gamma) \) be its image, the element \( \overline{x}^{[p]} \in \mathcal{L}^p_i(\Gamma) \) is the image of \( x^p \in \gamma_{ip}^p(\Gamma) \). In particular, the \( p \)-th power operation on \( \mathcal{L}^p(\Gamma) \) takes \( \mathcal{L}^p_1(\Gamma) \) to \( \mathcal{L}^p_1(\Gamma) \).

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 \( \mathcal{FL}^p_i(S) \), the degree 1 piece \( \mathcal{FL}^p_1(S) \) is an \( \mathbb{F}_p \)-vector space with basis \( S \). The \( p \)-restricted Lie algebra \( \mathcal{FL}^p(S) \) is generated by \( \mathcal{FL}^p_1(S) \) 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 \( \mathcal{FL}^p_1(S) \).

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 $\Psi : C \to \mathbb{Z}/p$ such that the following two conditions hold.

- $H_1(G; \mathbb{F}_p) = \mathbb{F}_p^n$.
- For all $g \in G$ whose image in $H_1(G; \mathbb{F}_p)$ 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 $H_1(G; \mathbb{F}_p) \cong G/\gamma_2^p(G) \cong F/\gamma_2^p(F) \cong \mathbb{F}_p^n$.

By Theorem 2.11, we have $L_p^p(G) = \bigoplus_{i=1}^{p^k} \mathcal{F}\mathcal{L}_i^p(S)$.

Letting $C = \gamma_p^{p^k}(G) \cong \gamma_p^p(F)/\gamma_{p^{k+1}}^p(F) \cong \mathcal{F}\mathcal{L}_{p^k}^p(S)$, the fact that $\gamma_{p^{k+1}}^p(G) = 1$ implies that $C$ is central in $G$. The needed homomorphism $\Psi : C \to \mathbb{Z}/p$ 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 $\Psi : \mathcal{F}\mathcal{L}_{p^k}^p(S) \to \mathbb{F}_p$ such that $\Psi(v^{p^k}) \neq 0$ for all nonzero $v \in \mathcal{F}\mathcal{L}_1^p(S)$.

**Proof.** We begin with some preliminary observations. Let $A^p(S)$ be the free associative $\mathbb{F}_p$-algebra on $S$. The algebra $A^p(S)$ 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 $A^p_i(S)$ be its $i$th graded piece, so

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

The associative algebra $A^p(S)$ can be endowed with the structure of a $p$-restricted Lie algebra via the bracket $[x, y] = xy - yx$ $(x, y \in A^p(S))$ and the ordinary $p$th power operation $x^{[p]} = x^p$ $(x \in A^p(S))$.

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

We have a commutative diagram

$$\begin{array}{ccc}
\mathcal{F}\mathcal{L}_1^p(S) & \cong & A^p_1(S) \\
\downarrow & & \downarrow \\
\mathcal{F}\mathcal{L}_{p^k}^p(S) & \longrightarrow & A^p_{p^k}(S)
\end{array}$$
whose horizontal arrows are $\iota$ and whose vertical arrows are the $p^\text{th}$-power operations. To construct a linear map $\Psi: \mathcal{F}L_p^p(S) \to \mathbb{F}_p$ such that $\Psi(v^{p^k}) \neq 0$ for all nonzero $v \in \mathcal{F}L_p^1(S)$, it is thus enough to construct a linear map $\Phi: A_{p^k}^p(S) \to \mathbb{F}_p$ such that $\Phi(w^{p^k}) \neq 0$ for all nonzero $w \in A_z^1(S)$.

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

$$f_\Phi(a_1, \ldots, a_n) = \Phi \left( \left(a_1 x_1 + \cdots + a_n x_n\right)^{p^k} \right) \quad (a_1, \ldots, a_n \in \mathbb{F}_p).$$

We must therefore construct some linear map $\Phi: A_{p^k}^p(S) \to \mathbb{F}_p$ such that $f_\Phi(a_1, \ldots, a_n) \neq 0$ for all nonzero $(a_1, \ldots, a_n) \in F^n_p$.

