VARIABLES SEPARATED POLYNOMIALS, THE GENUS 0 PROBLEM AND MODULI SPACES

MICHAEL D. FRIED

ABSTRACT. The *monodromy method*—featuring braid group action—first appeared as a moduli space approach for finding solutions of arithmetic problems that produce reducible variables separated curves. Examples in this paper illustrate its most interesting aspect: investigating the moduli space of exceptions to a specific diophantine outcome. Explicit versions of Hilbert's irreducibility theorem and Davenport's problem fostered this technique and motivated the *genus 0* problem started by J. Thompson and taken up by many group theorists. We review progress on the genus 0 problem in 0 characteristic, and its quite different contributions in positive characteristic.

Example: Let f and h be polynomials with coefficients in a number field K. The classification of finite simple groups shows there is a bound on exceptional degrees for f to the following result. If f is indecomposable and h is not a composition with f, then $f(x) - h(y)$ is irreducible. This answered challenge problems on factorization of variables separated polynomials posed by A. Schinzel in the early 60's. This limitation result holds, however, only in characteristic 0, one difference between the Genus 0 Problem here and in positive characteristic. Finite field example—Davenport's Problem: For each finite field $\mathbb{F}_q$ there are infinitely many surprising polynomial pairs (f, h) (of degree prime to the characteristic) whose value sets are equal over $\mathbb{F}_{q^t}$, $t = 1, 2, \ldots$.

Though we include unpublished results from 30 years ago, a new set of problems stretch the methods. Example of a general theme: Let M_d be the elements of $\bar{\mathbb{Q}}$ of degree no more than d over $\mathbb{Q}$. The *degree d reducibility* set of f, $\mathcal{R}_f(d)$ is $\mathcal{R}_f(d) = \{z_0 \in M_d \mid f(y) - z_0 \text{ is reducible over } \mathbb{Q}(z_0)\}$. Similarly, there is a *value* set $\mathcal{V}_f(d)$ (degree 1 fiber). Following a reduction due to G. Frey, for any integer d, there are polynomials f of unbounded degree satisfying $\mathcal{R}_f(d) \setminus \mathcal{V}_f(d)$ is finite.

The full monodromy method finds precise arithmetic information by extending observations from modular curves. A semi-classical observation: Divisors with support in cusp points on modular curves generate a torsion group on the Jacobian of the curve. Illustrations here (from alternating group covers) show generalizations of this issue are ubiquitous with the monodromy method.

Date: October 25, 2001.

1991 *Mathematics Subject Classification.* Primary 12F05; Secondary 14H40, 14D20, 14E20.

Key words and phrases. Moduli spaces of covers, Hilbert's Irreducibility Theorem, Siegel's Theorem, permutation representations.

Support from NSF #DMS-9622928 and from Alexander von Humboldt Foundation and Institut für Experimentalle Mathematik, July 1996. Bob Guralnick has been a valuable consultant on several group theory points, the genus 0 problem in positive characteristic and on the contributions of Ram Abhyankar. Belated thanks to John McLaughlin, who taught me much finite group theory at the blackboard when I was a graduate student. I've often said this: *The 20th century of mathematics belong to group theory; and I don't just mean Lie groups.* After an early period in diophantine approximation, I passed through algebraic number theory heading towards algebraic geometry. Still, before he died, Harold Davenport and I found a common topic in finite fields through his questions on polynomials having equal value sets.

Contents

1. Historical Introduction

Andrzej Schinzel posed basic problems about possible reducibility of separated variables polynomials $f(x)-h(y)$. I heard these when I was a graduate student (University of Michigan, 1964–1967) in talks of Davenport, Lewis and Schinzel. These same mentors researched Hilbert's irreducibility theorem, diophantine generalities related to using finite fields, and collections of curves whose individual members had only finitely many integral points. Exposure to these disparate problems revealed a common element. Aspects of problems involving reducibility, value sets of polynomial (Davenport's problem in particular) and explicit statements about Hilbert's irreducibility theorem had rephrasing with fiber products. With the *monodromy method*, it was possible to solve good chunks of these problems producing easy to state results. One example: If $f \in \mathbb{C}[x]$ is indecomposable, there are only a finite number of possible degrees ($\deg(f) = 7$, 11, 13, 15, 21 and 31) giving nontrivial examples of variables separated $f(x) - h(y)$ that factor. This result, however, has

a different outcome in positive characteristic: part of the story of this paper. §2.1 discusses further the influence of Schinzel.

1.1. **Finiteness results.** Problems about curve covers in characteristic 0 often show a finiteness phenomenon. Usually, there is some finite set of counterexample degrees to the expected behavior. Describing and explaining the finite type variety of exceptions, as in §8 describing *Davenport Polynomials* of degree 13, was often the most exciting work. This direction led to the *braid group* technique for treating the *Inverse Galois problem*. Still, with the Harbater-Raynaud solution of Abhyankar's Conjecture, it is time for analogous problems in positive characteristic.

Nothing here, however, is so simple as it was in characteristic 0. The reducibility results, Davenport's problem, the genus 0 problem; all have applications over a given finite field. Though characteristic zero results guide what happens in positive characteristic, §5 illustrates by example the difference. Even when restricting degrees of polynomials to be prime to the characteristic, allowing wild ramification permits hordes of genus 0 monodromy groups not appearing in characteristic 0. This is one of three topics this paper takes beyond present literature. In particular, over every finite field $\mathbb{F}_q$ ($q = p^r$), we produce infinitely many degrees n, prime to p, where there are polynomial pairs (f, h) with these properties.

(1.1a) (f, h) are not linearly related though both have degree n.
(1.1b) $\mathcal{V}_f(\mathbb{F}_{q^t}) = \mathcal{V}_h(\mathbb{F}_{q^t})$ for each positive integer t.

1.2. **Moduli space examples and the genus 0 problem.** The monodromy approach to considering families of curves for practical problems has immediate benefits. Suppose the problem interprets a property of curves as a covering property. Then, the method displays each appropriate curve as a member of a Hurwitz family. This paper aims to dispell the idea this rubric introduces extra abstraction. Compelling problems about curves, of all levels of abstraction, usually attract our attention through covering properties. An example, of course, are problems on variables separated polynomials. These suit covering space and Galois theory formulations through fiber products (§2.1). The group theory here is an algebraists analog of how (nonabelian) harmonic analysis appears in studying solutions of variables separated partial differential equations.

Group theory is the main tool for using this approach. A researcher's background and concerns, however, can inform an appropriate technical comfort level. We illustrate with two examples:

(1.2a) Families of Davenport polynomial pairs of degree 13 (§8).
(1.2b) Families of curves deriving from the appearance of the alternating group as the monodromy of the cover (§7).

The text justifies our choices by answering this basic question: How can one sufficiently decide the nature of this family to see if it contains curves with appropriate arithmetic properties? Then, having revealed this structure, the technique uses the new information to generate related investigations. So, Schinzel's original questions about reducibility of variables separated polynomials inspired methods influencing the literature around the Inverse Galois problem and ranks of abelian variety points over $\mathbb{Q}$. For these topics we revisit the territory (and relationship of) [Fri90] and [Mes90]. The examples in this paper stress formulas connecting such families to covers of the classical j-line. Structured connections to (and generalizations of)

modular curves create both a challenge and an aid. We emphasize the former, including a natural Inverse Galois Problem question that requires knowing the group of divisor classes generated by cusp points (Thm. 7.4). [FB98] uses *projective systems* of cusp points on a *Modular Tower* to develop the structure of this example.

Properties of curve families appear in the embeddings of these curves in their jacobians, and these bring challenges to the monodromy method. Serre's eclectic book [Ser97] could be the start of many issues applying the monodromy method. §1.3 gives our second precise problem in this direction. We conclude here, however, with the pervading role of the genus 0 problem (§6).

Let $f \in \mathbb{C}(x)$ be a rational function. Denote the Galois group of the splitting field Ω_{f-z} of $f(y) - z$ over $\mathbb{C}(z)$ by G_f. The genus 0 problem says, excluding cyclic, alternating and symmetric groups, it is a rare group occuring as G_f for *any* indecomposable rational function f. Our examples reveal its significance and also that something completely different occurs in positive characteristic.

The genus 0 problem makes a partial contribution to a tough problem from classical algebraic geometry. D. Mumford privately (1989) pointed to a confusing relation between them, so I set that straight. 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 (§2.1.3). 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. Lemma 6.7 makes more pointed comments and §1.3 elaborates in detail on a related problem.

1.3. **New aspects of irreducibility.** §2.4 introduces the stronger Frey-Type version of Hilbert's irreducibility. Showing Frey-Type irreducibility holds requires variants on the following. Suppose $f(x) \in \mathbb{C}[x]$ and d' is a positive integer. Consider the Galois group G_f of $\Omega_{f(x)-z} = \Omega$ over $\mathbb{C}(z)$ as a subgroup of S_n. For k satisfying $2 \le k \le n-2$, denote by $\Omega^{(H_k)}$ the fixed field in Ω of the subgroup $H_k < G$ leaving the set $\{1, \dots, k\}$ invariant. Problem: Show for n large there are polynomials f of degree n where $\Omega^{(H_k)}$ contains no element t with $[\Omega^{(H_k)} : \mathbb{C}(t)] < d'$. This should hold (with f fixed) for all $2 \le k \le n-2$. Our examples responding to this situation (provided by Faltings' proof of Lang's conjecture) illustrate fascinating challenges.

Finally, §2.5 lets us compare with pure diophantine interests of other researchers. Several speakers at the Schinzel conference (Summer 1997) considered how to decipher from a collection of variables separated curves over $\mathbb{Q}$ if each has but finitely many integral points. Theoretically [Fri73b] listed all such. I compare this with their results to illustrate the value of even simple aspects of the *monodromy method*.

1.4. **Comment on the classification.** We use the classification of finite simple groups. §9 completes the group theory limiting degrees of reducible examples of variables separated polynomials. [Mül95] lists the complete set of monodromy groups of *indecomposable* polynomials in characteristic 0 (Def. 2.3). [Mül96] lists the monodromy groups of rational functions of form $f(x)/x$ with f a polynomial.

Still, the first motivating problem in the subject, Thm. 2.6, required considering factorization of variable separated *rational functions* (with special denominators; see Thm. 2.6 and (2.8)). [DF99, §5] discusses the role of [Fri86] in both Müller papers. These use the results in §9 and in [Fri]. The latter finishes the group theory for the case of factorization requiring special denominators.

These papers show that increasing the rational function denominator degrees increases how hard it is to decide their monodromy groups. This is because the monodromy groups of polynomials of degree n (resp. rational functions of form $f(x)/x$) have an n-cycle (resp. $n-1$-cycle). Until the mid-20th century, the predominant literature considered permutation representations with small nearly transitive subgroups. The genus 0 problem goes far beyond this territory (§6).

Still, group theory applied to the problems motivating this paper went far on simple classical results. Example: Representation theory appears in the splitting of a doubly transitive degree n representation into a sum of a 1-dimensional representation an irreducible $n-1$ dimensional representation (proof of Lemma 5.4). As a consequence, if f is indecomposable, then considering $f(x)-h(y)$ reducible reduces to where h has these properties.

(1.3a) h is indecomposable.
(1.3b) the (doubly transitive) permutation representations for h and f are equivalent as group representations.

This observation brought in the combinatorial tool of difference sets of doubly transitive designs, allowing *hand calculation—a necessity in 1968* of all exceptional cases within a few days. This is a different *explicit* calculation from seeing the coefficients of the polynomials.

2. Explicit Topics

This section gives the history and specific goals of the topics from §1.

2.1. **Variables separated curves as fiber products.** In his renown 1982 book [Sch82], Schinzel considered topics on separated variables polynomials only sporadically. We comment on these.

(2.1a) [Sch82, p. 19–39] proves Ritt's Theorem.
(2.1b) [Sch82, p. 57] notes reducibility of $T_4(x)+T_4(y)$, T_4 the degree four Chebyshev polynomial ($T_4(\cos(\theta))=\cos(4\theta)$; example of [DLS61], see §11.3).

He then suggests:

> For further instances of reducibility of $[f(x)-h(y)]$ over $\mathbb{C}$ see [reference for [Fri73a]].

2.1.1. *Comments on* (2.1a). [Sch82, p. 40–42] notes Ritt's Theorem essentially describes all polynomials $\varphi(x,y)$ over $\mathbb{Q}$ with the following properties.

(2.2a) $\varphi(x,y)=0$ has infinitely many quasi-integral solutions (over $\mathbb{Q}$).
(2.2b) $\varphi(x,y)=f(x)-h(y)$ is a variables separated polynomial.
(2.2c) $(\deg(f),\deg(h))=1$.

[Fri73b, p. 47] already has this observation and then it gives a short proof of Ritt's Theorem. [Sch82, p. 42] then states:

> Neither the lemma nor the theorem is true in this case [without the assumption $(\deg(f), \deg(h)) = 1$]. More general but less precise results can be found in Fried [reference for [Fri73b]].

That suggests [Fri73b] isn't explicit. We review those results in §2.5. [Fri73b] shows that describing *all* $\varphi(x, y)$ satisfying (2.2a) and (2.2b) requires only adding to this result the possibilities that occur if $(\deg(f), \deg(h)) = 2$ (instead of 1). Though harder than Ritt's Theorem, it is still explicit.

2.1.2. *Comments on* (2.1b). Though [Sch82] has only the factorization of $T_4(x) + T_4(y)$ (see §11.3), Schinzel spent much research time on variables separated polynomials. The titles and topics of [DLS61], [DLS64], [Sch63], [Sch67] show this. His 1970 International Congress talk, [Sch70] (including brief reports on [Fri70] and [Fri73a]), especially concentrates on variables separated polynomials and searches for examples of reducibility. For practical applications, variables separated polynomials have several qualities to recommend them.

- (2.3a) They correspond to a natural geometric construction: *fiber product*.
- (2.3b) Using (2.3a) supports Galois theory and Riemann's Existence Theorem.
- (2.3c) Fiber products allow comparing the arithmetic of two covers of the sphere.
- (2.3d) Resonant classical examples, including modular curves, contribute to arithmetic resolution of many problems producing fiber products.

On the other hand, Schinzel's influence on the author was straightforward in the topic of Bauerian fields and Hilbert's irreducibility theorem. Schinzel's main papers on these topics appeared just before the author met him the first time. Bauerian fields make their appearance in a strong form in this paper. Davenport's problem over a finite field (§5.5) is a classification problem asking when a suitably restricted pair of function field extensions are Bauer (or Kronecker) conjugates.

2.1.3. *Fiber product notation.* There is rarely any harm in replacing any curve that appears here by its unique nonsingular projective model. To do so requires only applying the process of normalization. We explain more why we do this.

Given a curve X over a field K, complete it to $\bar{X}$ in any ambient project space which contains it. Then, the normalization $\bar{X}^*$ of $\bar{X}$ has a canonical K-surjection $\bar{X}^* \to \bar{X}$. This is an isomorphism in a neighborhood of any nonsingular point of $\bar{X}$. You can normalize any variety. The result, however, may be singular (if the variety is not a curve) along a subset of codimension at least 2. For curves it is exactly analogous to considering the complete ring of algebraic integers in a number field rather than the ring generated by the zeros of a 1-variable polynomial.

Denote the sphere by $\mathbb{P}^1 = \mathbb{P}^1_z$: the affine line union with a disjoint point at ∞. Let $\varphi_X : X \to \mathbb{P}^1_z$ and $\varphi_Y : Y \to \mathbb{P}^1_z$ be two (nonsingular curve) covers of the sphere. The set theoretic fiber product $X \times_{\mathbb{P}^1_z} Y$ is the points $(x, y) \in X \times Y$ with $\varphi_X(x) = \varphi_Y(y)$. This has a natural algebraic curve structure. The next lemma, however, shows a problem from singularities.

Lemma 2.1. *A point (x_0, y_0) on $X \times_{\mathbb{P}^1_z} Y$ is singular if and only if both x_0 and y_0 ramify over $\mathbb{P}^1_z$. Let e_{x_0} be the ramification index of x_0 over its image, and e_{y_0} the ramification index of y_0 over its image. Suppose* $\mathrm{char}(K)$ *divides neither e_{x_0} nor e_{y_0}. Then, the greatest common divisor of e_{x_0} and e_{y_0}, (e_{x_0}, e_{y_0}), is the number of*

geometric points on the normalization of $(x, y) \in X \times Y$ *lying over* x_0*. Each such point has ramification index* $e_{y_0}/(e_{x_0}, e_{y_0})$ *(over* x_0*).*

Proof. See, for example, [DF99, Lemma 7.1]. The idea is (before normalization, and if $\mathrm{char}(K)$ divides neither e_{x_0} nor e_{y_0}) a neighborhood of (x_0, y_0) is like a neighborhood of $(0, 0)$ on the curve $x^{e_{x_0}} = y^{e_{y_0}}$. □

Thus, it behooves us to form the normalization of the curve above immediately. This allows assuming the fiber product is a nonsingular curve, covering naturally both X and Y by projection on each factor. Fiber products let us compare properties of the arithmetic fibers of φ_X and φ_Y. There is much literature on this type of problem over finite fields, and Hilbert's Irreducibility Theorem is an example statement that occurs over number fields. Here is a fundamental question.

Question 2.2. When is $X \times_{\mathbb{P}^1_z} Y$ irreducible?

The particular case with $X = \mathbb{P}^1_x$ and $Y = \mathbb{P}^1_y$ (copies of $\mathbb{P}^1_z$ with maps by rational functions) still seems difficult. Yet, fundamental investigations occurred in the late 60's and early 70's, motivated by problems of Schinzel [Sch63]. These resolved many issues when the maps are by polynomials (and some rational function cases).

2.1.4. *Indecomposability.* There is a general notion that a cover, $\varphi : X \to Z$, is indecomposable. That is, φ does not *decompose* into $\psi_X : X \to W$ and $\psi : W \to Z$ with $\deg(\psi_X) > 1$ and $\deg(\psi_Y) > 1$. For rational functions this is especially explicit.

Definition 2.3. We say $f \in K(y)$ is *decomposable* (over K) if $f = f_1(f_2(y))$ for rational functions $f_1, f_2 \in K(y)$ with $\deg(f_i) > 1$, $i = 1, 2$. Otherwise, f is *indecomposable*. Further, $f, h \in K(y)$ are *linearly related* (over K) if $h = f(L(y))$ with L a linear fractional transformation (over K).

The author wrote three papers related to this topic: [Fri73a], [Fri73b] and [Fri87]. [Fri73b, Corollary on p. 47 to Thm. 3] lists all $f(x) - h(y)$ having a genus 0 factor with infinitely many quasi-integral points over a number field K. Comments from [Fri87] remind of the simply stated (n, m)-problem. This problem relaxs completely the stringent condition that f is indecomposable, for factorization of $f(x) - h(y)$ §11.4. The next three subsections each describe a classical arithmetic problem, with a synopsis of modern developments.

2.2. **Explicit Hilbert's Irreducibility Theorem for special covers.** *Nielsen classes* capture *much* (though sometimes not all) of the discrete data separating covers into connected families. It is useful in even the most down-to-earth problems.

2.2.1. *Monodromy groups and Nielsen classes.* Suppose $\varphi : X \to \mathbb{P}^1_x$ is an absolutely irreducible cover defined over a field K. Then, it is easy to characterize when φ is equivalent to a polynomial map over K. The conditions are these.

(2.4) There is a unique point of X lying over ∞; and X has genus 0.

The word equivalent here means φ is equivalent (according to (7.4)) to a cover given by a polynomial map. If we are comfortable extending coordinate changes to an algebraic closure $\bar{K}$ of K, then some map equivalences are simplified. Example: For polynomial maps, cyclic covers are equivalent to $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ given by $x \mapsto (x - a)^n + b$ for some $a, b \in \bar{K}$. If φ is a polynomial cover, but not cyclic, then only the point ∞ ramifies totally.

More general data comes by carefully labeling the ramification type of the cover. Let $\hat{X} \to \mathbb{P}^1_x$ be the Galois closure of the cover, and let G be its group. Notice: G sometimes depends on K. Trivial Example: $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ by $x \mapsto x^n$ is cyclic of order n over an algebraically closed field (of characteristic prime to p). Over $\mathbb{Q}$, however, the Galois closure of f has group $\mathbb{Z}/n \times^s (\mathbb{Z}/n)^*$. The *arithmetic* monodromy group of φ is the Galois closure group $\hat{G}$ over K. The *geometric* monodromy group G is the Galois closure group G over $\bar{K}$. Geometric ramification gives the best clue for computing the group of the Galois closure of a cover.

Let $z_1, \dots, z_r$ be the branch points of φ (§3.1). Apply §3.2.2 to attach a canonical set of geometric monodromy group conjugacy classes $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$ to the tame part of inertia over the branch points.

Definition 2.4. Finally, suppose all ramification is tame. To the data $(G, \mathbf{C})$ associate its *Nielsen class*:

$$\mathrm{Ni}(G, \mathbf{C}) = \mathrm{Ni}(\mathbf{C}) = \begin{array}{l}\{\boldsymbol{g} \in G^r \mid \langle \boldsymbol{g} \rangle = G,\ g_1 \cdots g_r = 1 \\ \quad \text{and there exists } \sigma \in S_r,\ g_{(i)\sigma} \in \mathrm{C}_i, i = 1, \dots, r\}.\end{array} \tag{2.5}$$

Elements of G act on $\mathrm{Ni}(G, \mathbf{C})$ by conjugation. Let $N_{S_n}(G, \mathbf{C})$ be the subgroup of S_n that normalizes G and permutes the conjugacy classes $\mathbf{C}$ (preserving the multiplicity of their appearance). If $h \in N_{S_n}(G, \mathbf{C})$, then h maps $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$ to $h\boldsymbol{g}h^{-1}$, conjugation of all entries in the r-tuple by h.

Example 2.5 (S_5 acting on A_5)**.** Consider the case $\mathbf{C} = (\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}_3)$ with C_1 the conjugacy class of 3-cycles, and $C_2 = C_3$ the conjugacy class of $(1\,2\,3\,4\,5)$. Then, $N_{S_5}(G, \mathbf{C}) = A_5$ because conjugation by $(2\,3)$ maps $(1\,2\,3\,4\,5)$ to an element of A_5 not conjugate to $(1\,2\,3\,4\,5)$ in A_5. Consider the conjugacy class of $(1\,3\,2\,4\,5)$, C^*. Similarly, the normalizer is still A_5 if we put C^* in place of C_1. Yet, if $\mathbf{C}^* = (\mathrm{C}_1, \mathrm{C}_2, \mathrm{C}^*)$, the normalizer is S_5: conjugation by $(2\,3)$ switches C_2 and C^*.

Let $\boldsymbol{z}$ be any r distinct points of $\mathbb{P}^1_z$. Then, Riemann's Existence Theorem 3.2 neatly interprets the elements $\mathrm{Ni}(G, \mathbf{C})/N_{S_n}(G, \mathbf{C})$. They correspond one-one with degree n covers having branch points $\boldsymbol{z}$ with $\mathbf{C}$ as associated conjugacy classes, up to equivalence (§7.3). Assume the center of G is trivial. There is a related interpretation for $\mathrm{Ni}(G, \mathbf{C})/G$; these elements correspond to Galois covers having a canonical identification of the group with G. Grothendieck's Theorem (Thm. 3.3) extends this correspondence to characteristic p if p does not divide the order of G.

2.2.2. *HIT for polynomial covers.* Here is a result from [Fri74] and [Fri86] motivating this paper. Let $\mathcal{A}$ be a fractional ideal of $\mathbb{Q}$. For $f \in \mathbb{Q}[y]$ denote $\{z_0 \in \mathcal{A} \mid f(y) - z_0 \text{ is reducible}\}$ by $\mathcal{R}_f(\mathcal{A})$. Also, denote $\mathcal{A} \cap f(\mathbb{Q})$ by $\mathcal{V}_f(\mathcal{A})$. Use the notation $f \in S_{\mathcal{A}}$ if the following holds:

(2.6) $f \in \mathbb{Q}[y]$ with $\mathcal{R}_f(\mathcal{A}) \setminus \mathcal{V}_f(\mathcal{A})$ infinite.

Theorem 2.6 (Explicit HIT)**.** [Fri86]*: Suppose $f \in S_{\mathcal{A}}$. Then:*

(2.7a) *either* $\deg(f) = 5$*; or*

(2.7b) *f is decomposable over $\mathbb{Q}$.*

Further, if f satisfies (2.7a)*, then one from the following holds. Either f is in the family defined by the Nielsen class of $(S_5, \mathbf{C})$ with representative*

$$((2\,3)(4\,5), (1\,2), (1\,4), (1\,2\,3\,4\,5)^{-1}),$$

or the cover has only two finite branch points and its Nielsen class comes from coalescing an element of $\mathrm{Ni}(S_5, \mathbf{C})$.

[DF99] discussed geometric and arithmetic properties of the family of the Nielsen class $(S_5, \mathbf{C})$. It showed this family gives nontrivial examples of $f \in S_{\mathcal{A}}$.

