Contemporary Mathematics
Volume 00, 0000

Introduction to MODULAR TOWERS:

Generalizing dihedral group–modular curve connections

MICHAEL D. FRIED

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

Supported by NSF #DMS-99305590, RIMS Institute March 1994, Alexander von Humboldt Foundation during a stay at Erlangen Universität, Fall 1994.

I thank Y. Ihara, M. Matsumoto and H. Nakamura for listening to me justify the first presentation of these topics. W. Feit, R. Howe, J. G. Thompson and H. Voelklein helped me with modular representations applied to the universal frattini cover. An unpublished 1987 preprint included the construction of the universal exponent p frattini covers of A_5. Others may have gone over that territory since. J.-P. Serre, in particular, gave an Ext interpretation to simplify our arguments to efficient use of Loewy displays of projective indecomposables (§II.B). R. Guralnick has advised on these matters recently (including part of Ex. D.4 of §App.D). F. Leprévost produced dihedral group challenge problems, from which I developed the $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization lemma of §I.D. G. Malle suggested the $\mathrm{PSL}_2(q)$ example of exceptionally ramified primes in §III.E. Lectures at Erlangen gave me confidence applications of modular towers to arithmetic and geometry could surmount their technicalities. My hosts, D. Geyer and G. Frey, were particularly enthusiastic on the mix of problems. They influenced the balance of group theory, algebraic geometry and diophantine considerations in this introduction to modular towers. I apologize in advance to any group theorists who already knew how to explicitly produce the universal p-frattini covers. Also, a recent conversation with D. Benson completed my argument the Center Hypothesis (Def. 3.5 and Lemma 3.6) holds for perfect groups.

Abstract. To each finite group G we can attach a projective profinite group, $\tilde{G}$: the *universal frattini cover* of G [**FrJ**, §20.6] (§II.A-B). Further, for any collection of r conjugacy classes $\mathbf{C}$ of G, there is a natural moduli space. Its points are equivalence classes of covers of the Riemann sphere $\mathbb{P}^1$ ramified over r points. The particular covers have geometric monodromy group G and $\mathbf{C}$ is the set of conjugacy classes of branch cycles of the cover. We conjoin these two constructions. The moduli space construction applies to a natural cofinal collection of finite quotients of $\tilde{G}$. This produces arithmetic invariants for the theory of curve covers. A special case uses a prime p dividing $|G|$ and conjugacy classes $\mathbf{C}$ of orders relatively prime to p. This *p-unramified lifting invariant*, $\nu(G,p,\mathbf{C})$, is compatible with terminology of [**Se3**]. It also produces a tower of moduli spaces. We denote them formally as $(G,p,\mathbf{C})$-moduli spaces. In looser terminology, these are a *modular tower*. This moduli space material is in Part III.

Arithmetic geometers know a special case: the tower of covers $X_0(p) \leftarrow X_0(p^2) \leftarrow X_0(p^3)\cdots$ of modular curves. Points on $X_0(p^n)$ correspond to pairs of elliptic curves with a cyclic p^n-power isogeny. Here G is the dihedral group D_p of order $2p$. Also, $r=4$ and $\mathbf{C}$ is four repetitions of the involution conjugacy class in D_p [**DFr**, §5.1–5.2]. Part I (especially, §I.D) discusses example problems with ready applications for modular towers. These include a highly structured version of the inverse Galois problem and construction of *general exceptional covers*.

Part II discusses *universal frattini covers* of a finite group. Each level of a modular tower comes from a quotient of a universal p-frattini cover. Moduli space difficulties at a particular level will have a modular representation interpretation. For example, this holds for the appearance of a center in the quotient group for a particular level (see The Center Hypothesis of §III.B). We illustrate these matters with an application to A_n and 3-cycles. This is another classical connection: to theta functions with characteristics. Much we know of any modular tower comes from the lifting invariant. This lives in the p-part of the kernel $\tilde{G} \to G$. Part II shows it is possible to compute this invariant. The A_n examples (§III.C) show the lifting invariant detecting obstructed towers. Sometimes a component of a modular tower attached to $(G,p,\mathbf{C})$ has finite length. Modular curve towers have only one component and that has no obstruction.

Applications of $\nu(G,p,\mathbf{C})$ point to a test for the *Drinfeld-Grothendieck-Ihara relations on* $G_{\mathbb{Q}}$ [**I**]. Conjectures on the *Grothendieck Teichmüller group* imply it should detect fields of definition of components of these moduli spaces (when $r \ge 5$). Modular towers have suitable profinite aspects to make this test explicit. Ihara and Matsumoto [**IM**] have reproduced the appearance of $\widehat{\mathcal{G}T}$ making it applicable to Hurwitz spaces. Their construction produces a natural section to the map from the arithmetic fundamental group of projective r-space minus the discriminant locus. §App.C suggests a use for [**IM**] by modeling how to precisely find the field of definition of Hurwitz space components. It bases the model on a special case: How to decide if a component has field of definition $\mathbb{R}$. §App.D considers the compatible problem of finding *real points on modular towers*. §I.B summarizes Parts IV and V. This includes a discussion of the $\widehat{\mathcal{G}T}$ action on modular towers, to appear in the continuation paper.

Points over finite fields are a persistent diophantine subtopic. In particular, consider realizing a given group G as a regular extension of $\mathbb{F}_p(x)$. [**FrV**] notes there are only finitely many p exceptional for G. It, however, gives no bound on these. A more refined form, for realizations with branch cycles in a given *Nielsen class*, has many applications. In this form, §App.E gives an explicit upper bound on exceptional p. Such a realization, however, comes from one $\mathbb{F}_p$ point on an infinite collection of varieties over $\mathbb{F}_p$. We use the Lang-Weil bound. Yet, modular towers call for an analog of [**I2**] and later works. Lang-Weil can tell us little of the points on modular towers over a given finite field.

PART I. INTRODUCTION AND MOTIVATING PROBLEMS

This part motivates generalizing the connection between the inverse Galois problem and modular curves. §I.A explains what about modular curves we want to generalize. Later parts of the paper refer to this introduction to connecting dihedral groups to modular curves. §I.B tells the main contributions of the paper. §I.C gives notation for the theory of covers. Finally, §I.D and §I.E give diophantine motivation for the generalization of natural towers of modular curves we call *modular towers*. Previous results of the author applied modular curves to investigate cases of these topics. These fall under the heading $(G,\hat{G},\mathbf{C})$ *realizations* by regular extensions $L/F(x)$. Usually, F is a number field or finite field. These include diophantine results about modular curves that haven't appeared in quite this form. Still, we mean §I.D and §I.E to show diophantine problems appropriate for modular towers. (Part V in the continuation of this paper goes further.) These sections emphasize the role of counting points on curves over finite fields. The influence for this came from papers of Y. Ihara, and a result of Frey. The latter used Faltings' proof of Lang's conjecture. He thereby gave an insight into simple finite field questions and points over number fields.

§I.F and §I.G present different views on the Galois closure process. Especially, the construction of §I.G gives a geometric view of automorphisms in the arithmetic theory of covers. Throughout, G_F is the absolute Galois group of a given field F. Unless otherwise said, all curves will be projective and nonsingular. Further, points on varieties means *geometric* points.

§I.A. Focus on modular curves. Part III has reminders of the properties of Hurwitz spaces. These join Part I motivations to Part II group theory to produce modular curve generalizations. The modular curve tower $X_0(p) \leftarrow X_0(p^2) \leftarrow X_0(p^3)\cdots$ (and $X_1(p) \leftarrow X_1(p^2) \leftarrow X_1(p^3)\cdots$) encodes collective information on ℓ-adic ($\ell = p$ here) representations of subgroups of $G_{\mathbb{Q}}$.

For example, suppose you have a projective sequence $\boldsymbol{p}_i \in X_1(p^i)$, $i = 1,\ldots$: for each i, $\boldsymbol{p}_i$ maps to $\boldsymbol{p}_{i-1}$. When $i = 1$ this means $\boldsymbol{p}_1$ maps to the j-invariant $j(\boldsymbol{p}_1)$ of the common elliptic curve supporting these points (see §I.D). Suppose $j(\boldsymbol{p}_1)$ lies in a number field F. Then, G_F acts on the sequence $\{\boldsymbol{p}_i\}_{i=1,\ldots}$. There is a standard interpretation. Let $\boldsymbol{x} = \{x_1, x_2, x_3, x_4\}$ be the four branch points of the elliptic curve $E_{\boldsymbol{x}}$ in Weierstrass normal over the x-line $\mathbb{P}^1 = \mathbb{P}^1_x$. (Weierstrass normal form takes x_4 to be ∞, lying under the origin for addition on $E_{\boldsymbol{x}}$. The main point is x_4 is rational over $\mathbb{Q}$. Eventually we allow any collection of four distinct points on $\mathbb{P}^1_x$.) Regard $\boldsymbol{p}_i \in X_1(p^i)$ as a pair $(E_{\boldsymbol{x}}, e_i)$ with e_i a point of order p^i (exactly) on $E_{\boldsymbol{x}}$. The map from $X_1(p^i) \to X_1(p^{i-1})$ derives from $e_i \mapsto pe_i$. The isogeny $E_{\boldsymbol{x}} \to E_{\boldsymbol{x}}/e_i$ has a *dual isogeny*: $E_{\boldsymbol{x}}/e_i \to E_{\boldsymbol{x}}$, Galois with group $\mathbb{Z}/p^i$. Such a cover comes from a homomorphism $\psi_i : \pi_1(E_{\boldsymbol{x}}) \to \mathbb{Z}/p^i$. Actually, it comes from an equivalence class of homomorphisms: The same cover derives from composing ψ_i with an automorphism of $\mathbb{Z}/p^i$. To normalize, choose from this equivalence class the homomorphism sending e_i to $1 \in \mathbb{Z}/p^i$.

