Séminaires & Congrès
13, 2006, p. 343–366

THE GROUP THEORY BEHIND MODULAR TOWERS

by

Darren Semmen

Abstract. — Geometric considerations identify what properties we desire of the canonical sequence of finite groups that are used to define modular towers. For instance, we need the groups to have trivial center for the Hurwitz spaces in the modular tower to be fine moduli spaces. The Frattini series, constructed inductively, provides our sequence: each group is the domain of a canonical epimorphism, which has elementary abelian p-group kernel, having the previous group as its range. Besides satisfying the desired properties, this choice is readily analyzable with modular representation theory.

Each epimorphism between two groups induces (covariantly) a morphism between the corresponding Hurwitz spaces. Factoring the group epimorphism into intermediate irreducible epimorphisms simplifies determining how the Hurwitz-space map ramifies and when connected components have empty preimage. Only intermediate epimorphisms that have central kernel of order p matter for this. The most important such epimorphisms are those through which the universal central p-Frattini cover factors; the elementary abelian p-Schur multiplier classifies these.

This paper, the second of three in this volume on the topic of modular towers, reviews for arithmetic-geometers the relevant group theory, culminating with the current knowledge of the p-Schur multipliers of our sequence of groups.

2000 ***Mathematics Subject Classification.*** — Primary 20C20; Secondary 14G32, 20C05, 20D25, 20E18, 20E22, 20F69, 20J05, 20J06.
Key words and phrases. — Modular tower, universal cover, Frattini, modular representation, Schur multiplier.

Many thanks to CIRM for their hospitality, to Professors Daniel Bertrand and Pierre Dèbes for organizing this conference, to the NSA for travel support, and to Professors David Harbater and Michael Singer for arranging the support from the NSA.

***Résumé* (Théorie des groupes pour les tours modulaires).** — Des considérations géométriques permettent d'identifier quelles propriétés nous souhaitons pour la suite canonique de groupes finis qui sont utilisés pour définir les tours modulaires. Par exemple, les groupes doivent être de centre trivial pour que les espaces de Hurwitz constituant la tour modulaire soient des espaces de modules fins. Notre suite est donnée par la série de Frattini, qui est définie inductivement : chaque groupe est le domaine d'un épimorphisme canonique, lequel a comme noyau un p-groupe abélien élémentaire, et le groupe précédent comme image. En plus de satisfaire les propriétés désirées, ce choix s'interprète naturellement en termes de théorie des représentations modulaires.

Chaque épimorphisme entre deux groupes induit (de manière covariante) un morphisme entre les espaces de Hurwitz correspondants. La factorisation de l'épimorphisme de groupes en épimorphismes irréductibles intermédiaires permet de déterminer plus simplement comment l'application entre espaces de Hurwitz se ramifie et quand les composantes connexes ont des images inverses vides. Pour cela, seuls comptent les épimorphismes intermédiaires qui ont un noyau central d'ordre p. Les plus importants de ces épimorphismes sont ceux à travers lesquels le p-revêtement universel de Frattini se factorise ; ils sont classifiés par le p-groupe élémentaire abélien des multiplicateurs de Schur.

Cet article, le deuxième de trois sur les tours modulaires dans ce volume, revient, à l'intention des arithméticiens-géomètres, sur la théorie des groupes nécessaire à cette théorie, pour aboutir à l'état actuel des connaissances sur les p-groupes de multiplicateurs de Schur de notre suite de groupes.

Contents

1. Introduction

This survey broadly divides into two parts. The first part (§2 and §3) recaps Dèbes' presentation [**Dèb**] of the universal p-Frattini cover and of modular towers. In particular, §2 illustrates difficulties arising from the use of Zorn's lemma in the "top-down" construction of the universal p-Frattini cover, while §3 concentrates on the consequences which the properties of the finite groups G_n have on the modular towers they define. The second part constructs the groups G_n and derives their properties from the "bottom-up", using modular representation theory and, especially, the categorical equivalence of Gruenberg and Roggenkamp [**Gru76**, §10.5]. The appendix displays the functors for this categorical equivalence, since it doesn't seem to be well-known.

Despite relatively few explicit citations herein, many of the results surveyed have been comprehensively catalogued (and produced) by Fried in his work on modular towers. His series of papers on the subject are a primary source: [**Fri95**], [**FK97**], [**Fri02**], [**BF02**], [**Fri**], and [**FS**]. I have tried to introduce required results from modular representation theory steadily but gently; for a general reference, I recommend Benson's text [**Ben98a**].

Before proceeding, recall some elementary categorical definitions.

Definition 1.1. — In any category, for any objects X and Y, a morphism $\phi \in \mathrm{Hom}\,(X,Y)$ is **epic** iff, for all objects Z and for all morphisms $\psi_1, \psi_2 \in \mathrm{Hom}\,(Y,Z)$, if $\psi_1 \circ \phi = \psi_2 \circ \phi$ then $\psi_1 = \psi_2$.

This purely categorical definition is synonymous with "surjective" in the categories of abstract groups, profinite groups, and modules.

Definition 1.2. — An object P of a category $\mathcal{C}$ is **projective** iff, for any objects X and Y of $\mathcal{C}$, any morphism $\psi \in \mathrm{Hom}\,(P,Y)$, and any epic morphism $\phi \in \mathrm{Hom}\,(X,Y)$, there exists a morphism $\pi \in \mathrm{Hom}\,(P,X)$ such that $\phi \circ \pi = \psi$, as illustrated in the following commutative diagram:

$$\begin{array}{ccc} P & \xrightarrow{\forall\psi} & Y \\ \Big\downarrow{\scriptstyle \exists\pi} & & \Vert \\ X & \xrightarrow{\forall\phi} & Y \end{array}$$

An object F of $\mathcal{C}$ is **Frattini** iff every morphism to F is epic, i.e., for any object X of $\mathcal{C}$ and any morphism $\phi \in \mathrm{Hom}\,(X,F)$, ϕ is epic.

Given an object X of a category $\mathcal{C}$, a cover of X is defined to be an epic morphism in $\mathrm{Hom}\,(Y,X)$ for some object Y. The collection of covers of X comprise the class of objects of a category whose morphisms are as follows — given two covers, $\phi_1 \in \mathrm{Hom}\,(Y,X)$ and $\phi_2 \in \mathrm{Hom}\,(Z,X)$, $\mathrm{Hom}\,(\phi_1,\phi_2)$ is defined to be the set of morphisms ψ in $\mathrm{Hom}\,(Y,Z)$ such that $\phi_2 \circ \psi = \phi_1$. We also sometimes consider subcategories where we restrict the covers under consideration, but in these cases the set of morphisms between two objects remains the same as in the full category of covers, i.e., these subcategories are full in the technical sense. In the categories of covers we will consider, epic morphisms will always turn out to be surjective. Hence, equivalences between these categories pass along surjectivity of morphisms.

Conventions. The number p is always a positive prime rational integer, G is always a finite group, and k is always a field with characteristic p. The cyclic group of order

n is C_n, the dihedral group of order $2n$ is D_n, the alternating group on n letters is A_n, and the symmetric group on n letters is S_n. The conjugate gag^{-1} of one element a of G by another element g is denoted by ${}^g a$. The commutator $[g,h]$ of two elements g and h of G is $g^{-1}h^{-1}gh$. All modules are finitely generated left-modules. The ring of p-adic integers is denoted by $\mathbb{Z}_p$, and the field with q elements by $\mathbb{F}_q$.

2. The universal p-Frattini cover

Fix a finite group G and consider the category of covers of G within the category of profinite groups; call this category of covers $\mathcal{C}(G)$. A projective Frattini object in this category is called the **universal Frattini cover** of G, as is its domain, which is given the notation $\tilde{G}$. The first construction of this, due to Cossey, Kegel, and Kovács [**CKK80**, Statement 2.4], used Zorn's lemma: projective profinite groups are precisely those isomorphic to closed subgroups of free profinite groups [**FJ05**, Proposition 22.4.7], so take a minimal closed subgroup mapping onto G in any epimorphism onto G with domain a free profinite group. The kernel of the universal Frattini cover is (pro-)nilpotent by the Frattini Argument from which its name derives. Hence, it is the product of its p-Sylows; being closed subgroups of a projective profinite group, they will have to be projective as well, and projective pro-p groups must be free as pro-p groups [**FJ05**, Proposition 22.7.6].

Now consider ${}_p\tilde{G}$, the quotient of $\tilde{G}$ by the p'-Hall subgroup of the kernel of $\tilde{G} \twoheadrightarrow G$, i.e., the product of all of the s-Sylows of the kernel, where s denotes a rational prime distinct from p. This quotient profinite group is called the **universal p-Frattini cover** of G, as is the natural map to G which it inherits. This map is also characterized by being a projective Frattini object in the full subcategory $\mathcal{C}_{p^\infty}(G)$ of $\mathcal{C}(G)$ whose objects are precisely those objects of $\mathcal{C}(G)$ with kernel a pro-p group. The kernel of the universal p-Frattini cover is a free pro-p group called $\mathbf{ker_0}$.

The easiest example is when G is a p-group; then, ${}_p\tilde{G}$ is a free pro-p group with the same minimal number of (topological) generators as G. As a consequence of Schur-Zassenhaus, if G merely has a normal p-Sylow P, then G is a semi-direct product $P \rtimes H$, where $H \simeq G/P$; we say G is **p-split**. When G is p-split, ${}_p\tilde{G} \simeq \hat{F}_n(p) \rtimes H$, where n is the minimal number of generators of the p-Sylow P of G and $\hat{F}_n(p)$ is the pro-p completion of the free group on n generators. The rank (minimal number of topological generators) of $\ker_0$ is $1 + (n-1)|P|$, by the Schreier formula.

Example 2.1. — The alternating group on four elements is isomorphic to $V_4 \rtimes C_3$, where a given generator g of C_3 acts on the Klein four-group V_4 by cyclically permuting the three non-trivial elements. Two (topological) generators a and b of $\hat{F}_2(2)$ may be chosen so that conjugation by g on $\hat{F}_2(2)$ (in ${}_2\tilde{A}_4 \simeq \hat{F}_2(2) \rtimes C_3$) is given by ${}^g a = b$ and ${}^g b = b^{-1}a^{-1}$. Clearly, a and b generate a discrete, dense, free subgroup F_2 of

$\hat{F}_2(2)$ which is stabilized by C_3. We get the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F_2 & \longrightarrow & F_2 \rtimes C_3 & \longrightarrow & C_3 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \hat{F}_2(2) & \longrightarrow & {}_2\tilde{A}_4 & \longrightarrow & C_3 & \longrightarrow & 1 \end{array}$$

By the Schreier formula, $\ker_0$ has rank 5 and its intersection with F_2 is a free group F_5 of rank 5, normal inside of F_2. There is another commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F_5 & \longrightarrow & F_2 \rtimes C_3 & \longrightarrow & A_4 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \hat{F}_5(2) & \longrightarrow & {}_2\tilde{A}_4 & \longrightarrow & A_4 & \longrightarrow & 1 \end{array}$$

where the vertical maps are dense group monomorphisms.