What has Thm. 2.6 to do with reducibility of variables separated polynomials? Suppose $f(x) - h(y)$ factors into $\varphi_1(x,y)\varphi_2(x,y)$, and h is not composite with f. Then, values $h(y_0) = z_0$ with $y_0 \in \mathbb{Q}$ produce factorizations $\varphi_1(x,y_0)\varphi_2(x,y_0)$ of $f(x) - z_0$. That infinitely many $y_0 \in \mathbb{Q}$ must satisfy $h(y_0) \in \mathcal{A}$ puts a restriction on h from Siegel's famous theorem [Sie29]. [Fri74, Introd.] notes these two possibilities.

(2.8a) Either $h(y)$ is a polynomial, or;
(2.8b) $h(y) = u(y)/(m(y))^k$ with $u, m \in \mathbb{Q}[y]$, $\deg(m) = 2$, and m has real roots, conjugate over $\mathbb{Q}$.

2.3. **Synopsis of the group theory handling** (2.8)**.** Suppose (2.8a) occurs over some field K of characteristic 0. Let $\Omega_{f(x)-z}$ be the Galois closure of the extension $K(x)/K(z)$. Then, Lemmas 4.3 and 5.4 put the following limitation on the group of $\hat{G} = G(\Omega_{f(x)-z}/K(z))$.

2.3.1. *Use of doubly transitive groups.* There are two faithful transitive permutation representations $T_1, T_2 : \hat{G} \to S_n$ with $n = \deg(f) = \deg(h_1)$, h_1 is a composition of h and the following hold.

(2.9a) T_1 and T_2 are both doubly transitive.
(2.9b) T_1 and T_2 are equivalent as group representations, though they are inequivalent as permutation representations.
(2.9c) There exists $g_\infty \in G$ with $T_1(g_\infty)$ (and $T_2(g_\infty)$) an n-cycle.

Equivalent as group representations means the *traces* (number of fixed points) of $T_1(g)$ and $T_2(g)$ are the same for all $g \in G$.

[Fri73a, Thm. 2] excluded possibility (2.8a) if

$$K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}. \tag{2.10}$$

This exclusion was by pure arithmetic, without using the classification of finite simple groups. The argument required two steps.

(2.11a) Showing there is an integer j, $(j,n) = 1$, with the n-cycle g_∞ not conjugate in $N_{S_n}(G)$ to g_∞^j.
(2.11b) Applying the general *branch cycle argument* ([Fri77], [Fri95a] or [Fri94b]) to conclude from (2.11a), no cover with group G and just one branch cycle in this conjugacy class has field of definition K satisfying (2.10).

The author's approach to producing the variables separated polynomials of exceptional degrees required modest knowledge of group theory, as the proof of Thm. 9.1 shows. It relies on the notion of *difference set* and that a double transitive design with a Singer n-cycle must have an attached difference set appearing in the linear relation between the x_i's and the y_i's. A succinct description, with all the details for the exceptional degrees, is in [Fri73a, p. 134-135].

2.3.2. *Appearance of the classification.* [Fri73a] also contains the conjecture whose proof appears now in [CKS76]. The classification of finite simple groups lists all doubly transitive representations of groups (of degree n) containing an n-cycle. This practical result appears in the proof of the next result's first statement.

Theorem 2.7. *Groups G having permutation representations T_1 and T_2 satisfying* (2.9) *consist of a group of degree 11, and groups between* $\mathrm{PSL}_k(\mathbb{F}_q)$ *and* $P\Gamma L_k(\mathbb{F}_q)$ *for some $k \geq 3$ and q. These latter groups have degree $(q^k-1)/(q-1)$. Further, the only groups among these that could be the geometric monodromy group of a polynomial in characteristic 0 have degrees* 7, 11, 13, 15, 21 and 31.

For each degree in Theorem 2.7 there are polynomials in characteristic 0 having the appropriate group as monodromy group. §8 uses the Nielsen class description of the complete space of the degree 13 polynomials, showing this is a rational variety. Let α be a generator of the degree four extension of $\mathbb{Q}$ in $\mathbb{Q}(e^{\frac{2\pi i}{13}})$. This parameter space has $\mathbb{Q}(\alpha)$ as field of definition.

2.3.3. *Further comments on using group theory.* Thm. 2.7 might leave the impression this monodromy approach requires intricate knowledge of group theory. It never completely removes us from dealing with *particular* polynomials, and it does require learning some group theory. Still, it effortlessly opens territory in seeking examples of phenomena. So, it is worth pausing to consider how it relies on the classification. In particular, should someone find a gap in the classification, we should know exactly how it would affect this result. The proof of Thm. 2.7 in §9.1 traces to [CKS76] a classic paper extracting practical tools from the classification.

§5 shows there is no bound on degrees like that of Thm. 2.7 when considering monodromy groups of polynomials over finite fields. This is true even if we restrict polynomial degrees to be prime to the characteristic. Some subtle differences do occur in the group theory for polynomial covers in positive characteristic. See especially §5.4.3 and §5.4.4 for a character statement from the *geometry* relating f and h in a variables separated statement. Yet, in the examples appearing here, it is wild ramification in the inertia groups in positive characteristic giving unbounded degrees. So, Riemann's Existence Theorem (RET) doesn't apply. This confounding of the genus 0 problem in positive characteristic has many arithmetic applications. For example, one expects value sets of polynomials on all extensions of a given finite field to determine the polynomial up to linear equivalence. A significant set, however, of indecomposable counterexamples to this come from the failure of Thm. 2.7 in positive characteristic (§5.5).

2.3.4. *Case* (2.8b) *from Thm. 2.6.* The classification of doubly transitive groups containing an n-cycle is essential to (2.8b). There are more groups in this classification than appear in Thm. 2.7. Example: The alternating (when n is odd) and symmetric groups appear here (with S_5 producing the exceptional case of Thm. 2.6). Then, one considers which of these groups also has a degree $2n$ permutation representation T_2 with these properties.

- (2.12a) There exists $g_\infty \in G$ with $T_1(g_\infty)$ an n-cycle and $T_2(g_\infty)$ has disjoint cycle structure $(n)(n)$.
- (2.12b) $G(T_2, 1)$, the stabilizer of 1 under T_2, is intransitive under T_1.

The next lemma shows why $G(T_2, 1)$ is automatically intransitive in T_1 in case (2.9).

Lemma 2.8. *Suppose $H \leq S_n$ is a subgroup each of whose elements fixes some integer. In particular, this holds for the subgroup stabilizing an integer in T_2 under the representation T_1. Then, H is intransitive.*

Proof. If H is transitive, the conjugates of the subgroup of H fixing an integer cover H. This is a well-known impossibility. That the hypotheses hold is because each element of $G(T_2,1)=\{g\in G \mid T_2(g)(1)=1\}$ fixes an integer. That means, the trace of each element of $G(T_2,1)$ in the representation T_2 is at least 1. Since T_1 is an equivalent representation, the traces of $T_1(g)$ and $T_2(g)$ are equal for each $g\in G$. So, $T_1(g)$ fixes an integer for each $g\in G(T_2,1)$. □

Yet, establishing (2.12) is harder than showing (2.9). It forces considering primitive, not doubly transitive representations of degree $2n$. For this, and because the representations that appear relate to incomplete aspects of §2.4, we postpone this result from [Fri86, §6] to [Fri].

2.4. **Frey type Hilbert's irreducibility problem.** After a definition, we specialize for a problem generalizing the focus of Thm. 2.6. To simplify notation, we don't replace $\mathbb{Q}$ by an arbitrary field.

2.4.1. *Decomposition group properties.* Fix two integers d,d'. Let M_d be those elements of $\bar{\mathbb{Q}}$ of degree at most d over $\mathbb{Q}$. Consider any $\mathbb{Q}$ cover $\varphi: X\to\mathbb{P}^1_z$, with its arithmetic monodromy group $\hat{G}=G(\hat{X}/\mathbb{P}^1)$. Suppose $z_0\in\mathbb{P}^1_z(\bar{\mathbb{Q}})$ and K is any extension of $\mathbb{Q}(z_0)$. There is a conjugacy class of decomposition groups for the place $z\mapsto z_0$ over K; denote a representative by $G_{z_0,K}$ (G_{z_0} when $K=\mathbb{Q}(z_0)$). As usual $\hat{G}(1)$ is the stabilizer of the integer 1 in the standard representation of $\hat{G}$ having degree $\deg(\varphi)$. Suppose groups H_1,H_2 are in $\hat{G}$. If H_1 is conjugate to a subgroup of H_2 write $H_1\le^\star H_2$. This data gives a diophantine set $\mathcal{R}_\varphi(d,d',H)$:

$$\{z_0\in M_d \mid G_{z_0,K}\le^\star H \text{ for some field } K \text{ with } [K:\mathbb{Q}(z_0)]\le d'\}. \tag{2.13}$$

We list special cases before concentrating on a particular problem.

(2.14a) $\mathcal{V}_\varphi(d,d')=\mathcal{R}_\varphi(d,d',\hat{G}(1))$: those z_0 where $\varphi^{-1}(z_0)$ contains a degree 1 point over $K\supset\mathbb{Q}(z_0)$, $[\mathbb{Q}(z_0):\mathbb{Q}]\le d$ and $[K:\mathbb{Q}(z_0)]\le d'$.

(2.14b) $\mathcal{R}_\varphi(d,1,H)=\mathcal{R}_\varphi(d,H)$: $G_{z_0}\le^\star H$.

(2.14c) $\mathcal{R}_\varphi(1,d',H)$: $G_{z_0,K}\le^\star H$ with $z_0\in\mathbb{Q}$ for some K with $[K:\mathbb{Q}]\le d'$.

(2.14d) $\mathcal{V}_\varphi(d)$ and $\mathcal{V}_\varphi(1,d')$ where $H=\hat{G}(1)$ in the previous cases.

Suppose $\mathbb{H}=\{H_1,\dots,H_t\}$ is a collection of subgroups of $\hat{G}(1)$. Then, definitions (2.14) support replacing H by $\mathbb{H}$: $G_{z_0,K}\le^\star H_i$ for some integer I, $i=1,\dots,t$.

2.4.2. *Reducibility questions.* Specific sets $\mathbb{H}$ of subgroups of $\hat{G}$ support reducibility questions. Let k be an integer, $2\le k\le n-2$. For each collection $I=\{i_1,\dots,i_k\}$ of distinct integers from $\{1,\dots,n\}$, let $\hat{G}(I)$ be the maximal subgroup of $\hat{G}$ mapping I into I. Given $\varphi: X\to\mathbb{P}^1_z$, let $X^{(k)}_{\mathbb{P}^1_z}$ be the (normalized) k-fold fiber product of φ with the (fat) diagonal removed. The group S_k acts as permutations of the coordinates, and the natural quotient action produces a curve $X^{(k)}_{\mathbb{P}^1_z}/S_k$. The next fiber product result slightly generalizes the introduction of [Fri74]. As usual, while we assume $\mathbb{Q}$ is the field of definition of φ, the result applies to any field of definition, assuming the cover is separable.

Lemma 2.9. *As I runs over k subsets of $\{1,\dots,n\}$, select one representative from each $\hat{G}$ conjugacy class of the groups $G(I)$. Denote the collection of representatives by $\mathbb{H}_k$. Elements of $\mathbb{H}_k$ correspond one-one with $\mathbb{Q}$ irreducible components of*

$X^{(k)}_{\mathbb{P}^1_z}/S_k$. *In particular,* $G_{z_0,K} \leq^\star H' \in \mathbb{H}_k$ *if and only if the component corresponding to* H' *has a* K *point.*

Proof. §6.4 notes how to interpret the Galois closure as a fiber product. Let $z \in \mathbb{P}^1_z$ be a generic point. List the points of $\varphi^{-1}(z)$ as $x_1, \dots, x_n = \boldsymbol{x}$. Generic points (lying over z) of the irreducible components of $X^{(k)}_{\mathbb{P}^1_z}/S_k$ are of the form $\{x_{i_1}, \dots, x_{i_k}\}$ as $\{i_1, \dots, i_k\}$ runs over k subsets of I. Two such generic points belong to the same component if and only if $\hat{G}$ maps one to the other. In this case the groups stabilizing these generic points are conjugate to each other by $\hat{G}$. □

Let $d \geq 2$ be a fixed positive integer and $f \in \mathbb{Q}[y]$. Note: $\mathbb{H}_k$ and $\mathbb{H}_{n-k}$ consist of the same groups. Let $\mathbb{H}_{\rm red}$ be the union of the elements of $\mathbb{H}_k$, $k = 1, \dots, \left[\frac{n}{2}\right]$. Write $R_\varphi(d)$ for $R_\varphi(d, \mathbb{H}_{\rm red})$. Consider the case φ is $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$, a polynomial of degree n. To measure specializations z_0 for which $f^{-1}(z_0)$ is reducible, consider these two similar sets:

$$\begin{aligned} \mathcal{R}_f(d) = &\quad \{z_0 \in \bar{\mathbb{Q}} \mid [\mathbb{Q}(z_0) : \mathbb{Q}] \leq d, f(y) - z_0 \text{ factors over } \mathbb{Q}(z_0)\}; \\ \mathcal{R}_f(1, d') = &\quad \{z_0 \in \mathbb{Q} \mid f(y) - z_0 \text{ factors over } K \text{ with } [K : \mathbb{Q}] \leq d'\}. \end{aligned} \tag{2.15}$$

Similarly, let $\mathcal{V}_f(d)$ and $\mathcal{V}_f(1, d')$ be the corresponding value sets of f.

Problem 2.10. Given d (resp. d'), find polynomials f for which $\mathcal{R}_f(d) \setminus \mathcal{V}_f(d)$ (resp. $\mathcal{R}_f(1, d') \setminus \mathcal{V}_f(1, d')$) is finite.

We concentrate on $\mathcal{R}_f(d)$. Prob. 2.10 comes down to this after applying Faltings' proof of Lang's conjecture and a method of Frey (§10). Find f so *no component of* $(\mathbb{P}^1_x)^{(k)}_f/S_k$, $2 \leq k \leq n-2$ has any map to $\mathbb{P}^1$ of degree at most $2d$. Even with f of arbitrary large degree n, how can one prevent the appearance of *some* such a low degree map? The method here uses finite fields, and it leaves many questions.

2.5. [Fri73b] **and Rational Points on Variables Separated Polynomials.** [Fri73b] gives a short proof of Ritt's famous theorem describing all compositionally commuting polynomial pairs. It is equivalent to describing all polynomial pairs (f, h) with $(\deg(f), \deg(h)) = 1$ and $f(x) - h(y)$ has a genus 0 factor. The analysis allowed much more.

Theorem 2.11. *There is an explicit description of all polynomial pairs* (f, h) *with* $(\deg(f), \deg(h)) = 2$ *and* $f(x) - h(y)$ *has a genus 0 factor. In particular, this explicitly gives all polynomial pairs* (f, h) *where the curve defined by* $f(x) - h(y) = 0$ *has infinitely many (quasi-)integral points over a number field.*

This result uses Siegel's Theorem [Sie29] in its strongest form. Still, the conclusion of [Fri73b, Cor. on p. 7] is that all possibilities are from a small list.

(2.16a) One of f or h is of degree ≤ 6, f and g appearing in [Fri73b, Thm. 3 and Remark 1] (including the case of $\deg(f) = 2$ and $h(z) = (z-a)(z-b)(r(z)^2)$, but having several others as well); or

(2.16b) f and h are one of Ritt's commuting pairs of polynomials [Fri73b, Thm. 2], and in particular compositions of cyclic and Chebyshev polynomials.

The argument uses two general techniques:

(2.17a) Galois reduction from [Fri73b, Lemma 7] (below Lemma 4.3); and

(2.17b) combinatorial computation with branch cycles.

It use no representation theory points from §5.5 (certainly no use of the classification of finite simple groups). Still, recent literature (including [BP], [BST99], [Haj98], [CaCo99]) motivates §11 to inspect from whose viewpoint Thm. 2.11 is explicit.

3. Basic Galois Theory Tools for Analyzing Covers

While this section reviews topics that appear elsewhere, it has some new comments on phenomena in positive characteristic. To increase its potential use for polynomial problems, we stick close to the problems guiding this paper. For example, Lemma 4.3 produces polynomials f and h with attached splitting fields Ω_{f-z} and Ω_{h-z} (of $f(x)-z$ and $h(y)-z$ over $K(z)$). The key conclusion of the lemma is $\Omega_{f-z}=\Omega_{h-z}$ and it has several strong deductions. If $(\deg(f),p)=1$, equality of the inertia group orders over ∞ gives $\deg(f)=\deg(h)$. I explain precisely the meaning of this and other tactics for using this data.

3.1. **Inertia groups.** To each place P (specialization into $\bar{K}\cup\infty$) of $\Omega_{f-z}/K(z)$ there is an *inertia group* I_P. It arises from an action of any $g\in G(\Omega_{f-z}/K(z))$ on these places: $P\circ g:\Omega_{f-z}\to\bar{K}\cup\infty$ is another place. Then, I_P is the subgroup of elements g producing the same specialization of Ω_{f-z}. See [FJ86, §5.1] for this and other statements on places, decomposition and inertia groups. We say P lies over z' if P extends the place $z\mapsto z'$. The Galois group is transitive on the places over z'. So, the set of subgroups of $\hat{G}=G(\Omega_{f-z}/K(z))$ conjugate to I_P depends only on z'. Call this the *inertia* conjugacy class $I_{z'}$ of $\hat{G}$. Values $z'\in\bar{K}\cup\infty$ with $I_{z'}$ nontrivial are the *branch points* of the extension (or cover).

3.2. **Tame covers and cyclic inertia groups.** Continue the notation above, replacing $K(x)$ by L and Ω_{f-z} by $\hat{L}$. So we consider an extension $L/\bar{K}(z)$ with Galois closure $\hat{L}$. There is a standard correspondence between function fields and (irreducible nonsingular projective) curves. If X is a curve, denote its field of functions (over K) by $K(X)$.

When $\mathrm{char}(K)=0$ inertia groups have cyclic generators. We now explain their appearance. This applies to any cover $\varphi:X\to Z$ (or corresponding field extension $K(X)/K(Z)$) and point $z_0\in Z$ under this *tame ramification* hypothesis.

(3.1) Each point $x'\in X$ above z_0 has ramification index prime to p.

First we concentrate on characteristic 0 where all ramification is tame. Then, we comment how this applies for tame covers in positive characteristic.

3.2.1. *Canonical inertia group generators.* Fix any embedding of the algebraic closure $\bar{K}$ of K in $\mathbb{C}$. This produces a *canonical* conjugacy class of elements $\mathrm{C}_{z'}$ in $G(\hat{L}/K(z))$. This conjugacy class contains at least one generator of any place P above z'. An explicit construction of $\mathrm{C}_{z'}$ starts by embedding $\bar{K}(z)$ in the Laurent series field $\bar{K}((z-z'))$. It then recognizes $M=\cup_{u=1}^{\infty}\bar{K}(((z-z')^{\frac{1}{u}}))$ as the algebraic closure of $\bar{K}((z-z'))$. There are $|G(\bar{K}\hat{L}/\bar{K}(z))|$ embeddings of $\bar{K}\hat{L}$ in M. Let $\hat{e}$ be the least integer giving an embedding $\tau_{z'}:\hat{L}\to\bar{K}(((z-z')^{\frac{1}{\hat{e}}}))$ (fixed on $\bar{K}(z)$).

Denote $e^{2\pi i/\hat{e}}$ by $\zeta_{\hat{e}}$. There is a natural automorphism of $\bar{K}(((z-z')^{\frac{1}{\hat{e}}}))$ induced by $(z-z')^{\frac{1}{\hat{e}}}\mapsto\zeta_{\hat{e}}(z-z')^{\frac{1}{\hat{e}}}$. Let $g_{\tau_{z'}}$ be its pullback to $\bar{K}\hat{L}$ (by $\tau_{z'}$). A different choice of $\tau_{z'}$ changes $g_{\tau_{z'}}$ by conjugation in $G(\bar{K}\hat{L}/\bar{K}(z))$. Thus, $g_{\tau_{z'}}$ is a representative of the conjugacy class of the canonical generator of I_P.

3.2.2. *Positive characteristic.* For integers e prime to p, replace $e^{2\pi i/\hat{e}}$ in characteristic 0 by a compatible system $\{\zeta_e\}_{(e,p)=1}$ of primitive roots of 1. That is,

(3.2) $\zeta_{em}^m = \zeta_e$ for all em prime to p.

While I_P is rarely cyclic if $p|e$, it has a descending filtration by groups $I_P^{(i)}$, $i = 0, \dots,$ with the following properties.

(3.3a) $I_P^{(i+1)}$ is normal in $I_P^{(i)}$ for all i.

(3.3b) $I_P^{(0)}/I_P^{(1)}$ is cyclic of order e_0 prime to p.

(3.3c) $I_P^{(i)}/I_P^{(i+1)}$ is an elementary abelian p-group for all $i > 0$.

Further, as in the tame case we can pick a canonical generator $I_P^{(0)}/I_P^{(1)}$ (dependent on ζ_{e_0}). This is because $I_P^{(0)}/I_P^{(1)}$ is the Galois group of a tamely and totally ramified subextension L_1/L_2 of $\bar{K}\hat{L}/\bar{K}(z)$. Then use that $L_2\bar{K}((z-z'))$ is of the form $\bar{K}((t))$. Finally, a simple case of the Schur-Zassenhaus Lemma says the sequence $I_P^{(1)} \to I_P^{(0)} \to I_P^{(0)}/I_P^{(1)}$ splits. In particular, this attaches a canonical conjugacy class of $G(\bar{K}\hat{L}/\bar{K}(z))$ to the tame part of ramification over each $z' \in \mathbb{P}^1_z$.

3.3. **Counting points over branch points.** Assume K is any perfect field. If $\mathrm{char}(K) > 0$, consider only separable covers (resp. field extensions). Suppose $L/\bar{K}(z)$ has degree n (corresponding to a projective nonsingular curve cover $\varphi : X \to \mathbb{P}^1_z$). If z' is not a branch point, there are exactly n places (resp. points) of L (resp. points of X) defined over $\bar{K}$. Let $\hat{L}$ (resp. $\hat{\varphi} : \hat{X} \to \mathbb{P}^1_z$) be the Galois closure of the extension (resp. cover). Group theory interprets properties of the places $P_1, \dots, P_t$ of L over a branch point z'. For this use the natural permutation representation of $T : G = G(\hat{L}/\bar{K}(z)) \to S_n$ from G acting as (right) multipliers of $G(\hat{L}/L)$ cosets [FJ86, Lemma5.5]

Lemma 3.1. *Let P be a place of $\hat{L}$ over z'. The complete list of places $P_1, \dots, P_t$ correspond one-one with the orbits of I_P in the representation T. Orbit lengths correspond to indexes of ramification. Contribution of an orbit to the Riemann-Hurwitz formula depends only the group representation of T applied to the filtration of the higher inertia groups (applied to the orbit).*

We say more on the Riemann-Hurwitz formula. Suppose $X \to \mathbb{P}^1$ is a cover of absolutely irreducible curves—irreducible over $\bar{K}$; $L/K(z)$ is a regular extension– - of degree n with X of genus $g(X)$. Then,

$$2(n + g(X) - 1) = \sum_{\boldsymbol{x} \in X} m_{\boldsymbol{x}}. \tag{3.4}$$

The contributions of the integers $m_{\boldsymbol{x}}$ appear in several forms. Suppose $\boldsymbol{x}$ lies over z' in the notation above. Let π be an element of L generating the maximal ideal of $\boldsymbol{x}$. Assume $u(y) \in K((z-z'))[y]$ is the minimal polynomial for π over $K((z-z'))$. Then, write $\frac{du}{dy}(\pi)$ as $\pi^{m_{\boldsymbol{x}}}\alpha$ with α invertible in the local ring for $\boldsymbol{x}$.

This computation rarely gives π and $m_{\boldsymbol{x}}$ explicitly for all places $\boldsymbol{x}$ ramified over $\mathbb{P}^1$. The following deductions are therefore computationally invaluable.

(3.5a) If the orbit of $T : I_P \to S_n$ corresponding to $\boldsymbol{x}$ has order $e_{\boldsymbol{x}}$ prime to $\mathrm{char}(K)$, then $m_{\boldsymbol{x}} = e_{\boldsymbol{x}} - 1$.

(3.5b) If $p \,|\, e_{\boldsymbol{x}}$ (*wild ramification*), then $m_{\boldsymbol{x}} \geq e_{\boldsymbol{x}}$.

(3.5c) $m_{\boldsymbol{x}}$ is a simple linear combination of the orders of the subgroups $\{g \in I_P \mid (\pi)g \equiv \pi \bmod (\pi^j)\} = I_j$, $j = 0, 1, \dots$.

Suppose characteristic 0 (or a cover is tame). Given branch cycles (Thm. 3.2), data for terms of (3.4) is usually transparent. We see this in examples from §7 and §8. In positive characteristic, when ramification is wild, it is more art than science to compute $m_{\boldsymbol{x}}$. This occurs in §5.2.

