Contemporary Mathematics
Volume **00**, 0000

Topics in Galois Theory

Based on J.-P. Serre: Research Notes in Mathematics, 1992

Jones and Bartlett Publishers, xvi+116 pp. ISBN 0-86720-210-6

MICHAEL D. FRIED

ABSTRACT. This is a corrected and expanded version of a review that appeared in the Bulletin of the American Math Society [**Fr4**]. About 2/3rds of the **Recent developments in the Inverse Galois Problem** conference talks might have started concisely referring to a section of Serre's book. This was especially true for practical talks based on classical realizations of groups over $\mathbb{Q}$ using covers with three branch points. This was less true of talks on the modern braid and profinite theories, especially where these topics used higher dimensional moduli. Still, these topics get a solid base from an elementary expansion of my review on the *Branch Cycle Argument*. The proofs for this §4 expansion are in the discussion before Theorem 5.1 in the 1977 paper [**Fr1**]. Yet, hindsight allows tweakings of its basic statements that makes them more memorable and practical. I have expanded the notation of rigidity type statements for their use on non-Galois covers applied to realization of geometric-arithmetic Galois group pairs. Further, I emphasize the failings of (plain) rigidity that encourage adoption of generalized *braid group* forms of rigidity.

Serre's book *is* a set of topics. It contains historical origins and applications of the inverse Galois problem. Its audience is the Mathematician who knows the ubiquitous appearance of Galois groups in diverse problems of number theory. Such a Mathematician has heard there has been recent progress on the inverse Galois problem. Serre has written a map through the part of this progress that keeps *classical landmarks* in sight. We'll describe Serre's view of present

1991 *Mathematics Subject Classification.* Primary 11F32, 11G18, 11G35, 11R18, 11R58; 11S20: Secondary 12E25, 12F12, 20B05, 20D25, 20F34.

Supported by NSF #DMS-99305590 and funds from the American Mathematical Society.

achievements toward that goal and comment on the territory he ignored. We denote Serre's book by [**Se**] throughout.

Galois theory is the supreme topic in an area once called the *Theory of Polynomials*. Versions of the inverse Galois problem have immediate application in algebraic number theory, arithmetic geometry, coding theory. This includes applications driven by the theory of finite fields. Until recently, however, attacks on the problem were ad hoc. Even when general approaches arose in the late 70's, acceptance took a long time. Then, special approaches still held promise. Examples now show why earlier methods won't solve the complete problem.

Still, hope springs eternal. For example, Colliot-Thélène has this observation [**Se**, Conjecture 3.5.8]. If K is a number field, then a K-unirational variety has a property Serre calls weak-weak approximation. Serre shows a Hilbertian property holds for such a variety. He thus—conjecturally—recovers Noether's original program. This asked: Are the invariants of $G \leq S_n$ acting on $K(x_1, \dots, x_n)$ a pure transcendental field? Although Swan produced a famous counterexample, Serre asks only if a version of Hilbert's irreducibility theorem holds for the extension. Shall we wait to see if this conjecture—a simple approach to the inverse Galois problem—holds? Serre doesn't. In this review fields will have 0 characteristic, usually subfields of $\mathbb{C}$, the complex numbers.

Why has the subject of the inverse Galois problem taken off recently? The classification of finite simple groups broke psychological ground. Thompson's application of *rigidity* (§5) to the *Monster* simple group attracted many. There was a prevalent thought: Realization of simple groups as Galois groups is tantamount to realizing all groups as Galois groups. If you could realize the Monster wouldn't easier simple groups follow: therefore the Inverse Galois Problem too? §8 tells why this was naive. Still, it renewed excitement in the topic.

[**Se**] is about 100 pages. With complete proofs it would have been 300 pages, yet it wouldn't have appeared quickly. There's something for most algebraists.

§0. THE INVERSE GALOIS PROBLEM

Suppose $L/\mathbb{Q}$ is a finite extension of fields. Then, there are $n = [L : \mathbb{Q}]$ field embeddings of L into the algebraic numbers $\bar{\mathbb{Q}}$. If $L = \mathbb{Q}(\alpha)$, each zero of the irreducible polynomial for α over $\mathbb{Q}$ gives an embedding. When all embeddings are automorphisms of L, L is *Galois* over $\mathbb{Q}$. The automorphism group $G(L/\mathbb{Q})$ is the *Galois group* of $L/\mathbb{Q}$. For any $L/\mathbb{Q}$, there is a minimal Galois extension $\hat{L}/\mathbb{Q}$ containing L: the Galois closure of $L/\mathbb{Q}$. Consider $G^L = G(\hat{L}/\mathbb{Q})$ as L runs over all finite extensions of $\mathbb{Q}$. Suppose $L \subset L'$. The restriction homomorphism $G(\hat{L}'/\mathbb{Q}) \xrightarrow{\text{rest}} G(\hat{L}/\mathbb{Q})$ takes each automorphism of $\hat{L}'$ to an automorphism of $\hat{L}$. Then, $G_{\mathbb{Q}} = G(\bar{\mathbb{Q}}/\mathbb{Q})$ is this subgroup of $\mathcal{G} = \prod_L G^L$: ∞-tuples $(\dots, \alpha_L, \dots)$ with $\text{rest}(\alpha_{L'}) = \alpha_L$ for each $L \subset L'$. Arithmetic geometers regard this as their most important mathematical object. Still, what do we know about it?

By its description, $G_{\mathbb{Q}}$ is a compact topological group having countably many topological generators. If there were a *free* set of generators, we would know a lot. For example: every finite group would be a quotient of it. That is, given finite G, there would exist L with $G(\hat{L}/\mathbb{Q}) = G$. This is the mildest version of the *inverse Galois problem*.

We know $G_{\mathbb{Q}}$ doesn't have free generators. For one, a free group doesn't have elements of finite order: $G_{\mathbb{Q}}$ contains an element of order 2, complex conjugation. Among its quotients there are the symmetric groups S_n, and the alternating groups A_n (Hilbert: 1896). Further, we know the quotients of $G_{\mathbb{Q}}$ include all sporadic simple groups (Belyi [**B**], Malle [**Mal**], Matzat [**Ma**] and Thompson [**Th**])—except possibly M_{23}, the Matthew group of degree 23. (Matzat and Malle have realized M_{24}, but not M_{23}, as the group of a regular extension of $\mathbb{Q}$ (§1).) They also include all solvable groups (Shafarevich: ???; see §6).

Chevalley groups, even over prime finite fields, are another matter. Much analysis in Serre's book uses *modular curves* and *rigidity*. With these he displays many Chevalley groups from $\mathrm{GL}_2(p)$, $\mathrm{PSL}_2(p)$ and $\mathrm{PGL}_2(p)$ as Galois groups (Belyi, Malle, Shih [**Sh**] especially). These are rank 1 Chevalley groups over the prime finite fields $\mathbb{F}_p$.

Serre records but a handful of Chevalley groups over non-prime finite fields as Galois groups [**Se**, p. 53]. None have rank exceeding 1. Meanwhile, Völklein [**V1**] and [**V2**] has realized series of higher rank Chevalley groups over non-prime finite fields. These use generalizations of rigidity not in [**Se**] (see §1 and Part E of the discussion of Rigidity Results in §4).

If $G_{\mathbb{Q}}$ had free generators, so would many normal subgroups of infinite index. The topological closure of its commutator subgroup $[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$, in particular [**FrJ**, Ex. 24.9]. This is the absolute Galois group of the maximal abelian extension $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$. Kronecker in the last century showed $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$, the field with all roots of 1 adjoined. The following conjecture would catch $G_{\mathbb{Q}}$ between well-known profinite groups, the countably generated free profinite group $\hat{F}_\omega$ and the invertible profinite integers $\hat{\mathbb{Z}}^*$. See §8 for proven analogs.

SHAFAREVICH'S CONJECTURE. *$G(\bar{\mathbb{Q}}/\mathbb{Q}^{\mathrm{cyc}})$ is free profinite. Thus, this sequence is exact:* $1 \to \hat{F}_\omega \to G_{\mathbb{Q}} \to G(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^* \to 1$.

§1. CLASSICAL TOPICS

[**Se**] remarks often that diverse areas depend on observations about Galois groups. It also moves well from the classical period—Shafarevich's theorem, using algebraic number theory—to the modern era. This starts in the early 80s when regular realizations took over. Indeed, after the first two chapters, the book concentrates on *regular extensions* $L/\mathbb{Q}(x)$: $L \cap \bar{\mathbb{Q}} = \mathbb{Q}$. Here x is an indeterminate we fix throughout.