To put all these covers together, identify integral homology with a lattice $L \cong \mathbb{Z}^2$ for the complex structure $\mathbb{C}/L$ on $E_{\boldsymbol{x}}$. The projective limit $\lim_{\infty \leftarrow i} L/p^i L$ equals $\lim_{\infty \leftarrow i} \frac{1}{p^i} L/L$. Therefore, it is the projective limit of p^i division points on $E_{\boldsymbol{x}}$. The system of points e_i, $i = 1, \dots,$ forms a p-adic line $\mathcal{L}$ in the two dimensional p-adic space $L \otimes \mathbb{Z}_p$. Let $\hat{\pi}_1^{(p)}(E_{\boldsymbol{x}}) = V_p$ be the pro-p quotient of the algebraic fundamental group. The group G_F acts on $E_{\boldsymbol{x}}$ torsion points. Therefore, it acts through $\mathrm{GL}(V_p) \cong \mathrm{GL}_2(\mathbb{Z}_p)$ on $\hat{\pi}_1^{(p)}(E_{\boldsymbol{x}})$.

A celebrated theorem of Serre implies the following [**Se5**]. If $E_{\boldsymbol{x}}$ is without complex multiplication, the image of G_F in $\mathrm{GL}(V_p)$ is an open subgroup. Further, for almost all primes p it is $\mathrm{GL}(V_p)$. So, for $[K : F] < \infty$, only finitely many p division points of $E_{\boldsymbol{x}}$ have field of definition K. For almost all primes p, none have. (This follows from [**Se5**] even if $E_{\boldsymbol{x}}$ has complex multiplication.)

Now we rephrase this discussion using the fundamental group of $\mathbb{P}^1 \setminus \boldsymbol{x}$. The projective system of unramified (Galois) covers of $E_{\boldsymbol{x}}$ comes from a quotient of the algebraic fundamental group $\hat{\pi}(\mathbb{P}^1 \setminus \boldsymbol{x})$. An explicit presentation of this quotient comes from Riemann's Existence Theorem (§1.F). Let $\sigma_1, \dots, \sigma_4$ freely generate $F_{\boldsymbol{\sigma}}$ subject to to the indentity

$$(*) \qquad \sigma_1\sigma_2\sigma_3\sigma_4 = 1.$$

Then, $\hat{\pi}(\mathbb{P}^1 \setminus \boldsymbol{x})$ is the profinite completion of all quotients of $\hat{F}_{\boldsymbol{\sigma}}$ by subgroups of finite index. Let $E' \to E_{\boldsymbol{x}}$ be any ramified cover. Compose this with the degree 2 cover $E_{\boldsymbol{x}} \to \mathbb{P}^1$ unramified outside of $\boldsymbol{x}$. Such covers correspond to representations of $\hat{F}_{\boldsymbol{\sigma}}$ that send $\sigma_1, \dots, \sigma_4$ into elements of order (exactly) 2. That is, the cover $E' \to \mathbb{P}^1$ ramifies of order 2 over each of the four branch points. Let $\hat{D}_{\boldsymbol{\sigma}}$ be the quotient of $\hat{F}_{\boldsymbol{\sigma}}$ by the relations

$$(**) \qquad \sigma_i^2 = 1,\ i = 1, 2, 3, 4.$$

Geometry shows $\hat{D}_{\boldsymbol{\sigma}}$ is $\hat{\mathbb{Z}}^2 \times^s \{\pm 1\}$, with $\hat{\mathbb{Z}}$ the profinite completion of $\mathbb{Z}$ with respect to all subgroups. Here is a combinatorial group theory argument for this. We show $\sigma_1\sigma_2$ and $\sigma_1\sigma_3$ are independent generators of $\hat{\mathbb{Z}}^2$. Then, σ_1 is a generator of $\{\pm 1\}$. First: $\sigma_1(\sigma_1\sigma_2)\sigma_1 = \sigma_2\sigma_1$ shows σ_1 conjugates $\sigma_1\sigma_2$ to its inverse. Also,

$$(\sigma_1\sigma_2)(\sigma_1\sigma_3) = (\sigma_1\sigma_3)\sigma_3(\sigma_2\sigma_1)\sigma_3 = (\sigma_1\sigma_3)(\sigma_1\sigma_2)$$

shows the said generators commute. The maximal pro-p quotient is $\mathbb{Z}_p^2 \times^s \{\pm 1\}$. Any line (pro-cyclic group) in $\mathbb{Z}_p^2$ produces a *dihedral group* D_{p^∞} from multiplication by -1 on this line.

The $\mathbb{P}^1$ cover approach has advantages. Suppose $\boldsymbol{x}$ is invariant as a set under G_F. Then, any degree 2 cover ramified at these four points is equivalent to a cover defined over F. Investigating covers of $\mathbb{P}^1$ ramified only over $\boldsymbol{x}$ includes realizing dihedral groups as Galois groups. To consider all realizations, we can't insist on a priori conditions on the branch points. This is especially true for showing realizations of certain type aren't possible (see §I.D). Also, this form allows us to replace dihedral groups by any finite group G.

Even a finite *simple* group G produces a tower of moduli spaces that encodes information on natural profinite representations of $G_{\mathbb{Q}}$. What is the analog of the dihedral group D_p acting on lines in a two dimensional p-adic space? Replacing the line is a free pro-p group mapping surjectively to a p-sylow of G. The kernel, ker, of this map comes with a filtration from its association with G. Here, p is a prime dividing the order of G. There is a short exact sequence $\ker \to {}_p\tilde{G} \xrightarrow{\phi} G$ in place of $\mathbb{Z}_p \to D_{p^\infty} \to D_p$. Part II shows how to compute much about the group ${}_p\tilde{G}$. Such computations aren't yet trivial. Still, we illustrate our two main principles by displaying this group when $G = A_5$ and $p = 2, 3$ or 5 (Prop. 2.9 and Remark 2.10).

§I.B. Introduction. Modular towers (§III.C) generalize towers of modular curves. These moduli spaces encode information on a collection of *nilpotent* representations of subgroups of $G_{\mathbb{Q}}$. It is the *universal frattini cover* $\tilde{G}$ of G that allows these constructions (§II.A). §II.B develops material for computing the kernel of the natural map $\tilde{G} \to G$. §II.C applies this in detail to A_5. Alternating groups also illustrate the lifting invariant $\nu(G, p, \mathbf{C})$ of §III.D. We note this example's relation to theta functions with characteristics and [**Se3,4**] and [**EKV**] in Remark 3.14. It illustrates properties that recommend it among our motivations, only second to modular curves.

The inductive process of §II.D helps compute successive *frattini* quotients of ${}_p\tilde{G}$, the universal p-frattini cover of G. §II.E computes the first nontrivial frattini quotient of ${}_2\tilde{A}_5$. Finally, §II.F displays ${}_2\tilde{A}_5$. While the principles aren't the same, it may be no more (no less) difficult to compute in universal p-frattini covers than in, say, $\mathrm{PSL}_n(\mathbb{Z}_p)$. We mention this analogy, because $\mathrm{PSL}_n(\mathbb{Z}_p) \to \mathrm{PSL}_n(\mathbb{Z}/p)$ is a frattini cover whenever $\mathrm{PSL}_n(\mathbb{Z}/p)$ is simple. Thus, the universal p-frattini cover of $\mathrm{PSL}_n(\mathbb{Z}/p)$ is a proper cover of $\mathrm{PSL}_n(\mathbb{Z}_p)$ (see (2.5) and Remark 2.10).

It is easy to prove the (absolute) irreducibility of modular curves. Yet, their irreducibility is significant. For these curves covers of the j-line this follows from their having the *rigidity* property. This is the simplest of a set of criteria ([**Se4**, Chap. 7] or [**Fr6**, §4]) for asserting the field of a definition of a cover is $\mathbb{Q}$.

Theorem 3.4 quotes [**FrV**] for results that depend on several assumptions. Most important is transitive action of the *Hurwitz monodromy group* H_r on *Nielsen classes*. The data for a Nielsen class comes from a collection of conjugacy classes in a finite group (§III.A). This transitivity result gives the analog for a level of a modular tower of the irreducibility of modular curves. [**FrV**] sought applications to the inverse Galois problem. The tools, however, allow precise statements about fields of definition of these moduli spaces even when we relax the transitivity assumption (§III.B). This will breach ground between braid group representations in the Ihara, Matsumoto and Nakamura program and the moduli approach to the inverse Galois problem of myself, Debes and Völklein. Practical applications in [**DFr**], [**FrV**], [**Ma^2**], and papers these reference, already show the way. We now connect Part III results to those of the continutation of this paper, Parts IV and V (to appear elsewhere).

The lowest level of a modular tower is a Hurwitz space $\mathcal{H} = \mathcal{H}(G, p, \mathbf{C})$. A simplifying assumption is the collection $\mathbf{C}$ of conjugacy classes of G is a *rational union* (§III.A). In this case, when G has no center, $\mathbb{Q}$ is a field of definition of $\mathcal{H}$. All arithmetic applications of these spaces require knowing fields of definition of (absolutely irreducible) components of these spaces. It can even aid an applications that $\mathcal{H}$ is reducible, if it has a $\mathbb{Q}$ component. The spaces arise abstractly from covering space theory. So, it can be *extremely* difficult to catch the field of definition of components. Transitivity of the Hurwitz monodromy group is equivalent to there being one component. The lifting invariant $\nu = \nu(G, p, \mathbf{C})$ gives a more general criterion. Regard $\nu(G, p, \mathbf{C})$ as a function on components of $\mathcal{H}$. Its values are collections of conjugacy classes in the kernel of the universal p-frattini kernel of G. The Main Theorem of §III.D says the following. If $\mathcal{H}_1$ is a component of $\mathcal{H}$, and $\sigma \in G_{\mathbb{Q}}$, then $\nu(\mathcal{H}_1) = \nu(\mathcal{H}_1^{\sigma})^{{}_p\psi(\sigma)}$. Here ${}_p\psi$ is the p-cyclotomic character. So, suppose $\mathcal{H}_2$ is another component of $\mathcal{H}$. If $1 \notin \nu(\mathcal{H}_2)$ and $1 \in \nu(\mathcal{H}_1)$, then $\mathcal{H}_1$ and $\mathcal{H}_2$ aren't conjugate. Part II applies in §III.D to show we can compute information about ν.