**Claim.** For any homogeneous polynomial $g \in \mathbb{F}_p[t_1, \ldots, t_n]$ of degree $p^k$, there exists a linear map $\Phi: A_{p^k}^p(S) \to \mathbb{F}_p$ 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 $\mathcal{E} = \{(e_1, \ldots, e_n) \in \mathbb{Z}_{\geq 0}^n \mid e_1 + \cdots + e_n = p^k\}$. For $e = (e_1, \ldots, e_n) \in \mathcal{E}$, define $t^e = t_1^{e_1} \cdots t_n^{e_n} \in \mathbb{F}_p[t_1, \ldots, t_n]$. Also, for $a = (a_1, \ldots, a_n) \in \mathbb{F}_p^n$ define $a^e = a_1^{e_1} \cdots a_n^{e_n} \in \mathbb{F}_p$. Write $g = \sum_{e \in \mathcal{E}} c_e t^e$ with $c_e \in \mathbb{F}_p$ for all $e \in \mathcal{E}$. The vector space $A_{p^k}^p(S)$ has a basis

$$B = \{x_1^{e_1} x_2^{e_2} \cdots x_n^{e_n} \mid 1 \leq i_1, \ldots, i_m \leq n \text{ and } e_1 + \cdots + e_m = p^k\}.$$

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

$$(a_1 x_1 + \cdots + a_n x_n)^{p^k} = \sum_{b \in B} a^{d(b)} b.$$

Define $\Phi: A_{p^k}^p(S) \to \mathbb{F}_p$ via the formula

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

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

$$f_\Phi(a_1, \ldots, a_n) = \Phi \left( \left(a_1 x_1 + \cdots + a_n x_n\right)^{p^k} \right) = \Phi \left( \sum_{b \in B} a^{d(b)} b \right) = \sum_{e \in \mathcal{E}} c_e a^e = g(a_1, \ldots, a_n). \quad \Box$$

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 $e'_i = 0$. 

10
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 \( p^k > (p - 1)(n - 1) \), 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

\[
e'_1 = p^k - (e'_2 + \cdots + e'_n) \equiv p^k - (e_2 + \cdots + e_n) = p^k + e_1 - (e_1 + \cdots + e_n) \equiv p^k + e_1 - 1 \equiv e_1,
\]

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

\[
Z(F(g, h)) = Z(g) \cap Z(h).
\] (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 \( a \in Z(F(g, h)) \). If \( a \notin Z(h) \), then

\[0 = F(g(a), h(a)) = g(a) - g(a)h(a)^{p^k-1} + h(a) = g(a) - g(a) + h(a) = h(a) \neq 0,\]

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

\[0 = F(g(a), h(a)) = g(a) - g(a)h(a)^{p^k-1} + h(a) = g(a),\]

so \( a \in Z(g) \) and thus \( a \in Z(g) \cap Z(h) \), 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 \( \emptyset \subset F_n \) be contained in the union of finitely many \( \text{Aut}(F_n) \)-orbits. Our goal is to construct a finite-index \( R \triangleleft F_n \) with \( H^1(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \). If \( \emptyset' \subset F_n \) satisfies \( \emptyset \subset \emptyset' \), then \( H^1(R; \mathbb{Q}) \subset H^1(R'; \mathbb{Q}) \). From this, we see that without loss of generality we can enlarge \( \emptyset \) and assume that \( \emptyset \) is actually equal to the union of finitely many \( \text{Aut}(F_n) \)-orbits. Let \( \mathcal{S} \subset F_n \) be the finite set such that \( \emptyset = \text{Aut}(F_n) \cdot \mathcal{S} \). Without loss of generality, we can assume that \( 1 \notin \mathcal{S} \).

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 \( s \in \mathcal{S} \), we construct a finite-index characteristic subgroup \( R^s_1 \triangleleft F_n \) 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 \( x^m \in R^s_1 \). Then \( [x^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero.

