

BOOK REVIEW

Topics in Galois Theory, by J.-P. Serre. Research Notes in Mathematics, 1992, Jones and Bartlett Publishers, xvi+116 pp. ISBN 0-86720-210-6

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 will describe Serre's view of present achievements toward that goal and comment on the territory he ignored. We will denote Serre's book by [Se] throughout the review.

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, and 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 1970s, acceptance took a long time. Then special approaches still held promise. Examples now show why earlier methods will not solve the complete problem.

Still, hope springs eternal. For example, Colliot-Théle'ne 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 if $G \leq S_n$ acting on $K(x_1, \dots, x_n)$ has invariants 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—simple and all encompassing—holds? Serre does not. 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 realization of all groups as Galois groups. If you could realize the Monster, would not easier simple groups follow; therefore the inverse Galois problem too? Section 8 comments why this was naive. Still, it renewed excitement in the topic.

The book is slightly over one hundred pages. With complete proofs it would have been three hundred pages. Yet, it would not have appeared quickly. There is something in it 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 $\overline{\mathbb{Q}}$. If $L = \mathbb{Q}(\alpha)$, each embedding corresponds to a zero of the irreducible polynomial for α over \mathbb{Q} . 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 \widehat{L}/\mathbb{Q} containing L , the Galois closure of L/\mathbb{Q} . Consider $G^L = G(\widehat{L}/\mathbb{Q})$ as L runs over all finite extensions of \mathbb{Q} . Suppose $L \subset L'$. The restriction homomorphism $G(\widehat{L}'/\mathbb{Q}) \xrightarrow{\text{rest}} G(\widehat{L}/\mathbb{Q})$ takes each automorphism of \widehat{L}' to \widehat{L} . Then $G_{\mathbb{Q}} = G(\widehat{\mathbb{Q}}/\mathbb{Q})$ is this subgroup of $\mathcal{G} = \prod_L G^L$: ∞ -tuples (\dots, α_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 big compact topological group having a countable number of topological generators. If there were a *free* set of generators, we would know a lot. For example, every finite group would be a quote of it. That is, given finite G , there would exist L with $G(\widehat{L}/\mathbb{Q}) = G$. This is the mildest version of the *inverse Galois problem*.

We know that $G_{\mathbb{Q}}$ does not have free generators. For example, a free group does not have elements of finite order. Yet $G_{\mathbb{Q}}$ contains an element of order 2, complex conjugation. Among its quotients we know there are the symmetric groups S_n and the alternating groups A_n (Hilbert). In addition, we know the quotients of $G_{\mathbb{Q}}$ include all sporadic simple groups (Feit, Matzat, and Thompson)—except possibly M_{23} , the Matthew group of degree 23, and all solvable groups (Shafarevich). See [Se] for explicit references on specific groups.

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 $\text{GL}_2(p)$, $\text{PSL}_2(p)$, and $\text{PGL}_2(p)$ as Galois groups (Belyi, Malle, and Shih especially). These are rank 1 Chevalley groups over the prime finite fields \mathbb{F}_p .

Serre records but a handful of Chevalley groups over nonprime finite fields as Galois groups [Se, p. 53]. None of these have rank exceeding 1. In the interim, Völklein [V1, V2] has realized series of higher rank Chevalley groups over nonprime finite fields. These use generalizations of rigidity not in [Se] (see §1).

If $G_{\mathbb{Q}}$ had free generators, so would many normal subgroups of infinite index, its commutator subgroup $[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$ in particular. This is the absolute Galois group of the maximal abelian extension \mathbb{Q}^{ab} of \mathbb{Q} . Kronecker in the last century showed $\mathbb{Q}^{\text{ab}} = \mathbb{Q}^{\text{cyc}}$, the field with all roots of 1 adjoined. The following conjecture would catch $G(\widehat{\mathbb{Q}}/\mathbb{Q})$ between well-known profinite groups, the countably generated free profinite group \widehat{F}_{ω} and the invertible profinite integers $\widehat{\mathbb{Z}}^*$.