§III.F has a criterion that guarantees every level of a modular tower has a $\mathbb{Q}$ absolutely irreducible component. This gives a second approach to detecting $\mathbb{Q}$ components. The example criterion introduces H(arbater)M(umford) representatives in a Nielsen class. This is the most practical criterion we have. It, however, applies less often than does the lifting invariant. Part IV relates the lifting invariant and generalizations of HM representatives.

[**IM**] produces a section β to the natural map from the arithmetic fundamental group of $\mathbb{P}^r \setminus D_r$ to $G_{\mathbb{Q}}$. Any such section gives an an action of $G_{\mathbb{Q}}$ (faithful, in this case) on the profinite completion of $\mathbb{P}^r \setminus D_r$ with respect to all subgroups of finite index. The latter group identifies with the pro-finite *Hurwitz monodromy group*. Different sections β, however, give different actions. [**IM**] uses a Deligne *Tangential Basepoint* to create a section with valuable properties. In particular, it identifies this action with the embedding of $G_{\mathbb{Q}}$ in the Grothendieck-Teichmüller group, $\widehat{\mathcal{G}T}$.

There is speculation $\widehat{\mathcal{G}T}$ might contain $G_{\mathbb{Q}}$ as an open subgroup. Parts IV and V consider the action of $\widehat{\mathcal{G}T}$ on components of modular towers at each level. The conjectured $\widehat{\mathcal{G}T}$-$G_{\mathbb{Q}}$ relation gives results for $G_{\mathbb{Q}}$ action on components of the modular towers. Part IV gives meaning to the statement that $\widehat{\mathcal{G}T}$ preserves the lifting invariant. As a prelude, §App.C reinterprets the criterion of [**DFr2**] for describing all real points on a Hurwitz space. This resembles the construction of the [**IM**] section. So, it lets us compare their $G_{\mathbb{Q}}$ action with the lifting invariant. This is appropriate because both limit the action of $G_{\mathbb{Q}}$ on Hurwitz space components.

This material also supports a companion topic, *real points on modular towers* (§App.D). This interprets existence of a projective system of real points on a given modular tower. Other groups appear here, natural for the problem at hand, yet not the universal frattini cover. In this case, it is the *universal Artin-Schreier cover* of a finite group G' equipped with a collection of conjugacy classes of involutions. Constructions in [**H**] are a forerunner. This shows the value of going beyond the elementary elegance of the p-unramified case of modular towers in this paper. (Part IV, in particular, computes a low level quotient of the 2-ramified invariant of L. Schnepp's 3-branch point cover of degree 20.) This is one from the summary of problems in the Appendix. Many of these problems belong to modular representations. Part IV compares this with the generators and relation presentation of $\widehat{\mathcal{G}T}$.

Part V concentrates on the diophantine topics from this list. For these we consider especially how to apply results of G. Faltings (say, using G. Frey's Finite Field Principle as in Theorem 1.1) and H. Nakamura (as in [**Na**, Thm. 2.3.1]). Every finite group G is a Galois group of a regular extension of $\mathbb{F}_p(x)$ for almost all primes p [**FrV**]. §App.E gives an explicit bound on the exceptional primes to this statement for a specific group G. A realizing cover for a given group G has an associated *Nielsen class*. This comes from the conjugacy classes of the r branch points of the realizing extension. We state our result depending on the Nielsen class of the realization. It is possible to get a statement bounding these primes, dependent only on G. Still, this reduces the structure in the problem. While we believe this result new, for the aspirations of this paper, it is inadequate. We accept the primes dividing $|G|$ as exceptional. Assume p does not divide $|G|$. Our test produces an infinite number of varieties over every finite field. One $\mathbb{F}_p$ point on any one of them gives a regular realization of G. Further, there's the tower above the lowest level (on each one). It is a waste to apply the standard Riemann hypothesis estimate to this situation. The curves of statement D_1 (below) motivate going far beyond this limited result. Our introduction concludes with two structured, yet opposed, diophantine themes.

D_1: Non-congruence subgroup curves. *Non-congruence* subgroup curves are an entertaining place to apply the above diophantine discussion. These are quotients of the upper half (complex) plane by a subgroup Γ of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index. (Technically, Γ shouldn't contain a congruence subgroup to deserve the non-congruence appellation.) Suppose Γ is a subgroup of the congruence subgroup $\Gamma_0(2)$. Then, ([**Fr4**] or [**Fr7**]) *every* such curve appears in the pullback to $(\mathbb{P}^1)^4$ of a component of a Hurwitz space of four branch point covers (see Problem (B.2) of §App.B). Thus, to each, §III.C associates a modular tower. This view offers chances to reconsider the special role of modular curves. These are curves. So, we need no extra machinery likely necessary to consider diophantine questions in full generality on modular towers. We don't yet know, for example, what is the analog of Theorem 1.1 for these non-congruence modular towers.

D_2: Changing the number of branch points. Classical diophantine topics are primarily limitation results. No problem suggested by this paper has more appli-

cations than producing rational points on Hurwitz spaces $\mathcal{H}(G,\mathbf{C})^{\rm in}$ or $\mathcal{H}(G,\mathbf{C})^{\rm ab}$ (§III.A) where $\mathbf{C}$ has many repetitions of conjugacy classes. [**FrV**] and [**FrV2**] show this would give much more than the inverse Galois problem; much more than Shafarevich's conjecture. This is part of the $(G,\hat{G},\mathbf{C})$-realization topic in §I.D. The $(D_p,\mathbb{A}_p,\mathbf{C}_{p+1})$-Lemma gives a success here. It produces the analog for suitably large genus hyperelliptic curves of $\mathbb{Q}$ non-cusp points on $X_0(p)$. (beginning of §App.D).

§I.C. Notation. Suppose x is an indeterminate over a perfect field F. An extension $L/F(x)$ is *regular* if $\bar{F}\cap L=F$ where $\bar{F}$ denotes the algebraic closure of F. Such an extension has *branch points*: values $x_1,\dots,x_r$ of x with fewer than $[L:\mathbb{Q}(x)]=n$ places of L lying over the place of $F(x)$ corresponding to the specialization $x\mapsto x_i$ (§I.F). Let $\hat{L}$ be the Galois closure of the extension $L/F(x)$. Suppose the extension is *tamely ramified*, say, as when the characteristic of F is 0. Then, associate a cyclic subgroup $\langle\sigma_i\rangle$ to each place $\boldsymbol{p}_i$ of $\hat{L}$ lying over x_i. The *ramification index* of x_i is the minimal integer e_i for which $\hat{L}$ embeds in the formal Laurent series field $\bar{F}(((x-x_i)^{1/e_i}))$.

Let ζ_e be a primitive e-th root of 1. Assume $\{\zeta_e \mid e=1,2,\dots\}$ forms a compatible system: $\zeta_{e_1e_2}^{e_2}=\zeta_{e_1}$. In characteristic 0 choose $\zeta_e=e^{2\pi i/n}$. Denote formal Laurent series in x over a field F by $F((x))$. From this define an automorphism σ of $\bar{F}(((x-x_i)^{1/e_i}))$ fixed on $\bar{F}$ that maps $(x-x_i)^{1/e_i}$ to $\zeta_{e_i}(x-x_i)^{1/e_i}$. Then, σ_i is restriction to $\hat{L}$ of σ. The collection $\sigma_1,\dots,\sigma_r$ is a *description of the branch cycles* of the cover when the following hold. First: $\sigma_1,\dots,\sigma_r$ generate $G=G(\bar{F}\hat{L}/\bar{F}(x)$, the *geometric* monodromy group of $L/F(x)$. Second: The product of $\sigma_1,\dots,\sigma_r$, in some order, is 1. §I.F has more on Riemann's existence theorem: production of covers from branch cycles.

The varieties of this paper are either affine or projective. For example, Hurwitz spaces are affine varieties. (Don't, however, expect to see equations for them.) Suppose Y is an algebraic variety (an irreducible locally closed subset of projective space) defined over a field F. (It may not be *absolutely irreducible*: over the algebraic closure, $\bar{F}$, Y may have several components.) Denote the field generated by coordinates of a point $\boldsymbol{p}\in Y$ by $F(\boldsymbol{p})$. In particular, if $\boldsymbol{p}$ is a (Weil) generic point of Y, then $F(\boldsymbol{p})$ is the function field of Y. Let $\phi: X\to Y$ be a finite cover. Further, suppose X and Y are *normal varieties*, and ϕ and the varieties have F as a field of definition. Let $\mathrm{Aut}_F(X/Y)$ denote the algebraic isomorphisms $\psi: X\to X$ defined over F with $\phi\circ\psi=\phi$ when applied to the points of X. We say ϕ is a *Galois cover* when the order of $\mathrm{Aut}_F(X/Y)$ equals the degree of ϕ. For any (separable) cover, $\phi: X\to Y$, over F, §I.G does a fiber product construction of the Galois closure over F. This is the minimal Galois cover of Y, defined over F, factoring through X. The group of this cover is the *arithmetic* monodromy group of $\phi: X\to Y$. The corresponding cover and group over $\bar{F}$ is the *geometric* monodromy group. If $\tau\in G_F$, then Y^τ is the variety you get by applying τ to coefficients of polynomials giving Y. In the next section $\mathbb{F}_q$ is the finite field of order q.