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

\[
R^s_1 = \bigcap_{\phi \in \text{Aut}(F_n)} \phi(T),
\]

so \( R^s_1 \) 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 \( x^m \in R^s_1 \). Our goal is to prove that \( [x^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero. Since \( R^s_1 \) is a characteristic subgroup of \( F_n \), the group \( \text{Aut}(F_n) \) acts on \( R^s_1 \) and thus on \( H_1(R^s_1; \mathbb{Q}) \). Observe that

\[
\phi([x^m]) = [\phi(x)^m] = [s^m] \in H_1(R^s_1; \mathbb{Q}).
\]

To prove that \( [x^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero, it is thus enough to prove that \( [s^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero. The inclusion map \( R^s_1 \rightarrow T \) takes \( s^m \) to \( s^m \), and thus the induced map \( H_1(R^s_1; \mathbb{Q}) \rightarrow H_1(T; \mathbb{Q}) \) takes \( [s^m] \in H_1(R^s_1; \mathbb{Q}) \) to \( [s^m] \in H_1(T; \mathbb{Q}) \). Since \( s \) is a primitive element of \( T \), it follows that \( [s] \in H_1(T; \mathbb{Q}) \) is nonzero and hence that \( [s^m] \in H_1(T; \mathbb{Q}) \) is nonzero. We conclude that \( [s^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero, as desired.

**Step 2.** We construct a finite-index characteristic subgroup \( R_1 \triangleleft F_n \) with the following property. Consider \( x \in \emptyset \). Pick \( m \geq 1 \) such that \( x^m \in R_1 \). Then, \( [x^m] \in H_1(R_1; \mathbb{Q}) \) is nonzero.

Define

\[
R_1 = \bigcap_{s \in \mathcal{S}} R^s_1.
\]

Since \( R_1 \) is a finite intersection of finite-index characteristic subgroups of \( F_n \), it is also a finite-index characteristic subgroup. Consider \( x \in \emptyset \) and some \( m \geq 1 \) such that \( x^m \in R_1 \). We must prove that \( [x^m] \in H_1(R_1; \mathbb{Q}) \) is nonzero. Let \( s \in \mathcal{S} \) be such that \( x \) is in the \( \text{Aut}(F_n) \)-orbit of \( s \). We have \( x^m \in R^s_1 \), and by the previous step the element \( [x^m] \in H_1(R^s_1; \mathbb{Q}) \) is nonzero. An argument like in the previous step now implies that \( [x^m] \in H_1(R_1; \mathbb{Q}) \) is nonzero, as desired.

**Step 3.** We construct a finite-index \( R \triangleleft F_n \) with \( H^1(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q}) \).
For each $s \in \mathfrak{g}$, pick $m_s \geq 1$ such that $s^{m_s} \in R_1$. Since each $[s^{m_s}] \in H_1(R_1; \mathbb{Q})$ is nonzero, there exists some large prime $p$ such that each $s^{m_s}$ projects to a nonzero element of $H_1(R_1; \mathbb{F}_p)$. Applying Theorem D to $R_1$, we can find a finite-index subgroup $R < R_1$ such that $H_1^{D_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q})$, where here $D_p$ refers to the $p$-primitive elements of $R_1$, not of $F_n$. We claim that $H_1^{D_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q})$, where by $H_1^{D_p}(R; \mathbb{Q})$ we are considering $R$ as a subgroup of $F_n$. To prove this, it is enough to prove that $H_1^{D_p}(R; \mathbb{Q}) \subset H_1^{D_p}(R; \mathbb{Q})$. Consider some $x \in \mathcal{O}$. Pick $\phi \in \text{Aut}(F_n)$ and $s \in \mathfrak{g}$ such that $\phi(x) = s$. Since $R_1$ is a characteristic subgroup of $F_n$, the group $\text{Aut}(F_n)$ acts on $R_1$ and thus on $H_1(R_1; \mathbb{F}_p)$. We have

$$\phi([x^{m_s}]) = [\phi(x)^{m_s}] = [s^{m_s}] \in H_1(R_1; \mathbb{F}_p).$$

Since $[s^{m_s}] \in H_1(R_1; \mathbb{F}_p)$ is nonzero, so is $[x^{m_s}] \in H_1(R_1; \mathbb{F}_p)$. Pick $m \geq 1$ such that $(x^{m_s})^m \in R$. We then have $[(x^{m_s})^m] \in H_1^{D_p}(R; \mathbb{Q})$, as desired.