In general, the approach we've been following so far fails to provide detailed information about the universal p-Frattini cover, the preceding example being a rare counterexample describable by a discrete analogue. Even p-split groups can often not be described this way. One reason to expect this failure is the non-constructiveness of using Zorn's lemma to create the universal cover. Consider two examples illustrating the limitations.

Example 2.2. — Our first example comes from Holt and Plesken [**HP89**]. Embedding A_4 into A_5 leads to an embedding of ${}_2\tilde{A}_4$ into ${}_2\tilde{A}_5$ and the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \hat{F}_5(2) & \longrightarrow & {}_2\tilde{A}_4 & \longrightarrow & A_4 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & \hat{F}_5(2) & \longrightarrow & {}_2\tilde{A}_5 & \longrightarrow & A_5 & \longrightarrow & 1 \end{array}$$

The leftmost vertical map is an isomorphism. However, there is NO group Γ which can fit into a commutative diagram of exact sequences of the following form, where the vertical maps are dense monomorphisms:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F_5 & \longrightarrow & \Gamma & \longrightarrow & A_5 & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \hat{F}_5(2) & \longrightarrow & {}_2\tilde{A}_5 & \longrightarrow & A_5 & \longrightarrow & 1 \end{array}$$

The proof examines the character of the 2-adic Frattini lattice (cf. §7) of $\mathrm{SL}_2(\mathbb{F}_5)$ and is beyond the scope of these limited notes.

Example 2.3. — A result of Dyer and Scott [**DS75**] says that, for any automorphism σ of prime order s acting on a discrete free group F, there is a basis X of F such that one of the following holds for every x in X:

i) $\sigma(x) = x$

ii) x belongs to a subset of X containing exactly s elements which are cyclically permuted by σ

iii) x belongs to a subset $\{x_1, \ldots, x_{s-1}\}$ of X such that $\sigma(x_j) = x_{j+1}$ when $j < s-1$, while $\sigma(x_{s-1}) = x_{s-1}^{-1} \cdots x_1^{-1}$.

As a corollary, the induced action of σ on the free abelian group (and hence $\mathbb{Z}\langle\sigma\rangle$-module) $F/[F,F]$ would force the latter to be a direct sum of copies of the trivial module $\mathbb{Z}$, the group ring $\mathbb{Z}\langle\sigma\rangle$, and the augmentation ideal of the group ring.

Now let $G = \mathbb{F}_8 \rtimes \mathbb{F}_8^*$, where $\mathbb{F}_8$ denotes the additive group of the field, $\mathbb{F}_8^*$ denotes the multiplicative group, and the action of the latter on the former is multiplication. Then, $G \simeq (C_2 \times C_2 \times C_2) \rtimes C_7$, where a generator g of C_7 cyclically permutes the non-trivial elements of the 2-Sylow of G. The universal 2-Frattini cover ${}_2\tilde{G}$ is isomorphic to $\hat{F}_3(2) \rtimes C_7$, but there is no automorphism of order 7 of the discrete free group F_3.

Furthermore, $\ker_0$ will be a free pro-2 group of rank 17. Recall that, for a commutative ring R and a group Γ, an $R\Gamma$-lattice is an $R\Gamma$-module that is free as an R-module. Conjugation by a lift of g in ${}_2\tilde{G}$ produces a natural $\mathbb{Z}_2C_7$-lattice structure on $\ker_0 / \overline{[\ker_0, \ker_0]}$, whose fixed points under the action of C_7 form a sublattice of rank 2. Suppose there was a group Γ that fit into a commutative diagram of exact sequences of the following form, where the vertical maps are dense monomorphisms:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & F_{17} & \longrightarrow & \Gamma & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \ker_0 & \longrightarrow & {}_2\tilde{G} & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

Then $F_{17}/[F_{17}, F_{17}]$ would be a $\mathbb{Z}C_7$-lattice with a dense monomorphism into $\ker_0 / \overline{[\ker_0, \ker_0]}$; the fixed points of the action of C_7 on $F_{17}/[F_{17}, F_{17}]$ would thus form a sublattice of rank 2. However, the result of Dyer-Scott would force the fixed point sublattice to have rank at least 5, a contradiction.

3. Modular towers

A modular tower is a canonical sequence of Hurwitz spaces $\mathcal{H}(G_n, \mathbf{C})^{\mathrm{in}}$ attached to any choice of finite group G and r-tuple of p'-conjugacy classes of G, i.e., conjugacy classes whose elements have order prime to p; the groups G_n are certain canonical quotients of ${}_p\tilde{G}$.

For any group G and r-tuple $\mathbf{C} = (C'_1, \ldots, C'_r)$ of conjugacy classes of G, the inner Nielsen class $\mathrm{Ni}(G, \mathbf{C})^{\mathrm{in}}$ is defined to be the set of equivalence classes of r-tuples $(g_1, \ldots, g_r)$ of G satisfying:

i) $\{g_1, \ldots, g_r\}$ generates G,

ii) $g_1 \cdots g_r = 1$, and

iii) there exists $\sigma \in S_r$ such that, for all i, $g_{(i)\sigma} \in C'_i$;

two r-tuples $(g_1, \dots, g_r)$ and $(g'_1, \dots, g'_r)$ are equivalent iff there exists $h \in G$ such that $({}^h g_1, \dots, {}^h g_r) = (g'_1, \dots, g'_r)$. The space $\mathbb{P}^r(\mathbb{C}) \setminus D_r$ parametrizes subsets of $\mathbb{P}^1(\mathbb{C})$ of cardinality r. The Hurwitz monodromy group $H_r := \pi_1(\mathbb{P}^r(\mathbb{C}) \setminus D_r)$ has generators $q_1, \dots, q_{r-1}$ with a right action on $\mathrm{Ni}\,(G, \mathbf{C})^{\mathrm{in}}$:

$$(g_1, \dots, g_r)q_i = (g_1, \dots, g_{i-1}, g_i g_{i+1} g_i^{-1}, g_i, g_{i+2}, \dots, g_r).$$

This permutation representation of H_r produces an unramified cover $\mathcal{H}\,(G, \mathbf{C})^{\mathrm{in}} \twoheadrightarrow \mathbb{P}^r(\mathbb{C}) \setminus D_r$ with fibre $\mathrm{Ni}\,(G, \mathbf{C})^{\mathrm{in}}$, whose domain is called a Hurwitz space; connected components of the Hurwitz space correspond one-to-one to orbits of the action of H_r on the inner Nielsen class. When G has trivial center (i.e., no non-trivial element of G commutes with all elements of G), this is a fine moduli space for equivalence classes of Galois covers $X \twoheadrightarrow \mathbb{P}^1(\mathbb{C})$ *together* with an identification of the monodromy group with G such that the ramification data is described by an element of $\mathrm{Ni}\,(G, \mathbf{C})^{\mathrm{in}}$ — the equivalence of covers here must be G-equivariant.

Now to the definition of the groups G_n. The Frattini subgroup $\Phi(P)$ of a pro-p group P is equal to $\overline{P^p[P,P]}$, the closure of the subgroup generated by the p-th powers and commutators of elements of P. Iteratively defining $\Phi^{n+1}(P) := \Phi(\Phi^n(P))$ yields the Frattini series, a descending series of closed subgroups of P. The intersection of the members of the Frattini series is trivial since this holds true in any finite p-group. Define iteratively $\ker_{n+1} := \Phi(\ker_n)$, beginning with the kernel $\ker_0$ of the map from ${}_p\tilde{G}$ down to G, and define G_n to be ${}_p\tilde{G}/\ker_n$. Each canonical epimorphism $\varphi_n : G_{n+1} \twoheadrightarrow G_n$ is a projective Frattini object in the full subcategory $\mathcal{C}_{\mathbb{F}_p G}(G)$ of $\mathcal{C}(G)$ whose objects have elementary abelian p-group kernel.

Whenever $H_2 \twoheadrightarrow H_1$ is a group epimorphism with p-group kernel, every p'-conjugacy class of H_1 has a unique lift to a p'-conjugacy class of H_2. Hence (cf. [**Dèb**, Lifting Lemma 1.1]), if $\mathbf{C}$ is an r-tuple of p'-conjugacy classes, there is a canonical modular tower

$$\dots \longrightarrow \mathcal{H}\,(G_{n+1}, \mathbf{C})^{\mathrm{in}} \xrightarrow{\psi_n} \mathcal{H}\,(G_n, \mathbf{C})^{\mathrm{in}} \longrightarrow \dots$$

where the map ψ_n between Hurwitz spaces is induced by applying the epimorphism $\varphi_n : G_{n+1} \twoheadrightarrow G_n$ coordinatewise to the inner Nielsen class $\mathrm{Ni}\,(G_{n+1}, \mathbf{C})^{\mathrm{in}}$.

The property of $G_{n+1} \twoheadrightarrow G_n$ having a p-group kernel allows for the definition of a modular tower. Two other properties of this group epimorphism have convenient consequences for the modular tower. First, if G is p-perfect (i.e., has no non-trivial p-group quotient) and has trivial center then, for all natural numbers n, G_n is also p-perfect and has trivial center (see Proposition 4.8 below); in this case, all of the Hurwitz spaces of the modular tower will be fine moduli spaces.

Second, since the epimorphism is Frattini, only the product-one condition (part (ii) in the definition of the inner Nielsen class) can cause obstruction: a connected component $\mathcal{O}$ of $\mathcal{H}\,(G_n, \mathbf{C})^{\mathrm{in}}$ is called *obstructed* if its preimage under ψ_n is empty. Namely, let $(g_1, \dots, g_r)$ be a representative of an element of the H_r-orbit of $\mathrm{Ni}\,(G_n, \mathbf{C})^{\mathrm{in}}$ corresponding to $\mathcal{O}$ and let $(g'_1, \dots, g'_r)$ be an element of G_{n+1}^r such that, for all i,

$\varphi_n(g_i') = g_i$ and g_i' has order prime to p. Then, the tuple $(g_1', \ldots, g_r')$ will already satisfy conditions (i) and (iii) in the definition of the inner Nielsen class $\mathrm{Ni}\,(G_{n+1}, \mathbf{C})^{\mathrm{in}}$. The lifting invariant $\nu_{n+1}(\mathcal{O})$ (cf [**Dèb**, §1.4]) encapsulates this idea ($\mathcal{O}$ is obstructed iff $1 \notin \nu_{n+1}(\mathcal{O})$) and also provides a means to distinguish components.