§**I.D. Motivating problems.** This section discusses two example problems. They interpret points on modular curves as realization of certain pairs of groups as (arithmetic and geometric) monodromy groups of a cover. More formally, let G and $\hat{G}$ be transitive subgroups of S_n for some integer n, with G normal in $\hat{G}$. Further, consider $(G, \hat{G}, \mathbf{C})$ where $\mathbf{C}$ is a collection of r conjugacy classes (with possible repetitions) of G.

DEFINITION. $(G, \hat{G}, \mathbf{C})$*-realizations.* Let $L/F(x)$ be a regular *tame* extension. We say it is a $(G, \hat{G}, \mathbf{C})$-realization under the following conditions.

(c_1) $L/F(x)$ has arithmetic monodromy group $\hat{G}$.
(c_2) $\bar{F}L/\bar{F}(x)$ has geometric monodromy group G.
(c_3) Branch cycle descriptions of $L/F(x)$ have attached conjugacy classes $\mathbf{C}$.

Problem statements.

A. Involution realizations of dihedral groups as regular extensions over $\mathbb{Q}$ [**DFr**, §5.1-5.2].
B. Production of *median value curves*—projective nonsingular curves C over $\mathbb{F}_q$—with exactly q^t+1 points over $\mathbb{F}_{q^t}$ for infinitely many t. [**Fr1**, §3]

Problem A: $(D_p, D_p, \mathbf{C}_r)$*-realizations;* $\mathbf{C}_r$ *being* r *repetitions of the class of involutions.* Problem A comes from [**DFr**]. Let p be an odd prime. It is easy to realize the dihedral groups D_{p^n} as regular extensions $L/\mathbb{Q}(x)$ over $\mathbb{Q}$. Known ways, however, require many branch points—at least $p^n - p^{n-1} + 1$—for primes p larger than 7. It is *impossible* to get fewer branch points in a $\mathbb{Q}$ regular realization unless all the branch cycles are involutions. When $r = 4$, such *involution realizations* correspond to $\mathbb{Q}$ non-cusp points on the modular curves classically called $X_1(p^n)$ [**DFr**, Theorem 5.1]. Here is why for the case $n = 1$.

Suppose $L/\mathbb{Q}(x)$ is a degree p regular extension ramified at $r = 4$ points. Further, assume its Galois closure is an involution realization of D_p. Apply the Riemann-Hurwitz formula to $L/\mathbb{Q}(x)$. Since $r = 4$, the genus $g(L)$ of L is 0:

$$2([L:\mathbb{Q}(x)] + g(L) - 1) = 4([L:\mathbb{Q}(x)] - 1)/2$$

with $[L:\mathbb{Q}(x)] = p$. This is because involutions in the degree p representation fix one integer, and switch $(p-1)/2$ others in pairs. The Galois closure, however, is the regular function field $\hat{L}$ of a genus 1 curve $\hat{X}$. Further, the automorphisms—also defined over $\mathbb{Q}$—have among them one, say α, of order p. Consider the quotient $\hat{X}/\langle\alpha\rangle$ of $\hat{X}$ by the group α generates. The degree p map $\hat{X} \to \hat{X}/\langle\alpha\rangle$ is unramified. While $\hat{X}$ and $\hat{X}/\langle\alpha\rangle$ may not have rational points, their jacobians, elliptic curves, do. Further, the genus 0 function field L, of odd degree over $\mathbb{Q}(x)$, must be $\mathbb{Q}(x')$ for some transcendental x'. This is the classical Hilbert-Hurwitz argument. In summary: The original extension has form $\mathbb{Q}(x')/\mathbb{Q}(x)$, arising from a rational function $f(x') = x$. Trace f to an isogeny of degree p from a rational p-division point on an elliptic curve [**Fr1**, §3].

This isogeny produces a $\mathbb{Q}$ rational non-cusp point on $X_1(p^n)$: the moduli space of pairs of elliptic curves with a p-division point. Mazur's Theorem says such rational points don't exist if $p > 7$ [**M**]. Thus, for $r = 4$ and $p > 7$ there is no regular realization of D_p as a Galois group. Let r_0 be any integer. A conjecture of [**DFr**] states: Only finitely many values of p^n produce regular realizations of D_{p^n} with fewer than r_0 branch points.

This conjecture, however, doesn't properly reveal our ignorance on involution realizations of D_{p^n}. We suspect there *exist* many involution realizations of D_{p^n} over $\mathbb{Q}$. F. Leprévost suggested an example that isn't an involution realization of D_p. Still, it is close. Further, it helps us explain why variants on the pair $X_0(p^n)$ and $X_1(p^n)$ appear throughout the modular tower theory (as in Problem D.1 of §App.D).

Consider the Fermat curve W, complete and nonsingular, with associated affine set $\{(u, v) \mid u^p + v^p = 1\}$. As usual, p is an odd prime. Take Z to be the hyperelliptic curve with associated affine set $\{(x, y) \mid y^2 = 4x^p + 1\}$: $\psi : Z \to \mathbb{P}^1_x$ is the canonical degree 2 cover.

The genus of W is $g(W) = (p-1)(p-2)/2$ and $g(Z) = (p-1)/2$. Consider $\phi : W \to Z$ by $\phi(u, v) = (x, y)$ with $x = -uv$ and $y = u^p - v^p$: $(u^p - v^p)^2 = 4(-uv)^p + 1$. To simplify notation denote the semi-direct product $\mathbb{Z}/p \times^s (\mathbb{Z}/p)^*$ (multiplication action of $(\mathbb{Z}/p)^*$ on $\mathbb{Z}/p$) by $\mathbb{A}_p$. With C the conjugacy class of involutions in D_p, let $\mathbf{C}_r$ be r repetitions of C.

Lemma: $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization over $\mathbb{Q}$. *The morphism ϕ is of degree p, unramified and defined over $\mathbb{Q}$. The cover $\phi' = \psi \circ \phi : W \to \mathbb{P}^1_x$ is a $(D_p, \mathbb{A}_p, \mathbf{C}_{p+1})$-realization over $\mathbb{Q}$.*

Proof. Write $u + v = u + x'/v$, subject to relations $u^p + v^p = 1$ and $x = -uv = -x'$. Part A below shows properties of a polynomial $T_p(z) \in Q[x, z]$. It is of degree p in z, and $T_p(u+x'/u) = u^p+(x'/u)^p$. Further, $T_p(z)-1$ is (absolutely) irreducible as a polynomial in $\mathbb{Q}[x, z]$. Conclude: $L = Q(x', u+x'/u)$ is a degree p extension of $\mathbb{Q}(x)$. Now, $F = \mathbb{Q}(u, v)$ is a degree 2 extension of L. Also, $K = Q(x, y)$ is a degree 2 extension of $\mathbb{Q}(x)$, contained in L. Apply transitivity of degrees to compute that F is a degree p extension of K. There remain three parts: construction of T_p; computing a Galois closure; and concluding remarks.

Part A: How to get T_p. There exists an odd polynomial C_p giving the relation $C_p(t + 1/t) = t^p + 1/t^p$. Indeed, choose C_p from DeMoivre's formula:

$$e^{i\theta p} = (\cos(\theta) + i\sin(\theta))^p = \cos(p\theta) + i\sin(p\theta). \tag{†}$$

Take real parts of both sides, and re-express $\sin^2$ as $1 - \cos^2$. This gives H_p satisfying $H_p(\cos(\theta)) = \cos(p\theta)$. Write $C_p(z) = 2H_p(z/2)$. Since $C_p(t + 1/t) = t^p + 1/t^p$ for all t of form $e^{i\theta}$, it holds for all t. Exchange θ for $-\theta$ to see C_p is an odd polynomial: $C_p(-x) = -C_p(x)$.

Now, make a substitution: $t = u/a$, or

$$C_p(u/a + a/u) = C_p(1/a(u + a^2/u)) = 1/a^p(u^p + a^{2p}/u). \tag{‡}$$

Let $a^2 = x'$. Since C_p is an odd polynomial, deduce this gives T_p. Finally, we show $T_p(z) - 1$ is irreducible. By construction, the leading term of $T_p(z) - 1$ is $(p+1)z^p$: from the coefficient of $\cos^p$ in

$$\cos^p + p(\cos^{p-2})(-\sin^2) = (p+1)\cos^p + p\cos^{p-2}.$$

Excluding the lead and constant terms, the other coefficients of $T_p(z) - 1$ have a positive power of x as a factor. As p is a prime, if $T_p(z) - 1$ factors, it must have proper factors with coefficients in $\mathbb{Q}[x]$. Now specialize x to 0 to conclude $(p+1)z^p - 1$ has proper factors over $\mathbb{Q}$. This is clearly false.

Part B: Properties of the Galois closure of $L/\mathbb{Q}(x)$. Let $\hat{L}$ be the Galois closure of the extension of $L/\mathbb{Q}(x)$. A trick simplifies this. Adjoin $x^{\frac{1}{2}}$ to L. Then, $L(x^{\frac{1}{2}}) = \mathbb{Q}(x^{\frac{1}{2}}, u+v) = Q((1/x^{\frac{1}{2}})(u+v), x^{\frac{1}{2}})$. From (‡), the splitting field of $L(x^{\frac{1}{2}})/\mathbb{Q}(x^{\frac{1}{2}})$ is the splitting field of $C_p(z) - (1/x^{\frac{1}{2}})^p$ over $\mathbb{Q}(x^{\frac{1}{2}})$. Let $t + 1/t = z$ and $s = (1/x^{\frac{1}{2}})^p$. Then, the splitting field $\Omega_{C_p - s}$ of $C_p(z) - s$ over $\mathbb{Q}(s)$ is $\mathbb{Q}(\zeta_p^i t + 1/(\zeta_p^i t), i = 0, \dots, p-1)$. Add $\zeta_p^i t + 1/(\zeta_p^i t)$ to its complex conjugate to see $\cos(2\pi/p)(t+1/t)/(t+1/t) = \cos(2\pi/p)$ is in Ω_{C_p-s}.