4 Transvections: Theorem E

In this section, we prove Theorem E, which concerns the subgroup of $\text{Out}(F_n)$ 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 $\text{Aut}(F_n)$ on chains

In this section, we construct a family of linear representations $\mathcal{M}_R$ of subgroups of $\text{Aut}(F_n)$ that are indexed by subgroups $R < F_n$. 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 $R < F_n$ and a field $k$. Set $G = F_n/R$. The conjugation action of $F_n$ on $R$ induces an action of $G$ on $H_1(R; k)$. When $R$ is finite-index and $k$ has characteristic 0, this $G$-module is described by Theorem 2.2 above. Define

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

The group $\text{Aut}(F_n, R)$ acts on $H_1(R; k)$; however, this action can be very complicated. To help us understand it, we embed $H_1(R; k)$ into a larger vector space. This requires some topological preliminaries.

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

Lifting homotopy-equivalences. Let $\pi: (\tilde{X}_n, \tilde{\ast}) \to (X_n, \ast)$ be the based cover corresponding to $R \subset F_n$, so $H_1(\tilde{X}_n; k) = H_1(R; k)$. For a continuous map $f: (X_n, \ast) \to (X_n, \ast)$, we know from covering space theory that $f$ can be lifted to a map $\tilde{f}: (\tilde{X}_n, \tilde{\ast}) \to (\tilde{X}_n, \tilde{\ast})$ if and only if $f_*(R) \subset R$. From this, we see that the group $\text{Aut}(F_n, R)$ acts on $\tilde{X}_n$ by homotopy equivalences that fix $\tilde{\ast}$. The resulting action of $\text{Aut}(F_n, R)$ on $H_1(\tilde{X}_n; k) = H_1(R; k)$ is precisely the action arising from the restriction of the action of $\text{Aut}(F_n, R)$ to $R$. 

13
Action on chains. Since $\tilde{X}_n$ is a 1-dimensional cell complex, the vector space $H_1(\tilde{X}_n; k)$ is a subspace of the cellular chain group $C_1(\tilde{X}_n; k)$. Namely,

$$H_1(\tilde{X}_n; k) = \ker(C_1(\tilde{X}_n; k) \xrightarrow{\partial} C_0(\tilde{X}_n; k)).$$

The action of $\text{Aut}(F_n, R)$ on $\tilde{X}_n$ by homotopy equivalences induces an action of $\text{Aut}(F_n, R)$ on $C_1(\tilde{X}_n; k)$ that restricts to the above action on $H_1(\tilde{X}_n; k)$. It turns out that $C_1(\tilde{X}_n; k)$ is far easier to understand than $H_1(\tilde{X}_n; k)$. 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 $\tilde{X}_n$ endows each cellular chain group $C_k(\tilde{X}_n; k)$ with the structure of a $G$-module. It is easy to understand these $G$-modules:

- We can identify the vertices of $\tilde{X}_n$ with $G$ via the bijection taking $g \in G$ to $\tilde{g}$. Using this identification, we obtain a $G$-equivariant isomorphism $C_0(\tilde{X}_n; k) \cong k[G]$.
- For $1 \leq i \leq n$, let $\tilde{e}_i$ be the oriented edge of $\tilde{X}_n$ that starts at $\tilde{v}$ and projects to $e_i \in S_n$. The edges of $\tilde{X}_n$ are precisely $\{g(\tilde{e}_i) \mid g \in G, 1 \leq i \leq n\}$. Using this, we obtain a $G$-equivariant isomorphism $C_1(\tilde{X}_n; k) \cong (k[G])^n$.

The boundary map $\partial : C_1(\tilde{X}_n; k) \to C_0(\tilde{X}_n; k)$ is $G$-equivariant, so $H_1(R; k) \subset C_1(\tilde{X}_n; k)$ is a $G$-submodule. This $G$-action agrees with the action of $G$ on $H_1(R; k)$ induced by the conjugation action of $F_n$ on $R$ via the surjection $F_n \to G$.