Shafarevich's conjecture. $G(\widehat{\mathbb{Q}}/\mathbb{Q}^{\text{cyc}})$ is free profinite. Thus, this sequence is exact:

$$1 \rightarrow \widehat{F}_{\omega} \rightarrow G(\widehat{\mathbb{Q}}/\mathbb{Q}^{\text{cyc}}) \rightarrow G(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^* \rightarrow 1.$$

1. CLASSICAL TOPICS

[Se] demonstrates 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 1980s when regular realizations took over. Indeed, after the first two chapters the book concentrates on *regular extensions* $L/\mathbb{Q}(x): L \cap \overline{\mathbb{Q}} = \mathbb{Q}$. 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, Chapter 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 you to realize 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 of the applications of his irreducibility theorem. Regular realizations of G over Hilbertian K produce infinitely many disjoint Galois extensions of K with group G . This deduction 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: 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 $x \in L$. [Se] offers variants and deductions from it, sometimes without attribution (the observations of [Se, §4.6] outlining [FrJ, Theorem 12.7]). Regular realizations do more, so it must be a surprise that finding regular realizations has had more success than just finding realizations.

The main technique of *rigidity* dominates later chapters (see §4). The book, however, does not analyze limitations of rigidity. For example, there are solid reasons why rigidity cannot—as in *cannot possibly*—realize most groups as Galois groups. Indeed, for several years now it is generalizations of rigidity, and not rigidity, that have produced new groups as Galois groups over \mathbb{Q} . Serre's book does not comment on its generalizations. (These were present long before rigidity in [Fr].) Such general results, however, require conceptual additions that overwhelm the value of rigidity alone.

In §3 we comment slightly on these additions. Section 7 has an example that connects to the modular curve subtheme of [Se, Chapter 5]. Modular curves are covers of the sphere $\varphi: X \rightarrow \mathbb{P}^1$ ramified at three points in \mathbb{Q} . Indeed, the classical j function from complex variables uniformizes the copy of the sphere here. We may take the points of ramification of φ to be 0, 1, and ∞ . These particular curves, 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 its Galois closure has group generated by an element of order 2 and an element of order 3. This cover therefore appears as a quotient of the upper half-plane in \mathbb{C} by a subgroup

of $\mathrm{PSL}_2(\mathbb{Z})$ of finite index. Most such curves, however, are not modular curves. For modular curves each point on the curve has geometric significance. We explain briefly how [Sh] exploited that.

Let N be a positive integer. Consider the subgroup $\Gamma_0(N)$ of $\mathrm{PSL}_2(\mathbb{Z})$ with representing matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ where $c \equiv 0 \pmod{N}$. We especially want the case when the natural compactification $X = X_N$ of $H/\Gamma_0(N)$ is of genus 0. Classical theory defines this over \mathbb{Q} , but it also follows from rigidity (§4) generalized to include non-Galois covers. Various of the $\mathrm{PSL}_2(\mathbb{F}_p)$'s appear by interpreting rational points on twists of this cover when X_N is of genus 0. Serre reminds, without citation, this occurs only when $N \leq 18$ and $N \neq 7, 9, 11, 14-17$. There is a natural involution w on X_N . Consider points on X_N as pairs (E, E') of elliptic curves with a cyclic isogeny $E \rightarrow E'$, of degree N . The dual to this isogeny gives $E' \rightarrow E$. Define w from $w(E, E') = (E', E)$.