Thus, $\mathbb{Q}(\cos(2\pi/p)$ is the extension of constants (see §I.E) from going to the Galois closure of $\mathbb{Q}(z)/\mathbb{Q}(s)$: $\Omega_{C_p-s} = \mathbb{Q}(t+1/t, \zeta_p t + 1/(\zeta_p t), \cos(2\pi/p))$. The Galois group $G(\Omega_{C_p-s}/\mathbb{Q}(s))$ is $\mathbb{A}_p$, and the geometric monodromy group is D_p. Adjoin $i = \sqrt{-1}$ to the splitting field of $C_p(z) - s$ over $\mathbb{Q}(x^{\frac{1}{2}})$ to get $\mathbb{Q}(t, \zeta_p, x^{\frac{1}{2}}) = L'$. As $t + x'/t$ is in this field, take $t = u$ to see L' contains F. Do the remainder of the lemma by working in L'.

Part C: Comments on the proof. This example centered on the cover of the x-line defined by $C_p(z) - x^p = 0$. All other covers come from pullback of this one, which had geometric monodromy group D_p. For this cover, ramification over ∞ is a p-cycle. Pulling this back over a cover ramified of order p over ∞ gives an involution realization. Still, the real subfield of $\mathbb{Q}(\zeta_p)$ appears in the Galois closure. $\square$

Earlier we found that a $(D_p, D_p, \mathbf{C}_4)$-realization over $\mathbb{Q}$ produces a non-cusp $\mathbb{Q}$ point on $X_1(p)$. Similarly, for $D_p \triangleleft \hat{G} \le S_p$. Finding a $(D_p, \hat{G}, \mathbf{C}_4)$-realization over $\mathbb{Q}$ produces a non-cusp $\mathbb{Q}$ point on $X_0(p)$.

§App.D and §App.E explain natural diophantine generalizations to every finite group G, prime p dividing the order of G, and collection of conjugacy classes of G. Suppose the conjugacy classes of G are of elements of orders relatively prime to p. Then, we construct a *tower* of varieties from the Hurwitz spaces $\mathcal{H}(G, \mathbf{C})^{\mathrm{ab}}$. This generalizes the tower $X_0(p) \leftarrow X_0(p^2) \cdots$. (The analog of $X_1(p) \leftarrow X_1(p^2) \cdots$ is from the Hurwitz spaces $\mathcal{H}(G, \mathbf{C})^{\mathrm{in}}$.) This also produces a $G_{\mathbb{Q}}$ invariant of the *braid group orbit* of any curve cover (§III.D). Now we turn to Problem B.

Problem B: $(G, \hat{G}, \mathbf{C})$-realizations over finite fields. Let $\mathbb{F}_q$ be the finite field of order q. Suppose a pair of groups $(G, \hat{G})$ is the respective geometric/arithmetic monodromy group pair of an extension $L/\mathbb{F}_q(x)$. (Assume, also, G has no center.) Necessary conditions are

(a) $G \triangleleft \hat{G}$, $\hat{G}/G$ is cyclic, and
(b) no element of $\hat{G} \setminus G$ centralizes G [**Fr5**, Prop. 2].

Then, [**Fr1**, Th. 2.5] shows this converse.

THEOREM: G/A MONODROMY EXISTENCE OVER FINITE FIELDS. *$(G, \hat{G})$ is the geometric/arithmetic monodromy group pair of a regular extension $L/\mathbb{F}_{p'}(x)$ for all but finitely many primes p'.*

§App.E bounds exceptional primes to this statement. Still, as in §I.B, there is so much structure here, it behooves us to toss Lang-Weil estimates. We explain with the special case $G = D_p$, and $\hat{G}$ is a proper overgroup normalizing G. These produce examples of median value curves sought by Problem B.

Construction of *exceptional covers* is a recurrent application. These give function field extensions $L/\mathbb{F}_q(x)$ where each $x \in \mathbb{F}_{q^t} \cup \{\infty\}$ has exactly one $\mathbb{F}_{q^t}$ place of L above it for infinitely many t.

EXCEPTIONALITY STATEMENT [**Fr1–3**]. *Regular extension $L/\mathbb{F}_q(x)$ is exceptional exactly when each orbit of $\hat{G}(1)$ acting on $\{2, \dots, n\}$ breaks into strictly smaller orbits under $G(1)$. Equivalently: If $(t, |\hat{G}/G|) = 1$, each $x \in \mathbb{F}_{q^t} \cup \{\infty\}$ has exactly one $\mathbb{F}_{q^t}$ place of L above it.*

The unique nonsingular projective curve, up to isomorphism, with function field L, is a *median value curve*. It has exactly $q^t + 1$ rational points in $\mathbb{F}_{q^t}$ for infinitely many t. Potential applications of median value curves require explicit realizations of them.

Take $q = r^a$ for some odd prime $r \neq p$. [**Fr1**, Cor. 3.5] produces genus 0 exceptional covers of degree p. Reduce $X_0(p)$ modulo r. Call this $X_0(p)^{(r)}$. You get one of these degree p rational functions over $\mathbb{F}_q$ for each $\mathbb{F}_q$ point of $X_0(p)^{(r)}$ with nontrivial frobenius in the cover $X_1(p)^{(r)} \to X_0(p)^{(r)}$ (see §I.E). We don't know of refined estimates for such points on $X_0(p)^{(r)}$. Still, Lang-Weil applied to twists of modular curves is not the right tool. Over $\mathbb{F}_{p^2}$ we could use the same supersingular curves that appear in the proof of Theorem 1.1. Complex multiplication (as [**Fr4**] notes) precisely describes this problem. Again, these ideas generalize. The variant question in Theorem 1.1 is the production of such rational functions f over number fields that reduce modulo infinitely many primes to these examples.

§I.E. Exact Constants Sequence. Suppose $L/F(x)$ is a regular extension with Galois closure $\hat{L}$. This gives an exact sequence

$$1 \to G(\hat{L}/\hat{F}(x)) \to G(\hat{L}/F(x)) \to G(\hat{F}/F) \to 1. \tag{1.1}$$

Consider realizing a group G as a Galois group of a regular extension of F. We might want the first term of (1.1) to be G and $G(\hat{F}/F)$ to be 1. Recognize $\hat{F}$ as the smallest extension of F containing the constants of a Galois closure of

$L/F(x)$. Especially, the functions giving the automorphisms of the extension have field of definition $\hat{F}$. For other applications, including Problems A and B, $G(\hat{F}/F)$ should be as large as possible. Either way, we need to know the possibilities for $G(\hat{F}/F)$. With $\hat{G} = G(\hat{L}/F(x))$ this is the topic of $(G, \hat{G})$-realizations over a field F: we've dropped explicit dependence on $\mathbf{C}$.

For example, again take $G = D_p$ with p an odd prime. Let F be an algebraic number field: $[F : \mathbb{Q}] < \infty$. Suppose $L/F(x)$ is of degree p, with geometric monodromy group D_p. Since $G(\hat{L}/F(x))$ is in S_p, §I.D shows the largest group it can be is $\mathbb{A}_p$.

Suppose the extension has involutions as branch cycles and there are $r = 4$ branch points. If it's not an involution realization of D_p, then $\hat{F} \neq F$. From §I.D, the extension gives a rational function f with $f : \mathbb{P}^1 \to \mathbb{P}^1$ an exceptional cover for infinitely many primes $\boldsymbol{r}$ of the number field F. To be precise, let $\mathbb{F}_{\boldsymbol{r}}$ be the residue class field of $\boldsymbol{r}$.

Assume $\boldsymbol{r}$ does not divide p where f reduces to a rational function $f_{\boldsymbol{r}}$ of degree p. Let $\Omega_{f_{\boldsymbol{r}}}$ be the splitting field of $f_{\boldsymbol{r}}(y) - x$ over $\mathbb{F}_{\boldsymbol{r}}(x)$. With care, we can assure there is a corresponding sequence to (1.1):

$$(1.2) \qquad 1 \to D_p = G(\Omega_{f_{\boldsymbol{r}}}/\hat{\mathbb{F}}_{\boldsymbol{r}}(x)) \to G(\Omega_{f_{\boldsymbol{r}}}/\mathbb{F}_{\boldsymbol{r}}(x)) \to G(\hat{\mathbb{F}}_{\boldsymbol{r}}/\mathbb{F}_{\boldsymbol{r}}) \to 1.$$

Let $\mathcal{T}_F$ be the primes of F whose frobenius element in the extension $\hat{F}/F$ is nontrivial. For almost all $\boldsymbol{r} \in \mathcal{T}_F$ the Exceptionality Statement (§I.D) shows $f_{\boldsymbol{r}}$ to be an *exceptional rational function* [**Fr4**, §4]. So, now we look at how abundant are these fields F producing such rational functions f.

Follow classical terminology. Write $\mathbb{Q}(X_0(1)) = \mathbb{Q}(j)$ with j the j-invariant of the generic elliptic curve over $\mathbb{Q}$. Results of Faltings give a goal for concise statements on the diophantine properties of modular towers. The analog of $\mathbb{A}_p$ for D_{p^n} is $\mathbb{A}_{p^n} = \mathbb{Z}/p^n \times^s (\mathbb{Z}/p^n)^*$.