For most applications, regular realizations are best. Here is why. Applications require realization of the group with side conditions. Extra latitude in the realization assures a complicated construction such as [**Se**, Chap. 2] for ℓ-groups can satisfy such side conditions. Here are conditions you might need to construct a group G over a given field K.

A construction over a field L forces realizing G as $G(M/\mathbb{Q})$ with $M \cap L = \mathbb{Q}$: a *disjointness condition*. Or, you require M to satisfy local conditions—related to completions by valuations.

Hilbert stated one application of his irreducibility theorem. Regular realizations of G over Hilbertian K produce infinitely many disjoint Galois extensions of K with group G. This is a mild exercise in use of *decomposition groups*, a technique known to many, but not all, algebraists. Also, it gives wreath products of G with another group that has a realization over $\mathbb{Q}$. This latter realization need not be regular. ([**Se**, p. 36] merely remarks on this valuable fact.)

Serre's book is much taken with Hilbert's irreducibility theorem. It looks innocuous. A field L is Hilbertian if each irreducible polynomial $f(x, y) \in L[x, y]$ (of positive degree in y) remains irreducible for infinitely many specializations of $x \in L$. Number fields are Hilbertian, and so are many other fields. For example, Hilbertianity of $\mathbb{Q}^{\text{ryc}}$ (due to Kuyk [**FrJ**, Th. 15.6]; see §8) has had many generalizations. [**Se**] offers variants and deductions from Hilbert's Theorem; sometimes without attribution (the observations of [**Se**, §4.6] outlining [**FrJ**, Theorem 12.7]). Regular realizations do more. So, it's surprising that finding regular realizations has had more success than just finding realizations.

The technique of *rigidity* dominates later chapters (see §4). There is, however, little comment on the limitations of rigidity. For example, there are solid reasons rigidity can't—as in *cannot possibly*—realize most groups as Galois groups. Indeed, for several years it is (braid group) generalizations of rigidity, and not rigidity, that have produced new groups as Galois groups over $\mathbb{Q}$. [**Se**] mentions none of this. (These were present in [**Fr1**] long before Thompson used the name *rigidity* for the special case.) Such general results, however, require conceptual additions that overwhelm the value of rigidity alone.

In §3–§4, we comment on these additions using examples. The §7 example connects to the modular curve subtheme of [**Se**, Chap. 5]. Modular curves are covers of the sphere $\phi : X \to \mathbb{P}^1$ ramified at three points in $\mathbb{Q}$. The classical j function from complex variables uniformizes this copy of the sphere. We may take the points of ramification of ϕ to be 0, 1, ∞. These particular curve covers, however, come as compactifications of the upper half plane modulo *congruence subgroups* of $\mathrm{PSL}_2(\mathbb{Z})$. Serre spends many pages on Shih's Theorem on regular realization of $\mathrm{PSL}_2(\mathbb{F}_p)$ (over $\mathbb{Q}$). The next section describes what he accomplishes by milking modular curves to serve the inverse Galois problem.

§2. SHIH'S THEOREM

Note: An element of order 2 and an element of order 3 freely generate $\mathrm{PSL}_2(\mathbb{Z})$. Consider any three branch point cover of the sphere. Assume the group of its Galois closure has generators an element of order 2 and an element of order 3. This cover therefore appears as a quotient of the upper half plane $\mathbb{H}$ in $\mathbb{C}$ by a subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index. Most such curves, however, aren't modular curves. For modular curves each point on the curve has geometric significance. We explain how [**Sh**] used the tradition exploiting that.

Let N be a positive integer. Consider the subgroup $\Gamma_0(N)$ of $\mathrm{PSL}_2(\mathbb{Z})$ with representing matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ where $c \equiv 0 \mod N$. We especially want the case when the natural compactification $X = X_N$ of $\mathbb{H}/\Gamma_0(N)$ is of genus 0. Classical theory defines this over $\mathbb{Q}$; it also follows from rigidity (§4) generalized to include non-Galois 3-branch point covers (see $(G, H, \mathbf{C})$-rigidity of §4). Various $\mathrm{PSL}_2(\mathbb{F}_p)$s appear by interpreting rational points on twists of this cover when X_N is of genus 0. Serre reminds, without citation, this implies $N \leq 18$, and unequal to $4, 9, 11, 14$–17. There is a natural involution w on X_N. Consider points on X_N as pairs (E, E'): elliptic curves with a cyclic isogeny $E \to E'$, of degree N. The dual to this isogeny gives $E' \to E$. Define w by $w(E, E') = (E', E)$.

Consider a quadratic extension $K/\mathbb{Q}$ with σ its nontrivial automorphism. Identify Galois groups $G(\mathbb{Q}(X_N)/\mathbb{Q}(X_N/\langle w\rangle))$ and $G(K/\mathbb{Q})$ with $\mathbb{Z}/2$. Therefore, $G(K(X_N)/\mathbb{Q}(X_N/\langle w\rangle))$ is $\mathbb{Z}/2 \times \mathbb{Z}/2$. The diagonal here has fixed field a function field of a curve X_N^K of genus 0 defined over $\mathbb{Q}$.

Take the case $K = \mathbb{Q}\Big(\sqrt{(-1)^{\frac{p-1}{2}}p}\Big)$ and $\left(\frac{N}{p}\right) = -1$ with p a prime. Consider an elliptic curve E over K with E and E^σ isogenous. Then:

(*) $G_{\mathbb{Q}}$ acts on p-division points of E—a vector space over dimension 2 over $\mathbb{F}_p$—with image $\mathrm{PSL}_2(\mathbb{F}_p)$ (rather than a larger subgroup of $\mathrm{PGL}_2(\mathbb{F}_p)$).

When $X_N^K = X_N^p$ has a rational point, its function field is $\mathbb{Q}(x)$ for some x. Thus, (*) gives regular realization of $\mathrm{PSL}_2(\mathbb{F}_p)$. When $N = 2, 3$ or 7, Serre sketches a modular interpretation that the fixed points of w are rational. They thus produce a rational point on X_N^p. So, primes p for such a regular realization of $\mathrm{PSL}_2(\mathbb{F}_p)$ are those with one of $\left(\frac{N}{p}\right) = -1$, $N = 2, 3$ or 7. It is clear Serre would honor continuations of these results, special though they are.

§3. THE BRANCH CYCLE ARGUMENT—PRELUDE TO RIGIDITY

[**Se**, Chap. 6] gives complete references for *Riemann's existence theorem*. It is the heart of rigidity. We'll state a light version of it: without pedantic (albeit, important) equivalences. Let $L/\mathbb{C}(x)$ be a degree n extension, with $\hat{L}/\mathbb{C}(x)$ its Galois closure (§0). Then, $G(\hat{L}/\mathbb{C}(x))$ faithfully embeds in S_n. This embedding

is unique modulo conjugation of the image by an element of S_n.

Geometric field theory makes valuable use of formal Laurent series $\mathbb{C}((x-x'))$ in $x-x'$, $x' \in \mathbb{C} \cup \{\infty\}$. Replace $x-x'$ by $1/x$ if $x' = \infty$. The algebraic closure of $\mathbb{C}((x-x'))$ is $\cup_{e=1}^{\infty} \mathbb{C}(((x-x')^{1/e}))$. Thus, the absolute Galois group of $\mathbb{C}((x-x'))$ is pro-cyclic. A natural generator $\sigma_{x'}$ has the effect $(x-x')^{1/e} \mapsto \zeta_e (x-x')^{1/e}$, $e = 2, 3, \ldots$. Here $\zeta_e = e^{2\pi i/e}$. The extension $\hat{L}\mathbb{C}((x-x'))/\mathbb{C}((x-x'))$ is finite. Thus, there is a minimal integer e with $\hat{L}$ embedding in $\mathbb{C}(((x-x')^{1/e}))$ as the identity on $\mathbb{C}(x)$. Since $\hat{L}/\mathbb{C}(x)$ is Galois, e is independent of the embedding. Compose any one embedding $\psi_{x'} : \hat{L} \to \mathbb{C}(((x-x')^{1/e}))$ 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 $\boldsymbol{x} = (x_1, \ldots, x_r)$, the *branch points* of the cover. If ψ_i is the embedding attached to x_i, name the corresponding automorphism σ_i. The r-tuple $\boldsymbol{x}$ thus gives $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_r)$, an r-tuple of conjugacy classes in G. These are the *branch cycle* conjugacy classes of $L/\mathbb{C}(x)$. 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 (the transitive group) G.*

Conversely, if $x_1, \ldots, x_r \in \mathbb{C}$ are distinct, and $\sigma_1, \ldots, \sigma_r \in S_n$ satisfy (i) and (ii) with G transitive in S_n, there exists $L/\mathbb{C}(x)$ producing this data.

