数理解析研究所講究録 1267 巻 2002 年 70-95

Moduli of relatively nilpotent algebraic extensions

Michael D. Fried (University of California, Irvine)

Abstract: The Main Conjecture on Modular Towers: For a prime p, and finite p-perfect group G, high levels of a (G,p)-Modular Tower have no rational points. When p is an odd prime and G is the dihedral group D_p we call the towers Hyper-modular. [**BFr02**] proves cases of the Main Conjecture for Modular Towers with $p=2$ and G an alternating group. We use differences between Hyper-modular and general Modular Towers to give new moduli applications. Their similarities give these applications insights successful with modular curves.

The universal p-Frattini cover of G and a collection of p' conjugacy classes define a particular Modular Tower's levels. The number of components at a level and how cusp ramification grows from level to level relate to the appearance of Schur multipliers. [**BFr02**] applies formulas of the author and Serre to spin covers to handle the case $p=2$. We give here an exposition on going beyond that analysis.

As with modular curves, the tower levels are moduli spaces. We use a Demjanenko-Manin result and a construction from [**Fri95**] to more directly approach rational points than does Falting's Theorem.

1991 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11R58, 14G32; Secondary 20B05, 20C25, 20D25, 20E18, 20F34.

Conversations with Darren Semmen were extremely valuable in reporting on progress in this exposition extending my talks at RIMS in October 2001. Thanks to NSF Grant #DMS-9970676 and #DMS-0202259 and RIMS for support. Special thanks to Yasutaka Ihara and his four colleagues Makoto Matsumoto, Shin Mochizuki, Hiroaki Nakamura and Akio Tamagawa for an apposite and challenging conference.

CONTENTS

1. Basic goals of Modular Towers

Suppose the prime p divides the order of a finite group G. We say G is p-perfect if G has no $\mathbb{Z}/p$ quotient. A *perfect* group is p-perfect for each prime dividing its order. Equivalently, G equals its commutator subgroup. A p' conjugacy class (subgroup, element, etc.) of G has elements of order prime to p. Being p-perfect is equivalent to having p' generators.

We think of *Hyper-modular Towers* relating to *Modular Towers* as (D_p, p) (p odd) relates to (G, p), with G a p-perfect finite group. A Hyper-modular Tower comes with an even number r of involution conjugacy classes. A modular curve tower has $r = 4$ and its kth level is the space $X_1(p^{k+1})$ without its cusps. A (G, p) Tower has a collection of p' conjugacy classes $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$. We call r the *p-dimension* of a Nielsen class. Then $r-3$ is its *j-dimension*. The p-dimension is the dimension of the Hurwitz space tower levels. Each level is an affine cover of $\mathbb{P}^r \setminus D_r$, projective r space minus its discriminant locus.

Let $\mathbb{P}^1_z = \mathbb{C}_z \cup \{\infty\}$ be projective 1-space with a uniformizing variable z. Recall the space J_r: $\mathrm{PGL}_2(\mathbb{C})$ equivalence classes of unordered distinct points $\mathbb{P}^1_z$. Then, the *reduced* Hurwitz space at the kth level of a $(G,p,\mathbf{C})$ modular tower has dimension equal to the j-dimension. We explain below the notation $\mathcal{H}(G_k,\mathbf{C})^{\mathrm{in,rd}} = \mathcal{H}(G_k,\mathbf{C})^{\mathrm{rd}}$ $(G_0=G)$ for this inner Hurwitz space. It has an affine (so surjective with finite fibers) map to J_r.

When $r=4$ the Modular Tower levels are covers of $\mathbb{P}^1_j \setminus \{\infty\} = J_4$, the classical j-line, and they are quotients of the upper half-plane by a finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$. We normalize so their ramified points are $j=0,1,\infty$ with any ramified points over 0 (resp. 1) having index 3 (resp. 2). The points of the projective completion of the curve levels over ∞ are *cusps*. Computing their *widths* (ramification indices) is subtle and significant (§1.2).

1.1. Topics of this paper and the Main Conjecture. An hypothesis on G_0 seeding a Modular Tower is always in force, unless otherwise said, throughout this paper: That G_0 is a centerless p-perfect group. We often remind the reader of that by using the phrase p-perfect, though it also means centerless so as to apply the consequence from Thm. 2.10 that all the G_ks also are centerless. The Main Conjecture is that for $(G,p,\mathbf{C})$ above (with $G=G_0$ a p-perfect centerless group) and k large, $\mathcal{H}(G_k,\mathbf{C},p)^{\mathrm{in,rd}}$ has no rational points. We state a geometric version.

CONJECTURE 1.1 (Geometric Conjecture). For k large, nonsingular projective completions of all components of a Modular Tower at level k have general type.

Characteristic p-Frattini covers $\{G_k\}_{k=0}^{\infty}$ of $G=G_0$ define the reduced Modular Tower levels, $\mathcal{H}(G_k,\mathbf{C})^{\mathrm{in,rd}} = \mathcal{H}_k^{\mathrm{rd}}$. Since $\mathbf{C}$ consists of p' conjugacy classes, each C_i pulls back to unique conjugacy classes in each covering group $G_k \to G_0$. That means the notation for $(G_k,\mathbf{C})$ reduced Nielsen classes makes sense (§1.3).

When $r=4$, the genus of a level k component depends on elliptic ramification and cusp ramification, respectively, $\mathrm{ind}(\gamma_0)+\mathrm{ind}(\gamma_1)$ and $\mathrm{ind}(\gamma_\infty)$ in (1.4c). For Modular Towers these engage us in a moduli interpretation related to (G_k,p). Though this is akin to the simplest case $(D_{p^{k+1}},p)$ for modular curves, there are four new challenges.

Two deal with the moduli interpretation of γ_0 and γ_1 fixed points and for *orbit shortening*. Our goal is to find a level at which each disappears (§3.2). The 3rd is to locate those p-divisible cusps at level $k+1$ that lie above level k cusps that aren't p-divisible. These are the contributors to the U_is of (3.2). We nailed these contributions in the [**BFr02**] examples for $p = 2$ as coming from spin covers of finite groups. This used formulas of the author and Serre. A harder spin cover analysis then found the components of these example Modular Tower levels.

Here is a list of topics in this paper. Several of these include the case $r \geq 5$.

(1.1a) §2.2.2: Computing effectively the characteristic p-Frattini module M_k inductively defining G_{k+1} from G_k (hinted at in [**Fri95**, Rem. 2.10]).
(1.1b) §3: Heuristics for the Main Conjecture on Modular Tower levels when the j-dimension is 1. [**BFr02**, §8.1].
(1.1c) §4.2: Classifying for all p how Schur multipliers figure in a change of p-divisible cusps from level k to level $k+1$.
(1.1d) §5.2: The Demjanenko-Manin effective diophantine approach when the j-dimension is 1, and its potential for all Modular Towers.
(1.1e) §6: Situations assuring there are projective systems of absolutely irreducible $\mathbb{Q}$ components on each Modular Tower level.

1.2. Reduced Hurwitz space components. Each Modular Tower comes with p' conjugacy classes $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$. These give the Nielsen class elements:

$$\mathrm{Ni} = \mathrm{Ni}(G, \mathbf{C}) = \{\boldsymbol{g} = (g_1, \dots, g_r) \mid g_1 \cdots g_r = 1, \langle \boldsymbol{g} \rangle = G \text{ and } \boldsymbol{g} \in \mathbf{C}\}.$$

The notation $\boldsymbol{g} \in \mathbf{C}$ means there is a $\pi \in S_r$ with $g_{(i)\pi} \in \mathrm{C}_i$, $i = 1, \dots, r$. The elements of *inner* equivalence classes are the collections $\{h^{-1}\boldsymbol{g}h\}_{h \in G}$. Suppose r is even and G has $r/2$ conjugacy classes $\mathrm{C}'_1, \dots, \mathrm{C}'_{r/2}$ so with elements $g_i \in \mathrm{C}'_i$, $i = 1, \dots, r/2$, that generate G. Let $\mathbf{C}$ be the conjugacy classes with $\mathrm{C}_{2i} = \mathrm{C}'_i$, $\mathrm{C}_{2i-1} = (\mathrm{C}'_i)^{-1}$, $i = 1, \dots, r/2$. Then, $\mathrm{Ni}(G, \mathbf{C})$ contains this Harbater-Mumford representative (H-M rep.): $(g_1^{-1}, g_1, g_2^{-1}, g_2, \dots, g_{r/2}^{-1}, g_{r/2})$. The relation to cusps of H-M reps. appears repeatedly in [**BFr02**].

Many applications use Hurwitz spaces with points that are equivalence classes of $(G, \mathbf{C})$ covers having branch cycle descriptions from a permutation representation $T : G \to S_n$. Then the covers have degree n and the corresponding equivalence classes $\{h^{-1}\boldsymbol{g}h\}_{h \in N_{S_n}(G)}$ with $N_{S_n}(G)$ the normalizer of G in S_n. Example: The case with $G = D_p$ (p odd, $r = 4$) above produces the modular curve $Y_0(p) = X_0(p) \setminus \{\text{cusps}\}$ using the standard degree p representation, $N_{S_p}(D_p) = \mathbb{Z}/p \times^s (\mathbb{Z}/p)^*$

and reduced equivalence (below) of covers. When, however, we equivalence only by conjugation by D_p (inner classes), the result is $Y_1(p)$. Permutation representations appear in any precise analysis of Modular Towers. The Main Conjecture, however, assumes reduced inner equivalence on Nielsen classes.We concentrate here on that case; conjugation by G gives Nielsen classes.

When r is at least 4, a braiding action gives important invariants of the reduced Hurwitz space $\mathcal{H}(G,\mathbf{C})^{\mathrm{rd}}$. Each component corresponds to an orbit for the action of two operators:

(1.2a) The shift: $(g_1,\dots,g_r) \mapsto (g_2,\dots,g_r,g_1) = (\boldsymbol{g})\mathbf{sh}$; and
(1.2b) The 2-twist: $(g_1,\dots,g_r) \mapsto (g_1, g_2g_3g_2^{-1}, g_2,\dots,g_r) = (\boldsymbol{g})\gamma_\infty$.

You may replace the 2-twist by the i-twist q_i, $1 \le i \le r-1$. Just one twist and the shift generate all the braidings. The cases $r = 4$ and $r \ge 5$ differ slightly.