THEOREM 1.1. *Let p be any odd prime and n a positive integer. An infinity of $\boldsymbol{x} \in X_0(p^n)(\bar{\mathbb{Q}})$ produce a $(D_{p^n}, \mathbb{A}_{p^n}, \mathbf{C}_4)$-realization over $F = \mathbb{Q}(\boldsymbol{x})$. Suppose, however, we fix F. Then, for p^n large, only finitely many $\boldsymbol{x} \in X_0(p^n)$ have coordinates in F. Even stronger, fix an integer d. Assume p^n large (dependent on d). Only finitely many $\boldsymbol{x} \in X_0(p^n)$ have coordinates in a field of degree at most d over $\mathbb{Q}$.*

PROOF. For the first part apply Hilbert's irreducibility theorem (HIT), done as follows for this point in [**Fr4**]. The extension $\mathbb{Q}(X_1(p^n))/\mathbb{Q}(X_0(p^n))$, has degree $p^{n-1}(p-1)/2$. Pick a specialization ν of $\mathbb{Q}(X_1(p^n))$ over $j_0 \in \mathbb{Q}$. Let its residue class field be $\hat{F}$. Let the residue class field of restriction of ν to $\mathbb{Q}(X_0(p^n))$ be F. From HIT, $[\hat{F} : F]$ has degree $p^{n-1}(p-1)/2$ for infinitely many $j_0 \in \mathbb{Q}$. Conclude from the discussion of §I.D.

Now for the second part where we fix F. The classical Riemann-Hurwitz computation for $X_0(p^n)$ (as a cover of the j-line) shows its genus grows large with p^n. Apply Faltings' Theorem: Over any number field F, a curve of genus exceeding 1 has only finitely many F points.

Consider the statement on bounding the values p^n for which $X_0(p^n)$ has infinitely many points over fields F with $[F:\mathbb{Q}] \le d$. This is from [**F**, Cor. 2]. Frey's argument was for p, but applies to p^n. The conclusion of the theorem holds for $p^n > 120d$ using [**Fa2**] and a subtle finite field argument.

Let W_d be the d-th symmetric product of $X_0(p^n)$ in its Picard component of degree d. Suppose W_d contains an infinite number of F rational points. Then, [**Fa2**] says W_d contains the translate of an abelian variety. Further, $\mathbb{Q}$ is a field of definition for the translating divisor, the abelian variety and infinitely many of its points. [**F**, Cor. 2] concludes with 2-steps. First: It shows this implies there is a cover $\phi : X_0(p) \to \mathbb{P}^1$, over $\mathbb{Q}$, of degree no more than $2d$. This argument is general, having nothing to do with modular curves. Reducing this situation modulo a prime $\boldsymbol{r} \neq p$ produces $\phi_{\boldsymbol{r}} : X_0(p^n)^{(\boldsymbol{r})} \to \mathbb{P}^1$ (as in §I.D), with $\phi_{\boldsymbol{r}}$ of degree at most $2d$. Such a reduction is possible; Frey quotes Deuring's reduction theory results. Now we come to the final argument.

Take any finite field $\mathbb{F}'$ containing $\mathbb{F}_{\boldsymbol{r}}$. Existence of $\phi_{\boldsymbol{r}}$ bounds $X_0(p^n)(\mathbb{F}')$ independently of p^n by $(|\mathbb{F}'|+1)2d$. Take, however, $\boldsymbol{r}=2$, and $\mathbb{F}'$ the quadratic extension of $\mathbb{F}_{\boldsymbol{r}}$. Then, [**I2**] (or [**R**, pgs. 226–239]) shows $X_0(p)(\mathbb{F}')$ has at least $\left[\frac{p^n}{12}\right]+1$ points. These points derive from *supersingular elliptic curves* for the prime 2. Supersingular curves have defining field the quadratic extension of $\mathbb{F}_2$. This contradiction gives explicit bounds on exceptional values of p^n. □

§I.F. Algebraist's version of Riemann's existence theorem. Consider an extension $L/\mathbb{C}(x)$ of degree n. Suppose its Galois closure $\hat{L}/\mathbb{C}(x)$ has group G. Then, $G(\hat{L}/\mathbb{C}(x))$ faithfully embeds in S_n. The image is unique up to conjugation by an element of S_n.

For any $x' \in \mathbb{C} \cup \{\infty\}$, consider the formal Laurent series $\mathbb{C}((x-x'))$ in $x-x'$. Replace $x-x'$ by $1/x$ if $x'=\infty$. The algebraic closure of $\mathbb{C}((x-x'))$ is $\cup_{e=1}^{\infty}\mathbb{C}(((x-x')^{\frac{1}{e}}))$. Thus, the absolute Galois group of $\mathbb{C}((x-x'))$ is pro-cyclic. Its generator $\sigma_{x'}$ has the effect $(x-x')^{\frac{1}{e}} \mapsto \zeta_e(x-x')^{\frac{1}{e}}$, $e=2,3,\dots$. Here $\zeta_e = e^{2\pi i/e}$. There is a minimal integer e with $\hat{L}$ embedding in $\mathbb{C}(((x-x')^{\frac{1}{e}}))$ as the identity on $\mathbb{C}(x)$. Compose any one embedding $\psi_{x'} : \hat{L} \to \mathbb{C}(((x-x')^{\frac{1}{e}}))$ with an automorphism of $\hat{L}$, to get any other. Therefore, restriction of $\sigma_{x'}$ to $\hat{L}$ defines a conjugacy class of elements in $G(\hat{L}/\mathbb{C}(x))$.

Only finitely many x' have $e=e_{x'}>1$. Label these $\boldsymbol{x}=(x_1,\dots,x_r)$, the *branch points* of the cover. For embeddings ψ attached to these points, name the corresponding automorphisms by $\boldsymbol{\sigma}=(\sigma_1,\dots,\sigma_r)$. Let e_i be the e attached to x_i: the *ramification index* at x_i.

Riemann's Existence Theorem. *For some choice of ψ s,*

(i) $\sigma_1 \cdots \sigma_r = 1$, *and*
(ii) *the σ_i s generate G.*

Conversely, suppose $x_1,\dots,x_r$, and $\sigma_1,\dots,\sigma_r \in S_n$ satisfy (i) *and* (ii) *with G transitive in S_n. Then, there exists $L/\mathbb{C}(x)$ producing this data as above.*

§I.G. Geometric Galois closure. Riemann's existence theorem gives topological existence to the covers of $\mathbb{P}^1$. It is, however, harder to see the relation between a cover and its automorphisms. For example, if a field F is the field of definition of a cover, what is the defining field of the cover's Galois closure?

The Galois closure construction (below) reduces finding the field of definition of automorphisms to finding a connected component of a curve. It is a form of Kronecker's old construction of the Galois group of a polynomial. Its use of fiber products lends itself to forming Galois closures of families of covers.

Consider a cover $\phi : X \to \mathbb{P}^1$ of degree n. Assume X is absolutely irreducible. Suppose F is a field of definition of the cover. Form the fiber product of the curve with itself n times. This is $X^n_{\mathbb{P}^1}$, n-tuples from X whose coordinates have a common image under ϕ. Remove an obvious set of components where two or more coordinates are equal, the *fat diagonal* Δ. Denote $X^n_{\mathbb{P}^1} \setminus \Delta$ by $X_1^{(n)}$. Note: S_n acts as permutations of the coordinates of $X_1^{(n)}$. Normalize this curve so the result is complete and nonsingular. It may not be absolutely irreducible. Still call this $X_1^{(n)}$. Let $\hat{X}$ be an F-connected component of $X_1^{(n)}$. Projection on the first coordinate gives a map

$$\hat{\psi} : \hat{X} \to X \xrightarrow{\phi} \mathbb{P}^1. \tag{1.3}$$

THEOREM: GALOIS CLOSURE CONSTRUCTION. *The cover $\phi \circ \hat{\psi} : \hat{X} \to \mathbb{P}^1$ is the Galois closure of ϕ over F. The group of $\hat{X} \to \mathbb{P}^1$ is the subset of S_n that leaves $\hat{X}$ invariant.*

PROOF. We derive this from the function field use of Galois theory. The curves in the cover are normal. Therefore, elements of $\mathrm{Aut}(\hat{X}/\mathbb{P}^1)$ correspond to automorphisms of $F(\hat{X})/F(x)$ where x uniformizes $\mathbb{P}^1$. Let α be a primitive element for the field extension $F(X) = F(\alpha, x)$ over $F(x)$.

Conjugates $\alpha_1, \dots, \alpha_n$ of α over $F(x)$ correspond to points of X over the generic point x on $\mathbb{P}^1$. Thus, there is a one-one relation between points of $X_1^{(n)}$ over x and different n-tuples

$$\{(\alpha_{\pi(1)}, \dots, \alpha_{\pi(n)}), \pi \in S_n\}.$$

Let $\hat{\boldsymbol{p}} = (\boldsymbol{p}'_1, \dots, \boldsymbol{p}'_n)$ be a generic point of $\hat{X}$ over x: the $\boldsymbol{p}'$s are an ordering of the points of X over x. Let $\hat{G}$ be the group of the Galois closure of $F(X)/F(x)$. This has an orbit on ordered n-tuples of conjugates of α. Conjugates of $\hat{\boldsymbol{p}}$ are permutations of the entries of $\hat{\boldsymbol{p}}$. Further, such conjugates are exactly the points of $\hat{X}$ over x. Conclude: $\hat{X}/\mathbb{P}^1$ is Galois. Its automorphisms are permutations of $\alpha_1, \dots, \alpha_n$ by $\hat{G}$. □

PART II. UNIVERSAL FRATTINI COVERS

The *rank* of a profinite group G is the minimal number of elements that topologically generate G. Again, D_n is the dihedral group of order $2n$. For

$G \le H$ groups and M a representation module for G, $\mathrm{ind}_G^H(M)$ is the induced representation module for H. This is G-equivariant functions from H into M:

$$\{f \in \mathrm{Maps}(H,M) \mid g(f(h)) = f(gh),\ g \in G, h \in H\}.$$

§II.A. Universal p-frattini cover of a finite group G.