3.4. **Riemann's Existence Theorem.** Using branch cycles (inertia group generators) strengthens conclusions greatly, especially when you combine it with Riemann's Existence Theorem. Here is an algebraist's version of *Riemann's Existence Theorem* [Fri95a, p. 20].

Only finitely many z' have $e = e_{x'} > 1$ (for some x' over z'). Label these *branch points* by $\boldsymbol{z} = \{z_1, \dots, z_r\}$. If ψ_i is the embedding attached to z_i, name the corresponding automorphism g_i. The r-tuple $\boldsymbol{z}$ thus gives $\mathbf{C} = (\mathrm{C}_1, \dots, \mathrm{C}_r)$, an r-tuple of conjugacy classes in G. These are the *branch cycle* conjugacy classes of $L/K(z)$. Let e_i be the e attached to z_i: the *ramification index* at z_i.

Theorem 3.2 (Riemann's Existence Theorem [Ser92], [Völ96])**.** *There is a choice of ψ_i, $i = 1, \dots, r$, where the following hold.*

(3.6a) *Product one condition:* $g_1 \cdots g_r = \Pi(\boldsymbol{g}) = 1$.
(3.6b) *Generation condition:* $\langle \boldsymbol{g} \rangle = G$.

Conversely, suppose $z_1, \dots, z_r \in \mathbb{C}$ are distinct, and $g_1, \dots, g_r \in S_n$ satisfy (3.6) *with G transitive in S_n. Then, there exists $L/\mathbb{C}(x)$ producing this data.*

An r-tuple satisfying (3.6) is a description of *branch cycles* for $L/\mathbb{C}(x)$.

3.5. **Grothendieck's Extension.** RET seems to apply only to characteristic 0. Grothendieck, however, showed the following result; [Ful69] has details when the residue class field is algebraically closed. Let R be a discrete valuation ring with residue class field k an algebraic extension of $\mathbb{F}_p$, and let K be the quotient field of R. A smooth curve $X_R \to \mathrm{Spec}(R)$ over R consists of a nonsingular projective curve X_K over K with a nonsingular projective specialization X_k over the residue class field of R. In the notation below, an R-divisor $D_R = \sum_{j=1}^{t} m_j \boldsymbol{x}_j$ consists of a set of distinct geometric points $\boldsymbol{x}_1, \dots, \boldsymbol{x}_t$ (each defined over $\bar{K}$) on X_K and integers $m_1, \dots, m_t$ with the following properties.

(3.7a) G_K (acting on points of X_K over $\bar{K}$) fixes the formal sum $\sum_{j=1}^{t} m_j \boldsymbol{x}_j$.
(3.7b) $\boldsymbol{x}_1, \dots, \boldsymbol{x}_t$ modulo the maximal ideal of R remain distinct (on X_k).

Theorem 3.3 (Grothendieck's Theorem [Gro59])**.** *Assume $Y \to X$ is a tamely ramified cover of nonsingular projective curves defined over k. Further suppose $X_R \to \mathrm{Spec}(R)$ is a smooth curve with special fiber X. Finally, let D_R be an R-divisor with special fiber the branch locus of $Y \to X$. Then, there exists a unique cover (up to equivalence as in §7.3) $Y_K \to X_K$ with these properties.*

(3.8a) *Specialization of $Y_K \to X_K$ modulo the maximal ideal of R is the cover $Y \to X$.*
(3.8b) *The branch locus of $Y_K \to X_K$ is the general fiber of D_R.*

Conversely, given an R divisor on X_R, and a curve cover $Y_K \to X_K$, suppose p does not divide the order of the geometric monodromy group of the cover. Then, there exists a tamely ramified finite extension K'/K with ring of integers R' with these properties.

(3.9a) *Extension of $Y_K \to X_K$ to K' is equivalent to a cover $Y' \to X_K$ (§7.3; defined over K') whose reduction modulo p is in the same Nielsen class.*

(3.9b) *K'/K is the Galois closure of a totally tamely ramified extension K^*/K of degree dividing $|G|$.*

3.6. **Remarks on the proof of Thm. 3.3.** We remark on the Galois closure versions of Thm. 3.3 and on how to extend Fulton's version of the proof to allow non-algebraically closed residue class field.

3.6.1. *Galois closures.* The relation between $Y \to X$ and $\hat{Y} \to X$, the Galois closure of $Y \to X$, extends to the lifting as given by Grothendieck's Theorem. That is because automorphisms of $\hat{Y} \to X$ lift canonically. This doesn't require anything new; [Ful69] was overly pedantic on the point. More efficient is to identify $\hat{Y}$ as a component of the n fold fiber product of $Y \to X$ §6.4.

3.6.2. *Arithmetic residue class fields.* The proof in [Ful69] has R with an algebraically closed residue class field. Still, the proof of the first part works without this restriction by inspection of the method. If π is the maximal ideal of R, you lift with the required properties to $R/(\pi^2)$ and then continue inductively. To make the lift to $R/(\pi^2)$, start by lifting over *explicit* affine pieces $X^{(0)}$ of $X_{R/(\pi^2)}$. It is easy to reduce to the case where X is $\mathbb{P}^1_z$. To see there is an explicit lifting, start by finding lifts in Zariski neighborhoods of any specific point of X. Here, however, choose such neighborhoods to be defined over $R/(\pi)$ and the lifts to be defined over $R/(\pi^2)$. Take open subsets for which the cover Y restricts to be isomorphic to a hypersurface $X^{(0)} = \{(x, y) \mid f(x, y) = 0\}$ in $\mathbb{P}^2$ and the covering map is projection on one of the coordinates. Since Y is nonsingular, it is always possible to cover X with such neighborhoods where a lift is possible and explicit. References might include [Mum66a, Thm. 4, p. 359] for great generality; any algebraic number theory book will show this for curves because they are Dedekind domains. [Ful69] could have done it had he considered the potential for number theory applications.

Here is why any *by-hand* affine lift over $X^{(0)}$ as above is unique (up to §7.3 equivalence). Keep the notation Y for the restriction of the original Y over $X^{(0)}$. Suppose Y_1 and Y_2 are two lifts over $X^{(0)} \otimes R/(\pi^2)$ with $D_R \otimes R/(\pi^2) = D_{R/(\pi^2)}$ as branch locus. They are given by equations (resp.) of form $f_1(x, y_1)$ and $f_2(x, y_2) = f_1(x, y_2) + \pi h(x, y_2)$ with the covering maps given by projection on the x-axis. Further, modulo π, y_1 and y_2 are both y. Now, consider why there is an expression for $y_2 = y_1 + \pi m(x, y_1)$ that satisfies this identically. Expansion gives

$$f_1(x, y_1) + \pi m(x, y_1)\frac{\partial f_1}{\partial y_1} + \pi h(x, y_2).$$

So, you can solve for $m(x, y_1)$ to make the difference between the two sides zero. The condition that both f_2 and f_1 have $D_{R/(\pi^2)}$ as branch locus guarantees the ratio $\frac{\partial f_1}{\partial y_1}/h(x, y_1)$ is invertible on $X^{(0)}$. We have by-hand lifting (unique up to a unique isomorphism) over nice affine sets. Now we need that a lifting exists (and is unique) over *any* affine $X^{(0)}$.

Grothendieck's approach saw a lifting over a covering by good open sets as a 1-cocycle with values in the sheaf of tangent vectors (actually, relative tangent vectors, for he kept a fixed lifting of X and its functions). From nonsingularity of the curves, we have uniqueness of the lifting over special open sets. So, we can

patch these together using the usual cocycle argument. Still, we comment further on the Grothendieck approach, which generalizes immensely.

An algebraic tangent vector $\boldsymbol{v}$ in a (Zariski or étale) neighborhood U gives a linear map $L_{\boldsymbol{v}}$ from the ring of functions to themselves over U. Call the set of these $\mathbb{T}(U)$. Further, to be a tangent vector, this map should satisfy Leibniz's rule:

$$L_{\boldsymbol{v}}(m_1(x,y)m_2(x,y)) = m_1(x,y)L_{\boldsymbol{v}}(m_2(x,y)) + m_2(x,y)L_{\boldsymbol{v}}(m_1(x,y).$$

Suppose U and V are two affine Zariski open sets on the affine space $X^{(0)}$ where we have respective lifts of the equation $f(x,y) = 0$ to $f_U(x,y_U)$ and $f_V(x,y_U)$. On the overlap $U \cap V$, from above, you have a lift of any function $h(x,y)$ to $h_U(x,y_U)$ and $h_V(x,y_V)$. On the overlap, their difference $h_U(x,y_U) - h_V(x,y_V)$ has the form $\pi m_{h,U,V}(x,y)$. Let $L_{U,V}(h) = m_{U,V}(x,y)$. Check easily: $L_{U,V}$ is a tangent vector over $U \cap V$ (satisfies Leibniz's rule). It defines a Čech 1-cocycle [Har77, p. 218] with values in $\mathbb{T}(X^{(0)})$: for a triple (U,V,W) of open sets,

$$m_{V,W}(x,y) - m_{U,W}(x,y) + m_{U,V}(x,y) = 0.$$

Also (above), over nice affine pieces U we could adjust any given lift by an element of $\mathbb{T}(U)$ to get any other lift. An assignment of elements in $\mathbb{T}(U)$, for a cover by special open sets U gives a Čech 0-cocycle. Here is the conclusion for showing existence of a lifting. Create lifts over each U_i in a collection $\{U_i\}_{i\in I}$ of special neighborhoods covering $X^{(0)}$. This gives a 1-cocycle α. Let γ be any 0-cycle, by which we adjust the lifts. The new 1-cycle from the adjusted lifts has value $\beta(U,V) = \alpha(U,V) + \gamma(V) - \gamma(U)$. A global lift exists when we can choose γ so $\beta(U,V) = 0$. That is, the cocycle is trivial. Such a γ exists because the cohomology space $H^1(X^{(0)}, \mathbb{T}(X^{(0)}))$ (of an affine curve) with coefficients in the sheaf of relative tangent vectors is trivial. Chevalley observed this statement on cohomology doesn't depend on k being algebraically closed and from here [Ful69] continues with no dependency on this either.

4. Basics on Variables Separated Polynomials

The appearance of doubly transitive representations needs explanation. It is an essential ingredient from the proof of the *Schur Conjecture* [Fri70]. We review material leading to [Fri73a, Thm 1], to prepare for what happens in positive characteristic. Denote the splitting field of the polynomial $f(x) - z$ (in x; over the field $K(z)$) by Ω_{f-z}. Throughout this paper, assume all geometric covers are *separable*; they correspond to separable field extensions. In particular, when a rational function $f \in K(x)$, produces a cover, the derivative of f is not identically zero.

4.1. **Notations.** Suppose $f \in K(y)$ and $\deg(f) = n$. Denote the set of permutations of $\{1,\dots,n\}$ by S_n. Act on zeros (in $\overline{K(z)}$) of $f(x) - z$ for a natural (faithful) permutation representation $T_f : G(\Omega_{f-z}/K(z)) \to S_n$. Denote this *arithmetic* Galois (monodromy) group image by $\hat{G}$. Let $\hat{K}$ be the constants of Ω_{f-z}. While $\hat{K}$ is usually K, in crucial arithmetic situations—as in the Schur conjecture and its variants—it is not. (Detecting when $\hat{K} \neq K$ may be the heart of the problem.) Replacing K by $\hat{K}$ gives the *geometric monodromy* group $G = G(\Omega_{f-z}/\hat{K}(z))$. Any correspondence between the elements of $\{1,\dots,n\}$ and the zeros of $f(y) - z$ gives a permutation representation T_f. So, this defines T_f only up to conjugation by an element of S_n. Note: Elements of S_n act on the *right* of $\{1,\dots,n\}$ in this

paper. In particular, if $g_1 = (1\,2), g_2 = (1\,3)$ the product would be $(1\,2\,3)$ and not $(1\,3\,2)$ (the result of acting on the left). A permutation representation of a group G defines a stabilizer $G(1) = \{g \in \hat{G} \mid (1)g = 1\}$. For subsets $T_1, \ldots, T_t$ of G, $\langle T_1, \ldots, T_t \rangle$ denotes the subgroup they generate.

4.2. **Basic permutation representation definitions.** The following properties for a subgroup G of S_n appear below.

(4.1a) G is *transitive* if for each $i \in \{1, \ldots, n\}$ there exists $g \in G$ with $(1)g = i$.
(4.1b) G is *primitive* if it is transitive and for any $g \in G \setminus G(1)$, $\langle g, G(1) \rangle = G$.
(4.1c) G is *doubly transitive* if G is transitive and for each $i \in \{2, \ldots, n\}$ there exists $g \in G(1)$ with $(2)g = i$. Doubly transitive implies primitive.

4.3. **Translating curve properties to group theory.** Using T_f provides a uniform group theory language to reexpress disparate properties of covers.

Lemma 4.1 ([Fri70])**.** *Suppose $f \in K(y)$. Then, $T_f : \hat{G} \to S_n$ is primitive if and only if f is indecomposable (over K). Stronger conclusions come for polynomials.*

Assume $f \in K[y]$ has degree n with $(n, \mathrm{char}(K)) = 1$. Then, f is indecomposable over K if and only if it is indecomposable over $\bar{K}$. If f is indecomposable, then:

(4.2a) *either $T_f : G(\Omega_{f-z}/\hat{K}(z)) = G \to S_n$ is doubly transitive; or*
(4.2b) *n is a prime and f is linearly related over $\bar{K}$ to x^n or the nth Chebyshev polynomial T_n.*

Proof. To illustrate this group theory umbrella, consider how it produces a common playing field for these three properties: f is a polynomial, $(\deg(f), \mathrm{char}(K)) = 1$ and f is indecomposable. The first gives total ramification over ∞: Given $f(y) = z$, there is exactly one place of the function field lying over the place $z \mapsto \infty$. From $(\deg(f), \mathrm{char}(K)) = 1$ the ramification is tame. Thus, the inertia group for a place of Ω_{f-z} over ∞ has a cyclic transitive generator g_∞. From (3.5), g_∞ must be an n-cycle. Finally, indecomposability of f says T_f is a primitive representation acting on the geometric monodromy group.

As in [Fri70], use Schur's Theorem [Sch33]: A primitive permutation group of non-prime degree n, containing an n-cycle is doubly transitive. If n is a prime and G is not doubly transitive, Burnside's Theorem tells us G is a subgroup of $\mathbb{Z}/n \times^s (\mathbb{Z}/n)^*$. Using this [Fri70] easily identifies the prime degree polynomials with G not doubly transitive, up to change of variables over $\bar{K}$. □

Remark 4.2 (Composition factors of f when $\mathrm{char}(K) | \deg(f)$). [FGS93, Cor. 11.2] generalizes the characteristic zero result to describe all polynomials with geometric monodromy group G of this form: $V \times^s C$ with C cyclic acting on a vector space V over $\mathbb{F}_p$. This produces examples of $f \in K[x]$ indecomposable over K, and decomposable over the algebraic closure.

[Fri70] shows equivalence of indecomposability over K and $\bar{K}$ (if $(n, \mathrm{char}(K)) = 1$). Still, [FGS93, §4.b, Cocycle Lemma], valuable when $\mathrm{char}(K) | \deg(f)$, characterizes this situation better, especially for fields like $\mathbb{F}_q$ with trivial Brauer group.

4.4. **Reduction to equal splitting fields.** The following result is in [Fri73a, Prop. 2] and [Fri73b, Lemma 7].

Lemma 4.3. *Suppose $f, h \in K(x)$ and $f(x) - h(y)$ is reducible. Then, there exist $f_1, f_2, h_1, h_2 \in K(x)$ with $f(x) = f_1(f_2(x))$ and $h(y) = h_1(h_2(y))$ with $\Omega_{f_1 - z} = \Omega_{h_1 - z}$. In particular, branch points for $f_1 : \mathbb{P}^1_x \to \mathbb{P}^1_z$ are identical to those for h_1. Since inertia groups are invariants of the Galois closure of a cover, a branch point of f_1 is tamely ramified if and only if it is tamely ramified for the h_1 cover.*

Further, there is a one-one association between factors φ of $f_1(x) - g_1(y)$ and those of $f(x) - g(y)$: $\varphi(x, y) \mapsto \varphi(f_2(x), g_2(y))$.

Lemma 4.3 works in great generality; you can replace rational functions f and g by maps from curves X and Y to $\mathbb{P}^1_z$. For this, replace $f(x) - h(y)$ by the fiber product of X and Y of over $\mathbb{P}^1_z$ and its components. This is [Fri73a, Cor. 1.2] and a good idea even for rational functions. The alternative is a convoluted definition for factors of $f(x) - h(y)$ (as in [Fri73b]).

We continue, however, on the case of rational functions and especially polynomials. Lemma 4.3 allows replacing (f, h) by respective composition factors (f_1, h_1) where the covers for f_1 and for h_1 have the same Galois closure. Further, this replacement loses none of the essential data on the reducibility of $f(x) - g(y)$. The next subsection adds an organizing definition (from [Fri87]) to this reduction.

4.5. **Newly reducible pairs.** Suppose for $f(x), h(x) \in K(x)$, $f(y) - h(z)$ is reducible: by abuse (f, h) is reducible. Further, assume one of $f_1, h_1, \in K(x)$ has degree exceeding 1. We say $(f(f_1), h(h_1))$ has *inherited reducibility* (over K).

Definition 4.4. Call (f, h) *newly reducible* (over K) if the following hold.

(4.3a) (f, h) is reducible but hasn't inherited reducibility.
(4.3b) f and h are not linearly related.

Of course, if f and h are indecomposable, then (f, h) is newly reducible. For $T : G \to S_n$ a permutation representation, denote the stabilizer of 1 by $G(T, 1)$.

Lemma 4.5. *Assume (f, h) is a newly reducible rational function pair over K. This is equivalent to the following.*

(4.4a) *$\Omega_{f-z} = \Omega_{h-z} = \Omega'$, so $G = G(\Omega_{f-z}/K(z)) = G(\Omega_{h-z}/K(z))$.*
(4.4b) *T_f and T_h (on G) are inequivalent permutation representations.*
(4.4c) *$G(T_h, 1)$ is intransitive in the representation T_f.*
(4.4d) *If $f = f_1(f_2(x))$, $h = h_1(h_2(x))$, with $f_1, f_2, h_1, h_2 \in K(x)$ and $\deg(f_2) + \deg(h_2) > 2$, then $T_{f_1} : G(T_{h_1}, 1) \to S_{\deg(f_1)}$ is transitive.*

4.6. **Applying RET.** Riemann's Existence Theorem reduces describing newly reducible polynomial pairs to pure group theory in these situations:

(4.5a) K has characteristic 0; or
(4.5b) one of f or h gives a tamely ramified cover of the z-line.

Lemma 4.3 replaces f and h with composition factors, so with no loss the splitting fields of $f(x) - z$ and $h(y) - z$ are the same. In particular, if f is a tamely ramified cover, then we may assume h is also. Here is a group theory rephrasing of Lemma 4.5 using a branch cycle description $\boldsymbol{g}$ of $G(\Omega'/K(z))$ (from Thm. 3.2).

Lemma 4.6. *Suppose (f, h) is a newly reducible rational function pair with $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ tamely ramified and unramified over $\mathbb{P}^1 \setminus \{z_1, \dots, z_r\}$. This is equivalent to the following. There is a group $G = G(\boldsymbol{g})$ with $\langle \boldsymbol{g} \rangle = G$ and $g_1 \cdots g_r = 1$ (as in Thm. 3.2). Also, G has inequivalent faithful permutation representations T_i, $i = 1, 2$, with $\deg(T_1) = n$ and $\deg(T_2) = m$. Further, the following hold.*

(4.6a) *The order of g_j is prime to p, $j = 1, \dots, r$ (tame ramification).*
(4.6b) $\sum_{j=1}^{r} \mathrm{ind}(T_1(g_j)) = 2(n-1)$ *(f has genus 0).*
(4.6c) $\sum_{j=1}^{r} \mathrm{ind}(T_2(g_j)) = 2(m-1)$ *(h has genus 0).*
(4.6d) *Restriction of T_1 to $G(T_2, 1)$ is intransitive (reducibility condition).*
(4.6e) *Suppose a set of imprimitivity for T_i produces a representation T_i^* of G, $i = 1, 2$. Then, restriction of T_1^* to $G(T_2^*, 1)$ is transitive if $n - \deg(T_1^*) + m - \deg(T_2^*) > 0$.*

Suppose $z_r = \infty$. Then, some linear fractional change of variables changes f and h into polynomials if and only if the following holds.

(4.7) *$n = m$, and $T_1(g_r)$ and $T_2(g_r)$ are both n-cycles.*

Remark 4.7. The rational function f is indecomposable if and only if T_1 is primitive. If we seek only newly reducible *polynomial* pairs, then (4.7) restricts us to the case $n = m$. Also, there is no reason to consider only rational functions (or genus 0 curve coverings). For example, suppose we drop condition (4.6b), and replace the polynomial condition with having $T_1(g_r)$ an n-cycle and $T_2(g_r)$ an m-cycle (total ramification). Then, the group theoretic translation works the same including that conclusion (4.7) holds if the fiber product $X \times_{\mathbb{P}^1_z} Y$ is newly reducible.

4.7. **Drawing conclusions from Lemma 4.3.** We summarize precise results about reducibility of $f(x) - h(y)$ in characteristic 0 when f is indecomposable. §5 tightens the proof of [Fri73a] to reveal new elements when $\mathrm{char}(K) > 0$. By contrast, when f is decomposable, consider the open (n, m) *problem* §11.4.

Theorem 4.8. *Assume* $\mathrm{char}(K) = 0$, (4.6) *and* (4.7) *hold for polynomials (f, h). Suppose further, f is indecomposable, and $\boldsymbol{g}$ is a description of the branch cycles of $\Omega'/K(z)$. Then, for each $g \in G(\Omega'/K(z))$, $T_f(g)$ is conjugate to $T_h(g)$ in S_n. That is, $T_f(g)$ and $T_h(g)$ have the same disjoint cycle pattern. Further, there are only finitely many degrees (7, 11, 13, 15, 21, 31) possible for f (see the proof of Thm. 5.2 and §8).*

§5 shows the conclusions of Thm. 4.8 require $\mathrm{char}(K) = 0$. In particular, over every finite field $\mathbb{F}_q$, there are infinitely many degrees for inequivalent newly reducible polynomial pairs (f, h) with $(\deg(f), \mathrm{char}(\mathbb{F}_q)) = 1$ and f indecomposable.

5. Positive Characteristic—Loss of Riemann's Existence Theorem

We consider how double transitivity enters Thm. 4.8. This shows the difference for the genus 0 problem in characteristic p from characteristic 0 phenomena. Davenport's problem in characteristic p exemplifies this difference.

5.1. **Simple groups as a resource for investigations into affine groups.** Specifically, we hope this progress on Davenport's problem inspires completing the description of exceptional polynomial (and rational function) covers. [FGS93] reduced this latter problem (using the classification) to investigating arithmetic–geometric monodromy group pairs $(\hat{G}, G)$ with $G = V \times^s H$ (affine group), and H acting irreducibly on a vector space V, of order p^r. Recall: A polynomial f (or rational function) is exceptional if and only if $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is one-one on the $\mathbb{F}_{q^t}$ points of $\mathbb{P}^1_x$ for infinitely many values of t.

[Fri94a] used an Inverse Galois problem approach over the field $\mathbb{F}_q(z)$. In particular, suppose a pair $(\hat{G}, G)$ could feasibly arise as the groups attached to an

exceptional *cover* $\varphi : X \to \mathbb{P}^1_z$ over a finite field $\mathbb{F}_q$. Then, it does appear as an actual cover under the following conditions [Fri94a, §2, Main Theorem].

(5.1a) With $q = p^r$, $p \not| |G|$.
(5.1b) q is suitably large ([Fri95c, App. E] makes this explicit).

Further, such covers had the limitation that X may have large (though computable) genus. The method for this result extends that producing the alternating group covers of §7.9 and Davenport polynomials of §8.

Yet, it doesn't include wild ramification. Extending it to consider classifying Davenport polynomials in positive characteristic is a suitable challenge, for we can still take advantage of corollaries of the classification of finite simple groups. (Lack of a practical listing of primitive affine groups complicates a classification of exceptional polynomials.) Divining explicit production of the groups that appear below as Galois groups is the work of Ram Abhyankar. He has committed himself to finding such group realizations over finite fields; in particular producing polynomial covers with projective linear groups.