Consider a quadratic extension of K/\mathbb{Q} . Identify Galois groups $G(\mathbb{Q}(X_N)/\mathbb{Q}(X_N/\langle w \rangle))$ and $G(K/\mathbb{Q})$ with $\mathbb{Z}/2$. Thus, $G(K(X_N)/\mathbb{Q}(X_N/\langle w \rangle))$ 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 $K = \mathbb{Q}(\sqrt{(-1)^{(p-1)/2}})$ and $(\frac{N}{p}) = -1$ with p a prime. Consider an elliptic curve E over K with E and E^σ isogenous. Then

$$(*) \quad G_{\mathbb{Q}} \text{ acts on } p\text{-division points of } E \text{ with image in } \mathrm{PSL}_2(\mathbb{F}_p) \\ \text{(instead of in } \mathrm{PGL}_2(\mathbb{F}_p)\text{)}.$$

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 $(\frac{N}{p}) = -1$ or $N = 2, 3$, or 7 . It is clear Serre would honor continuations of these special results.

3. THE BRANCH CYCLE ARGUMENT-PRELUDE TO RIGIDITY

[Se, Chapter 6] gives complete references in support of *Riemann's existence theorem*. It is at the heart of rigidity and its generalizations. We will state a light version of it, without pedantic (albeit, important) equivalences. Suppose $L/\mathbb{C}(x)$ is a finite extension of degree n . Let $\widehat{L}/\mathbb{C}(x)$ be its Galois closure (§0). Then $G(\widehat{L}/\mathbb{C}(x))$ faithfully embeds in S_n . This embedding is unique up to conjugation of the image 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 $\frac{1}{x}$ if $x' = \infty$. The algebraic closure of $\mathbb{C}((x-x'))$ is $\bigcup_{e=1}^{\infty} \mathbb{C}(((x-x')^{1/e}))$. Thus, the absolute Galois group of $\mathbb{C}((x-x'))$ is pro-cyclic. Its generator $\sigma_{x'}$ has the effect $(x-x')^{1/e} \mapsto \zeta_e(x-x')^{1/e}$, $e = 2, 3, \dots$. Here $\zeta_e = e^{2\pi i/e}$. Since $\widehat{L}\mathbb{C}((x-x'))/\mathbb{C}((x-x'))$ is Galois, there is a minimal integer e with \widehat{L} embedding in $\mathbb{C}(((x-x')^{1/e}))$ as the identity on $\mathbb{C}(x)$. Compose any one embedding $\psi_{x'}: \widehat{L} \rightarrow \mathbb{C}(((x-x')^{1/e}))$ with an automorphism of \widehat{L} to get any other. Therefore, restriction of $\sigma_{x'}$ to \widehat{L} defines a conjugacy class of elements in $G(\widehat{L}/\mathbb{C}(x))$.

There are only finitely many x' with $e = e_{x'} > 1$. Label these $\mathbf{x} = (x_1, \dots, x_r)$, 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.

Now we explain the *branch cycle argument* from [Fr; prelude to Theorem 5.1]. Suppose $L/\mathbb{Q}(x)$ is a regular extension. Let $\widehat{L}/\mathbb{Q}(x)$ be the Galois closure of the extension. Take the constants of \widehat{L} to be $\widehat{\mathbb{Q}}$. The *arithmetic monodromy* group of the extension is $\widehat{G} = G(\widehat{L}/\mathbb{Q}(x))$. Similarly, the *geometric monodromy* group is $G = G(\widehat{L}/\widehat{\mathbb{Q}}(x))$. Then $G_{\mathbb{Q}}$ permutes the branch points x_1, \dots, x_r of $L/\mathbb{Q}(x)$. This permutation is a valuable invariant of the extension.

Take an embedding $\widehat{L} \subset \overline{\mathbb{Q}}((x - x_i)^{1/e_i})$. Adjoin all roots of 1 to \mathbb{Q} to get \mathbb{Q}^{cyc} . Let $\tau \in G(\overline{\mathbb{Q}}/\mathbb{Q})$ act on roots of 1 through restriction: $G(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow G(\mathbb{Q}^{\text{cyc}}/\mathbb{Q}) \cong \widehat{\mathbb{Z}}^*$ as in §0. Therefore, identify the image of τ with a supernatural integer $n_{\tau} \in \mathbb{Z}^*$. Also, identify action of τ on the x_i 's with a permutation of $1, \dots, r$. Suppose C_1, \dots, C_t is a collection of conjugacy classes of \widehat{G} . We say $C_1 \cup \dots \cup C_t$ is a *rational union* if it is closed under putting its elements to powers relatively prime to the orders of all elements in the union.