The profinite limit

$$\lim_{\infty \leftarrow n} D_{p^n} = D_{p^\infty} = {}_p\tilde{G} = \mathbb{Z}_p \times^s \mathbb{Z}/2$$

collects the finite groups D_{p^n} for all integers n. This section discusses the analog of this for any finite group G and any prime p dividing $|G|$. For later reference replace D_{p^∞} by ${}_p\tilde{G}$ and D_p by G.

Recover finite quotients of ${}_p\tilde{G}$ through the frattini kernel of the natural map $\ker \to {}_p\tilde{G} \to G$. This produces a sequence of characteristic subgroups of ${}_p\tilde{G}$:

$$\text{(2.1)}\quad \ker = \ker_0,\ \ker_0^p[\ker_0,\ker_0] = \ker_1, \dots, \ker_{n-1}^p[\ker_{n-1},\ker_{n-1}] = \ker_n, \dots$$

As usual, we understand $\ker_{n-1}^p[\ker_{n-1},\ker_{n-1}]$ to be the closed subgroup of ${}_p\tilde{G}$ with generators from the elements of this set. The quotient ${}_p\tilde{G}/\ker_n$ is $D_{p^{n+1}}$. Since ker is $p\mathbb{Z}_p$, commutators $[\ker_n,\ker_n]$ here are trivial. They won't be in the general case. Summarizing [**FrJ**, §20.7], we explain how this applies to the universal frattini cover of any finite group G.

A *frattini cover* is a surjective homomorphism $\psi : H \to G$ of groups with this property. For a subgroup $H' < H$, if $\psi(H') = G$, then $H' = H$. Two frattini covers $\psi_1 : H_1 \to G$ and $\psi_2 : H_2 \to G$ have a common cover. Indeed, let $H = H_1 \times_G H_2$ be the fiber product:

$$H = \{(h_1,h_2) \in H_1 \times H_2 \mid \psi_1(h_1) = \psi_2(h_2)\}.$$

Suppose H' is a minimal subgroup of H that projects surjectively onto each factor of H. Then, H' is a common frattini cover of H_1 and H_2. There is a universal object: $\tilde{G}$ is the minimal *projective* cover of G. [**FrJ**, Prop. 20.33]: If $\psi : H \to G$ is any frattini cover, there exists a cover $\gamma : \tilde{G} \to H$ with $\psi \circ \gamma = \tilde{\psi}$.

Furthermore, $\tilde{G}$ is a profinite projective group. That is, given a cover $\tilde{G} \to A$ and a cover $B \to A$, there is a homomorphism $\psi : \tilde{G} \to B$ completing a natural commutative triangle. Note: Don't expect ψ to be a cover (surjective) even when B is a quotient of $\tilde{G}$ [**FrJ**, Ex. 23.27]. Nor is there a unique ψ. One construction explains this projective property almost trivially. Let $\sigma_1, \dots, \sigma_r$ be generators of G and let $\tilde{F}_r$ be the free profinite group on r generators. That is, $\tilde{F}_r$ is the profinite completion, using all subgroups of finite index, of the free group on r generators. Map $\tilde{F}_r$ to G by mapping its canonical generators to the collection $\sigma_1, \dots, \sigma_r$. Since $\tilde{F}_r$ is a profinite group, any descending chain $H_1 > H_2 > \cdots$ of closed subgroups has nontrivial (closed subgroup) intersection. Apply this to find a minimal subgroup $\tilde{G} < \tilde{F}_r$ that maps surjectively by restriction to G. This is a frattini cover because no proper closed subgroups maps surjectively to G. A closed subgroup of a projective group is projective. Thus, $\tilde{G}$ is projective. Other easy points are in [**FrJ**,§20.7]. Characterize $\tilde{G} \to G$ as a frattini cover where the p-sylows of $\tilde{G}$ are projective, and therefore free profinite groups.

The frattini kernel of the map ${}_p\tilde{G} \to G$ is a nilpotent group $\ker = \ker_0$. Its nilpotency is the profinite analog of knowing the frattini subgroup of any finite group is nilpotent. For each $p \mid |G|$, there is *universal p-frattini cover*. Call this ${}_p\tilde{G}$. It is universal for frattini covers of G with p-group kernel. The p-sylows of ker are nontrivial exactly for those primes dividing $|G|$: $\ker = \prod_{p \mid |G|} P_p$. Each P_p is a characteristic closed subgroup of $\tilde{G}$, so ${}_p\tilde{G} = \tilde{G}/\prod_{p' \mid |G|, p' \neq p} P_p$. Compare with the universal central extension of a perfect group.

Suppose G is perfect: generated by its commutators $[G,G]$. Then, $\tilde{G}$ is the closure of $[\tilde{G},\tilde{G}]$ because the commutator image generates G. The universal central extension of a perfect group is a finite group. Yet, the universal frattini cover, being a projective group, has no elements of finite order. An important point: The universal frattini cover factors through the universal central extension.

§II.B. Properties of ${}_p\tilde{G}$. Sequence (2.1) helps check properties of ${}_p\tilde{G}$. Denote the quotient ${}_p\tilde{G}/\ker_n$ by ${}^n_p\tilde{G}$. When $n = 0$ this gives ${}^0_p\tilde{G} = G$. Suppose M is a G module and $\alpha \in H^i(G, M)$. Say α is *supported* by $\mathbb{F}_p[G]$ module $M'' \subset M$ if α is the image of $\beta \in H^i(G, M'')$ (from inclusion).

Lemma 2.1. *For any integer $n \geq 0$, the universal p-frattini cover of ${}^n_p\tilde{G}$ is ${}_p\tilde{G}$. There is a natural action of ${}^n_p\tilde{G}$ on the $\mathbb{F}_p$ vector space $\ker_n / \ker_{n+1}$. Characterize $M = \ker_0 / \ker_1$ as the maximal $\mathbb{F}_p[G]$ module having $\alpha \in H^2(G, M)$ with this property. For any nontrivial $\mathbb{F}_p[G]$ module quotient M' of M, the natural image α' of α in $H^2(G, M')$ is nonzero. Equivalently: M is maximal for having $\alpha \in H^2(G, M)$ not supported by a proper submodule of M.*

Proof. ${}_p\tilde{G}$ is the smallest frattini cover of G with a projective p-Sylow. Thus, the first sentence restates the projectivity property of ${}_p\tilde{G}$. The action of ${}^n_p\tilde{G}$ on $\ker_n / \ker_{n+1}$ is conjugation. That is, $g \in {}^n_p\tilde{G}$ lifts to $\tilde{g} \in {}_p\tilde{G}$; define $g(k \cdot \ker_{n+1})$ to be $\tilde{g}k\tilde{g}^{-1} \ker_{n+1}$ for each $k \in \ker_n$. Two lifts $\tilde{g}_1$ and $\tilde{g}_2$ produce the same action because $\tilde{g}_1\tilde{g}_2^{-1} = k_1$ is in $\ker_n$: $k_1 k k_1^{-1} = k$ modulo $\ker_{n+1}$.

The last sentence is cohomology for the existence of a universal exponent p frattini cover of G with abelian kernel. For example see [**N**, §10.10–replace $\mathbb{Z}$-modules there with $\mathbb{F}_p$-modules]. Suppose $H \to G$ is any exponent p frattini cover with G module kernel M. This defines a nontrivial element $\alpha \in H^2(G, M)$. Moreover, if M/Q is a nontrivial G-quotient, the natural extension $H/Q \to G$ also is nontrivial. Otherwise, let G_1 be a splitting of G. Then, $\langle Q, G_1\rangle$ would be a proper subgroup of H mapping surjectively to G. This contradicts the frattini cover property. □

Remark 2.2. Call $\ker_0 / \ker_1$ in Lemma 2.1 the universal *p-frattini module* for G. The groups $\ker_0 / \ker_1$ and $\ker_0$ in Lemma 2.1 have the same rank. Lemma 2.1 makes computation of $\ker_0$ effective (see Prop. 2.3). This allows an inductive approach to computing properties of ${}^n_p\tilde{G}$ (see Prop. 2.7). So, what would it mean to *know* the universal p-frattini cover of a finite group G? The display of ${}_2A_5$ in §II.F gives a model for this. $\square$

Denote the algebraic closure of $\mathbb{F}_p$ by K_p. We list ingredients from the theory of *modular representations* [**A**, Chaps. 1-3]. Brauer's Theorem (below) on simple G modules forces considering, at times, $\dot{\mathcal{G}} = K_p[G]$ modules instead of $\mathbb{F}_p[G] = \mathcal{G}$ modules. Translation between statements about $\mathcal{G}$ modules to $\dot{\mathcal{G}}$ modules is usually straightforward. A $\dot{}$-over notation for a $\mathcal{G}$ module means we've tensored with K_p to make it a $\dot{\mathcal{G}}$ module. An *indecomposable* $\dot{\mathcal{G}}$ module is one without a nontrivial direct summand. A *simple* (or *irreducible*) $\dot{\mathcal{G}}$ module is one with no proper submodules. Let M be a $\dot{\mathcal{G}}$ module. Its *radical* is the smallest submodule $\mathrm{rad}(M)$ whose quotient $M/\mathrm{rad}(M)$ is a direct sum of simple modules [**A**, p. 3].

Let H be any subgroup of G. Denote the corresponding subalgebra by $\dot{\mathcal{H}}$. For M a $\dot{\mathcal{G}}$ module, let M_H be the corresponding $\dot{\mathcal{H}}$ module. The dimension of M is its vector space dimension over K_p.

(2.2a) *Brauer's theorem.* Simple $\dot{\mathcal{G}}$ modules correspond to G conjugacy classes whose elements have order prime to p [**A**, p. 14].