1.3. The sh-incidence matrix for $r = 4$. [**BFr02**, Prop. 4.4] shows how to compute the genuses of $\mathcal{H}(G,\mathbf{C})^{\mathrm{rd}}$ components. This uses a Klein 4-group $\mathcal{Q}''$ that acts on Nielsen classes. We give its generators in $q_1,\dots,q_{r-1}$ notation:

(1.3a) $q_1q_3^{-1}$: $(g_1,\dots,g_4) \mapsto (g_1g_2g_1^{-1}, g_1, g_3g_4g_3^{-1}, g_3)$.
(1.3b) $\mathbf{sh}^2$: $(g_1,\dots,g_4) \mapsto (g_3,g_4,g_1,g_2)$.

Form *reduced* (inner) Nielsen classes: $G\backslash \mathrm{Ni}(G,\mathbf{C})/\mathcal{Q}'' = \mathrm{Ni}(G,\mathbf{C})^{\mathrm{rd}}$. With $\gamma_1 = \mathbf{sh}$ and γ_∞ the 2-twist (or middle twist) acting on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{rd}}$, we draw conclusions for the $\bar{M}_4 = \langle \gamma_1, \gamma_\infty \rangle$ action.

(1.4a) Components of $\mathcal{H}(G_k,\mathbf{C})^{\mathrm{rd}}$ correspond to $\bar{M}_4$ orbits $\bar{O}$ on $\mathrm{Ni}(G_k,\mathbf{C})^{\mathrm{rd}}$. Use $\mathcal{H}_{k,\bar{O}}$ for the level k component corresponding to $\bar{O}$.
(1.4b) The cusps of $\mathcal{H}_{k,\bar{O}}$ correspond to γ_∞ orbits $O_1,\dots,O_t$ on $\bar{O}$; cusp widths are the orbit lengths.
(1.4c) The genus $g_{\bar{O}}$ of $\mathcal{H}_{k,\bar{O}}$ appears in the formula

$$2(|\bar{O}| + g_{\bar{O}} - 1) = \mathrm{ind}(\gamma_0) + \mathrm{ind}(\gamma_1) + \mathrm{ind}(\gamma_\infty), \text{ with } \gamma_0 = (\gamma_1\gamma_\infty)^{-1}.$$

List as $O_1,\dots,O_u$ all γ_∞ orbits on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{rd}}$, without regard in which $\bar{M}_4$ orbit they fall. The symbol $(O_i)\mathbf{sh}$ means to apply $\mathbf{sh}$ to each reduced equivalence class in O_i. The (i,j) term of the $\mathbf{sh}$-incidence matrix $A(G,\mathbf{C})$ is $|(O_i)\mathbf{sh} \cap O_j|$. As $\mathbf{sh}$ has order two on reduced Nielsen classes, this is a symmetric matrix. Reorder $O_1,\dots,O_u$ to arrange $A(G,\mathbf{C})$ into blocks along the diagonal. Each block corresponds to an irreducible component of $\mathcal{H}(G,\mathbf{C})^{\mathrm{rd}}$ [**BFr02**, Lem. 2.26]. [**BFr02**, §2.10] shows how efficient is the shift incidence matrix in computing orbits by doing the case $(A_5, \mathbf{C}_{3^4})$ with $\mathbf{C}_{3^4}$ indicating four repetitions of the conjugacy class of 3-cycles. The harder case $(G_1, \mathbf{C}_{3^4})$ appears in [**BFr02**, §8.5]. The **sh**-incidence matrix works for general r similarly, though for $r \geq 5$ there is no corresponding group $\mathcal{Q}''$ and the matrix is no longer symmetric [**BFr02**, §2.10.2].

2. p-perfect groups and associated modular curve-like towers

Let G be a finite group with p a prime dividing $|G|$. Suppose $r \geq 3$ and we have an r-tuple of p' conjugacy classes of $G = G_0$. This produces a natural tower $\{\mathcal{H}_k\}_{k=0}^\infty$ of affine moduli spaces covering $\mathbb{P}^r \setminus D_r$. If G is p-perfect, then Thm. 2.10 says each tower level is a fine moduli space.

2.1. Module theory for the split case. With $\mathbb{Z}_p$ the p-adic integers, let -1 acting on $\mathbb{Z}_p$ by multiplication. For p odd, $\mathbb{Z}_p \times^s \{\pm 1\} \to \mathbb{Z}/p \times^s \{\pm 1\}$ is a cover of p-perfect groups. With p dividing the order of G, we generalize this by considering the universal p-Frattini cover $\varphi : {}_p\tilde{G} \to G_0$. Then, φ has a pro-free pro-p kernel. In the p-split case, $G = G_0 = P_0 \times^s H$ with P_0 the p-Sylow of G and H is a p' group. The H action extends to the minimal pro-free pro-p cover $\varphi : \tilde{P} \to P_0$ [**BFr02**, Prop. 5.3]. We explain the characteristic groups in this easy case.

We inductively consider $\ker_0 = \ker(\varphi)$ and $\ker_k$, the kth iterate of the Frattini subgroup of $\ker_0$. So, $\ker_1$ is the Frattini subgroup of $\ker_0$, generated by pth powers and commutators of $\ker_0$; $\ker_2$ is he Frattini subgroup of $\ker_1$, etc. The action of H extends to $\tilde{P}$ and to $\tilde{P}/\ker_k = P_k$, $k \geq 0$, in many ways [**BFr02**, Rem. 5.2]. Denote the characteristic quotients of $\tilde{P} \times^s H$ by $\{G_k = G_k(P_0 \times^s H) = P_k \times^s H\}_{k=0}^\infty$. Define M_k as $\ker_k / \ker_{k+1}$. This is a right G_k module as follows: $g \in G_k$ maps $k \in \ker_k / \ker_{k+1}$ to $\hat{g}^{-1} k \hat{g}$ (right action), with $\hat{g}$ any lift of $g \to G_{k+1}$.

LEMMA 2.1. *Let U be the Frattini subgroup of P_0, and let V^* be the dual space to $P_0/U = V$. We characterize $G_0 = P_0 \times^s H$ being p-perfect by the induced map of H on V^* has no nontrivial H invariant vector $v^* \in V^*$.*

PROOF. Suppose $v^* \in V^* \setminus \{0\}$ is H invariant. Let U' be the pullback to P of $\ker(v^*)$. Consider $\psi : P_0 \times^s H \to \mathbb{Z}/p$ by $hk \mapsto k \bmod U'$, for $h \in H$ and $k \in P_0$. We check this is a homomorphism: $hkh'k' = hh'((h')^{-1}kh')k'$ and $(h')^{-1}kh' \bmod U' \equiv k \bmod U'$. Reverse the steps for the converse. □

Let K be a field. For any finite group G, the group ring $\Lambda = K[G]$ is an augmentation algebra from the ring homomorphism aug : $\sum_i a_i g_i \mapsto$

$\sum_i a_i$. The quotient vector space from aug is the identity module $\mathbf{1}_G = K$ for Λ from

$$\sum_i a_i g_i \alpha = (\sum_i a_i)\alpha \text{ for } \alpha \in \Lambda/\ker(\text{aug}).$$

Also, maximal 2-sided ideals are in ker(aug). So, the Jacobson radical $\text{Rad}(\mathbb{F}_p[G])$, the intersection of he maximal 2-sided ideals of Λ, is also. When G is a p-group, the Jacobson radical is exactly ker(aug).

DEFINITION 2.2 (Involution pairing). Suppose $V = K^n$, and $h \in S_n$ has order 2 acting as permutations on the standard basis vectors for V. Define an inner (dot) product pairing: $v_1 = (x_1, ..., x_n)$ and $v_2 = (y_1, ..., y_n)$ pair to $\langle v_1, v_2\rangle_h = \sum_{i=1}^n x_i y_{(i)h}$. Then, $\langle\cdot,\cdot\rangle_h$ is symmetric.

DEFINITION 2.3. Let Λ be a commutative, associative algebra with unit 1_Λ. Suppose there is a nondegenerate inner product $\langle,\rangle$ with $\langle ab, c\rangle = \langle a, bc\rangle$, $a, b, c \in \Lambda$. We call Λ a *Frobenius* algebra.

EXAMPLE 2.4. With K a field, let $\Lambda = K[G]$. Elements of G form a K basis of Λ. We take $h = h_{\text{inv}}$ to permute G by $g \mapsto g^{-1}$. Then, $\langle a, b\rangle$ is the coefficient of 1_G in ab, and $\langle ab, c\rangle$ is the coefficient of 1_G in abc. So, associativity of multiplication in $K[G]$ makes $K[G]$ a Frobenius algebra.

For Λ a symmetric Frobenius algebra, any left Λ module is isomorphic to its dual $\Lambda^* = \text{Hom}_k(\Lambda, k)$, a right Λ module. Conclude: The projective and injective Λ modules are the same. A *primitive idempotent* of Λ is one we can't decompose as a nontrivial sum of orthogonal idempotents. These correspond to projective indecomposables.

Let M and N be right $K[G]$ modules. The *Hopf algebra* structure on $K[G]$ comes from $\sum_i a_i g_i \mapsto \sum_i a_i g_i \otimes g_i$. This gives $M \otimes_K N$ a $K[G]$ module structure. The projective indecomposables P satisfy $\text{Soc}(P) \equiv P/\text{Rad}(P)$. So, the simple modules G at the top and bottom *Loewy layers* (see §2.3) of a projective indecomposable module are the same.

2.2. Module theory for (G_0, p) in the general case. Let $\tilde{P}$ be a pro-free pro-p group with the same rank as the p group P_0. Assume $G_0' = P_0 \times^s H$ is the p-split case. Then, $\tilde{P} \times^s H$ is the universal p-Frattini cover of G_0'. Now we do the nonsplit case. Every group $G = G_0$ with p dividing $|G_0|$ has a (nontrivial) universal p-Frattini cover ${}_p\tilde{G}_0$. It is versal for covers of G_0 with p-group kernel as is $\mathbb{Z}_p \times^s \{\pm 1\}$ versal for covers of D_p with p-group kernel ([**FJ86**, Chap. 21], [**Fri95**, Part II] and [**BFr02**, §3.3]).

It is harder, however, to describe ${}_p\tilde{G}_0$ for general G_0. Let P_0 be a p-Sylow of G_0. Use G_0' for the normalizer in G_0 of P_0. (Don't confuse G_0' with the commutator of G_0.) By Schur-Zassenhaus, $G_0' = P_0 \times^s H$ with H a (maximal) p'-split quotient of G_0'. Let $\varphi_{k,t} : G_k \to G_t$, $t \le k$ be the natural map. We apply $'$ to modules and groups associated with the universal p-Frattini cover of G_0' in §2.1:

$$\{M_k' = \ker(G_{k+1}' \to G_k') = \ker(\varphi_{k+1,k}')\}_{k=0}^{\infty}.$$

2.2.1. *Inducing from G_0' to G_0*. Now remove the $'$, as in such notation as $\{M_k = \ker(\varphi_{k+1,k})\}_{k=0}^{\infty}$, for groups and modules corresponding to G_0. We regard $\mathbb{F}_p[G_0]$ as a left $\mathbb{F}_p[G_0']$ module and as a right $\mathbb{F}_p[G_0]$ module. The induced module $\text{ind}_{G_0'}^{G_0}(M_0')$ is the G_0 module

$$M_0' \otimes_{\mathbb{F}_p[G_0']} \mathbb{F}_p[G_0] = M_0' \otimes_{\mathbb{F}_p} \mathbb{F}_p[G_0/G_0'].$$

The notation $\mathbb{F}_p[G_0/G_0']$ is for the right G_0 module written as the vector space generated by right cosets of G_0' in G_0. Then, $\text{ind}_{G_0'}^{G_0}(M_0')$ is a right G_0 module.