Call an r-tuple arising from $L/\mathbb{C}(x)$, satisfying (i) and (ii), a description of its *branch cycles*. We explain the *Branch Cycle Argument* [**Fr1**, prelude to Th. 5.1]. Suppose $L/\mathbb{Q}(x)$ is a regular extension. Let $\hat{L}/\mathbb{Q}(x)$ be the Galois closure of the extension. Take the constants of $\hat{L}$ to be $\hat{\mathbb{Q}} = \hat{\mathbb{Q}}_L$. The *arithmetic monodromy* group of the extension is $\hat{G} = G(\hat{L}/\mathbb{Q}(x))$. Similarly, the *geometric monodromy* group is $G = G(\hat{L}/\hat{\mathbb{Q}}(x))$. Elements of $G_{\mathbb{Q}}$ permute the branch points $x_1, \ldots, x_r$ of $L/\mathbb{Q}(x)$: a valuable permutation invariant of the extension.

Adjoin all roots of 1 to $\mathbb{Q}$ to get $\mathbb{Q}^{\mathrm{cyc}}$. Let $\tau \in G_{\mathbb{Q}}$ act on roots of 1 through restriction: $G_{\mathbb{Q}} \to G(\mathbb{Q}^{\mathrm{cyc}}/\mathbb{Q}) \cong \hat{\mathbb{Z}}^*$ as in §0. Thus, identify the image of τ with a supernatural integer $m_\tau \in \hat{\mathbb{Z}}^*$ from the invertible integers of the profinite completion of $\mathbb{Z}$. Also, use τ for the action of τ on $x_1, \ldots, x_r$ and on $\mathrm{C}_1, \ldots, \mathrm{C}_r$. Suppose $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_t)$ is a collection of conjugacy classes of G. Denote the least common multiple of orders of the elements $\mathrm{C}_1, \ldots, \mathrm{C}_t$ by $N_{\mathbf{C}} = N$. We say $\mathbf{C}$ is a *rational union* if putting the elements of $\mathrm{C}_1 \cup \cdots \cup \mathrm{C}_t$ to any power m prime to N gives the same set.

Let C be a conjugacy class of G. For H a group containing G, denote the conjugacy class in H of the elements of C by C^H.

BRANCH CYCLE ARGUMENT. *Take $L/\mathbb{Q}(x)$ and the x_i s as above. Conjugacy*

classes $C_{\tau(i)}^{m_\tau}$ *and* C_i *in* $\hat{G}$ *are the same,* $i = 1, \dots, r$. *For each* i, *denote the union of the conjugacy classes of* $C_{\tau(i)}^{\hat{G}}$ *in* $\hat{G}$ *by* $\hat{\mathbf{C}}(i)$: τ *runs over* $G_{\mathbb{Q}}$. *Then,* $\hat{\mathbf{C}}(i)$ *is a rational union in* $\hat{G}$ *for each* $i = 1, \dots, r$. *Further, let* $\beta \in \hat{G}$. *Consider* $\tau \in G_{\mathbb{Q}}$ *whose restriction to* $\bar{\mathbb{Q}}_L$ *equals the restriction of* β. *Then, with* $m = m_\tau$, *conjugacy classes* $\beta C_i \beta^{-1}$ *and* $C_{\tau(i)}^m$ *of* G *are equal,* $i = 1, \dots, r$.

AN ILLUSTRATIVE CASE. Suppose $x_1 \in \mathbb{Q}$. Let m be relatively prime to $\mathrm{ord}(\sigma_1)$. We show mth powers of the conjugacy class of σ_1 in $\hat{G}$ gives the same class. Here's why. Choose $\tau \in G_{\mathbb{Q}}$ with $\tau(\zeta_{e_1}) = \zeta_{e_1}^m$. Apply τ to the coefficients of elements in $\bar{\mathbb{Q}}((x - x_1)^{1/e_1}))$. Restricting τ to the image of an embedding of $\hat{L}$ gives an automorphism of $\hat{L}$. Compute what conjugation by τ does to σ_1:

$$\tau\sigma_1\tau^{-1}((x - x_1)^{1/e_1}) = \tau(\zeta_{e_1}(x - x_1)^{1/e_1}) = \zeta_{e_1}^m(x - x_1)^{1/e_1}.$$

It has the same effect as σ_1^m.

This leaves the statement on $\beta \in \hat{G}$. Consider the effect β has on the conjugacy class C_i in G. Our From $x_1 \in \mathbb{Q}$, τ acts on puiseux expansions around x_1. This determines a decomposition group element for a place of $\hat{L}$ above x_1. Conclude from the first paragraph argument. □

The Branch Cycle Argument has a more general statement over any field F. The complication is keeping track of the intersection of F with $\mathbb{Q}^{\mathrm{cyc}}$. Examples at the end of §4 and in §7 show how to apply the Branch Cycle Argument.

§4. RIGIDITY AND ITS GENERALIZATIONS

Continue notation from §3. [**Fr1**, Th. 5.1] gives a partial converse to the Branch Cycle Argument. It uses moduli spaces to consider extensions $L/\mathbb{Q}(x)$ with a given pair $(G, \hat{G})$ as arithmetic and geometric monodromy groups (§3). If $[L : \mathbb{Q}(x)] = n$, both G and $\hat{G}$ are naturally subgroups of S_n. In addition, G is a normal subgroup of $\hat{G}$. For applications, start with G and conjugacy classes $\mathbf{C} = (C_1, \dots, C_r)$ of generators $(\sigma_1, \dots, \sigma_r) \in G^r$.

We say we have a $(G, H, \mathbf{C})$ realization over $\mathbb{Q}$ if there exists $L/\mathbb{Q}(x)$ of degree n with these properties. The geometric (resp., arithmetic) monodromy group of $L/\mathbb{Q}(x)$ is G (resp., H) and the geometric Galois closure $\bar{\mathbb{Q}}\hat{L}/\bar{\mathbb{Q}}(x)$ has conjugacy class data $\mathbf{C}$ in G. Given $(G, \mathbf{C})$ the Branch Cycle Argument shows there is a maximal group containing all possible groups H:

$$\hat{G}^{\mathbf{C}} = \{\beta \in S_n \mid \exists\, \tau \in S_r,\, m \in (\mathbb{Z}/N_{\mathbf{C}})^* \text{ with } \beta C_i \beta^{-1} = C_{\tau(i)}^m, i = 1, \dots, r\}.$$

Let H be a group between G and $\hat{G}^{\mathbf{C}}$. As before the Branch Cycle Argument, denote the conjugacy classes in H corresponding to $\mathbf{C}$ by $\mathbf{C}^H$. Assume:

(iii)$_H$ $\mathbf{C}^H$ is a rational union of conjugacy classes in H; and

(iv) G has no center (so, with no loss, no element of $H \setminus G$ centralizes G).

Explanation of (iv): This is a statement about the Galois closure process for an extension $L/\mathbb{Q}(x)$ and not pure group theory. It is equivalent to the following. Consider elements $\tau \in G(\hat{\mathbb{Q}}/\mathbb{Q})$ that are images from $\hat{G} = G(\hat{L}/\mathbb{Q}(x))$ of a $\hat{\tau}$ for which conjugation on G by $\hat{\tau}$ equals conjugation by $\gamma \in G = G(\hat{L}/\hat{\mathbb{Q}}(x))$. Since $L/\mathbb{Q}(x)$ is regular, we may assume $\hat{\tau}$ is fixed on L. As G has no center, given $\hat{\tau}$, γ is unique. Such τ form a subgroup H of $G(\hat{\mathbb{Q}}/\mathbb{Q})$. What (iv) says is that H is trivial [**Fr1**, Prop. 2].