5.2. **Producing monodromy groups in** $\mathrm{PGL}_{m+1}(\mathbb{F}_q)$**.** A separable projective q-polynomial of q-prodegree m over a field $\mathbb{F}_q(z)$ has the form

$$M(x) = M(x,z) = \textstyle\sum_{i=0}^m a_i x^{\langle m-i\rangle}, \quad a_i \in \mathbb{F}_q(z),\ a_0 \neq 0, \\ a_m \neq 0 \text{ and } \quad \langle j\rangle = \langle j\rangle_q = 1 + q + q^2 + ... + q^j. \tag{5.2}$$

There is a related polynomial $F(x)$ given by the formula

$$M(x^{q-1})x = F(x) = \sum_{i=0}^{m+1} a_i x^{q^i}. \tag{5.3}$$

Equations like (5.2) have appeared elsewhere. Cohen used a variant to produce exceptional p-power degree polynomials [Coh90]: replace x^{q-1} by x^k with k a divisor of $q-1$. [FGS93, Cor. 11.2] used this to generalize the proofs of both the Schur and Dickson conjectures to characterize exceptional polynomials f with $G(T_f, 1)$ cyclic. Further, the group theory behind this produced polynomials (of degree divisible by p) indecomposable over $\mathbb{F}_q$, yet decomposable over $\bar{\mathbb{F}}_q$.

Lemma 5.1. *The splitting field over $\bar{\mathbb{F}}_q(z)$ of the polynomial $M(x)$ in* (5.2) *has Galois group a subgroup of* $\mathrm{PGL}_m(\mathbb{F}_q)$*. Further, the natural permutation representation on zeros of $M(x)$ is (permutation) equivalent to* $\mathrm{PGL}_m(\mathbb{F}_q)$ *acting on points of m-dimensional projective space over $\mathbb{F}_q$.*

Proof. Let Ω_M (resp. Ω_F) be the splitting field of M (resp. F) over $\mathbb{F}_q(z)$. The zeros of F are closed under addition and scalar multiplication by $\mathbb{F}_q$. Thus, they correspond to elements of the vector space $\mathbb{F}_q^{m+1}$; a structure that $G(\Omega_F/\mathbb{F}_q(z))$ respects. Equivalence two nonzero roots of $F(x,z)$ if their $q-1$st powers are equal. This is the same as the equivalence of two points in the vector space if they lie on the same line. Formula (5.3) identifies $G(\Omega_M/\mathbb{F}_q(z))$ as the induced action of $G(\Omega_F/\mathbb{F}_q(z))$ on these equivalence classes of *nonzero* roots of $F(x,z)$. This corresponds to the natural map $\mathrm{GL}_{m+1}(\mathbb{F}_q) \to \mathrm{PGL}_{m+1}(\mathbb{F}_q)$, thus identifying $G(\Omega_M/\mathbb{F}_q(z))$ with a subgroup of $\mathrm{PGL}_{m+1}(\mathbb{F}_q)$. □

5.3. **Examples of Abhyankar.** We follow [Abh97], adding comments clarifying the arithmetic of the situation when the field of definition doesn't contain $\mathbb{F}_q$. The following result is especially interesting when $k = \mathbb{F}_p$. Denote the range of a polynomial f on a finite field k' by $V_f(k')$: the set of values of f on k'.

Theorem 5.2. [Abh97, Claim 1.2] *Let k be any finite field containing $\mathbb{F}_p$ and assume $m \geq 3$. Consider $f(x) = f_{m,q}(x) = x^{\langle m-1\rangle} + x \in k[x]$. This gives a cover of the z-line with geometric monodromy group $\mathrm{PGL}_m(\mathbb{F}_q)$. The geometric monodromy group equals the arithmetic monodromy group if $k \supset \mathbb{F}_q$. Otherwise, $\Omega_F \cap \bar{k} = \mathbb{F}_q \cdot k$ and the quotient group $G(\Omega_F/k(x))/\mathrm{PGL}_m(\mathbb{F}_q)$ is cyclic of order $[\mathbb{F}_q \cdot k : k]$. When $m \geq 3$, there exists $h(y)$ also of degree $\langle m-1\rangle_q$ with the following properties.*

(5.4a) $\Omega_{f-z} = \Omega_{h-z} = \Omega'$.
(5.4b) $V_f(k') = V_h(k')$ *for all finite extensions k' of k.*
(5.4c) $f(x) - h(y)$ *factors as $\varphi_1(x,y)\varphi_2(x,y)$ with φ_1 of degree $\langle m-2\rangle_q$ and both φ_1 and φ_2 are absolutely irreducible.*

5.4. **Part of Thm. 5.2 characterizing (5.4c).** The first five subsection steps partially classify the following with $f, h \in K[x]$.

(5.5) (f,h) is newly reducible with f indecomposable and $(\deg(f), p) = 1$.

(In characteristic 0 the classification is complete.) §5.5 shows (5.4b) follows from (5.5). A preliminary step produces h given f. Note the *modular* representation that arises in the proof, and the possibility of characteristic zero phenomena about doubly transitive representations not holding in positive characteristic. We expect polynomial monodromy groups in the Davenport and factorization problems when f is indecomposable and $(\deg(f), p) = 1$, are the same as listed in Thm. 9.1. Still, the failure of a convenient Riemann's Existence Theorem allows many possible degrees for f over each finite field. That is, in positive characteristic there are many reducible variables separated and Davenport polynomials.

5.4.1. *Results on the degrees of f and h* [FJ86, Chap. 19] *and* [Fri87]. For any polynomial f the extension $K(x)/K(z)$ totally ramifies—there is just one prime of $K(x)$—over $z = \infty$. If the degree of f is prime to p, the extension tamely ramifies over ∞. Any composition of tamely ramified extensions tamely ramifies. So the primes of the splitting field Ω' over ∞ tamely ramify. The ramification index of any such prime over ∞ is the degree of f. As (5.4a) holds, the inertia groups for $\Omega_{f(x)-z}$ and $\Omega_{h(y)-z}$ are the same. Thus, this degree is also the degree of h.

5.4.2. *Given f, in the cases of Thm. 5.2, constructing h.* By construction, T_f is a representation of the geometric monodromy group (equal to $\mathrm{PGL}_m(\mathbb{F}_q)$) acting on the points of projective space. (Note: The arithmetic monodromy group is in $\mathrm{P\Gamma L}(\mathbb{F}_q)$ and also acts on these points). The representation T_h from the polynomial h is the action on the hyperplanes of m-dimensional projective space. As usual, $G(T_h, 1)$ is the stabilizer of an integer in the representation T_h. Denote the fixed field of $G(T_h, 1)$ in Ω' by L. To produce h we have only to show $L/\mathbb{F}_q(z)$ totally ramifies over ∞ and L has genus 0.

Representations T_f and T_h are permutation inequivalent, though they are equivalent as group representations (Thm. 9.1). As in §2.3, this means $T_f(g)$ and $T_h(g)$ have the same disjoint cycle pattern for each $g \in G(\Omega'/\mathbb{F}_q(z))$. If g_r is the inertia

group generator for tame ramification over ∞, then $T_h(g_r)$ is also an n-cycle. Applying Lemma 3.1, $L/\mathbb{F}_q(z)$ totally ramifies over $z=\infty$. Now, check ramification over $z=0$, the only other branch point of $f:\mathbb{P}^1_x\to\mathbb{P}^1_z$.

Bob Guralnick supplied the next lemma. We apply it when G is the geometric monodromy group $H_1=G(T_f,1)$, $H_2=G(T_h,1)$ and $H=I_1$, the first higher ramification group. From Lemma 3.1, this immediately shows L has the same number of ramified places lying over $z=0$ as does $K(x)$.

Lemma 5.3. *Let G be a finite group, H_1 and H_2 subgroups whose permutations representations have the same group character. Let H be any subgroup of G. Then, H has the same number of orbits on the cosets of H_1 as on the cosets of H_2.*

Proof. The orbit information comes from a formula of classical representation theory. Induce the representation T_{H_i} from the identity representation $\mathbf{1}_{H_i}$ on H_i, $i=1,2$. Count orbits of H on the cosets of H_i (orbits of H under the representation T_{H_i}) as the number of appearances of $\mathbf{1}_H$ in the restriction of T_{H_i} to H. Reason: Each orbit is a transitive permutation representation and the identity appears exactly once in the character of a transitive permutation representation. Thus, applying the complex inner product of representation theory, this number is $\langle \mathbf{1}_H, \mathbf{1}^G_{H_i}\rangle_H$ (as in §5.4.5; the subscript H means take the inner product in H). From Frobenius reciprocity this equals $\langle \mathbf{1}^G_H, \mathbf{1}^G_{H_i}\rangle_G$. The lemma follows since the characters $\mathbf{1}^G_{H_i}$ are the same for $i=1$ and 2. □

From the discussion following Lemma 3.1, the contribution of a branch point z' to the Riemann-Hurwitz formula depends only on knowing the orbits ([Frö67] or [Ser67]). In this example, the ramified points of $\mathbb{P}^1_x$ over $z=0$ are exactly the zeros of $\frac{df}{dx}=x^{q\langle m-2\rangle_q}+1$. That is, one place over $z=0$ is unramified, while the other $\langle m-2\rangle_q$ points are each ramified of order q (with minimal possible contribution of q to the Riemann-Hurwitz computation).

5.4.3. *Relation between T_f and T_h when* (5.5) *holds.* Since$(\deg(f),p)=1$, an affine change in x allows assuming the penultimate coefficient of $f(x)-z$ is 0. Thus, there is one obvious linear relation among the zeros $x_1,\dots,x_n$ of $f(x)-z$; their sum is 0. If f is indecomposable, then Lemma 4.1 implies $T_f:G\to S_n$ is doubly transitive or G is the Galois group of the splitting field of a Chebyshev or cyclic polynomial. These last (geometric monodromy groups) are dihedral and cyclic. They would have no permutation inequivalent representation corresponding to T_h. Check the degree $k-1$ terms of a degree k factor $\varphi_1(x,y)$ of $f(x)-h(y)$. Conclude: Reducibility of $f(x)-h(y)$ implies there is a relation

(5.6) $ay_1+b=\sum_{i\in I}x_i$ with I a proper subset of $\{1,\dots,n\}$ and x_i (resp. y_j) running over zeros of $f(x)-z$ (resp. $h(y)-z$).

§5.4.4 explains why $a\neq 0$, even in positive characteristic. Then, it explains why the following holds if $(p,|G|)=1$ (includes characteristic 0; expected to hold even if $p\,|\,|G|$) [Fri73a, p. 131] (or [FJ86, Lemma 19.31]).

(5.7) Representations T_f and T_h are equivalent as group representations.

The argument distinguishes pure group theory conclusions of (5.6) from the consequences of $\mathrm{char}(K)$ being 0 or positive.

5.4.4. *Separating* $\mathrm{char}(K)=0$ *from* $\mathrm{char}(K)>0$. Suppose $T:G\to S_n$ is any permutation representation. Then, T defines a representation on a vector space V

over any field K: V has basis $X_1, \dots, X_n$ with the obvious action of G. Suppose $G = G(K(x_1, \dots, x_n, z)/K(z))$ with $x_1, \dots, x_n$ the zeros of a polynomial $f(x, z) = 0$, as in our usual setup. Then, invariant G submodules of V correspond to Galois group invariant linear subspaces of the K-span of $x_1, \dots, x_n$. In particular, suppose the Galois group maps $\alpha = \sum_{i=1}^n a_i x_i$ into K multiplies of α. This produces a 1-dimensional G invariant subspace of V. If the action of G on this space is trivial, denote it by $\mathbf{1}_G$; $\sum_{i=1}^n X_i$ gives a copy of $\mathbf{1} = \mathbf{1}_G$.

When $f(x, z) = f(x) - z$, denote the vector space for G action by V_f. The condition $a \neq 0$ in (5.6) gives a G map $\mu : V_h \to V_f$. Representations V_f and V_h are equivalent if this map (of n dimensional vector spaces) is onto. The next lemma shows when this happens. If $a = 0$, then V_f has a one dimensional invariant subspace, distinct from $\mathbf{1}$. The lemma also eliminates this possibility.

Lemma 5.4. *Assume $f \in K[x]$ with $(\deg(f), \mathrm{char}(K)) = 1$. Then, $V_f = \mathbf{1}_G \oplus V_1$. If, further, f is indecomposable, then $\mathbf{1}_G$ is the only G-invariant one-dimensional subspace of V_f.*

If V_1 is irreducible, then T_f and T_h are equivalent as group representations and both are doubly transitive permutation representations. If $\mathrm{char}(K)$ is 0 or does not divide $|G|$, V_1 is irreducible (has no proper invariant subspaces).

The proof of Lemma 5.4 occupies the next three subsections.

5.4.5. *Splitting off $\mathbf{1}_G$.* Classical representation theory gives an inner product on representations by the following formula:

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)}. \tag{5.8}$$

This inner product, however, is not available if $p \,|\, |G|$. Still, there are versions of it.

For example, let $X_1, \dots, X_n$ represent the cosets of H and a basis of the corresponding representation. Then, $\sum_{i=1}^n X_i$ is a basis vector for a 1-dimensional invariant subspace. Assume X_1 represents the coset of the identity. Write $V = V(X_1, \dots, X_n)$ as $\mathbf{1} \oplus V'$ with $V' = V(X_2, \dots, X_n)$. Then, V' is H-invariant, though maybe not G-invariant. Let $P_{\mathbf{1}} : V \to \mathbf{1}$ be the projection onto $\mathbf{1}$. (For this argument with an action on a vector space, act on the left of V, unlike our computations of permutation elements, which are usually on the right.)

Use $(n, p) = 1$ to average $P_{\mathbf{1}}$ over the cosets of H: $\frac{1}{n} \sum_{i=1}^n P_{\mathbf{1}}(g_i(v)) = \bar{P}(v)$ with $g_1, \dots, g_n$ a complete set of coset representatives and $v \in V$. As H preserves the splitting of V, $\bar{P}$ is independent of the choice of coset representatives. For any $g \in G$, $g_1 g, \dots, g_n g$ are new coset representatives. Check from this $\bar{P}$ is G-invariant, $\bar{P}$ acting as the identity on $\mathbf{1}$. Its kernel gives a G-invariant splitting of V.

5.4.6. *V_f contains no additional 1-dimensional subspace.* Suppose V^* is a one dimensional submodule of V_f, distinct from $\mathbf{1}_G$. Note: Any one-dimensional subspace on which a transitive subgroup H acts trivially must be the unique copy of $\mathbf{1}$ we have already identified. Let G^* be the subgroup of G acting as the identity on V^*. So G^* is not transitive. On the other hand, G^* is the kernel of a 1-dimensional character of G, so it is a normal subgroup of G. Now use that any nontrivial normal subgroup of a primitive group is transitive. This argument used only primitivity and not the full force of Lemma 4.1 (or even $(\deg(f), p) = 1$). It does use that

G/G^* is abelian, and G^* is not trivial. Only, however, in the cyclic polynomial case does this happen, and here there are other 1-dimensional subspaces of V_f.

5.4.7. *Using that T_f is doubly transitive.* If $(|G|, p) = 1$, it is well-known that T_f double transitivity implies V_1 in $V_f = \mathbf{1}_G \oplus V_1$ is an irreducible G module (of dimension $n-1$). This isn't deep; it uses only the inner product on representations of (5.8) and the following fact: A function m on conjugacy classes of G is the trace of a representation if and only if $\langle \chi, f \rangle$ is a nonnegative integer for all irreducible characters χ [Isa94, Cor. 15.6].

Conclude the proof of Lemma 5.4 by noting $\mu : T_h \to T_f$ in §5.4.4 is onto if V_1 is irreducible. The argument above shows this if the induced map $V_h/\mathbf{1}_G \to V_f/\mathbf{1}_G$ is onto. If not, then the image of $V_h/\mathbf{1}_G$ is a nontrivial proper G submodule of V_1, contrary to assumption.

Remark 5.5 (When is V_1 irreducible?). Even if $(n, p) = 1$, it may happen V_1 is reducible. Thm. 9.1 gives a classification of doubly transitive groups containing an n-cycle. Further, Abhyankar's examples guarantee all groups appearing in Thm. 9.1 are geometric monodromy groups of polynomials in some positive characteristics. So, possible reducibility of V_1 is a practical question whose answer amounts to inspecting modular representations arising from projective linear groups acting on points of projective space. [Fri] will remark on this.

Remark 5.6 (Classifying reducible variables separated polynomials). Consider f, h in $K[x]$. There may be a reasonable classification of those $f(x) - h(y)$ that are reducible with f indecomposable of degree n, even without assuming $(n, p) = 1$. Note: It is not clear h will also have degree n if $(n, p) \neq 1$. As previously, this case reduces to where the splitting fields Ω_{f-z} and Ω_{h-z} are equal. If I_∞ is the inertia group over ∞, then I_∞ is transitive in both representations T_f and T_h (§3.1). For I_∞ cyclic of order n, this implies both representations are of degree n. Other groups, however, might have several faithful transitive representations.

5.5. **Davenport's problem in positive characteristic.** [FJ86, §19.6] treats Davenport's problem over a global field. It shows the Kronecker conjugate condition on the Galois group is equivalent to polynomials having the same value sets for all finite extensions of a finite field K (especially [FJ86, Lemma 19.27]). If $f \in k[x]$, denote values of f on K by $V_f(k)$. In previous notation, the result is this.

Theorem 5.7. *Suppose $f, g \in \mathbb{F}_q[x]$. Then, the following are equivalent.*

(5.9a) *$V_f(\mathbb{F}_{q^t}) = V_h(\mathbb{F}_{q^t})$ for all positive integers t.*
(5.9b) *$\cup_{i=1}^n G(T_f, i) = \cup_{j=1}^m G(T_h, j)$.*

Suppose these conditions hold, and

(5.10) *$\deg(f) = n$ and $\deg(h) = m$ are prime to p.*

Then, $\Omega_{f-z} = \Omega_{h-z}$ (as in Lemma 4.5) and $f(x) - h(y)$ is reducible.

Conversely, suppose (5.10)*, $f(x) - h(y)$ is reducible and f is indecomposable. Then,* (5.9) *holds. In particular, the Abhyankar examples of Thm. 5.2 give infinitely many indecomposable polynomial pairs over any finite field satisfying* (5.9)*.*

Remark 5.8 (Comments on the Proof of Thm. 5.7). Condition (5.10) is from identifying the degree of f as the order of the cyclic inertia group generator (Rem. 5.6). If $p \,|\, \deg(f)$, then the inertia group I_∞ of a prime of Ω_{f-z} over ∞ is transitive in the representation T_f. For Davenport's problem, there may be ways to weaken this hypothesis for what [Fri73a, p. 137] uses of it. On the other hand, the relation

between newly reducible polynomials and the Kronecker conjugate hypothesis is more complicated. A simple piece of Galois theory in [Fri73a] shows (5.9) implies the following. Any composition factor f_1 of f ($f = f_1(f_2(x))$) has a corresponding composition factor h_1 of h with $\Omega_{f_1-z} = \Omega_{h_1-z}$ and $f_1(x) - h_1(y)$ is reducible.

Even if two polynomials f_2 and h_2 have quite unrelated values in $\mathbb{F}_q^t$ for most t, there might be $g \in \mathbb{F}_q[x]$ with

$$V_{g(f_2)}(\mathbb{F}_{q^t}) = V_{g(h_2)}(\mathbb{F}_{q^t}) \text{ for all } t. \tag{5.11}$$

[Mül98] gives examples of this (§11.5). Classifying these considers monodromy groups of decomposable polynomials, though sometimes these don't give *newly* reducible variables separated polynomials: $g(x) - g(y)$ is already reducible.

6. The genus 0 problem and its relation to this paper

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. It serves this paper to note their results generalize [Fri86] and [Fri73a] in showing there are only finitely many monodromy groups giving factorizations of $f(x)-g(y)$ with f an indecomposable polynomial. Example: Müller's explicit results list *all* monodromy groups for polynomials. This applies, however, only for polynomials over characteristic 0 fields. Compatible with the results of Thm. 5.2, [GS95] gives a potential list of geometric monodromy groups of indecomposable covers with exactly one totally ramified point in positive characteristic. Abhyankhar has shown many do occur as polynomial covers.

6.1. **Resolution of the original conjecture.** [GT90] laid out the composition factor question. They noted (as did [Fri70]) that monodromy groups of compositions of rational functions are subgroups of the wreath product of the monodromy groups of the composition factors. This reduced the problem to where the monodromy group is primitive. [GT90] then applied the classification based taxonomy of primitive groups by Aschbacher-O'Nan-Scott [AS85] (into five types; see exposition of [FGS93, §13]). Further, they did several primitive cases. One is of affine groups (§5.1) $V \times^s H$ with H acting irreducibly on the vector space V. [Neu93] improved the results of [GT90] in the affine case. [Mag93] handled the case of primitive groups arising from sporadic simple groups. A result from [LS91] on fixed point ratios joined with [GT90] 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. [FM98] and [LS98] 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. This completed the proof of the Guralnick-Thompson conjecture for composition factors of genus g cover, and the original formulation of the genus 0 problem.

6.2. **More precise expectations.** We expect among indecomposable covers of any genus g, a finite number of examples together with a small number of natural families. The alternating and symmetric groups appear in many ways for all values of g. It is still unknown in what ways these appear for the generic curve of genus g. (See §6.3 for the 3-cycle appearance of A_n in its natural degree n representation.) For $g = 0$ and 1 at least, one gets dihedral groups and groups related to $S_m \wr \mathbb{Z}/2$ (of degree m^2). For $g = 0$, there are Euclidean groups (the Galois closure is an elliptic curve). Guralnick has the most precise conjecture [Gur97].

Suppose $g = 0$ and G is alternating or symmetric and the degree of the cover is large. Then, [Gur97] suggests the only permutation representations are the natural permutation action or the action on subsets of $\{1, \dots, n\}$ of cardinality two. These both give genus zero covers and with many types of branch cycles (Nielsen classes). Examples: The representation of S_5 on subsets of cardinality two is the exceptional case in Thm. 2.6; and the many examples from [DF99, §4: Siegel and Néron Families]. [GS98] has made significant progress on excluding other representations of the symmetric and alternating groups.

Describing further hard cases requires a definition. The *Fitting subgroup* $F(G)$ is the maximal nilpotent normal subgroup. A *component* H of G has these properties:

(6.1a) H is a subnormal subgroup (from it to G there is a composition series);
(6.1b) H is perfect (equal to its commutator subgroup); and
(6.1c) modulo its center, H is simple.

The components of G generate $E(G)$. Then, $F(G)$ and $E(G)$ generate the generalized Fitting subgroup $F^*(G)$. When G has a faithful primitive permutation representation, $F^*(G)$ is the direct product of the minimal normal subgroups of G. Group theorists say G is *almost simple* when $F^*(G)$ is simple. Only one case from [AS85] has two minimal normal subgroups.

The two most difficult primitive permutation group cases occur with G almost simple and when $F^*(G) = E(G)$ is a direct product of t (> 1) copies of a nonabelian simple group L. In the latter case the intersection of $G(1)$ and $E(G)$ is the direct product of the point stabilizers of the components in $E(G)$. There exists a possibly very small genus cover $X \to \mathbb{P}^1_z$ having L appear as the generalized Fitting subgroup of the geometric monodromy group. [GN95] showed t must be relatively small ($t \le 8$, and—unpublished—$t \le 4$). The hardest cases are for groups having the form $S_m \wr H$ with H cyclic of order $t \le 3$ or S_3. For H of order 2, there are genus 0 and genus 1 examples [GN95].

6.3. **Appearance of generic curves of genus g.** There are several equivalent definitions of a *generic* curve (of genus g). The simplest is that it is a curve C_g with the following properties relative to a generic point $\boldsymbol{p}^*$ of the moduli space $\mathcal{M}_g$ of curves of genus g.

(6.2a) C_g has equations with coefficients in the coordinates of $\boldsymbol{p}^*$.
(6.2b) C_g represents the isomorphism class of curves corresponding to $\boldsymbol{p}^*$.

The following is in [GS98] (using [GN95] and [GM98]).

Theorem 6.1. *Let C_g be a generic curve as above. Suppose $g \ge 4$ and there is a cover $\varphi_{C_g} : C_g \to \mathbb{P}^1_z$. Even if φ_{C_g} decomposes, the factorization is through another genus 0 cover (see, for example,* [Fri77, p. 26]*; certainly known to Riemann). So,*

replace φ_{C_g} by its minimal factorization to $\mathbb{P}^1_z$, of degree n. Then, the monodromy group of φ_{C_g} must be A_n or S_n.

Whether the monodromy group in Theorem 6.1 can be A_n is still open. For example, consider the case when $G = A_n$, $n \geq 5$ and the branch cycle description is $\mathbf{C}$ consisting of r repetitions of the 3-cycle conjugacy class. We know precisely the number of components such families of covers have. It is two if $r \geq n$ (see §7.1). Further, there are two reduced Hurwitz space (absolutely irreducible and defined over $\mathbb{Q}$) components, $\mathcal{H}^{\rm rd}_+(n,r)$ and $\mathcal{H}^{\rm rd}_-(n,r)$. These spaces, of dimension $r-3$ ([Fri96], or [Fri95c, Ex. 3.12]), are akin to the curves appearing in the example of Thm. 7.3 below. Now suppose $r = g+n-1$ (and assume $g \geq 2$). The dimension of the moduli space of curves of genus g is then $3g-3$. There are natural maps $\Psi_{+,n,r} : \mathcal{H}^{\rm rd}_+(n,r) \to \mathcal{M}_g$ and $\Psi_{-,n,r} : \mathcal{H}^{\rm rd}_-(n,r) \to \mathcal{M}_g$.