The representation. Combining the above action of $\text{Aut}(F_n, R)$ on $C_1(\tilde{X}_n; k)$ with the above identification of $C_1(\tilde{X}_n; k)$ with $(k[G])^n$, we obtain a homomorphism

$$\widehat{M}_R : \text{Aut}(F_n, R) \to \text{Aut}_k((k[G])^n).$$

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

$$\widehat{M}_R(\phi)(g \cdot v) = \phi_*(g) \cdot \widehat{M}_R(\phi)(v) \quad (\phi \in \text{Aut}(F_n, R), g \in G, v \in (k[G])^n),$$

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

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

We then obtain a homomorphism

$$M_R : \text{Aut}_R(F_n) \to \text{Aut}_G((k[G])^n).$$

Note that since the action on 1-chains induces the action on homology, this representation $M_R$ is an extension of the action on $H_1(R; k) \subset C_1(\tilde{X}_n; k) \cong (k[G])^n$. For computations in coordinates with $M_R$, we will need to use a basis. The standard basis for $(k[G])^n$ is the set $\{\overline{e}_1, \ldots, \overline{e}_n\}$, where $\overline{e}_i \in (k[g])^n \cong C_1(\tilde{X}_n; k)$ is the chain corresponding to the oriented edge $\tilde{e}_i$ of $\tilde{X}_n$.

Remark 4.1. The precise representation $\text{Aut}_R(F_n) \to \text{Aut}_G((k[G])^n)$ depends on the choice of basis $S$ of $F_n$, but it is always an extension of the action on $H_1(R; k)$. □
Image of a transvection. Recall that $S = \{x_1, \ldots, x_n\}$. In the introduction we defined the transvection $\tau_{S,x_1,x_2} \in \text{Aut}(F_n)$ via the formula

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

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

**Lemma 4.2.** For some $n \geq 1$, let $R < F_n$ be finite-index, let $k$ 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 $\{e_1, \ldots, e_n\}$ be the standard basis for $(k[G])^n$. If $m \geq 1$ is such that $x_i^m \in R$, then

$$
M_R(\tau_{S,x_1,x_2}^m) = \begin{cases} 
\tilde{e}_1 + \tilde{e}_2 + g_2 \cdot \tilde{e}_2 + g_2^2 \cdot \tilde{e}_2 + \cdots + g_2^{m-1} \cdot \tilde{e}_2 & \text{if } i = 1, 
\tilde{e}_i & \text{if } i \neq 1 
\end{cases} \quad (1 \leq i \leq n).
$$

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

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

The lemma follows. $\square$

### 4.2 Theorem E

We now give the proof of Theorem E. The heart of our argument is the following more precise result for $\text{Aut}(F_n)$. For its statement, observe that if $G$ is a finite group, $\pi: F_n \to G$ is a surjection with kernel $R$, and $V$ is an irreducible representation of $G$ over a field $k$ of characteristic 0, then the action of $\text{Aut}_R(F_n)$ on $H_1(R;k)$ preserves the $V$-isotypic component.

**Proposition 4.3.** For some $n \geq 2$, let $G$ be a finite group and let $\pi: F_n \to G$ 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 $W \subset H_1(R;\mathbb{Q})$ be the $V$-isotypic component, and let $\Phi: \text{Aut}_R(F_n) \to \text{GL}(W)$ be the restriction to $W$ of the action of $\text{Aut}_R(F_n)$ on $H_1(R;\mathbb{Q})$. Then the following hold.

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

**Proof.** Farb–Hensel [5, Theorem 1.1] proved that the $\text{Aut}_R(F_n)$-orbit of a nonzero vector in $H_1(R;\mathbb{Q})$ is infinite. Moreover, they showed that for any nonzero $v \in H_1(R;\mathbb{Q})$, there is a $\phi \in \text{Aut}_R(F_n)$ such that $\{\phi^k(v) | k \in \mathbb{Z}\}$ is infinite. Since the action of $\text{Aut}_R(F_n)$ on $H_1(R;\mathbb{Q})$ preserves $W$ (which is nonzero by Theorem 2.2), we deduce that the image of $\Phi$ 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 $M_R: \text{Aut}_R(F_n) \to \text{Aut}_G((\mathbb{Q}[G])^n)$ defined in §4.1.
Let \( \{ \bar{e}_1, \ldots, \bar{e}_n \} \) 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

\[
M_R(\tau_{S,x_1,x_2}^m)(\bar{e}_i) = \begin{cases} 
\bar{e}_i + \bar{e}_2 + g_2 \cdot \bar{e}_2 + g_2^2 \cdot \bar{e}_2 + \cdots + g_2^{m-1} \cdot \bar{e}_2 & \text{if } i = 1, \\
\bar{e}_i & \text{if } i \neq 1 
\end{cases} \quad (1 \leq i \leq n).
\]