The Branch Cycle Argument converse associates an algebraic set $\mathcal{H}(G, H, \mathbf{C})$ to $(G, H, \mathbf{C})$. This has a natural unramified covering map to the space $\mathbb{P}^r \setminus D_r$ of unordered distinct r-tuples of elements of $\mathbb{P}^1$. (If you recognize these must be Hurwitz spaces, here is an aside; [**Fr2**, Part III] gives details. Examples at the end of this section illustrate.) The definition of $\mathcal{H}(G, H, \mathbf{C})$ includes conjugation by H to equivalence r-tuples of branch cycles attached to $\mathbf{C}$, as in Riemann's Existence Theorem. From $(\text{iii})_H$, $\mathbb{Q}$ is a field of definition of $\mathcal{H}(G, H, \mathbf{C})$ and its map to $\mathbb{P}^r \setminus D_r$: $(\text{iii})_H$ is necessary and sufficient for this.

Further, suppose $G \le H \le H' \le \hat{G}^{\mathbf{C}}$. Then, there is a (finite) map

$$(\dagger) \qquad \Psi_{H,H'} : \mathcal{H}(G, H, \mathbf{C}) \to \mathcal{H}(G, H', \mathbf{C}).$$

If $(\text{iii})_H$ and $(\text{iii})_{H'}$ hold, $\mathbb{Q}$ is also a field of definition for $\Psi_{H,H'}$. Restriction of $\Psi_{H,H'}$ to a component of $\mathcal{H}(G, H, \mathbf{C})$ is a Galois cover of the image of this map. The group is isomorphic to a subgroup of H/G. The next statement considers points $\boldsymbol{p} \in \mathcal{H}(G, G, \mathbf{C})$. Take V to be an absolutely irreducible component of $\mathcal{H}(G, G, \mathbf{C})$ containing $\boldsymbol{p}$. Automatically—because $\mathcal{H}(G, G, \mathbf{C})$ is a manifold—$\mathbb{Q}(\boldsymbol{p})$, the field generated by the $\boldsymbol{p}$ coordinates, contains the field of definition of V. Also, $G(1)$ denotes the stabilizer in $G \le S_n$ of the integer 1.

CONVERSE OF BRANCH CYCLE ARGUMENT: [**Fr1**], [**FrV**]. *Besides* (iv), *assume the embedding of G in S_n satisfies one of these:*

(v) *it is the regular representation of G; or*
(vi) *the normalizer of $G(1)$ in G is just $G(1)$.*

Here is a diophantine condition equivalent to existence of a $(G, H, \mathbf{C})$ realization, $L/\mathbb{Q}(x)$ of degree n, over $\mathbb{Q}$. There is $\boldsymbol{p} \in \mathcal{H}(G, G, \mathbf{C})$ whose image in $\mathcal{H}(G, H, \mathbf{C})$ has coordinates in $\mathbb{Q}$ and $[\mathbb{Q}(\boldsymbol{p}) : \mathbb{Q}] = (H : G)$. (Since the $\mathcal{H}$ s are moduli spaces, this applies with any field K replacing $\mathbb{Q}$.)

For the inverse Galois problem, take $G \le S_n$ the regular representation of G and $H = G$. Note: Without $[\mathbb{Q}(\boldsymbol{p}) : \mathbb{Q}] = (H : G)$, $\hat{G}/G$ is only a subgroup of H/G. For equality, exchange H for another group $H' \le \hat{G}^{\mathbf{C}}$. Condition $(\text{iii})_G$ is that the collection $\mathbf{C}$ forms a rational union of conjugacy classes in G.

Conclude: the regular version of the inverse Galois problem is equivalent to finding $\mathbb{Q}$ points on one from the $\mathcal{H}(G, G, \mathbf{C})$ s with $\mathbf{C}$ satisfying $(\text{iii})_G$.

The spaces $\mathcal{H}$ are manifolds. Thus, they can't have rational points unless they have absolutely irreducible components over $\mathbb{Q}$. To investigate this, we go through the special case of rigidity [**Se**, §7.3]. Rigidity rarely applies unless $r = 3$. When $r = 3$, an $\mathcal{H}$ is either $(\mathbb{P}^1)^3$ with the *fat diagonal* Δ_3 removed, or its quotient by a subgroup of S_3. Trivially, these have a dense set of rational points. §5 follows [**Se**] to consider a renown example.

Take $(\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3) = \mathbf{C}$ to be three conjugacy classes from G. Let $\Sigma(\mathbf{C}^H)$ be the collection of $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3) \in G^3$ where (i) and (ii) hold (§1) and $\sigma_i \in \mathrm{C}_i^H$, $i = 1, 2, 3$. Here $h \in H$ acts on $\Sigma(\mathbf{C}^H)$ by conjugation:

$$h\boldsymbol{\sigma}h^{-1} = (h\sigma_1 h^{-1}, h\sigma_2 h^{-1}, h\sigma_3 h^{-1}).$$

Rigidity Condition. Assume $(G, H, \mathbf{C})$ satisfies $(\mathrm{iii})_H$ and (iv). Then, $(G, H, \mathbf{C})$-rigidity holds if H is transitive on $\Sigma(\mathbf{C}^H)$. For $r > 3$, [**Fr1**, Th. 5.1] and [**FrV**] generalize transitivity of G with *braid transitivity* This is transitivity of the combined action of the *Artin braid group* and H on the set analogous to $\Sigma(\mathbf{C}^H)$ (see Ex. 4.5).

Turn the definition of $\hat{G}^{\mathbf{C}}$ upside down to produce the group of a valuable cyclotomic field. Consider H with $G \le H \le \hat{G}^{\mathbf{C}}$. Recall $N_{\mathbf{C}}$. Define:

$$M_H = \{m \in (\mathbb{Z}/N_{\mathbf{C}})^* \mid \exists\, \tau \in S_r, \exists\, \beta \in H \text{ with } \beta \mathrm{C}_i \beta^{-1} = \mathrm{C}_{\tau(i)}^m, i = 1, \dots, r\}.$$

Ridigity Results. *Assume $(G, G, \mathbf{C})$-Rigidity and* (v) *hold. Then, there is a regular extension $\hat{L}/\mathbb{Q}(x)$ with Galois group G. More generally, suppose $(G, H, \mathbf{C})$-Rigidity and either* (v) *or* (vi) *hold. Then, there is an extension $L/\mathbb{Q}(x)$ giving a $(G, H', \mathbf{C})$ realization over $\mathbb{Q}$ with $G \le H' \le H$. Further, $\hat{L} \cap \bar{\mathbb{Q}} = \hat{\mathbb{Q}}$ contains the fixed field in $\mathbb{Q}(\zeta_{N_{\mathbf{C}}})$ of the group M_H.*

Discussion of proof/asides. These statements apply rarely if $r > 3$.

A. Addition of the braid action. With the braid action (as in (4.4) below) included in $(G, G, \mathbf{C})$-rigidity, Ridigity Results apply often for $r > 3$. For example, suppose $(\mathrm{iii})_H$ and (iv), the Schur multiplier of G is trivial, and each conjugacy class appears in $\mathbf{C}$ with suitably many repetitions. Then, $\mathcal{H}(G, H, \mathbf{C})$ is absolutely irreducible and defined over $\mathbb{Q}$ [**FrV**, App.]. Thus, for r suitably large (dependent on G), the problem is to find $\mathbb{Q}$ points on these varieties over $\mathbb{Q}$. [**Fr2**] discusses improvements and simplications effectively bounding r to guarantee these absolutely irreducible components over $\mathbb{Q}$. For $r = 4$, by hand calculations often produce rational spaces $\mathcal{H}(G, H, \mathbf{C})$ (or at least unirational—see Ex. 4.5 and §7), as in the many applications of [**DFr**], [**Fr5-7**] and [**Ma**]. Still, the modular curve example of §7 shows this isn't the general case.

B. Thompson's rigidity. The case of Rigidity Results with $H = G$, $r = 3$ and *each* conjugacy class rational in G, is Thompson's rigidity in [**Th**]. Suppose

$(G, G, \mathbf{C})$-rigidity and (vi) hold. Replace the representation giving (vi) with the regular representation to give (v). Take the fixed field of $G(1)$ in the field from the conclusion of the Rigidity Results. Thus, recover existence of the degree n extension giving the prescribed Galois closure. Conclude: The first statement of the Rigidity Results is equivalent to the statement with (v) replacing (vi).