Fried and Kopeliovich [**FK97**, Obstruction Lemma 3.2] reduced the determination of obstruction to a sequence of smaller steps. Fix a G_n-composition series of $\ker_n / \ker_{n+1}$. For any two adjacent entries $N_2 \subset N_1$ of the series, there is a canonical cover

$$\Gamma_2 := G_{n+1}/N_2 \twoheadrightarrow \Gamma_1 := G_{n+1}/N_1$$

whose kernel will be a simple $\mathbb{F}_p\Gamma_1$-module (in fact, a simple $\mathbb{F}_pG$-module). The map ψ_n factors into a sequence of irreducible maps

$$\mathcal{H}\,(G_{n+1}, \mathbf{C})^{\mathrm{in}} \to \cdots \to \mathcal{H}\,(\Gamma_2, \mathbf{C})^{\mathrm{in}} \to \mathcal{H}\,(\Gamma_1, \mathbf{C})^{\mathrm{in}} \to \cdots \to \mathcal{H}\,(G_n, \mathbf{C})^{\mathrm{in}}.$$

Note that even if all of the groups G_n have trivial center, many of the intermediate groups will not (see Fact 6.3 below).

***Fact 3.1* ([FK97]).** — *If the kernel of $\Gamma_2 \twoheadrightarrow \Gamma_1$ is in the center of Γ_2, then $\mathcal{H}\,(\Gamma_2, \boldsymbol{C})^{\mathrm{in}} \to \mathcal{H}\,(\Gamma_1, \boldsymbol{C})^{\mathrm{in}}$ is injective. Otherwise, it is surjective.*

Idea of proof. — Use the invariance of the lifting invariant under powers of $q_1 \cdots q_r \in H_r$ and the fact that, for any set of generators $\{g_1, \ldots, g_r\}$ of Γ_1 and any simple $k\Gamma_1$-module S having non-trivial Γ_1-action, S equals the sum of the vector subspaces $(g_i - 1)S$. □

Thus, only intermediate epimorphisms $\Gamma_2 \twoheadrightarrow \Gamma_1$ with central kernel can produce obstruction. These intermediate epimorphisms with central kernel can also influence genus computations through the ramification of the map that ψ_n induces between compactified Hurwitz spaces (cf. [**BF02**, §9.7]). These observations motivated the analysis leading to Fact 6.3. Unfortunately, the simple subquotients lying deep in a composition series of $\ker_n / \ker_{n+1}$ are inaccessible at the moment; fortunately, Weigel has recently observed that the only subquotients that matter for obstruction are those classified by the elementary abelian p-Schur multiplier, i.e., those that can occur at the top of a composition series.

Specifically, Weigel has shown (cf [**Wei05**, Theorem A]) that there is, independent of n, an orientable p-Poincaré duality group Γ of dimension 2 such that the elements of $\mathrm{Ni}\,(G_n, \mathbf{C})^{\mathrm{in}}$ correspond to conjugacy classes of epimorphisms from Γ to G_n. The obstruction to lifting an element of $\mathrm{Ni}\,(G_n, \mathbf{C})^{\mathrm{in}}$ to $\mathrm{Ni}\,(G_{n+1}, \mathbf{C})^{\mathrm{in}}$ thus lies in the elementary abelian p-Schur multiplier of G_n.

4. The p-Frattini module

Modular representation theory is the right context to produce the canonical sequence of finite groups G_n whose projective limit is the universal p-Frattini cover, as this approach is entirely constructive.

Let R be a commutative ring with 1. Every group ring RG has a rank-one trivial simple module, a copy of R on which every element of G acts as the identity; we denote it by $\mathbf{1}_{RG}$, omitting the subscript when the context is obvious. The kernel of the canonical RG-module epimorphism from RG to $\mathbf{1}_{RG}$, sending every element of G to 1, is called the augmentation ideal and is denoted by ω_{RG}. We also omit the subscript on this object when the context is obvious.

For any RG-module M, let $\mathcal{C}_{RG}(M)$ be the category of covers of M (in the category of RG-modules). Let $\mathcal{C}_{RG}(G)$ represent the category of covers $\Gamma \twoheadrightarrow G$ of G (in the category of groups) whose kernels are abelian groups with a specified R-module structure that commutes with conjugation (by elements of Γ); note that these kernels are naturally RG-modules where the action of an element $g \in G$ is conjugation by any element of Γ in the preimage of $\{g\}$. The morphisms in this category are those morphisms of the covers that restrict to RG-module homomorphisms on the kernels.

Fact 4.1 **(Gruenberg-Roggenkamp)**. — *There is an equivalence of categories between $\mathcal{C}_{RG}(G)$ and $\mathcal{C}_{RG}(\omega_{RG})$ under which corresponding objects have isomorphic kernels.*

Note: When R is $\mathbb{Z}$ or $\mathbb{F}_p$, the group structure of the kernel determines its R-module structure. If R is $\hat{\mathbb{Z}}$ (or $\mathbb{Z}_p$) and the kernel is a finitely (topologically) generated R-module, the domain of the cover is naturally a profinite group; conversely, if the domain of the cover is given a profinite group structure, the kernel will inherit a canonical $\hat{\mathbb{Z}}$-module structure. Finally, note that the finite-index subgroups of any finitely (topologically) generated profinite group are closed (cf Nikolov-Segal [**NS03**]), so when R is $\hat{\mathbb{Z}}$ and the kernel is a finitely (topologically) generated R-module, the *group structure* of the domain will determine the topology. Of course, this assumes that G is finite, as was our assumption; the Gruenberg-Roggenkamp equivalence holds without this assumption, but these last comments obviously don't.

Remark 4.2. — Forming the categories $\mathcal{C}_{RG}(G)$ and $\mathcal{C}_{RG}(\omega_{RG})$ is functorial in G. For any homomorphism $\varphi : H \to G$, there is a covariant functor res_φ from $\mathcal{C}_{RG}(G)$ to $\mathcal{C}_{RH}(H)$ given by taking the fibre product with φ. There is a covariant functor res_φ from $\mathcal{C}_{RG}(\omega_{RG})$ to $\mathcal{C}_{RH}(\omega_{RH})$ given by taking the fibre product with the natural RH-module homomorphism $\omega_{RH} \to \omega_{RG}$. These two functors commute with the Gruenberg-Roggenkamp categorical equivalence.

For every finitely generated kG-module M, there exists a projective Frattini object in $\mathcal{C}_{kG}(M)$. The domain of such an object is a projective kG-module denoted by

$\mathbb{P}_{kG}(M)$; the kernel of a projective Frattini object in $\mathcal{C}_{kG}(M)$ is denoted by $\Omega_{kG}M$. The process of assigning such a kernel to a module is called the Heller operator (denoted by Ω_{kG}, of course), and iterations of it are defined inductively[(1)]: $\Omega^{n+1}_{kG}M := \Omega_{kG}(\Omega^n_{kG}M)$.

By the Gruenberg-Roggenkamp categorical equivalence, there is a projective Frattini object in $\mathcal{C}_{\mathbb{F}_pG}(G)$; the domain of this object is denoted by ${}^1_p\tilde{G}$ and is called the **universal elementary abelian p-Frattini cover** of G. The sequence of finite groups used in the definition of a modular tower can be defined inductively from this: ${}^{n+1}_{p}\tilde{G} := {}^1_p\widetilde{\left({}^n_p\tilde{G}\right)}$.

Theorem 4.3. — *For every natural number n, $G_n \simeq {}^n_p\tilde{G}$, and so ${}_p\tilde{G} \simeq \varprojlim {}^n_p\tilde{G}$.*

Proof. — The second isomorphism follows from the first because ${}_p\tilde{G} \simeq \varprojlim G_n$. (By convention, ${}^0_p\tilde{G} = G$.) Note that if $H \twoheadrightarrow G$ is Frattini with p-group kernel, what we call a p-Frattini cover, then ${}_p\tilde{H} \simeq {}_p\tilde{G}$. The first isomorphism will thus be proven by induction once it is shown that $G_1 \simeq {}^1_p\tilde{G}$, but this is true because both groups are the domain of a projective Frattini object in $\mathcal{C}_{\mathbb{F}_pG}(G)$. □

One can specify the isomorphism class of the kernel (the ***p*-Frattini module**) of the universal elementary abelian p-Frattini cover of G precisely in terms of the modular representation theory of G:

***Theorem 4.4* ([Gas54])**. — *The p-Frattini module of G is isomorphic to $\Omega^2_{\mathbb{F}_pG}\mathbf{1}$.*

Proof. — Since projective kG-modules are precisely those isomorphic to a direct summand of a free kG-module, there is a projective $\mathbb{F}_pG$-module N such that $\mathbb{F}_pG \simeq N \oplus \mathbb{P}_{\mathbb{F}_pG}(\mathbf{1})$ and hence $\omega_{\mathbb{F}_pG} \simeq N \oplus \Omega_{\mathbb{F}_pG}\mathbf{1}$. Thus, $\mathbb{P}_{\mathbb{F}_pG}(\omega_{\mathbb{F}_pG}) \simeq N \oplus \mathbb{P}_{\mathbb{F}_pG}(\Omega_{\mathbb{F}_pG}\mathbf{1})$ and the result follows from the equivalence of Gruenberg and Roggenkamp. □

Remark 4.5. — A minor corollary of the theorem is that the p-Frattini module has dimension congruent to 1 modulo the order of the p-Sylow P of G, since $|P|$ must divide the dimension of any projective kG-module (cf. [**Ben98a**, §3.14]).

Projective kG-modules are injective (cf. [**Ben98a**, §1.6]) so, by dimension-shifting,

$$\begin{aligned} \mathrm{H}^2(G, \Omega^2_{\mathbb{F}_pG}\mathbf{1}) &\simeq \mathrm{Ext}^2_{\mathbb{F}_pG}(\mathbf{1}, \Omega^2_{\mathbb{F}_pG}\mathbf{1}) \\ &\simeq \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbf{1}, \Omega^1_{\mathbb{F}_pG}\mathbf{1}) \\ &\simeq \mathrm{Hom}_{\mathbb{F}_pG}(\mathbf{1}, \mathbf{1}) \\ &\simeq \mathbb{F}_p \end{aligned}$$

and there is a unique group (up to isomorphism) providing a non-split extension of G by its p-Frattini module. This must be ${}^1_p\tilde{G}$.

(1) Note that some authors use the *sub*script to denote iterations of the Heller operator.

Recall the concepts of restriction and induction. Fix a subgroup H of G. The restriction $M{\downarrow_{kH}}$ of a kG-module M to kH simply means: regard M as a kH-module via the canonical inclusion of kH in kG. Given a kH-module M, the induced kG-module $M{\uparrow^{kG}}$ is the tensor product $kG \otimes_{kH} M$. Since projective modules are exactly those isomorphic to direct summands of free modules, over a group ring both the restriction and induction of a projective module are projective.

