RECENT PROGESS ON THE INVERSE GALOIS PROBLEM

MICHAEL D. FRIED

1. Introduction

I discuss three problems related to the geometric (regular) realization of groups as Galois groups. The first two are over $\mathbb{Q}$, the last is over $\mathbb{C}$. Let k_0 be the algebraic closure of a finite field. I decided against adding a fourth: progress on describing fundamental groups of projective curves over k_0. We expect these groups will be different for each conjugacy class of curves. Still, combining work of Fried-Stevenson-Tamagawa has given a model for how to describe possibilities for these fundamental groups. I'm working on a paper explaining that.

1.1. **documentation.** The result of Thompson-Voelklein in §2 has appeared, though with little exposition, which I add here. Precise description of the completion of the genus 0 problem in §4, its applications and the new problems it exposes appears in my paper, "Variables separated polynomials, the genus 0 problem and moduli spaces," soon to appear in the conference volume for A. Schinzel's 60th birthday. This and the papers documenting results on Modular Towers and their application to the Inverse Galois Problem (§3) (including in the conference "Recent developments in the Inverse Galois problem" and in the Schneps edited volume #243 of the London Math. Soc.) are available by e-mail as Latex files.

1.2. **Brief notation.** Take z to be an indeterminate, algebraically independent of any elements in the complex numbers $\mathbb{C}$. For a field K (usually $K \leq \mathbb{C}$) G_K denotes the absolute Galois group of the Galois closure of K. A regular realization of a (finite) group G over a field K is a Galois field extension $L/K(z)$ having group G with L containing no nontrivial constants. It corresponds uniquely to a Galois cover $\phi_L : X_L \to \mathbb{P}^1_z$ of projective nonsingular, geometrically irreducible curves over K. The number r of branch points ($z_0 \in \mathbb{C} \cup \{\infty\}$ over which X_L has less than $\deg(\phi_L)$ geometric points) is the roughest measure of the complexity of the realization. When we say *regular realization* without mentioning the field, we mean over $\mathbb{Q}$. Groups with a central p-Sylow (for some prime p) suit Shafarevic's approach to the Inverse Galois problems. Regular realizations, however, work for all other groups. We say a group has rank t if t is the minimal number of elements that generate it. The symmetric group of degree n is S_n, the alternating group A_n.

2. Chevalley groups of arbitrary rank over a given finite field

Serre's book, "Topics in Galois Theory," p. 53, says even by 1992 the only Chevalley groups over nonprime finite fields with known regular realizations were $\mathrm{PSL}_2(\mathbb{F}_{p^2})$, $p = \pm 2 \bmod 5$, and a small further finite list. Fried-Voelklein proved (Annals 1992) that $G_{\mathbb{Q}}$ is an extension of a profree group by the infinite product of

Date: October 10, 1998.

the groups S_n, $n = 2, 3, \ldots$. Voelklein used the method to realize many high rank Chevalley groups over $\mathbb{F}_q$ for any prime power q.

To systemize this progress, Thompson-Voelklein recently aimed to prove the following. For each finite field $\mathbb{F}_q$, excluding finitely many exceptions, each Chevalley group has a *large family* of regular realizations parametrized by a unirational Hurwitz space over $\mathbb{Q}$. The problem breaks naturally into showing this for each Chevalley group series. They proved it this year for the symplectic family $\mathrm{Sp}_n(\mathbb{F}_q)$, $n = 1, 2, \ldots$ and each square q different from a power of 2. This precise result bodes well for predicting which conjugacy classes produce the crucial property: Hurwitz spaces that are near abelian covers of the moduli space of unordered branch points.

3. Perfect groups associated to a simple group

§2 gives progress on regular realizations of simple groups. Is there a natural way to extend that to all finite groups? For example, is there a serious generalization of Serre's idea of considering spin group covers of alternating groups.

There is, and it falls under the following rubric. Let G be any finite, centerless perfect group. Example: G any nonabelian simple group. Let p be a prime dividing the order of G. Then there exists a sequence of perfect, centerless group covers $\cdots \to G_{k+1} \to G_k \to \cdots G_0 = G$, with each morphism having a nontrivial p as kernel that are the exact analog for G as the sequence $\cdots \to \mathbb{Z}/p^{k+2} \times^s \{\pm 1\} \to \mathbb{Z}/p^{k+1} \times^s \{\pm 1\} \to \cdots \mathbb{Z}/p \times^s \{\pm 1\} = D_p$ is to D_p. When $G_0 = A_n$ and $p = 2$, this generalizes Serre's program; G_1 factors through the spin cover, and the geometry of the spin cover figures significantly for this case. Further properties:

(3.1a) The groups G_k all have the same rank as does $G = G_0$.

(3.1b) Conjugacy classes of elements of order prime to p in G lifts uniquely to classes of the same order in G_k.

(3.1c) If $H \to G$ is any finite group cover with p-group kernel, then there exists an integer k for which $G_k \to G$ factors through $H \to G$.

Note: A regular realization of G_k produces a regular realization of all G_i s. $i \le k$.

Even the most refined braid rigidity results (the main tool for regular realization) give no reason why realization of G_k is hard if realization of G_0 is easy (as in the A_5 case below). Distinguishing the G_k s for regular realizations requires a diophantine subtlety. Here is one way to say this.