Branch cycle argument. *The assumptions on $L/\mathbb{Q}(x)$ and the x_i 's are as above. The conjugacy class of $\sigma_{\tau(i)}^{n_{\tau}}$ in \widehat{G} is the same as the conjugacy class of σ_i , $1, \dots, r$. In particular, the union of the conjugacy classes of $\sigma_{\tau(i)}$, $i = 1, \dots, r$, is a rational union of conjugacy classes in \widehat{G} .*

An illustrative case. Suppose in the above $x_1 \in \mathbb{Q}$. Let m be an integer relatively prime to $|\sigma_1|$. The result says taking m th powers of the conjugacy class of σ_1 in \widehat{G} maps this class into itself. Here is why. Choose $\tau \in G_{\mathbb{Q}}$ with $\tau(\zeta_{e_1}) = \zeta_{e_1}^m$. Apply τ to the coefficients of the images of \widehat{L} in $\mathbb{C}((x - x_1)^{1/e_1})$. This gives an automorphism of \widehat{L} . Compute the effect of the conjugation by τ on 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 .

4. RIGIDITY AND ITS GENERALIZATIONS

Theorem 5.1 of [Fr] gives a partial converse to the branch cycle argument. It uses moduli spaces to consider extensions $L/\mathbb{Q}(x)$ that produce the pair (G, \widehat{G}) as arithmetic and geometric monodromy groups of the Galois closure of the extension. If $[L: \mathbb{Q}(x)] = n$, both groups are naturally subgroups of S_n . In addition, G is a normal subgroup of \widehat{G} . For applications start by giving G and the conjugacy classes \mathbf{C} of generators $\sigma_1, \dots, \sigma_r \in G$. Assume

- (iii) *the union of these conjugacy classes is rational as from the branch cycle argument (see example in §7).*

Then there is a maximal group G^* that contains all possible \widehat{G} 's. Consider any group H between G and G^* . With extra conditions on G —especially G is centerless—the converse produces an algebraic set $\mathcal{H}(\mathbf{C}, G, H)$, defined over \mathbb{Q} . In addition, there are (finite) maps $\mathcal{H}(\mathbf{C}, G, G^*) \rightarrow \mathcal{H}(\mathbf{C}, G, H)$, also defined over \mathbb{Q} .

Converse of branch cycle argument ([Fr], with refined conditions in [FrV]). *Here is a diophantine condition equivalent to existence of $L/\mathbb{Q}(x)$ realizing (G, H) as monodromy groups of the Galois closure $\widehat{L}/\mathbb{Q}(x)$ with conjugacy*

class data \mathbf{C} . There is $\mathbf{p}^* \in \mathcal{H}(\mathbf{C}, G, G^*)$ whose image in $\mathcal{H}(\mathbf{C}, G, H)$ has coordinates in \mathbb{Q} and $\mathbb{Q}(\mathbf{p}^*)/\mathbb{Q} = (G^* : H)$. (Since the \mathcal{H} 's are moduli spaces, these apply with any field K replacing \mathbb{Q} .)

For the inverse Galois problem take $G \leq S_n$ the regular representation of G and $H = G^*$.

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

Section 7 discusses the case that includes modular curves (§2). The spaces \mathcal{H} are manifolds. Thus, they cannot have rational points unless they are absolutely irreducible over \mathbb{Q} . To investigate this point, we go through the special case of rigidity [Se, §7.3]. Rigidity rarely applies unless $r = 3$. When $r = 3$, the \mathcal{H} 's are either $(\mathbb{P}^1)^3$ with the *fat diagonal* removed or its quotient by a subgroup of S_3 . Trivially, these have a dense set of rational points. Our next sections follow [Se] to consider historical examples.