It is easy to determine the number of simple $\mathbb{F}_pG$-modules. The Prüfer group $\widehat{\mathbb{Z}}$ has a natural action on the set of elements of G that have order prime to p: 1 sends each element to its p-th power. The monomorphism of the absolute Galois group $G_{k\cap\overline{\mathbb{F}}_p}$ of $k \cap \overline{\mathbb{F}}_p$ into the absolute Galois group of $\mathbb{F}_p$, followed by the identification of the latter group with $\widehat{\mathbb{Z}}$ that sends the absolute Frobenius to 1, provides a natural action of $G_{k\cap\overline{\mathbb{F}}_p}$ on the set of elements of G that have order prime to p — and hence on the set of p'-conjugacy classes of G. The number of $G_{k\cap\overline{\mathbb{F}}_p}$-orbits in the latter set equals the number of simple kG-modules (cf. [**Ben98a**, §5.3]). Notice the analogy with the Branch Cycle Argument 1.5 in Dèbes' article [**Dèb**].

Example 4.6. — For odd primes p, the modular curve $Y_1(p^{n+1})$ is isomorphic over $\mathbb{Q}$ to the reduced Hurwitz space associated to $D_{p^{n+1}}$ with $r = 4$ and each conjugacy class the set of involutions (cf. [**BF02**, §2.8.2]). Let's see that $D_{p^{n+1}}$ is a universal elementary abelian p-Frattini cover of D_{p^n} when $n \geq 1$.

There are two simple $\mathbb{F}_pD_{p^n}$-modules: the trivial module $\mathbf{1}$ and the sign module Sgn_p, which consists of a copy of $\mathbb{F}_p$ with the involutions of D_{p^n} acting as multiplication by -1 and the other elements acting trivially. Let H be a 2-Sylow of D_{p^n}. By the Nakayama relations (aka Frobenius reciprocity, cf [**Ben98a**, Proposition 3.3.1]), there is an epimorphism from $S{\downarrow_{\mathbb{F}_pH}}{\uparrow^{\mathbb{F}_pD_{p^n}}}$ to S. Since any $\mathbb{F}_pH$-module is projective, $S{\downarrow_{\mathbb{F}_pH}}{\uparrow^{\mathbb{F}_pD_{p^n}}}$ is isomorphic to $\mathbb{P}_{\mathbb{F}_pD_{p^n}}(S)$, because the dimension of $S{\downarrow_{\mathbb{F}_pH}}{\uparrow^{\mathbb{F}_pD_{p^n}}}$ equals the order of a p-Sylow of D_{p^n}. It is straightforward to calculate that $\mathrm{Ext}^1_{\mathbb{F}_pD_{p^n}}(\mathbf{1},\mathbf{1})$ is zero and that $\mathrm{Ext}^1_{\mathbb{F}_pD_{p^n}}(\mathbf{1},\mathrm{Sgn}_p)$ has dimension one, so that $\mathbb{P}_{\mathbb{F}_pD_{p^n}}(\mathrm{Sgn}_p) \simeq \mathbb{P}_{\mathbb{F}_pD_{p^n}}(\Omega_{\mathbb{F}_pD_{p^n}}\mathbf{1})$. Conclude from counting dimensions that the p-Frattini module for D_{p^n} is one-dimensional (in fact, it is Sgn_p); the dihedral groups are a model for the very restricted class of groups for which this happens (see Fact 6.1).

Now note that the natural map $D_{p^{n+1}} \twoheadrightarrow D_{p^n}$ is Frattini and, since its kernel is one-dimensional, must be a universal elementary abelian p-Frattini cover.

Proposition 4.7. — *Let $\varphi : H \twoheadrightarrow G$ be a p-Frattini cover. Then, H is p-perfect iff G is p-perfect.*

Proof. — It is clear that H is not p-perfect if G is not. So, suppose that H has a normal subgroup N such that H/N is a non-trivial p-group. Since φ is Frattini, $\varphi(N) \neq G$ and so $G/\varphi(N)$ is a non-trivial p-group. □

At this point, we can prove the previously referenced property that ensures the Hurwitz spaces in a modular tower are fine moduli spaces.

Proposition 4.8. — *If G is p-perfect and has trivial center then, for all natural numbers n, ${}_p^n\tilde{G}$ has trivial center.*

Proof. — Using induction, it suffices to prove this is true for $n = 1$. A finite group G is p-perfect iff $\mathrm{H}^1(G, \mathbf{1}_{\mathbb{F}_pG}) = 0$. Since $\mathrm{H}^1(G, \mathbf{1}_{\mathbb{F}_pG}) \simeq \mathrm{Ext}^1_{\mathbb{F}_pG}(\mathbf{1}, \mathbf{1})$, $\mathbb{P}_{\mathbb{F}_pG}(\Omega_{\mathbb{F}_pG}\mathbf{1})$ will not have a quotient isomorphic to $\mathbf{1}$. This implies that the p-Frattini module of G has no non-zero element fixed by every element of G, since every simple submodule of a projective $\mathbb{F}_pG$-module is isomorphic to a quotient of the projective module (cf. [**Ben98a**, Theorem 1.6.3]). As G had trivial center, we conclude that ${}_p^1\tilde{G}$ does also. □

Remark 4.9. — Using Facts 6.1 and 6.2, it is straightforward to show that, for any p-Frattini cover $H \twoheadrightarrow G$, ${}_p^1\tilde{H}$ has trivial center if G is p-perfect and has trivial center.

In the sequel, to remove the notational heaviness, ${}_p^n\tilde{G}$ will be denoted by G_n and $\Omega^2_{\mathbb{F}_p{}_p^n\tilde{G}}\mathbf{1}$ by M_n.

5. Restriction to the normalizer of a p-Sylow

There are explicit methods for computing the p-Frattini module of a p-split group (i.e., a group with normal p-Sylow), e.g. through the use of an expansion of Jennings' theorem [**Sem05**]. I omit these here for reasons of brevity, but will show a relationship between the p-Frattini module of the normalizer of a p-Sylow and that of the whole group. We will also see more intricate examples of p-Frattini modules.

Lemma 5.1. — *Let H be a subgroup of G. The pullback of H in the cover ${}_p^1\tilde{G} \twoheadrightarrow G$ is a projective object in $\mathcal{C}_{\mathbb{F}_pH}(H)$. There is a projective $\mathbb{F}_pH$-module N such that $M_0{\downarrow_{\mathbb{F}_pH}} \simeq N \oplus \Omega^2_{\mathbb{F}_pH}\mathbf{1}$.*

Proof. — The pullback of H in the group cover corresponds under the Gruenberg-Roggenkamp equivalence to the pullback of $\omega_{\mathbb{F}_pH}$ in the cover $\mathbb{P}_{\mathbb{F}_pG}(\omega_{\mathbb{F}_pG}) \overset{\varphi}{\twoheadrightarrow} \omega_{\mathbb{F}_pG}$ (cf. Remark 4.2). There is a free $\mathbb{F}_pH$-module N' such that $\omega_{\mathbb{F}_pG}{\downarrow_{\mathbb{F}_pH}} \simeq N' \oplus \omega_{\mathbb{F}_pH}$. Since N' is projective, it splits in the cover φ (regarded as an $\mathbb{F}_pH$-module homomorphism), and so $\mathbb{P}_{\mathbb{F}_pG}(\omega_{\mathbb{F}_pG}){\downarrow_{\mathbb{F}_pH}}$ is a direct sum of N' and some projective cover of $\omega_{\mathbb{F}_pH}$: this latter projective cover corresponds to the pullback of H. The final statement follows from the decomposition of this projective cover into the direct sum of a projective module N and $\mathbb{P}_{\mathbb{F}_pH}(\omega_{\mathbb{F}_pH})$. □

Remember that a module is indecomposable iff it has no non-trivial direct sum decomposition. It is straightforward to see that a kG-module M is indecomposable and non-projective iff $\Omega_{kG}M$ is. Hence, the p-Frattini module of G is indecomposable and non-projective when p divides the order of G.

Together, the next lemma and the fact following it show a dichotomy between level 0 and the higher levels. The notation $N_G(H)$ denotes the subgroup of elements of G that normalize a given subgroup H of G.

Lemma 5.2. — *Let P be a p-Sylow of G. Then, M_0 is isomorphic to a direct summand of $\left(\Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}\right)\uparrow^{\mathbb{F}_p G}$.*

Proof. — Every $\mathbb{F}_pG$-module M is a direct summand of $M{\downarrow_{\mathbb{F}_p N_G(P)}}\uparrow^{\mathbb{F}_p G}$ by mapping $m \in M$ to the element

$$\frac{1}{(G : N_G(P))} \sum_{gN_G(P)\subseteq G} g \otimes g^{-1}m$$

of $\mathbb{F}_pG \otimes_{\mathbb{F}_p N_G(P)} M$; the number $(G : N_G(P))$ is the index of $N_G(P)$ in G, i.e., $|G|/|N_G(P)|$. Now, by Lemma 5.1, $M_0{\downarrow_{\mathbb{F}_p N_G(P)}}\uparrow^{\mathbb{F}_p G}$ is isomorphic to a direct sum of $\left(\Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}\right)\uparrow^{\mathbb{F}_p G}$ and some projective $\mathbb{F}_pG$-module. Since M_0 is indecomposable and non-projective, it must be a direct summand of $\left(\Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}\right)\uparrow^{\mathbb{F}_p G}$. □

Those versed in Green's correspondence will note that it commutes with the Heller operator, and recognize the previous lemma as a special case.

***Fact 5.3* ([Sem])**. — *Let $n \geq 1$. Regard M_{n-1} as a subgroup of G_n. Let H be any subgroup of G_n containing M_{n-1}. Then $M_n \downarrow_{\mathbb{F}_p H}$ is isomorphic to the p-Frattini module of H. In particular, this holds when H is the normalizer of a p-Sylow of G_n.*

The next three examples consider A_5 for the three rational primes dividing its order. There are systematic ways of computing its p-Frattini module, using its isomorphisms with $\mathrm{SL}_2(\mathbb{F}_4)$ and $\mathrm{PSL}_2(\mathbb{F}_5)$ or, perhaps, using the theory of Specht modules; for example, Weigel [**Wei**, §3] has computed the isomorphism class of the ℓ-Frattini module of $\mathrm{PSL}_2(\mathbb{F}_q)$ except when q is divisible by, but not equal to, ℓ — in the latter case, he has still determined the dimension of the module. Here I will keep the computation and notation elementary (and hence ad hoc).

Recall that, for every finite group G with a split BN-pair of characteristic p (and in particular for a Chevalley group over a finite field of characteristic p), there is a projective simple kG-module called the Steinberg module. When G is $\mathrm{PSL}_2(\mathbb{F}_q)$ or $\mathrm{SL}_2(\mathbb{F}_q)$, this is the quotient of a permutation module by the one-dimensional submodule of elements fixed by G, the G-set defining the permutation module being the projective line $\mathbb{P}^1(\mathbb{F}_q)$ with the natural action of G.