C. The spaces $\mathcal{H}(G, H, \mathbf{C})$ when $r = 3$. When rigidity holds and $r = 3$, the natural cover $(\mathbb{P}^1)^3 \setminus \Delta_3 \to \mathbb{P}^3 \setminus D_3$ factors through $\mathcal{H}(G, H, \mathbf{C})$. For example, if a triple $(\sigma_1, \sigma_2, \sigma_3)$ has distinct conjugacy classes in H, then $\mathcal{H}(G, H, \mathbf{C})$-rigidity implies $\mathcal{H}(G, H, \mathbf{C})$ is $(\mathbb{P}^1)^3 \setminus \Delta_3$. Thus, branch points of a cover—corresponding to a point of $\mathcal{H}(G, H, \mathbf{C})$—determine the cover. Assuming rigidity, this cover has field of definition $\mathbb{Q}$ exactly when the branch points are in $\mathbb{Q}$. This is what makes the case $r = 3$ easy.

D. Diophantine information from modular curves. §7 applies modular curves to display cases where $\mathcal{H}(G, H, \mathbf{C})$ is absolutely irreducible over $\mathbb{Q}$, yet it has *no* rational points. Here, G is a dihedral group and $r = 4$. Completion of the inverse Galois problem for G follows from finding $\mathbf{C}$ where $\mathcal{H}(G, G, \mathbf{C})$ has rational points. [**FrV**, App.] says every finite group has a covering group G with corresponding $\mathbf{C}$ so $\mathcal{H}(G, G, \mathbf{C})$ is absolutely irreducible over $\mathbb{Q}$ (see A above). Finding rational points on $\mathcal{H}(G, G, \mathbf{C})$, or asserting this is unirational under these conditions, generalizes the dihedral group version of this problem in §7.

E. Production of $(G, H, \mathbf{C})$ realizations when $H \neq G$. If $(G, G, \mathbf{C})$-Rigidity holds, the arithmetic monodromy group must equal the geometric monodromy group. This is another contrast between the case $r = 3$ and $r > 3$. Look at the map (†) near the beginning of this section. [**FrV**, Prop. 3] shows—under conditions that happen for ∞-ly many $\mathbf{C}$ for a given G—$\mathcal{H}(G, G, \mathbf{C})$ is absolutely irreducible. So, the group of the cover $\Psi_{G,H}$ is H/G. Suppose further: $\mathcal{H}(G, G, \mathbf{C})$ has a single $\mathbb{Q}$ point and the function field of $\mathcal{H}(G, H, \mathbf{C})$ $\mathbb{Q}$ is pure transcendental. Then, a $\mathbb{Q}$ point on $\mathcal{H}(G, G, \mathbf{C})$ produces a $(G, G, \mathbf{C})$ realization over $\mathbb{Q}$. Still, by Hilbert's Irreducibility Theorem (§1), there are infinitely many $\mathbb{Q}$ points of $\mathcal{H}(G, H, \mathbf{C})$ producing $(G, H, \mathbf{C})$ realizations. This situation occurs often in the literature (see [**DFr**]). In practical cases this contrast occurs in moving from $r = 3$ to $r = 4$, where braid group action predominates.

Völklein's practical technique in [**V1**] and [**V2**] exploits this, playing on its theoretical use in [**FrV1-2**]. He simplifies calculations to prove $\mathcal{H}(G, H, \mathbf{C})$ is irreducible with pure transcendental function field by taking G an elementary affine group. His examples contrive G/H to include many Chevalley groups over non-prime finite fields. Thus, it is the function field of $\mathcal{H}(G, G, \mathbf{C})$ over the function field of $\mathcal{H}(G, H, \mathbf{C})$ that realizes the desired group as a Galois group.

F. Producing challenging situations when $r = 3$. We give one common example. Suppose $r = 3$, the union $\mathrm{C}_1 \cup \mathrm{C}_2 \cup \mathrm{C}_3$ is rational in G, and G is

centerless. Let α be an outer automorphism—without representative in S_n—of G that permutes the conjugacy classes of $\mathbf{C}$. Apply α to $\Sigma(\mathbf{C})$ by applying it to the coordinates of $\boldsymbol{\sigma} \in \Sigma(\mathbf{C})$. Then, $(G, G, \mathbf{C})$-rigidity can't hold; $\alpha(\boldsymbol{\sigma})$ is outside the orbit of $\boldsymbol{\sigma}$ under G. Now, consider the group $H = \langle G, \alpha \rangle$. Even if $(G, H, \mathbf{C})$-rigidity holds, it's not obvious what is the arithmetic monodromy group of a cover corresponding to a point of $\mathcal{H}(G, H, \mathbf{C})$. It might be G, H or something in between. □

A simple example shows how to compute by hand with Ridigity Results. This will draw the reader into H-versions of these definitions.

AN (A_5, S_5) REALIZATION BY A DEGREE 5 POLYNOMIAL OVER $\mathbb{Q}$. Let $\mathbf{C}$ be the conjugacy classes of the triple $(\sigma_1, \sigma_2, \sigma_3) \in S_5^3$ with $\sigma_1 = (1\,2\,3)$, $\sigma_2 = (1\,4\,5)$ and $\sigma_3 = (1\,2\,3\,4\,5)^{-1}$. These generate A_5. The union, however, of $\mathbf{C}$ isn't rational: the conjugacy class of σ_3 isn't rational. Indeed, σ_3^2 isn't conjugate to σ_3 in A_5, but it is in S_5. Still, S_5 is transitive on $\Sigma(\mathbf{C})$.

With no loss assume $\tau = (\tau_1, \tau_2, \tau_3)$ with $\tau_3 = \sigma_3$. Hold this condition while conjugating by powers of σ_3 to assume the common integer between τ_1 and τ_2 is one. Now, the product condition detects the τs exactly equal the σs. With $H = S_5$, the integer -1 generates M_H as a subgroup of $(\mathbb{Z}/5)^*$. Conclusion from the Rigidity Results: There is a unique (up to equivalence) degree 5 cover, $\phi : X \to \mathbb{P}^1$, having these branch cycles, defined over $\mathbb{Q}$ with 0, 1 and ∞ as branch points. Its monodromy group pair is (A_5, S_5). It produces $L/\mathbb{Q}$ with $\hat{L} = \mathbb{Q}(\sqrt{5})$. By the Riemann-Hurwitz formula its genus is 0 and the point over ∞ totally ramifies. A polynomial map gives this. □

Easily generalize this example to any odd non-square integer n.

EXERCISE 4.1. *Let $n > 5$ be an odd non-square. Show there are two conjugacy classes of n-cycles and neither is a rational conjugacy class. Assume:*

(4.1) *$(\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3)$ are, respectively, the conjugacy class of a 3-cycle, an $(n-2)$-cycle, and an n-cycle.*

Show this gives an (A_n, S_n) realization by a polynomial over $\mathbb{Q}$.

Indeed, you don't need rigidity for Ex. 4.1. You can play with these easy polynomials by hand. Here is a more substantial application of rigidity.

EXERCISE 4.2. *Assume* (4.1) *holds and $n > 5$ is an odd square. Show there are, as in Ex. 4.1, two conjugacy classes of n-cycles in A_n, but both are rational. Show this gives an $(A_n, A_n, \mathbf{C})$ realization by a polynomial over $\mathbb{Q}$.*

Polynomial problems are easy if each element of $\mathbf{C}$ is the conjugacy class of a disjoint cycle. The smallest digression from that increases the difficulty.

EXERCISE 4.3. *Assume $n > 4$ is an odd non-square. Let $\mathbf{C}$ be the conjugacy classes of the triple $(\sigma_1, \sigma_2, \sigma_3) \in A_n^3$ with $\sigma_1 = (1\,2)(3\,4)$, $\sigma_2 = (1\,3\,5\,6\,7\ldots n)$ and $\sigma_3 = (1\,2\ldots n)^{-1}$. Show the geometric monodromy group is A_n. For any distinct points, $x_1, x_2 \in \mathbb{Q}$, show there are $(n-3)/2$ inequivalent polynomial covers having x_1 and x_2 as finite branch points. Show there is an $(A_n, S_n, \mathbf{C})$ realization by a polynomial over $\mathbb{Q}$ if and only if*

$$g_n(\alpha) = ((n-2)\alpha^{n-1} - 2(\alpha + \cdots + \alpha^{n-2}) + (n-2))/(\alpha-1)^2 \tag{4.2}$$

has a zero of degree at most 2 over $\mathbb{Q}$.