The element \( \bar{e}_2 + g_2 \cdot \bar{e}_2 + g_2^2 \cdot \bar{e}_2 + \cdots + g_2^{m-1} \cdot \bar{e}_2 \) 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 \( M_R(\tau_{S,x_1,x_2}^m) \) acts as the identity on the \(V\)-isotypic component of \((\mathbb{Q}[G])^n\), which implies that \( \tau_{S,x_1,x_2}^m \in \ker(\Phi) \), as desired. \( \square \)

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 \( \pi: F_n \to G \) be a surjection. Assume that for some field \( k \) of characteristic 0, there exists a \( k \)-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 \( k \) 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. \( \square \)

**Proof of Theorem E.** We first recall the statement. Fix some \( n \geq 2 \), and for \( k \geq 1 \) let \( \mathfrak{S}_{n,k} \subset \text{Out}(F_n) \) 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 \( \text{Out}(F_n)/\mathfrak{S}_{n,k} \) 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 \( \text{Out}(F_n)/\mathfrak{S}_{n,p^e} \) contains infinite-order elements. Lemma 4.4 and the proof of Theorem D gives the following:

- A surjection \( \pi: F_n \to G \) 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 \( H_1(R; \mathbb{Q}) \) and let \( \Phi: \text{Aut}_R(F_n) \to \text{Aut}_G(W) \) be the resulting action. Define \( \Gamma = \text{Im}(\Phi) \). Proposition 4.3 implies that \( \Gamma \) contains infinite-order elements and that \( (p^e)^{th} \) powers of transvections lie in \( \ker(\Phi) \). This implies that the quotient of \( \text{Aut}(F_n) \) by the subgroup generated by \( (p^e)^{th} \) powers of transvections contains infinite-order elements.

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

\[
\text{Inn}_R(F_n) = \{ x \in F_n \mid \pi(x) \in G \text{ is central} \}.
\]
The image $\Phi(\text{Inn}_R(F_n)) \subset \Gamma$ is a finite subgroup of the center of $\Gamma$. Letting

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

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

## 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 $\rho: F_n \to \text{GL}_d(\mathbb{Z})$ with the following two properties.

- The image of $\rho$ 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 $R < F_n$ such that $H_1^{D_p}(R; \mathbb{Q}) \neq H_1(R; \mathbb{Q})$. Define $G = F_n/R$ and $\widehat{\Gamma} = F_n/[R,R]$. We thus have a short exact sequence

$$1 \to H_1(R; \mathbb{Z}) \to \widehat{\Gamma} \to G \to 1.$$  

The action of $G$ on $H_1(R; \mathbb{Z})$ preserves the subgroup $H_1^{D_p}(R; \mathbb{Z})$, and hence $H_1^{D_p}(R; \mathbb{Z})$ is a normal subgroup of $\widehat{\Gamma}$. Define $\Gamma = \widehat{\Gamma}/H_1^{D_p}(R; \mathbb{Z})$. Setting $A = H_1(R; \mathbb{Z})/H_1^{D_p}(R; \mathbb{Z})$, we thus have a short exact sequence

$$1 \to A \to \Gamma \to G \to 1.$$  

Since $H_1^{D_p}(R; \mathbb{Q})$ is a proper subspace of $H_1(R; \mathbb{Q})$, the group $A$ is infinite. Let $\pi: F_n \to \Gamma$ 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 $H_1^{D_p}(R; \mathbb{Z})$ 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 $A \hookrightarrow \text{GL}_{d'}(\mathbb{Z})$ for some $d' \geq 1$. Since $A$ is a finite-index subgroup of $\Gamma$, we can induce this representation up to $\Gamma$ to get a faithful integral linear representation $\Gamma \hookrightarrow \text{GL}_d(\mathbb{Z})$ for some $d \geq 1$. The desired integral linear representation of $F_n$ is then the composition

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

## References

[13] A. Hadari, Non virtually solvable subgroups of mapping class groups have non virtually solvable representations, preprint, arxiv.org/abs/1805.01527
[28] Representations of p-groups where 1 is never an eigenvalue, URL (version: 2016-02-26): https://mathoverflow.net/q/232227

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