Example 5.4. — Let $p = 5$. There are three isomorphism classes of simple $\mathbb{F}_5A_5$-modules: $\mathbf{1}$, the Steinberg module St_5 (via the isomorphism of A_5 with $\mathrm{PSL}_2(\mathbb{F}_5)$), and a three-dimensional module W (the adjoint representation of $\mathrm{PSL}_2(\mathbb{F}_5)$). The latter is a subquotient of a permutation module: the A_5-set defining $\mathbf{1}_{\mathbb{F}_5 A_4}\!\uparrow^{\mathbb{F}_5 A_5}$ is $\{1,2,3,4,5\}$ with the usual action of A_5. There is a homomorphism φ from $\mathbf{1}_{\mathbb{F}_5 A_4}\!\uparrow^{\mathbb{F}_5 A_5}$ to $\mathbf{1}$ given by taking an element of the former module to the sum of its coefficients (with respect to the permutation basis just described); the simple module W is the quotient of $\ker(\varphi)$ by the one-dimensional submodule of elements fixed by A_5.

The normalizer of the 5-Sylow of A_5 is isomorphic to D_5 and its 5-Frattini module is the sign module Sgn_5 of Example 4.6. The induced module $\mathrm{Sgn}_5\!\uparrow^{\mathbb{F}_5 A_5}$ is six-dimensional, so, by Remark 4.5, M_0 can be either one-dimensional (and hence $\mathbf{1}$) or the entire induced module; the former can't happen because $M_0\!\downarrow_{\mathbb{F}_5 D_5}\supseteq \mathrm{Sgn}_5$, by Lemma 5.1. (Fact 6.1 also shows that M_0 cannot be one-dimensional in this case.) A simple use of the Nakayama relations shows that M_0 has neither a submodule nor a quotient isomorphic to $\mathbf{1}$. Therefore, M_0 has one simple submodule, a copy of W, and its quotient by this submodule is also isomorphic to W.

Example 5.5. — Let $p = 3$. There are three isomorphism classes of simple $\mathbb{F}_3 A_5$-modules: $\mathbf{1}$, a four-dimensional module S, and a six-dimensional module T. The normalizer of the 5-Sylow of A_5 is isomorphic to D_5 and T is isomorphic to $N\!\uparrow^{\mathbb{F}_3 A_5}$, where N is a one-dimensional $\mathbb{F}_3 D_5$-module on which the involutions of D_5 act as multiplication by -1 and the other elements of D_5 act trivially. The A_5-set defining the permutation module $\mathbf{1}_{\mathbb{F}_3 A_4}\!\uparrow^{\mathbb{F}_3 A_5}$ is $\{1,2,3,4,5\}$ with the usual action of A_5 — S is isomorphic to the quotient of this module by the one-dimensional submodule of elements fixed by A_5.

The normalizer of the 3-Sylow of A_5 is isomorphic to D_3 and its 3-Frattini module is the sign module Sgn_3 of Example 4.6. The induced module $\mathrm{Sgn}_3\!\uparrow^{\mathbb{F}_3 A_5}$ is ten-dimensional and is isomorphic to $S \oplus T$, as can be seen using the Nakayama relations together with Mackey decomposition (cf. [**Ben98a**, Theorem 3.3.4]). Since T is projective, M_0 must be isomorphic to S.

Example 5.6. — Let $p = 2$. There are three isomorphism classes of simple $\mathbb{F}_2 A_5$-modules: $\mathbf{1}$, a four-dimensional simple module U, and the Steinberg module St_4 (via the isomorphism of A_5 with $\mathrm{SL}_2(\mathbb{F}_4)$). The simple module U is just the natural module for $\mathrm{SL}_2(\mathbb{F}_4)$, a copy of $\mathbb{F}_4^2$, but regarded as a vector space over $\mathbb{F}_2$.

The methods presented in this paper are insufficient to derive the 2-Frattini module of A_5 but can still describe it. The normalizer of the 2-Sylow of A_5 is isomorphic to A_4, a 2-split group. As noted in Example 2.1, the kernel of the universal 2-Frattini cover of A_4 will have rank 5, and so the 2-Frattini module will have dimension 5. The 2-Frattini module M_0 for A_5 also has dimension 5 and so $M_0\!\downarrow_{\mathbb{F}_2 A_4}\simeq \Omega^2_{\mathbb{F}_2 A_4}\mathbf{1}$; on the other hand, inducing $\Omega^2_{\mathbb{F}_2 A_4}\mathbf{1}$ up to A_5 produces a module with dimension 25. The 2-Frattini module M_0 can also be (spuriously) described as a quotient of a permutation module by $\mathbf{1}$: the A_5-set defining the permutation module $\mathbf{1}_{\mathbb{F}_2 D_5}\!\uparrow^{\mathbb{F}_2 A_5}$ is the set of 5-Sylows of A_5 acted on by conjugation — M_0 is isomorphic to the quotient of this module by the one-dimensional submodule of elements fixed by A_5. It turns out that

M_0 has one simple submodule, a copy of U, and its quotient by this submodule is isomorphic to $\mathbf{1}$. See [**Fri95**, §II.E] for the details of the derivation of this Frattini module.

Finally, it should be noted that a cocycle in $\mathrm{H}^2(G, M_0)$ defining the universal elementary abelian p-Frattini cover can be computed using the Eckmann-Shapiro lemma ([**Ben98a**, Corollary 2.8.4]):

$$\mathbb{F}_p \simeq \mathrm{H}^2(N_G(P), \Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}) \xrightarrow{\simeq} \mathrm{H}^2(G, \left(\Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}\right)\uparrow^{\mathbb{F}_p G})$$

via the exterior trace map. The latter cohomology group is isomorphic to $\mathrm{H}^2(G, M_0)$, since $\left(\Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1}\right)\uparrow^{\mathbb{F}_p G}$ is isomorphic to the direct sum of M_0 and some projective $\mathbb{F}_p G$-module. Thus, some cocycle in the image (under the exterior trace map) of a generator of $\mathrm{H}^2(N_G(P), \Omega^2_{\mathbb{F}_p N_G(P)}\mathbf{1})$ will take values in M_0. When the restriction of M_0 to the normalizer of a p-Sylow is isomorphic to the p-Frattini module of this normalizer (as in Example 5.6), and in particular for computing cocycles in $\mathrm{H}^2(G_n, M_n)$ when $n \geq 1$, the computation can be done directly with the transfer map instead.

6. Asymptotics of the p-Frattini modules M_n

The first recursive formula was hinted at in Fact 5.3. If M_n is regarded as a p-group, then its universal p-Frattini cover is a free pro-p group of rank equal to the dimension of M_n. The Schreier formula takes the form:

$$\dim_{\mathbb{F}_p}(M_{n+1}) = 1 + |M_n| \left[\dim_{\mathbb{F}_p}(M_n) - 1\right].$$

Since $|M_n|$ is equal to p raised to the power of the dimension of M_n, this forces the dimension of M_n to rise very rapidly with n via recursive exponentiation, provided $\dim_{\mathbb{F}_p}(M_0) > 1$; but if $\dim_{\mathbb{F}_p}(M_0)$ is 0 or 1 then $\dim_{\mathbb{F}_p}(M_n)$ is the same for all natural numbers n. Of course, $\dim_{\mathbb{F}_p}(M_0) = 0$ iff p does not divide the order of G, while Griess and Schmid ([**GS78**, Theorem 3]) determined precisely the rare circumstance when $\dim_{\mathbb{F}_p}(M_0) = 1$. For the maximal normal p'-subgroup (i.e., having order prime to p) of G, group theorists use the notation $O_{p'}(G)$.

***Fact 6.1* ([GS78]).** — *The p-Sylow of $G/O_{p'}(G)$ is non-trivial, cyclic, and normal iff* $\dim_{\mathbb{F}_p}(M_0) = 1$.

The dihedral groups (Example 4.6) provide the natural example of Fact 6.1.

The group G_n does not necessarily act faithfully on the module M_n; Griess and Schmid also determined the kernel of this action, the set $\mathrm{Cen}_{G_n}(M_n)$ of elements of G_n that centralize M_n. Let $\phi : G \twoheadrightarrow G/O_{p'}(G)$ denote the natural quotient and let H be the maximal normal p-subgroup of $G/O_{p'}(G)$; the subgroup $O_{p'p}(G)$ of G is defined to be $\phi^{-1}(H)$.

Fact 6.2 **([GS78])**. — $\mathrm{Cen}_{G_n}(M_n) = \begin{cases} O_{p'p}(G_n) & \textit{if } \dim_{\mathbb{F}_p}(M_n) = 1 \\ O_{p'}(G_n) & \textit{if } \dim_{\mathbb{F}_p}(M_n) \neq 1 \end{cases}$

In some sense, we can reduce to the case where $O_{p'}(G) = 1$. Let $H = G/O_{p'}(G)$. Then G_n is isomorphic to the fibre product over H of ${}_p^n\tilde{H}$ and G; the cover $G_n \twoheadrightarrow G$ induces an isomorphism $O_{p'}(G_n) \simeq O_{p'}(G)$ for all n.

The final result here is an asymptotic result on the composition series. Every normal p-subgroup of a finite group Γ acts trivially on every simple $k\Gamma$-module; hence, the simple kG_n-modules are naturally simple kG-modules. The number of times a simple module S appears as a subquotient in a given composition series of a kG_n-module M is an invariant of M denoted by $\#_S(M)$; the density $\varrho_S(M)$ of S in M is defined to be $\#_S(M)/\dim_k(M)$.

Fact 6.3 **([Sem])**. — *If* $\dim_{\mathbb{F}_p}(M_0) > 1$ *then, for any simple* $\mathbb{F}_pG$*-module* S, $\lim_{n\to\infty} \varrho_S(M_n) = \varrho_S(\mathbb{F}_pG/O_{p'}(G))$. *In particular, for large enough* n*, every simple* $\mathbb{F}_pG/O_{p'}(G)$*-module is a composition factor of* M_n.

The proof of Fact 6.3 provides precise recursive formulae for $\#_S(M_n)$.

7. The p-Schur multiplier

Recall that an element g of a group Γ is central iff g commutes with all elements of Γ. Every finite group G has a universal central p-Frattini cover, i.e., a projective Frattini object in the full subcategory of $\mathcal{C}_{\mathbb{Z}_pG}(G)$ consisting of objects whose kernels are central. A finite group G is p-perfect iff its universal central p-Frattini cover is finite (cf. [**Sem**]); in this case, the kernel of the universal central p-Frattini cover is what we call the p-Schur multiplier.