Take $(C_1, C_2, C_3) = \mathbf{C}$ to be three conjugacy classes from G . Let $\Sigma(\mathbf{C})$ be the collection of $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ where (i) and (ii) hold from §3 and $\sigma_i \in C_i$, $i = 1, 2, 3$. Here G acts on $\Sigma(\mathbf{C})$ by conjugation:

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

Rigidity condition. *In addition to (iii), G with no center is rigid on \mathbf{C} if it acts transitively on $\Sigma(\mathbf{C})$. For $r > 3$ [Fr; Theorem 5.1, FrV] generalize this by replacing transitivity of G by transitivity of an action of the Artin braid group.*

5. APPLYING RIGIDITY TO THE MONSTER

[At] contains a compendium on the sporadic simple groups. Indeed, [Se, §§7.4.4–7.4.7] is a lesson in using listings of conjugacy classes and characters that appear in [At]. Here he follows Thompson [Th] to apply rigidity to the *Fischer-Griess Monster*.

The Monster M has rational conjugacy classes [At] labels $2A$, $3B$, and $29A$. These have elements of respective orders 2, 3, and 29. To prove this set of conjugacy classes is rigid, you 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.

One must still prove all such triples generate the full Monster (condition (ii)). The plot thickens. [At] does not list maximal subgroups of the Monster; we do not know them yet. 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. Here [Se, p. 79] pauses to comment on the classification.

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 that there are no simple groups whose orders satisfy the above conditions. We might want more detail. At present we have only that this agrees with the orders of simple groups that appear in [At]. With the death of Daniel Gorenstein, who will guarantee completion of the *revision* project? More than to complete the classification, Gorenstein wanted the classification accessible to a researcher not dedicated to group theory.

6. SOLVABLE GROUPS AND REGULAR REALIZATIONS

Shafarevich's theorem is that all solvable groups are Galois groups over \mathbb{Q} . Yet, do they have *regular* realizations? We do not even know if l -groups are regular [Se, p. 9]. Still, [Se, Chapter 2] has a proof that l -groups are Galois groups over \mathbb{Q} . This progression occurs on [Se, p. 17] following the realization of l -groups.

Proposition [Se, Proposition 2.2.4]. *Any solvable group G is a quotient of a semidirect product of a nilpotent group by a solvable group of order smaller than $|G|$.*

Proposition 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.*

From this, induction shows realization of solvable groups over number fields. The chapter concludes with a proof of Claim 2.2.5 for split embedding problems with *abelian* kernels. There it is from Serre's viewpoint. Others declare the full claim is in order. Still, this shows solvable groups are not a piece of cake.

7. DIHEDRAL GROUPS

Could it be that 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 are a pro-cyclic group with cofinite subgroups of index p^n for some integer n . Answer: 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 , a prime. It is of order $2l$ and two involutions generate it. Wreath products allow realization of D_l , for l a prime, as

the Galois group of a *regular extension* of $\mathbb{Q}(x)$. The obvious realization, however, has covers with l -cycles as inertia group generators of ramified places. Apply the *branch cycle argument* as above. Elements of the group of an l -cycle represent $(l-1)/2$ distinct conjugacy classes of D_l . The number of branch points of $L/\mathbb{Q}(x)$ must be at least $(l-1)/2$.

Are there D_l realizations for *all* l using just involutions as branch cycles? This is an *involution realization* of D_l .

Theorem 1 [DFr, Theorem 5.1]. *For $l > 7$ 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 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 that this produces a rational point on the modular curve $X_1(l) \setminus \{\text{cusps}\}$. As $l > 7$, this contradicts Mazur's theorem ([M] or [Se2, Theorem 3]).

Contrast this with realizing the Monster. It is a Galois 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_l 's.

Conjecture 2. *Let l run over odd primes. For any finite r_0 , only finitely many D_l 's are the group of a regular extension $L/\mathbb{Q}(x)$ with at most r_0 branch points.*

Suppose r_0 contradicts the conjecture. The proof of Theorem 1 shows we must have involution realizations for all but finitely many D_l 's. We restate Conjecture 2.