Suppose N is a right G_0 module. Any $\mathbb{Z}/p[G_0']$ homomorphism $\psi : M \to N$ extends to a $\mathbb{Z}/p[G_0]$ module homomorphism $\text{Ind}_{G_0'}^{G_0}(M) \to M$ by $m \otimes g \mapsto \psi(m)^g$. Recall that M_0 is an indecomposable G_0 module ([**Ben91**, p. 11, Exec. 1] or [**FK97**, Indecom. Lem. 2.4]). To characterize M_0 as the versal module for exponent p extensions of G_0, we use this result [**Fri95**, Prop. 2.7].

PROPOSITION 2.5. *The cohomology group $H_2(G_0, M_0)$ has dimension one over $\mathbb{F}_p$. The 2-cocycle for the short exact sequence*

$$1 \to M_0 \to G_1 \to G_0 \to 1$$

represents a generator. We define any nontrivial $\alpha \in H_2(G_0, M_0)$ as G_1 up to an automorphism fixed on the G_0 quotient and multiplying M_0 by a scalar.

REMARK 2.6 (Automorphisms of M_0). Suppose G acts on a vector space M. Assume $L : M \to M$ is a linear map (though our notation is multiplicative) commuting with G. Let $\psi \in H^2(G, M)$. So, ψ makes $G \times M$ into a group through this formula:

$$(g_1, m_1) * (g_2, m_2) = (g_1 g_2, m_1^{g_1} m_2 \psi(g_1, g_2)),\ g_1, g_2 \in G,\ m_1, m_2 \in M.$$

By replacing $\psi(g_1, g_2)$ by $L(\psi(g_1, g_2)) \stackrel{\text{def}}{=} \psi_L(g_1, g_2)$ we preserve the cocycle condition. Scalar multiplication by $u \in \mathbb{Z}/p$ replaces $\psi(g_1, g_2)$ by $\psi(g_1, g_2)^u$. Even when M_0 is the characteristic p-Frattini module for G_0, there may be nontrivial maps L (not given by scalar multiplication) that preserve the cocycle. This produces nontrivial automorphisms of

G_1 that induce the identity on G_0. Such an L exists when $G_0 = K_4$, the Klein 4-group, and M_0 has dimension 5 in §4.3.2.

2.2.2. *Using the indecomposability of M_k as a $\mathbb{Z}/p[G_k]$ module.* We use an observation on the natural extension $\varphi_{1,0} : G_1 \to G_0$.

LEMMA 2.7. *The extension $\varphi_{1,0}^{-1}(G_0') \to G_0'$ is not split.*

PROOF. We apply Thm. 2.10. Then, any $g \in G_0$ having order p lifts to have order p^2 in G_1. This holds if g is in a p-Sylow P_0 of G_0'. This is a contradiction if if $\varphi_{1,0}^{-1}(G_0') \to G_0'$ splits. □

PROPOSITION 2.8. *A natural extension* $\mathrm{Ind}_{G_0'}^{G_0}(M_0') \to G^* \xrightarrow{\alpha^*} G_0$ *induces a surjective G_0 module homomorphism ψ :* $\mathrm{Ind}_{G_0'}^{G_0}(M_0') \to M_0$. *This gives a G_0 splitting $M \oplus N$ of* $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ *that makes G^*/N isomorphic to G_1. So, if* $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ *is indecomposable, we see that G^* is isomorphic to G_1 as a cover of G_0.*

PROOF. An element $\alpha' \in H^2(G_0', M_0')$ defines the extension $G_1' \to G_0'$. By Shapiro's Lemma, $H^2(G_0', M_0') = H^2(G_0, \mathrm{Ind}_{G_0'}^{G_0}(M_0'))$ [**Ben91**, p. 42]. So α' canonically defines $\alpha \in H^2(G_0, \mathrm{Ind}_{G_0'}^{G_0}(M_0'))$. The extension $\mathrm{Ind}_{G_0'}^{G_0}(M_0') \to G^* \xrightarrow{\alpha^*} G_0$ represents α. Regard $\{\alpha(h,h')\}_{h,h' \in G_0'}$ as giving a multiplication on $G_0' \times M_0'$: $(h,m)*(h',m') = (hh', m^{h'}m'\alpha(h,h'))$. The associative law for this multiplication is the cocycle condition. Extend it to $\mathrm{Ind}_{G_0'}^{G_0}(M_0') \times G_0$ using the following rules involving right coset representatives $g_1, \dots, g_n$ with $n = (G_0 : G_0')$:

(2.1a) $m^{g_i} = m \otimes g_i$, $m \in M_0'$; and

(2.1b) $\alpha(hg_i, h'g_{i'}) = \alpha(h, h'')$ with h'' satisfying the equation $h''g_j = g_i h' g_i^{-1}$ for some j.

Since $G^* \to G_0$ is a cover with exponent p kernel, there exists $\beta : G_1 \to G^*$ covering G_0. Let $H^* = (\alpha^*)^{-1}(G_0')$ and $H_1 = \varphi_{1,0}^{-1}(G_0')$. There exists a homomorphism $\gamma : G_1' \to H_1$ because G_1' is the universal exponent p Frattini cover of G_0'. Lemma 2.7 says $H_1 \to G_0'$ does not split. Further, the induced map $M_0' \to M_0$ extends to a map of G_0 modules $\mathrm{Ind}_{G_0'}^{G_0}(M_0') \to M_0$ by $m_i' \otimes g_i \mapsto \gamma(m_i)^{g_i}$.

So, the cocycle defining the extension $G^* \to G_0$ maps to a cocycle defining an extension $\psi : G^\dagger \to G_0$ with $\ker(\psi) = M_0$. Since the restriction of ψ over G_0' is nonsplit, Prop. 2.5 says $\psi : G^\dagger \to G_0$ identifies with the extension $G_1 \to G_0$. This produces the corresponding homomorphism of groups $G^* \to G_1$. We also call this γ. As $G_1 \to G_0$ is a Frattini cover, γ must be surjective.

Consider $\beta \circ \gamma = \mu$ and let $\mu^{(t)}$ be its tth iterate restricted to $\mathrm{Ind}_{G_0'}^{G_0}(M_0'))$. We apply Fitting's Lemma [**Ben91**, Lem. 1.4.4]. Conclude, for suitably high t, $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ decomposes as a G_0 module into a direct sum of the kernel and range of $\mu^{(t)}$. The range will be an indecomposable G_0 summand isomorphic to the indecomposable module M_0. If $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ is already indecomposable, it must be isomorphic to M_0. □

2.2.3. *A difference between M_0 and M_k, $k \geq 1$.* For $k \geq 1$, the universal p-Frattini cover of G_k is still ${}_p\tilde{G}$. We see this from the characterization of ${}_p\tilde{G}$ as the minimal p-projective cover of G_k [**FJ86**, Prop. 20.33 and Prop. 20.47]. By its definition, M_k is a G_k module. So, for $k \geq 1$, it is also the 1st characteristic module for the p-Sylow of G_k.

We designed Prop. 2.8 to handle level 0 where there can be a distinctive difference between $M_0(P_0)$ and $M_0(G_0)$. Ex. 2.11 shows the most extreme case of this, according to Prop. 2.8, with $\mathrm{Ind}_{G_0'}^{G_0}(M_0') = M_0$. There are several types of intermediate situations by considering groups $G^\dagger$, properly containing $N_{G_0}(G_0')$ with $M_0(P_0)$ a $G^\dagger$ module extending the action of $N_{P_0}(G_0)$. To assure $M_0(G^\dagger) = M_0'$, we need a nontrivial $\alpha \in H^2(G^\dagger, M_0(P_0))$. Since $(G^\dagger : N_{P_0}(G_0)), p) = 1$, restriction to the one-dimensional $H^2(N_{P_0}(G_0), M_0(P_0))$ (Prop. 2.5) is injective. So, the extension for α gives the group G_1 for $G^\dagger$.

An example of this is $G_0' = A_4 \leq G_0 = A_5$ and $p = 2$. This shows the other extreme of Prop. 2.8: $M_0' = M_0(P_0) = M_0(G_0)$ ([**BFr02**, Prop. 5.4] for a quick constructive proof, or [**Fri95**, Prop. 2.9]).

REMARK 2.9 (Extending Prop. 2.8). Suppose the situation above occurs with a nontrivial α for $G^\dagger$. The argument for Prop. 2.8 applies by replacing $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ with $\mathrm{Ind}_{G^\dagger}^{G_0}(M_0')$. We could have a complicated sequence applying this process before confidently proclaiming the exact summand of $\mathrm{Ind}_{G_0'}^{G_0}(M_0')$ giving $M_0(G_0)$.

2.3. Radical layers and the appearance of $\mathbf{1}_{G_k}$. *Radical layers* of M_k are the G_k module quotients

$$\mathrm{Rad}(\mathbb{Z}/p[G_k])^j M_k / \mathrm{Rad}(\mathbb{Z}/p[G_k])^{j+1} M_k, \qquad (j \geq 0).$$

These radical layers gives a maximal sequence of G_0 submodule quotients, with each a direct sum of simple G_0 modules. The Loewy display captures this data. It includes arrows showing how simple modules from different layers form subquotient extensions. One example occurs in Ex. 2.11. [**BFr02**, Cor. 5.7] exploits one case for A_5 and $p = 2$. We see it in its restriction to A_4 and to $K_4 \leq A_4$ in §4.3.2.

Appearances of $\mathbf{1}_{G_k}$, the trivial G_k module, in the Loewy layers of M_k usually effect the structure of the kth level of a Modular Tower. The appearance of $\mathbf{1}_{G_k}$ at the tail of M_k interprets that G_{k+1} has a center. Thm. 2.10 includes one reason for the hypothesis that G_0 is p-perfect [**BFr02**, Prop. 3.21].