Even when G is not p-perfect, it will possess a finite universal elementary abelian central p-Frattini cover, which can be obtained from a quotient of a universal elementary abelian p-Frattini cover of G. Analogously, the kernel is called the elementary abelian p-Schur multiplier and is computed by modular representation theory to be $\mathrm{H}_2(G, \mathbf{1}_{\mathbb{F}_pG})$. Use dimension shifting or inspection of the p-Frattini module to see that $\mathrm{H}_2(G, \mathbf{1}_{\mathbb{F}_pG})$ is isomorphic to $(\Omega^2_{\mathbb{F}_pG}\mathbf{1})/(\omega_{\mathbb{F}_pG}\Omega^2_{\mathbb{F}_pG}\mathbf{1})$.

Whenever N is a normal subgroup of a group G and M is an RG-module (R being a commutative ring), the action of G on N by conjugation induces an $R(G/N)$-module structure on $\mathrm{H}_n(N, M{\downarrow}_{RN})$ (cf. [**Bro94**, III.8.2]). The maximal quotient on which G/N acts trivially is denoted by $\mathrm{H}_n(N, M{\downarrow}_{RN})_{G/N}$.

Proposition 7.1. — *For every natural number* n,

$$\mathrm{H}_2(G_{n+1}, \mathbf{1}_{\mathbb{F}_pG_{n+1}}) \simeq \mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_pM_n})_{G_n}.$$

Proof. — This reflects Fact 5.3, i.e., that $\left(\Omega^2_{\mathbb{F}_pG_{n+1}}\mathbf{1}\right)\downarrow_{\mathbb{F}_pM_n}\simeq \Omega^2_{\mathbb{F}_pM_n}\mathbf{1}$. The action of G_n on $(\Omega^2_{\mathbb{F}_pM_n}\mathbf{1})/(\omega_{\mathbb{F}_pM_n}\Omega^2_{\mathbb{F}_pM_n}\mathbf{1})$ is induced from the action of G_{n+1} on $\Omega^2_{\mathbb{F}_pG_{n+1}}\mathbf{1}$ and, hence,

$$\begin{aligned}\mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})_{G_n} &\simeq (\Omega^2_{\mathbb{F}_pG_{n+1}}\mathbf{1})/(\omega_{\mathbb{F}_pG_{n+1}}\Omega^2_{\mathbb{F}_pG_{n+1}}\mathbf{1})\\ &\simeq \mathrm{H}_2(G_{n+1},\mathbf{1}_{\mathbb{F}_pG_{n+1}}).\quad \square\end{aligned}$$

Therefore, computing the elementary abelian p-Schur multiplier of G_{n+1} reduces to computing the $\mathbb{F}_pG_n$-module structure of $\mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})$; note that $\mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})\downarrow_{\mathbb{F}_pM_n}$ is the head (i.e., maximal semi-simple quotient) of $M_{n+1}\downarrow_{\mathbb{F}_pM_n}$ and so some quotient of $\mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})$ is the head of M_{n+1}. Every group ring $k\Gamma$ has a Hopf algebra structure, which provides a canonical way to extend the action of $k\Gamma$ to the tensor product (over k) of two $k\Gamma$-modules: let the group elements act diagonally and then extend linearly; this also provides an action of $k\Gamma$ on the exterior product. The universal coefficient theorem (a special case of Künneth's formula) yields the following exact sequence of $\mathbb{F}_pG_n$-modules:

$$0\longrightarrow \wedge^2 M_n\longrightarrow \mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})\longrightarrow M_n\longrightarrow 0. \tag{1}$$

For example, see the discussion preceding Theorem V.6.6 of Brown's text [**Bro94**]. This exact sequence can also be derived using Jennings' theorem, and an elementary presentation of this sequence will come after Fact 7.3.

The quotient module isomorphic to M_n is best described as the "antecedent" quotient of M_{n+1} coming from multiplication by p in the p-adic Frattini lattice $\Omega^2_{\mathbb{Z}_pG_n}\mathbf{1}_{\mathbb{Z}_pG_n}$. The finite group G_n possesses a universal abelian p-Frattini cover, i.e., a projective Frattini object $\vec{G}_n\twoheadrightarrow G_n$ in $\mathcal{C}_{\mathbb{Z}_pG_n}(G_n)$. The kernel of this cover is a $\mathbb{Z}_pG_n$-lattice (i.e., a $\mathbb{Z}_pG_n$-module that is a free $\mathbb{Z}_p$-module) which I shall denote by L_n. Notice that $M_n\simeq L_n/pL_n\simeq pL_n/p^2L_n$ as $\mathbb{F}_pG_n$-modules. Consider the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc}0&\longrightarrow&pL_n/p^2L_n&\longrightarrow&\vec{G}_n/p^2L_n&\longrightarrow&G_{n+1}&\longrightarrow&0\\ &&\uparrow&&\uparrow&&\|&&\\ 0&\longrightarrow&M_{n+1}&\longrightarrow&G_{n+2}&\longrightarrow&G_{n+1}&\longrightarrow&0\end{array}$$

The up-arrows come from the defining property of the bottom row and must be group epimorphisms because the surjection in the top row is a Frattini cover. The commutative diagram forces the epimorphism $M_{n+1}\twoheadrightarrow pL_n/p^2L_n$ to be one of $\mathbb{F}_pG_{n+1}$-modules; since the subgroup M_n of G_{n+1} acts trivially on pL_n/p^2L_n, this epimorphism factors through $\mathrm{H}_2(M_n,\mathbf{1}_{\mathbb{F}_pM_n})$.

For a finite group G, the dual $\mathrm{H}_2(G,\mathbf{1}_{\mathbb{F}_pG})\widehat{\ }$ is naturally isomorphic to $\mathrm{H}^2(G,\mathbf{1}_{\mathbb{F}_pG})$, which parametrizes equivalence classes of simple central p-extensions of G, group extensions of G having central kernel of order p:

$$0\longrightarrow \mathbf{1}_{\mathbb{F}_pG}\longrightarrow \mathrm{S}\longrightarrow G\longrightarrow 1;$$

two such extensions are equivalent if there is a group isomorphism between the middle terms that induces the identity maps between the other terms of the extensions. A simple central p-extension of G_{n+1} is called *antecedent* if the element of $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})\hat{}$ defining the extension factors through the antecedent quotient (as a map on $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$). Note that $\mathrm{H}^1(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$ and the dual $M_n\hat{}$ are isomorphic as $\mathbb{F}_p G_n$-modules; the linear map $\mathrm{H}^1(M_n, \mathbf{1}_{\mathbb{F}_p M_n}) \to \mathrm{H}^2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$ whose image consists of the antecedent elements is known as the Bockstein (cf. [**Ben98b**, §4.3]).

Proposition 7.2. — *A simple central p-extension $\varphi : H \twoheadrightarrow G_{n+1}$ is antecedent iff $\varphi^{-1}(M_n)$ is abelian.*

Proof. — If $\varphi^{-1}(M_n)$ is abelian, the universal abelian p-Frattini cover of G_n factors through the composition of φ and the canonical map from G_{n+1} to G_n. Conversely, if the extension is antecedent, $\varphi^{-1}(M_n)$ will be isomorphic to a quotient of L_n/p^2L_n. □

Hence, Fried also calls antecedent simple central p-extensions *abelian*.

There is a natural correspondence between the simple central p-extensions of G_n and the antecedent simple central p-extensions of G_{n+1}: both are defined by an element of $\mathrm{Hom}_{\mathbb{F}_p G_n}(M_n, \mathbf{1}_{\mathbb{F}_p G_n})$. We can phrase this correspondence as: each abelian simple central p-extension of G_{n+1} is antecedent to a unique simple central p-extension of G_n.

The height of a simple central p-extension $S \twoheadrightarrow G$ of G is the supremum of the positive rational integers n for which there exists a central p-Frattini cover of G that both factors through $S \twoheadrightarrow G$ and has cyclic kernel of order p^n. Constructing the antecedent simple central p-extensions via the p-adic Frattini lattice easily yields:

***Fact 7.3* ([FS])**. — *The height of a non-split abelian simple central p-extension of G_{n+1} equals the height of the simple central p-extension of G_n to which it is antecedent.*

Let us return to the exact sequence (1) that follows Proposition 7.1. Consider the universal elementary abelian central p-Frattini cover of M_n:

$$0 \longrightarrow \mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n}) \longrightarrow {}_{p}^{1}\hat{M}_n \xrightarrow{\varphi} M_n \longrightarrow 1$$

where we regard the group operation in M_n and ${}_{p}^{1}\hat{M}_n$ as multiplicative. There is a natural homomorphism from G_{n+1} to the automorphism group of ${}_{p}^{1}\hat{M}_n$, where the action of G_{n+1} comes from conjugation via the following commutative diagram:

$$\begin{array}{ccc} {}_{p}^{1}\hat{M}_n & \twoheadrightarrow & M_n \\ \downarrow & & \downarrow \\ G_{n+2}/(\omega_{\mathbb{F}_p M_n} M_{n+1}) & \twoheadrightarrow & G_{n+1}. \end{array}$$

The induced actions of G_n on M_n and $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$ are the usual ones.

Fix a subset $\{x_1, \ldots, x_N\}$ of ${}_{p}^{1}\hat{M}_n$ that maps bijectively via φ to a basis (over $\mathbb{F}_p$) of M_n. The set of elements of the form either x_i^p or $[x_i, x_j]$ (for $i < j$) is a basis of $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$. Since they are central, the set of elements of the form $[x_i, x_j]$

generates the entire commutator subgroup of ${}^1_p\hat{M}_n$; the action of G_n makes it naturally isomorphic to $\wedge^2 M_n$ as an $\mathbb{F}_p G_n$-module.

The exact sequence (1) splits when p is odd. Let x and y be arbitrary elements of ${}^1_p\hat{M}_n$; then $x^p y^p = (xy)^p [x,y]^{p(p-1)/2}$. Hence, when p is odd, the p-th powers form a characteristic subgroup of ${}^1_p\hat{M}_n$ and the action of G_n makes this subgroup naturally isomorphic to M_n. In terms of the universal coefficient theorem, this occurs because a canonical vector space splitting exists when p is odd; in the context of Jennings' theorem, it is because the p-th powers reside in a lower socle layer of $\Omega^2_{\mathbb{F}_p M_n}\mathbf{1}$ than do the commutators. In even characteristic, the squares *generate* ${}^1_2\hat{M}_n$; this is just the well-known fact that a group is abelian if all of its non-trivial elements have order 2. The formula $x^2y^2 = (xy)^2[x,y]$ then allows computation of the $\mathbb{F}_2 G_n$-module $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_2 M_n})$.

This dichotomy between p being even or odd mirrors the dichotomy in the cohomology rings $\mathrm{H}^*(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$ (which are graded-commutative rings using the cup product for multiplication). When p is odd, the homogeneous part of degree two separates into a direct sum of two pieces, one being the set of cup products of degree-one elements and the other the image of the Bockstein map.