Question 6.2. Suppose $n \geq 2g-2$. Are the maps $\Psi_{+,n,r}$ or $\Psi_{-,n,r}$ dominant?

I don't know the answer for any allowed values of (n,r). Yet, the analog for genus 1 is affirmative.

Theorem 6.3 ([FKK98])**.** *For $n \geq 5$, both maps $\Psi_{+,n,n} : \mathcal{H}^{\rm rd}_+(n,n) \to \mathcal{M}_1$ and $\Psi_{-,n,n} : \mathcal{H}^{\rm rd}_-(n,n) \to \mathcal{M}_1$ are dominant.*

Finally, Bob Guralnick poses the following conjecture.

Question 6.4. Let $\varphi : X \to \mathbb{P}^1$ be an indecomposable cover, $g(X) = g$, with φ of degree n. Let G be the monodromy group of the cover. Then there exists a function $N(g)$ for which if $n > N(g)$, one of the following occurs.

(6.3a) $F^*(G) = A_n$;
(6.3b) $F^*(G) = A_m \times A_m$ with $n = m^2$;
(6.3c) $F^*(G) = A_m$ with $n = m(m-1)/2$;
(6.3d) G is cyclic of prime order; or
(6.3e) G is metabelian and $[G,G]$ has order p^a with $1 \leq a \leq 2$ where $G/[G,G]$ cyclic of order $d = 2, 3, 4$ or 6 with d not dividing $p-1$ in case $a = 2$.

6.4. **Qualitative implications of the genus 0 problem.** Let $f \in \mathbb{C}(x)$, and consider the cover $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$. Using the construction of §2.1, define the n-fold fiber product $(\mathbb{P}^1_x)^{(n)}_{\mathbb{P}^1_z} = W^{(n)}$ of f. It is the iteration n times of the fiber product of f with itself; then, normalize the result. This has components of no interest here: the *fat diagonal*. Let Δ be the diagonal on $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_x$. Any pair of coordinates on $W^{(n)}$ gives a natural projection to $\mathbb{P}^1_x \times_{\mathbb{P}^1_z} \mathbb{P}^1_x$. Unions of pullbacks of the diagonal under these projections comprise the fat diagonal. Let $X^{(n)}_f = X_f$ be any other component of $W^{(n)}$. Note: S_n acts on $W^{(n)}$ by permutation of coordinates.

Lemma 6.5. *If the degree of f is n, then $X_f \to \mathbb{P}^1_z$ is the minimal Galois closure cover of f. This works over any field K (and with any cover of $\mathbb{P}^1_z$ replacing f) containing a field of definition of f. The minimal Galois cover of f over K is a K component of the n-fold fiber product of f. The Galois group is the largest subgroup of S_n mapping X_f into itself.*

As noted in the introduction, Galois theory and fiber products are mathematical cousins. Suppose X is *any* projective, nonsingular, curve over $\mathbb{C}$.

Definition 6.6 (Genus 0 hull)**.** Assume X has a presentation of the following kind. There exists $f \in \mathbb{C}(x)$ with a surjective map $\varphi_{f,X} : X_f \to X$. We say

X is in the genus 0 hull (of $\mathbb{P}^1_z$, by f). Let proj_z be projection of X_f onto $\mathbb{P}^1_z$. Suppose there exist nonconstant maps $\varphi_{X,w} : X \to \mathbb{P}^1_w$, $\varphi_{z,w} : \mathbb{P}^1_z \to \mathbb{P}^1_w$ with $\varphi_{z,w} \circ \text{proj}_z = \varphi_{X,w} \circ \varphi_{f,X}$. Then, we say X is in the strong genus 0 hull of $\mathbb{P}^1_z$ (by f). Assume $\varphi_{X',X} : X \to X'$ is a surjective map of curves. Then, (X, X') (or $\varphi_{X',X}$) is in the strong genus 0 hull if some f puts X in the strong genus 0 hull of $\mathbb{P}^1_z$ where $\varphi_{X,w}$ factors through $\varphi_{X',X}$.

The next lemma shows how results on the genus 0 problem preclude some maps $\varphi_{X',X}$ from being in the strong genus 0 hull.

Lemma 6.7. *Given a curve cover $\varphi_{X',X} : X \to X'$, suppose X is in the genus zero hull by $f \in \mathbb{C}(x)$. Then, $\varphi_{X',X}$ is in the strong genus 0 hull by f if and only if there exists a curve Y whose automorphism group contains two subgroups H_f and $H_{X'}$ with these properties.*

(6.4a) *There exists $\psi_{X'} : Y \to X'$ factoring through X, Galois with group $H_{X'}$, and $\psi_z : Y \to \mathbb{P}^1_z$ factoring through X_f, Galois with group H_f.*

(6.4b) *$\langle H_{X'}, H_f \rangle$ is a finite group.*

If Y has genus at least 2 (for example, if X has genus at least 2), then (6.4b) *is automatic from* (6.4a). *Further, if the monodromy group of $X \to X'$ contains a composition factor H not of genus 0, then $\varphi_{X',X}$ is not in the strong genus 0 hull.*

Proof. Properties (6.4) have a purely field theoretic rephrasing. It is that the function fields $\mathbb{C}(X')$ and $\mathbb{C}(z)$ are subfields of a common function field $\mathbb{C}(Y)$ which is simultaneously Galois over each. Assume the rest of the field construction takes place in an algebraic closure of $\mathbb{C}(X_f)$.

Further, $\mathbb{C}(Y)$ contains $\mathbb{C}(X_f)$ and $\mathbb{C}(X)$ compatible with their containing the respective fields $\mathbb{C}(z)$ and $\mathbb{C}(X')$ through the maps $X_f \to \mathbb{P}^1_z$ and $\varphi_{X',X}$. Then, the groups $H_{X'}$ and H_z are the respective Galois groups of the extension $\mathbb{C}(Y)/\mathbb{C}(X')$ and $\mathbb{C}(Y)/\mathbb{C}(z)$. Take $\mathbb{C}(w)$ to be the intersection of the fixed fields of $H_{X'}$ and H_z. From Galois theory, such a nonconstant w exists if and only if $\langle H_X, H_z \rangle$ is a finite group. The automorphism group of a curve of genus at least 2 is finite (reliably bounded), so it is a finite group if Y has genus at least 2.

Suppose $\varphi_{X',X}$ is in the strong genus 0 hull, so such a cover Y exists. This gives a cover $f^* : \mathbb{P}^1_x \to \mathbb{P}^1_w$ factoring through $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$. Let X_{f^*} be the Galois closure of this cover: a Galois cover of $\mathbb{P}^1_w$. Write f^* as $g \circ f$. Then $G(X_{f^*}/\mathbb{P}^1_w)$ is a natural subgroup of $H^{\deg(g)} \times^s G$ with $H = G(X_f/\mathbb{P}^1_z)$ and $G = G(X_g/\mathbb{P}^1_w)$ containing copies of H and having G as a quotient. That is, it is a subgroup of the *wreath product* of H and G [Fri70]. Further, X_{f^*} covers X_f because they are respective Galois closures of $\mathbb{P}^1_x \to \mathbb{P}^1_w$ and $\mathbb{P}^1_x \to \mathbb{P}^1_z$, by a map factoring through $X \to X'$. Conclude: $G(X_{f^*}/\mathbb{P}^1_w)$ has as composition factors any composition factor of the monodromy group of $X \to X'$. □

Remark 6.8. Any finite group occurs as a cover $X \to \mathbb{P}^1_z$ from Riemann's Existence Theorem. Reader, please note, refined statements about which groups are composition factors of genus g curves are part of the genus g ($g \geq 0$) problem. That is relevant to refinements of Lemma 6.7 relating the genus 0 and strong genus 0 hulls.

7. Parameter spaces for arithmetically related covers

This section shows, by example, how to compute information about spaces of covers (here rational function covers) arising as exceptional cases in the problems of this paper. The techniques have been around awhile, though we take this opportunity to show a few refinements and tricks. Still, the examples have a long history and the author talked on several of them in the early 70's, before the community had acclimated to the braid group method. First we put the problems in a background stemming from Thompson's formulation of the genus 0 problem.

Davenport polynomials of degree 7 and 13 fall in nontrivial families. These are families of polynomial pairs (f, h) with properties contributing solutions to the following problems: Thm. 2.6 serving Hilbert's irreducibility theorem; §4.5 giving newly reducible variables separated polynomials; and Thm. 5.7, polynomials having the same value sets over any finite field of reduction. We show how to answer questions for the family in the $\deg(f) = 13$ case ([Fri95b, Lemma 4.6, Part D] does the degree 7 case).

(7.1a) What is the dimension of the space of these polynomials pairs? Answer: 4, though another reasonable answer, after changes of variable has the essential dimension as 1.

(7.1b) Does the parameter space of polynomial pairs have a good moduli space structure, and how many components does it have? Answer: It has a great moduli space structure, and there are four components.

(7.1c) Is there a natural field of definition of this moduli space and what is it? Answer: It is a good moduli space, so its minimal field of definition is the field of moduli, and this is the degree four extension of $\mathbb{Q}$ in $\mathbb{Q}(e^{2\pi i/13})$.

(7.1d) Over the field of definition, are there lots of rational points? Answer: Yes, they are dense.

(7.1e) Are these calculations easy, and does it work for similar examples? First: Yes, I did these calculations in 1968 by hand in a day or so. Second: Parts work in generality, though if it were *very* easy, we would have completed the Inverse Galois Problem and Shafarevich's conjecture long ago.

7.1. **Prelude on components of families.** §8 lists properties of degree 13 Davenport polynomials using this method. We start by reviewing how the method can detect rational points on the moduli space. No Davenport polynomials are defined over $\mathbb{Q}$. The first example is a family of rational function covers where the total family and a dense set of members of it have field of definition $\mathbb{Q}$. All examples are families of covers with $r = 4$ branch points.

When $r = 4$, the parameter space for these families produces natural covers of the classical j-line. These are also quotients of the upper half plane by finite index subgroups of $\mathrm{PSL}_2(\mathbb{Z})$. Rarely, however, are they *modular curves*; the finite index subgroup of $\mathrm{PSL}_2(\mathbb{Z})$ is not a congruence subgroup. Both examples illustrate this.

Consider any family of covers of $\mathbb{P}^1_z$ of a given degree. Such families separate naturally into topological components depending on data about the covers in the family. Distinct Nielsen classes will have different components. Sometimes a given Nielsen class may contain several components. For example, [Fri96] describes precisely the number of topological components in the moduli space of (connected) covers of $\mathbb{P}^1_z$ of degree n having r 3-cycle branch points. It is exactly two, if $r \geq n$

and exactly one if $r = n-1$ (smaller values of r produce no such covers). Our first example from [Fri90, §5.2] gives the details of this result when $n = 5$ and $r = 4$. We use the example on new problems, correct a typo and improve the computation. *Computing* has a different meaning than in related examples of [Mes90].

7.2. **For the Inverse Galois Problem: $G = A_5$, $\mathbf{C} = \mathbf{C}_{3^4}$.** Consider degree five rational functions with four 3-cycles as branch cycles. We describe the family and then give quick conclusions about the Galois closure of these covers. To wit:

(7.2a) There is one connected family of such covers.
(7.2b) Many members of the family have equations over $\mathbb{Q}$ and a Galois closure realizing the alternating group of degree 5 as a Galois group over $\mathbb{Q}$.
(7.2c) Covers satisfying (7.2b) are quotients of a regular realization of the universal central extension of A_5 over $\mathbb{Q}$.
(7.2d) Many family members have equations over $\mathbb{Q}$ with Galois closure a non-regular realization of S_5 as a Galois group over $\mathbb{Q}$.

7.3. **Expectations of the universal parameter space of such covers.** We are describing a set $\mathcal{H} = \mathcal{H}(A_5, \mathbf{C}_{3^4})$. Its $\mathbb{C}$ points are equivalence classes of rational functions f whose covers have these properties.

(7.3a) $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is of degree 5 with 4 branch points.
(7.3b) If x_0 is a multiple point of the fiber over z_0, then the multiplicity of x_0 in this fiber is three.

The equivalence here is simple. Given two rational functions f_1 and f_2 satisfying (7.3), they are equivalent if there exists a linear fractional transformation α for which $f_1(\alpha(x)) = f_2(x)$. Abstractly, and more relevant to general computations:

(7.4) there exists $\alpha : \mathbb{P}^1_x \to \mathbb{P}^1_x$ for which $f_1 \circ \alpha = f_2$.

In this example $\mathcal{H}$ is a fine moduli space; A_5 is a primitive group, so there are no nontrivial automorphisms of a cover $\varphi : X \to \mathbb{P}^1_z$ in the Nielsen class commuting with φ. Also, $\mathcal{H}$ covers the space $\mathbb{P}^4 \setminus D_4 = U_4$ where D_4 is the usual discriminant locus in projective 4-space. The cover comes from mapping f to the unordered set of branch points of its associated cover. Denote this cover by $\Psi_4 : \mathcal{H} \to U_4$. An easy consequence of Thm. 3.2 shows this cover has the same number of preimage points over each point of U_4. It is the number of elements in the Nielsen class $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})$ (§2.2.1) up to conjugating by the normalizer (S_5) of A_5 in S_5. This turns $\mathcal{H}$ into an analytic manifold covering U_4. The computations below are details on recognizing this manifold from data on the fundamental group of U_4.

These simple definitions apply to any family of rational functions. There is one subtlety! Our computations below show $\mathcal{H}$ has one component defined over $\mathbb{Q}$. Suppose $\boldsymbol{p} \in \mathcal{H}$ is a $\mathbb{Q}$ point. Then, we expect the following:

(7.5) $\boldsymbol{p}$ corresponds to a rational function $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ with field of definition $\mathbb{Q}$.

For rational functions, however, in general we can only say the following.

(7.6) $\boldsymbol{p}$ produces $X_{\boldsymbol{p}} \to \mathbb{P}^1_z$ over $\mathbb{Q}$ giving a rational function $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ in the desired Nielsen class over some finite extension of $\mathbb{Q}$.

The distinction between (7.5) and (7.6) is whether X in (7.6) has a $\mathbb{Q}$ point. Here this is automatic; the covers have odd (five) degree. We'll use this (documented many places, including [DF99]) to get rational points on $\mathcal{H}$.

7.4. **Representatives of absolute Nielsen classes.** Conjugating by S_5 produces a representative $\boldsymbol{g}$ of an element of $\mathrm{Ni}(\mathbf{C}_{3^4})^{\mathrm{abs}}$ having $g_1 = (1\,2\,3)$ with g_2 having either 1, 2 or 3 integers in its 3-cycle in common with $\{1,2,3\}$. If there are three integers in common, then $g_2 = g_1^{-1}$ and $g_3 = (1\,4\,5)$. If two integers, then we may assume $g_2 = (2\,1\,4)$. If only one integer in common, then $g_2 = (1\,4\,5)$. This allows listing the (g_2, g_3, g_4) entries of *absolute* Nielsen class representatives (Figure 1).

FIGURE 1. List $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{abs}$

X_1: ((1 3 2), (1 4 5), (1 5 4)); X_2: ((1 4 5), (1 5 4), (1 3 2));
X_3: ((1 4 5), (2 1 5), (2 4 3)); X_4: ((1 4 5), (3 2 4), (1 5 4));
X_5: ((1 4 5), (4 3 2), (4 1 5)); X_6: ((1 4 5), (5 4 3), (5 2 1));
X_7: ((2 1 4), (2 4 5), (5 3 2)); X_8: ((2 1 4), (3 2 5), (5 4 3));
X_9: ((2 1 4), (4 3 5), (2 4 5)).

Replace X_i by the integer i, $i = 1, \dots, 9$, to give a degree 9 representation of H_4. Here is the effect of braid group generators Q_i, $i = 1, 2, 3$ (§7.5) on $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{abs}}$:

(7.7) $\quad Q_1 = (2\,5\,3\,6\,4)(7\,9\,8), \quad Q_2 = (1\,4\,9\,8\,5)(3\,6\,7)$ and $Q_3 = (2\,5\,3\,6\,4)(7\,9\,8)$.

Transitive action of H_4 on $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{abs}}$ means $\mathcal{H}^{\mathrm{abs}}$ is irreducible (see Prop. 7.1).

7.5. **Groups B_r, H_r and M_r.** The *braid group* B_r has generators $Q_1, \dots, Q_{r-1}$ modulo two relations:

(7.8) $\quad Q_iQ_j = Q_jQ_i$ for $|i-j| > 1$ and $Q_{i+1}Q_iQ_{i+1} = Q_iQ_{i+1}Q_i$, $1 \le i \le r-2$.

There are two other significant words:

(7.9a) $Q_1 \cdots Q_{r-1}Q_{r-1} \cdots Q_1$; and
(7.9b) $(Q_1 \cdots Q_{r-1})^r$.

The *Hurwitz monodromy group* H_r is the quotient of B_r modulo (7.9a). The *mapping class group* M_r is the quotient of H_r modulo (7.9b). Most significant, the braid group acts on a Nielsen class. For $\boldsymbol{g} \in \mathrm{Ni}(G, \mathbf{C})$,

(7.10) $\quad (\boldsymbol{g})Q_i = (g_1, \dots, g_{i-1}, g_ig_{i+1}g_i^{-1}, g_i, g_{i+2}, \dots, g_r), i = 1, \dots, r-1.$

The word $w \in B_r$ appearing in (7.9a) conjugates $\boldsymbol{g}$ by g_1:

$$\boldsymbol{g} \mapsto (\boldsymbol{g})w = g_1\boldsymbol{g}g_1^{-1} = (\dots, g_1g_ig_1^{-1}, \dots).$$

7.6. **Modulo PSL_2 action.** We follow the procedure from [DF99, Prop. 6.4 and Prop. 6.5]. When $r = 4$, this gives a cover of the j-line. For simplicity, assume the three points of ramification are at $0, 1, \infty$ rather than at the traditional locations given by modular curves. Here is the idea behind the computation. There is a *strong* equivalence relation between covers.

(7.11) $\quad \varphi_i : X_i \to \mathbb{P}^1$, $i = 1, 2$, are equivalent if there exists $\alpha : X_1 \to X_2$ and $\beta : \mathbb{P}^1 \to \mathbb{P}^1$ with $\varphi_2 \circ \alpha = \beta \circ \varphi_1$.

[DF99, Prop. 6.4] explains the existence of $\mathcal{H}/\mathrm{PSL}_2(\mathbb{C}) = \mathcal{H}^{\mathrm{rd}}$ as an affine algebraic variety covering $\mathbb{P}^1_j \setminus \{\infty\}$. The cover ramifies over two points; its projective closure ramifies over 3 points including $j = \infty$. Each component of $\mathcal{H}^{\mathrm{rd}}$ has a branch cycle description of its projective completion $\bar{\mathcal{H}}^{\mathrm{rd}}$ as a ramified cover of $\mathbb{P}^1_j$. Our examples have only one component. For notational simplicity, assume irreducibility of $\mathcal{H}$ (equivalent to irreducibility of $\mathcal{H}^{\mathrm{rd}}$).

7.7. **Special generators of $\pi_1(\mathbb{P}^1_j \setminus \{0,1,\infty\})$.** Let q_1, q_2, q_3 be the images of Q_1, Q_2, Q_3 in the mapping class group M_4 (7.9b). Form one further equivalence on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ (or on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$). Recall: For $\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})$, $g_1g_2g_3g_4 = 1$. For $\boldsymbol{g} \in \mathrm{Ni}(G,\mathbf{C})$, $(Q_1Q_3^{-1})^2$ has this effect:

$$\boldsymbol{g} \mapsto (g_1g_2g_1g_2^{-1}g_1^{-1}, g_1g_2g_1^{-1}, g_4^{-1}g_3g_4, g_4^{-1}g_3^{-1}g_4g_3g_4) \equiv^G \boldsymbol{g}. \tag{7.12}$$

Form $\mathrm{Ni}(G,\mathbf{C})/\langle Q_1Q_3^{-1}\rangle = \mathrm{MQ}(G,\mathbf{C})$ for *mapping quotient* classes. Action of H_4 on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ induces $H_4/\langle Q_1Q_3^{-1}\rangle = \bar{H}_4$ acting on $\mathrm{MQ}(G,\mathbf{C})$. This gives quotient sets $\mathrm{MQ}(G,\mathbf{C})^{\mathrm{abs}}$ and $\mathrm{MQ}(G,\mathbf{C})^{\mathrm{in}}$ analogous to $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ and $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$.

7.8. **Branch cycle description of $\bar{\mathcal{H}}^{\mathrm{rd}} \to \mathbb{P}^1_j$.** [DF99, Prop. 6.5] gives the branch cycle description for which we aim.

Proposition 7.1 (j-Line Branch Cycles)**.** *The group $\bar{H}_4$ has generators $\alpha = q_1q_2$ and $\gamma = q_1q_2q_1$ subject to the relations $\alpha^3 = \gamma^2 = 1$: $\bar{H}_4 \equiv \mathrm{PSL}_2(\mathbb{Z})$. Orbits of $\bar{H}_4$ on $\mathrm{MQ}(G,\mathbf{C})^{\mathrm{abs}}$ (resp. $\mathrm{MQ}(G,\mathbf{C})^{\mathrm{in}}$) correspond one-one to orbits of H_4 on $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{abs}}$ (resp. $\mathrm{Ni}(G,\mathbf{C})^{\mathrm{in}}$). In particular, let α' and γ' be respective actions of α and γ on $\mathrm{MQ}(G,\mathbf{C})^{\mathrm{abs}}$. Then (α', γ', q_2') is a description of the branch cycles of the cover $\bar{\mathcal{H}}^{\mathrm{rd}} \to \mathbb{P}^1_j$.*

Finally, $\bar{\mathcal{H}}^{\mathrm{rd}}$ is unirational over K if and only its genus is 0 and

(7.13) *it has a K rational divisor of odd degree.*

When $r = 4$, any K point on $\bar{\mathcal{H}}^{\mathrm{rd}}$ produces a K point above it on $\mathcal{H}$ [DF99, Prop. 6.8]. [Fri] illustrates this isn't true if $r > 4$, though it is still true that a dense set of rational points on $\bar{\mathcal{H}}^{\mathrm{rd}}$ implies a dense set of rational points on $\mathcal{H}$.

7.9. **Showing $\bar{\mathcal{H}}^{\mathrm{rd}} = \mathbb{P}^1_w$ over $\mathbb{Q}$.** The computation works to show $\mathcal{H}$ has many rational points because it shows us this curve has genus zero and one rational point. Then, it automatically has infinitely many. Apply (7.7) to display the branch cycles for $\bar{\mathcal{H}}^{\mathrm{rd}}$ as a cover of $\mathbb{P}^1_j$:

$$\begin{array}{rl} \alpha' = q_1'q_2' = & (2\,1\,4)(3\,7\,8)(5\,6\,9), \gamma' = q_1'q_2'q_1' = (2\,1)(4\,5)(6\,8)(3\,9) \text{ and} \\ q_2' = & (1\,4\,9\,8\,5)(3\,6\,7). \end{array} \tag{7.14}$$

Thus, the genus $g = g^{\mathrm{abs}}$ of $\bar{\mathcal{H}}^{\mathrm{rd}}$ appears in the Riemann-Hurwitz formula:

(7.15) $2(9 + g - 1) = 6 + 4 + 6$, $g = 0$, with the right side the respective sum of the contributions from (7.14).

Note: $(\alpha')^5$ is a 3-cycle, and $(\alpha')^3$ is a 5-cycle. Thus, the geometric monodromy group of this cover is A_9: It is a primitive subgroup of A_9 containing a 3-cycle.