Theorem 3.1 (Fried)**.** *Let r_0 be any integer (like two trillion). Suppose each G_k has a regular realization with no more than r_0 branch points. Result: Then, there exists some integer $r \le r_0$, conjugacy classes $C_1, \ldots, C_r = \mathbf{C}$ on G of orders prime to p and a Modular Tower*

$$(*) \cdots \to \mathcal{H}(G_{k+1}, \mathbf{C}) = \mathcal{H}_{k+1} \to \mathcal{H}(G_k, \mathbf{C}) = \mathcal{H}_k \to \cdots \mathcal{H}(G, \mathbf{C}) = \mathcal{H}_0$$

such that each level $\mathcal{H}_k$ has a $\mathbb{Q}$ point.

Part of the result is, of course, investigating the spaces $\mathcal{H}_k$. The main conjecture is that this can't happen: If k is large, then $\mathcal{H}_k$ has no $\mathbb{Q}$ point. When $r = 4$, sequence (*) consists of quotients of the upper half plane, covering the j-line (minus ∞). Sequence (*) is the classical tower of modular curves $\cdots X_1(p^{k+1}) \to X_1(p^k) \cdots$ when $G = D_p$ and $\mathbf{C}$ is four copies of the involution conjugacy class. Showing the Main Conjecture would generalize Serre's theorem for $G_{\mathbb{Q}}$ acting on torsion points on elliptic curves. This year saw the first nontrivial new case of this conjecture:

$G = A_5$, $p = 2$ and $\mathbf{C}$ is four repetitions of the conjugacy class of 3-cycles. It suggests diophantine considerations rule out easy ways to get regular realizations from pure group theory on *rational* unions of conjugacy classes. Yet, looking at options left open from §2 (assuming the Main Conjecture holds) forces looking for such realizations in places here-to-fore unsuspected.

4. Genus 0 problem

Let $f \in \mathbb{C}(x)$ be a rational function. Denote the Galois (monodromy) group of the splitting field Ω_{f-z} of $f(y) - z$ over $\mathbb{C}(z)$ by G_f. The genus zero problem: Excluding alternating and cyclic groups, only finitely many simple groups occur as composition factors (subquotients) of monodromy groups of rational functions. Contributors toward the genus 0 problem include Aschbacher, Guralnick, Magaard, Müller, Neubauer, Thompson and many others.

Monodromy groups of compositions of rational functions are subgroups of the wreath product of the monodromy groups of the composition factors. This reduces the problem to considering indecomposable rational functions; the monodromy group is primitive. Guralnick-Thompson then applied the classification based taxonomy of primitive groups by Aschbacher-ONan-Scott. Further, they did several primitive cases. One is of affine groups $V \times^s H$ with H acting irreducibly on the vector space V. A result of Liebeck and Saxl on fixed point ratios joined with Guralnick-Thompson to exclude Chevalley groups over sufficiently large fields. A small list of exceptions exists over finite fields of cardinality at most 113.

This showed, for fixed g, only finitely many Chevalley groups over a field of cardinality at least 113 occur as composition factors of monodromy groups of genus g covers. (As g grows, there will be more Chevalley groups over $\mathbb{F}_q$, $|q| > 113$; the number, however, is still finite.) That left, however, Chevalley groups of arbitrarily large rank over these unconsidered finite fields. Frohardt-Magaard and Liebeck-Shalev together show Chevalley groups of sufficiently large rank (depending on g, though over any field) are not composition factors of monodromy groups of genus g covers. This applies to covers of any fixed genus—though the rank goes up. Thus, 1998 saw completion of the Guralnick-Thompson conjecture for composition factors of genus g covers, and the original formulation of the genus 0 problem.

4.1. **Relation to pure geometry.** The genus 0 problem makes a partial contribution to a tough problem from classical algebraic geometry. Forming the Galois closure of the degree n cover $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is an algebraic process. The minimal Galois closure cover $\hat{f} : \hat{X}_f \to \mathbb{P}^1_z$ of f is a component of the n-fold fiber product of f. Galois theory and fiber products are mathematical cousins. What is the relevance of this?

Suppose X is *any* projective, nonsingular, curve over $\mathbb{C}$. Assume also X has a presentation of the following kind. There exists f for which $\hat{X}_f$ maps surjectively to X. Then, this gives a completely algebraic construction of X from rational functions in x: none of Riemann's transcendental theory needed here. The genus 0 problem, however, is not precise about what curves X appear in this way. Several problems, including the generalization of Hilbert's irreducibility theorem called Frey irreducibility, desperately require this extra information.

4.2. **Types of covers by a generic curve of genus g.** We expect indecomposable covers of any genus g to have a few natural families of monodromy groups, with

finitely many exceptional groups. The alternating and symmetric groups appear in many ways for all values of g. It isn't known in what ways these appear for the generic curve of genus g. For example, Hurwitz spaces of A_n, 3-cycle covers with r branch points have exactly two components, unless the covers have genus 0 (then they have exactly one component). Each component maps to the moduli space of curves $\mathcal{M}_g$ of genus $g = r - n + 1$. Fried-Klassen-Kopeliovic recently showed each component (with $g \geq 0$) has image dimension in $\mathcal{M}_g$ at least one. It isn't known if for each g there exist (r, n) with the map to $\mathcal{M}_g$ generically surjective.

Suppose $g = 0$ and G is alternating or symmetric and the degree of the cover is large. Then, a paper of Guralnick suggests the only permutation representations are the natural permutation action or the action on subsets of $\{1, \ldots, n\}$ of cardinality two. These both give genus zero covers and with many types of branch cycles (Nielsen classes).

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