When p is even, the cup products of degree-one elements yield the entire homogeneous part of degree two, as the Bockstein of a degree-one element is just the cup product of that element with itself when $p = 2$. In fact, the homogeneous part of degree one is isomorphic to $M_n^\frown$ and generates the cohomology ring, which is a polynomial ring over $\mathbb{F}_2$ with generating degree-one indeterminates given by a basis of $M_n^\frown$. Since G_n acts as algebra automorphisms of the cohomology ring, there is an $\mathbb{F}_2 G_n$-module epimorphism $M_n^\frown \otimes M_n^\frown \xrightarrow{\cdot\cup\cdot} \mathrm{H}^2(M_n, \mathbf{1}_{\mathbb{F}_2 M_n})$ given by the cup product. Dualizing shows that $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_2 M_n})$ is isomorphic to the kernel of the canonical epimorphism $M_n \otimes M_n \twoheadrightarrow \wedge^2 M_n$.

The following examples end this article by illustrating the behavior with n of the elementary abelian p-Schur multiplier of ${}^n_p\tilde{A}_5$. This may suggest the behavior in the general case, but the ad hoc nature of these arguments prevents straightforward extrapolation.

Example 7.4. — Let us begin with $p = 3$, the case where the structure of M_0 (and hence $\mathrm{H}_2(M_0, \mathbf{1}_{\mathbb{F}_p M_0})$) is simplest. Refer to Example 5.5 for notation, where it was seen that M_0 is isomorphic to the simple $\mathbb{F}_3 A_5$-module $S \simeq \mathbf{1}_{\mathbb{F}_3 A_4}{\uparrow}^{\mathbb{F}_3 A_5} / \mathbf{1}$. There is a basis of M_0 that A_4 permutes in the natural fashion. Then, $\wedge^2 M_0{\downarrow}_{\mathbb{F}_3\langle(123)\rangle}$ is a free module; since $\langle(123)\rangle$ is a 3-Sylow of A_5, $\wedge^2 M_0$ must be a projective $\mathbb{F}_3 A_5$-module. By inspection, (12)(34) doesn't fix any non-zero vector in the two-dimensional subspace fixed by (123). Thus, $\wedge^2 M_0$ cannot be $\mathbb{P}_{\mathbb{F}_3 A_5}(\mathbf{1})$. It also cannot be $\mathbb{P}_{\mathbb{F}_3 A_5}(S)$ because the latter is nine-dimensional. Therefore, $\wedge^2 M_0 \simeq T$ and $\mathrm{H}_2(M_0, \mathbf{1}_{\mathbb{F}_3 M_0}) \simeq S \oplus T$. Hence, the 3-Schur multiplier is zero for ${}^1_3\tilde{A}_5$.

By the Schreier formula, the dimension of M_1 is 244; the isomorphism class of M_1 lies outside of comfortable hand-calculation. Since $S \oplus T$ is a quotient of M_1, $(S \oplus T) \oplus \wedge^2(S \oplus T)$ will be a quotient of $\mathrm{H}_2(M_1, \mathbf{1}_{\mathbb{F}_3 M_1})$ and, hence, of M_2. The exterior product $\wedge^2(S \oplus T)$ decomposes into a direct sum of $S \otimes T$, $\wedge^2 S$, and $\wedge^2 T$. Since T is projective, so is $S \otimes T$ (cf. [**Ben98a**, Proposition 3.1.5]), and Brauer character calculations (cf. [**Ben98a**, §5.3]) show it to be isomorphic to $T \oplus \mathbb{P}_{\mathbb{F}_3 A_5}(S)^2$. We already know that $\wedge^2 S \simeq T$. It is easy to find a basis of T that is permuted freely by a 3-Sylow of A_5; the induced basis on $\wedge^2 T$ is thus also permuted freely, and so $\wedge^2 T$ is projective. Another Brauer character calculation shows $\wedge^2 T \simeq T \oplus \mathbb{P}_{\mathbb{F}_3 A_5}(S)$. Therefore, M_2 has a quotient isomorphic to $S \oplus T^4 \oplus \mathbb{P}_{\mathbb{F}_3 A_5}(S)^3$. Since this is a small part of $M_1 \oplus \wedge^2 M_1$, it is possible that ${}^2_3\tilde{A}_5$ has non-zero 3-Schur multiplier.

But now we know that M_3 has a quotient isomorphic to the direct sum of three copies of $\mathbb{P}_{\mathbb{F}_3 A_5}(S) \otimes \mathbb{P}_{\mathbb{F}_3 A_5}(S)$. Yet another Brauer character calculation will show that $\mathbb{P}_{\mathbb{F}_3 A_5}(S) \otimes \mathbb{P}_{\mathbb{F}_3 A_5}(S) \simeq T^4 \oplus \mathbb{P}_{\mathbb{F}_3 A_5}(S)^5 \oplus \mathbb{P}_{\mathbb{F}_3 A_5}(\mathbf{1})^2$. So, the elementary abelian 3-Schur multiplier of ${}^3_3\tilde{A}_5$ has dimension at least six.

A similar procedure will show that the elementary abelian p-Schur multiplier of ${}^n_p\tilde{A}_5$ will have dimension at least two when $n > 2$, for all rational primes p dividing the order of A_5. In each case, a direct calculation of $\wedge^2 M_0$ will show it to have a projective summand $\mathbb{P}$. In even characteristic, the exact sequence (1) may not split, but $\mathbb{P}$ will still float to the top of the second-homology. Hence, for each p, $\mathrm{H}_2(M_0, \mathbf{1}_{\mathbb{F}_p M_0})$ will have a quotient isomorphic to $M_0 \oplus \mathbb{P}$. As in the case of $p = 3$, take the direct sum of this module with its exterior product, and iterate this procedure until multiple copies of $\mathbb{P}(\mathbf{1})$ appear.

For any group G, if the dimension of the elementary abelian p-Schur multiplier of G_n is $m > 1$ then the dimension of the elementary abelian p-Schur multiplier of G_{n+1} is at least $m(m+1)/2$. This is a corollary of exact sequence (1) when p is odd, and of the the exact sequence

$$0 \to \mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_2 M_n}) \to M_n \otimes M_n \to \wedge^2 M_n \to 0$$

when p is even: if M' is a quotient of M_n on which G_n acts trivially, then $\mathrm{H}_2(M_n, \mathbf{1}_{\mathbb{F}_p M_n})$ will have a quotient isomorphic to $M' \oplus \wedge^2 M'$. Therefore, the dimensions of the elementary abelian p-Schur multipliers of ${}^n_p\tilde{A}_5$ have no bound.

Example 7.5. — The composition series of a p-Frattini module may be loaded with trivial simple modules, but the p-Frattini module may still have no non-trivial quotient with trivial group action. Consider $p = 5$; refer to Example 5.4 for notation. The 5-Frattini module M_0 of A_5 is isomorphic to $\mathrm{Sgn}_5\!\uparrow^{\mathbb{F}_5 A_5}$, a module which strongly resembles the simple $\mathbb{F}_3 A_5$-module T. (They are both reductions of the same $\mathbb{Z}A_5$-lattice.) It is easy to find a basis of M_0 that consists of one vector fixed by the action of a 5-Sylow and another five vectors that are cyclically permuted by the same 5-Sylow. Since the induced basis of $\wedge^2 M_0$ is acted on freely by the 5-Sylow, $\wedge^2 M_0$ is projective and a Brauer character calculation shows it to be isomorphic to $\mathbb{P}_{\mathbb{F}_5 A_5}(W) \oplus \mathrm{St}_5$. Therefore, the head of M_1 is isomorphic to $W^2 \oplus \mathrm{St}_5$. However, the Schreier formula shows that the dimension of M_1 is 78126, while the recursive formulas for $\#_S(M_n)$ (alluded to after Fact 6.3) show that any composition series of M_1 contains exactly 6476 simple factors isomorphic to $\mathbf{1}_{\mathbb{F}_5 A_5}$.

For any finite group G, the modules M_n all have isomorphic socle (i.e., maximal semi-simple submodule) since $\mathrm{H}^1(H, S) \simeq \mathrm{H}^1(G, S)$ for any simple $\mathbb{F}_p H$-module S and any p-Frattini cover $H \twoheadrightarrow G$ (cf. [**Sem**]); in the case of $G = A_5$ and $p = 5$, the socle is W. Above, we calculated the head of M_1 to have dimension 11. Furthermore, using Jennings' theorem on $M_1{\downarrow}_{\mathbb{F}_p M_0}$, it is easy to see that M_1 has at most 75 radical layers, so at least one of these layers must have dimension greater than 1070. The shape of M_1 is thus like a spindle, with a fat middle, but pointy at each end. This is not so unusual, since projective indecomposable modules will also have this shape, but it suggests that we cannot expect the heads of the M_n to grow quickly.

Example 7.6. — Finally, $p = 2$, $n = 0$, and $G = A_5$ together provide an example of the exact sequence (1) being non-split. This sequence would split if and only if it split on restriction to a 2-Sylow V_4 of A_5. The 2-Frattini module of V_4 is isomorphic to $M_0{\downarrow}_{\mathbb{F}_2 V_4}$, so this example is in fact minimal for showing non-splitness. There is a basis $\{x_1, \dots, x_5\}$ of M_0 such that two generators a and b of V_4 act as follows:

$$a \begin{cases} x_1 & \mapsto & x_1 \\ x_2 & \mapsto & x_2 \\ x_3 & \mapsto & x_4 \\ x_4 & \mapsto & x_3 \\ x_5 & \mapsto & \sum_{i=1}^5 x_i \end{cases} \qquad b \begin{cases} x_1 & \mapsto & x_2 \\ x_2 & \mapsto & x_1 \\ x_3 & \mapsto & x_4 \\ x_4 & \mapsto & x_3 \\ x_5 & \mapsto & x_5 \end{cases}$$

Inside $\mathrm{H}_2(M_0, \mathbf{1}_{\mathbb{F}_2 M_0})$, use x_i again to denote the square of a pullback of x_i in the universal elementary abelian central 2-Frattini cover of M_0; use $x_j \wedge x_k$ to denote the commutator of pullbacks of x_j and x_k. The actions of a and b are then given by:

$$a \begin{cases} x_1 & \mapsto & x_1 \\ x_2 & \mapsto & x_2 \\ x_3 & \mapsto & x_4 \\ x_4 & \mapsto & x_3 \\ x_5 & \mapsto & \sum_{i=1}^5 x_i + \sum_{1 \le j < k \le 5} x_j \wedge x_k \end{cases} \qquad b \begin{cases} x_1 & \mapsto & x_2 \\ x_2 & \mapsto & x_1 \\ x_3 & \mapsto & x_4 \\ x_4 & \mapsto & x_3 \\ x_5 & \mapsto & x_5 \end{cases}$$

where both a and b fix $\sum_{1 \le j < k \le 5} x_j \wedge x_k$. Hence, the cocycle in $\mathrm{Ext}^1_{\mathbb{F}_2 V_4}(M_0{\downarrow}_{\mathbb{F}_2 V_4}, (\wedge^2 M_0){\downarrow}_{\mathbb{F}_2 V_4})$ takes its values in a copy of $\mathbf{1}$. The six-dimensional $\mathbb{F}_2 V_4$-module extending $M_0{\downarrow}_{\mathbb{F}_2 V_4}$ by this copy of $\mathbf{1}$ will be isomorphic to $\mathbf{1}_{\mathbb{F}_2\langle a \rangle}{\uparrow}^{\mathbb{F}_2 A_4}{\downarrow}_{\mathbb{F}_2 V_4}$, where A_4 is the normalizer of V_4. (This isomorphism is seen through some elementary manipulation of the matrices for a and b defining the action of V_4 on this six-dimensional module.) Since $\mathbf{1}_{\mathbb{F}_2\langle a \rangle}{\uparrow}^{\mathbb{F}_2 A_4}{\downarrow}_{\mathbb{F}_2 V_4}$ is isomorphic to a direct sum of three indecomposable $\mathbb{F}_2 V_4$-modules of dimension two, while $M_0{\downarrow}_{\mathbb{F}_2 V_4}$ is indecomposable, the cocycle must not be a coboundary. Using the transfer map to compute the cocycle in $\mathrm{Ext}^1_{\mathbb{F}_2 A_5}(M_0, \wedge^2 M_0)$ shows that the values of the cocycle lie in a copy of $\mathbf{1}_{\mathbb{F}_2 A_5}$.