Conjecture 2'. *For any r_0 only finitely many D_l 's have involution realizations with at most r_0 branch points.*

Consider 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. That is, T is the function field of a hyperelliptic curve of genus $(r-2)/2$. Also, L/T is a cyclic unramified extension of degree l .

We want $\varphi: \widehat{X} \rightarrow \mathbb{P}^1$ of degree $2l$. It should have *branch cycles* $(\sigma_1, \dots, \sigma_r)$ with each σ_i an involution. A complete combinatorial count of these is easy. From this deduce irreducibility of the *Hurwitz space* $\mathcal{H}(\mathbf{C}) = \mathcal{H}(r, l)$ that parametrizes the desired equivalence classes of covers.

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

Take $\alpha \in D_l$ of order l . Form $\widehat{X}/\langle \alpha \rangle = Y$, the quotient of \widehat{X} by the group generated by α . The degree 2 cover $Y \rightarrow \mathbb{P}^1$ presents Y as a hyperelliptic curve of genus $(r-2)/2$. Also, \widehat{X} is a cyclic degree l unramified cover of Y . [DFr, Lemma 5.3] interprets existence of \widehat{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 $T_l = T_l(Y)$. Then $G(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ acts on T_l . If $\mathbf{p} \in T_l \setminus \{0\}$ is a \mathbb{Q} point, then $G(\overline{\mathbb{Q}}/\mathbb{Q})$ has trivial action on $\langle \mathbf{p} \rangle$. When a point has this property, denote the group it generates by \mathbb{Z}/l . This says $G_{\mathbb{Q}}$ has trivial action on it.

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

Lemma. *Involution realizations of D_l from a fixed Y as above correspond to a subset of $G_{\mathbb{Q}}$ equivariant injections from μ_l into $T_l(Y)$. The image includes all $G_{\mathbb{Q}}$ equivariant injections $\mu_l \rightarrow T_l(Y)$ when $\text{Pic}^1(Y)$ has a \mathbb{Q} point.*

This puts us in the territory of results of [KM]. Indeed, Conjecture 2' is stronger in many ways than the statements in [KM] conjecturing bounded torsion over F with $[F : \mathbb{Q}] = d$ on elliptic curves over \mathbb{Q} for all d .

Problem. *For fixed l and large r are the Hurwitz spaces $\mathcal{H}(r, l)^{\text{in}}$ 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 . Thus, there would be involution realizations of D_l . We do not, however, know how to produce any involution realizations 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 $D_{l\infty}$ of D_{l^n} 's. Could there be a regular realization of $D_{l\infty}$? First: This would be an involution realization of $D_{l\infty}$.

The kernel \mathbb{Z}_l of the $\mathbb{Z}/2$ quotient of $D_{l\infty}$ corresponds to an extension $L/\mathbb{Q}(x)$ of degree 2. Suppose the $D_{l\infty}$ realization is ramified over L . Then the inertia group for a branch point is a cyclic subgroup C of \mathbb{Z}_l of finite index. Consider the branch point of $\mathbb{Q}(x)$ having C as inertia group for the whole realization. For each integer m there is a regular extension $L_m/\mathbb{Q}(x)$ where this branch point has corresponding inertia group of order l^m . Use the branch cycle argument. This extension has at least $(p^m - p^{m-1})/2$ branch points. Since each will be branch points for $L_1/\mathbb{Q}(x)$, we have a contradiction. A regular realization of $D_{l\infty}$ is an involution realization.

For each n conclude that 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 $A \bmod p$. Since the number of points on A is finite, taking n large gives a contradiction.

Conclusion. *There is no regular realization of $D_{l\infty}$ 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} between \tilde{G} and G are these totally nonsplit covers of G . The kernel of the natural map $\tilde{G} \rightarrow G$ is a pronilpotent group whose (supernatural) order is divisible exactly by the primes dividing G . This is the *universal frattini cover* of G [FrJ, Chapter 21].