THEOREM 2.10. *Suppose p divides the order of $g \in G_k$. Then, any lift $\hat{g} \in G_{k+1}$ has order $p \cdot \mathrm{ord}(g)$. Assume $g \in G_k$ is a p' element. A unique p' conjugacy class of G_{k+1} lifts g. If G_0 is centerless and p-perfect, so is G_k for all k.*

EXAMPLE 2.11 (A_5 and $p = 5$). The normalizer of P_0 in A_5 is a dihedral group G_0' and M_0' is $\mathbb{Z}/5$. From Prop. 2.8, M_0 is an indecomposable component of the rank $(G_0 : G_0') = 6$ module $\mathrm{ind}_{G_0'}^{G_0} M_0'$. There is an obvious 5-Frattini cover

$$\varphi' : \mathrm{PSL}_2(\mathbb{Z}/5^2) \to \mathrm{PSL}_2(\mathbb{Z}/5) = A_5.$$

The kernel of φ' is the adjoint representation U_3 for $\mathrm{PSL}_2(\mathbb{Z}/5)$. The rank of M_0 determines the rank (minimal number of generators) of $\ker_0$ as a pro-free pro-5 group. Conclude, if the rank of M_0 is 3, then $\varphi : \mathrm{PSL}_2(\mathbb{Z}_5) \to \mathrm{PSL}_2(\mathbb{Z}/5)$ would be the universal 5-Frattini cover of A_5. The kernel, however, of φ is not a pro-free group. Since there is no rank 2 simple $\mathbb{Z}/5[A_5]$ module, the Loewy display for M_0 either has three copies of the trivial representation in it, it is $U_3 \oplus U_3$, or it is $U_3 \to U_3$. The first fails Thm. 2.10 for then G_1 would have a nontrivial center. The second fails indecomposability of M_0. So, the last of these gives M_0.

3. Heuristics for the Main Conjecture when $r = 4$

Assume $r = 4$, $G = G_0$ is p-perfect and $\mathbf{C}$ is a collection of p' conjugacy classes of G_0 for which $\mathrm{Ni}(G_k, \mathbf{C})$ is nonempty for each integer $k \geq 0$. We given an intuitive justification why each component of $\mathcal{H}(G_k, \mathbf{C})^{\mathrm{rd}}$ has large genus if k is large.

3.1. The setup. [**BFr02**, §9.6] assumes we have no control over level 0 component genuses. So, a test for genus growth starts with assuming level 0 has a genus 0 component. Let $\bar{O}_k$ be a $\bar{M}_4$ orbit on $\mathrm{Ni}(G_k, \mathbf{C})^{\mathrm{rd}}$ at level $k \geq 0$. Assume its corresponding component has genus 0. Suppose $\bar{O}_{k+1}$ is a $\bar{M}_4$ orbit on $\mathrm{Ni}(G_{k+1}, \mathbf{C})^{\mathrm{rd}}$ lying above it. Let $O_1, \dots, O_t$ be the γ_∞ orbits on $\bar{O}_k$.

If a level k component has genus 1, then it is usually easy to find evidence of some ramification from $\bar{O}_k$ to $\bar{O}_{k+1}$. This assures the genus of $\bar{O}_{k+1}$ is at least 2, and the genus rises for orbits at higher levels over

$\bar{O}_{k+1}$ automatically. So, we give simple reasons why we expect the rise of the genus follows from (1.4). Our setup is to compute the genus of a component (corresponding to a $\bar{M}_4$ orbit) $\bar{O}_{k+1}$ at level $k+1$ lying over a component $\bar{O}_k$ at level k, assuming $\bar{O}_k$ has genus 0.

3.2. Elliptic ramification and orbit shortening. We denote the component corresponding to $\bar{O}_{k+1}$ by $\mathcal{H}^{\rm rd}_{\bar{O}_{k+1}}$. Each $\boldsymbol{p}_{k+1} \in \mathcal{H}_{\bar{O}_{k+1}}$ represents a cover

$$\varphi_{\boldsymbol{p}_{k+1}} : X_{\boldsymbol{p}_{k+1}} \to \mathbb{P}^1_z.$$

Suppose $\boldsymbol{p}_{k+1}$ over 0 or 1 on $\mathbb{P}^1_j$ actually ramifies over its image $\boldsymbol{p}_k \in \mathcal{H}^{\rm rd}_{\bar{O}_{k+1}}$. So, it contributes 2 (resp. 1) to $\text{ind}(\gamma_0)$ (resp. $\text{ind}(\gamma_1)$) on the right of (1.4c) (when $\bar{O} = \bar{O}_{k+1}$). Ramification from $\boldsymbol{p}_k$ to $\boldsymbol{p}_{k+1}$ implies that in going from $0 \in \mathbb{P}^1_j$ (or 1) up to $\boldsymbol{p}_k$ there is no ramification. That is, there is a nontrivial element $\alpha \in \text{PGL}_2(\mathbb{C})$ and another cover $\varphi_{\boldsymbol{p}'_{k+1}} : X_{\boldsymbol{p}'_{k+1}} \to \mathbb{P}^1_z$ with the following properties.

(3.1a) $\varphi_{\boldsymbol{p}'_{k+1}}$ lies over $\varphi_{\boldsymbol{p}'_k} : X_{\boldsymbol{p}'_k} \to \mathbb{P}^1_z$.

(3.1b) There is an isomorphism $\mu_k : X_{\boldsymbol{p}_k} \to X_{\boldsymbol{p}'_k}$ with $\varphi_{\boldsymbol{p}'_k} \circ \mu_k = \alpha \circ \varphi_{\boldsymbol{p}_k}$.

(3.1c) There is *no* such isomorphism $\mu_{k+1} : X_{\boldsymbol{p}_{k+1}} \to X_{\boldsymbol{p}'_{k+1}}$ lying over μ_k.

We refer to (3.1) as saying there is *elliptic ramification* from $\bar{O}_k$ to $\bar{O}_{k+1}$. If each $\bar{M}_4$ orbit $\bar{O}_{k+1}$ over $\bar{O}_k$ has no points $\boldsymbol{p}_k$ giving elliptic ramification, we say $\bar{O}_k$ has no elliptic ramification. This is exactly what happens in inner space examples from [**BFr02**, §8.1.1] and with modular curves at level 0.

CONJECTURE 3.1. We assume the Main Conjecture hypotheses and that k is large. Then, there is no elliptic ramification above any component at level k.

The last sentence of Thm. 2.10 assures G_k has no center. In turn this is equivalent to inner Hurwitz space covers having fine moduli. We test for reduced (inner) Hurwitz spaces to have fine moduli in two steps [**BFr02**, Prop. 4.7]. Denote the pullback of $\bar{O}_k$ to $G\backslash\text{Ni}(G_k, \mathbf{C})$ by $\bar{O}^*_k$. Then, $\mathcal{H}^{\rm rd}_{\bar{O}_k}$ has *b-fine moduli* (fine moduli off the fibers over $j=0$ and 1) if and only if Q'' (§1.3) is faithful on $\bar{O}^*_k$. Given b-fine moduli, then $\mathcal{H}^{\rm rd}_{\bar{O}_k}$ has fine moduli if and only if neither γ_0 nor γ_1 has fixed points on $\bar{O}_k$. If $\mathcal{H}^{\rm rd}_{\bar{O}_k}$ has b-fine (resp. fine) moduli, then so does $\mathcal{H}^{\rm rd}_{\bar{O}_{k+1}}$.

Orbit shortening is another phenomenon that affects the Riemann-Hurwitz formula for computing the genus of $\mathcal{H}^{\rm rd}_{\bar{O}_k}$ components. [**BFr02**, Lem. 8.2] explains orbit shortening as reducing the length of q_2 orbits in

$\bar{O}_k^*$ to their image γ_∞ orbits in $\bar{O}_k$. Though this is significant for precise data about cusps, for it too there is a natural working hypothesis.

CONJECTURE 3.2. For k large, there is no orbit shortening above $\mathcal{H}^{\rm rd}_{\bar{O}_k}$.

3.3. p-growth of cusps. We differentiate between two types of γ_∞ orbits.

3.3.1. *p-divisible cusps.* For $\boldsymbol{g} = (g_1, g_2, g_3, g_4) \in O_i$, denote $|\langle g_2 g_3\rangle|$ by $\mathbf{mp}(\boldsymbol{g})$, the *middle product* of $\boldsymbol{g}$. Call O_i (or $\boldsymbol{g}$) *p-divisible* if $p|\mathbf{mp}(\boldsymbol{g})$. Suppose $\boldsymbol{g}' \in \bar{O}_{k+1}$ lies above $\boldsymbol{g}$: $\boldsymbol{g}' \mod M_k = \boldsymbol{g}$. Express this with the notation $\boldsymbol{g}'/\boldsymbol{g} \in \bar{O}_{k+1}$. The $\bar{M}_4$ action guarantees the number of elements of $\bar{O}_{k+1}$ lying over $\boldsymbol{g} \in \bar{O}_k$ depends only on $\bar{O}_k$. Denote $|\bar{O}_{k+1}|/|\bar{O}_k|$, the *degree* of $\bar{O}_{k+1}$ over $\bar{O}_k$, by $[\bar{O}_{k+1}, \bar{O}_k]$.

Choose one representative ${}_i\boldsymbol{g}$ in each O_i, $i = 1, \dots, t$. Order the orbits so the first t' of these, $O_1, \dots, O_{t'}$, are the p-divisible cusps. For $i \le t'$ and $\boldsymbol{g}'/{}_i\boldsymbol{g} \in \bar{O}_{k+1}$, Thm. 2.10 implies $\mathbf{mp}(\boldsymbol{g}') = p \cdot \mathbf{mp}(\boldsymbol{g}_i)$. For $i \ge t'+1$, let U_i be the number of p-divisible $\boldsymbol{g}'/{}_i\boldsymbol{g} \in \bar{O}_{k+1}$.

Assume the genus of $\bar{O}_k$ is 0 and the conclusion of Conj. 3.2 holds for $\bar{O}_k$: No orbits shorten from $\bar{O}_k$ to $\bar{O}_{k+1}$. Then, the following holds [**BFr02**, Lem. 8.2]:

$$g_{\bar{O}_{k+1}} \ge \Big(\frac{(p-1)}{2p}t' - 1\Big)[\bar{O}_{k+1}, \bar{O}_k] + 1 + \frac{(p-1)}{2} \sum_{t'+1 \le i \le t} U_i. \tag{3.2}$$

The next proposition is essentially in [**BFr02**, Lem. 8.2].

PROPOSITION 3.3. *To the previous assumptions add that the conclusion of Conj. 3.1 holds for $\bar{O}_k$: There is no elliptic ramification from $\bar{O}_k$ to $\bar{O}_{k+1}$. Then, $g_{\bar{O}_{k+1}}$ equals the right side of* (3.2).