Appendix A

The Gruenberg-Roggenkamp equivalence

Define the functor $\Phi : \mathcal{C}_{RG}(G) \to \mathcal{C}_{RG}(\omega_{RG})$ as follows. Let $f : H \twoheadrightarrow G$ be an object of $\mathcal{C}_{RG}(G)$ with kernel K. The action of H on the module $\omega_{\mathbb{Z}H;K} := \omega_{\mathbb{Z}H}/(\omega_{\mathbb{Z}K}\omega_{\mathbb{Z}H})$ has kernel K, so the natural epimorphism $\omega_{\mathbb{Z}H;K} \twoheadrightarrow \omega_{\mathbb{Z}G}$ induced by f is one of $\mathbb{Z}G$-modules. The kernel is naturally isomorphic to $K{\downarrow_{\mathbb{Z}G}}$ via the map sending $k \in K$ to $\overline{k-1} := (k-1) + \omega_{\mathbb{Z}K}\omega_{\mathbb{Z}H}$:

$$\overline{(k_1 - 1)} + \overline{(k_2 - 1)} = \overline{(k_1 k_2 - 1)}$$
$$\text{and}$$
$$g \cdot \overline{(k-1)} = \overline{({}^g k - 1)}$$

for all $g \in G$ and $k, k_1, k_2 \in K$. Since $\omega_{\mathbb{Z}G}{\downarrow_{\mathbb{Z}}}$ is free, the sequences are exact in the following pushout diagram (induced by the multiplication map $RG \otimes_{\mathbb{Z}G} (K{\downarrow_{\mathbb{Z}G}}) \to K$):

$$\begin{array}{ccccccccc} 0 & \longrightarrow & RG \otimes_{\mathbb{Z}G} (K{\downarrow_{\mathbb{Z}G}}) & \longrightarrow & RG \otimes_{\mathbb{Z}G} (\omega_{\mathbb{Z}H;K}) & \longrightarrow & \omega_{RG} & \longrightarrow 0 & \\ & & \downarrow & & \downarrow & & \| & & ; \\ 0 & \longrightarrow & K & \longrightarrow & (RG \otimes_{\mathbb{Z}G} (\omega_{\mathbb{Z}H;K}))/I & \xrightarrow{\Phi(f)} & \omega_{RG} & \longrightarrow 0 & \end{array}$$

I is the submodule generated by elements of the form $\left[r \otimes \overline{(k-1)}\right] - \left[1 \otimes \overline{(rk-1)}\right]$, where $r \in R$ and $k \in K$. Given a morphism $\varphi \in \mathrm{Hom}(f_1, f_2)$ between objects $f_1 : H_1 \twoheadrightarrow G$ and $f_2 : H_2 \twoheadrightarrow G$, $\Phi(\varphi)$ is induced by the natural action of φ that sends an element of $\omega_{\mathbb{Z}H_1}$ to one of $\omega_{\mathbb{Z}H_2}$.

The functor $\Psi : \mathcal{C}_{RG}(\omega_{RG}) \to \mathcal{C}_{RG}(G)$ is even easier to construct. Let $s : M \twoheadrightarrow \omega_{RG}$ be an object in $\mathcal{C}_{RG}(\omega_{RG})$. There is a group monomorphism θ from G to the semi-direct product $\omega_{RG} \rtimes G$ that sends $g \in G$ to $(g-1, g)$. Using this, $\Psi(s)$ comes from the fiber product (i.e., pullback) in the following commutative diagram:

$$\begin{array}{ccc} (s,1)^{-1}(\theta(G)) & \overset{\Psi(s)}{\twoheadrightarrow} & G \\ \downarrow & & \downarrow \theta \\ M \rtimes G & \overset{(s,1)}{\twoheadrightarrow} & \omega_{RG} \rtimes G \end{array}$$

where $(s,1)(m,g) := (s(m), g)$ for all $(m,g) \in M \rtimes G$. Given a morphism $\psi \in \mathrm{Hom}(s_1, s_2)$ between objects $s_1 : M_1 \twoheadrightarrow \omega_{RG}$ and $s_2 : M_2 \twoheadrightarrow \omega_{RG}$, $\Psi(\psi)$ is the restriction to $(s_1, 1)^{-1}(\theta(G))$ of the map $(\psi, 1) : M_1 \rtimes G \to M_2 \rtimes G$.

References

[Ben98a] D. J. Benson – *Representations and Cohomology. I: Basic Representation Theory of Finite Groups and Associative Algebras*, second ed., Cambridge Studies in Advanced Mathematics, no. 30, Cambridge University Press, Cambridge, 1998.

[Ben98b] ———, *Representations and Cohomology. II: Cohomology of Groups and Modules*, second ed., Cambridge Studies in Advanced Mathematics, no. 31, Cambridge University Press, Cambridge, 1998.

[BF02] P. Bailey & M. Fried – Hurwitz Monodromy, Spin Separation and Higher Levels of a Modular Tower, in *Arithmetic Fundamental Groups and Noncommutative Algebra* (M. D. Fried & Y. Ihara, eds.), Proceedings of Symposia in Pure Mathematics, vol. 70, American Mathematical Society, 2002, Proceedings of the 1999 von Neumann Conference held at the Mathematical Sciences Research Institute, Berkeley, California, p. 79–220.

[Bro94] K. S. Brown – *Cohomology of Groups*, Graduate Texts in Mathematics, vol. 87, Springer-Verlag, New York, 1994, Corrected Reprint of the 1982 Original.

[CKK80] J. Cossey, O. H. Kegel & L. G. Kovács – Maximal Frattini Extensions, *Archiv der Mathematik* **35** (1980), no. 3, p. 210–217.

[Dèb] P. Dèbes – Modular Towers: Construction and Diophantine Questions, In this volume.

[DS75] J. L. Dyer & G. P. Scott – Periodic Automorphisms of Free Groups, *Communications in Algebra* **3** (1975), p. 195–201.

[FJ05] M. D. Fried & M. Jarden – *Field Arithmetic*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 11, Springer, Berlin, 2005.

[FK97] M. Fried & Y. Kopeliovich – Applying Modular Towers to the Inverse Galois Problem, in *Geometric Galois Actions II Dessins d'Enfants, Mapping Class Groups and Moduli*, London Mathematical Society Lecture Notes, vol. 243, Cambridge University Press, 1997, p. 172–197.

[Fri] M. Fried – Alternating Groups and Lifting Invariants, preprint, October 2004, available at `http://math.uci.edu/~mfried/psfiles/hf_can.html`. Submitted.

[Fri95] ———, Introduction to Modular Towers: Generalizing Dihedral Group–Modular Curve Connections, in *Recent Developments in the Inverse Galois Problem* (M. D. Fried et al., eds.), Contemporary Mathematics, vol. 186, American Mathematical Society, 1995, p. 111–171.

[Fri02] ———, Moduli of Relatively Nilpotent Extensions, in *Communications in Arithmetic Fundamental Groups* (Kyoto), Sūrikaisekikenkyūsho Kōkyūroku, no. 1267, Kyoto University, Research Institute for Mathematical Sciences, June 2002, Papers from the workshops held at the Research Institute for Mathematical Sciences, Kyoto University, Kyoto, February 8-10, 1999 and October 29-31, 2001, p. 70–94.

[FS] M. D. Fried & D. Semmen – Schur Multiplier Types and Shimura-like Systems of Varieties, preprint available at: `http://math.uci.edu/~mfried/#mt`.

[Gas54] W. Gaschütz – Über modulare Darstellungen endlicher Gruppen, die von freien Gruppen induziert werden, *Mathematische Zeitschrift* **60** (1954), p. 274–286.

[Gru76] K. W. Gruenberg – *Relation Modules of Finite Groups*, Conference Board of the Mathematical Sciences Regional Conference Series in Mathematics, no. 25, American Mathematical Society, Providence, R.I., 1976.

[GS78] R. L. Griess & P. Schmid – The Frattini Module, *Archiv der Mathematik* **30** (1978), p. 256–266.

[HP89] D. F. Holt & W. Plesken – *Perfect Groups*, Oxford Mathematical Monographs, Oxford Science Publications. The Clarendon Press, Oxford University Press, New York, 1989, With an appendix by W. Hanrath.

[NS03] N. Nikolov & D. Segal – Finite Index Subgroups in Profinite Groups, *Comptes rendus de l'Académie des Sciences, série A, Paris* **337** (2003), no. 5, p. 303–308.

[Sem] D. Semmen – Asymptotics of p-Frattini Covers and Hausdorff Dimensions in Free Pro-p Groups, preprint available at: `http://www-rcf.usc.edu/~semmen/`. Submitted.

[Sem05] ———, Jennings' Theorem for p-Split Groups, *Journal of Algebra* **285** (2005), no. 2, p. 730–742.

[Wei] T. Weigel – On the Universal Frattini Extension of a Finite Group, preprint, May 10, 2004. Submitted.

[Wei05] ———, Maximal ℓ-Frattini Quotients of ℓ-Poincaré Duality Groups of Dimension 2, *Archiv der Mathematik* **85** (2005), no. 1, p. 55–69.

D. Semmen, University of Southern California, Dept. Maths, 3620 South Vermont Ave., KAP 108, Los Angeles, California 90089-2532, U.S.A. • *E-mail :* `dsemmen@gmail.com`
Url : `http://members.cox.net/dsemmen`