A projective profinite group has *no* elements of finite order. This gives some feeling for how many of these covers there are.

For each prime l dividing the order of G , there is a variant \tilde{G}_l on \tilde{G} . When $G = D_l$, \tilde{G}_l is D_{l^∞} . Even when G is the alternating group A_5 of degree 5 and $l = 2$, \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.

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 \tilde{A}_n of A_n , extending the realization of $L_n/\mathbb{Q}(x)$. The nonsplit cover $\tilde{A}_n \rightarrow A_n$ has kernel $\mathbb{Z}/2$ in the center of \tilde{A}_n . The book ends with elaborate exercises based on Mestre [Me] for achieving this realization. Serre is saying simple groups are not the whole story. This considers only a small, well-understood quotient of \tilde{A}_n .

The cyclotomic numbers have the property they are a Hilbertian field with projective absolute Galois group. [FrV2] conjectures these two properties alone suffice for the conclusion of Shafarevich's conjecture (§0).

Projective-HIT conjecture. *If $K \subset \overline{\mathbb{Q}}$ is Hilbertian and G_K is projective, then G_K is free profinite.*

[FrV2] proves this conjecture when a condition stronger than projective holds. Here are two corollaries of this. 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. These results use the full converse to the branch cycle argument to solve embedding problems over large subfields of $\overline{\mathbb{Q}}$. Indeed, solving embedding problems is at the heart of what we would like from solutions of the inverse Galois problem.

So, [Se] considers an active field with tools available for much further progress. It is fitting 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*, Clarendon Press, New York, 1985.
- [B] G. V. Belyi, *On extensions of the maximal cyclotomic field having a given classical group*, J. Crelle **341** (1983), 147–156.
- [DFr] P. Debes and M. Fried, *Nonrigid situations in constructive Galois theory*, Pacific J. Math. (1993), in proof August 1993.
- [Fr] M. Fried, *Fields of definition of function fields and Hurwitz families and Groups as Galois groups*, Comm. Algebra **5** (1977), 17–82.
- [FrJ] M. Fried and M. Jarden, *Field arithmetic*, Ergeb. Math. Grenzgeb., vol. 11, Springer-Verlag, Berlin and New York, 1986.
- [FrV] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), 771–800.
- [FrV2] ———, *The embedding problem over an Hilbertian-PAC field*, Ann. of Math. (2) **135** (1992), 1–13.
- [KM] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Columbia University Number Theory Seminar, 1992, Astérisque (to appear).
- [KL] N. Katz and S. Lang, *Torsion points on abelian varieties in cyclotomic extensions* (Appendix by K. Ribet), Enseign. Math. **27** (1981).

- [M] B. Mazur, *Rational points on modular curves*, Lecture Notes in Math., vol. 601, Springer, New York, 1977, pp. 107–148.
- [Ma] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math., vol. 1284, . Springer, New York, 1987.
- [Ma1] 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. Algebra **131** (1990), 483–495.
- [Se] J.-P. Serre, *Topics in Galois theory*, Res. Notes in Math., vol. 1, Jones and Bartlett, Boston and London, 1992.
- [Se2] ———, *Points rationnels des courbes modulaires*, Sémin. Bourbaki, 30ème année no. 511 (1977/78).
- [Se3] ———, Conversation at Walter Feit’s birthday celebration at Oxford in 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 fields*, Math. Ann. **207** (1974), 99–120.
- [Th] J. G. Thompson, *Some finite groups which appear as $\text{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$* , J. Algebra **89** (1984), 437–499.
- [V1] H. Völklein, *$\text{GL}_n(q)$ as Galois group over the rationals*, Math. Ann. **293** (1992), 163–176.
- [V2] ———, *Braid group action, embedding problems and the groups $\text{PGL}_n(q)$, $\text{PU}_n(q^2)$* , Forum Math. (1994) (to appear).

MICHAEL FRIED
 UNIVERSITY OF CALIFORNIA AT IRVINE
E-mail address: mfried@math.uci.edu