Lemma 7.2. *There is no integer N for which $\mathrm{PSL}_2(\mathbb{Z}/N)$ maps surjectively to A_9. In particular, $\bar{\mathcal{H}}^{\mathrm{rd}}$ is not a congruence curve.*

Proof. Suppose $X \to \mathbb{P}^1_j$ is a compactification of an upper half plane by a subgroup $\Gamma \le \mathrm{PSL}_2(\mathbb{Z})$. Then, it is a congruence curve if there is an integer N with Γ containing the kernel of $\mathrm{PSL}_2(\mathbb{Z}) \to \mathrm{PSL}_2(\mathbb{Z}/N)$ by reduction modulo N. In particular, to be a modular curve, the monodromy group of a cover of a j-line must be a quotient of $\mathrm{PSL}_2(\mathbb{Z}/N)$ for some integer N. There are, by the way, other ways to present $\mathrm{PSL}_2(\mathbb{Z}/N)$ as a quotient of $\mathrm{PSL}_2(\mathbb{Z})$. So, this is not an if and only if criterion for being a modular curve. To conclude the proof, note that A_9 is a simple group, and the only simple quotients of $\mathrm{PSL}_2(\mathbb{Z}/N)$ are groups $\mathrm{PSL}_2(\mathbb{Z}/p)$ for primes p dividing N. These groups, however, have order $(p^2-1)p/2$ (if $p \neq 2$) and in particular, cannot have the order of A_9. □

7.10. **Branch cycle description of $\bar{\mathcal{H}}^{\mathrm{in,rd}} \to \mathbb{P}^1_j$.** Let $\boldsymbol{p} \in \mathcal{H}^{\mathrm{rd}}(\mathbb{Q})$. Then, $\boldsymbol{p}$ produces a cover $f_{\boldsymbol{p}} : \mathbb{P}^1_x \to \mathbb{P}^1_z$ (by rational functions with coefficients in $\mathbb{Q}$) of degree 5 in the Nielsen class $\mathrm{Ni}(S_5, \mathbf{C})^{\mathrm{abs}}$. In the Inverse Galois Problem, we want to know about the Galois closure of $\hat{\varphi}_{\boldsymbol{p}} = \mathbb{P}^1_x : \hat{X}_{\boldsymbol{p}} \to \mathbb{P}^1_z$. This is the minimal Galois cover (with group A_5) over $\mathbb{Q}$ factoring through f. Being over $\mathbb{Q}$ means all the automorphisms of $\hat{X}_{\boldsymbol{p}}$ also have field of definition $\mathbb{Q}$. To translate to field theory, the field of $\mathbb{Q}$ rational functions on $\hat{X}_{\boldsymbol{p}}$ is the Galois closure of the extension $\mathbb{Q}(x)/\mathbb{Q}(z)$ (with $f_{\boldsymbol{p}}(x) = z$). This Galois closure has group in S_5 (from action on the conjugates of x over $\mathbb{Q}(z)$). So, the Galois group is either S_5 or A_5. If it is S_5, then $\hat{X}_{\boldsymbol{p}}$ has two connected components over $\bar{\mathbb{Q}}$ conjugate by the action of $G_{\mathbb{Q}}$. The remaining computation shows both Galois closures happen often.

Theorem 7.3. *A dense set of $\boldsymbol{p} \in \mathcal{H}^{\mathrm{abs}}(\mathbb{Q})$ have Galois closure group A_5 for $f_{\boldsymbol{p}}$. Also, a dense set of $\boldsymbol{p} \in \mathcal{H}^{\mathrm{abs}}(\mathbb{Q})$ have Galois closure group S_5 for $f_{\boldsymbol{p}}$.*

Proof. We can use the previous work. The result follows by interpreting Galois closure covers as corresponding to points of $\mathcal{H}^{\mathrm{in}}$ [FV91]. Computations for branch cycles for $\mathcal{H}^{\mathrm{in,rd}} \to \mathbb{P}^1_j$ are exactly as for $\bar{\mathcal{H}}^{\mathrm{rd}} \to \mathbb{P}^1_j$ except replace $\mathrm{Ni}(A_5, \mathbf{C})^{\mathrm{abs}}$ by $\mathrm{Ni}(A_5, \mathbf{C})^{\mathrm{in}}$. To do this, conjugate elements from $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{abs}}$ by $(4\,5)$ to get these new additions for (g_2, g_3, g_4) (Figure 2).

FIGURE 2. List $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\mathrm{in}}$

X_{10}: $((1\,3\,2), (1\,5\,4), (1\,4\,5))$; X_{11}: $((1\,5\,4), (1\,4\,5), (1\,3\,2))$;
X_{12}: $((1\,5\,4), (2\,1\,4), (2\,5\,3))$; X_{13}: $((1\,5\,4), (3\,2\,1), (1\,4\,5))$;
X_{14}: $((1\,5\,4), (5\,3\,2), (5\,1\,4))$; X_{15}: $((1\,5\,4), (4\,5\,3), (4\,2\,1))$;
X_{16}: $((2\,1\,5), (2\,5\,4), (4\,3\,2))$; X_{17}: $((2\,1\,5), (3\,2\,4), (4\,5\,3))$;
X_{18}: $((2\,1\,5), (5\,3\,4), (2\,5\,4))$.

Refer to Q_1 and Q_2 acting on $\mathrm{MQ}(A_5, \mathbf{C}_{3^4})^{\mathrm{in}}$ by q_1^* and q_2^* respectively:

$$\begin{aligned} q_1^* &= (1\,10)(2\,5\,3\,6\,4)(7\,9\,8)(11\,14\,12\,15\,13)(16\,18\,17) \\ q_2^* &= (2\,11)(1\,4\,18\,8\,5)(10\,13\,9\,17\,14)(3\,15\,16)(12\,6\,7). \end{aligned} \tag{7.16}$$

Again, the action of $\langle q_1^*, q_2^* \rangle$ is transitive on the 18 integers of the representation. Here are the branch cycles for the cover.

$$\begin{aligned} \alpha^* &= q_1^* q_2^* && = (1\,13\,2)(3\,7\,17)(4\,11\,10)(5\,15\,9)(6\,18\,14)(8\,12\,16) \\ \gamma^* &= q_1^* q_2^* q_1^* && = (1\,11)(2\,10)(3\,9)(4\,14)(5\,13)(6\,17)(7\,16)(8\,15)(12\,18); \\ & \text{and } q_2^* && = (2\,11)(1\,4\,18\,8\,5)(10\,13\,9\,17\,14)(3\,15\,16)(12\,6\,7). \end{aligned} \tag{7.17}$$

Since the action is transitive, there is a natural unramified covering map $\psi : \bar{\mathcal{H}}^{\mathrm{in,rd}} \to \bar{\mathcal{H}}^{\mathrm{rd}}$ of degree two. For $\boldsymbol{p}' \in \mathcal{H}^{\mathrm{in,rd}}(\mathbb{C})$, let $\hat{\varphi} : \hat{X}_{\boldsymbol{p}} \to \mathbb{P}^1_z$ be a representing cover. The data for this moduli space (as in [FV91]) identifies the automorphism group of $\hat{\varphi}$ over $\mathbb{Q}(\boldsymbol{p})$ with A_5. Take A_4 as the stabilizer of 1 in A_5. The quotient $\hat{X}_{\boldsymbol{p}}/A_4$ by A_4 is then a cover corresponding to a point $\boldsymbol{p} \in \mathcal{H}^{\mathrm{rd}}$. The covering ψ maps $\boldsymbol{p}'$ to $\boldsymbol{p}$.

Thus, the genus g^{in} of $\bar{\mathcal{H}}^{\mathrm{in,rd}}$ appears in the Riemann-Hurwitz formula:

$$2(18 + g^{\mathrm{in}} - 1) = 12 + 9 + 13 = 34, \text{ or } g^{\mathrm{in}} = 0, \tag{7.18}$$

with the right side the respective sum of the contributions from (7.17). This is an 18 degree cover of the j-line, so the odd degree principle doesn't produce a rational point on $\bar{\mathcal{H}}^{\rm in,rd}$. Compare, however, γ^* in (7.17) with γ' in (7.14). The disjoint cycle (7 16) corresponds to a ramified point of $\bar{\mathcal{H}}^{\rm in,rd}$ lying over the only unramified point of $\bar{\mathcal{H}}^{\rm rd}$ corresponding to the branch point for γ'. From this identifying description, $G_{\mathbb{Q}}$ fixes the point. So, it is the $\mathbb{Q}$ point we seek. □

7.11. **Adding the branch points.** Variants on basic Hurwitz spaces add data about points above the branch points in the members of the family to the parameter space data. These give *marked* Nielsen classes ([BF82] and in [DF90] for general genus 0 families of covers). The easiest, very classical, use puts an ordering on the branch points. [DF99] explains this carefully. Consider the case $r = 4$. After quotienting by action of $\mathrm{PSL}_2(\mathbb{C})$, the parameter space of distinct unordered 4-tuples from $\mathbb{P}^1_z$ is the classical λ-line. Then, $\bar{\mathcal{H}}^{\rm rd,\lambda}$ is the normalization of any irreducible component of $\bar{\mathcal{H}}^{\rm rd} \times_{\mathbb{P}^1_j} \mathbb{P}^1_\lambda$. Projection of $\bar{\mathcal{H}}^{\rm rd,\lambda}$ onto $\bar{\mathcal{H}}^{\rm rd}$ is a component of the pullback of $\bar{\mathcal{H}}^{\rm rd}$ over the degree six cover, $\mathbb{P}^1_\lambda \to \mathbb{P}^1_j$.

7.11.1. *The $a_{i,j}$ s on* $\mathrm{Ni}(A_5, \mathbf{C}_{3^4})^{\rm abs}$. Action of $a_{1,2} = q_1^2$, $a_{1,3} = q_1^{-1}q_2^2q_1$ and $a_{1,4} = q_1^{-1}q_2^{-1}q_3^2q_2q_1$ on an appropriate absolute or inner Nielsen class orbit gives the corresponding branch cycle description. Riemann-Hurwitz (on absolute Nielsen classes) gives the genus g^λ of $\bar{\mathcal{H}}^{\rm rd,\lambda}$. Here are the corresponding branch cycles for $\bar{\mathcal{H}}^{\rm rd,\lambda} \to \mathbb{P}^1_\lambda$:

$$\begin{array}{ll} a'_{1,2} = & (2\,3\,4\,5\,6)(7\,8\,9), \\ a'_{1,3} = & (1\,8\,3\,2\,7)(4\,6\,9), \text{ and} \\ a'_{1,4} = & (9\,5\,4\,8\,1)(7\,6\,3). \end{array} \tag{7.19}$$

From transitivity of the $a'_{1,j}s$, $\mathcal{H}^{\rm rd,\lambda}$ is irreducible. Then, $2(9 + g^\lambda - 1) = 3 \cdot 6 = 18$. That is, $g^\lambda = 1$. The points of ramification in this cover of the λ-line are $0, 1, \infty$, and above each of the branch points are three points of different ramification indices (resp. 1, 3, and 5). So, each is a $\mathbb{Q}$ point. Thus, the genus 1 curve $\mathcal{H}^{\rm rd,\lambda}$ has at least nine $\mathbb{Q}$ points. In an obvious notation, label these

$$P^{\rm ram} = \{\boldsymbol{p}_{0,1}, \boldsymbol{p}_{0,3}, \boldsymbol{p}_{0,5}, \boldsymbol{p}_{1,1}, \boldsymbol{p}_{1,3}, \boldsymbol{p}_{1,5}, \boldsymbol{p}_{\infty,1}, \boldsymbol{p}_{\infty,3}, \boldsymbol{p}_{\infty,5}\}. \tag{7.20}$$

Use $\boldsymbol{p}_{0,1}$ as the basepoint for an elliptic curve structure on $\bar{\mathcal{H}}^{\rm rd,\lambda}$.

7.11.2. $\mathbb{Q}$ *points on* $\mathcal{H}^{\rm rd,\lambda}$. Identify $\bar{\mathcal{H}}^{\rm rd,\lambda}$ with its Picard group $\mathrm{Pic}^0(\bar{\mathcal{H}}^{\rm rd,\lambda}) = \mathrm{Pic}^0$ of divisor classes modulo linear equivalence. The set $\{\boldsymbol{p} - \boldsymbol{p}_{0,1}\}_{\boldsymbol{p} \in P^{\rm ram}}$ generates a subgroup $\bar{D}(P^{\rm ram})$ of Pic^0. The divisors $\boldsymbol{p}_{0,1} + 3\boldsymbol{p}_{0,3} + 5\boldsymbol{p}_{0,5} - \boldsymbol{p}_{1,1} - 3\boldsymbol{p}_{1,3} - 5\boldsymbol{p}_{1,5}$ and $\boldsymbol{p}_{0,1} + 3\boldsymbol{p}_{0,3} + 5\boldsymbol{p}_{0,5} - \boldsymbol{p}_{\infty,1} - 3\boldsymbol{p}_{\infty,3} - 5\boldsymbol{p}_{\infty,5}$ are linearly equivalent to 0; they are the differences of two fibers of a function. Further, because the curve has genus 1, its differential 1-forms have divisor linearly equivalent to the trivial divisor. This applies to $d\bar{\psi}$ ($\psi : \mathcal{H}^{\rm rd,\lambda} \to \mathbb{P}^1_\lambda$). This calculation shows the rank of $\bar{D}(P^{\rm ram})$ is at most five. If $\mathcal{H}^{\rm rd,\lambda}$ were a modular curve, then $\bar{D}(P^{\rm ram})$ would be a finite group (rank 0; [Dri73] and [Man72]). Though $\mathcal{H}^{\rm rd,\lambda}$ is not a modular curve, it has modular curve like properties. These arise from it being a moduli space fitting in what [Fri95c] calls a Modular Tower. Compatible with this, [FB98] shows the following.

Theorem 7.4. *The group $\bar{D}(P^{\rm ram}) \equiv \mathbb{Z}/(2)\times\mathbb{Z}/(2)\times\mathbb{Z}/(3)$ has order 12. Thus, from Mazur's theorem describing possible groups of rational points on elliptic curves over $\mathbb{Q}$ (see §11.1), $\bar{D}(P^{\rm ram})$ is the complete subgroup of torsion elements on $\mathcal{H}^{{\rm rd},\lambda}$. Any point $\boldsymbol{p}\in\bar{\mathcal{H}}^{{\rm rd},\lambda}(\mathbb{Q})$ lying over $\mathbb{P}^1_\lambda\setminus\{0,1,\infty\}$ produces a degree 5 cover $X_{\boldsymbol{p}}\to\mathbb{P}^1_z$ in the Nielsen class ${\rm Ni}(A_5,\mathbf{C}_{3^4})$ having its branch points in $\mathbb{Q}$. Further, the rank of the points is 0, and these are the only $\mathbb{Q}$ points on $\bar{\mathcal{H}}^{{\rm rd},\lambda}$.*

Since $\mathcal{H}^{{\rm rd},\lambda}(\mathbb{Q})$ is not dense, it exemplifies the following phenomenon. A Hurwitz space $\mathcal{H}^{\rm rd}(G,\mathbf{C})$ (covering the j-line) has a dense set of $\mathbb{Q}$ points corresponding to covers $X\to\mathbb{P}^1_z$ in the Nielsen class defined over $\mathbb{Q}$. Still, the following hold:

(7.21a) The conjugacy classes $\mathbf{C}$ are each rational; and
(7.21b) excluding a finite, identifiable subset of covers, no $\mathbb{Q}$ cover $X\to\mathbb{P}^1_z$ in this Nielsen class has branch points in $\mathbb{Q}$.

7.11.3. *Same questions for $\mathcal{H}^{{\rm rd},{\rm in},\lambda}$.* Consider the same questions as above, but for realizations of A_5 by covers in the Nielsen class ${\rm Ni}(A_5,\mathbf{C}_{3^4})$. There are questions about the analogous curve $\mathcal{H}^{{\rm rd},{\rm in},\lambda}$ covering $\mathbb{P}^1_\lambda\setminus\{0,1,\infty\}$ and its nonsingular projective closure $\bar{\mathcal{H}}^{{\rm rd},{\rm in},\lambda}$. Compute the genus $g^{{\rm in},\lambda}$ of this curve from the shape of $(q_1^*)^2$ and $(q_2^*)^2$ in (7.16): $2(18+g^{{\rm in},\lambda}-1)=3\cdot 12=36$, or $g^{{\rm in},\lambda}=1$. More directly, from the branch cycle structure, each point of $\bar{\mathcal{H}}^{{\rm rd},\lambda}$ has exactly two points of $\bar{\mathcal{H}}^{{\rm rd},{\rm in},\lambda}$ above it. That is, over $\mathbb{C}$ these are isogenous elliptic curves (by a degree 2 isogeny). The following argument shows $\bar{\mathcal{H}}^{{\rm rd},{\rm in},\lambda}$ does have $\mathbb{Q}$ points.

Lemma 7.5. *Let x' be the point of $\bar{\mathcal{H}}^{{\rm rd},{\rm in}}$ corresponding to the disjoint cycle of q_2^* of length 2 in* (7.17)*. The preimage of this in $\bar{\mathcal{H}}^{{\rm rd},{\rm in},\lambda}$ consists of six $\mathbb{Q}$ points.*

Proof. The cover $\mathbb{P}^1_\lambda\to\mathbb{P}^1_j$ has three rational points $0,1,\infty$ over ∞. The map $w\mapsto w^2$ produces $\mu:\mathbb{P}^1_u\to\mathbb{P}^1_z$. Before normalization, $\bar{\mathcal{H}}^{{\rm rd},{\rm in}}\times_{\mathbb{P}^1_j}\mathbb{P}^1_\lambda$ over x' looks locally like three disjoint copies of the fiber product of μ with itself over $z=0$. The fiber product of μ with itself locally has the form $\{(w,w')\mid w^2-(w')^2\}$ around $(0,0)$. After normalization this locus consists of two rational points. □

8. Degree 13 Davenport Polynomials

For degree 13 Davenport polynomials, separation of the family of covers into components comes from elementary group theory. [Fri95b, Lemma 4.6, Part E of proof] does the case of Davenport polynomials of degree 7. Suppose (f,h) gives a reducible variables separated polynomial of degree 13 with f and h linearly inequivalent over $\mathbb{C}$. From the second paragraph of the Thm. 9.1's proof, a branch cycle description has either 3 or 4 branch points.

8.1. **Group theory setup for Davenport polynomials of degree 13.** We describe the Nielsen classes for $r=4$. Those with $r=3$ branch points come from coalescing the branch cycles of a Nielsen class with $r=4$. First we list elements $\boldsymbol{g}\in{\rm Ni}({\rm PSL}_3(\mathbb{Z}/3),\mathbf{C})$ of the Nielsen class (§7.4) with g_4 a 13-cycle. As forced by Thm. 9.1, this means g_1, g_2 and g_3 are each a product of four disjoint 2-cycles. Up to absolute equivalence, assume $g_4=g_\infty=(1\,2\,\ldots\,13)^{-1}$. Following the proof of Thm. 9.1, consider the zeros $y_1,\ldots,y_{13}$ of $h(y)-z$ as representing lines of $\mathbb{P}^2(\mathbb{Z}/3)$. These relate to $x_1,\ldots,x_{13}$ of $f(x)-z$ (representing points of $\mathbb{P}^2(\mathbb{Z}/3)$) by the formula $y_1=x_1+x_{\alpha_2}+x_{\alpha_3}+x_{\alpha_4}$. Here $\mathcal{D}=\{1,\alpha_2,\alpha_3,\alpha_4\}$ is a *difference set*

modulo 13; nonzero differences from $\mathcal{D}$ repeat every residue class the same number of times (once in this case).

Up to translation there are 4 difference sets modulo 13. All cases are similar. so we choose $\{1,2,4,10\}$ to be specific. The others come from multiplications by elements of $(\mathbb{Z}/(13))^*$. Note: Multiplication by $\langle 3\rangle$ preserves this difference set (up to translation). Each of g_1, g_2, g_3 fixes all points of some line. If for g_1 this line corresponds to y_1, then g_1 must be an element from List A.

FIGURE 3. Transvection List A

(7 8)(5 11)(6 12)(9 13);	(3 11)(7 13)(6 8)(9 12);
(3 12)(5 8)(7 9)(11 13);	(5 13)(6 9)(11 12)(3 8);
(5 6)(3 7)(8 11)(12 13);	(6 7)(8 11)(5 12)(3 13);
(3 5)(7 12)(6 13)(8 9);	(3 6)(5 9)(7 11)(8 13);
(5 7)(6 11)(8 13)(3 9).	

8.2. **Listing elements of a Nielsen class.** Each entry of List A corresponds to one of the 9 remaining fixed numbers. Compute directly possibilities for g_1, g_2, g_3:

8.2.1. *Degree 13 Davenport cycles* (g_1, g_2, g_3) *List B.*

X_1 :	(6 7)(8 11)(5 12)(3 13),	(2 3)(13 4)(6 8)(9 10),	(1 2)(13 5)(6 12)(9 11)
X_2 :	(6 7)(8 11)(5 12)(3 13),	(1 2)(13 5)(6 12)(9 11),	(1 3)(5 4)(12 8)(11 10)
X_3 :	(3 5)(7 12)(6 13)(8 9),	(1 6)(2 3)(13 7)(12 10),	(8 10)(12 11)(6 2)(5 4)
X_4 :	(3 5)(7 12)(6 13)(8 9),	(8 10)(12 11)(6 2)(5 4),	(1 2)(6 3)(13 7)(11 8)
X_5 :	(5 6)(3 7)(9 11)(12 13),	(1 3)(4 5)(8 12)(11 10),	(2 3)(7 4)(1 8)(12 9)
X_6 :	(5 6)(3 7)(9 11)(12 13),	(9 12)(2 3)(7 4)(1 8),	(8 2)(7 5)(1 9)(11 10)
X_7 :	(5 6)(3 7)(9 11)(12 13),	(1 9)(2 8)(7 5)(10 11),	(4 5)(3 8)(9 2)(12 1)
X_8 :	(5 6)(3 7)(9 11)(12 13),	(4 5)(3 8)(9 2)(12 1),	(12 2)(9 3)(7 4)(11 10)
X_9 :	(8 9)(7 12)(13 6)(3 5),	(1 2)(6 3)(13 7)(11 8),	(1 3)(5 4)(12 8)(11 10)
X_{10} :	(6 7)(8 11)(5 12)(3 13),	(1 3)(4 5)(12 8)(11 10),	(6 8)(10 9)(4 13)(3 2)
X_{11} :	(7 3)(5 6)(12 13)(9 11),	(1 2)(7 5)(3 12)(8 9),	(1 3)(5 4)(12 8)(11 10)
X_{12} :	(5 6)(3 7)(9 11)(12 13),	(10 11)(2 12)(3 9)(7 4),	(1 2)(3 12)(7 5)(9 8)
X_{13} :	(8 9)(6 13)(7 12)(3 5),	(1 3)(5 4)(12 8)(11 10),	(2 3)(1 6)(7 13)(10 12).

8.2.2. *Comments on Davenport cycles List B.* Only powers of g_4 commute with $(1\,2\,\ldots\,13)^{-1} = g_4$. So, if (g_1, g_2, g_3, g_4) is conjugate to (g_1', g_2', g_3', g_4), the conjugation is by some power of g_4. Thus, assume g_1 is one of the elements in List A. Conjugating elements from List A by powers of g_4 gives the complete set of products of four disjoint 2-cycles in G. In the 2-cycle support of any two of these elements at least four integers appear in common. So, g_2 and g_3 together are missing one integer from their support. Call it $i+1$. Conclude g_1 must contain $(i\,i+1)$. Thus only 5 elements from List A are suitable choices for g_1. All entries in the branch cycles for List B are conjugates by powers of g_4 of these choices. Now complete List B through trial and error.

Similarly, assume $(1\,2\,\ldots\,13)^{-1}$ appears in any one of the four positions in a branch cycle 4-tuple. Also, the element of order 2 closest to the left fixes the points

of the block $\{1,2,4,10\}$. Thus, up to equivalence, there are $4 \cdot 13 = 52$ possible descriptions of the branch cycles. Denote the entire collection by $\mathrm{Ni}(\{1,2,4,10\})$.

8.3. **Conclusions from the computation of Q_1 and Q_2.** Continue as in §7.9. Since, Q_1 and Q_2 map elements in List B among themselves, first restrict them to List B, after renaming the elements of List B to be $\{1,2,\dots,13\}$. Compute:

$$\begin{array}{ll} Q_1 = & (1\,6\,13\,7)(2\,12\,11\,10\,9\,3)(4\,8\,5), \\ Q_2 = & (1\,10\,2)(3\,13\,9\,4)(5\,11\,12\,8\,7\,6). \end{array} \tag{8.1}$$

From this, conclude transitive action of H_4 on $\mathrm{Ni}(\{1,2,4,10\})$. In particular, this shows the irreducibility of the family of polynomials in the Nielsen class $\mathrm{Ni}(\{1,2,4,10\})$. The goal here is to investigate equivalence classes of polynomial covers. In particular, it is about absolute equivalence of covers. As the centralizer of G in S_{13} is trivial, there is a unique total family of covers representing these equivalence classes:

$$\mathcal{T}(\{1,2,4,10\}) \xrightarrow{\Phi} \mathcal{H}(\{1,2,4,10\}) \times \mathbb{P}^1_z. \tag{8.2}$$

It has this property: For $\boldsymbol{p} \in \mathcal{H}(\{1,2,4,10\})$, the set of points of $\mathcal{T}(\{1,2,4,10\})$ lying over $\boldsymbol{p} \times \mathbb{P}^1$ is a ramified cover of $\mathbb{P}^1_z$ in the equivalence class of $\boldsymbol{p}$.