(2.2b) Indecomposable projectives M correspond to simple $\dot{\mathcal{G}}$ modules via the map $M \to M/\mathrm{rad}(M)$ [**A**, p. 31].

(2.2c) M is a projective $\dot{\mathcal{G}}$ module if and only if M_{P_p} is a free $K_p[P_p]$ module [**A**, p. 33 and 66].

Lemma 2.3 describes the maximal pair (M_G, α_G). This is the universal exponent p frattini cover of G with abelian kernel in Lemma 2.1. The universal p-frattini module is M_G. Any $\mathbb{F}_p$ module A has a smallest projective cover

$$0 \to I \to P \to A \to 0,$$

where P is projective and has minimal dimension. This sequence is unique up to an obvious equivalence. Denote I by $\Omega(A)$. Benson [**Be**] calls this Heller's construction. Inductively, define $\Omega^r(A)$ for any $r \geq 1$ by iterating this on $\Omega^{r-1}(A)$. Apply this to the trivial module $\mathbf{1} = \mathbb{F}_p$. The next result follows [**Se2**].

Projective Indecomposable Lemma 2.3. *M_G is isomorphic to $\Omega^2(\mathbf{1})$. The class α_G is canonically defined in $H^2(G, \Omega^2(\mathbf{1}))$.*

Proof. All modules in the proof are finitely generated. Note: $H^r(G, A)$ is just $\mathrm{Ext}^r_G(\mathbf{1}, A)$ [**N**, p. 223, Th. 4]. We show $\Omega^2(\mathbf{1}) = M$ is the maximal module having $\alpha \in \mathrm{Ext}^2_G(\mathbf{1}, M)$ not supported on a submodule M'' (see Lemma 2.1). Use induction. For each integer $r \geq 1$ and $\mathcal{G}$ module B, consider pairs (M, α), $\alpha \in \mathrm{Ext}^r_G(B, M)$ not supported on a proper submodule. We show there is a maximal such, $M = \Omega^r(B)$. Further, the universal element of $\mathrm{Ext}^r_G(B, \Omega^r(B))$ represents α.

Let P be the smallest projective cover of B. Dimension shift on the canonical sequence $0 \to \Omega(B) \to P \to B \to 0$ in the first position of Ext_G. This shows $\mathrm{Ext}^r_G(B, M) = \mathrm{Ext}^{r-1}_G(\Omega(B), M)$. Suppose the *maximal* M for $r = 1$ is $\Omega(B)$. Then, inductively, $\Omega(\Omega^{r-1}(B))$ is the *maximal* M for general r.

We now show $\Omega(B)$ is the maximal M for $r = 1$. First: $\mathrm{Ext}^1_G(B,M)$ is equivalence classes of extensions of B by M [**N**, p. 129]. As in Lemma 2.1, first show no proper submodule M'' of M supports the canonical sequence. With no loss, replace B by a nontrivial simple quotient of one of its direct summands. Suppose, contrary to this, there is a split sequence: $M/M'' \to P/M'' \to B$ (with B simple). A splitting would show P/M'' to have a quotient with two (or more) simple summands. This contradicts (2.2b): B uniquely determines P by being its unique simple quotient (with multiplicity 1).

Finally, consider the relation of P to any short exact sequence $M' \to W \to B$. Since P is projective, the morphism $P \to B$ induces the short exact sequence $\Omega_1 \to P \xrightarrow{\tau} W$ that gives a natural diagram:

$$\begin{array}{ccccc} \Omega_1 & \longrightarrow & P & \xrightarrow{\tau} & B \\ \downarrow & & \downarrow & & \| \\ M' & \longrightarrow & W & \longrightarrow & B \end{array} \tag{2.3}$$

From [**N**, p. 129], the exact sequence of cohomology on the covariant 2nd slot produces $\mathrm{Ext}^1_G(B,\Omega_1) \to \mathrm{Ext}^1_G(B,M')$. The element of $\mathrm{Ext}^1_G(B,\Omega_1)$ defining the upper row of (2.3) maps to the element of $\mathrm{Ext}^1_G(B,M')$ defining the lower row of (2.3). This shows universality of the upper row extension of (2.3). □

§II.C. A_5**—checking properties of** ${}_p\tilde{G}$**.** Consider $A_5 = G$. The next statement is central to [**Se1**, p. 658]. The universal central extension $\bar{A}_5$ of A_5 fits in a commutative diagram

$$\begin{array}{ccccccc} 1 & \longrightarrow & \langle \pm 1 \rangle & \longrightarrow & \bar{A}_5 & \xrightarrow{\delta} & A_5 \\ \| & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \langle \pm 1 \rangle & \longrightarrow & \mathrm{Spin}(5,\mathbb{Q}) & \longrightarrow & \mathrm{SO}(5,\mathbb{Q}) \end{array} \tag{2.4}$$

This is important for the determination of the universal 2-frattini module of A_5.

A classical identification has A_5 equal to $\mathrm{PSL}_2(\mathbb{Z}/5)$. This allows us to identify $\bar{A}_5$ with $\mathrm{SL}_2(\mathbb{Z}/5)$. The first invariant of the universal frattini cover of a group G is the collection of ranks of the universal p-frattini modules. In particular, we now show how to compute these. For A_5 these are the ranks of P_2, P_3 and P_5 with $\ker = P_2 \times P_3 \times P_5$ (§II.A). For any group G, if you compute the groups ${}_p\tilde{G}$ for $p \,|\, |G|$, then $\tilde{G}$ is the fiber product of these groups over G.

To orient to this problem, note A_5 has a cyclic 5-sylow. Further,

$$\ker' \to \mathrm{PSL}_2(\mathbb{Z}_5) \to \mathrm{PSL}_2(\mathbb{Z}/5) = A_5 \tag{2.5}$$

is a frattini cover. For example, combinatorially check that any lift of $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ will generate $\mathrm{PSL}_2(\mathbb{Z}_5)$. Still, $\mathrm{PSL}_2(\mathbb{Z}_5)$ is not the universal 5-frattini cover of A_5 (Remark 2.10). The adjoint representation of $\mathrm{PSL}_2(\mathbb{Z}_5)$ appears as

$${}_5S_c = \ker' / (\ker')^p [\ker', \ker'],$$

2×2 matrices of trace 0. Here $\mathrm{PSL}_2(\mathbb{Z}/5)$ acts by conjugation.

There are three conjugacy classes of A_5 of orders relatively prime to 5. Thus, (2.2a) says there are three simple $\dot{\mathcal{G}}$ modules when $p = 5$:

(2.6a) ${}_5S_a = \mathbf{1}$;
(2.6b) ${}_5S_b$, the standard degree 5 representation modulo $\mathbf{1}$; and
(2.6c) ${}_5S_c$ as above.

We explain ${}_5S_b$ further. Suppose G is a doubly transitive subgroup of S_n, and p is relatively prime to n. Then, the standard representation is a direct sum of the identity and an irreducible representation of degree $n-1$. When, however, $p|n$, the one dimensional space of G invariant vectors isn't a direct summand of the standard representation. Here, restriction of the degree 5 standard representation to the cyclic 5-sylow gives its regular representation. From (2.2c) it is the principal indecomposable for the 4-dimensional simple representation. See Remark 2.10 for completion of this case.

Similarly, there are four simple $\dot{\mathcal{G}}$ modules when $p = 2$:

(2.7a) ${}_2S_a = \mathbf{1}$;
(2.7b) ${}_2S_b$, reduction modulo 2 of the degree 4 summand of the standard representation; and
(2.7c) ${}_2S_c'$ and ${}_2S_c''$, conjugate degree two representations from $A_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$.

The elements of the 2-sylow of S_5 are representatives of the four nontrivial cosets of the stabilizer of 1 in the standard representation of A_5. Since these four nontrivial cosets span ${}_2S_b$, the 2-sylow acts freely on it. Thus, (2.2c) says it is a projective indecomposable.

Simple representations for $p = 3$ follow those of (2.7) except use ${}_2S_c'$ and ${}_2S_c''$, reductions modulo 3 of the complex degree 3 representations. There is a standard procedure for this. Find a lattice L in the representation module invariant under G and form the quotient L/pL. For K a subgroup of A_5, denote $\mathrm{ind}_K^{A_5}(\mathbf{1})$ (of dimension $(A_5 : K)$) by $\mu_K(\mathbf{1})$.

Proposition 2.4. *Take $p = 2$. Identify the normalizer of the subgroup $\langle(1\,2\,3\,4\,5)\rangle$ with the dihedral group $\mathbb{Z}/5 \times^s \langle\pm 1\rangle = H$. The universal 2-frattini module of A_5 is the dimension 5 quotient $\mu_H(\mathbf{1})/\mathbf{1}$. Also, any frattini cover of A_5 with 2-group kernel factors through $\bar{A}_5 \to A_5$.*

Proof. Apply Lemma 2.3. Let $P_{\mathbf{1}}$ be the projective indecomposable of $\mathbf{1}$ for the prime $p = 2$. We show this is the induced module $\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}) \stackrel{\text{def}}{=} N_{\mathbf{1}}$. Since $\mathbb{Z}/5$ has order relatively prime to 2, all modules for it are projective (Mashke's Theorem). From (2.2c), $\mu_H(\mathbf{1})$ is projective. It has $\mathbf{1}$ as the augmentation ideal quotient: a formal sum $\sum_{i=1}^t a_i\tau_i$ of cosets of $\mathbb{Z}/5$ maps to $\sum_{i=1}^t a_i$. We have only to show it is indecomposable.

Apply Frobenius reciprocity in the form

$$\mathrm{Hom}_{\mathbb{Z}/5}(\mathbf{1}, M_{|\mathbb{Z}/5}) = \mathrm{Hom}_{A_5}(\mathrm{ind}_{\mathbb{Z}/5}^{A_5}(\mathbf{1}), M)$$