EXAMPLE 3.4 (Situations where the genus rises). We keep the assumptions of Prop. 3.3. Then, the genus rises if $t' > 2p/(p-1)$. If $t' = 0$, expression (3.2) requires that some of the U_i s are positive. So, we have p-divisible cusps on $\bar{O}_{k+1}$. At the next level that forces $t' > 0$. Notice with these assumptions that $[\bar{O}_{k+1}, \bar{O}_k] \ge p$, for there must be some ramification. There are a few boundary cases of concern, like $p = 2$, $t' = 4$ and $[\bar{O}_{k+1}, \bar{O}_k] = 2$.

4. Types of Schur multipliers

Continue notation from §2.3. Suppose the first radical layer of M_k contains $\mathbf{1}_{G_k}$. This means G_k has a nontrivial p part to its Schur multiplier. Several mysterious events can occur from this.

(4.1a) A $\bar{M}_r$ orbit $\bar{O}_k \subset \mathrm{Ni}(G_k, \mathbf{C})^{\rm rd}$ may have nothing over it in $\mathrm{Ni}(G_{k+1}, \mathbf{C})^{\rm rd}$.

(4.1b) Suppose O is a γ_∞ orbit in $\bar{O}_k$ that is not p-divisible. Still, it may have all γ_∞ orbits in $\mathrm{Ni}(G_{k+1}, \mathbf{C})$ above it p-divisible.

[**BFr02**, §9.3] illustrates (4.1a), while [**BFr02**, §5.4–5.5] illustrates (4.1b).

4.1. Setting up for appearance of Schur multipliers. Often we expect the genus to go up dramatically with the level, even from level 0 to level 1, even if there are components of genus 0 at level 0. Example: [**BFr02**, Cor. 8.3] computes in the $(A_5, \mathbf{C}_{3^4}, p=2)$ Modular Tower the genuses (12 and 9) of the two level 1 components over the one level 0 component of genus 0. The nontrivial Schur multiplier of G_0 gives many p-divisible cusps at level 1, though there are none at level 0. From the nontrivial Schur multiplier of G_1 there comes a complete explanation of the two very different components at level 1. For example, the genus 9 component has no component above it at level 2. We now show how to go beyond the spin cover situations that gave previous progress.

Let D be a G_{k+1} submodule of M_{k+1} with

(4.2) M_{k+1}/D the trivial (1-dimensional) G_k module $\mathbf{1}_{G_k}$.

Assuming G_0 is p-perfect assures there is a *unique* (up to isomorphism) cover $R_D = G_{k+2}/D \to G_k$ factoring through G_{k+1} as a central extension having kernel $\mathbb{Z}/p$ [**BFr02**, §3.6.1]. Often we identify D with the particular $\mathbb{Z}/p$ quotient of M_{k+1}. We refer to D or R_D as a *Schur quotient* at level k.

[**BFr02**] sometimes uses computations in the characteristic modules M_k in additive notation. That won't work in §4.2; we consider these as subgroups of G_{k+1} and quotients of subgroups of R_D.

4.2. Little p central extensions. Use the previous notation for the characteristic sequence $\{M_k\}_{k=0}^\infty$ of p-Frattini modules. Let $\{P_k\}_{k=0}^\infty$ be a projective system of p-Sylows of the corresponding groups $\{G_k\}_{k=0}^\infty$. §2.2.3 noted that

$$M_0(P_k) = M_k = \ker(P_{k+1} \to P_k) \text{ for } k \geq 1,$$

though this may not hold for $k=0$. Let D be an index p subgroup of the 1st Loewy layer of M_{k+1} and let R_D be the corresponding Schur quotient for ${}_p\tilde{G}$:

$$\ker(R_D \to G_{k+1}) = \mathbb{Z}/p \text{ with trivial } G_{k+1} \text{ action.}$$

Let $V_D^0 \subset M_k$ be those nonidentity elements of M_k with order p (rather than order p^2) lift to R_D. Use V_D to be V_D^0 augmented by the identity element of M_k (its lifts have order 1 or p).

Denote the map $R_D \to G_k$ by φ_D. Use the notation $\hat{M}_D$ (resp. $\hat{V}_D$) for the pullback of M_k (resp. V_D) in R_D. We will see that sometimes V_D is not a group. Still, the notation is valid. Use $\hat{m}$ for some lift of $m \in M_k$ to $\hat{M}_D$. Since $\hat{M}_D$ is a central extension of M_k, $\hat{m}^p$ depends only on m, and not on $\hat{m}$. We display the context for groups of order p^3 appearing in our calculations.

- $\mathbb{Z}/p^2 \times^s \mathbb{Z}/p = U_p$ with a generator of the right copy of $\mathbb{Z}/p$ mapping $1 \in \mathbb{Z}/p^2$ to $1+ap$ for some a prime to p.
- $(\mathbb{Z}/p)^2 \times^s \mathbb{Z}/p = W_p$ with a generator of the right $\mathbb{Z}/p$ acting as the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$.
- H_p is the small Heisenberg group : 2×2 unipotent upper triangular matrices with every element of order p.

LEMMA 4.1. *The group H_p $(p > 2)$ is isomorphic to W_p.*

PROOF. Note: H_p has a normal subgroup H' of index p. So H' is $(\mathbb{Z}/p)^2$. Further, the map $H_p \to H_p/H' = \mathbb{Z}/p$ splits (every element in H_p has order p). Finally, with some choice of basis, $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ has order p (acting on $(\mathbb{Z}/p)^2$). $\square$

The following lemma has notation appropriate for our applications. Still it is very general: We could have M_k can be any $\mathbb{Z}/p$ module, $\hat{M}_D$ any Frattini extension of it with $\mathbb{Z}/p$ kernel and V_D^0 the elements of M_k lifting to have order p in $\hat{M}_D$.

LEMMA 4.2. *Consider pairs $m_1, m_2 \in M_k$ where $\langle m_1, m_2\rangle$ has dimension 2. Denote the group generated by their lifts by $\langle \hat{m}_1, \hat{m}_2\rangle$.*

Suppose $m_1, m_2 \in V_D$. If $p = 2$, then $\langle \hat{m}_1, \hat{m}_2\rangle$ is either a Klein 4-group or it is D_4. If $p \neq 2$,then it is either $(\mathbb{Z}/p)^2$; U_p; or it is H_p and the commutator $(\hat{m}_1, \hat{m}_2)$ generates the kernel of $\langle \hat{m}_1, \hat{m}_2\rangle \to \langle m_1, m_2\rangle$.

Suppose $m_1, m_2 \in M_k \setminus V_D$. If $p = 2$, then $\langle \hat{m}_1, \hat{m}_2\rangle$ is either $\mathbb{Z}/2^2 \times \mathbb{Z}/2$ or it is Q_8 (the quaternion group). For $p \neq 2$, $\langle \hat{m}_1, \hat{m}_2\rangle$ is $\mathbb{Z}/p^2 \times \mathbb{Z}/p$ or it is U_p.

If $m_1 \in V_D^0$ and $m_2 \in M_k \setminus V_D$, $\langle \hat{m}_1, \hat{m}_2\rangle$ is either $\mathbb{Z}/p^2 \times \mathbb{Z}/p$ or U_p.

PROOF. The cases for $p = 2$ are in [**BFr02**, Lem. 2.24]. Now consider the cases where p is odd. If $m_1, m_2 \in V_D^0$, then their lifts $\hat{m}_1, \hat{m}_2$ have order p. Further, they either commute or $(\hat{m}_1, \hat{m}_2)$ generates the kernel of $\langle \hat{m}_1, \hat{m}_2\rangle \to \langle m_1, m_2\rangle$. These properties determine the group to be the two cases in the statement.

If $m_1, m_2 \in M_k \setminus V_D$ then $\hat{m}_1, \hat{m}_2$ have order p^2. If $\hat{m}_1$ and $\hat{m}_2$ commute, the result is that in the lemma. Assume, however, they don't commute. Let H be an index p (normal) subgroup of $\langle\hat{m}_1,\hat{m}_2\rangle$. Suppose the natural map

$$\mu:\langle\hat{m}_1,\hat{m}_2\rangle\to\langle\hat{m}_1,\hat{m}_2\rangle/H$$

splits. Then, the group is either U_p or it is $W_p=H_p$. The latter, however, has no elements of order p^2. So it is the former. We are done if we show μ splits. Equivalently, with C the center of $\langle\hat{m}_1,\hat{m}_2\rangle$, we are done if some nontrivial element of $\langle\hat{m}_1,\hat{m}_2\rangle/C$ lifts to have order p in $\langle\hat{m}_1,\hat{m}_2\rangle$.

Conjugate $\hat{m}_2$ by $\hat{m}_1$. Since the quotient $\langle\hat{m}_1,\hat{m}_2\rangle/C$ is abelian, the conjugate $\hat{m}_1\hat{m}_2\hat{m}_1^{-1}$ is $\hat{m}_2^{1+pa}$ for some integer $1\le a<p$. Compute:

$$A(\hat{m}_1,\hat{m}_2)\stackrel{\text{def}}{=}(\hat{m}_1\hat{m}_2)^p=(\prod_{i=1}^{p}(\hat{m}_1^i\hat{m}_2\hat{m}_1^{-i})^p\hat{m}_1^p=\hat{m}_2^{\sum_{i=1}^{p}(1+ap)^i}(\hat{m}_1)^p=\hat{m}_2^p\hat{m}_1^p.$$

Replace $\hat{m}_1$ by some p' power of it to assure $A(\hat{m}_1,\hat{m}_2)$ is 1, though $\hat{m}_1$ and $\hat{m}_2$ still generate $\langle\hat{m}_1,\hat{m}_2\rangle/C$. So $\hat{m}_1\hat{m}_2$ has order p, giving the desired splitting.

The last case works as the split case of the previous argument. □

Lem. 4.2 differentiates between $p=2$ and general p.

COROLLARY 4.3. *Assume $\hat{m}_i$ is a lift of $m_i\in M_k\setminus V_D$ to $\hat{M}_D$, $i=1,2$. Suppose too that $\langle m_1\rangle\ne\langle m_2\rangle$ and $V_D^0\cap\langle m_1,m_2\rangle$ is nonempty. Then, $H_{m_1,m_2}=\langle\hat{m}_1,\hat{m}_2\rangle$ is isomorphic to $\mathbb{Z}/p^2\times\mathbb{Z}/p$.*

PROOF. The hypotheses say that H_{m_1,m_2} has two generators of order p^2. It also has two generators with respective orders p^2 and p. The resulting group has order p^3, and $(\mathbb{Z}/p)^2$ as a quotient. Only $\mathbb{Z}/p^2\times\mathbb{Z}/p$ has these properties: elements of order 4 (resp. p^2) don't generate the dihedral group (resp. U_p); and the quaternion group's only element of order 2 is in its center. □

We use the following hypotheses to describe the possible groups $\hat{M}_D$ that actually can occur as $\varphi_D^{-1}(M_k)$ with M_k the Frattini module for G_k.