Hint: If representing $f(y)$ for these covers is in $\mathbb{Q}[y]$, its derivative is $h(y) = (y-a)(y-b)y^{n-3} \in \mathbb{Q}[y]$. Conclude a, b are either in $\mathbb{Q}$ or they are conjugate over $\mathbb{Q}$. There are two other conditions:

$$f(x) = y^n/n - (a+b)y^{n-1}/(n-1) + aby^{n-2}/(n-2) + d; \text{ and } f(a) = f(b). \tag{4.3}$$

The last half of (4.3) gives a degree n equation in $b/a = \alpha$.

For $n = 5$, $g_5(\alpha) = 3\alpha^2 + 4\alpha + 3 = 0$. The two complex conjugate roots are in $\mathbb{Q}(\sqrt{-5})$. For this case, there is a polynomial over $\mathbb{Q}$.

PROBLEM 4.4. *For what odd $n > 5$ are the polynomials $g_n(\alpha)$ of Ex. 4.3 irreducible over $\mathbb{Q}$?*

Hint: *Mathematica* says they are irreducible for all n I tried (up to 31). Finally, a more challenging problem. As before, assume $n > 5$ is an odd non-square. We already noted we get (A_n, S_n) realizations from polynomials with all finite branch cycles 3-cycles. Instead, however, of 3-cycles, assume each finite branch cycle is a product of two disjoint 2-cycles. That is, $\mathbf{C} = (\mathrm{C}_1, \ldots, \mathrm{C}_{r-1}, \mathrm{C}_r)$ with each of $\mathrm{C}_1, \ldots, \mathrm{C}_{r-1}$ the conjugacy class of $(1\,2)(3\,4)$. If $n > 7$, such elements generate A_n [**Mu**]. Call such an f a (2)(2) polynomial.

EXERCISE 4.5. *Suppose $f \in \bar{\mathbb{Q}}[y]$ is a (2)(2) polynomial and $n = 7$. Show the geometric monodromy group of f is either $\mathrm{PSL}_2(\mathbb{Z}/2)$ (acting either on points or lines of projective 2-space), or it is A_7.*

Show both types occur and they fall into four families like those labeled $\mathcal{H}(G, H, \mathbf{C})$ above. Show the two families with geometric monodromy group $\mathrm{PSL}_2(\mathbb{Z}/2)$ are conjugate over $\mathbb{Q}(\sqrt{-7})$.

Hint: You'll need the braid group action on r-tuples. Here is the i-th *braid* operation Q_i acting on r-tuple $\boldsymbol{\sigma}$:

$$(\boldsymbol{\sigma})Q_i = (\sigma_1, \ldots, \sigma_{i-1}, \sigma_i\sigma_{i+1}\sigma_i^{-1}, \sigma_i, \sigma_{i+2}, \ldots, \sigma_r),\ i = 1, \ldots, r-1. \tag{4.4}$$

In Ex. 4.5, the *other* two families have geometric monodromy group A_n. Both are defined over K with $[K : \mathbb{Q}] \le 2$. We don't know which. If $K = Q$, the

two components of $\mathcal{H}(A_7, S_7, \mathbf{C})$ are unirational over $\mathbb{Q}$ and there are $(A_7, S_7, \mathbf{C})$ realizations by polynomials over $\mathbb{Q}$. If $[K : \mathbb{Q}] = 2$, there are none. For $n > 7$, all (2)(2) polynomials have A_n as geometric monodromy group. If they are in $\mathbb{Q}[y]$, they give (A_n, S_n) realizations. We don't know if there are any such.

§5. APPLYING RIGIDITY TO THE MONSTER

The Atlas [**At**] is a compendium on the sporadic simple groups. [**Se**, §7.4.4-§7.4.7] shows how to use listings of conjugacy classes and characters from [At]. Following Thompson [**Th**] it applies rigidity to the *Fischer-Griess Monster*.

The Monster M has rational conjugacy classes the Atlas labels $2A$, $3B$ and $29A$. These have elements of respective orders 2, 3, and 29. To prove this set of conjugacy classes is rigid, start by showing there are $|M|$ triples $(\sigma_1, \sigma_2, \sigma_3)$ satisfying (i) from these classes. For an ordinary group this would be a classical character computation, based on the *structure constant formula*. For M it is a computer calculation—done by a collaborator of Thompson. Anyone can now do this calculation using the program **GAP**, available by anonymous **ftp**. **GAP** contains the character table of the monster.

One must still prove all such triples generate the full Monster (condition (ii)). The plot thickens. Neither we nor the Atlas know the maximal subgroups of the Monster. The argument is therefore indirect. Some simple quotient of the group generated by $(\sigma_1, \sigma_2, \sigma_3)$ would have order $2 \cdot 3 \cdot 29 \cdot k$ dividing M. By the classification, no such simple group exists. [**Se**, p. 79] comments:

> "Although the proof of the classification has been announced, described and advertised since 1980, it is not clear on whether it is complete or not: the part on *quasi-thin* groups has never been published."

Manuscripts by Mason (circa 1979) and Aschbacher (1992) together prove the classification of quasi-thin groups. The scattered pieces of the classification proof may be complete. Still, consider the statement there are no simple groups whose orders satisfy the above conditions. We might want more detail. At present we have only this agrees with the orders of simple groups that appear in the Atlas. With the death of Daniel Gorenstein, who will guarantee completion of the *revision* project? More than to complete our confidence in the classification, Gorenstein wanted it accessible to a researcher not dedicated to group theory.

§6. SOLVABLE GROUPS AND REGULAR REALIZATIONS

Shafarevich's theorem: All solvable groups are Galois groups over $\mathbb{Q}$. Yet, do they have *regular* realizations? We don't even know if ℓ-groups are regular [**Se**, p. 9]. [**Se**, Chap. 2] proves ℓ-groups are Galois groups over $\mathbb{Q}$. This progression occurs on [**Se**, p. 17] following the realization of ℓ-groups.

PROP. 2.2.4 OF [**Se**]. *A solvable group G is a quotient of a semidirect product*

of a nilpotent group by a solvable group of order smaller than $|G|$.

Prop. 2.2.4 could appear in a first year graduate course in algebra. The next result, attributed to Shafarevich, Serre labels a claim.

CLAIM 2.2.5. *Split embedding problems with nilpotent kernels are solvable over number fields.*

Following this, induction shows realization of solvable groups over number fields. A proof of Claim 2.2.5 for split embedding problems with *abelian* kernels concludes the chapter. There you have it from Serre's viewpoint. Others declare the full claim is in order. Matzat gave a talk on 10/11/94 at U. Florida that had convincing detail. He says it will be in his soon to appear book with Malle. Still, this shows solvable groups aren't a piece of cake.

§7. DIHEDRAL GROUPS

Could it be dihedral groups are tougher than, say, the Monster? For regular realizations, the answer is "Yes!" Note: One Monster will face a hoard of dihedral groups. We start with an exercise from Serre's book.

EXERCISE 1 P. 36. *Show $\mathbb{Z}_p$ is not the Galois group of any regular extension of $\mathbb{Q}(x)$.* Recall: The p-adic numbers $\mathbb{Z}_p$ is a pro-cyclic group with cofinite subgroups of index p^n for some integer n. **Ans:** If it is, then $\mathbb{Z}/p^n$ is a quotient realization $L_n/\mathbb{Q}(x)$ of this regular extension. Among the generators of this Galois extension, there must be at least one of order p^n. This requires ramification in $L_n/\mathbb{Q}(x)$ of order p^n in at least one place. Consider conjugacy classes $\mathbf{C}$ representing inertia group generators for this extension. By the *Branch Cycle Argument* (§3), $\mathbf{C}$ is a rational union of conjugacy classes.

Each element, however, in an abelian group is in its own conjugacy class. Thus, there are at least $p^n - p^{n-1}$ appearances of elements of order p^n in $\mathbf{C}$. Each branch point for $L_n/\mathbb{Q}(x)$ also will be a branch point for $L_1/\mathbb{Q}(x)$. Here, L_1 is the field fixed by the index p subgroup of the Galois group. Thus, there is no bound on the number of branch points of $L_1/\mathbb{Q}(x)$, a contradiction. □

Take D_ℓ to be the *dihedral group* of degree ℓ, an odd prime. It is of order 2ℓ and two involutions generate it. Wreath products allow realizing D_ℓ as the group of a *regular extension* of $\mathbb{Q}(x)$. Obvious realizations, however, have covers with ℓ-cycles as inertia group generators of ramified places. Apply the Branch Cycle Argument. Elements of the group of an ℓ-cycle represent $(\ell-1)/2$ distinct conjugacy classes of D_ℓ. There are at least $(\ell-1)/2$ branch points. Are there *involution*—only involutions as branch cycles–realizations of D_ℓ for *all* ℓ?