8.4. **Defining field for $\mathcal{H}(\{1,2,4,10\})$.** Let $\zeta_{13} = e^{2\pi i/13}$. Identify $G(\mathbb{Q}(\zeta_{13})/\mathbb{Q})$ with $(\mathbb{Z}/(13))^*$. Denote the multiplier group of $\{1,2,4,10\}$ by $M(\{1,2,3,4\})$: elements of $(\mathbb{Z}(13))^*$ that multiply $\{1,2,4,10\}$ into a translate of this set. Let K_{13} be the fixed field of $M(\{1,2,4,10\})$ in $\mathbb{Q}(\zeta_{13})$. Therefore K_{13} is $\mathbb{Q}(\zeta_{13}+\zeta_{13}^3+\zeta_{13}^9)$, a degree 4 extension of $\mathbb{Q}$. Note: Elements of $M(\{1,2,4,10\})$ are exactly integer powers of g_4 conjugate to g_4 in $N_{S_{13}}(G)$. Thus, the stabilizer in $G(\mathbb{Q}(\zeta_{13}/\mathbb{Q})$ of the Nielsen class has fixed field K_{13}. This is therefore the field of definition of $\mathcal{H}(G,\mathbf{C})$. Further, each of the four families of polynomials correspond to a particular difference set; $G_{\mathbb{Q}}$ conjugates them among each other. The following is a special case of the *branch cycle argument* of [Fri77, prior to Thm. 5.1], though it appeared in [Fri73a] as a forerunner. Expositions like [Fri95a] and [Fri94b] quote the branch cycle argument only for $K = \mathbb{Q}$. The example here, however, requires the full statement.

8.4.1. *Cyclotomic action.* Let $(G,\mathbf{C})$ be a group together with any collection $\mathbf{C}$ of conjugacy classes in G. Denote the least common multiple of orders of elements in these conjugacy classes by $N_{\mathbf{C}} = N$. With $\zeta_N = e^{\frac{2\pi i}{N}}$, identify $G(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ with $(\mathbb{Z}/(N))^*$, the invertible integers modulo N. Then, for any field K containing $\mathbb{Q}$, $G(K(\zeta_N)/K) = G(\mathbb{Q}(\zeta_N)/K \cap \mathbb{Q})$ is a subgroup of $(\mathbb{Z}/(N))^*$. For the problem at hand, we have these assumptions:

(8.3) G is a transitive subgroup of S_n, and the centralizer of G in S_n is trivial.

Also, the equivalence on Nielsen class elements is by conjugation by $N_{S_n}(G,\mathbf{C}) = G^*$ (§2.2.1). For other problems, as in applications to the Inverse Galois Problem, we might replace G^* by another group between $N_{S_n}(G,\mathbf{C})$ and G. It doesn't matter, the same idea holds whatever is the equivalence.

8.4.2. *Equivalence of Nielsen classes under $G(K(\zeta_N)/K)$.* Any $\sigma \in G(K(\zeta_N)/K)$ gives an integer n_σ. Let $\mathbf{C}^{n_\sigma}$ be the conjugacy class collection from putting elements in conjugacy classes of $\mathbf{C}$ to the power n_σ. Write $\mathbf{C}^{n_\sigma} \cong^{G^*} \mathbf{C}$ if $\mathrm{Ni}(G,\mathbf{C}^{n_\sigma})/G^* = \mathrm{Ni}(G,\mathbf{C})/G^*$. This defines a subgroup $H_{G^*,\mathbf{C},K} = H$ of $G(K(\zeta_N)/K)$.

Theorem 8.1. *Assume* (8.3). *Then,* $\mathcal{H}(G,\mathbf{C})^{\rm abs}$ *has the fixed field* $L=\mathbb{Q}(\zeta_N)^{(H)}$ *of* H *in* $\mathbb{Q}(\zeta_N)$ *as field of definition. If the braid group action is transitive on* $\mathrm{Ni}(G,\mathbf{C})/G^*$, *then* $\mathcal{H}(G,\mathbf{C})^{\rm abs}$ *has exactly one absolutely irreducible component with field of definition* L.

Consider the elements $a_{1,2}, a_{1,3}$ and $(a_{1,2}a_{1,3})^{-1}$ from (7.19). We show $\langle a_{1,2}, a_{1,3}\rangle$ is transitive on $\mathrm{Ni}(\{1,2,4,10\})$. So conclude from Thm. 8.1 there are exactly four families of Davenport polynomials of degree 13. Each has field of definition K_{13} and all are conjugate by $G_{\mathbb{Q}}$.

$$\begin{aligned} a_{1,2} &= Q_1^{-2} = (1\,13)(6\,7)(2\,9\,11)(12\,3\,10)(4\,8\,5);\\ a_{1,3} &= Q_1Q_2^{-2}Q_1^{-1} = (1,4,12)(2,8,13)(3,7,11)(5,6)(9,10);\\ (a_{12}a_{13})^{-1} &= (1,10,2)(6,8,11)(7,12,5)(4,13)(3,9). \end{aligned} \tag{8.4}$$

Transitivity is clear.

8.5. **Rationality of** $\mathcal{H}(\{1,2,4,10\})$**.** This subsection gives the computations that show $\mathcal{H}(\{1,2,4,10\})$ has a dense set of K_{13} points, and therefore there are many Davenport polynomials of degree 13 over K_{13} producing maps $f:\mathbb{P}^1_x\to\mathbb{P}^1_z$ having 3 finite (4 total) branch points.

Theorem 8.2. *Let* σ *be a generator of* $G(K/\mathbb{Q})$. *There exists an indeterminate* s *and a polynomial* $f^*(s,x)\in K[s,x]$ *for which* $(a\cdot f^*(s,x)+b, a\cdot f^*(s,x)^{\sigma^2}+b)$ *and* $(a\cdot f^*(s,x)^{\sigma}+b, a\cdot f^*(s,x)^{\sigma^3}+b)$ *give all newly reducible polynomial pairs with* $n=13$ *as* a,b *and* s *run over* $\mathbf{C}$. *In addition, one can choose* s *so that* $K(s,a,b)$ *contains the coordinates of the branch points of* $f^*(s,x):\mathbb{P}^1_x\to\mathbb{P}^1_z$.

Comments. This amounts to showing the compactification of the reduced space $\bar{\mathcal{H}}^{\mathrm{rd},\lambda}$ covering the λ-line has genus 0 (as in §7.11). The result means the points of the moduli space corresponding to covers over K_{13}, having branch points also in K_{13}, are dense in the moduli space.

Here is the computation:

$$2(13+g^{\mathrm{rd},\lambda}-1)=\sum_{j=2}^{4}a_{1,j}=8+8+8. \tag{8.5}$$

Thus, $g^{\mathrm{rd},\lambda}=0$. Also, the degree of the cover is $n'=13$. So, the function field of $\bar{\mathcal{H}}^{\mathrm{rd},\lambda}$ is of the form $K_{13}(s)$, and it has branch points 0, 1, ∞. Each point on $\mathcal{H}^{\mathrm{rd},\lambda}$ (excluding points over branch points) gives a cover in the Nielsen class $\mathrm{Ni}(\{1,2,4,10\})$ having the last three of the branch points $0,1,\infty$. The 1st branch point z_1 of a generic cover, attached to one of the involution classes, has coordinates a function of s. Specify z_2 and z_3. Then, choose a and b so that $z\mapsto az+b$ has the effect of $0\to z_2$ and $1\to z_3$. □

9. Using the Classification

The group theoretic situation in (2.9) is this: G has faithful transitive permutation representations T_1 and T_2 of degree n with these properties.

- (9.1a) T_1 and T_2 are doubly transitive, with the same characters, but permutation inequivalent, and
- (9.1b) G contains g_∞ for which $T_i(g_\infty)$ is an n-cycle, $i=1,2$.

From [CKS76], the classification of finite simple groups [Gor82] yields the classification of all simple groups with a faithful doubly transitive representation. In particular, it lets us us draw the following conclusions.

Theorem 9.1. *If* (9.1) *holds, then either* $n = 11$ *and* $G = PSL(2, \mathbb{Z}/11)$ *or* $PSL_k(\mathbb{F}_q)$ *with* $n = (q^k - 1)/(q - 1)$ *for some* $k \geq 3$ *and* $q = p^t$ *for some prime* p.

Assume in addition, (4.6) *holds. Then, possible degrees of newly reducible (*§4.5*) polynomial pairs* (f, g) *with* f *indecomposable are exactly 7, 11, 13, 15, 21 and 31.*

9.1. **Proof of Thm. 9.1.** Our argument here quotes from [Fei70], [Fei73] ([Mül95] corrects an error in this paper), [Fei80] and [Fri80]. The general linear group $\mathrm{GL}(k, \mathbb{F}_q)$ acts on $\mathbb{F}_q^k$. Denote the group generated by $\mathrm{GL}(k, \mathbb{F}_q)$ and the pth-power map on the coordinates by $\Gamma L(k, \mathbb{F}_q)$.

9.1.1. *Action of* $\mathbb{P}^{k-1}$. Let $\mathbb{P}^{k-1}(\mathbb{F}_q)$ be the points of projective $k-1$-space with coordinates in $\mathbb{F}_q$. Then $P\Gamma L(k, \mathbb{F}_q)$ is the quotient of $\Gamma L(k, \mathbb{F}_q)$ induced by the action of $\Gamma L(k, \mathbb{F}_q)$ on the points of $\mathbb{P}^{k-1}(\mathbb{F}_q)$. Finally, $\mathrm{PSL}(k, \mathbb{F}_q)$ (resp. $\mathrm{PGL}(k, \mathbb{F}_q)$ is the image in $P\Gamma L(k, \mathbb{F}_q)$ of the subgroup $\mathrm{SL}(k, \mathbb{F}_q)$ of matrices of determinant 1 (resp. of $\mathrm{GL}(k, \mathbb{F}_q)$). We replace $\mathbb{F}_q$ by q below.

9.1.2. *Tying together references.* The first sentence of the theorem is from [CKS76]. The second sentence is outlined in [Fri80, p. 592], and completed in detail in [Fei70, Theorem 4]. These include simple demonstrations that possible branch cycles occur only in $(S_n)^r$ with $r = 3$ or 4 and that $r = 4$ only if $n = 7$ or 13. This uses the Riemann-Hurwitz conditions (4.6) and that the doubly transitive designs are those listed in the statement of the theorem. Thus, this is dependent on the classification of finite simple groups.

9.2. **Exceptional groups.** The following groups occur [Fei73]: $n = 11$ and $G = PSL(2, \mathbb{Z}/11)$; and $G = PSL(k, q)$ with $(k, q) = (3, 2), (4, 2), (5, 2), (3, 3)$ and $P\Gamma L(3, 4)$, exactly the examples that had been produced previously by the author and explained to W. Feit in their original correspondence. The degree 11 *nonstandard* representations of $PSL(2, \mathbb{Z}/(11))$ arise from an *Hadamard design* [Hal67, p. 291, item #5 in Table 1]. The author produced this with an approach that let combinatorics lead the way. Without knowing there was a design of degree 11, he looked for a difference set—whose existence came from [Fri73a, p. 134-135]. Having found it, the author then looked in [Hal67] where he found this special degree 11 design. Since no other unusual designs—outside projective linear groups—had produced variables separated factorization, the author ventured they didn't exist, a fact that agreed with their absence in the literature.

9.2.1. *Comments on work in the late 60's.* Feit, involved by late 1968 ([Fei73]), also considered the case $n = 13$—completed by the author exactly as done in List B above—using characters (the structure constant formula). For these low degrees, by hand calculation using difference sets seemed especially efficient, especially in the case $n = 11$. Around the same time, [Cas68] reported on work in England on the factorization of variables separated polynomials. They used neither Riemann's Existence Theorem nor doubly transitive groups, though D.J. Lewis told the author he had reported at Cambridge on the work that we describe here. Still, Birch and Guy had found the degree 11, but not the degree 13, case by hand factorization.

So far as we know, until J.-M. Couveignes [CaCo99] applied H. Cohen's program **Pari**, no one else has inspected the degree 13 examples in detail. I saw how [CaCo99, §5.3] presents this case as I was finishing this paper. You see the rubric in [CaCo99, p. 14]; the factorization $f(x) - h(y)$ comes from knowing there is a factorization and exploiting the Puiseux expansion around (∞, ∞). On the other hand, **Pari** does the work, based on some arbitrary programmer choices. Analyzing the relative work, and the place of presenting the final moduli space as a cover of the j-line requires more thought on my part. Since [CaCo99, §5.4] also has the degree 15 case, [Fri] will use this to compare exclusive use of the moduli method with exploiting the coefficients of these polynomials using **Pari**. [CaCo99] finds representative branch cycles using **Pari** after it has found polynomial equations. That is, this justifiable method almost entirely avoids any group theory, or even checking Nielsen classes.

9.2.2. *The case $n = 31$.* Eliminating $(k, q) = (3, 5)$ goes like this. In the action of the group on $\mathbb{P}^2(\mathbb{F}_5)$ [Fri80, p. 592] reduces to $r = 3$, g_1 is of order 2, g_2 is of order 3, and $\text{ind}(g_1) = (31-5)/2 = 13$. From (4.6) conclude $\text{ind}(g_2) = 17$, a contradiction to g_2 of order 3. Thus, $n = 31$ arises from collineations acting on the points of $\mathbb{P}^4(\mathbb{F}_2)$. We easily find elements g_1 and g_2 of order 2 and 3 whose indices correctly sum to 30. Slight additional work guarantees they generate a transitive group. From these two conditions, an application of the Riemann-Hurwitz formula shows $g_1 g_2 = g_3^{-1}$ must have index $n - 1$. Thus it is an n-cycle. The alternative procedure of [Fei73] uses the character table to show that in certain conjugacy classes represented by elements g_1 and g_2 of order 2 or 3 there are elements g_1' and g_2' whose product is an n-cycle. Feit's method has the advantage it automatically identifies the group $\langle g_1, g_2 \rangle$ as a particular subgroup of $P\Gamma L(k, \mathbb{F}_q)$.

10. Polynomials with Frey-type Irreducibility

Recall the question from §2.4.

Question 10.1. Are there polynomials f for which $\mathcal{R}_f(d) \setminus \mathcal{V}_f(d)$ is finite?

Of course, there is an analog question for $\mathcal{R}_f(1, d') \setminus \mathcal{V}_f(1, d')$. At this stage the goal, dependent on d (or d'), will be only to find polynomials of arbitrary large degree satisfying the conclusion of Question 10.1. As there, let $M_d = \{\alpha \in \bar{\mathbb{Q}} \mid [\mathbb{Q}(\alpha) : \mathbb{Q}] \le d\}$.

10.1. **The covering space setup.** Consider any $\mathbb{Q}$ cover $\varphi : X \to \mathbb{P}^1_z$. Lemma 2.9 says we need to show the following for each $2 \le k \le n-2$:

(10.1) no $\mathbb{Q}$ component of $Y_k = X^{(k)}_{\mathbb{P}^1_z}/S_k$ has infinitely many M_d points.

Let C be one of the $\mathbb{Q}$ irreducible components of Y_k. For any integer t, form the symmetric product $C^{(t)} = \overbrace{C \times \cdots \times C}^{t \text{ times}}/S_t$. This is a full symmetric product, not a fiber product; $C^{(t)}$ is the set of positive divisors of degree t on C. Suppose C has a point in $\bar{\mathbb{Q}}$ of degree t over $\mathbb{Q}$. Then, the unordered collection of conjugates of this point have coordinates on $C^{(t)}$ in $\mathbb{Q}$. Repeating this unordered collection of conjugates u times produces a $\mathbb{Q}$ point in $C^{(tu)}$. The following is a variant of the argument of [Fre94].

Theorem 10.2. *Suppose C above has infinitely many points over fields of degree at most d over $\mathbb{Q}$. Then, the symmetric product of $C^{(t)}$ for some $t \le d$ has infinitely many $\mathbb{Q}$ points. Conclude there exists a map $\psi : C \to \mathbb{P}^1_w$ of degree at most $2d$.*

§10.2 outlines the proof of this. As with using Siegel's Theorem in previous sections, its realiance on Faltings' proof of Lang's conjecture [Fal95] is not effective. §10.3 produces polynomial maps $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ ($X = \mathbb{P}^1_x$), $\deg(f) = n$, where Y_k is irreducible and it supports no function of degree at most 2d, $2 \le k \le n-2$. Arbitrarily large values of n work, though we don't show it for *all* large values of n. Our construction will start with a polynomial $\bar{f}$ over a suitable finite field $\mathbb{F}_q$ (of characteristic p). Then, the polynomials f have their reduction equal to $\bar{f}$. Thus, we can assure constructions of objects from f (like fiber products) reduce modulo p, and have for their reduction the corresponding construction in positive characteristic. To go along with this, assume C above has good reduction modulo some prime p. Frey's construction also assumes it has a $\mathbb{Q}$ point.

10.2. **Applying Faltings' Theorem.** Let $\mathrm{Pic}^t(C)$ be the linear equivalence class of divisors of degree t on C. Since C is a projective nonsingular curve, $\mathrm{Pic}^t(C)$ is a projective nonsingular variety of dimension $g = g(C)$. It is isomorphic, after some, possibly nontrivial, finite extension of $\mathbb{Q}$ to the jacobian variety of C. If C has a rational point c_0 you can use that to give the isomorphism over $\mathbb{Q}$: translate $\mathrm{Pic}^t(C)$ by $-tc_0$ to get a $\mathbb{Q}$ isomorphism with $\mathrm{Pic}^0(C)$, which we identify with the Jacobian of C. Without a $\mathbb{Q}$ point on C, you must consider the relation between $\mathrm{Pic}^t(C)$ and $\mathrm{Pic}^0(C)$ one integer t at a time. On the other hand, if t is a multiple of $2g(C) - 2$ you can always use translation by a multiple of the canonical class (always $\mathbb{Q}$ rational).

For any integer t, there is a natural map $\Phi^{(t)} : C^{(t)} \to \mathrm{Pic}^t(C)$: map a positive divisor to the linear equivalence class of the divisor [Mum66b, p. 133]. This map isn't *flat* if t is small; the dimension of the fibers varies. Suppose, $\Phi^{(t)}$ is not injective on $C^{(t)}$. Let $m \in \mathrm{Pic}^t(C)(\mathbb{Q})$ for which $F_m = (\Phi^{(t)})^{-1}(m)$ is neither empty nor a point. Then, $(\Phi^{(t)})^{-1}(m)$ is a copy of projective space, representing the linear system of divisors in the equivalence class represented by m.

10.2.1. *Reduction to $\Phi^{(t)}$ injective on $\mathbb{Q}$ points.* Even with all these maps defined over $\mathbb{Q}$ we can only assert F_m is isomorphic to a positive dimensional projective space over some finite extension of $\mathbb{Q}$. On the other hand, with just one $\mathbb{Q}$ point on F_m, this *Brauer-Severi variety* is automatically isomorphic to projective space. Further, you can join two $\mathbb{Q}$ points of F_m by a line L over $\mathbb{Q}$. Then, there is a natural map from C to L: map a geometric point $c \in C$ to the divisor in the linear system L containing c. (Modify this accordingly if L contains base points.) The degree of the map is the degree of the divisors in L after you have removed base points. This gives the following conclusion.

Lemma 10.3. *For some $t \le d$, $C^{(t)}(\mathbb{Q})$ is infinite if and only if C has infinitely many points of degree at most d over $\mathbb{Q}$. Suppose $\Phi^{(t)}$ is not injective on $\mathbb{Q}$ points. Then, there exists a nonconstant $\mathbb{Q}$ map of C to $\mathbb{P}^1$ of degree at most t.*

Our goal is to conclude from $|C^{(t)}(\mathbb{Q})| = \infty$ that there is a low degree map from C to $\mathbb{P}^1$. So, if we already know C has a low degree map (over $\mathbb{Q}$) we are done for this part of the argument. Thus, the basic assumption is this:

(10.2) $\Phi^{(t)}$ is injective on $C^{(t)}(\mathbb{Q})$.

If (10.2) holds, then $C^{(t)}(\mathbb{Q})$ infinite implies $\Phi^{(t)}(C^{(t)})(\mathbb{Q}) = W(t)(\mathbb{Q})$ infinite.

10.2.2. *Frey's argument applying Faltings' Theorem.* In this subsection, let $n(d)$ be the number of solutions of $\sum_{i=1}^{d} e_i = d$ with $e_i \in \{0,1,2\}$.

Proposition 10.4 ([Fre94])**.** *Assume there exists $\boldsymbol{p} \in C^{(d)}(\mathbb{Q})$ and at least $n(d)+1$ points $b_0, \dots, b_{n(d)} \in \mathrm{Pic}^0(\bar{\mathbb{Q}})$ such that $\Phi^{(d)}(\boldsymbol{p}) \pm b_i \in W(d)$. Then, there is a $\mathbb{Q}$ cover $\pi : C \to \mathbb{P}^1$ of degree at most $2d$.*

Proof. Denote $\Phi^{(d)}$ by Φ. Suppose $\Phi(\boldsymbol{p}) + b_i$ and $\Phi(\boldsymbol{p}) - b_i$ are both in $W(d)$. So, $2\boldsymbol{p} = \sum_{i=1}^{d} R_i + \sum_{i=1}^{d} Q_i = \mathcal{R} + \mathcal{Q}$. Here, the R_is and Q_is are points on C. Suppose the P_is in $\boldsymbol{p}$ are distinct. Denote the number of appearances of P_j in $\mathcal{Q}$ by e_j. Then, $e_j \le 2$, and the sum of e_js is d. So the number of $\mathcal{Q}$s for which there exists $\mathcal{R}$ is $n(d)$. If the P_js aren't distinct, the number is at most $n(d)$.

Since b_is are distinct, there exists at least one for which $\mathcal{Q} + \mathcal{R} \ne 2\boldsymbol{p}$, though $\mathcal{Q} + \mathcal{R}$ is linearly equivalent to $2\boldsymbol{p}$. Thus, $L(2\boldsymbol{p}) > 1$ and there exists $C \to \mathbb{P}^1$ of degree at most $2d$. □

Corollary 10.5. *Suppose for $\boldsymbol{p} \in C^{(d)}(K)$, $W(d)_{-\Phi(\boldsymbol{p})}$ (the set translated by $\Phi(\boldsymbol{p})$) contains a subgroup T of $\mathrm{Pic}^0(\bar{\mathbb{Q}})$ of order exceeding $n(d)$. Then C has a $\mathbb{Q}$ map to $\mathbb{P}^1$ of degree at most $2d$, and reduction of C modulo p has at most $2d(q+1)$ over the finite field $\mathbb{F}_q$. These conclusions hold if $W(d)(\mathbb{Q})$ is infinite.*

Proof. Add $\Phi(\boldsymbol{p})$ to the points of T to conclude from Prop. 10.4. Suppose $C \to \mathbb{P}^1$ has degree at most $2d$ over $\mathbb{F}_q$. Then, bound the $\mathbb{F}_q$ points on C by the worst case: each of the $q+1$ points of $\mathbb{P}^1(\mathbb{F}_q)$ has a totally split fiber. This bound gives no more than $(q+1)2d$ points on C. [Fre94, Cor. 2] quotes Deuring's reduction theory: If $\varphi : X \to \mathbb{P}^1$ with X having good reduction, then the morphism φ reduces, too.

Now we use G. Faltings [Fal95] on the hypothesis that $W(d)(\mathbb{Q})$ is infinite. The conclusion is the following hold.

(10.3a) $W(d)$ contains the translate of an abelian variety A.

(10.3b) $\mathbb{Q}$ is a field of definition for the translating divisor, $\mathrm{Pic}^0(C)$ and infinitely many of its points.

If $b \in A$ is a rational point, then so is $-b$ in A, and so both $\Phi(\boldsymbol{p}) \pm b$ are in $W(d)$. Thus, the hypotheses of the first part apply if $W(d)(\mathbb{Q})$ is infinite. □

Remark 10.6 (Frey's modular curve application). The curve C in Frey's application was the modular curve $X_0(p^u)$. Let r be a prime different from p, so the modular curve has good reduction. Take any finite field $\mathbb{F}'$ containing $\mathbb{F}_r$. His goal was to show $X_0(p^u)$ has only finitely many points in fields of degree at most d over $\mathbb{Q}$, if p^u is suitably large. The reduction from Cor. 10.5 is that if not, $|X_0(p^u)(\mathbb{F}')|$ is at most $(|\mathbb{F}'|+1)2d$ for all p^u. Take, however, $r = 2$, and $\mathbb{F}'$ the quadratic extension of $\mathbb{F}_r$. Then, [Iha75] (or [Rob73, pgs. 226–239]) shows $X_0(p)(\mathbb{F}')$ has at least $\left[\frac{p^n}{12}\right] + 1$ points. These points derive from *supersingular elliptic curves* for the prime 2. Supersingular curves have defining field the quadratic extension of $\mathbb{F}_2$. This contradiction gives explicit bounds on exceptional values of p^u.

10.3. **Finding f satisfying Question 10.1 conclusion.** Assume $f : \mathbb{P}^1 \to \mathbb{P}^1$ has simple branching. The group of the cover is S_n, and the k-times fiber products are all irreducible.

Question 10.7. Given $f \in \mathbb{Q}[x]$, a simple branched cover of the sphere, how can we assure the curves Y_k below have no low degree map to $\mathbb{P}^1$?

Take any polynomial f over the finite field $\mathbb{F}_q$. Let $f^{(k)} : Y_k = (\mathbb{P}^1_x)^{(k)}_{\mathbb{P}^1_z} \to \mathbb{P}^1_z$ be the kth fiber product of this cover, $2 \le k \le n-2$. From Cor. 10.5, we have only to show that for some f, $Y = Y_k = (\mathbb{P}^1_x)^{(k)}$ has more than $(q+1)\cdot 2d$ points. For example, this would follow if all finite values of x lie over a common value of z. Then, there would be at least $q(q-1)\cdots(q-k+1)/|k!|$ points on Y_k (all lying over the same value of z). The following lemma arranges this for a positive answer to Question 10.1.