(4.3a) For each $m_1,m_2\in M_k\setminus V_D$, with $\langle m_1\rangle\ne\langle m_2\rangle$, $V_D^0\cap\langle m_1,m_2\rangle\ne\emptyset$.

(4.3b) Elements of $M_k\setminus V_D$ generate M_k.

(4.3c) V_D is a submodule of M_k.

PROPOSITION 4.4. *There always exists $\alpha_D\in M_k\setminus V_D$.*

Suppose (4.3a) *and* (4.3b) *hold. Then $\hat{M}_D$ is an abelian group, and therefore a $\mathbb{Z}/p^2[G_k]$ module. Further,* (4.3c) *then holds and* $\cup_{j=0}^{p-1}V_D\alpha_D^j=$

If $p = 2$, then (4.3c) *holds if and only if $\hat{V}_D$ is an abelian group isomorphic to $V_D \times \mathbb{Z}/2$. If both* (4.3a) *and* (4.3c) *hold, then $\hat{M}_D$ is a $\mathbb{Z}/4[G_k]$ module.*

PROOF. Suppose $M_k \setminus V_D$ is empty. Then, a lift of any $m \in M_k$ (excluding the identity) to R_D has order p. So, $R_D \to G_k$ (a Frattini extension) has kernel of exponent p. Since, however, $G_{k+1} \to G_k$ is the universal exponent p-Frattini cover of G_k, this shows $\hat{M}_D$ is a quotient of M_k. This contradiction produces $\alpha_D \in M_k \setminus V_D$.

Now suppose (4.3a). Cor. 4.3 implies, if $m_1, m_2 \in M_k \setminus V_D$, then H_{m_1,m_2} is an abelian group. If, further, (4.3b) holds, then $\hat{M}_D$ has pairwise commuting generators. So, $\hat{M}_D$ is an abelian group. For $\hat{g}$ a lift of $g \in G_k$ to R_D, $\hat{g}$ conjugation action on $\hat{M}_D$ depends only on g. This shows $\hat{M}_D$ is a $\mathbb{Z}/p^2[G_k]$ module.

Continue assuming (4.3a) and (4.3b) hold. Then, for any $\hat{m}$ lifting $m \in M_k$ to R_D, there is an integer j with

$$((\hat{m})(\hat{\alpha}_D)^{-j})^p = \hat{m}^p(\hat{\alpha}_D)^p = 1.$$

Therefore $m\alpha_D^{-j} \in V_D$ and $\langle \alpha_D \rangle$ fills out $M_k/V_D = \mathbb{Z}/p$.

Now assume $p = 2$, and (4.3a) and (4.3c) hold. If $m_1 \in M_k \setminus V_D$ and $v_2 \in V_D^0$, then (4.3c) says $m_2 = m_1 v_2$. So, H_{m_1,m_2} satisfies the hypotheses of Cor. 4.3 and is abelian. Consider H_{v_1,v_2} with $v_1, v_2 \in V_D$. If this group has order larger than 4, then it contains an order 4 element. Thus, $\langle v_1, v_2 \rangle$ contains an element of $M_k \setminus V_D$, contrary to (4.3c). Conclude: For any $m_1, m_2 \in M_k$, H_{m_1,m_2} is abelian. As elements $\hat{m}$ with $m \in M_k$ generate $\hat{M}_D$, this implies $\hat{M}_D$ is abelian. □

4.3. When $\hat{M}_D$ is abelian. We now characterize when $\hat{M}_D$ is an abelian group (and so a $\mathbb{Z}/p^2[G_k]$ module). This will play a big role in the expanded version of this paper. When this happens we call D an *abelian* $\mathbb{Z}/p$ Schur quotient (of the level k Schur multiplier). The tool for this characterization of abelian Schur quotients starts with [**BFr02**, Prop. 9.6]. We remind of the setup.

Let $\psi_k : R_k \to G_k$ be the universal exponent p central extension of G_k. This exists from the p-perfect assumption [**BFr02**, Def. 3.18]. Write R_k as ${}_p\tilde{G}/\ker_k^*$. Denote the closure of $\langle (\ker_k, \ker_k^*), (\ker_k^*)^p \rangle$ in $\ker_{k+1}$ by $\ker'_{k+1}$. Then, $\ker'_{k+1}$ defines ${}_p\tilde{G}/\ker'_{k+1} = R'_{k+1}$.

A lift of $m \in \ker(\varphi_{k+1,k})$ to $\ker(R'_{k+1} \to G_k)$ has order p^2 if and only the image of m in $\ker(R_k \to G_k)$ is nontrivial. We now take advantage of how elements of M_k with trivial images in $\ker(R_k \to G_k)$ form a submodule. This is the heart of Prop. 4.6, except we substitute a $\mathbb{Z}/p$ quotient $R_{D_{k-1}}$ of R_k for R_k, etc.

4.3.1. *Antecedents to a $\mathbb{Z}/p$ Schur quotient.* Let $R_{D_{k-1}}$ (resp. R_{D_k}) be a Schur quotient at level k (resp. level$k+1$).

DEFINITION 4.5. Suppose $\alpha \in {}_p\tilde{G}$ generates $\ker(R_{D_{k-1}} \to G_k)$ and α^p generates $\ker(R_{D_k} \to G_{k+1})$. Refer to $R_{D_{k-1}}$ as *antecedent* to R_{D_k}.

PROPOSITION 4.6. *In the notation above, there exists $R_{D_{k-1}}$ antecedent to R_{D_k} if and only if the conditions of* (4.3) *hold for R_{D_k}.*

OUTLINE OF PROOF. Assume there exists $R_{D_{k-1}}$ antecedent to R_{D_k}. [**BFr02**, Prop. 9.6]: V_{D_k} consists of $m \in M_k$ that map trivially to $\ker(R_{D_{k-1}} \to G_k)$; those m that don't map trivially to $\ker(R_{D_{k-1}} \to G_k)$ form the nonidentity cosets in M_k of V_{D_k}. Clearly these generate M_k. That shows (4.3a). Suppose $m_1, m_2 \in M_k \setminus V_D$, and $\langle m_1, m_2\rangle$ has rank 2. Since the image of $\langle m_1, m_2\rangle$ in $\ker(R_{D_{k-1}} \to G_k)$ has rank 1, there must be elements of V_D^0 in the kernel. This establishes (4.3b).

Now consider the converse. Assume the conditions of (4.3) hold for R_{D_k}. Prop. 4.4 implies that V_D is a $\mathbb{Z}/p$ module, so a $\mathbb{Z}/p[G_k]$ module, having codimension 1 in M_k. So, M_k/V_D is a 1-dimensional G_k module. In notation from Prop. 4.4, choose $\alpha_D \in M_k \setminus V_D$ to have its image generate M_k/V_D.

Suppose M_k/V_D is not the trivial G_k module. We can generalize [**BFr02**, Prop. 9.6] to suit any 1-dimensional G_k module appearing in the 1st Loewy layer of M_k. This would produce $\alpha \in {}_p\tilde{G}$ mapping to the image of α_D in $\ker(R_{D_{k-1}} \to G_k)$ with the image of α^p generating $\ker(R_{D_k} \to G_{k+1})$. Since, however, G_k does not act trivially on $\alpha_D \bmod \ker_k$, G_{k+1} would not act trivially on $\alpha^p \bmod \ker_{k+1}$. This contradicts that $\ker(R_{D_k} \to G_{k+1})$ is the trivial G_{k+1} module. $\square$

4.3.2. *The example A_4 and $p=2$.* For $p=2$, we stretch the module theory discussion of [**BFr02**, Ex. 9.2]. As above, with $G_1 = G_1(A_4)$, let R_1 be the universal exponent 2 central extension of G_1. Then, $\ker(R_1 \to G_1)$ is a Klein 4-group K_4. We have $A_4 = K_4 \times^s H$ with $H \simeq \mathbb{Z}/3$ acting irreducibly on the K_4. This H action extends to all the M_ks (see comment §2.1). So, we differentiate between actions on the Klein 4-groups by writing write $K_{4,H}$ for K_4 when the H action is nontrivial.

Consider the three distinct $\mathbb{Z}/2$ Schur quotients D_1, D_2, D_3 for G_1. (The subscripts are only decoration, not with the same meaning as in Prop. 4.6.) One Schur quotient has antecedent the Schur multiplier of A_4 (at level 0). We identify this with D_1. The Loewy display for $\ker(G_1 \to G_0) = M_0$ is $K_{4,H} \to K_{4,H} \oplus \mathbf{1}_{A_4}$ [**BFr02**, Cor. 5.7].

We found the complete description of the $\hat{M}_{D_i}$s by finding three central 2-Frattini extensions of $M = K_{4,H} \oplus \mathbf{1}_{A_4}$, the 1st Loewy layer of M_0. Then, we pulled these back from the map $M_0 \to M$, knowing that this would give all three possible Schur quotients. This makes it clear the elements of the left most $K_{4,H}$ lift to have order 2 in each of the $\hat{M}_{D_i}$ s. Here is the list.

$$\begin{aligned} \hat{M}_{D_1} &= K_{4,H} \to K_{4,H} \oplus \mathbb{Z}/4, \\ \hat{M}_{D_2} &= K_{4,H} \to Q_8 \oplus \mathbb{Z}/2, \\ \hat{M}_{D_3} &= K_{4,H} \to (Q_8 \cdot_{\mathbb{Z}/2} \mathbb{Z}/4). \end{aligned}$$

We have chosen to notation using a $\to$. It means that quotienting out by an appropriate $\mathbb{Z}/2$ center gives the corresponding Loewy display.

4.4. Next steps in investigating Schur quotients. The followup paper will expand the application of [**BFr02**, Prop. 9.8] to $(G_0 = A_5, \mathbf{C}_{3^4}, p = 2)$. In this situation we refer to $\boldsymbol{g} \in \mathrm{Ni}(G_0, \mathbf{C}_{3^4})$ as a *perturbation* of an H-M rep. if it has the form $(g_1, ag_1^{-1}a, bg_2b, g_2^{-1}) = \boldsymbol{g}_{a,b} \in \mathrm{Ni}(G_1, \mathbf{C}_{3^4})^{\mathrm{rd}}$ and it lies over

$$(g_1', (g_1')^{-1}, g_2', (g_2')^{-1}) \in \mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{rd}}, \text{ with } g_1' = (1\,2\,3) \text{ and } g_2' = (1\,4\,5).$$

[**BFr02**, Prop. 9.8] referenced H-M reps. to find and characterize the resulting $\bar{M}_4$ orbits: $\bar{O}_1$ (genus 12) and $\bar{O}_2$ (genus 9). We describe this in the language above.