THEOREM 1 [**DFr**, Theorem 5.1]. *Suppose $\ell > 7$ is a prime. If D_ℓ is the group of a regular extension of $\mathbb{Q}(X)$, the extension has at least six branch points.*

The Branch Cycle Argument above handles most of Theorem 1. The essential case eliminates involution realizations of D_ℓ with $r = 4$ branch points. Here is the main observation. Such a realization $L/\mathbb{Q}(x)$ has L a genus 1 function field whose Picard group has a point of order ℓ defined over $\mathbb{Q}$. It is classical this produces a rational point on the modular curve $X_1(\ell) \setminus \{\text{cusps}\}$. As $\ell > 7$, this contradicts Mazur's theorem ([**M**] or [**Se2**, Theorem 3]).

Contrast this with realizing the Monster. It is the group of a regular extension of $\mathbb{Q}(x)$ having 3 branch points. We conjecture there is no uniform bound on the number of branch points for realizing D_ℓs. Here, ℓ runs over odd primes.

CONJECTURE 2. *For any $r_0 < \infty$, only finitely many D_ℓs are the group of a regular extension $L/\mathbb{Q}(x)$ with at most r_0 branch points.*

Suppose r_0 contradicts this. The proof of Theorem 1 shows all but finitely many D_ℓs have involution realizations. We restate Conjecture 2.

CONJECTURE 2′. *For any r_0, only finitely many D_ℓs have involution realizations with at most r_0 branch points.*

Let $L/\mathbb{Q}(x)$ be an involution realization of D_ℓ. An automorphism of order ℓ fixes a degree 2 extension $T/\mathbb{Q}(x)$ with r (even) branch points. Also, L/T is a cyclic unramified extension of degree ℓ. That is, T is the function field of a hyperelliptic curve of genus $\frac{r-2}{2}$.

We want $\phi : \hat{X} \to \mathbb{P}^1$ of degree 2ℓ. It should have *branch cycles* $(\sigma_1, \dots, \sigma_r)$ with each σ_i an involution from D_ℓ. A complete combinatorial count of these is easy. From this deduce irreducibility of the *Hurwitz space* $\mathcal{H}(\mathbf{C}) = \mathcal{H}(r, \ell)$ parametrizing the desired equivalence classes of covers [**Fr3**, §3.2].

The converse to the Branch Cycle Argument (§3) shows there is a $\mathcal{H}(\mathbf{C})^{\text{in}} = \mathcal{H}(r, \ell)^{\text{in}}$, defined over $\mathbb{Q}$, that covers $\mathcal{H}(r, \ell)$ [FrV1]. Rational points on $\mathcal{H}(r, \ell)^{\text{in}}$ exactly correspond to involution realizations of D_ℓ. Our problem is to decide if $\mathcal{H}(r, \ell)^{\text{in}}$ has $\mathbb{Q}$ points. We relate $\mathcal{H}(r, \ell)^{\text{in}}$ to more classical looking objects.

Take $\alpha \in D_\ell$ of order ℓ. Form $\hat{X}/\langle\alpha\rangle = Y$, the quotient of $\hat{X}$ by the group generated by α. The degree 2 cover $Y \to \mathbb{P}^1$ presents Y as a hyperelliptic curve of genus $\frac{r-2}{2}$. Also, $\hat{X}$ is a cyclic degree ℓ unramified cover of Y. [**DFr**, Lemma 5.3] interprets existence of $\hat{X}$ as a property of $\text{Pic}^0(Y)$. This is essentially the Jacobian of Y. Denote the points of order ℓ on $\text{Pic}^0(Y)$ by $T_\ell = T_\ell(Y)$. Then, $G_\mathbb{Q}$ acts on T_ℓ. If $\boldsymbol{p} \in T_\ell \setminus \{0\}$ is a $\mathbb{Q}$ point, then $G_\mathbb{Q}$ has trivial action on $< \boldsymbol{p} >$. When a point has this property, denote the group it generates by $\mathbb{Z}/\ell$. This says $G_\mathbb{Q}$ has trivial action on it.

Similarly, $G_\mathbb{Q}$ acts on ℓ-th roots of 1. This is another copy of $\mathbb{Z}/\ell$, but to show $G_\mathbb{Q}$ has a particular nontrivial action on it, denote it by μ_ℓ. Consider the set $G_\ell(d)$, $d = \frac{r-2}{2}$, of involution realizations of D_ℓ defined over $\mathbb{Q}$ with r branch points. Let $\text{Pic}^1(Y)$ be the Picard space of degree 1 divisor classes on Y.

LEMMA. *Involution realizations of D_ℓ from a fixed Y as above correspond to certain $G_{\mathbb{Q}}$ equivariant injections from μ_ℓ into $T_\ell(Y)$. The image includes all $G_{\mathbb{Q}}$ equivariant injections $\mu_\ell \to T_\ell(Y)$ when $\mathrm{Pic}^1(Y)$ has a $\mathbb{Q}$ point.*

This falls in the territory of [**KM**]. They start with any integer $d > 0$. Their results support bounding number of torsion points with coordinates in F on all elliptic curves over $\mathbb{Q}$ over *all* F with $[F : \mathbb{Q}] = d$. [**DFr**, §5.3] lists the position of this and Conjecture $2'$ in a panoply of reasonable variants. A uniform bound on torsion on abelian varieties over $\mathbb{Q}$ of a given dimension implies both.

PROBLEM. *For fixed ℓ and large r is the Hurwitz space $\mathcal{H}(r,\ell)^{\mathrm{in}}$ unirational?*

A *Yes* answer would say this for each ℓ. If r is suitably large, involution realizations of D_ℓ with r branch points fall on a unirational variety. A variety W is unirational if it is the image of projective t-space for some t. If W and the map from this t-space have equations over $\mathbb{Q}$, we say W is unirational over $\mathbb{Q}$. Projective t-space has a dense set of rational points. Therefore, so would W have. Thus, there would be involution realizations of D_ℓ. We don't, however, know how to produce *any* involution realization of D_ℓ for an arbitrary ℓ.

Here is an analog of the problem from [**Se**] on regular realization of $\mathbb{Z}_p$. Fix a prime ℓ and form the projective limit D_{ℓ^∞} of D_{ℓ^n} s. Could there be a regular realization of D_{ℓ^∞}? First: This would be an involution realization of D_{ℓ^∞}.

The kernel $\mathbb{Z}_\ell$ of the $\mathbb{Z}/2$ quotient of D_{ℓ^∞} gives an extension $L/\mathbb{Q}(x)$ of degree 2. Suppose the D_{ℓ^∞} realization is ramified over L. Then, the inertia group for a branch point is a cyclic subgroup C of $\mathbb{Z}_\ell$ of finite index. Consider the branch point x' of $\mathbb{Q}(x)$ having C as inertia group for the whole realization. For each m, there is a regular extension $L_m/\mathbb{Q}(x)$ where the inertia group of x' has order ℓ^m. Use the Branch Cycle Argument: $L_m/\mathbb{Q}(x)$ has at least $(\ell^m - \ell^{m-1})/2$ branch points. Each will be a branch point for $L_1/\mathbb{Q}(x)$, a contradiction. A regular realization of D_{ℓ^∞} is an involution realization.

For each n, conclude the Jacobian A of L is isogenous to a variety B_n with a $\mathbb{Q}$ point of order ℓ^n. Follow Ribet's appendix to [**KL**]. Reduction modulo p gives a contradiction. Choose a prime p of good reduction of A different from ℓ. Since A and B_n are isogenous, their reductions have the same number of points over $\mathbb{F}_p$. Thus, ℓ^n divides the number of points on A mod p. Since the number of points on A is finite, taking n large gives a contradiction.

CONCLUSION. *There is no regular realization of D_{ℓ^∞} over $\mathbb{Q}(x)$.*

Our final comments use this conclusion to relate to other [Se] topics.

§8. AFTER SIMPLE GROUPS, THEN WHAT?

Every finite group G has infinitely many distinct totally nonsplit covers by finite groups. These fit together as a *projective* profinite group $\tilde{G}$. Quotients

of $\tilde{G}$ are these totally nonsplit covers of G. The kernel of the natural map $\tilde{G} \to G$ is a pronilpotent group. Primes dividing G are exactly those dividing the (supernatural) order of $\tilde{G}$, the *universal frattini cover* of G ([**FrJ**, Chap. 21]; for some serious examples, [**Fr2**, Part II]). A projective profinite group has *no* elements of finite order. This shows how many of these covers there are.