Lemma 10.8. *Suppose $n = q+1$ for q large enough that $q(q-1)/2$ exceeds $2d(q+1)$. Then, there exists f over $\mathbb{F}_q$ with simple branching of degree at n and $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ has a fiber consisting of exactly q rational values of x. In particular, these f give an affirmative answer to Quest. 10.1, assuring an affirmative answer to Quest. 10.7.*

Proof. Check the zeros of the derivative of $f(x) = (x^q - x)(x+b)$: $x^q - 2x - b$. This has no multiple roots (take the derivative). Now consider if the roots of f' give distinct values when plugged back into f. If x_0 is such a root, then we are asking if $(x_0+b)^2$ runs over distinct values if the x_0 runs over these roots. That is, if x_1 and x_0 are both roots of f', could $x_0 + b = -(x_1 + b)$? That is, $x_1 = -x_0 - 2b$. This gives a relation: $(-2b)^q - 2(-2b) = 0$. Assume $b \neq 0$ and 2 not 0, then the equation says $-2b + 4b = 0$, or we are fine. Thus, $f(x)$ is a polynomial satisfying the desired hypotheses. □

11. Problems from Variables Separated Polynomials

Recent literature brings up interesting problems forcing us to inspect from whose viewpoint Thm. 2.11 is explicit. Equations of the form

$$x(x+a)\dots(x+(k-1)a) = y(y+b)\dots(y+(m-1)b), \tag{11.1}$$

the subject of [BST99], do not explicitly appear in [Fri73b]. So, one must exclude the short list of exceptional cases of degree at most six listed in Theorem 3 and its Corollary. This, by the way is immediate if you know $\frac{df}{dx}$ has only simple zeros, for the exceptions don't have this property. That leaves only checking that (11.1) does not include polynomials linearly equivalent to Chebyshev polynomials.

11.1. **Comments on** [BST99]**.** [BST99] shows (11.1) has only finitely many integer (or rational) solutions, excluding a few exceptional cases. Further, they inspect those exceptional cases. As §2.1 notes [Fri73b, Cor. on p. 47] reduces the problem of integral solutions to one of two cases:

(11.2a) either their equaton is one of the items listed in [Fri73b, Thm. 3]; or
(11.2b) f(x)-h(y) has a factor of degree 1 or 2.

The reductions are especially easy when the cover $f : \mathbb{P}^1_x \to \mathbb{P}^1_z$ is a simple branched cover. That, by the way, is equivalent to it having $\deg(f)$ distinct branch points (including ∞). It is easy to see this holds when f (in (11.1)) has odd degree: Rolle's theorem and an induction. It is harder, when $\deg(f)$ is even. Reason: f is composite; from a slight change of variables with a quadratic polynomial. Accepting this, the analysis is the same, and the other composite of f has the symmetric group as monodromy group. Here, however, [BST99] tested a stronger possibility: Does (11.1) have a genus 1 factor.

This is beyond what [Fri73b] considered, though they only do this for their special equation (11.1). [BST99, Prop. 5] identifies from their equations some genus one

curves. To show these particular equations have infinitely many rational points they use Mazur's Theorem. The rational torsion of an elliptic curve over $\mathbb{Q}$ is either $\mathbb{Z}/(n)$ with n between 1 and 12 (excluding 11) or it is $\mathbb{Z}/(2)\times\mathbb{Z}/(2n)$ with $n=1,2,3,4$. The inflection points of their curves are clear and there is a convenient rational inflection point in each case. Further, each case has several obvious rational points, and they use the degree 3 linear system to find a third rational point by drawing a line through any two.

Would [Fri73b] allow finding all the genus 0 and 1 factors of variables separated equations? For our present knowledge, that would require an assumption bounding the numbers of composition factors in one of f or h to use the strongest irreducibility results (as in Thm. 4.8), those assuming f is indecomposable. Müller's extension of Davenport's problem (in 0 characteristic) to the case f has at most two composition factors is a result in this direction (§11.5). What is most interesting is that beyond the examples we already knew (with f indecomposable), the new examples are of the form $(f(f_1), f(h_1))$ with f_1 (and h_1) indecomposable.

11.2. **Comments on** [Haj98] **and** [Haj97]**.** Consider

$$\begin{array}{ll} f_n(r)= & |\{(x_1,\dots,x_n)\in\mathbb{Z}^n : |x_1|+\cdots+|x_n|\le r\}| \\ & n=0,1,2,\dots \text{with specific cases :} \\ f_1(r)= & 2r+1,\ f_2(r)=2r^2+2r+1,\ f_3(r)=\frac{4}{3}r^3+2r^2+\frac{8}{3}r+1; \\ & \text{and } f_4(r)=\frac{2}{3}r^4+\frac{4}{3}r^3+\frac{10}{3}r^2+\frac{8}{3}r+1. \end{array} \tag{11.3}$$

Hajdu verifies f_n has degree n, and for $n\ge 1$ there is the following recursion:

$$f_n(r)=2\sum_{k=0}^{r-1} f_{n-1}(k) \ + \ f_{n-1}(r).$$

[Haj98] explicitly considers the (elliptic curve) equation $f_2(r)=f_n(R)$ for $n=3,4$, finding all the solutions. It cites a lemma based on Baker's Theorem; in principle finding all the integer points on an elliptic curve E.

[Haj97] considers the more general equation: $f_k(r)=f_n(R)$ completely solving the case where $(k,n)=(3,4)$ and $(4,6)$. There is a remark that [BP] obtained finiteness results concerning the solutions of equations of the type $f(x)=g(y)$, where f and g are polynomials with integer coefficients. The implication of [Haj97] is that since f and g are special in [BP], it is not applicable for these equations. Of course, as previously, if the equations are important, then the first question must be for which (k,n) are there infinitely many integral solutions, and there is plenty of data here to take the list of [Fri73b] as a guide.

11.3. **Reducibility of $f(x)-h(y)$ when f is composite.** Consider how to locate the Davenport-Lewis example ([Fri87, p. 18]) from the viewpoint of the monodromy method (§3). In this case, f has degree 4, and the geometric monodromy group G has two inequivalent representations of degree 4. It also contains a 4-cycle from ramification over ∞. It's not A_4 or S_4 (only one degree 4 representation). Quick inspection shows the only possibility is D_4, with the representations corresponding to coset representations on the *two* conjugacy classes of involutions. Take the corresponding groups to be H_f and H_h. Since H_f has order 2, it is intransitive on the four cosets of H_h. This translates to reducibility. The branch cycles have these shapes: $((2),(2)(2),(4))$ in one representation, and $((2)(2),(2),(4))$ in the other. You realize these examples from the Chebyshev polynomial T_4 of degree 4:

$T_4(x) = f(x)$ and $-T_4(x) = h(x)$. What stands out is that this newly reducible (§4.5) variables separated polynomial has f decomposable. In characteristic 0, apparently such examples happen rarely. §11.4, however, shows how difficult it has been to establish this, precisely because we haven't found a reduction of this problem to the primitive case.

11.4. **The (n, m) problem.** [Fri87] has only two sections. The first gives a two page proof that if you have *three* separated variables in a rational function, then the resulting rational function is irreducible. [Fri87, §2], however, describes how ignorant we are about variables separated factorization of $f(x) - h(y)$ when f is *decomposable*. The (n, m)-problem, applying to the case when f and g are polynomials, asks the following.

Question 11.1. Suppose f_1 and h_1 are any polynomials of respective degrees n and m. Are there polynomials f_2 and h_2 for which $f_1(f_2(x)) - h_1(h_2(y))$ is reducible?

Lemma 11.2. *To get an affirmative answer to Question 11.1 it suffices to consider any pair (f_1, h_1) satisfying these conditions.*

(11.4a) *Finite branch points for the covers $f_1 : \mathbb{P}^1_x \to \mathbb{P}^1_z$ and $h_1 : \mathbb{P}^1_y \to \mathbb{P}^1_z$ have attached branch cycles that are 2-cycles.*

(11.4b) *Finite branch points of f_1 are disjoint from finite branch points of h_1.*

Proof. Suppose there is an affirmative answer to Question 11.1 for some particular (f_1, h_1) satisfying conditions (11.4). Consider a branch cycle description of the function field $\Omega_{f_1 - z}\Omega_{h_1 - z} = \Omega$. Let $\boldsymbol{z}_f$ be the set of branch points of a cover given by a rational function f. Here are properties of a branch cycle description of the cover associated with $\Omega/K(z)$, when you compute it relative to some admissible set of paths on $\mathbb{P}^1_z \setminus \boldsymbol{z}_{f_1} \cup \boldsymbol{z}_{h_1}$. It consists of an $n_1 + m_1 - 1$-tuple $(g_1, \ldots, g_{n_1 - 1}, g'_1, \ldots, g'_{m_1 - 1}, g_\infty)$. Further, if g is one of g_i (or g'_i; or g_∞), then g restricts to Ω to have the form $(T_{f_1}(g), T_{h_1}(g))$ with the following properties.

(11.5a) $T_{f_1}(g_i)$ is a 2-cycle in S_{n_1}, $i = 1, \ldots, n_1 - 1$;
(11.5b) $T_{f_1}(g'_i)$ is the identity, $i = 1, \ldots, m_1 - 1$;
(11.5c) $T_{h_1}(g'_i)$ is a 2-cycle in S_{m_1}, $i = 1, \ldots, m_1 - 1$;
(11.5d) $T_{h_1}(g_i)$ is the identity, $i = 1, \ldots, n_1 - 1$; and
(11.5e) $T_{f_1}(g_\infty)$ is an n_1-cycle, and $T_{h_1}(g_\infty)$ is an m_1-cycle.

□

An affirmative answer to the (2,2) problem is easy from §11.3 ([Fri87, p. 17]). After that, it is hard, and the remainder of the section concentrates on the (2,3) problem, noting from [Fri73a, Lemma 7] we may assume $f_1 = x^2$, $g_1 = y(y + 1)(y + 2)$, and $\deg(f_2) = 3k$, $\deg(h_2) = 2k$, for some integer k. While the final result eliminates $k = 1$ and $k = 2$—and the latter is hard work—it isn't conclusive. Also, there was a near miss. So, it is not clear whether to expect an affirmative or negative answer to the (2,3)-problem. Riemann's Existence Theorem—the main tool I was pushing—makes everything completely group theoretic.

Finally, [Fri87, p. 17] points out we don't even know if there are infinitely many pairs of integers (n, m) for which there are *newly reducible* polynomial pairs (f, g) (an appropriate definition for this resonant problem). For, however, the rational function version of this problem, it is easy to say more. [Fri87, Ex. 2.4] gives the

pairs $(n, n(n-1)/2)$ for the production of newly reducible rational function pairs of these degrees.

11.5. **Mueller's results extending Davenport's problem.** Work related to the monodromy method, from the proof of the Schur conjecture, through the genus 0 and (n, m)-problems, shows how much harder it is to work with permutations representations that aren't primitive.

Two places occur where it was not feasible to assume primitive geometric monodromy group. One is in the problems in positive characteristic, like describing exceptional polynomials as in [FGS93]. If the characteristic divides the degree, then the conclusion of Lemma 4.1 no longer applies. In the description of exceptional polynomials we may assume the arithmetic monodromy group (in its natural covering representation) is primitive. Yet, we can't assume the same for the geometric monodromy group.

Even more serious is the problem in [Mül98] where Müller has gone after finding exceptions (over $\mathbb{Q}$) to Davenport's problem from polynomials with exactly two composition factors. His list [Mül98, p. 25] considers $f(x) = a(b(x)) \in K[x]$ with K a number field, and neither a nor b are strongly Kronecker conjugate over K to another polynomial. In these cases h is of form $a(b'(x))$, and he lists the small number of groups that arise for this situation. Note: b and b' are not Kronecker conjugate. Still, he notes [Mül98, p. 27] an old acquaintance from Lemma 4.5: T_h and T_f are equivalent as group representations in all examples that appear to date. Finally, he leaves a conjecture that has survived a decade of group theory.

Conjecture 11.3. Let $f, g \in \mathbb{Q}[x]$ be strongly Kronecker polynomials over $\mathbb{Q}$. Then, they are either linearly equivalent or $f(x) = g(x^8)$ and $h = g(ay^8)$ for some polynomial $g \in \mathbb{Q}[x]$ and constant a.

References

[Abh97] S.S. Abhyankar, *Projective polynomials*, Proc AMS **125** (1997), 1643–1650.

[AS85] M. Aschbacher and L. Scott, *Maximal subgroups of finite groups*, J. Alg. **92** (1985), 44–80.

[BST99] F. Beukers, T.N. Shorey and R. Tijdiman, *Irreducibility of polynomials and arithmetic progressions with equal products of terms*, Zakopane Conference on Number Theory, 1999, Proceedings of the Schinzel Festschrift, Summer 1997.

[BF82] R. Biggers and M. Fried, *Moduli spaces of covers and the Hurwitz monodromy group*, Crelles Journal **335** (1982), 87–121.

[BP] B. Brindza and Á. Pintér, *On the irreducibility of some polynomials in two variables*, Acta Arith. 18 (1997), 303-307.

[Cas68] J.W.S. Cassels, *Factorization of polynomials in several variables*, Proc. 15th Scand. Congress Oslo (1968), 1–17.

[CKS76] C.W. Curtis, W.M. Kantor and G.M. Seitz, *The 2-transitive permutation representations of the finite Chevalley groups*, TAMS **218** (1976), 1–59.

[Coh90] S. Cohen, *Exceptional polynomials and the reducibility of substitution polynomials*, L'Enseigment Math. **36** (1990), 309–318.

[CaCo99] M. Couveignes and P. Cassou-Nogues, *Factorisations explicites de $g(y) - h(z)$*, Acta. Arith., based on talk Zakopane Conference on Number Theory, 1999, Proceedings of the Schinzel Festschrift, Summer 1997, to appear.

[DLS61] H. Davenport, D.J. Lewis and A. Schinzel, *Polynomials of the form $f(x) - g(y)$*, Quart. J. Math. **Oxford (2) 12** (1961), 304–312.

[DLS64] H. Davenport, D.J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. **9** (1964), 107–116.

[DF90] P. Debes and M. Fried, *Arithmetic variation of fibers in families: Hurwitz monodromy criteria for rational points ...*, Crelles J. **409** (1990), 106–137.

[DF99] P. Debes and M. Fried, *Integral specialization of families of rational functions*, PJM (1999).

[Dri73] V. G. Drinfeld, *Two theorems on modular curves (in russian)*, Funk. Anal. I Prilozhen **7** (1973), 83–84.

[Fal95] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. Math. (2) 133 (1991), 549–576.

[FB98] M. Fried and G. Berger, *Rational cusps on noncongruence towers of the j-line*, Preprint in preparation.

[Fei70] W. Feit, *Automorphisms of symmetric balanced incomplete block designs*, Math. Zeit **118** (1970), 40–49.

[Fei73] W. Feit, *On symmetric balanced incomplete block designs with doubly transitive automorphism groups*, J. of Comb. Theory **14** (1973), 221–247.

[Fei80] W. Feit, *Some consequences of the classification of finite simple groups*, Santa Cruz Conference on Finite Groups, vol. 37, 1980, Proceedings of Symposia in Pure Math:, A.M.S., pp. 175–181.

[FJ86] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik III, vol. 11, Springer Verlag, Heidelberg, 1986.

[FM98] D. Frohardt and K. Magaard, *The Guralnick/Thompson conjecture for groups of bounded genus*.

[Fre94] G. Frey, *Curves with infinitely many points of fixed degree*, Israel J. **85** (1994), 79–83.

[Fri] M. Fried, *Moduli problems attached to Frey-type irreducibility*, preprint; includes the remainder of [Fri86].

[Fri70] M. Fried, *On a conjecture of Schur*, Mich. Math. J. **17** (1970), 41–55.

[Fri73a] 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.

[Fri73b] M. Fried, *A theorem of Ritt and related diophantine problems*, Crelles J. **264** (1973), 40–55.

[Fri74] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory **6** (1974), 128–146.

[Fri77] M. Fried, *Fields of definition of function fields and Hurwitz families and groups as Galois groups*, Communications in Algebra **5** (1977), 17–82.

[Fri80] M. Fried, *Exposition on an arithmetic-group theoretic connection via Riemann's existence theorem*, Santa Cruz Conference on Finite Groups, vol. 37, 1980, Proceedings of Symposia in Pure Math:, A.M.S., pp. 571–601.

[Fri86] M. Fried, *Applications of the classification of simple groups to monodromy, Part II: Davenport and Hilbert-Siegel problems*, preprint (1986), 1–55.

[Fri87] M. Fried, *Irreducibility results for separated variables equations*, J. of Pure and Applied Alg. **48** (1987), 9–22.

[Fri90] M. Fried, *Arithmetic of 3 and 4 branch point covers: a bridge provided by noncongruence subgroups of* $\mathrm{SL}_2(\mathbb{Z})$, Progress in Math. Birkhauser **81** (1990), 77–117.

[FGS93] M. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel J. **82** (1993), 157–225.

[Fri94a] M. Fried, *Global construction of general exceptional covers, with motivation for applications to encoding*, Cont. Math., vol. 168, pp. 69–100, AMS, Rhode Island, Editors G.L. Mullen an P.J. Shiue, 1994, Finite Fields: Theory, applications and algorithms.

[Fri94b] M. Fried, *review—Topics in Galois theory, J.-P. Serre*, BAMS **30 #1** (1994), 124–135, 1992, Bartlett and Jones Publishers, ISBN 0-86720-210-6.

[Fri95a] M. Fried, *Enhanced review: Serre's* Topics in Galois theory, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 15–32.

[Fri95b] M. Fried, *Extension of constants, rigidity, and the Chowla-Zassenhaus conjecture*, Finite Fields and their applications; Carlitz Volume **1** (1995), 326–359.

[Fri95c] M. Fried, *Introduction to modular towers: Generalizing the relation between dihedral groups and modular curves*, Proceedings AMS-NSF Summer Conference, vol. 186, 1995, Cont. Math series, Recent Developments in the Inverse Galois Problem, pp. 111–171.

[Fri96] M. Fried, *Alternating groups and lifting invariants*, Preprint as of 07/01/96 (1996), 1–34.

[FKK98] M. Fried, E. Klassen and Y. Kopeliovic, *Alternating groups as monodromy groups of generic genus one covers of the sphere*, PJM (1998).

[Frö67] A. Fröhlich, *Local fields*, vol. Algebraic Number Theory, ch. The ramification groups, pp. 33–39, Thompson Book Co. and Academic Press, 1967, Editor J. W. S. Cassels.

[Ful69] W. Fulton, *Hurwitz schemes and irreducibility of moduli of algebraic curves*, Annals of Math. **90** (1969), 542–575.

[FV91] M. Fried and H. Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Annalen **290** (1991), 771–800.

[GM98] R. M. Guralnick and K. Magaard, *Primitive permutation groups containing elements that fix at least half the points*, J. Algebra (1998), to appear.

[GN95] R. M. Guralnick and M. G. Neubauer, *Monodromy groups of branched coverings: the generic case*, Recent developments in the inverse Galois problem, vol. 186, Amer. Math. Soc., 1995, Contemp. Math, pp. 325–352.

[Gor82] D. Gorenstein, *Finite simple groups; an introduction to their classification*, Academic Press, 1982, New York.

[Gro59] A. Grothendieck, *Geometrie formelle et geometrie algebrique*, Seminaire Bourbaki **182** (1959).

[GS95] R.M. Guralnick and J. Saxl, *Monodromy groups of polynomials in groups of Lie type and their geometries*, London Math. Soc. Lecture Note Ser., vol. 207, pp. 125–150, Cambridge Univ. Press, Cambridge, 1995, Proceedings of the Como Conference, 1993.

[GS98] R. M. Guralnick and J. Shareshian, *On the genus of representations of the symmetric groups and coverings by generic Riemann surfaces*, in preparation.

[GT90] R.M. Guralnick and J.G. Thompson, *Finite groups of genus 0*, J. Alg. **131** (1990), 303–341.

[Gur97] R. Guralnick, *Some applications of subgroup structure to probabilistic generation and covers of curves*, preprint.

[Haj97] L. Hajdu, *On a diophantine equation concerning the number of integer points in special domains II*, Publ. Math. Debrecen **51 (3-4)** (1997), 331–342.

[Haj98] L. Hajdu, *On a diophantine equation concerning the number of integer points in special domains*, Acta. Math. Hungar. **78 (1-2)** (1998), 59–70.

[Hal67] M. Hall, *Combinatorial theory*, Blaisdell Pub. Co., 1967.

[Har77] R. Hartshorne, *Algebraic geometry*, Graduate Texts in Math., vol. 52, Springer-Verlag, 1977.

[Iha75] Y. Ihara, *On modular curves over finite fields*, Studies in Math., vol. 7, pp. 161–202, Oxford Univ. Press, Jan. 1975, Proc. Intern. Colloq. on Discrete Subgroups on Lie Groups, Bombay.

[Isa94] I. M. Isaacs, *Algebra, a graduate course*, 1st ed., Brooks/Cole, Pacific Grove, California, 1994.

[LS91] M.W. Liebeck and J. Saxl, *Minimal degrees of primitive permutation groups, with an application to monodromy groups of Riemann surfaces*, Proc. London Math. Soc **(3) 63** (1991), 266–314.

[LS98] M.W. Liebeck and A. Shalev, *Simple groups, permutation groups, and probability*, Proc. London Math. Soc (1998).

[Mag93] K. Magaard, *Monodromy and sporadic groups*, Comm. Alg **21** (1993), 4271–4297.

[Man72] Y. Manin, *Parabolic points and zeta functions of modular curves (in russian)*, Izv. Akad. Nauk SSSR **36** (1972), 19–66.

[Mes90] J.-F. Mestre, *Extensions régulières de $\mathbb{Q}(t)$ de groupe de Galois $\tilde{A}_n$*, J. of Alg. **131** (1990), 483–495.

[Mül95] P. Müller, *Primitive monodromy groups of polynomials*, Proceedings of the Recent developments in the Inverse Galois Problem conference, vol. 186, 1995, AMS Cont. Math series, pp. 385–401.

[Mül96] P. Müller, *Reducibility behavior of polynomials with varying coefficients*, Israel J. **94** (1996), 59–91.

[Mül98] P. Müller, *Kronecker conjugacy of polynomials*, TAMS **350** (1998), 1823–1850.

[Mum66a] D. Mumford, *Introduction to algebraic geometry; The Red Book*, Harvard Lecture Notes, 1966.

[Mum66b] D. Mumford, *Lectures on curves on an algebraic surface*, Annals of Math Studies, vol. 59, Princeton U. Press, Princeton, 1966.

[Neu93] M. Neubauer, *On primitive monodromy groups of genus zero and one, I*, Comm. Alg. **21 (3)** (1993), 711–746.

[Rob73] A. Robert, *Elliptic curves*, Lecture Notes, vol. 326, Springer Verlag, Heidelberg, 1973; second edition 1986.

[Sch33] I. Schur, *Zur Theorie der einfach transitiven Permutationsgruppen*, S.-B. Press Akad. Wiss (1933), 598–623, Phys.-Math. Kl.

[Sch63] A. Schinzel, *Some unsolved problems on polynomials*, In: Neki nerešeni problemi u matematici (Mat. Bibl. 25), 63-70. Beograd 1963.

[Sch67] A. Schinzel, *Reducibility of polynomials of form* $f(x) - g(y)$, Coll. Math. **18** (1967), 213–218.

[Sch70] A. Schinzel, *Reducibility of polynomials*, Actes Cong. Intern. Math. **1** (1970), 491–496.

[Sch82] A. Schinzel, *Selected topics on polynomials*, no. ISBN #0-472-08026-1, University of Michigan Press, 1982.

[Ser67] J.-P. Serre, *Local Class Field Theory*, vol. Algebraic Number Theory, ch. Ramification subgroups and conductors, pp. 155–161, Thompson Book Co. and Academic Press, 1967, Editor J. W. S. Cassels.

[Ser92] J.-P. Serre, *Topics in Galois theory*, no. ISBN #0-86720-210-6, Bartlett and Jones Publishers, 1992.

[Ser97] J.-P. Serre, *Lectures on the Mordell-Weil theorem*, 3rd ed., Aspects of Mathematics, vol. 15, Friedr. Vieweg and Sohn, Max-Planck-Institut, Bonn, 1997, Translated and edited by Martin Brown from notes of Michel Waldschmidt.

[Sie29] C.L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Pr. Akad. Wiss. **1** (1929), 41–69.

[Völ96] H. Völklein, *Groups as Galois groups*, Cambridge Studies in Advanced Mathematics, vol. 53, Camb. U. Press, Camb. England, 1996.

UC Irvine, Irvine, CA 92697, USA

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