Let R_{D_0} be the Frattini central extension of G_1 with antecedent the spin cover $\hat{A}_5 = \mathrm{SL}_2(\mathbb{Z}/5)$ of $A_5 = \mathrm{PSL}_2(\mathbb{Z}/5)$. So, D_0 gives an abelian quotient. Then, with no loss, we may choose $a, b \in M_0 \setminus V_{D_0}$ for the representatives of form $\boldsymbol{g}_{a,b}$ as above. There are two orbits for the action of A_5 on $M_0 \setminus V_{D_0}$, called M_3' (centralize elements of order 3) and M_5' (centralize elements of order 5). The 16 elements $\boldsymbol{g}_{a,b} \in \bar{O}_1$ (resp. $\in \bar{O}_2$) have a and b in the same (resp. in different) conjugacy classes from M_3' and M_5'.

We say in §4.3.2 that the case $(G_k(A_4), \mathbf{C}_{3^4})$, with $k = 1$, has a more complicated Schur quotient structure as k rises. In the expansion of this paper we extend this to the abelian cases at all levels of the $(A_4, \mathbf{C}_{3^4}, p = 2)$ and $(A_5, \mathbf{C}_{3^4}, p = 2)$ Modular Towers. We know the number of Schur quotients of $(G_k(A_4), \mathbf{C}_{3^4})$ rises with k. This is true for any *non-dihedral-like* split G_0 and any prime p [**Se01**]. [**BFr02**, §5.7] has a precise quote when $p = 2$ and a characterization of the phrase *dihedral-like*. We don't know yet how to extend it to the nonabelian $\mathbb{Z}/2$ Schur quotients. We don't know yet if for $k \geq 1$, $(G_k(A_4), \mathbf{C}_{3^4})$ has nonabelian $\mathbb{Z}/2$ Schur quotients, though we suspect so. For all non-split universal p-Frattini covers (assume p-perfect) it is a mystery what to expect of their Schur quotients.

5. The diophantine goal

It is instructive to see how the diophantine aspects of the long studied modular curves work. I base my remarks on [**Se97**, Chap. 5].

5.1. Setup diophantine questions. Question 5.2 is a version of the Main Conjecture. When $r = 4$ the §3 outline gives a good sense of it holding. The tests are for how properties of the universal p-Frattini cover of the finite group G contributes to the conjecture holding. [**BFr02**] tested many examples related to the case $G = G_0$ is an alternating group, $p = 2$ and the conjugacy classes have odd order. Details of those examples mirror what one often finds in papers on modular curves. An extra complication is that levels of a Modular Tower can have several components. Here's an example problem that is tougher than it first looks.

PROBLEM 5.1. For *each* number field K, find an easy argument for constructing a nonsingular curve X over K with $0 < |X(K)| < \infty$ (nonempty but finite).

Suppose G_0 is a p-perfect group, and $\mathbf{C}$ are p' conjugacy classes of G_0, such that all levels of the Modular Tower for $(G_0, \mathbf{C}, p)$ are nonempty.

PROBLEM 5.2. Give an elementary argument that for any number field K, $\mathcal{H}(G_k, \mathbf{C})^{\mathrm{rd}}(K) = \emptyset$ for k large.

Let $\bar{\mathcal{H}}(G_k, \mathbf{C})^{\mathrm{rd}} = \bar{\mathcal{H}}_k$ be a nonsingular projective closure of $\mathcal{H}(G_k, \mathbf{C})^{\mathrm{rd}}$. Even though $\mathcal{H}(G_k, \mathbf{C})^{\mathrm{rd}}(K) = \emptyset$, there may rational points on the cusps of $\bar{\mathcal{H}}(G_k, \mathbf{C})^{\mathrm{rd}}$.

PROBLEM 5.3. Same hypotheses as Ques. 5.2. Show, at suitably high levels of the tower, all components have general type.

We mean in Prob. 5.1 to avoid such heavy machinery as Falting's Theorem (proof of the Mordell Conjecture) or the Merel Theorem. We don't, however, expect a completely trivial argument for a general number field K. The property states that number fields are not *ample* (Pop's nomenclature). The goal is to produce a *witnessing* nonsingular curve X (given K) explicitly. This topic arose from [**Deb99**, §3.2.1]. We trace a set of ideas from Demjanenko and Manin as appropriate to our main point. Then, we connect Problems 5.1 and 5.2.

5.2. Outline of key points of [Ma69]-[De66]. The exposition from [**Se97**, Chap. 5] is convenient for this, especially for its review of effective aspects of Chabauty [**Ch41**].

THEOREM 5.4 (Chabauty). *Suppose a curve X generates an abelian variety A and Γ is a finitely generated subgroup of $A(K)$ with* $\text{Rank}(\Gamma) < \dim A = g'$. *Then,* $X(K) \cap \Gamma < \infty$.

EXPLICIT ASPECTS. Embed K in a finite extension of $\mathbb{Q}_p$ and regard it as that finite extension. Assume $0_A \in X(K)$, and let ω_i, $i = 1, \dots, g'$, be a basis of holomorphic differentials on A. These uniformize by $(\mathcal{O}_L)^{g'}$ an open subgroup $U \subset A(L)$ in the p-adic topology via the map $P \in A(L) \mapsto \int_{0_A}^{P}(\omega_1, \dots, \omega_{g'})$. With $\bar{\Gamma}$ the closure of Γ, suppose $X \cap \bar{\Gamma}$ is infinite. That gives a sequence of distinct points $P_i \mapsto P_0 \in X \cap \bar{\Gamma}$. Suppose $d < g'$ is the rank of the free group $\Gamma \cap U$. Change coordinates on U so the points $\gamma = (x_1, ..., x_{g'}) \in U \cap \bar{\Gamma}$ satisfy $x_1 = 0$ in a neighborhood of $0_A \in X$. Then the analytic curve intersects $x_1 = 0$ in infinitely many points. This implies $x_1 = 0$ in a neighborhood of 0_A in X. Since, however, X generates A, the pullback of $dx_1 = \omega_1$ is a nontrivial holomorphic differential. So, it has at most $2g(X) - 2$ zeros. □

[**Co85**] uses Thm. 5.4 to effectively bound the number of points on some curves, an analysis that includes finding a bound on $\text{Rank}(\Gamma)$ and bounding the number of torsion points of A that might meet X. An effective Manin Corollary comes down to effectively bounding the rank of $\text{Pic}^{(0)}(X_0(p^{k_0+1}))(K)$. The Weak-Mordell Weil Theorem gives such a bound [**Se97**, p. 52, §4.6]. Here, and for Modular Towers, we don't care that the bound does not precisely give the rank.

The Manin-Demjanenko argument reverts to Chabauty. We can see specific parameters we must compute to make Thm. 5.4 apply effectively. It starts by assuming X is any projective nonsingular absolutely irreducible variety over K, and A is an abelian variety over K for which there are morphisms $f_1, \dots, f_m : X \to A$ defined over K. With $P_0 \in X(K)$ assume $\bar{f}_i = f_i - f_i(P_0)$ satisfy these properties.

(5.1a) If $\sum_{i=1}^{m} n_i \bar{f}_i$ is zero on X, $n_1, \dots, n_m \in \mathbb{Z}$, then $(n_1, \dots, n_m)$ is 0.

(5.1b) The rank of the divisor classes modulo algebraic equivalence on X (the Néron-Severi group) is one.

If X is a curve, hypothesis (5.1b) is automatic. Depending on your patience, the following results are effective [**Se97**, p. 63].

THEOREM 5.5 (Conclusions of Manin-Demjanenko).

If $m > \text{Rank}(A(K))$, *then* $X(K)$ *is finite.*

COROLLARY 5.6 (Manin). *If $k(p,K)$ is large, then $X_0(p^{k+1})(K)$ is finite. So, we can choose $k(p,K)$ effectively dependent on bounding on* $\mathrm{Pic}^{(0)}(X_0(p^{k_0+1}))$.

KEY POINTS. Choose k_0 so the genus of $X_0(p^{k_0+1})$ exceeds 0. In parallel with the application to Modular Towers, [**BFr02**, Lem. 2.20] computes the cusp widths of $X_0(p^{k_0+1})$ (and so the growth of its genus) from a Hurwitz monodromy viewpoint. Let $A = Pic^{(0)}(X_0(p^{k_0+1}))$.

Assume the rank of $\mathrm{Pic}^{(0)}(X_0(p^{k_0+1}))(K)$ is m', and let $k(p,K) = k_0 + m' + 1$. We form the maps f_i, $i = 1, \ldots, m'+1$. They all go from $X_0(p^{k_0+m'+1})$ to $\mathrm{Pic}^{(0)}(X_0(p^{k_0+1}))$. Represent points on $X_0(p^{k_0+m'+1})$ by $(E, \langle \boldsymbol{p}_{k_0+m'+1}\rangle)$, a 2-tuple consisting of an elliptic curve and a $p^{k_0+m'+1}$ torsion point on it. Let $\boldsymbol{p}_i$ generate the cyclic subgroup of $\langle \boldsymbol{p}_{k_0+m'+1}\rangle$ of order p^i. Then, f_i maps the point $(E, \langle \boldsymbol{p}_{k_0+m'+1}\rangle)$ to $(E/\langle \boldsymbol{p}_i\rangle, \langle \boldsymbol{p}_{k_0+1+i}\rangle/\langle \boldsymbol{p}_i\rangle)$ (then to the Jacobian of $X_0(p^{k_0+1})$).

Suppose ω is a nonzero holomorphic differential on A. Then these $f_i^*(\omega))$, $i = 1, \ldots, m'$, are linearly independent over $\mathbb{C}$. To see this take any cusp and express ω in a neighborhood of that cusp as a power series $f(q)dq$ with $q = e^{2\pi i z}$, z close to $i\infty$. The condition for analyticity of ω at the cusp is that $f(q)$ is analytic and $f(0) = 0$. Now consider the pullbacks $\omega_i = f_i^*(\omega))$. The argument of [**Se97**, p. 68] is that f_i^* transforms q to q^{p^i}; so the ω_i s are linearly independent as power series in the variable q around the cusp. □

5.3. Using Demjanenko-Manin on Modular Towers. Each $X_0(p^{k+1})$ has cusps of unique widths that give rational points. This gives a relatively elementary construction of curves that demonstrably have some, but only finitely many, rational points over K. This is an acceptable answer to Prob. 5.1, though it is not so explicit a result as in [**Co85**]. In the expanded version of this paper we apply the argument of Cor. 5.6 to the abelianization of a Modular Tower with $r = 4$ [**BFr02**, §4.4.3]. It is crucial that the genus of tower components goes up (as outlined in §3). This is motivation for developing explicit versions on that argument.