For each prime ℓ dividing the order of G, there is a variant $\tilde{G}_\ell$ on $\tilde{G}$. When $G = D_\ell$, then $\tilde{G}_\ell$ is D_{ℓ^∞}. Even when G is the alternating group A_5 of degree 5, and $\ell = 2$, $\tilde{G}_2$ is unknown. To solve the inverse Galois problem, we need all quotients of $\tilde{A}_5$ as Galois groups. This calls for a technique of some abstraction. For example, [**Fr2**, Part III] constructs towers of moduli spaces it calls *modular stacks*. These generalize the tower of modular curves $X_0(p) \leftarrow X_0(p^2) \leftarrow \cdots$. There is such a tower for any finite group G, any prime $p|\,|G|$ and any collection of conjugacy classes $\mathbf{C}$ in G of orders relatively prime to p. The diophantine considerations above all generalize to this situation.

Chapter 9 (the last) of Serre considers a piece of this topic. Suppose we have a regular realization $L_n/\mathbb{Q}(x)$ of A_n. Consider regular realization of the spin cover $\hat{A}_n$ of A_n, extending the realization of $L_n/\mathbb{Q}(x)$. The non-split cover $\hat{A}_n \to A_n$ has kernel $\mathbb{Z}/2$ in the center of $\hat{A}_n$. The book ends with elaborate exercises based on Mestre [**Me**] for achieving this realization. Serre is saying simple groups aren't the whole story. This considers only a small well understood quotient of $\tilde{A}_n$.

The field $\mathbb{Q}^{cyc}$ is Hilbertian with projective absolute Galois group. [**FrV2**] conjectures these properties give the conclusion of Shafarevich's conjecture (§0).

PROJECTIVE-HIT CONJECTURE. *If $K \subset \bar{\mathbb{Q}}$ is Hilbertian and G_K is projective, then G_K is free profinite.*

[**FrV2**] proves this when a condition stronger than projective holds: K is *pseudo-algebraically closed* or PAC. Here are two corollaries of this result. First: $G_{\mathbb{Q}}$ is an extension of the product of all the symmetric groups, $\prod_{n=1}^{\infty} S_n$ by the (countably) free profinite group. Second: Any complex finite extension of the field of *totally real algebraic numbers* has free profinite absolute Galois group. Further, the absolute Galois group of the totally real numbers is (pro)-freely generated by involutions [**FrHV**], and this generalizes to the field of *totally p-adic numbers* [**Po**]. These results use the full converse to the Branch Cycle Argument to solve embedding problems over large subfields of $\bar{\mathbb{Q}}$. Solving embedding problems is at the heart of what we would like from solutions of the inverse Galois problem. Rigidity Results (§4) emphasize this with its practical uses for questions on realizing arithmetic-geometric monodromy group pairs.

Speaking of solving embedding problems, I conclude with a mystery. We mentioned the PAC property for a field K and some of the deductions drawn from it and its variants. For example, any complex extension of the totally real numbers is PAC. That means, every absolutely irreducible variety over such a

field has rational points over that field. The abelian and nilpotent closures of $\mathbb{Q}$ aren't PAC ([**Fy**] or [**FrJ**, Cor. 10.15]). Still, is the solvable closure of $\mathbb{Q}$ PAC? A more general statement has consequences for the Inverse Galois Problem.

HENSELIAN CLOSURE PROBLEM [**FrJ**, Prob. 10.16]. *Is there a subfield of $\bar{\mathbb{Q}}$, neither formally real nor PAC, whose Henselian hulls are all algebraically closed?*

[**Se**] considers an active field with tools available for much further progress. It fits to conclude with a statement from Serre:

> "The inverse Galois problem gives us excuses for learning a lot of new Mathematics [**Se3**]."

REFERENCES

[At] J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, and R.A. Wilson, *Atlas of finite groups: maximal subgroups and ordinary characters for simple groups*, New York, Clarendon Press, 1985.

[B] G. V. Belyi, *On extensions of the maximal cyclotomic field having a given classical group*, J. Crelle **341** (1983), 147–156.

[Fy] G. Frey, *Pseudo algebraically closed fields with no-archimedian valuations*, J. of Alg. **26** (1973), 157–168.

[DFr] P. Debes and M.D. Fried, *Nonrigid constructions in Galois theory*, Pac. Jour. **163 #1** (1994), 81–122.

[Fr1] M. Fried, *Fields of Definition of Function Fields and Hurwitz Families and; Groups as Galois Groups*, Comm. in Algebra **5** (1977), 17–82.

[Fr2] M. Fried, *Introduction to Modular Towers: Generalizing dihedral group–modular curve connections*, Recent Developments in the Inverse Galois Problem, Cont. Math., proceedings of AMS-NSF, vol. 186, 1995, pp. 111–171.

[Fr3] M. Fried, *Global construction of general exceptional covers, with motivation for applications to coding*, AMS Cont. Math. series, proceedings of 2nd Annual conf. in Finite Fields, Las Vegas, 1994, pp. 1–42.

[Fr4] M. Fried, *Review of "Topics in Galois Theory," J.-P. Serre, ISBN 0-86720-210-6, Bartlett and Jones, 1992.*, BAMS **30 #1** (1994), 124–135..

[Fr5] M. Fried, *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Ill. J. of Math. **17** (1973), 128–146.

[Fr6] M. Fried, *Exposition on an Arithmetic-Group Theoretic Connection via Riemann's Existence Theorem*, A.M.S. Publications, Proceedings of Symposia in Pure Math: Santa Cruz Conference on Finite Groups,, vol. 37, 1980, pp. 571–601.

[Fr7] M. Fried, *Rigidity and applications of the classification of simple groups to monodromy, Part II – Applications of connectivity; Davenport and Hilbert-Siegel Problems*, Preprint from 1986.

[FrHV] M. Fried, D. Haran and H. Völklein, *Absolute Galois group of the totally real numbers*, C.R. Acad. Sci. Paris **317**, 95–99.

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

[FrV1] M.D. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli space*, Math. Ann. **290** (1991), 771–800.

[FrV2] M.D. Fried and H. Völklein, *The embedding problem over a Hilbertian PAC-field*, Annals of Math. **135** (1992), 469–481.

[KM] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number field*, Asterisque.

[KL] N. Katz and S. Lang, *Torsion points on abelian varieties in cyclotomic extensions*, K. Ribet's appendix, Enseignement Mathematique **27** (1981).

[M] B. Mazur, *Lecture Notes in Mathematics*, vol. 601, Springer-Verlag, 1977, pp. 107–148.

[Ma] B. H. Matzat, *Lect. Notes in Math.*, vol. 1284, Springer-Verlag, 1987.

[Mal] G. Malle, *Exceptional groups of Lie type as Galois groups*, J. Crelle **392** (1988), 70–109.

[Me] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(T)$ de groupe de Galois $\tilde{A}_n$*, J. Alg. **131** (1990), 483–495.

[Mu] Peter Müller, *Recent developments in the inverse Galois problem*, Editor: Michael Fried, AMS, Cont. Math. Series, 1995.

[Po] F. Pop, *Hilbertian fields with a universal local-global principle*, preprint, Heidelberg (1993).

[Se2] J.-P. Serre, *Points rationnels des courbes modulaire*, Sém. Bourbaki **30ème année n• 511** (1977/78).

[Se3] J.-P. Serre, *Conversation: Feit's Birthday Celebration at Oxford*, April, (1990).

[Sh] I. R. Shafarevich, *The embedding problem for split extensions*, Dokl. Akad. Nauk SSSR **120** (1958), 1217–1219.

[S] K. Shih, *On the construction of Galois extensions of function fields and number field*, Math. Ann. **207** (1974), 99–120.

[Th] J. G. Thompson, *Some finite groups which appear as $Gal(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$*, J. Alg. **89** (1984), 437–499.

[V1] H. Völklein, *$\mathrm{GL}_n(q)$ as a Galois group over the rationals*, Math. Ann. **293** (1992), 163–176.

[V2] H. Völklein, *Braid groups, embedding problems and the groups $\mathrm{PGL}_n(q)$, $PU_n(q^2)$*, Forum Math. **6** (1994), 513–535.

UC Irvine, Irvine, CA 92717, USA

E-mail address: mfried@math.uci.edu