An even greater potential occurs in using such an argument for $r \geq 5$. The hypotheses of (5.1) do not assume X is a curve. An interesting consideration is whether some version of (5.1b) holds at high levels of a Modular Tower for a p-perfect group $G = G_0$. We guess that at high levels the albanese varieties of (a nonsingular closure of) $\mathcal{H}_k^{\mathrm{rd}}$ will not have a unique polarization. Are there are other approaches to this hypothesis?

6. Finding projective systems of components over $\mathbb{Q}$

Let $\{G_k\}_{k=0}^{\infty}$ be the characteristic sequence of p-Frattini quotients of ${}_p\tilde{G}$. Here is a result from [**FK97**].

PROPOSITION 6.1. *Let r_0 be any positive integer. Suppose each G_k has a K regular realization with K a number field and no more than r_0 branch points. Then, there exists a Modular Tower based on $(G_0, \mathbf{C})$ with $r \le r_0$ conjugacy classes and $\mathbf{C}$ a set of p' conjugacy classes.*

If there are rational points at each level of a Modular Tower, then there is a projective system of (we always mean absolutely irreducible in this subsection) K components at each level.

DEFINITION 6.2. Call $\mathbf{C}$ *gcomplete* if any subgroup meeting all conjugacy classes in it is all of G. It is *p-gcomplete* if any subgroup meeting each p' conjugacy class is automatically all of G.

EXAMPLE 6.3. The group A_5 is 2-gcomplete. It is not, however, 3-gcomplete or 5-gcomplete since it contains D_5 and A_4. Further, if G_0 is p-gcomplete, then each of the characteristic p-Frattini covers $G_k \to G_0$ is also p-gcomplete.

DEFINITION 6.4. Call $\mathbf{C}$ H-M-gcomplete if upon removing any two distinct inverse conjugacy classes C_i, C_j, the remaining conjugacy classes $\mathbf{C}_{i,j}$ are gcomplete.

We review a result from [**Fri95**, Thm. 3.21] on H-M reps. (§1.2).

PROPOSITION 6.5. *Suppose at each level of a Modular Tower for the prime p, the H-M reps. fall in one H_r (Hurwitz monodromy) orbit $\bar{O}_{\mathrm{HM}}$. Then the component corresponding to $\bar{O}_{\mathrm{HM}}$ has definition field K where K is the field of rationality of the conjugacy classes. This holds if the conjugacy classes $\mathbf{C}$ are p-gcomplete: Then there is a projective system of H-M components over K.*

REMARK 6.6. As in Debes-Deschamps [**DDes01**], for K a discrete valued field, you can get a result over K for a p-perfect group. For $g \in G$ of order n call d the *cyclotomic order* of g if d is minimal for $K(\zeta_d) = K(\zeta_n)$. Suppose $\mathrm{C}'_1, \dots, \mathrm{C}'_t$ is a p-gcomplete set of p' conjugacy classes. Let d_i be the cyclotomic order of elements of C'_i, $i = 1, \dots, t$. With $r = 2\sum_{i=1}^{t}[K(\zeta_{d_i}) : K]$, there are r conjugacy classes $\mathbf{C}$ so the Modular Tower for $(G, \mathbf{C}, p)$ has a projective system of K points.

PROBLEM 6.7. Suppose given (G, p) with G a p-perfect group. Is there a $\mathbf{C}$ (consisting of p' conjugacy classes) for which the Modular Tower for $(G, \mathbf{C}, p)$ has a projective system of $\mathbb{Q}$ components?

When $r = 4$ these gcomplete criteria fail to provide projective systems of $\bar{M}_4$ orbits over $\mathbb{Q}$. As an example problem consider this.

PROBLEM 6.8. Does the Modular Tower for $(A_5, \mathbf{C}_{3^4}, p = 2)$ have a projective system of $\mathbb{Q}$ (absolutely irreducible) components?

7. Remaining topics from 3rd RIMS lectures in October, 2001

Again, consider $r = 4$, so Modular Towers are upper half plane quotients. Modular Towers has practical formulas for analyzing how $G_{\mathbb{Q}}$ acts on projective systems of tangential base points attached to cusps. The talk concentration included these two topics which will appear in an expanded version of this paper.

(7.1a) Geometrically interpreting the **sh**-incidence matrix attached to a level.

(7.1b) The Ihara-Matsumoto-Wewers ([**BFr02**, App. D.3] and [**We01**] modifying [**IM95**]) formulas for $G_{\mathbb{Q}}$ acting on the fiber over tangential base points attached to Harbater-Mumford cusps (§1.2).

Some cusps so stand out, that we recognize their presence at all levels of some Modular Towers, even associated with specific irreducible components and having in their $\bar{M}_4$ orbits other related cusps. [**BFr02**, Prop. 7.11] describes a natural pairing on cusps attached to Harbater-Mumford (H-M) representatives and near H-M representatives at *all* levels of specific Modular Towers, when $p = 2$. An H-M rep. has a Nielsen class representative of form $(g_1, g_1^{-1}, g_2, g_2^{-1})$ (when $r = 4$). A near H-M rep. at level $k+1$ is a Nielsen class element that defines a real point though it is not an H-M rep. From the formulas of [**BFr02**, §6], a near H-M rep. has a specific form related to that of its corresponding H-M rep.

This applies to Schur quotients R_{D_k} at level k when $G_0 = A_5$. This is a case when the Schur quotient has an antecedent (§ 4.1 and §4.3.1). Since R_{D_k} has a nontrivial center, although the Hurwitz spaces $\mathcal{H}(R_{D_k}, \mathbf{C})$ and $\mathcal{H}(G_{k+1}, \mathbf{C})$ are the same complex analytic spaces, the former is not a fine moduli space. We therefore expect there are fields K and points $\boldsymbol{p} \in \mathcal{H}(R_k, \mathbf{C})(K)$ with no representing cover over K. Indeed, when $K = \mathbb{R}$, the H-M reps. give real points with representing covers over $\mathbb{R}$, while near H-M reps. give real points for which the corresponding covers cannot have definition field $\mathbb{R}$ [**BFr02**, Prop. 6.8]. In a later paper we will produce the p-adic version of this result. This applies to our final topic.

[**BFr02**, App. D] discusses the Hurwitz space viewpoint of Serre's Open Image Theorem, especially how one piece of Serre's Theorem extends to considering projective systems of Harbater-Mumford components. While speculative, this cusp approach goes around difficulties that appear in Serre's approach. Specifically: It avoids a generic abelian variety hypothesis (death to most sensible applications), and the cusp type replaces impossibly detailed analysis of many types of p-adic Lie Algebras. Serre extensively used a p-Frattini property of the monodromy groups of modular curves over the j-line. A Galois-Ihara problem arises when we inspect if this generalizes to each Modular Tower. The appearance of *Eisenstein series* and *theta nulls* brings us to the present research line [**BFr02**, App. B].

References

[BFr02] P. Bailey and M. Fried, *Hurwitz monodromy, spin separation and higher levels of a Modular Tower*, in Proceedings of Symposia in Pure Mathematics **70** (2002) editors M. Fried and Y. Ihara, 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16-27, 1999 MSRI, 79–221.

[Ben91] D.J. Benson, *I: Basic representation theory of finite groups and associative algebras*, Cambridge Studies in advanced math., vol. 30, Cambridge U. Press, Cambridge, 1991.

[Ch41] C. Chabauty, *Sur les points rationnels des courbes algébriques*, C.R. Acad. Sci. Paris 212 (1941), 882–885.

[Co85] R. Coleman, *Effective Chabauty*, Duke Math. J **52** (1985), 765–770.

[Deb99] P. Dèbes, *Galois covers with prescribed fibers: the Beckmann-Black problem*, Ann. Scuola Norm. Sup. Pisa, Cl. Sci. (4), **28**, (1999), 273–286.

[DDes01] P. Dèbes et B. Deschamps, *Corps ψ-libres et théorie inverse de Galois infinie*, preprint as of October, 2001.

[DDE00] P. Dèbes, J.-C. Douai and M. Emsalem, *Familles de Hurwitz et Cohomlogies non Abélienne*, Annales de l'institut Fourier, **50** (2000), 113–149.

[De66] V. A. Demjanenko, Rational points of a class of algebraic curves (in Russian), Izv. Akad. Nauk, SSSR 30 (1966), 1373–1396.

[Fal83] G. Faltings, *Endlichkeitssätze über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[FJ86] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, vol. 11, Springer Verlag, Heidelberg, 1986.

[FK97] M.D. Fried and Y. Kopeliovic, *Applying Modular Towers to the inverse Galois problem*, Geometric Galois Actions II Dessins d'Enfants, Mapping Class Groups and Moduli, vol. 243, Cambridge U. Press, 1997, London Math. Soc. Lecture Notes, pp. 172–197.

[Fri78] M. Fried, *Galois groups and Complex Multiplication*, Trans.A.M.S. **235** (1978) 141–162.

[FV91] M.D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Annalen **290** (1991), 771–800.

[FrV92] M.D. Fried and H. Völklein, *The embedding problem over an Hilbertian-PAC field*, Annals of Math **135** (1992), 469–481.

[Fri95] M. Fried, *Introduction to Modular Towers: Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 111–171.

[IM95] Y. Ihara and M. Matsumoto, *On Galois actions on profinite completions of braid groups*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, 173–200.

[Ma69] Y. Manin, The p-torsion of elliptic curves in uniformly bounded Izv. Akad. Nauk SSR (1969), 459–465 (=Math. USSR Izv. 3 (1969), 433–438.

[Se01] D. Semmen, *Modular representations attached to Hurwitz spaces*, thesis at UC Irvine, June 2002.

[Ser68] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, 1st ed., McGill University Lecture Notes, Benjamin, New York • Amsterdam, 1968, in collaboration with Willem Kuyk and John Labute.

[Se97] J.P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd Edition, Translated and edited by Martin Brown from notes of Michel Waldschmidt, Aspects of Math. Vieweg, 1997.

[We01] S. Wewers, *Field of moduli and field of definition of Galois covers*, in Proceedings of Symposia in Pure Mathematics **70** (2002) editors M. Fried and Y. Ihara, 1999 von Neumann Conference on Arithmetic Fundamental Groups and Noncommutative Algebra, August 16-27, 1999 MSRI, 222–246.

UC Irvine, Irvine, CA 92697, USA
E-mail address: mfried@math.uci.edu